# DE4A Project: Towards a Single Digital Gateway for European Public Services

José Pascual Gumbau-Mezquita[1], Francisco José Aragó-Monzonís[2] and José Traver-Ardura[3]
[1] Universitat Jaume I, Spain
[2] Universitat Jaume I, Spain
[3] Universitat Jaume I, Spain
gumbau@uji.es, farago@uji.es, traverj@uji.es

**Abstract**

Single Digital Gateway regulation is settling the grounds for the effective cross-border interoperability of European public administrations at the data and business procedure levels. As the natural step beyond the basic cross-border authentication interoperability eIDAS regulation is currently bringing forward, a core set of common administrative procedures including higher-education related administrative procedures has been identified, and efforts in all member states are underway to analyse them and agree on a common set of specifications to allow a citizen from any European state to complete the procedure in another state without having to produce any physical documentation, and what's more important, nor digitalised copies of said documentation which increases fraud risk and would require additional validation efforts. This regulation will enable a safer, more trusted, quicker, less costly, and easier procedure both for the citizen and for the administrations. DE4A project is an initiative by a strong consortium of multiple state agencies and other stakeholders in different sectors, both public and private, including universities. The project goal is to experiment the feasibility of deploying and running those procedures in a real environment, to identify the pitfalls and gain practical knowledge on the legal, technical, operational and governance challenges that will be faced by the SDGR implementors. This article will provide an overview of the developed infrastructure and its capabilities, as well as specific insight on the provisional outcomes of the academic pilot, still under execution until the end of 2022.

## 1 Introduction

Single Digital Gateway regulation (EU) 2018/1724 (SDGR) is a major step for the future achievement of the effective interoperability of data and public administration procedures across European Union countries.

A core set of public procedures has been identified and included on the regulation for the different states to mandatorily adapt them to be optionally able (old procedures must be left as an alternative) to receive the necessary evidence to be presented through a trusted electronic channel from its source in another member state on the user's demand, following the Only Once Principle (OOP). A well-established high-level strategy driver for the European Commission that states that citizens should only deliver data to the public administrations once, and mechanisms should be established for the administrations to be able to exchange the data on the user's request.

The identified procedures include the most common needs for EU citizens interacting with other EU countries, as a consequence of their personal, educational or economic activity: moving abroad, registering or enrolling in education courses, vehicle registration, business registration for public procurement, tax payment (for a full list, refer to the Annex II of the regulation), etc. Specifically affecting the academic community, we find three mandatory procedures, as described in Table 1, where the description of the procedure and the expected outcome is detailed.

| Procedures | Expected output |
|---|---|
| Applying for a tertiary education study financing, such as study grants and loans from a public body or institution | Decision on the application for financing or acknowledgement of receipt |
| Submitting an initial application for admission to public tertiary education institution | Confirmation of the receipt of application |
| Requesting academic recognition of diplomas, certificates or other proof of studies or courses | Decision on the request for recognition |

**Table 1:** SDGR Mandatory Academic Procedures

Digital Europe for All project (DE4A) is an initiative that aims at producing a pilot implementation of those procedures in real-life production conditions, to check for the viability of implementing it, as well as to identify the weak spots and possible issues that future larger scale deployments to enforce the regulation will probably face.

DE4A project works closely with the SDGR working groups, composed of state officials seeking the maximum alignment of efforts and knowledge sharing. It includes three pilots: Doing Business Abroad, Moving Abroad and Studying Abroad. We will focus on the outcomes of the third one, run by different universities and education agencies from Spain, Slovenia, and Portugal.

## 1.1 Background

SDGR follows on the footsteps of the electronic identification and trust services for electronic transactions in the internal market regulation (EU) N°910/2014 (eIDAS), which aims at achieving the mutual recognition of identities and signatures, through the interoperability of authentication and signature systems across EU member states. After the approval of the regulation, the efforts of different initiatives and working groups of state experts helped in shaping the technical infrastructure and organisational requirements to deliver the necessary tools to enforce the regulation, which were accepted through the approval of a series of implementing acts. SDGR is now undergoing the same process: after the approval of the regulation, many initiatives have been approved and coordinated by the European Commission in order to perform the necessary analysis and field work (especially in the technical and legal aspects) to create the necessary critical mass of knowledge to design and deploy the necessary infrastructure to allow the public administrations to comply with the regulation. DE4A project

is an integral part of those initiatives: many state agencies that are key part of the working groups are also part of DE4A, which served to get other partners (like the universities) invited to collaborate with the working groups.

