Attestation for the Registration Endpoint

HANNES TSCHOFENIG + JAN HERRMANN (SIEMENS), NED SMITH (INTEL), THOMAS HARDJONO (MIT)

draft-tschofenig-oauth-attested-dclient-reg-01.html
Motivating Use Case

Client demonstrates that it runs in a confidential compute environment
Client is configured with credentials and other meta-data.
Attestation in Dynamic Client Registration

Attestation can be used with different endpoints in OAuth.

This document supports attestation within the registration endpoint.

Draft uses RATS architecture.
  ◦ Details communication pattern for background check and passport models.
  ◦ A description of the passport model is in process.
Passport Model

1. Obtain Attestation Result (passport)

2. Dynamic Client Registration

3. Obtain Access Token

4. Present Access Token

Client

RATS Verifier

AS

Resource Server

this draft

existing OAuth2
Passport Model

1. Attestation Result (passport)
   - RATS Verifier
   - Obtain

2. Dynamic Client Registration
   - AS
   - Obtain Access Token

3. Access Token
   - Resource Server
   - Present Access Token

4. this draft
   - existing OAuth2

Verifier checks Client is a valid CCE

AS policy performs DCR if Client is a valid CCE

RS policy uses an AS that does attested DCR
Next Steps

Standardization effort of draft minimalistic – mostly architectural aspects
Prototype implementation to gain feedback
Input from interested parties welcome
Adopt?