CLAFIS CAAS

(Central Authentication and Authorization System)

Within the CLAFIS (EU-FP7-Project “Crop, Livestock and Forests Integrated System for Intelligent Automation”) environment many individual software components in agriculture need to communicate with each other. Here, safety and security is an important issue. On one hand, costly information should not be disclosed to unauthorized people, on the other hand, each component must be able to rely on the information it receives to be correct. To ensure this, a central Authentication and Authorization System (CAAS) has been developed for CLAFIS.

The CAAS environment runs at least one authentication server and one authorization server. These servers handle access privileges for arbitrary users and clients to resources of one or more resource servers. The authentication server checks the identity of users, whereas the authorization server manages privileges of users.

Fields of application and integration opportunities

CAAS is not limited to the agricultural domain. Users, clients, services, and resources from other domains can be supported as well.

Resource request by user:

A user wants to consume a service. Therefore, he needs to prove that he has permission to the required resources. To do this, the user has to prove his identity to the authentication server by sending it’s user credentials. Afterwards, the authenticated user requests a token, from the authorization server, that proves that he is allowed to access the required resources.

Resource request by client:

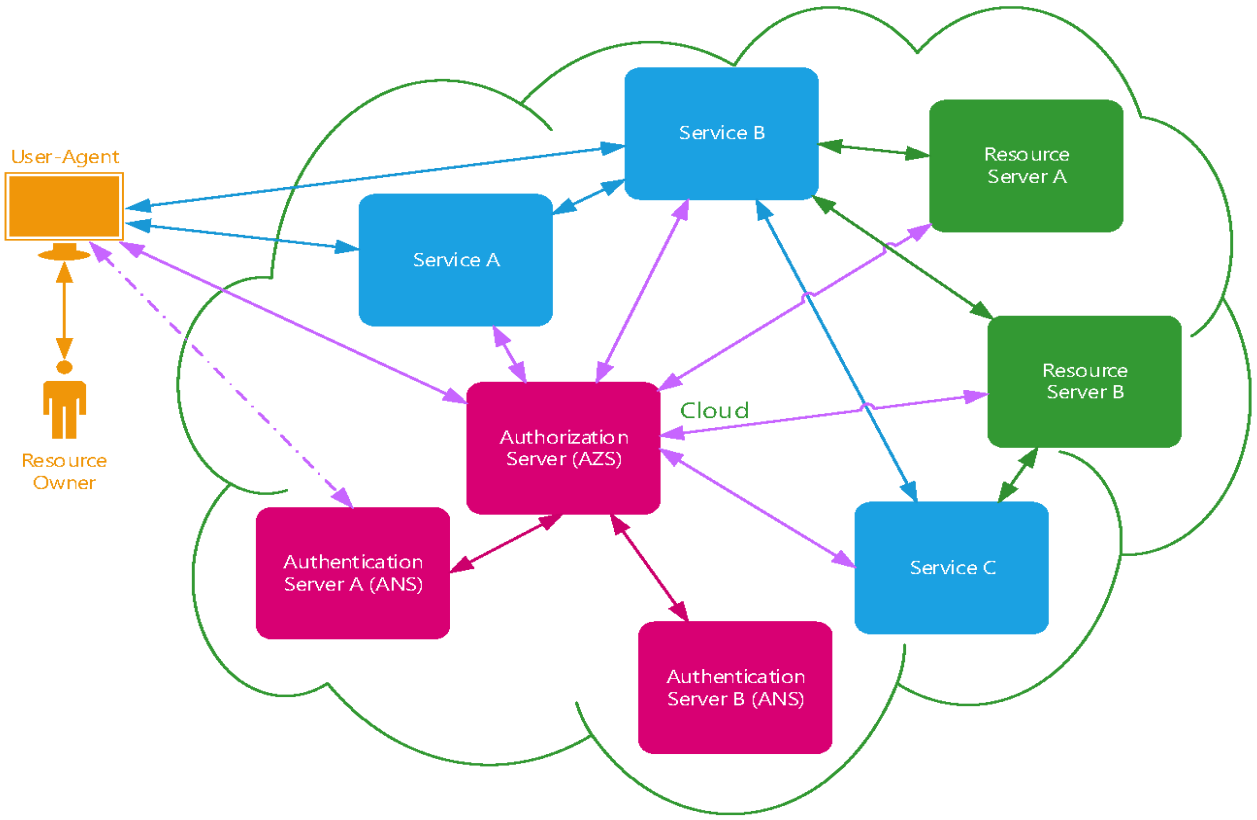
A client wants to consume a service. The client proves his identity to the authorization server by sending his asymmetrically signed client ID. The authorization server checks the signature and returns a token that proves that the client have permission to access the required resources.