# 2 Transport Infrastructure

The main outcome of the project as a whole has been the definition, development and deployment of a transport infrastructure that is a strong candidate to form the core of the future SDGR support infrastructure. It consists of a scalable, trusted, and secure infrastructure for the discovery and exchange of random size messages between participants and completely content-agnostic.

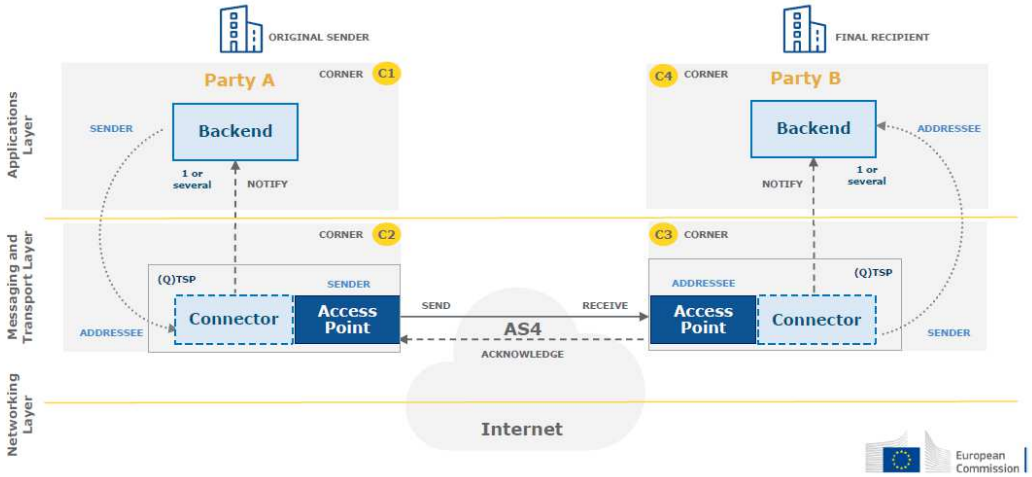



**Figure 1:** eDelivery Four Corner Model

The infrastructure is built using open software tools developed by the EC and currently in use in production in other European infrastructures. The core component is the CEF eDelivery Building Block, a messaging system based on the AS4 protocol which allows being deployed in multiple layouts. The chosen topology for the project is the four-corner model (see Figure 1). A network of Access Points (AP) trust each other to exchange messages delivered to the origin AP by the sending party, and delivered to the receiving party by the destination AP. Despite any participant can deploy an AP, the usual practice (and the one chosen by the project) is to deploy a central AP at a specific domain (in the case of DE4A, per country), to act as a hub for the message requests and responses to all the entities under that domain. This model offers the most scalable and manageable approach, as every sending/receiving party just needs to implement the specific API to manage the messages implemented by the connector (that can be common or country specific depending on each country's needs), and each country just needs to deploy and operate one AP, which is a heavy component that requires specific management: it needs to manage a Service Metadata Publisher (SMP), which is the component in charge of publishing the routing and messaging capabilities for every participant (APs, Receiving Parties, Sending Parties) under its domain, and this service is consumed by the Service Metadata Locator (SML), which is a central service to coordinate the discovery for all the infrastructure and the root of trust.

Besides these basic components of the eDelivery architecture, DE4A has developed specific components to fulfil the needs of the specific message exchange case it covers. Like for example the Lookup service, that allows to discover the Receiving Party based on search parameters, like the evidence type (i.e., an undergraduate diploma with average grade), country (the country where the evidence repository is located), which helps the Sending party produce a more user-friendly discovery interface. The canonical form for each one of the evidence items required to be exchanged on the use cases have also been analysed and defined during the project. A semantic lookup and translation mechanism to convert local evidence to a canonical form was explored as well, but due to time and effort constraints, the idea was dropped in favour of all repositories releasing the canonical form.

As a consequence of the use case needs, it has been observed that the basic exchange model of the eDelivery system is not enough: to this end, different interaction patterns were analysed, and the necessary components developed to support them. We will detail the implemented patterns on the next section.

## 2.1 Interaction patterns

We call interaction patterns the different theoretical situations that can be faced on the exchange of evidence, with distinct requirements.

