Notification of Revoked Access Tokens in the ACE Framework

draft-tiloca-ace-revoked-tokens-notification-03

Marco Tiloca, RISE
Ludwig Seitz, Combitech
Francesca Palombini, Ericsson
Sebastian Echeverria, CMU SEI
Grace Lewis, CMU SEI

IETF 109, ACE WG, November 18th, 2020

Recap

- An Access Token may be revoked, before expiration
  - Client or RS has been compromised, or decommissioned
  - Changed access policies or outcome of their evaluation
  - Changed ACE profile to use

- New interface at the Authorization Server (AS)
  - The AS maintains one Token Revocation List (TRL) resource
  - The TRL contains the hashes of revoked, not-yet-expired tokens
  - C/RS can GET or GET-Observe from the TRL
  - C/RS retrieve only their own pertaining portion of the TRL

- Benefits
  - Complement token introspection at the AS
  - No need for new endpoints at C or RS

Rationale

- Token hashes computed as per RFC 6920 (binary format)
- TRL resource at the AS
  - CBOR array of Token hashes
  - Add token hashes when Tokens are revoked
  - Remove token hashes when revoked Tokens expire
- Interaction
  - C and RS get the URL to the TRL endpoint upon registration
  - C and RS obtain only hashes of their own pertaining Tokens
  - A registered Administrator gets all Token hashes in the TRL
- Two modes of operations
  - **Full Query**: get all pertaining token hashes in the TRL
  - **Diff Query**: get the N most recent, pertaining updates to the TRL

Updates since -01

- Especially addressing
  - Review from Carsten [1] – Thanks!
  - Comments from Ben at the June interim – Thanks!

- Clarified how token hashes are computed
  - Consider what in 'access_token' of the AS response from /token
  - Added examples, for token transport in both CBOR or JSON

- Diff Query mode
  - Simpler interface
    - GET coaps://ace.as.com/revoke/trl?***diff=3***
  - Simpler format of payload response
    - Arrays rather than maps

```
token-hash = bytes
trl-patch = [* token-hash]
diff-entry = [removed: trl-patch,
              added: trl-patch]
diff payload = [* diff-entry]
```

[1] https://mailarchive.ietf.org/arch/msg/ace/ZoEJ6DulqJQcaMRrOdGkmbeFwwk/

Updates since -01

- Explicit signaling of the used hash algorithm
  - Now added in the registration response from the AS
- Added two interaction examples, using the Diff Query mode
- New Appendix A
  - Diff Query mode as an example of the Series Transfer Pattern (STP)
  - *draft-bormann-t2trg-stp-03*
- Ben's input for an improved diff-query mode
  - Rather than the N most recent TRL updates …
  - Get N updates "from where we stopped last time"
  - Revert to Full Query if not possible, e.g. information loss/removal at the AS
  - This might actually be a third mode of its own

Updates since -01

- New Appendix B
  - Builds on the “Cursor” pattern of the STP
  - Describes how to achieve the mode suggested by Ben
- Both (a) Full Query and (b) Diff Query requests return also a cursor
  - (a) Pointer to the most recent, pertaining TRL update
  - (b) Pointer to the most recent TRL update in the response
- In this “enhanced Diff Query” mode
  - A follow-up request may resume from after the cursor
  - Adjacent batches of TRL updates are possible, limiting excessive latencies
- Handled corner cases
  - No updates, or no updates after the cursor
  - Requested updates have been deleted as too old

Summary and next steps

- Notification of revoked Access Token
  - GET or GET-Observe; full query and diff query
  - Complement token introspection at the AS
  - No need for new endpoints on Clients and Resource Servers

- Version -03 incorporates:
  - Latest review from Carsten and comments from Ben on -01
  - Earlier review from Travis Spencer and comments from Jim on -00

- Next steps
  - (Third) query mode using the Series Transfer Pattern in the document body

- Ready for adoption call (?)

