Implement CIAM solutions in an easy way: Asgardeo is the last solution as a service from WSO2

Gabriele Gianoglio [1]
Profesia S.r.L.

1 Introduction

API are the main functionality in microservices architectures, these are the interface between the user experience and the backend program. An API is the interface to access several resources, these can be various elements on the IT infrastructure: a developed functionality (JAVA, PHP, ecc.), data stored in a database ecc. accessed by a given endpoint.

The defined endpoints do not need to implement the security criteria for the definition of authentication and authorization policies for the implemented applications, these can be defined at the API level. The authentication process can be implemented in different ways and with various methodologies, these depend on the technologies used within the infrastructure.

Microservices implement the application logic to perform the required operations, API defines the interface between the user and the core application, none of these implements the authentication criteria or the authorization logic, that is delegated to an Identity Provider.

In a Microservice Architecture authentication and authorization it is implemented in an Identity provider application that has the responsibility to implement, manage and maintain the authentication of the user and also authentication and authorization to access and consume API and microservice behavior.

Identity provider is an application that has information related to the user, user information may be stored in databases or LDAP servers on premises or can be inherited from external resources like email services, social networks ecc. This information cannot be accessed with proprietary functions, but should respect a standardized protocol. The Oauth [2] protocol defines a standard flow to authenticate users on top of HTTP protocol and is used in modern applications to authorize users to access resources and inhibit unauthorized operations.

As part of the entire architecture, an Identity provider is dedicated to standardize the process of authentication and authorization so that every app mobile or web site can perform a standard HTTP request to permit users to authenticate with the desired method.

[1] https://www.linkedin.com/in/gabroglio/
[2] https://oauth.net/2/

2 The authentication process

The recognition of a user can be engaged in the traditional way through the request for a username and password, but this is not the only way and at times it can also be considered the least secure, the use of devices such as biometric sensors or the use of QR codes are of help to verify the identity of a subject and avoid unauthorized access to sensitive data. [3]

Asgardeo[4] takes care of developers that need to interface with several IdP from one side and on the other side need to write the code to implement the authentication flow in a specific programming language, depending on the need, it may be necessary to request different levels of authentication which in some cases can also interact with devices owned by end users. [5]

This level of integration decouples the application that needs to start the user authentication process from the specific identity providers, at the configuration level it is possible to register different identity managers that can be engaged according to the different needs within the flow authentication itself.

In terms of GDPR, all the features are offered to make an application compliant with the current standard, having the ability to define in a capillary manner the request for the necessary consents for the completion of the specific request. All information collected during user registration can be removed when the need for cancellation occurs and the right to be forgotten is fulfilled.

3 Solution for enterprises

The IDaaS solution avoids companies the constraint of installing, within their infrastructure, a product for which they should undertake a maintenance process over time. This cloud native solution offers all the functionalities necessary to apply the necessary scalability in order to be fully and constantly efficient. [6]

Asgardeo provides internally a series of CIAM workflows, developers through a lowcode solution can easily integrate the templates proposed within their applications, significantly reducing both the development time and the debugging process.

---

[3] https://wso2.com/asgardeo/docs/guides/authentication/mfa/
[4] https://wso2.com/asgardeo
[5] https://wso2.com/asgardeo/docs/get-started/try-samples/
[6] https://www.globenewswire.com/news-release/2021/10/13/2313493/0/en/WSO2-Introduces-Asgardeo-Next-Generation-IDaaS-to-Cut-the-Complexity-Out-of-Managing-User-Access-to-Client-Facing-Applications.html