living draft-00
last edited on August 29, 2021

Correlated Authorization

Igor Zboran
izboran@gmail.com
August 29, 2021

Abstract

Correlated Authorization (CAZ) is a dual-authority, cross-domain authorization protocol built on top of User-Managed Access (UMA) and OAuth2 protocols that allows users (resource owners) to delegate access to other users (requesting parties) across security domains. The requesting party is responsible for creating the request, while the resource owner approves this request either when it is online or by creating a policy. The resource owner and the requesting party belong to different security domains administered by mutually isolated authorities, each with its own identity provider and authorization server. This concept uses a permission ticket issued by the resource owner's authorization server as a correlation handle that binds the requesting party's claims to the authorization process. An email address is used as the unique requesting party identifier for cross-domain access control.

Introduction

In ...

Problem

...

Current Situation

...

Current Flaws

cross-domain scenarios

Proposed Solution

.

Motivation

.

Main Concept

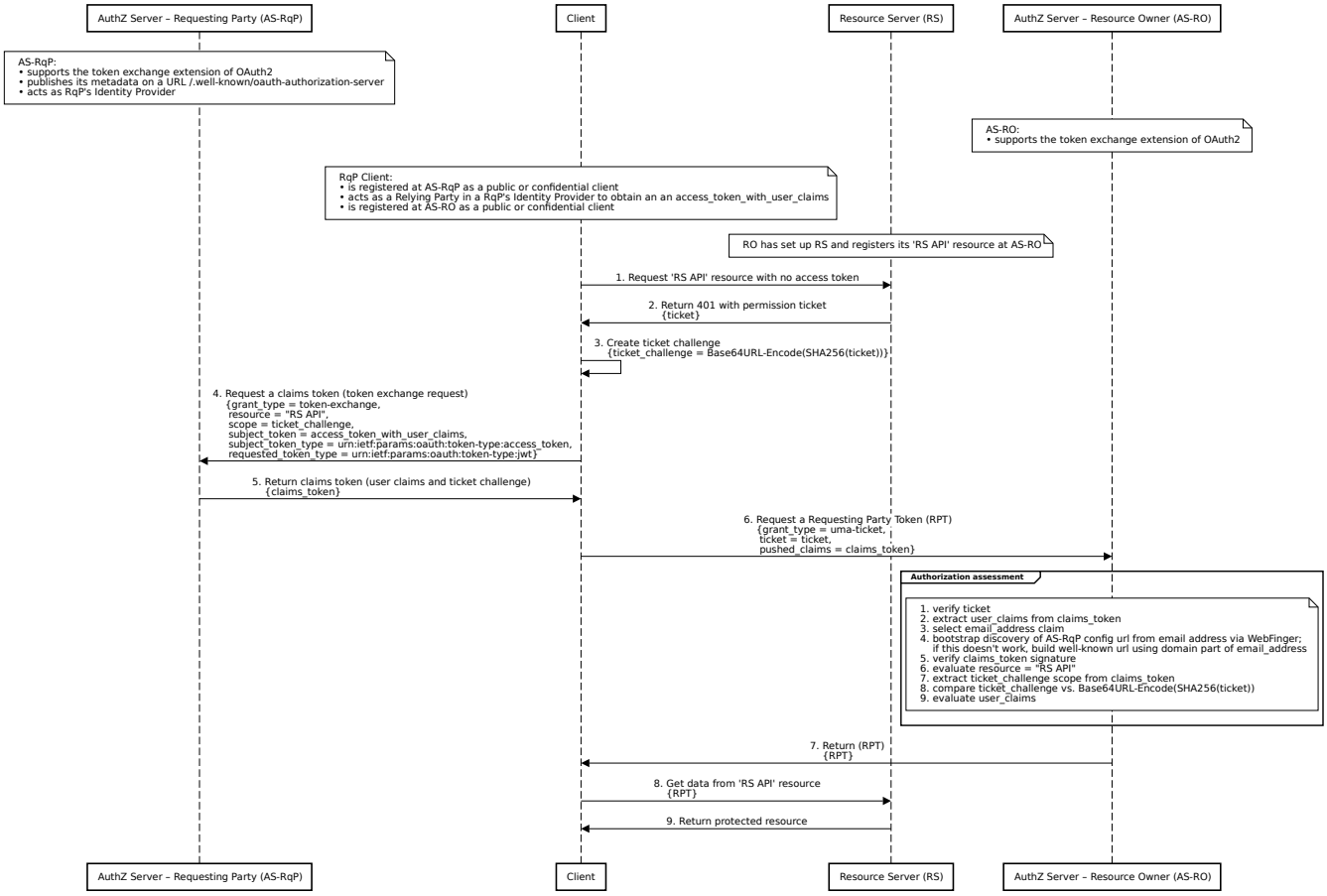
…

Sequence diagrams

There are two versions of the sequence diagram that describe the mechanism of the CAZ protocol. The first version represents the CAZ profile of the UMA protocol. The second version profiles the OAuth2 protocol. Both profiles rely on the token exchange extension of OAuth2, where an access token is used to obtain a claims token from the Security Token Service (STS) endpoint.