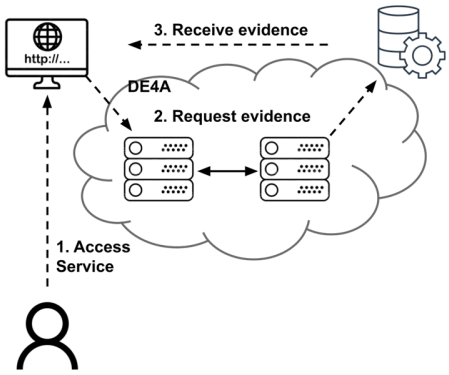



**Figure 2:** Intermediation Pattern

The basic model eDelivery implements can be called the "**Intermediation Pattern**" (IM), as can be seen on Figure 2. This is due to the fact that the user never interacts directly with the Data Repository (DR), only with the Requestor. The user accesses the procedure on the Requestor, which at some point (after authenticating the user) will ask the user for permission to request his data to the DR, which will happen on the back, through a secure channel. The Requestor needs to be a properly secured and tested application, as well as the DR that needs to keep an audit log and strict verifications of rightful use. The Requestor has full rights to ask for data from any user (as far as it knows his identifier), so if an attacker finds a way to inject a user identifier, breaking the procedure controls, a severe data leak can happen. This model is the most convenient for the user, as it only interacts with one system and doesn't have to face complex infrastructures. But on the other hand, if the identifier for the user that the Requestor sends does not match the one at the DR (for example, if the authenticator uses targeted identifiers to prevent tracing, or Requestor and DR belong to different countries with different ID schemes), it is impossible to fulfil the procedure without further action.

The above concerns, along with the requirement by Article 14 of the SDGR to allow the user to preview the data before it is delivered, bring us to the "**User-Supported Intermediation Pattern**" (USI). In this pattern (see Figure 4), all the data is transferred like on the IM pattern, through the

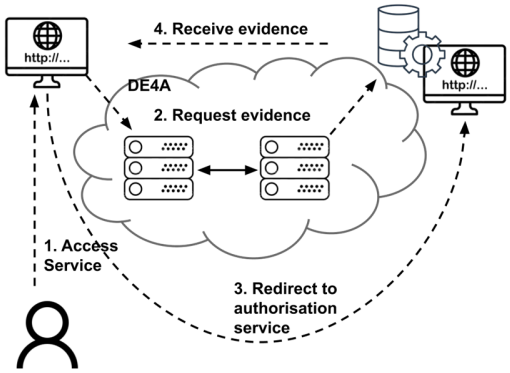



**Figure 4:** User-Supported Intermediation Pattern

eDelivery infrastructure, but the user, after interacting with the Requestor and starting the data request process, will be redirected to the authorisation interface of the DR, which will authenticate the user again and present him with the evidence to be exchanged, for the preview and get the user acceptance. After that, the user will be redirected back to the Requestor and the data exchange process will continue as in the IM pattern. In this case, the Requestor has less security concerns, as the DR will independently authenticate the user. Nevertheless, this opens the door to an attack where a second user, in collaboration with the first user, authenticates at the DR, effectively lending the second user's evidence to the first user, as if it was his own. This can only be mitigated by comparing any personal data accompanying the evidence with the authentication data at the Requestor, but being two different systems, the data can be recorded differently and cause false negatives/positives depending on the strictness of the matching. The user experience in this case will be more complex, as it interacts with different systems, but this pattern fully covers the rights the user has both in GDPR and SDGR.

