OAuth2 and UMA for ACE

draft-maler-ace-oauth-uma-00.txt

Eve Maler, Erik Wahlström,
Samuel Erdtman, Hannes Tschofenig

Agenda

1. Motivation behind draft-maler-ace-oauth-uma-00.txt.
2. Mapping of existing IAM technologies to:
   - draft-ietf-ace-usecases-04.txt
   - draft-gerdes-ace-actors-05.txt
3. Door lock scenario.
4. Example flows using OAuth2/UMA.
   - Non-constrained
   - Constrained
5. Work needed to adopt IAM stack to constrained devices to fulfil the door lock scenario.

Motivation

- Approach of adapting already standardized and deployed technologies.
- Connect things, both big and small, to existing IAM infrastructures.
  - Use capabilities in AS today.
- Web and IoT is a continuum rather than an either or.
- Draft is an overview of OAuth2 and UMA for constrained devices.

Extract from IETF ACE Charter

- "Existing authentication and authorization protocols will be evaluated and used where applicable to build the constrained-environment solution. This requires relevant specifications to be reviewed for suitability, selecting a subset of them and restricting the options within each of the specifications.”

Mapping of use cases to existing IAM technologies

Problem statement	Existing IAM technology	Reason
* U1.7 The container owner and the fruit vendor may not be present at the time of access and cannot manually intervene in the authorization process.	OAuth2	School book OAuth2 (with refresh tokens)
* U4.1 The building owner and the companies want to be able to add new devices to their administrative domain (commissioning).	UMA	UMA provides resource set registration.
* U4.9 The companies want to be able to interconnect their own subsystems with those from a different operational domain while keeping the control over the authorizations (e.g. granting and revoking permissions) for their endpoints and devices.	OpenID Connect	With the help of identity federation you can take authorization decisions based on authentication done in other domains.
* U5.7 When authorization policies are updated it is impossible, or at least very inefficient to contact all affected endpoints directly.	Introspection	Introspection endpoint makes it possible to always have up to date policies, even when tokens are long lived..
* U1.11 Messages between client and resource server might need to be forwarded over multiple hops.	Object security	That will need object security.

Problem statement	Existing IAM technology	Reason
U4.5 The building owner and the companies want to be able to define context-based authorization rules.	Claims gathering	To be able to verify if a person really is from the fire department they could ask for additional claims from third party systems.
Actors draft: “One of the use cases of [I-D.ietf-ace-usecases] describes spontaneous change of access policies - e.g. giving a hitherto unknown client the right to temporarily unlock your house door. “	Dynamic client registration	All clients that will communicate with the AS need client creds and registration to be able to authenticate.
Actors draft: "In some use cases RS needs to authenticate some property of C, in order to bind it to the relevant authorization information. In other use cases, authentication and authorization of C may be implicit, e.g. by encrypting the resource representation the RS only providing access to those who possess the key to decrypt."	POP tokens	POP tokens also makes it possible to authenticate a C using a private key.
Actors draft: “We assume that the necessary keys/credentials for protecting the control information between the potentially constrained nodes and their associated less-constrained nodes are pre-established, for example as part of the commissioning procedure.”	Key provisioning using SCEP, EST and others.	Client credentials needs to be pre-provisioned to clients and the resource owners.

Door lock use case

- To see the feasibility of the existing IAM technologies we the door lock use case.

- Buy 100 new fancy connected door locks.
- Your users, authentication, authorization and reporting.
  - Use own AS instead of lock-vendors AS.

Authentication and authorization to the door lock

- Operator from office maintenance department mounts locks in doors.
- Operator now wants to initialize door lock in companies cloud door management system that includes an AS.
- Operator starts an app and authenticate to AS and is authorized retrieve a token that lets a lock add it self to the system.
- Phone sends token over BLE to lock and bundles info about system and AS.
- Door lock requests and receives keys and registers it self.

