

EDHOC-OSCORE profile of ACE

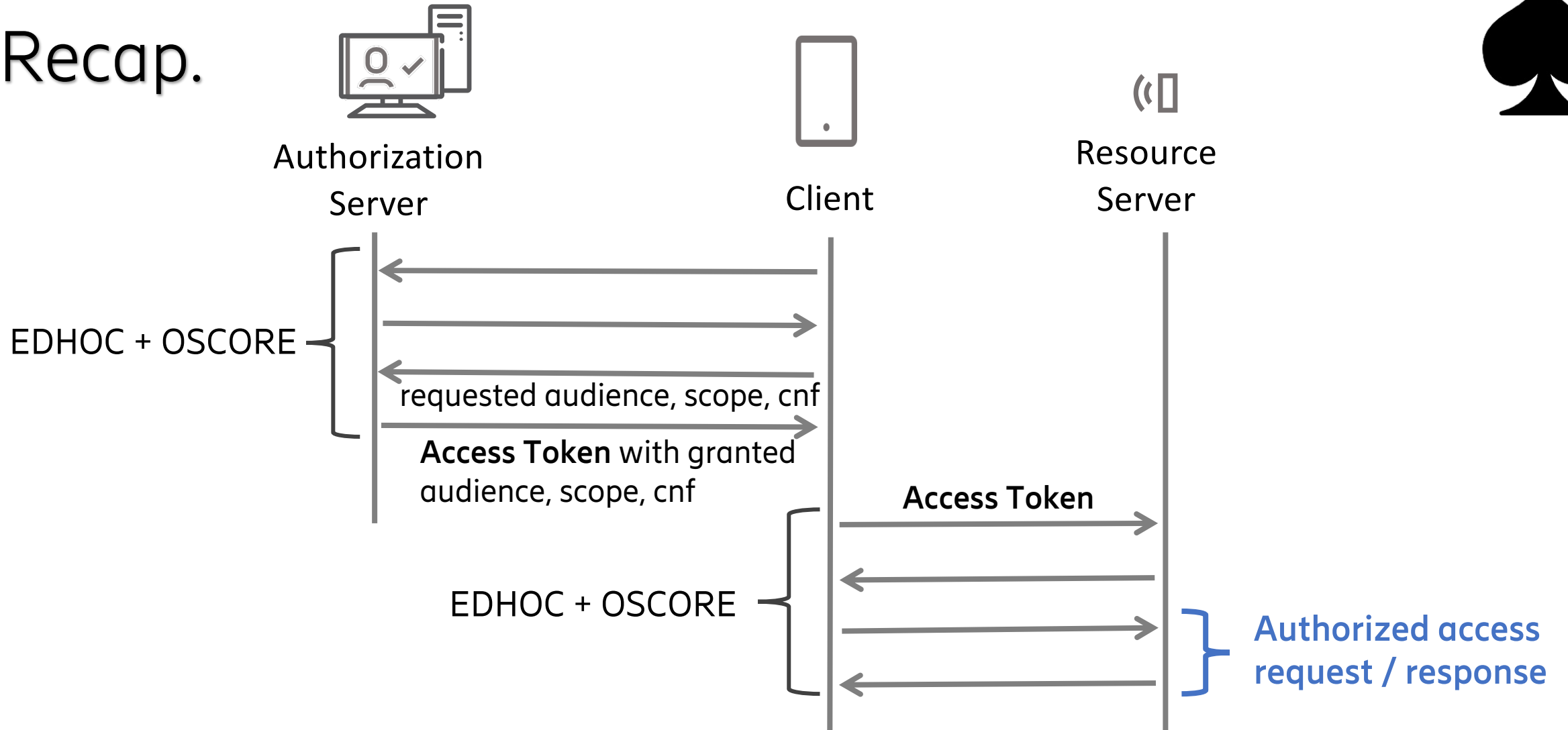
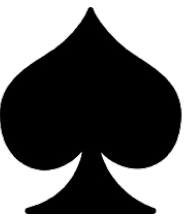


draft-ietf-ace-edhoc-oscore-profile-03

<https://github.com/ace-wg/ace-edhoc-oscore-profile>

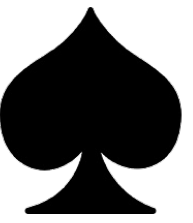
IETF 118, ACE WG, November 10, 2023

Recap.

