Follow-Up Activities

Marco Tiloca, RISE

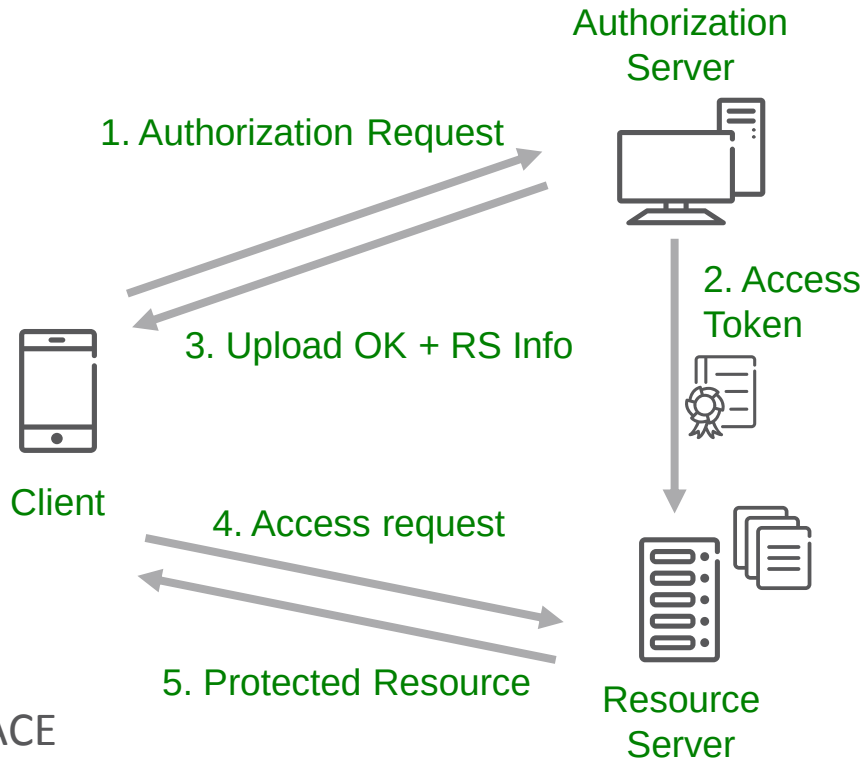
IETF 116 meeting – Yokohama – March 30th, 2023

Possible new work items

- **Ideas brought up while working on the EDHOC and OSCORE profile**
  - https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/
- **Some were mentioned during the 2023-01-23 ACE interim meeting**
  - https://notes.ietf.org/notes-ietf-interim-2023-ace-01-ace
- **Applicability**
  - Some are in the interest of the ACE framework as a whole
  - Some are for specific profiles of ACE

1. New workflow for token upload

- **Upload of the Access Token to the RS**
  - Done by the AS, on behalf of the Client
  - The AS confirms the outcome to the Client
- **Currently in the EDHOC profile [1]**
  - Started to be defined
  - Example in Appendix A.3
- **This has general applicability**
  - It abstracts away from the used profile of ACE



[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

2. New message parameters

- **Some new parameters would be useful**

- **Confirm a successful token upload done by the AS**
  - In the AS-to-Client response from /token
  - Now defined in the EDHOC profile [1], as the boolean “token_uploaded”

- **Provide the Client with public keys of multiple RSs**
  - The intended audience can comprise multiple RSs (for the same Access Token)
  - “rs_cnf” can specify only one public key
  - A new “rs_cnf2” could transport the public keys of all the RSs
  - A new “subject_id” could transport the RS identifiers paired with the public keys

[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

3. Certificates in DTLS/TLS profile

- **The DTLS/TLS profile [2][3] has an asymmetric mode**
  - Today it supports only COSE Keys as Raw Public Keys
- **The EDHOC profile [1] uses other asymmetric authentication credentials**
  - X.509/C509 certificates, CWTs, CCSs
  - Registered new CWT confirmation methods: x5chain, x5t, ...
- **The DTLS/TLS profile could also use certificates as authentication credentials**
  - Based on the same CWT confirmation methods registered in the EDHOC profile

[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/
[2] https://datatracker.ietf.org/doc/rfc9202/
[3] https://datatracker.ietf.org/doc/draft-ietf-ace-extend-dtls-authorize/

Summary and next steps

› **Possible new work items**

1. New workflow for uploading Access Tokens: AS → RS
2. New message parameters, e.g., “rs_cnf2” with multiple RS public keys
3. Certificates as authentication credentials in the DTLS/TLS profile

› **Write related Internet Drafts**

– One document can cover (1)(2)
– Another document can cover (3)
– Looking for interested co-authors

› **Comments and feedback are welcome**

Thank you!

Comments/questions?