Door lock access

- All employees of an organization have phone app.
- Phone sends a token to door, token is verified and the door is opened.
- Different policies
  - Daytime access, direct access.
  - Nighttime access, extra PIN.

Use cases shows following abstract interactions.

Abstract bootstrap flows – Step 1

- Out of scope for this talk but not from the use case.

- Resource servers and clients needs resource discovery, AS URI, and provisioning keys.
- Given to device by:
    - Chip manufacturer
    - OEM
    - Operator

Abstract bootstrap flows – Step 2

- Resource server registers to Authorization Server
  - using a predefined server
  - to any server
- Client registers to Authorization Server

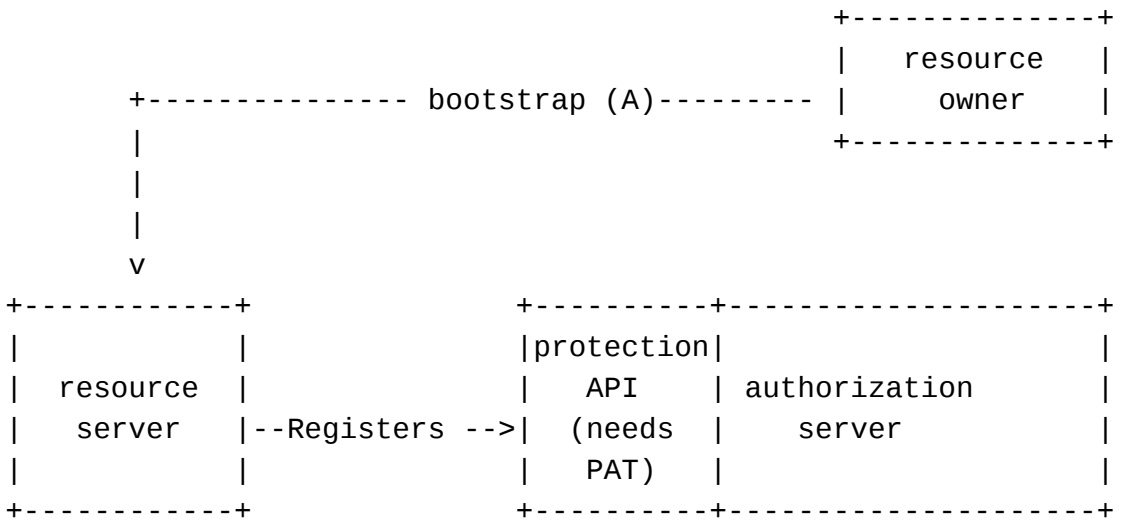
Abstract access flows

- Several difference access scenarios
  - Resource Server (door) and Client (phone or open button) are both online.
  - Resource Server is offline, but Client is online.
  - Client is offline, but Resource Server is online.
  - Resource server and client are both offline.
- Different constraints
  - Neither the Resource Server and the Client is constrained.
  - One of them are constrained.
  - Resource Server and the Client are both constrained.