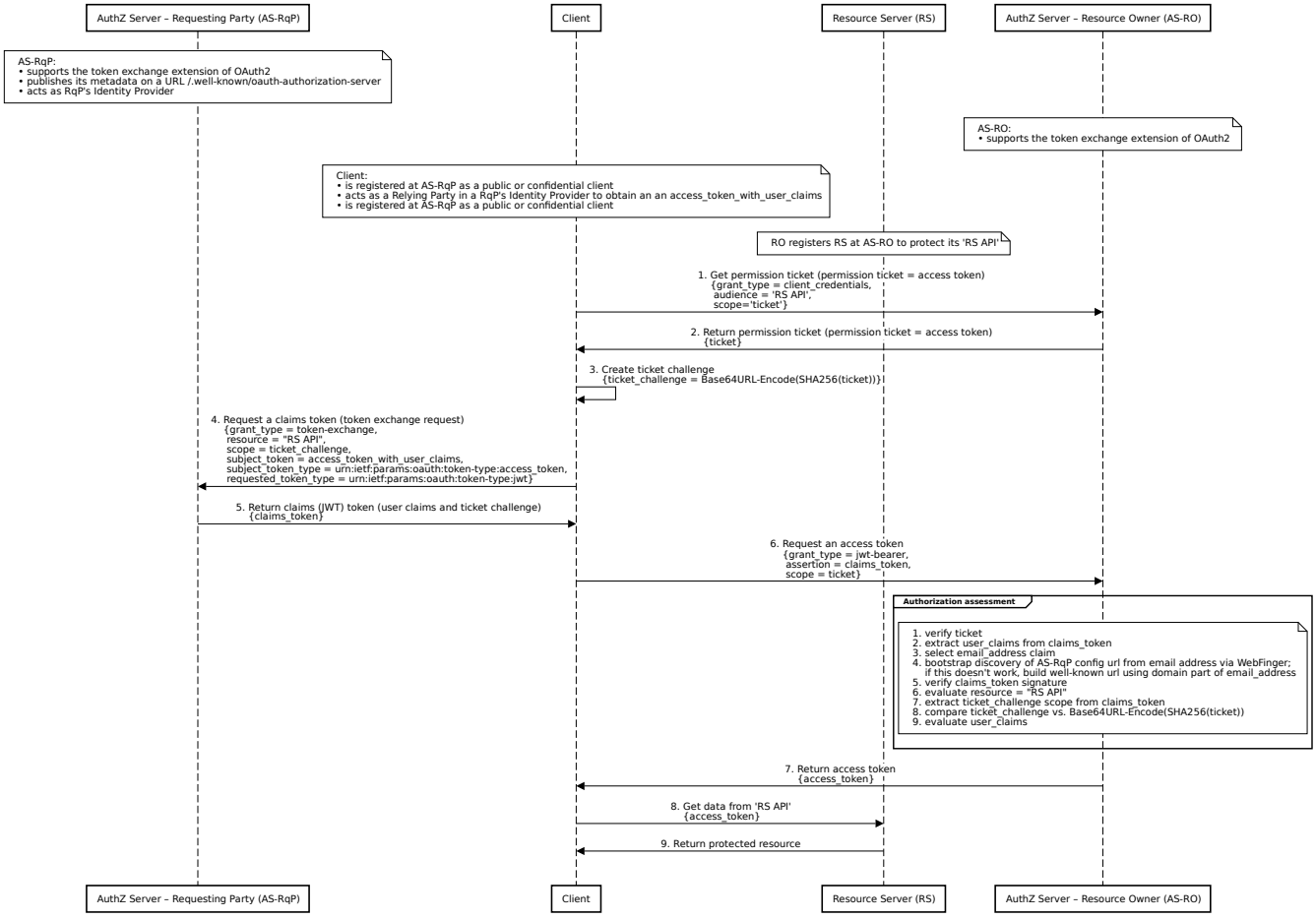
UMA profile

This diagram is in full compliance with the UMA specification.



OAuth2 profile

This diagram represents a profile of the OAuth2 protocol and lacks 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