AUTHLETE

OAuth 2.0

Introduction

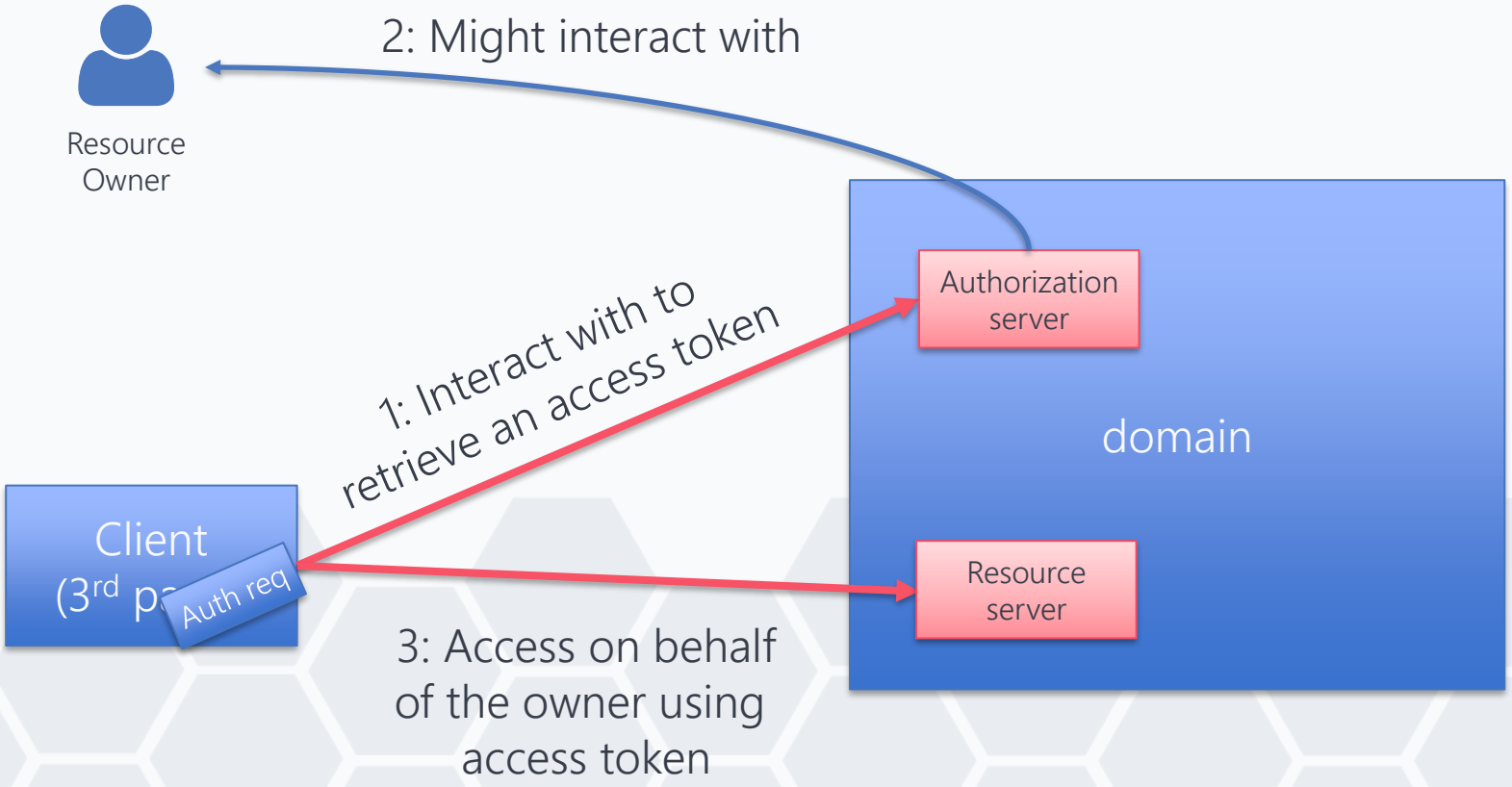
OAuth 2.0 Authorization Framework

- IETF standard published in 2012
  - RFC 6749
- Is not compatible with OAuth 1.0 that was published in 2010
- Simpler solution for simple use cases