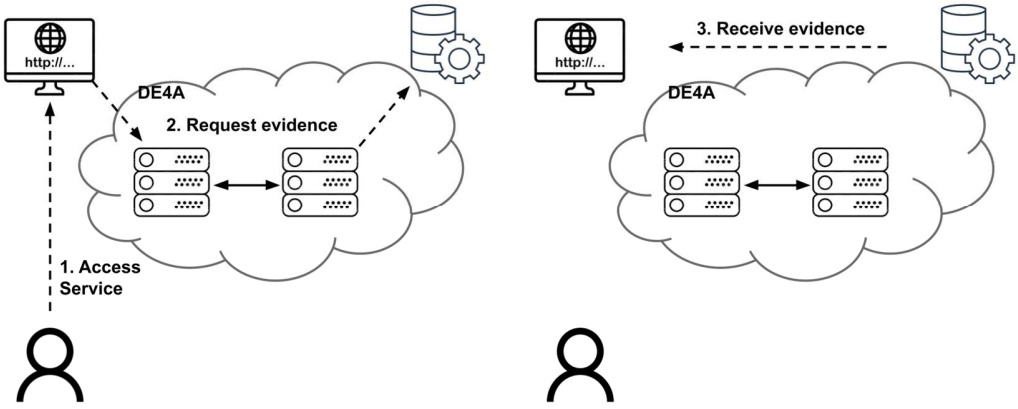



**Figure 3:** Registration and Notification Pattern

Besides the above-described patterns, some data exchanges cannot be fulfilled in an online way: either the data needs to be fetched in an offline (or even non-digital) data repository, or requires some form of human approval, review, or interaction before the transfer. To this end, the "**Registration and Notification Pattern**" (RN), as can be seen on Figure 3. This case is mostly equivalent to the IM pattern, but the Requestor will not expect the evidence to be delivered immediately but will only register the request on the DR and expect it to be delivered sometime in the future (and trigger the continuation of the procedure as soon as it happens).

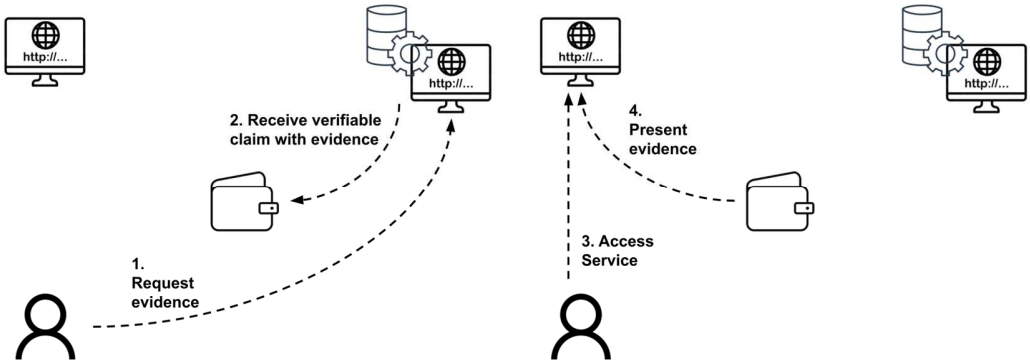



**Figure 5:** Verifiable Claims Pattern

An additional pattern has been developed, that could be considered an evolution of the one above, but holds many major changes and possibilities, the "**Verifiable Claims Pattern**" (VC). As can be seen on Figure 5, this pattern follows the principles of Decentralised Identity. The user interacts separately with the Requestor and with the DR, and stores the retrieved evidence on a wallet, to be delivered to any Requestor that might ask for it. In a way, this could be a digital transposition of the classic paper-based evidence exchange, where the user had to request the proper evidence on the proper desk and store it on his own portfolio and take it to the desk that requested it. Of course, mechanisms exist to streamline this access to the DP: the Requestor, if the wallet is unable to produce some evidence, it can redirect the user to the proper URL on the DP to trigger the evidence issuing procedure, but in any case, it is the most complex use case from the user experience point of view, presenting a considerable knowledge gap. Also, the freshness and custody of the evidence are concerns that need to be carefully studied before using this pattern: the integrity of the data depends on the cryptographic signature at the time of issuance, so to react against any flaws on this procedure, revocation mechanisms are needed to provide full guarantees to the Requestor, that might consult them before consuming some piece of evidence. Also, the data is being custodied on a user wallet. Despite the encryption of the wallet, if the user device is vulnerated, the attacker can most probably gain access to the data. It just impacts the data of on user (so it does not have the same impact as a data leak on a centralised server), but it also is more feasible than a leak on a centralised repository, which has stronger custody and access controls.

Each implemented use case involving data providers and data consumers will be able to choose the pattern that better fits the requirements: for example, if a certain exchange of data can legally happen without the direct and explicit authorisation of the user, IM pattern can be chosen. If the data source cannot deliver the data live to fulfil the procedure, and some wait period is needed, the VC or Registration patterns are the choice. The two most generic flexible patterns are USI and VC, being the

first the most usual one, as the data is always retrieved from its authoritative source, and VC the most innovative one, as it facilitates the user to be in possession of the data and enables him to use it without having to rely on the source being always available. It must be noted that VC pattern has clear similarities with the paper-based procedures: the evidence is presented as signed verifiable claims, which can be seen as a transposition of the officially issued, verified and sealed paper certificates. The user accesses the sources of the evidence independently and accumulates available evidence in a wallet (which can be seen as analogous to a document portfolio). This analogy can be of use to train the end user to be comfortable with the VC pattern.