Features and specifications

- Comprehensive security solution for arbitrary cloud environments
- Centralized administration of users and permission for all cloud resources
- Implements token-based concept described in current state of the art standards (OpenId, OAuth2.0)
- Guaranties a secure communication between the involved parties even without a secure server configuration
- Scalable to arbitrary large cloud environments
- System complexity is completely hidden from the user
- Permission can be manage at any degree of granularity an complexity
- Resource provider need not to deal with user credentials

The Project is supported by the EU-FP7 programme. Project acronym: CLAFIS. Project title: “CLAFIS – Crop, Livestock and Forests Integrated System for Intelligent Automation, Processing and Control”. Grant agreement No: 604659.

JOHANNES KEPLER UNIVERSITY LINZ

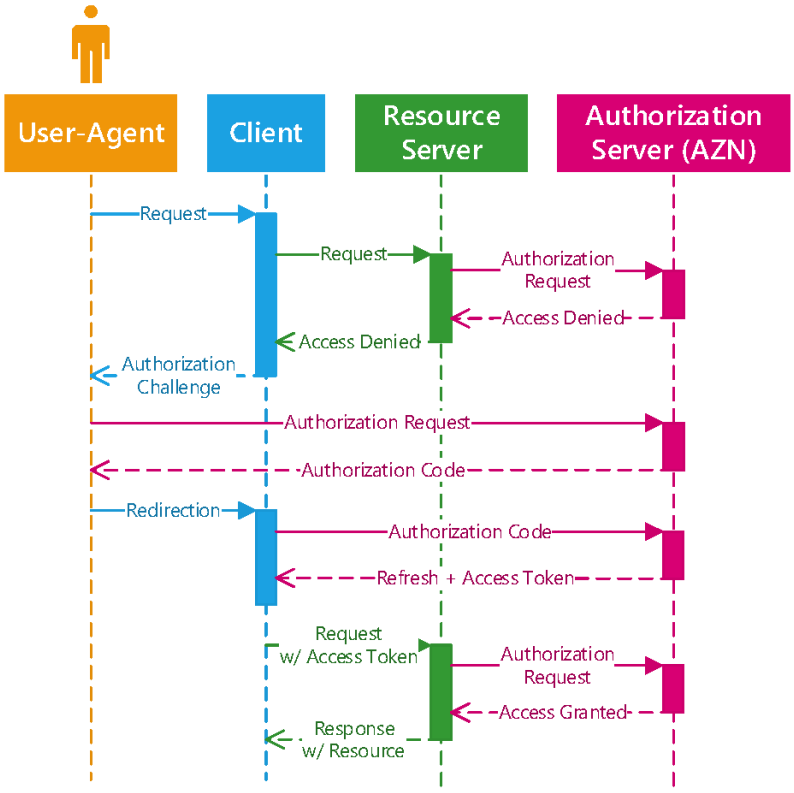


Authorization process

The sequence chart on the right presents the authorization process of an already authenticated user.

After the first resource request failed the client returns an Authorization Challenge containing a list of required permissions. The user sends an Authorization Request for these permissions to the Authorization Server. Afterwards the client uses the responded Authorization Code to obtain an Access Token from the Authorization Server.

Finally, the Access Token will be used by the Resources Server to verify that the user has permission to access the requested resource.



For further details contact:
Johannes Kepler University Linz
Faculty of Engineering and Natural Sciences (TNF)
Institute for Application Oriented Knowledge Processing (FAW)
Science Park 3
Altenberger Straße 69
4040 Linz, Austria

A.Univ.-Prof. DI Dr. Josef Küng
Phone: 0043 732 2468 4182
E-Mail: josef.kueng@jku.at

Stefan Nadschläger MSc
E-Mail: stefan.nadschlaeger@jku.at

DI Markus Jäger BSc
E-Mail: markus.jaeger@jku.at

DI Christian Huber BSc
E-Mail: christian.huber@jku.at

JOHANNES KEPLER UNIVERSITY LINZ

FAW