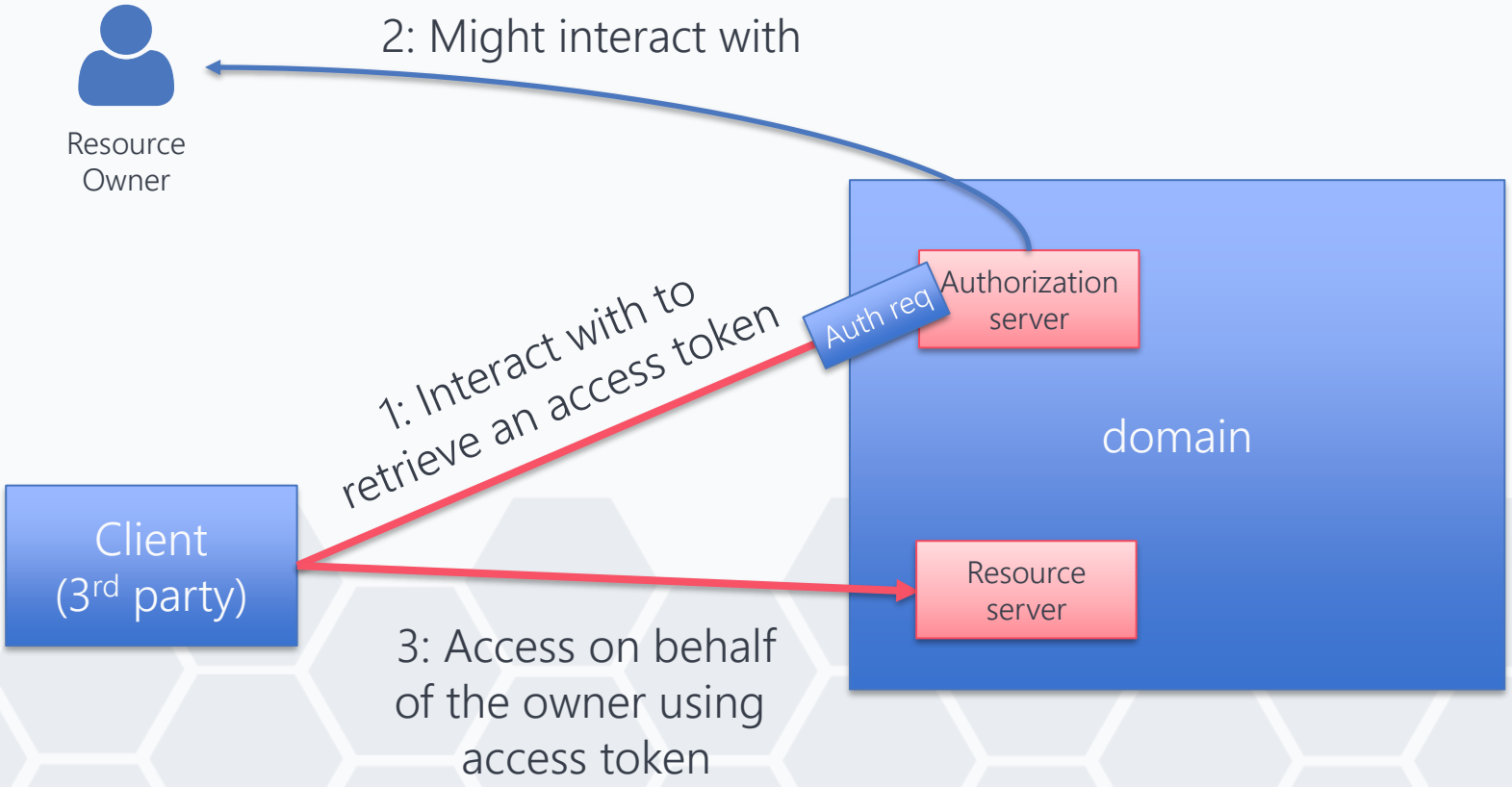
Scope of OAuth 2.0

It creates a framework for api clients accessing HTTP resources on a domain with a limited privileges granted by or on behalf of the owner of it.