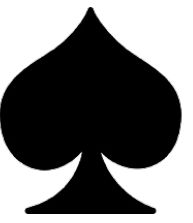


- Optimized workflow, appendix A.2
- EDHOC + OSCORE = draft-ietf-core-oscore-edhoc

This presentation slot



- News draft-ietf-ace-edhoc-oscore-profile-03
- Sketches of next steps
- Request WG feedback



New in -03:

- Restructured presentation of content
- Simplified description of the use of EDHOC_Information
- Merged the concepts of EDHOC "session_id" and identifier of token series
- Enabled the transport of the access token also in EDHOC EAD_3
- Defined semantics of the newly defined CWT/JWT Confirmation Methods
- Clarifications and editorial improvements

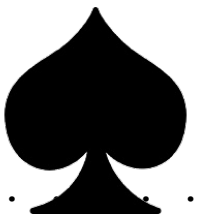
Restructure

-02:

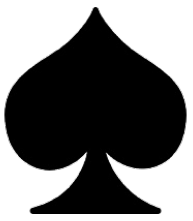
| | |
|------|---|
| 1. | Introduction |
| 1.1. | Terminology |
| 2. | Protocol Overview |
| 3. | Client-AS Communication |
| 3.1. | C-to-AS: POST to /token endpoint |
| 3.2. | AS-to-C: Access Token Response |
| 3.3. | The EDHOC_Information |
| 4. | Client-RS Communication |
| 4.1. | C-to-RS: POST to /authz-info endpoint |
| 4.2. | RS-to-C: 2.01 (Created) |
| 4.3. | EDHOC Execution and Setup of OSCORE Sec |
| 4.4. | Access Rights Verification |
| 5. | Secure Communication with AS |
| 6. | Discarding the Security Context |

-03:

| | |
|--------|---|
| 1. | Introduction |
| 1.1. | Terminology |
| 2. | Protocol Overview |
| 3. | Client-AS Communication |
| 3.1. | C-to-AS: POST to /token endpoint |
| 3.2. | Token Series |
| 3.3. | AS-to-C: Response |
| 3.3.1. | Access Token |
| 3.3.2. | Processing in C |
| 3.3.3. | Update of Access Rights |
| 3.4. | EDHOC_Information |
| 4. | Client-RS Communication |
| 4.1. | C-to-RS: POST to /authz-info endpoint |
| 4.2. | RS-to-C: 2.01 (Created) |
| 4.3. | Access Token in External Authorization Data |
| 4.4. | EDHOC Session and OSCORE Security Context |
| 4.4.1. | EDHOC message_1 |
| 4.4.2. | EDHOC message_2 |
| 4.4.3. | EDHOC message_3 |
| 4.4.4. | OSCORE Security Context |
| 4.5. | Update of Access Rights |
| 4.6. | Discarding the Security Context |
| 4.7. | Cases of Establishing a New OSCORE Security Context |
| 4.8. | Access Rights Verification |
| 5. | Secure Communication with AS |



Semantics of CWT/JWT confirmation methods



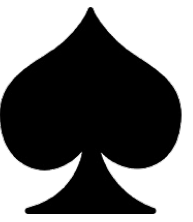
- CWT cnf methods mimicking COSE Header definitions of
 - RFC 9390
 - C509¹
 - EDHOC²

- JWT cnf methods mimicking
 - RFC 7515
 - RFC 9390
 - C509¹
 - EDHOC²

1. draft-ietf-cose-cbor-encoded-cert
2. draft-ietf-lake-edhoc

New in -03:

| | | |
|-------|--|--|
| 6. | CWT Confirmation Metods | |
| 6.1. | Ordered Chain of X.509 Certificates | |
| 6.2. | Unordered Bag of X.509 Certificates | |
| 6.3. | Hash of an X.509 Certificate | |
| 6.4. | URI Pointing to an Ordered Chain of X.509 Certificates | |
| 6.5. | Ordered Chain of C509 Certificates | |
| 6.6. | Unordered Bag of C509 Certificates | |
| 6.7. | Hash of a C509 Certificate | |
| 6.8. | URI Pointing to an Ordered Chain of C509 Certificates | |
| 6.9. | CWT Containing a COSE_Key | |
| 6.10. | CCS Containing a COSE_Key | |
| 7. | JWT Confirmation Metods | |
| 7.1. | Ordered Chain of X.509 Certificates | |
| 7.2. | Unordered Bag of X.509 Certificates | |
| 7.3. | Hash of an X.509 Certificate | |
| 7.4. | URI Pointing to an Ordered Chain of X.509 Certificates | |
| 7.5. | Ordered Chain of C509 Certificates | |
| 7.6. | Unordered Bag of C509 Certificates | |
| 7.7. | Hash of a C09 Certificate | |
| 7.8. | URI Pointing to an Ordered Chain of C509 Certificates | |
| 7.9. | CWT Containing a COSE_Key | |
| 7.10. | CCS Containing a COSE_Key | |

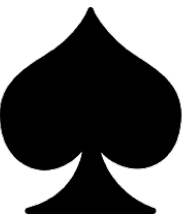


Identifier of token series = EDHOC session id

- Token series = sequence of Access Tokens updating each other
- General concept defined in draft-tiloca-ace-workflow-and-params
- Here: Coincide with access tokens during a particular EDHOC session
 - So token series can be identified with EDHOC session

```
EDHOC_Information = {  
    ? 0 => bstr,                ; id-session_id  
    ? 1 => int / array,         ; methods  
    ? 2 => int / array,         ; cipher_suites  
    ? 3 => true / false,        ; message_4  
    ? 4 => true / false,        ; comb_req  
    ? 5 => tstr,                ; uri_path  
    ? 6 => uint,                ; osc_ms_len  
    ? 7 => uint,                ; osc_salt_len  
    ? 8 => uint,                ; osc_version  
    * int / tstr => any  
}
```

