SEAL Project: enabling identity reconciliation and self-sovereign data management.

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

SEAL project has developed a trust broker service for access to personal and identity data, as well as to Know Your Costumer (KYC) services to enable identity reconciliation, everything designed around the user and giving the user control and custody over his personal data. The current rise of Self-sovereign solutions and decentralised data storage has raised the importance of this need to establish trusted relationships between the different identities some individual has across the Internet, while still preserving the rights of the data owner, especially for high-trust services like government, education, health, or banking. Service providers can trust on the origin of the data, but also need to know if data collected from two sources belong to the same citizen, without trusting the citizen on it, as there could be benefit from counterfeiting input data. In that case, the service provider must go over an expensive matching procedure (in resources and time) on the received data to get an appropriate level of assurance that said data belongs to the same person already registered on the provider, and that some of it was not borrowed from another person.

SEAL service is designed as hub for all the related aspects of identity management. SEAL allows the user to import data from external sources, generate new data derived from the existing data while keeping the trust, interacting with KYC providers, and exporting the data through federated interfaces or issuing verifiable claims, for interfacing with a self-sovereign environment. All of this is achieved through an extensible and modular architecture, so the user will be able to collect his data and then ask for trusted links to be established between the different collected data sets and keep everything on his personal datastore.

1 The SEAL Service

The main work carried by SEAL project has been to develop and deploy the SEAL service. The SEAL service is currently addressed at students and staff of the universities but can be exported to other sectors out of the box. When deployed, and using its module system, SEAL allows to establish trusted channels to external data providers, so the users are able to access those sources from SEAL and retrieve the data. Once the data is on the SEAL session, the user can store it on a personal storage (on his own device or on a personal cloud storage account) and load it any time to operate it or deliver it to a federated consumer or to a self-sovereign wallet. The user will be able to request a KYC service to issue a link between two imported data sets (after validating that to a certain level of assurance, both data sets belong to the same person). Higher-grade mechanisms involve more effort on the user. SEAL supports a grading scheme, so users can choose to start by building basic links and then improve them over time.

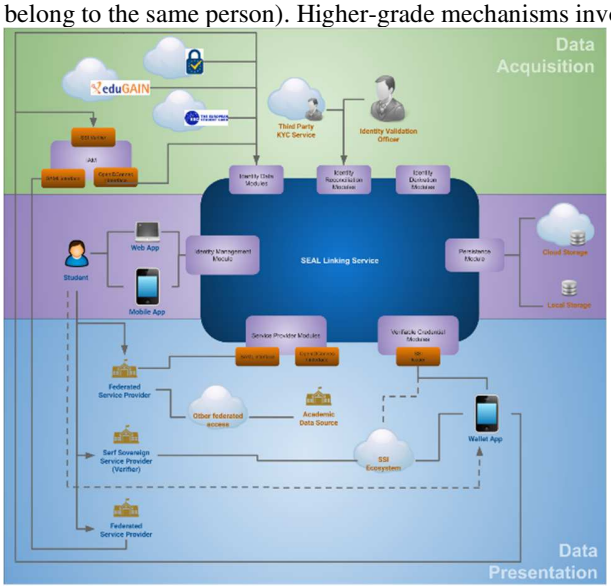


Figure 1: SEAL service architecture

From the user's perspective, SEAL is built as a backend API, which supports all the commands and operations, and an independent client, which can be compiled into a mobile client, and a web client, to minimise maintenance costs. It must be noted that the mobile client has added functionality that leverages the capabilities of the device (for example, to import data from machine-readable passports).

From the architecture perspective, SEAL is divided into three layers: a data acquisition/generation layer, a data management layer, and a data presentation layer: The first one implements interfaces for the data sources, linking mechanisms, and data derivation, each interface is implemented by specific service modules brokering the access to said data/procedure. The second one implements the command API (which the clients invoke), and the data storage API, where each module implements a storage mechanism (encrypted by the user, signed by SEAL, to prevent tampering from the user). The third one implements two interfaces for data access: federated access (SAML, OIDC consumers) and Self-sovereign (SSI) consumers (UPort environment is the only current implementation). Consumers will issue a secure request to SEAL, and the user will be asked either to access a live source of authentication/data or to load his own Personal Data Store and retrieve data from there. That data, for SSI consumers, will be built into a Verifiable Claim, and written on the user's UPort wallet, so the user can deliver that data without depending on SEAL to broker it.

The most notable information SEAL can deliver is the linking information. That is: if a consumer needs to know if some incoming data belongs to a locally authenticated user without trusting the user himself, the consumer can request the user through SEAL if the authenticated identity and the incoming data identity are the same person. SEAL has developed a portable framework to issue and consume the link information: levels of assurance and awarding criteria, how to infer the trust and how to represent the link in JSON and in URI format.

2 Outcomes and Benefits

SEAL follows the current tendency to put the user in control of his data, by enabling to establish trusted links between user's own data, allowing it to be consumed by service providers while moving the effort of identity reconciliation away from them, and bringing it to specialised and trusted third parties. This allows promoting the establishment of a lifelong digital identity, useful to pursue the achievement of the only once principle and the single digital gateway goal, two of the main focuses of the European Commission regarding interoperability. The user will be the keeper of his own data and rights, thus enforcing the concept of Self-sovereign Identity.

The working service is the most obvious outcome, but we consider the learning a better outcome: GDPR compliance and other legal considerations related to data management and linking, data formats, semantic interoperability, trust models and possible exploits. All these have been explored and a first overarching solution has been proposed, paving the ground for future discussion. SEAL aims to become a centrepiece to incrementally tackle and standardize this identity linking and user-centred data management. This way, SEAL can become a key piece in this interoperability scenario, which is constantly gaining importance over time.

3 Future Work

Despite nearing its end, Project SEAL has designed a plan to keep it running and growing, in search of self-sustainability. Starting by the commitment of the project partner to keep improving and disseminating the outcomes, the plan includes engaging the key stakeholders to gain support and build a community around the software. The main goal of it will be to open and widen the discussions to include all sector experts, in order to analyse the interoperability issues raised during the project with a wider more solid scope, seeking generalisation of the fluxes, improvements and potential standardisation.

Plans for the future include developing new modules for interacting with sources of data, new modules for derivation of datasets and to establish liaisons with KYC providers to develop compatibility modules, even for services that charge their clients or a client company.

Also, to allow a generalised deployment and to ensure interoperability, SEAL will develop a trust model to allow Personal Datastore interwork between multiple instances, with a fully automated key management system, including revocation.

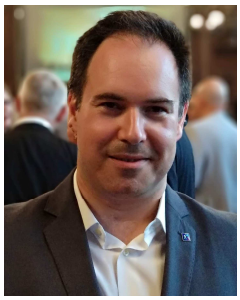
Finally, another key goal for the future of SEAL is keeping convergence with the European Blockchain infrastructure services, and to provide support for other SSI environments.

References

SEAL website (2021). *SEAL project*. Retrieved February 22, 2021, from: http://www.project-seal.eu/

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 participates on 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.