OSCORE Profile of ACE

https://tools.ietf.org/html/draft-ietf-ace-oscore-profile-11

Francesca Palombini, Ericsson AB
Ludwig Seitz, RISE SICS AB
Göran Selander, Ericsson
Martin Gunnarsson, RISE SICS AB

Status

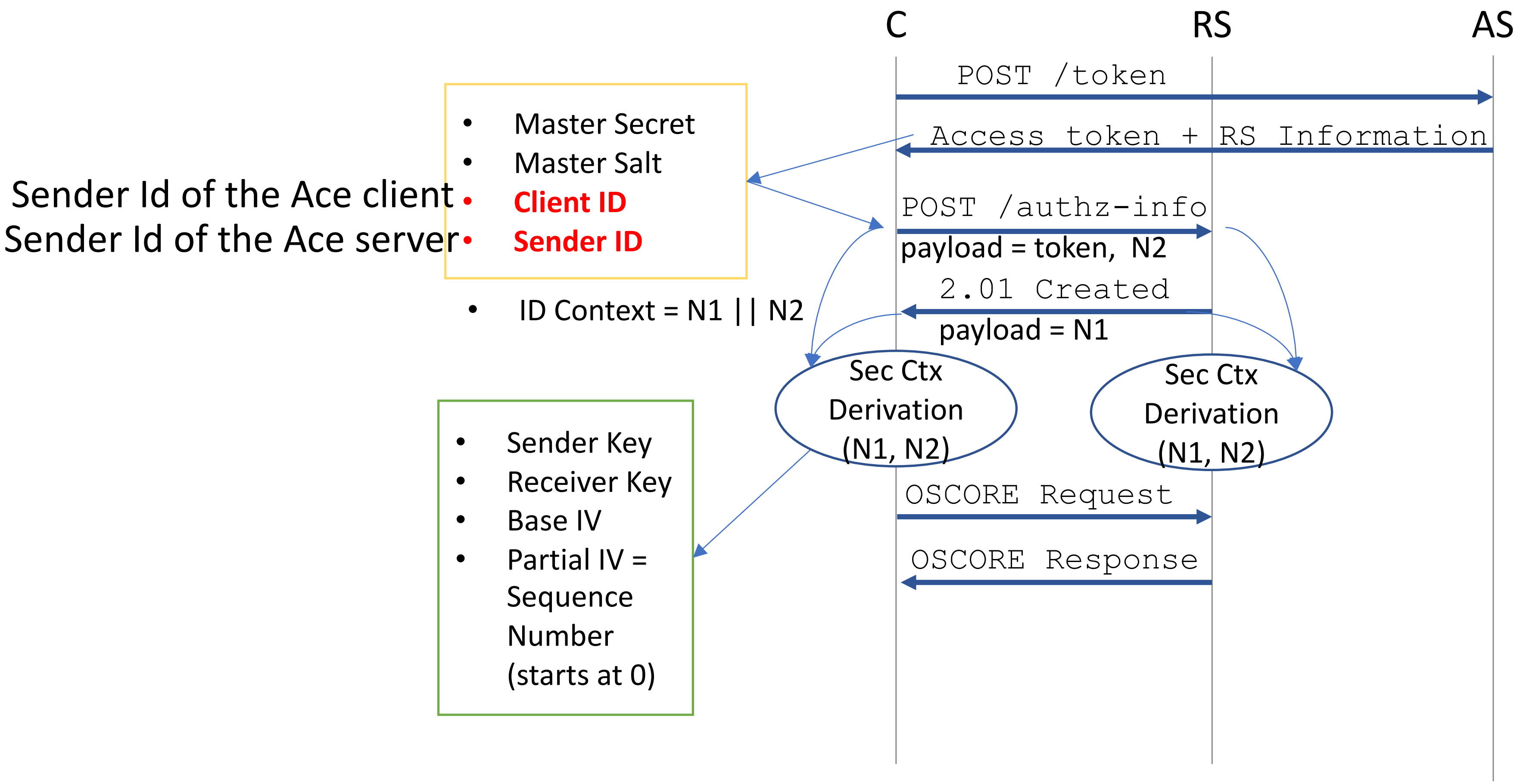
- All reviews from Last Call adressed:
  - https://datatracker.ietf.org/doc/review-ietf-ace-oscore-profile-11-opsdir-lc-dunbar-2020-07-19/ → OK
  - https://mailarchive.ietf.org/arch/msg/gen-art/dYccaGQYJbx3AL6kW4MjsLcfUfA/
    - *Did you have any thoughts about being clearer about the encryption/auth status of the various messages?*

