13/07/2020

Riccardo Giordano (944397) e Simone Caggese (948590)

Universita’ degli studi di milano

Progetto SOASEC

Immagine che contiene disegnando

Descrizione generata automaticamente

# Introduction

The project was created to offer the possibility of being able to manage the information and functions of the different cloud providers that offer authentication using the OAuth2 protocol in a single application.

Registered users can choose between two plans (free or premium) to have limited or full access to the APIs provided by the application.

From a main dashboard, it is possible to have a general overview of the different cloud providers which in turn will have a dedicated page to be able to view the active instances of the different services in more detail, with the possibility of performing some operations restricted to profiles. of a certain type.

# Protocols and tecnologies involved

## OAuth2

### Authlib

## Flask

## Bootstrap

## ….

# Security properties and solutions

## HTTPS

The cipher suite used is: TLS\_AES\_256\_GCM\_SHA384, it uses a digest algorithm SHA-384 to compute a Hash-based Message Authentication Code ([HMAC](https://en.wikipedia.org/wiki/Hash-based_message_authentication_code)). This message is then used to check data integrity for each record.

As explained in the [RFC 8446](https://tools.ietf.org/html/rfc8446), the primary goal of TLS is to provide a secure channel between two communicating peers; the only requirement from the underlying transport is a reliable, in-order data stream. Specifically, the secure channel should provide the following properties:

* Authentication: The server side of the channel is always authenticated; the client side is optionally authenticated.
* Integrity: Data sent over the channel after establishment cannot be modified by attackers without detection.
* Confidentiality : Data sent over the channel after establishment is only visible to the endpoints. TLS does not hide the length of the data it transmits, though endpoints are able to pad TLS records in order to obscure lengths and improve protection against traffic analysis techniques.

## ……

# Conclusion