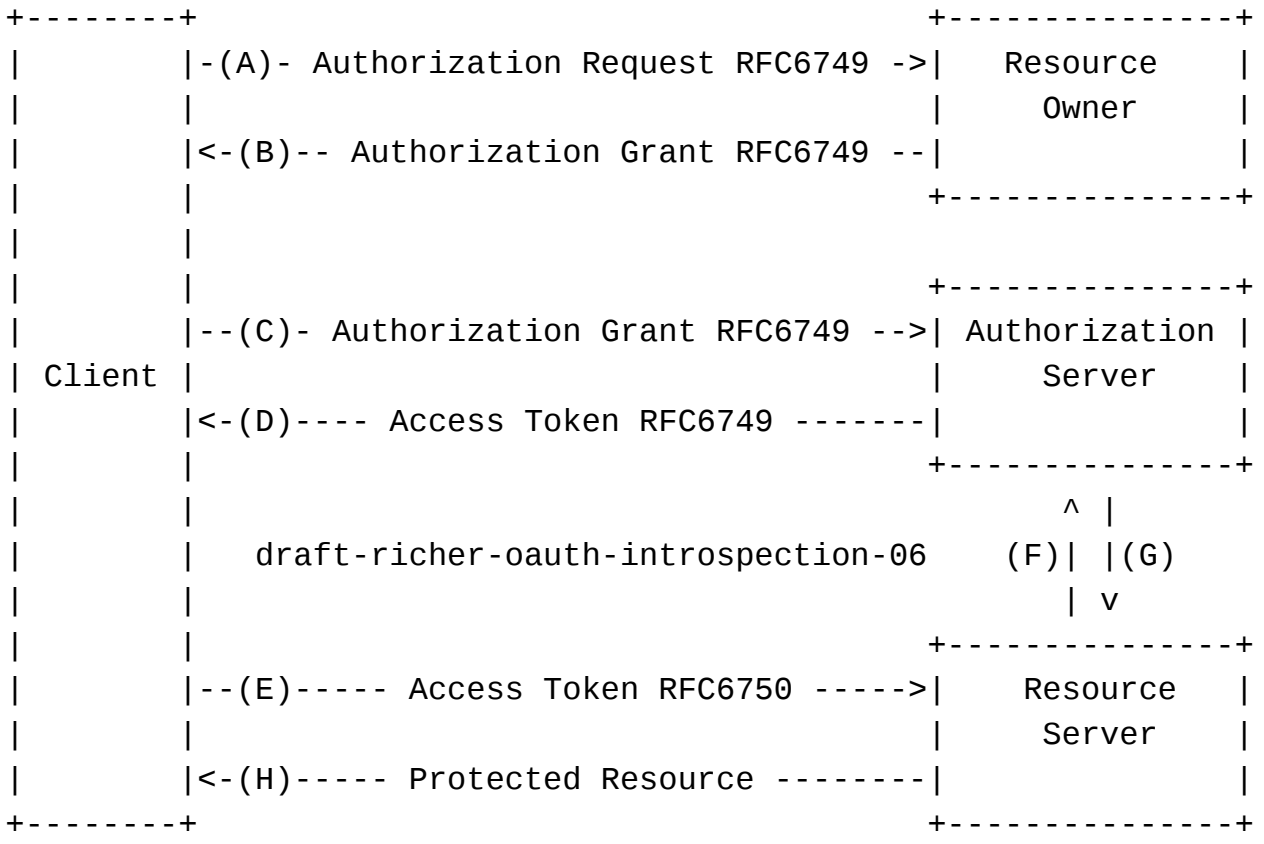
Existing IAM technology in AS

Unconstrained resource server and client.

