The Use of Attestation in OAuth 2.0 Dynamic Client Registration

draft-tschofenig-oauth-attested-dclient-reg-00

H. Tschofenig, J. Hermann

IETF#117
Motivation

- Renewed interest in remote attestation technologies based on available hardware, desire to improve security, and new technologies (e.g. confidential computing).
- Ongoing standardization to utilize attestation in
  - Network management protocols
  - Transport Layer security
  - Certificate Signing Requests
  - IoT device onboarding protocols
- Unfortunately a wide range of attestation technologies available (from TPMs to DICE).
Why do we want to use attestation?

- Information about the manufacturer of the hardware,
- the version of the firmware running on this hardware and
- potentially about the layers of software above the firmware,
- the presence of hardware security functionality and
- many more properties can be made available to remote parties in a cryptographically secured way.

Full story – RFC 9334 (RATS Architecture).
Examples of what can be exposed with attestation – EAT
Attestation Terminology

Document uses **passport model** from RFC 9334

- Attested
- Relying Party
- Verifier
- Evidence
- Attestation Result
Many attestation technologies rely on nonces for freshness.
Attestation for Dynamic Client Registration

- Improve security of dynamic client registration by using attestation technologies.
  - Think of it as a more secure version of a software statement.
  - Re-uses features of dynamic client registration (including key registration)
- Attestation technologies in general rely on the presence of some hardware root of trust.
  - Those have become available in form of Trusted Execution Environments (Enclaves), and Secure Elements.
- Work suggests to take advantage of ongoing work in other areas of the IETF to improve security of OAuth.
Collaboration appreciated.

Interest in running code?