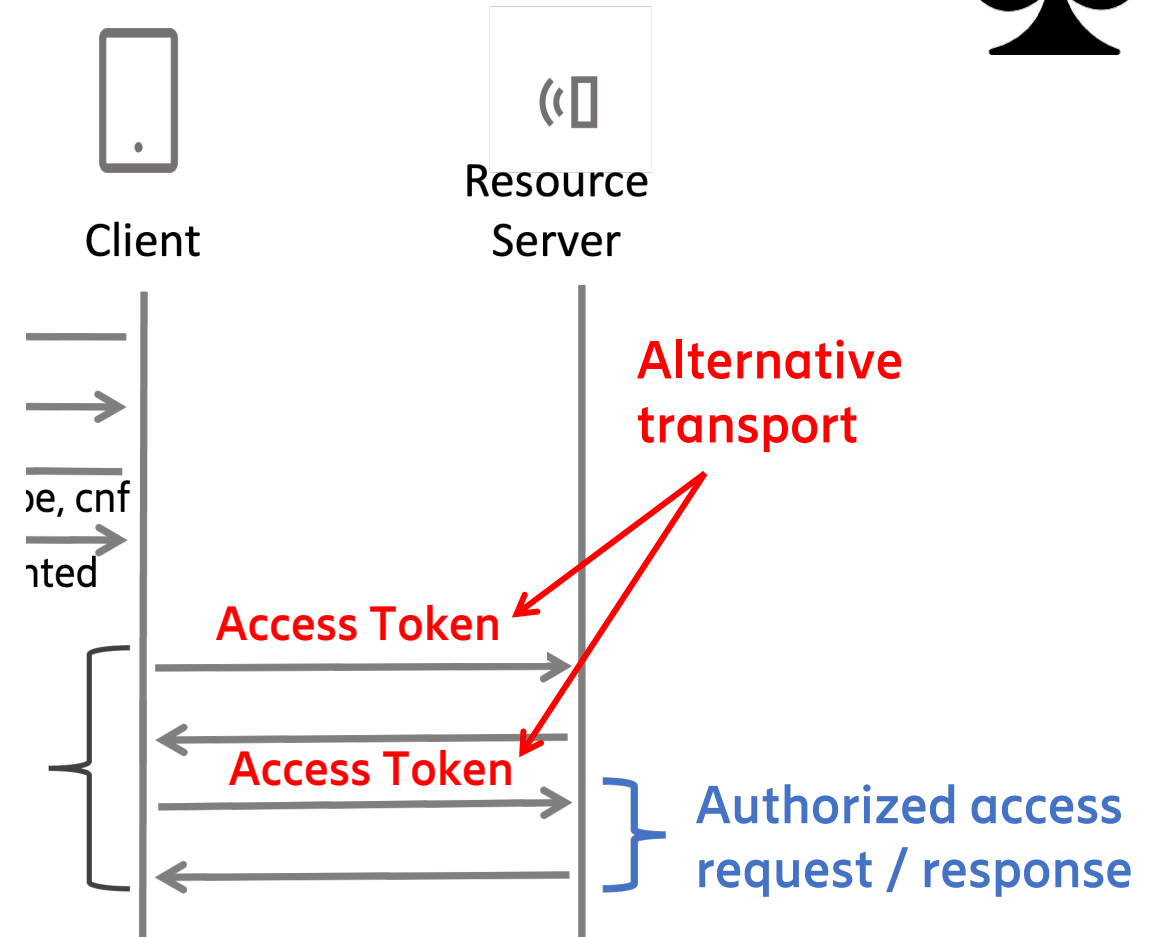

Transport of Access Token



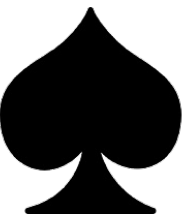
- Previous versions
 - May carry AT in EAD_1
- In -03:
 - May carry AT in EAD_1 or EAD_3
 - EAD_3 is encrypted, improved privacy

Question for WG:

- Only allow use of EAD_3?
 - (in addition to POST /authz-info for which AT is in plain text)



Next steps



- EDHOC application profile defined in draft-tiloca-lake-app-profiles
 - Array with EDHOC_Information
- Access Token for group-audience
 - multiple EDHOC_Information objects, and/or
 - common EDHOC_Information for multiple targets
 - dependency on draft-tiloca-ace-workflow-and-params
- Proof of possession of client private key to AS
 - Explicit PoP or EDHOC
- More security considerations, e.g. AT in EAD_3
- More reviews are welcome!

```
edhoc_info: {  
    session_id : h'01',  
    app_prof  : [2]  
}
```

instead of

```
edhoc_info: {  
    session_id : h'01',  
    methods    : 1,  
    cipher_suites : 0,  
    message_4   = true  
}
```