Experiences Using OAuth2.0 in Federated and Multichannel Open Service Platforms

Raman Kazhamiakin[1]

[1] Fondazione Bruno Kessler, Trento 38123, Italy
raman@fbk.eu

Abstract. The OAuth2.0 protocol has become a reference standard for the authentication and authorization when accessing APIs and services. Several challenges arise, however, when the services are exposed in large federated environments with multiple identity providers, service providers, and service consumptions channels. In this work we present our experience with adopting the protocol for securing the access to the Open Service Platform, a framework where the APIs are exposed to a multitude of independent clients, user groups, and channels in a uniform manner. We will show case different scenarios that go beyond the standard use of the protocol, show the limitations of the baseline solutions, and the ways they can be extended.

Keywords: OAuth2.0, Security, Open Services, Mobile Computing.

1 Introduction

In recent years the OAuth2.0 protocol has become a reference solution for protecting the access to the functionality and data. Being adopted by a variety of big providers, such as Google or Facebook, the protocol allows also the 3rd party web sites or applications to use those providers for the user authentication purposes without maintaining the user database and their credentials. But what is more important, the protocol addresses a scenario where the access to the functionality is performed via REST APIs, allowing one to appropriately scope and control the access to using the token-based mechanisms. This scenario is typical for software platforms that expose a wide range of operations over Internet allowing to build Web, mobile, or chat-based applications on top of that.

In Smart Community Lab we have been building an Open Service Platform, a solution aims at bringing the API management and usage to the level of a community. In these settings being *open* means, in particular

- Opening the platform for different ways of authentication, ranging from user registered users, to the user authenticated with external providers (e.g. ,Google) or with federated providers (e.g., local- or national-level authentication solutions). Performing a seamless integration of these solutions for the access control across different channels becomes a non-trivial problem.

- Opening the platform to different service providers who manage the API exposure and authorization in an independent manner. This requires in turn the management solutions that deal with complex role and scope models that go beyond the standard OAuth2.0 scenarios.
- Opening to different modes of service and data consumptions, where the standard OAuth2.0 setting do not fit well. This concerns, for example, mobile application authentication, Internet of Things protocol, exposure of resources without authentication headers (e.g., images).

In this presentation we will dive into these problems and highlight some of the solutions that has been adopted in Open Service Platform.