Roles



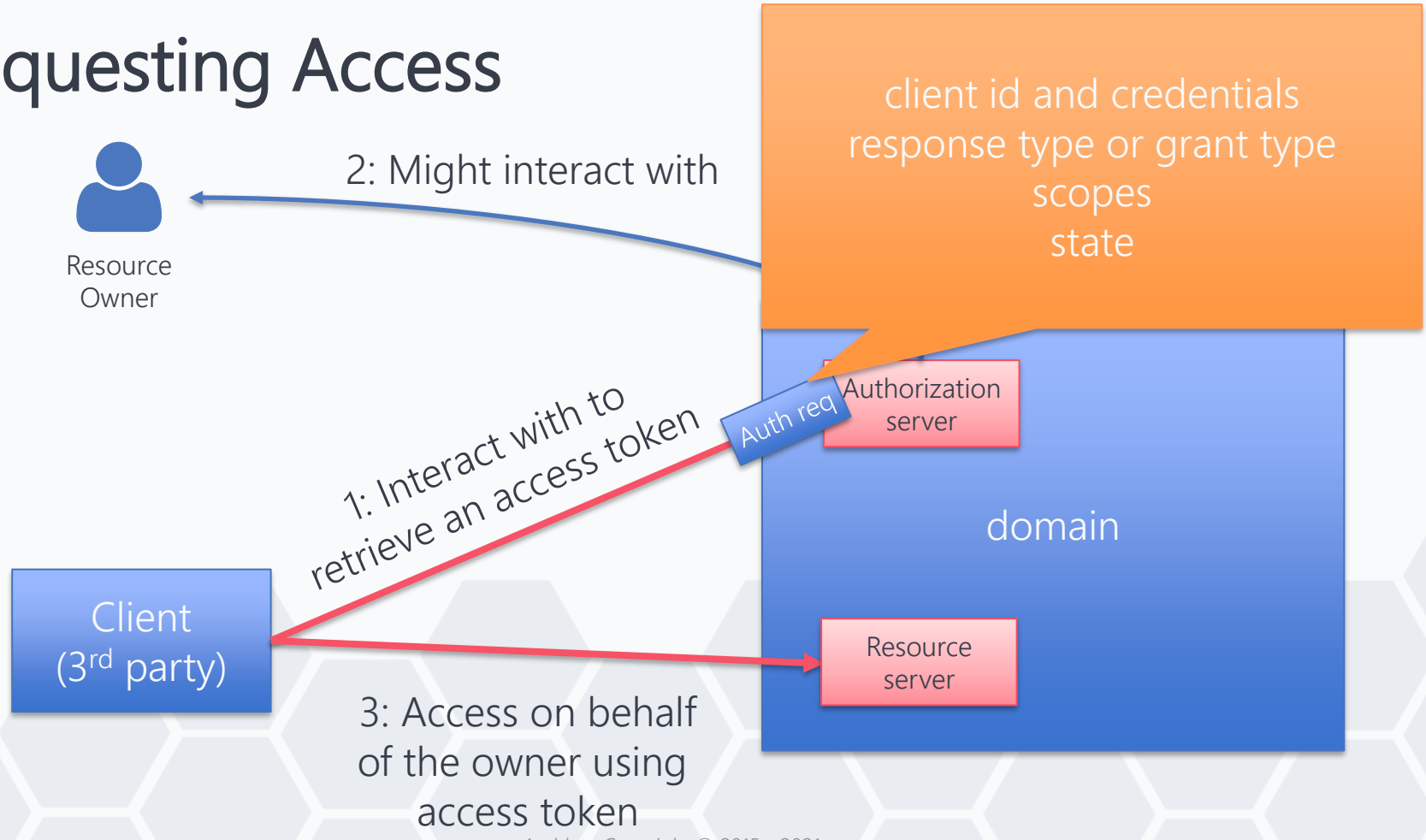
Requesting Access



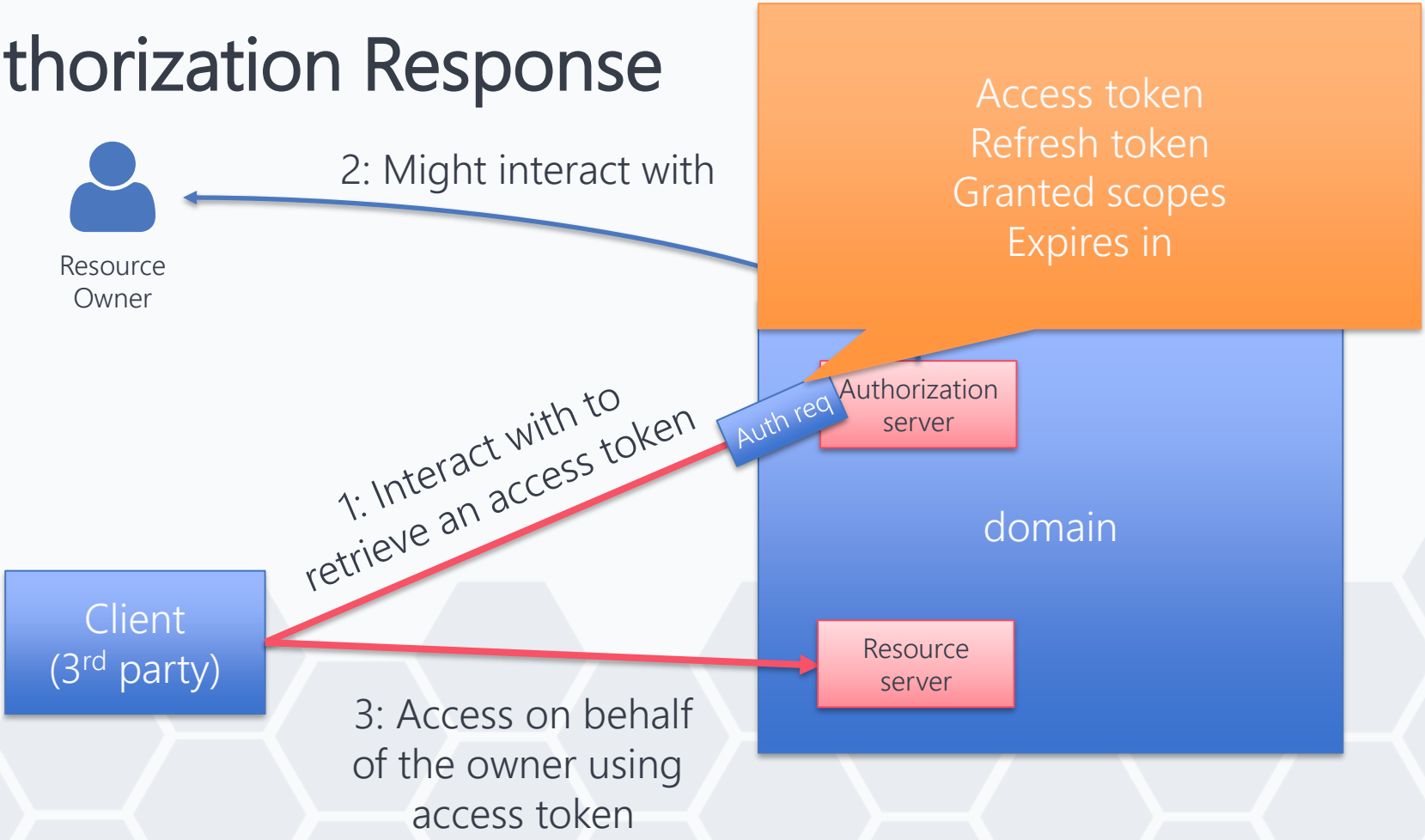
Authorization Server Endpoints

- Authorization
  - Used by the client to allow the resource owner interact with the authorization server in order to grant permissions
- Token
  - Used by the client to retrieve access tokens using grants from authorization or refresh tokens

