Raw-Public-Key and Pre-Shared-Key as OAuth client credentials

By
Samuel Erdtman and
Ludwig Seitz

Acknowledgements

This document is highly inspired by [I-D.ietf-oauth-mtls] written by B. Campbell, J. Bradley, N. Sakimura and T. Lodderstedt.

Thank you Brian Campbell for your review.

Two new OAuth Client Credentials

Raw-Public-Key

(D)TLS handshake is done according to [RFC7250] to authenticate the client.

Pre-Shared-Key

(D)TLS handshake is done according to [RFC4279] to authenticate the client

Scope

In Scope

Token requests and

Introspection requests

Out of Scope

Client binding of resource requests

Relates to

RFC 7521 - 7523

Specifies how to use assertions such as SAML and JWT as OAuth 2.0 client credentials

draft-ietf-oauth-mtls

Specifies how to use X.509 certificates as OAuth 2.0 client credentials

One credential per Client Software Instance

Common case in constrained environment

Devices are pre-provisioned with keys to identify them

Dynamic registration

This specification registers two new attributes to enable dynamic registration of the RPK and PSKs