Transporting Access Tokens

draft-seitz-ace-oauth-authz-00

Ludwig Seitz (ludwig@sics.se)

IETF ACE WG interim meeting
March, 2016

How to get there from here

- This issue is about getting the token from the Client to the Resource Server
- Possible options
  - POST to a well-known or discoverable resource (e.g. /authz-info)
  - Use a dedicated CoAP option
  - Use TLS supplemental data (RFC 4680)
  - Use psk_identity (DCAF)
  - Define new TLS certificate type (similar to RPK)
  - Other suggestions?

POST to /authz-info

+ Works for both (D)TLS and object security

+ Possible to update access token during a secure session

- Requires a resource without access control

- Requires a separate request

Dedicated CoAP option

+ Works for both (D)TLS and object security

+ Possible to update access token during a secure session

+ No additional messages (token sent with request)

+ Works for requests that have no payload (GET, DELETE)

- Can lead to problems with fragmentation

Use RFC 4680

+ Works for (D)TLS

+ Access token transferred during the handshake

- Requires new handshake to update token

- RFC 4680 : “Any such data MUST NOT need to be processed by the TLS protocol.”

    → Cannot transfer keys or certificates in the token that are used for the handshake

Use psk_identity

+ Works for (D)TLS

+ Access token transferred during the handshake

- Requires new handshake to update token

- Weird use of psk_identity (it's not really a key identity we are transmitting here)

Define new certificate type

+ Works for (D)TLS

+ Access token transferred during the handshake

+/- Could be done similarly to raw public keys (RFC 7250)

- Requires work in the TLS WG

- Defines a whole new handshake for a very specific problem

Thank you!

Questions/comments?