IANA questions

- https://mailarchive.ietf.org/arch/msg/ace/5IBR5CNBDtEQIfAqMw4CRiirSG8/

1. Where to register parameters that go in the C-to-RS and RS-to-C messages?
   - Needs to be registered in https://www.iana.org/assignments/oauth-parameters/oauth-parameters.xhtml#parameters
   - Needs to be reviewed by DE
2. Where to put the new “OSCORE Security Context parameters” registry?
   - CoRE?
   - Ace?

New Comment: Identifiers negotiation



C

RS

AS

POST /token

Access token + RS Information

- Master Secret
- Master Salt
- **Client ID**
- **Sender ID**

Sender Id of the Ace client

Sender Id of the Ace server

- ID Context = N1 || N2

POST /authz-info

payload = token, N2

2.01 Created

payload = N1

Sec Ctx Derivation (N1, N2)

Sec Ctx Derivation (N1, N2)

- Sender Key
- Receiver Key
- Base IV
- Partial IV = Sequence Number (starts at 0)

OSCORE Request

OSCORE Response

Problem

https://mailarchive.ietf.org/arch/msg/ace/gSICgDPXN69caNn2OEF5dJuQGm4/

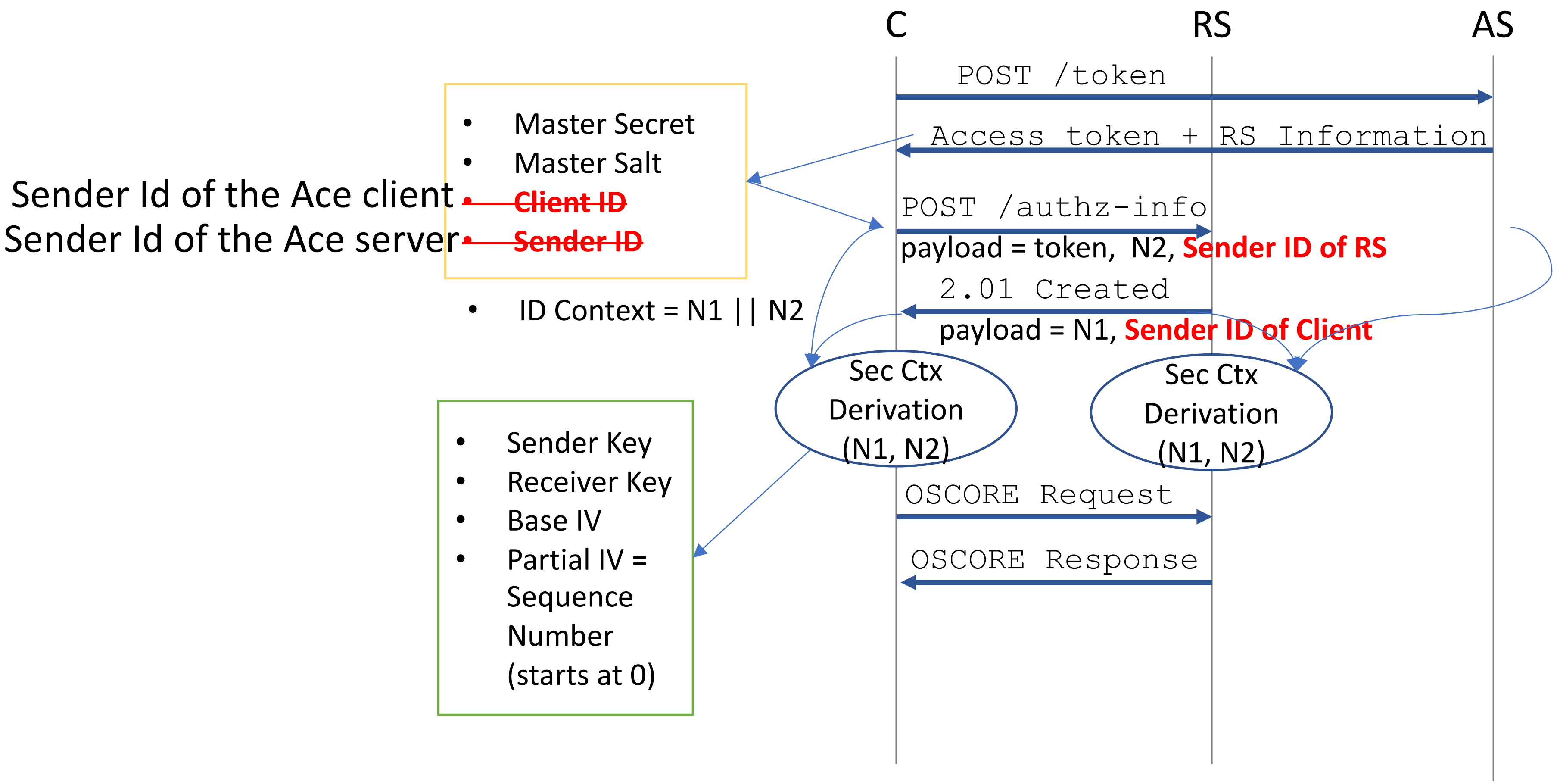
The current assignment mechanisms only works without problems in close systems where

