Progress in EPOS Authentication and Authorisation Solutions

Tomasz Szepieniec and Daniele Bailo

Kuvvet Atakan

Keith Jeffery

In the process of building and integrating technical subsystems of the EPOS Infrastructure, choosing the right solution for authentication and authorization is crucial. It is not only about enabling login into the EPOS service with a single account. But, it is all about trust and security of the system. We need to decide which login services we can trust, define and manage the roles of each user and, finally, execute actions in distributed environment on behalf of a user (this is called delegation). All those things done in federated fashion between ICS-C, TCSes and also ICS-D, pose a real challenge in implementation.

Fortunately, a federated approach to authentication is recently a popular subject among European e-Infrastructures. We can learn from the others good practices but also reuse their software, which otherwise would be costly to develop. Therefore, on the early stage of EPOS infrastructure development, there was an action defined to review existing solutions and create a prototype subsystem called AAAI (the name stands for Authentication, Authorisation, and Accounting Infrastructure). The idea was to integrate all aspects related to an EPOS user in the system which includes: logging into the environment with recognizable identity, verifying permissions to execute operations in the system and keeping records of all actions performed. In 2017 the most attention is put in the first A (Authentication), as the 2nd A (Authorisation) is built upon the previous, and so is the 3rd A (Accounting).

The process of collecting requirements related to Authentication, performed during the first few months of the EPOS IP project by WP6 and WP7 teams, revealed that there were some existing accounts and authentication providers that should be used. So, it became clear that rather than building the new authentication provider, the effort should be dedicated to integrate the existing sources of authentication and enable EPOS users to utilise them. This include the existing accounts provided by some universities (as part of
EDUGain) or some operating services related to TCSes (like EIDA within ORFEUS or IS-EPOS Platform). The technical challenge was related to the fact that the recognized methods of authentication differ in protocols. The solution was in authentication proxy architecture. It allows establishing connections using many authentication protocols and providing a consistent representation of authentication data needed. As a software basis of AAAI prototype, UNITY-IDM\(^1\) was chosen. It is open source solution that implements almost complete set of currently available authentication protocols and can act as a proxy identity provider. UNITY-IDM is widely used in e-Infrastructures also as code base of EUDAT B2ACCESS [2] service. The first version of EPOS AAAI prototype was configured by ACC Cyfronet AGH team and presented at the first EPOS Integration Workshop\(^2\).

The prototype is available at https://epos-aai.cyfronet.pl/

In the course of the project, it was also important to keep track of related development activities. So, AAAI team, invested some effort to understand other solutions and make them work for EPOS community. Especially fruitful were three collaborations that are shortly characterized below.

- EGI\(^3\) established a competence center with EPOS in order to understand EPOS needs and present their solutions. The result was an integration of EGI Check-In\(^4\) service as an identity provider for EPOS AAAI prototype. The way how the integration was implemented allows EPOS retain control of key authentication assets but, at the same time, provides access to plenty methods of authentication including EDUGain providers (more than 2500 institutes) and X.509 certificates that EGI Check-In offers. Other subject of collaboration with EGI is potential access to computing resources in context of ICS-D.

- AARC European Project\(^5\) was dedicated to the development of federated authentication solutions. EPOS was invited as a client e-infrastructure to the second edition of this project (named AARC2, launched June 2017) and is represented by ACC Cyfronet AGH. The main outcome of the initial AARC Project relevant to EPOS Infrastructure was Blueprint Architecture which provides a reference architecture for federated authentication and authorization. AARC acts also as an expert group, where technical challenges of EPOS Infrastructure case can be discussed.

- INDIGO-DataCloud Project\(^6\), concluded September 2017, aimed at developing cloud platform and provided many useful microservices. The most interesting from EPOS perspective was the fact, that those microservices are extensively using multilayer delegation (interaction where a service is using another service with a full context of a user). This was possible due to the implementation of the emerging
A standard called oAuth 2 Token Exchange in a component called IAM.

The delegation is very relevant to EPOS architecture as some TCSs require user contexts to perform their operations and provide data. Therefore, recently EPOS AAAI prototype has been extended to support the same protocol, that was used in INDIGO-DataCloud. This was possible thanks to the collaboration ACK Cyfronet AGH and UNITY-IDM developers. Now, the prototype is ready to serve delegation mechanism when needed.

To sum up the status of AAAI, we can say that most of the relevant technology is tested and ready to be deployed. This allows recently initiated ICS-C prototype integration with the AAAI prototype. Year 2018 will bring more development, including those on policy level related to authorization and authentication. It is also expected that integration of various Thematic Core Services with the AAAI prototype will start soon. However, this must wait for the result of ongoing discussion among EPOS WP7 team, on how to keep this process possibly least effort consuming by TCSes developers.

---

[2] https://www.eudat.eu/services/b2access
[6] https://aarc-project.eu

Back to newsletter