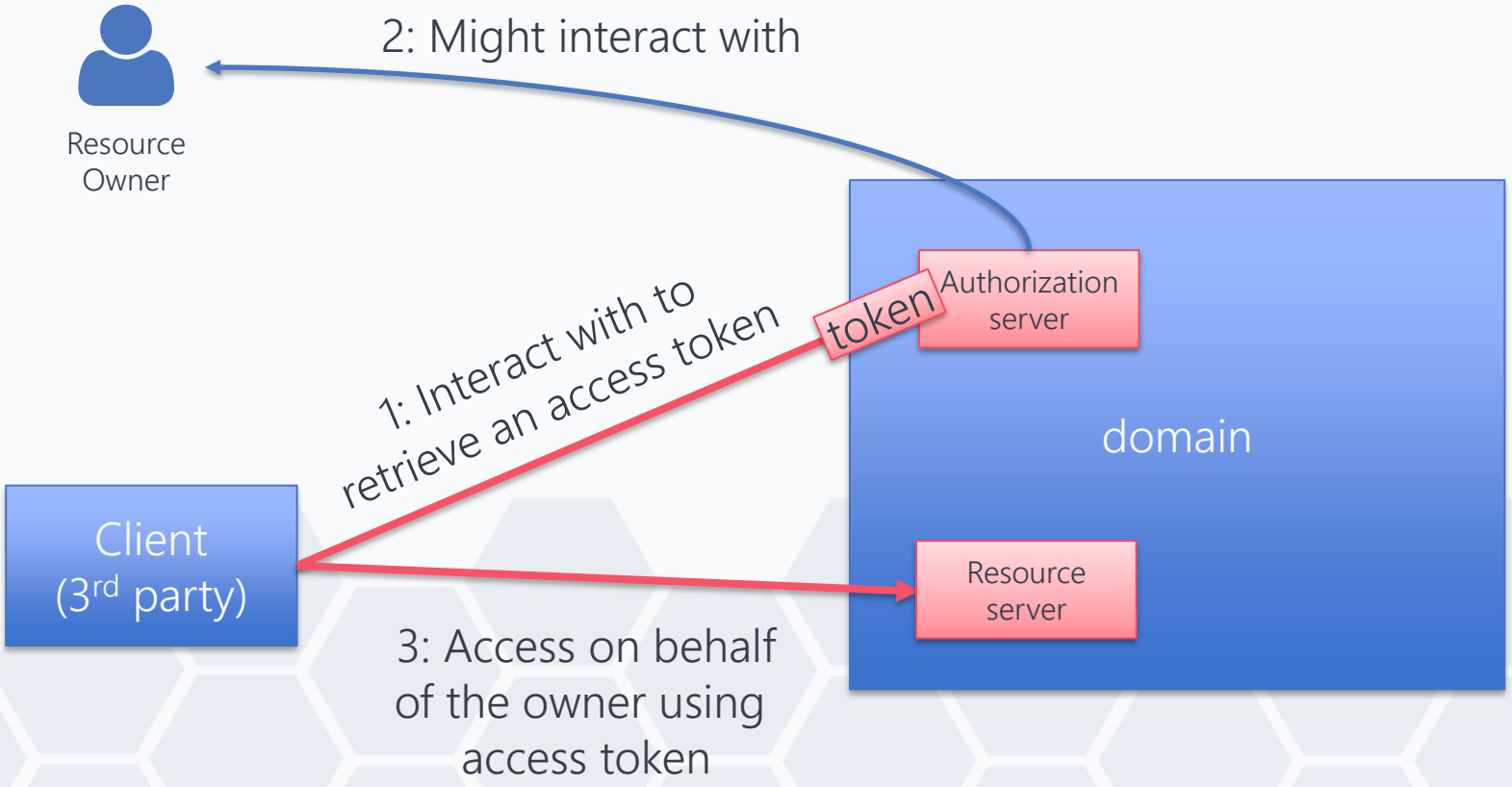
Requesting Access



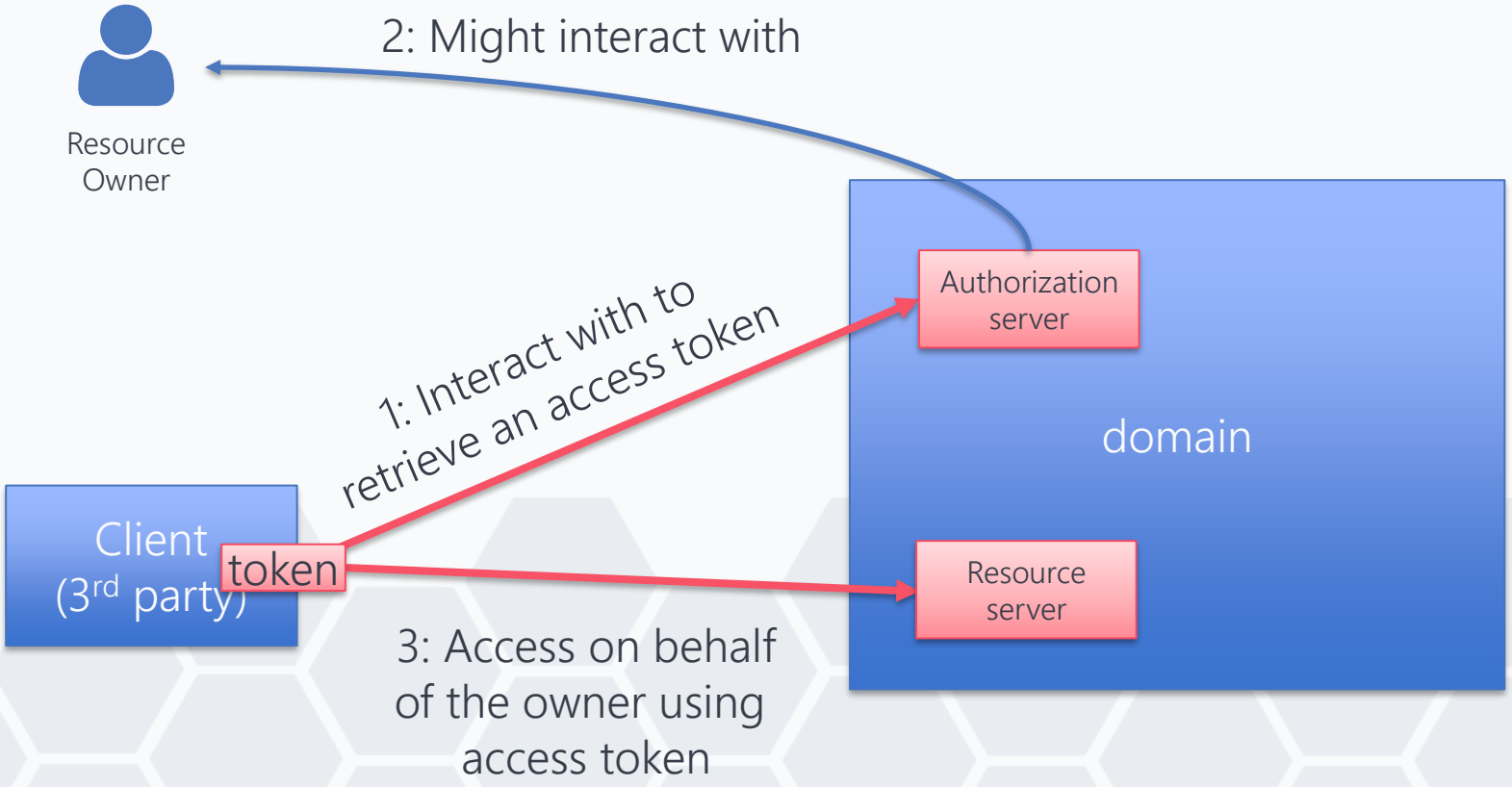
Authorization Response



Token Possession



Protected Resource Access



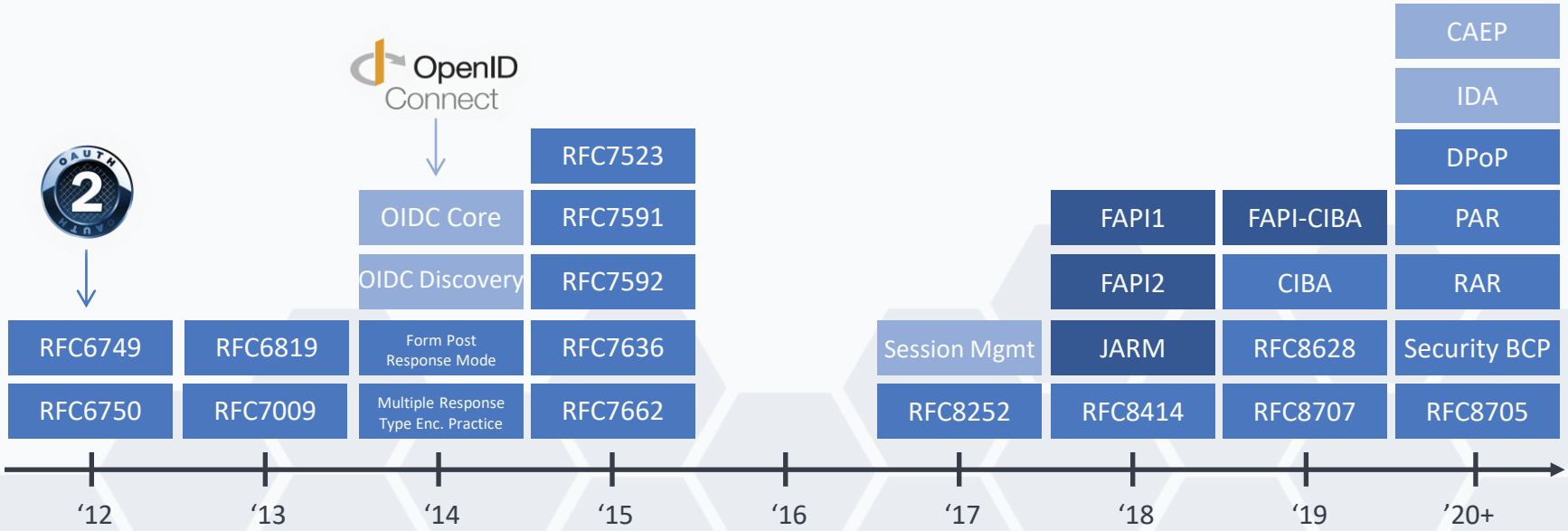
Client and Authorization Server interaction