# 3 Academic Pilot

The academic pilot of DE4A, involving two Slovenian and one Spanish universities, and a Portuguese education agency has deployed several services that align with the mandatory use cases descripted in the SDGR (as depicted in Table 1). To this end, a structured canonical model in XML of the Higher Education diploma was developed, in coordination with other efforts in the same area (Europass, EBSI and the SDGR Workgroups). The national education services on the three countries are able to deliver this canonical evidence for the students of the involved institutions at least (some are able to do it for all citizens), and they can be consumed by the services of the participants, which run in a production environment and with real users. For example, any Slovenian and Portuguese graduate students enrolling on a master's degree course at Universitat Jaume I are able to present their undergraduate diploma through the DE4A technical system, removing the requirement to present it as a scanned attachment (with the associated reduction in risk of fraud and error, and effort on the user) and removes the need for the officer processing the enrolment request to do phone security checks of the authenticity of the title with the university of origin (with the associated reduction in costs and risks on the institution). Exchange of evidence for the use cases in the academic pilot is done through the USI and VC patterns. USI pattern is the main option, as the user is allowed to review the data and explicitly authorise the data transfer from the source, safeguarding the user rights regarding data protection. Using IM pattern could potentially require a specific legal framework to operate, as the user cannot interact with the evidence source, and Registration pattern is not required, as the academic evidence is directly available live in the education government agencies. Another important aspect of the USI patter is that, as it performs double authentication of the user (at the data source and destination), it does not face identifier matching issues, leaving to the data consumer the effort of verifying that the evidence does effectively belong to the authenticated user. VC pattern is also implemented as an experiment aiming at finding the difficulties for the user to take custody of his own data, but no results can be yet shared on it at this point, as the project is still ongoing.

Interim results of the tests with students for the USI based enrolment services shown that students face a complex method. As it is a strongly guided flow, they were able to finish it, despite doing so with difficulties and very limited understanding of the steps being taken. After receiving basic guidance, they were able to easily repeat the procedure with much more independency, but with understanding still limited to the goals and overall flow of the procedure. In fact, this is the main point that can be provisionally excerpted from the user feedback, the knowledge gap for the user, who does not fully understand the generic concept of evidence, and the exchange model and trust model. Once the process is nearly finished, and the user previews the diploma, a better understanding is achieved, as well as a general acknowledgement that their diploma is being transferred from the education authority of their country of origin, to the university where they intend to enrol. One of the key stress points for the user experience is the requirement of eIDAS authentication both on the university and on the diploma provider. They see it redundant and complex. This adds to most students not owning valid eIDAS

credentials for their countries, which required to use test credentials on most supervised experiments. The other main observed difficulty in the user interaction is the lack of UI harmonisation between the different involved systems: The university enrolment service, the eIDAS country discovery, the eIDAS Identity Provider, and the data source. All of them have differing UI layouts and design, requiring the user to adapt to each one of them individually. Repeated use shows quick familiarisation, but the expected frequency of use of the SDGR technical solution is low, so holistically optimising and harmonising the business flow and appearance should be apriority. Also, before starting the procedure, users would greatly benefit from previous training to help minimise this gap.