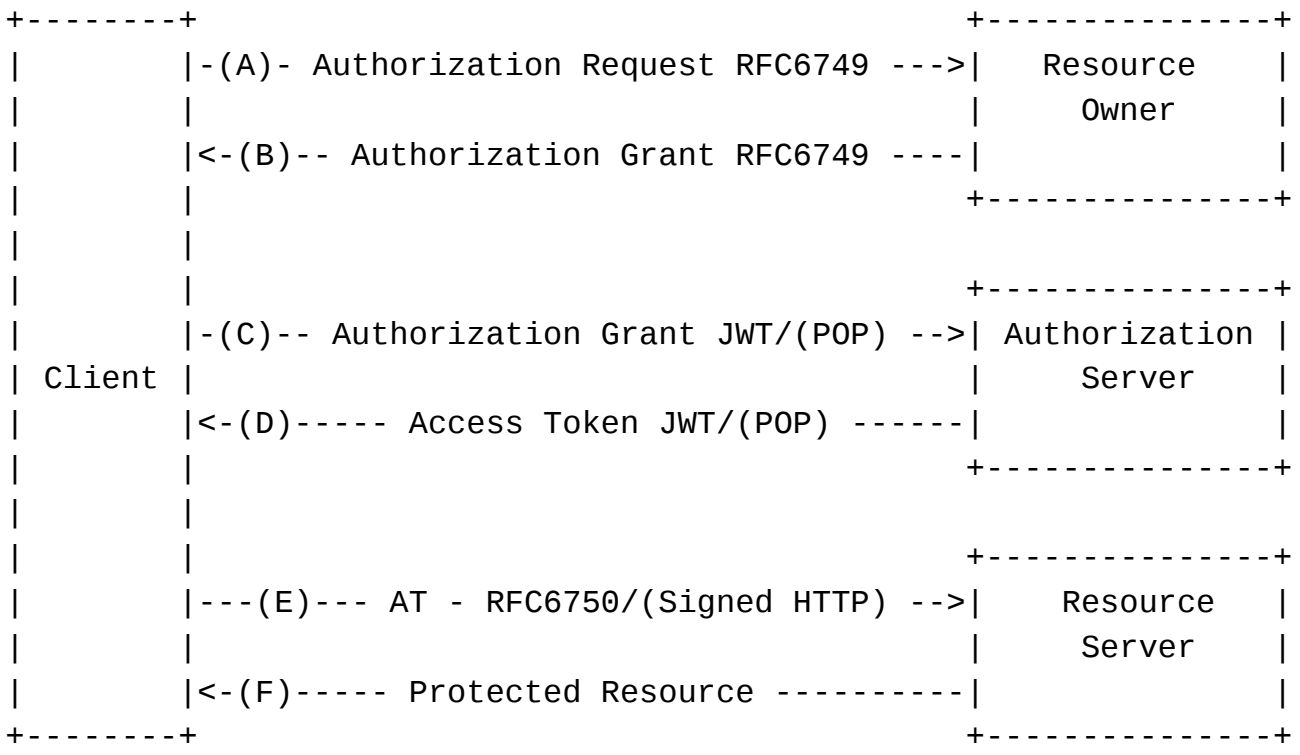
Bootstrapping resource registration



Both online


Client
Resource Owner
Authorization Server
Resource Server
(A)- Authorization Request RFC6749
(B)-- Authorization Grant RFC6749
(C)- Authorization Grant RFC6749
(D)---- Access Token RFC6749
(E)----- Access Token RFC6750
(F)
(G)
(H)----- Protected Resource
draft-richer-oauth-introspection-06