- *the RS does not have any other non-AS OSCORE connections,*
- *the CoAP client and CoAP server roles are fixed and cannot be switched, and*
- *only draft-ietf-ace-oscore-profile is used.*

In systems where the OSCORE nodes can switch between CoAP client and CoAP server (a feature explicitly supported by OSCORE) the current mechanism is likely to lead to RecipientID collisions.

Also in future systems where the AS also supports a more modern key management with PFS using e.g. a future draft-ace-edhoc-oscore-profile, the mechanism would not work together in an efficient way.

Proposal change



C

RS

AS

POST /token

Access token + RS Information

- Master Secret
- Master Salt
- ~~Client ID~~
- ~~Sender ID~~

Sender Id of the Ace client

Sender Id of the Ace server

- ID Context = N1 || N2

POST /authz-info

payload = token, N2, **Sender ID of RS**

2.01 Created

payload = N1, **Sender ID of Client**

Sec Ctx Derivation (N1, N2)

Sec Ctx Derivation (N1, N2)

- Sender Key
- Receiver Key
- Base IV
- Partial IV = Sequence Number (starts at 0)

OSCORE Request

OSCORE Response

Proposal change

- Add identifier negotiation
  - Each node (C, RS) choses the Sender ID of the other node.

- The OSCORE_Security_Ctx object needs new identifier (different from the Sender ID + ID Context)
  - Object Id?
  - Hash?

Other (minor) comments

- "server authentication"
    - *My understanding is that server authentication with this draft requires two additional things. That C trusts AS and that RS sends an OSCORE response back. The draft should point this out similarly to the way it points out that a OSCORE request is required for proof-of-possession. As C trust in AS, and RS sending an OSCORE response back are both optional, I would recommend to maybe remove "server authentication" from the abstract and intro.*

- Change name to OSCORE_Security_Context
    - Clarify that this is input material

- Change name to ClientId and ServerId

- Clarify client/server use
    - And that it refers to Ace roles

- RFC 8613 Appendix B.2
    - Is it ok to run that after Ace OSCORE profile?

Next steps

- Update

- Back to the WG?