- Different interaction are defined
  - Authorization code, Implicit, Resource owner
  - Client credentials
- Each interaction has different security properties and use differently the AS endpoints
- Other flows can be defined

OAuth 2

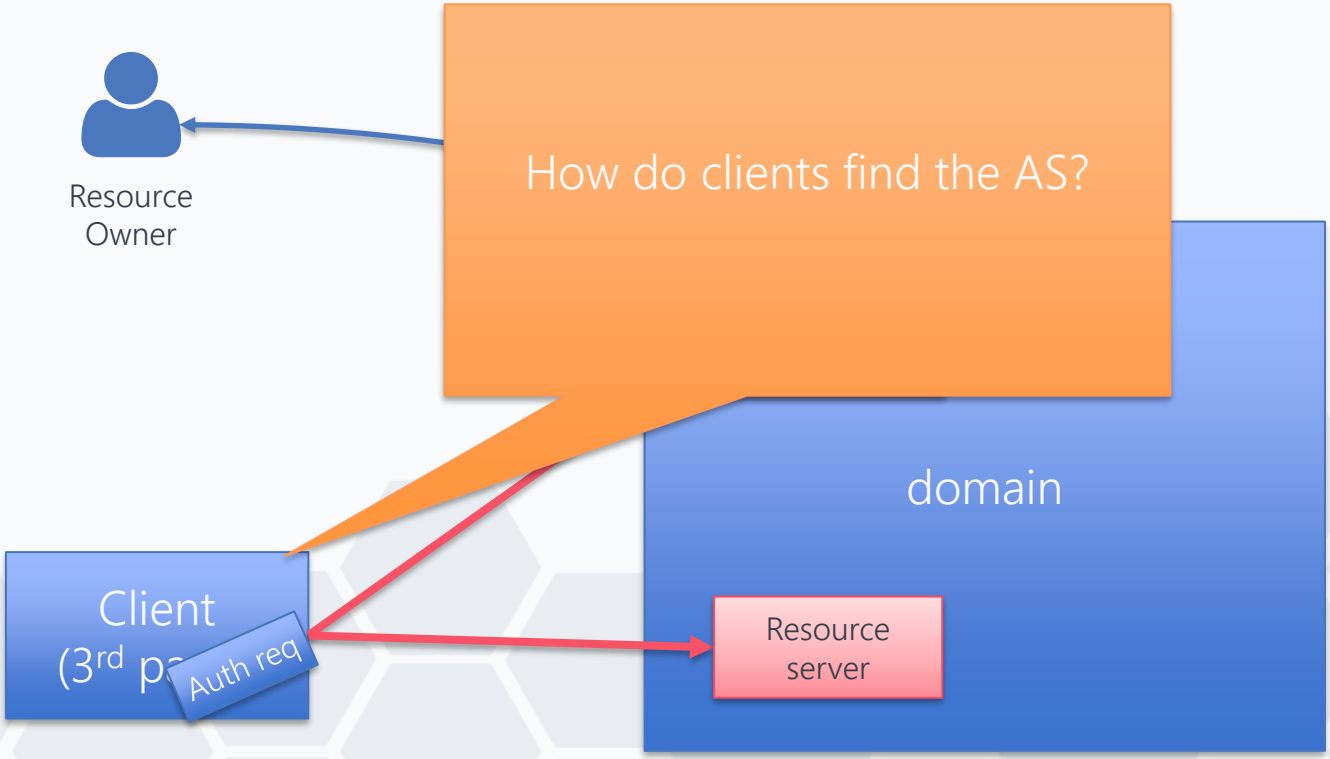
WHAT IS OUT OF SCOPE

Specifications towards financial industry