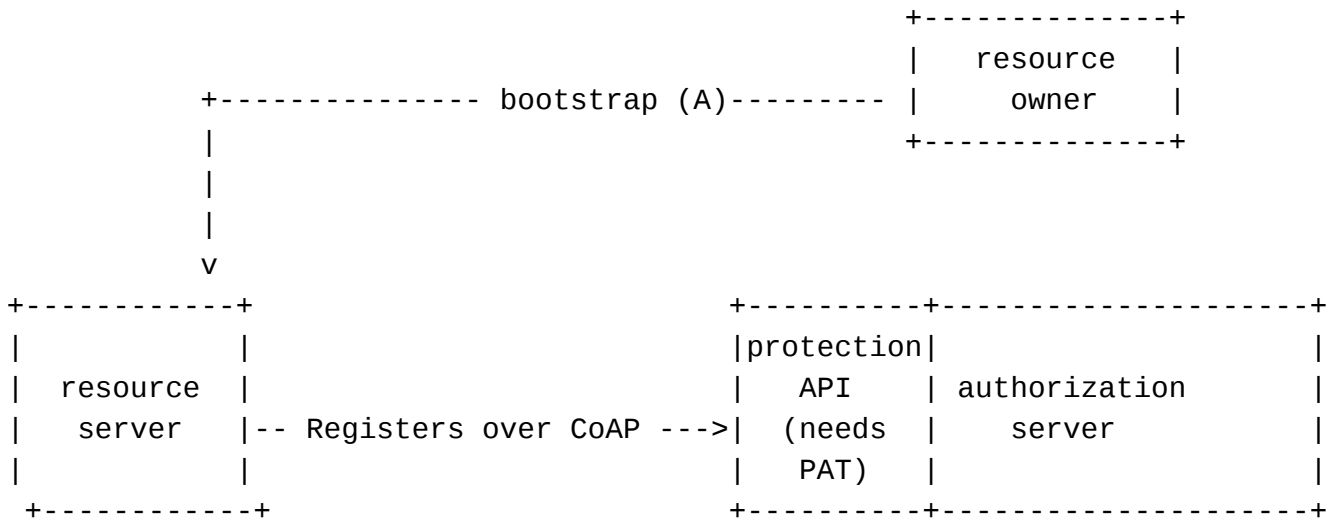
Both offline



Adopted technologies for constrained devices

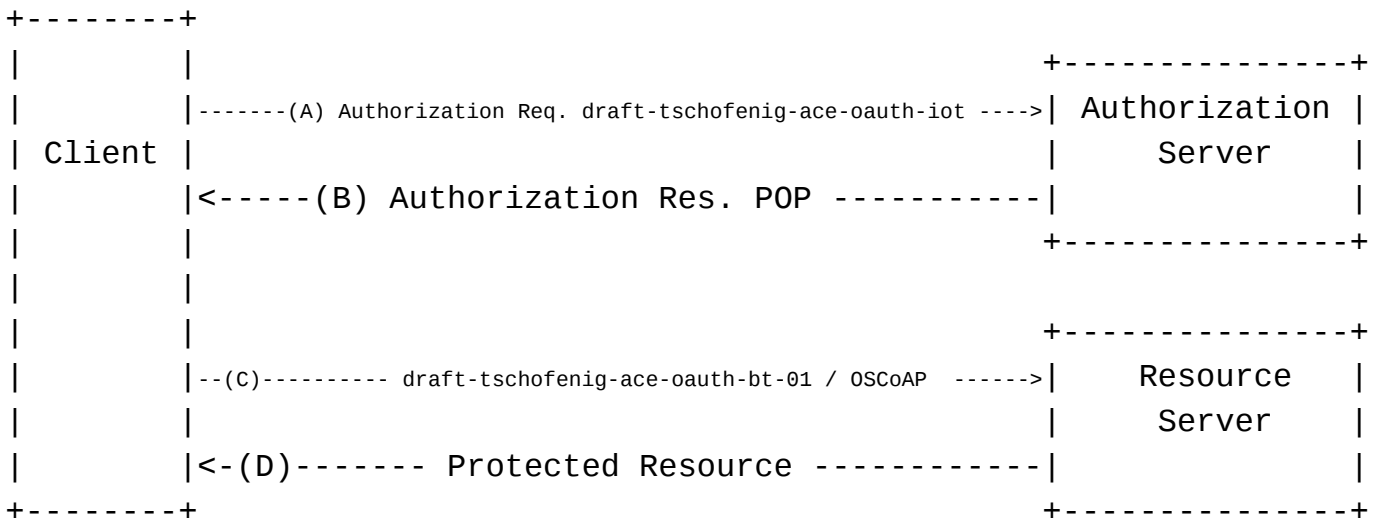
Constrained client and resource server

Bootstrapping resource registration



Resource Server and Client are both online

Both offline



Document Roadmap

	Function	Spec
Out of scope, but needed	**Initial device provisioning (keys, config)**	
	Discovery (/.well-known/ mapping)	
bootstrap	**CoAP mapping of UMA resource-set registration**	
access	**CoAP dynamic client registration**	
	CoAP client credentials grant flow	draft-tschofenig-ace-oauth-iot-01
	CoAP bearer token	draft-tschofenig-ace-oauth-bt-01
	CoAP introspection endpoint	draft-wahlstroem-ace-oauth-introspection-01
	Object security	draft-selander-ace-object-security-02
offline / proof of possession	**CoAP mapping for claims gathering in UMA**	
	POP key distribution	OAuth PoP

Next steps

- Seeking input from other IAM vendors on the integration with existing infrastructure.
- Work on missing specifications
- Gain more implementation experience