living draft-00
last edited on August 20, 2021

# Correlated Authorization

## (Dual Cross-Domain Authorization)

Igor Zboran
izboran@gmail.com
August 20, 2021

## Abstract

Correlated Authorization is a dual cross-domain authorization mechanism originated from the User-Managed Access (UMA) protocol that allows users (resource owners) to delegate access to other users (requesting parties). The requesting party is responsible for creating the request, while the resource owner approves the transaction asynchronously. The resource owner and the requesting party may belong to different security domains (realms) or may use mutually isolated instances of the authorization server residing on different network domains. They may also use independent identity providers, there is no need to share an OIDC provider or use federated OIDC providers. This concept uses a permission ticket as a correlation handler between two authorization processes and an e-mail address as a unique requesting party identifier for cross-domain access control.

## Introduction

In ...

## Problem

...

### Current Situation

...

### Current Flaws

cross-domain scenarios

# Proposed Solution

.

## Motivation

.

## Main Concept

…

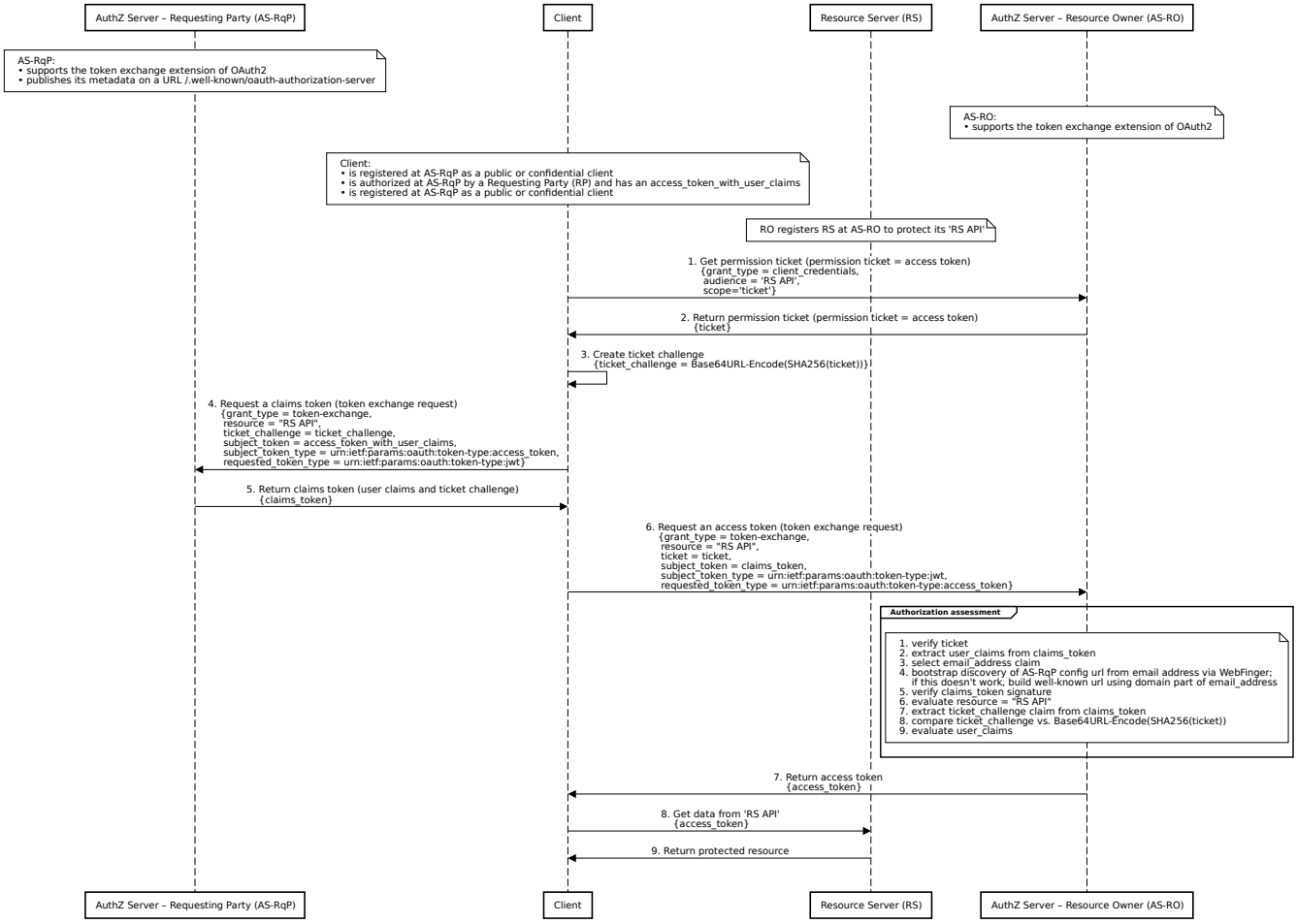
# Sequence diagrams

## UMA profile

This diagram is in full compliance with the UMA specification.

## Generic

This is a generic diagram missing some UMA features.



## About the Author

Igor Zboran is a mechanical engineer by education with professional experience as a software engineer, solutions architect and security architect. He'd like to transform his knowledge into a useful system or service that people would love to use.

Igor received Ing. degree in Mechanical Engineering from the University of Žilina, Slovakia in 1988. After graduating, he worked in several small private companies as a software developer. From 2008 to 2009, he provided expert advice to Prague City Hall IT department, Czech Republic as an external consultant. He invented a new decentralized Identity-Based Privacy (IBP) trusted model built around OAuth2 and OpenID Connect standards. Igor is a strong proponent of open source software and open standards.

## References

[1] OpenID Connect (OIDC) https://openid.net/connect/
[2] User-Managed Access (UMA) https://en.wikipedia.org/wiki/User-Managed_Access
[3] WG - User Managed Access https://kantarainitiative.org/confluence/display/uma/Home
[4] OAuth 2.0 Token Exchange https://datatracker.ietf.org/doc/html/rfc8693