Not on Scope

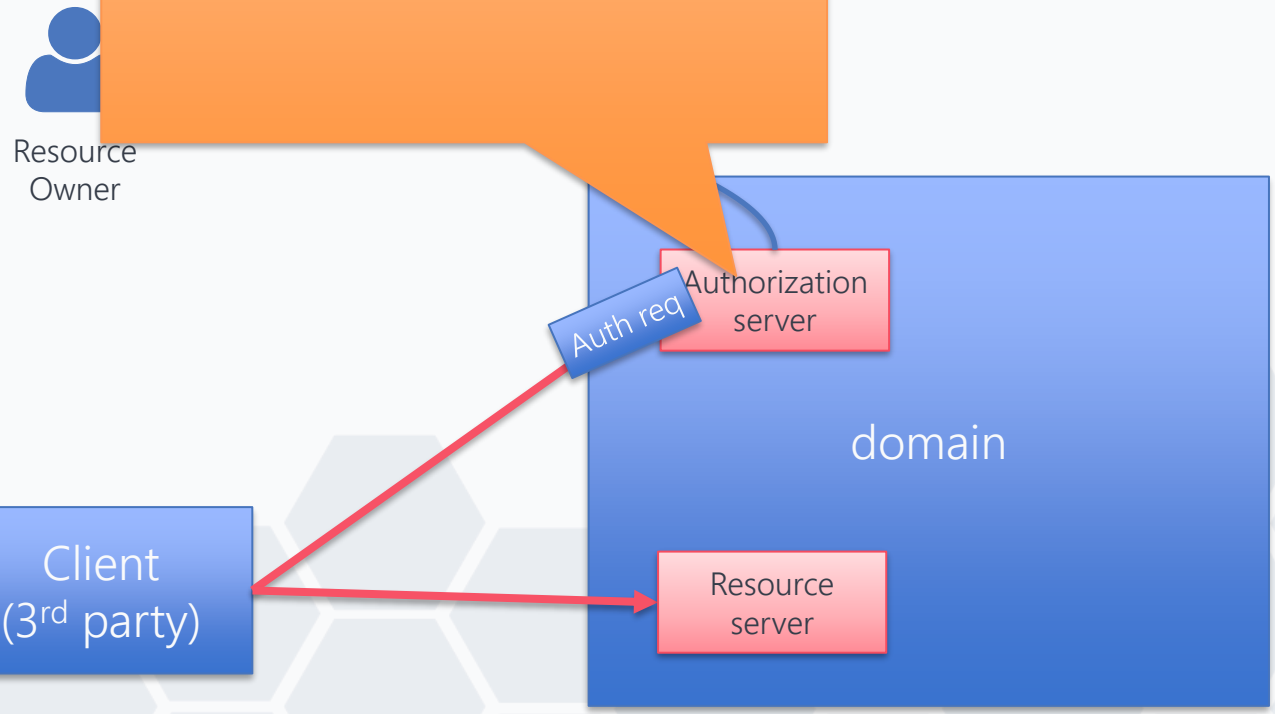
- OAuth Metadata
rfc8414



N

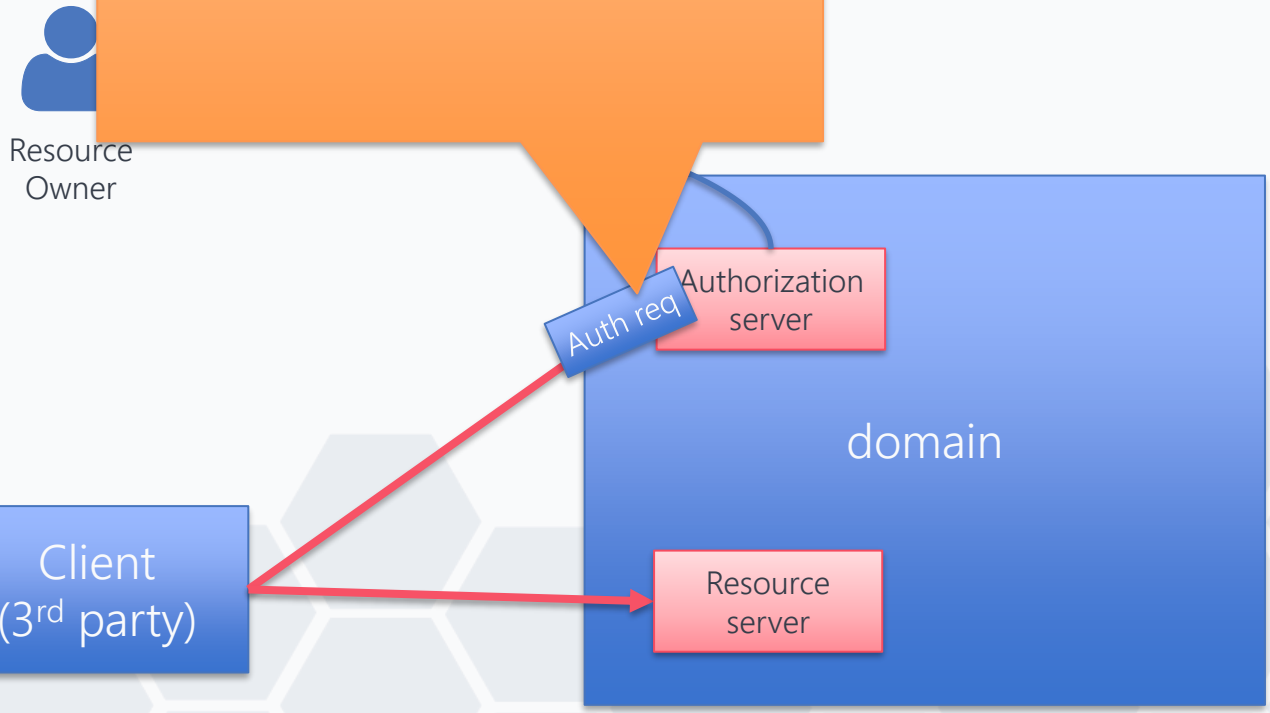
How are clients provisioned on AS?

- OAuth Metadata
  RFC8414
- Dynamic Client Reg.
  RFC5791



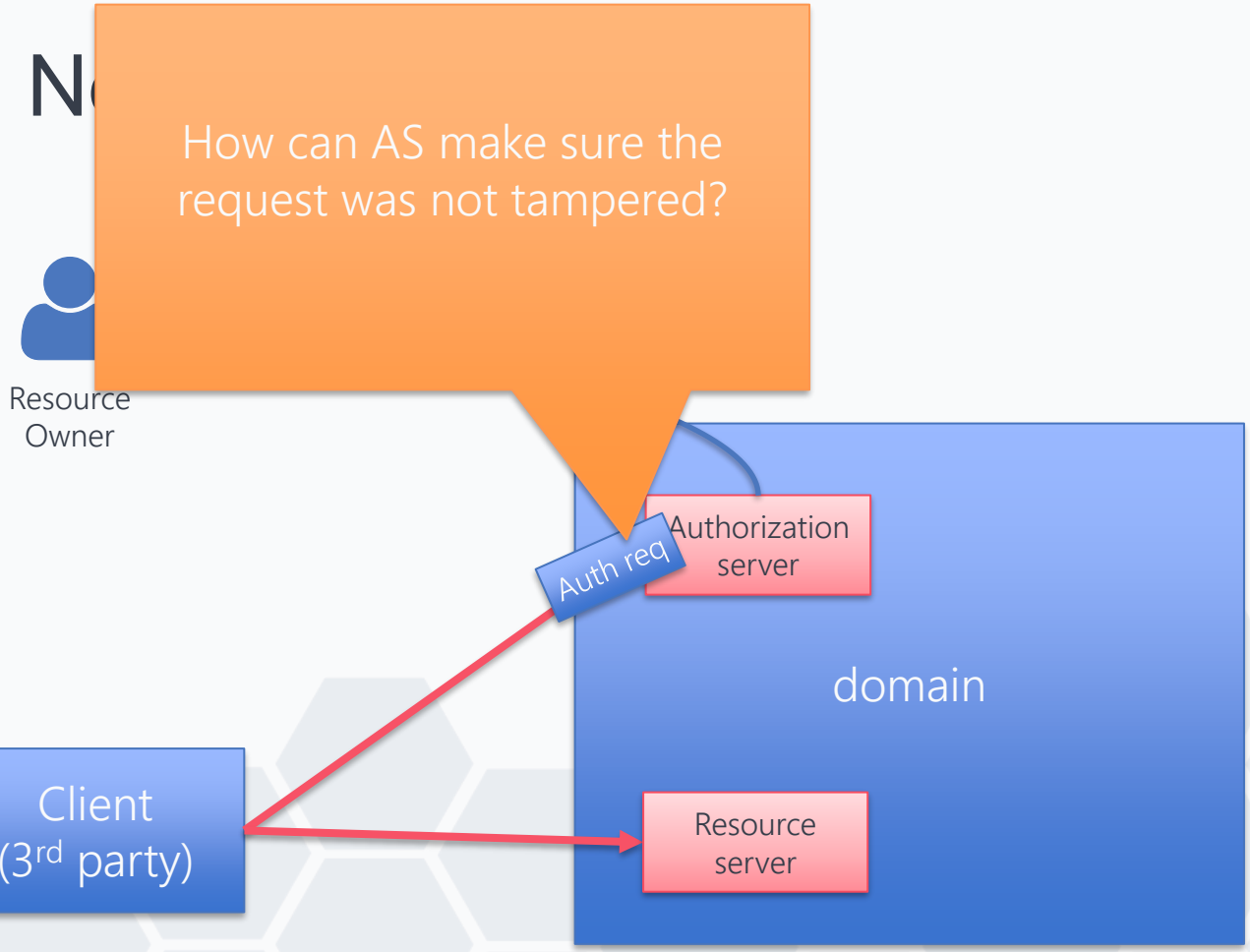
N

How can client express with resource it needs access?