One of the main design concerns since the beginning of the project had to do with the semantic interoperability. The initial ambition was to allow evidence data to be fully machine processable. Despite this has been accomplished to the syntactic level, fully achieving this goal implied the proper interpretation of the data content had to be discarded, due to the time and effort constraints. Nevertheless, we will share some of the main guidelines envisaged during the analysis phase, centred around the design of the evidence for the academic pilot: undergraduate diplomas. Each Country issues evidence on its own format, with its own dataset, and being each data element interpreted in a particular local way. DE4A addressed this issue by defining canonical forms for the evidences. That is, common structures that all countries should follow to deliver the data. This solves the syntactic interoperability problem, as is the most efficient approach. The defined evidence structure for the academic pilot is aligned with other initiatives, such as Europass and EBSI, and DE4A is closely collaborating with the SDGR working group, which are following a similar approach. The DE4A designs support multiple schemas of content. That is, for each machine-processable data entity, metadata on the representation schema used is added. This allows to extend the current usage in local data schemas to a common semantic framework in the future. As explained above, providing a semantic interoperability solution goes beyond what can be achieved by the project, but proposals were analysed. Currently, each country has their own officially issued procedure to interpret the diplomas from other countries. This approach allows full control for the destination country, but requires much effort, hardly scalable and maintainable (without the collaboration of authorities form the source country). Following the same canonical model as for the syntax seems a good strategy: agreeing on a central canonical evidence representation schema and scaling fitting the needs of all the participant countries and then collaborate to map the source schemas to the canonical one. This allows for a progressive and methodological approach, as effort can be fragmented per data entity and working group as needed. The data could then be issued in the canonical representation by each data authority following the agreed mapping rules, or data repositories could be established to keep the mappings in a standard scriptable format, to allow any participating entity to access and apply the rules on demand. These proposals would require extensive development and discussion, and despite not fitting the constraints of DE4A project, expectation is to raise awareness on the SDGR working groups so they can be evaluated there.

# 4 Conclusions

DE4A project has performed an important effort in defining and showcasing the success pathway for the execution of the Single Digital Gateway Regulation. A critical amount of knowledge and experience has been accumulated on the difficulties of deploying and operating the infrastructure. Guidelines to minimise participant efforts to integrate and to securely operate have been defined and shared with the working groups, as well as the analyses for the canonical data formats and the requirements of the mandatory procedures in several countries. But also, it has been identified that further effort to define support services and mechanisms, especially in the semantics area need to be coordinated across EU.

# References

Single Digital Gateway (2022). *European Commission*. Retrieved February 01, 2022, from: https://ec.europa.eu/growth/single-market/single-digital-gateway_en

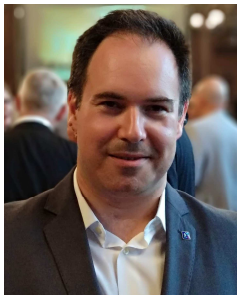
DE4A website (2022). *DE4A project*. Retrieved February 01, 2022, from: https://www.de4a.eu/

CEF Digital Programme (2022). *European Commission*. Retrieved February 01, 2022, from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home

# Author biographies

José Pascual Gumbau-Mezquita Graduated with a Master's Degree in Mathematics (majoring in Computation Sciences) and Certified Information Systems Auditor (CISA) by ISACA. He is Head of the Office for Innovation and IT Auditing at Universitat Jaume I in Castellón (UJI) and coordinator of the IT Innovation Laboratory (TecLab). He is member of the IT/IS Analysis, Planning and Governance Subgroup at the Spanish Rectors Conference ICT group (CRUE-TIC). From 2006 to 2017 he was director of the Technology Planning and Forecast Office and head officer of the STORK and STORK 2.0 e-academia pilots. He has also worked as a professor at the Computer Science and Engineering Department at Universitat Jaume I.

Francisco José Aragó-Monzonís graduated with a Master's Degree in Computer Engineering at Universitat Jaume I in Castellón, Spain, in 2008. Since then, he has developed a career as a programmer and analyst, both as a freelance and for the same university, in computer security and cryptography related projects. Participated in the final steps of STORK project as a programmer, but in STORK 2.0, took a more leading role in the eAcademia pilot, both in executive and technical aspects. Has an active collaboration with the Spanish NREN, RedIRIS, where he designed and operated a platform to facilitate the connection of public universities services to the national central authentication system, Cl@ve, and its interaction with eIDAS. Technical leader of ESMO and SEAL projects. Currently in DE4A and EDSSI projects.



José Traver-Ardura holds a Bachelor of Computer Science and a Master of Intelligent Systems degree from Universitat Jaume I de Castelló, Spain. He has been working in different IT-related departments at Universitat Jaume I in Castellón since 2002, coordinating and managing the corporate research computing clusters, designing, and managing different cloud migration solutions for on-premise infrastructure and supervising compliance with personal data protection and security-related national laws and regulations. He is also part-time lecturer at UJI's seniors education program with different publications on new ways to improve seniors education using emerging IT services. More Recently, he has participated in European research funded projects like ESMO or SEAL and currently working on DE4A and EDSSI.