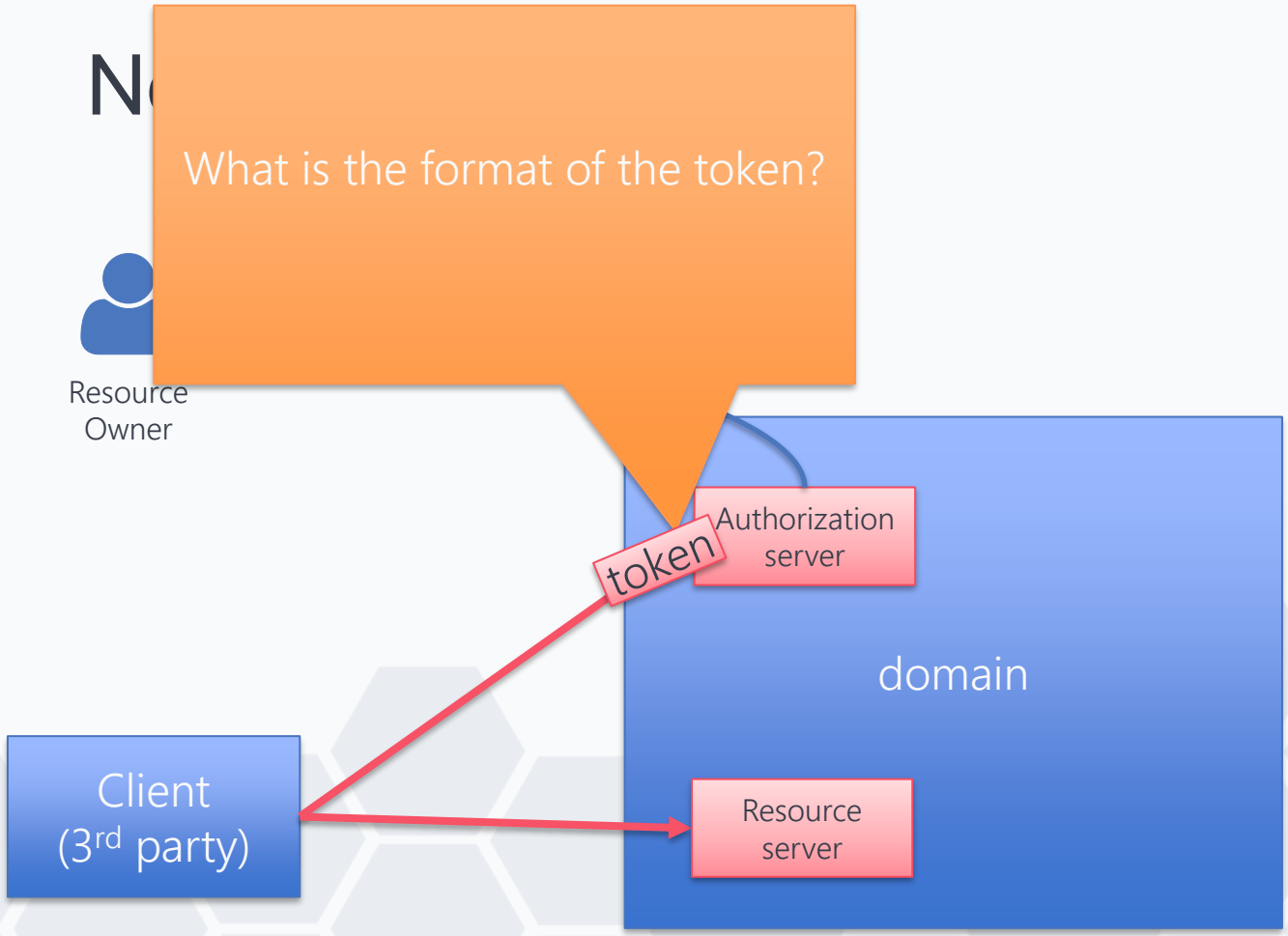


- OAuth Metadata RFC8414
- Dynamic Client Reg. RFC5791
- Resource Indicators RFC8707
- Rich Auth. Request RAR - Draft

N

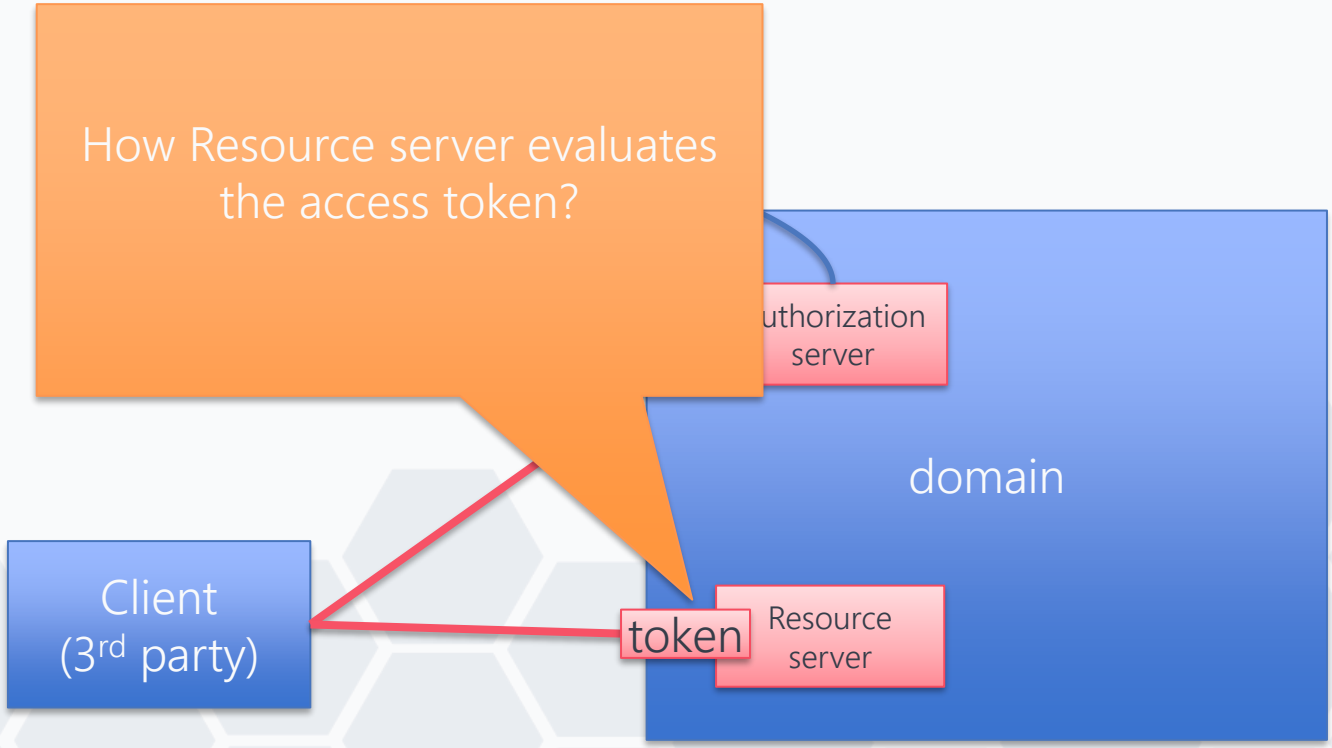


- OAuth Metadata
  RFC 8414
- Dynamic Client Reg.
  RFC 5791
- Resource Indicators
  RFC 8707
- Rich Auth. Request
  RAR - Draft
- Request Object
  OIDC Connect
- JWT Auth. Request
  RFC 9101
-



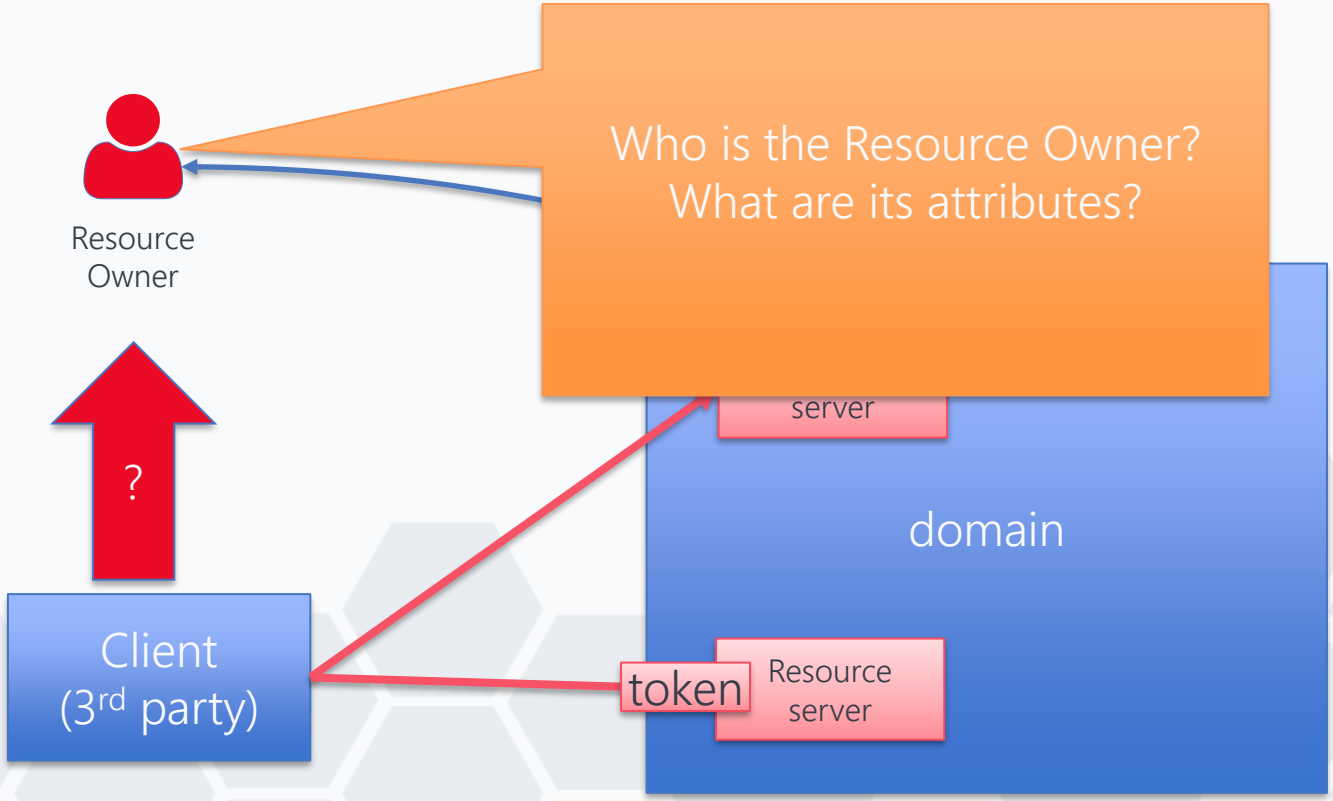
- OAuth Metadata
  RFC 8414
- Dynamic Client Reg.
  RFC 5791
- Resource Indicators
  RFC 8707
- Rich Auth. Request
  RAR - Draft
- Request Object
  OIDC Connect
- JWT Auth. Request
  RFC 9101
- JWT Profile
  RFC in queue

Not on Scope



- OAuth Metadata
  RFC 8414
- Dynamic Client Reg.
  RFC 5791
- Resource Indicators
  RFC 8707
- Rich Auth. Request
  RAR - Draft
- Request Object
  OIDC Connect
- JWT Auth. Request
  RFC 9101
- JWT Profile
  RFC in queue
- Access Token Introsp.
  RFC 7662

Not on Scope



- OAuth Metadata
  RFC 8414
- Dynamic Client Reg.
  RFC 5791
- Resource Indicators
  RFC 8707
- Rich Auth. Request
  RAR - Draft
- Request Object
  OIDC Connect
- JWT Auth. Request
  RFC 9101
- JWT Profile
  RFC in queue
- Access Token Introsp.
  RFC 7662
- OpenID Connect

OAuth 2.0

- Even with important requirements out of OAuth scope, it is a incredible success
  - A simple solution is provided for many use cases.
  - There are multiple extension mechanisms on OAuth and they are well consolidated.
    - It allowed OAuth to be used to build specifications for financial industry, health care ecosystems, IoT devices, etc.

AUTHLETE

OAuth 2.0

Introduction