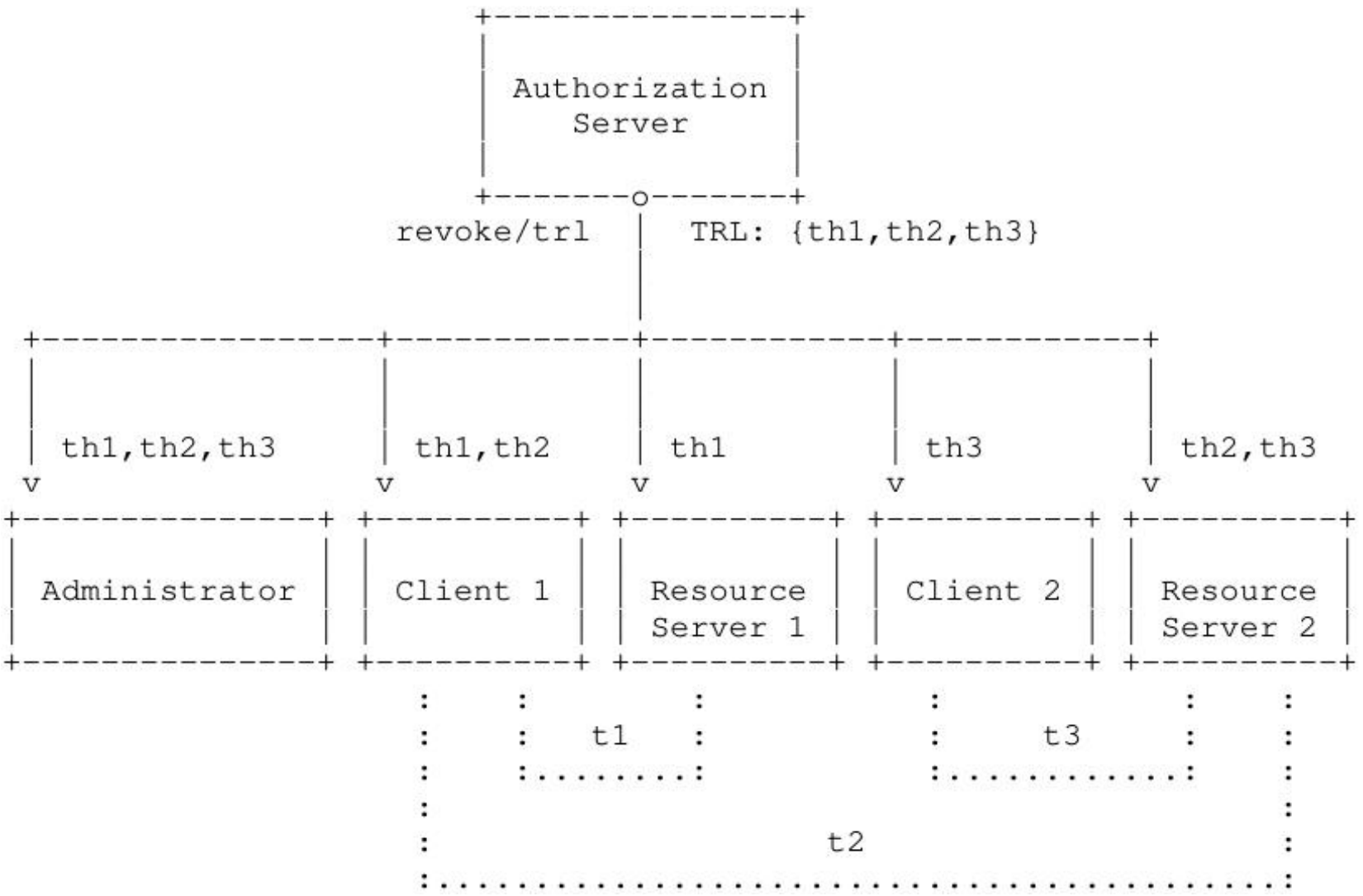
Thank you!

Comments/questions?

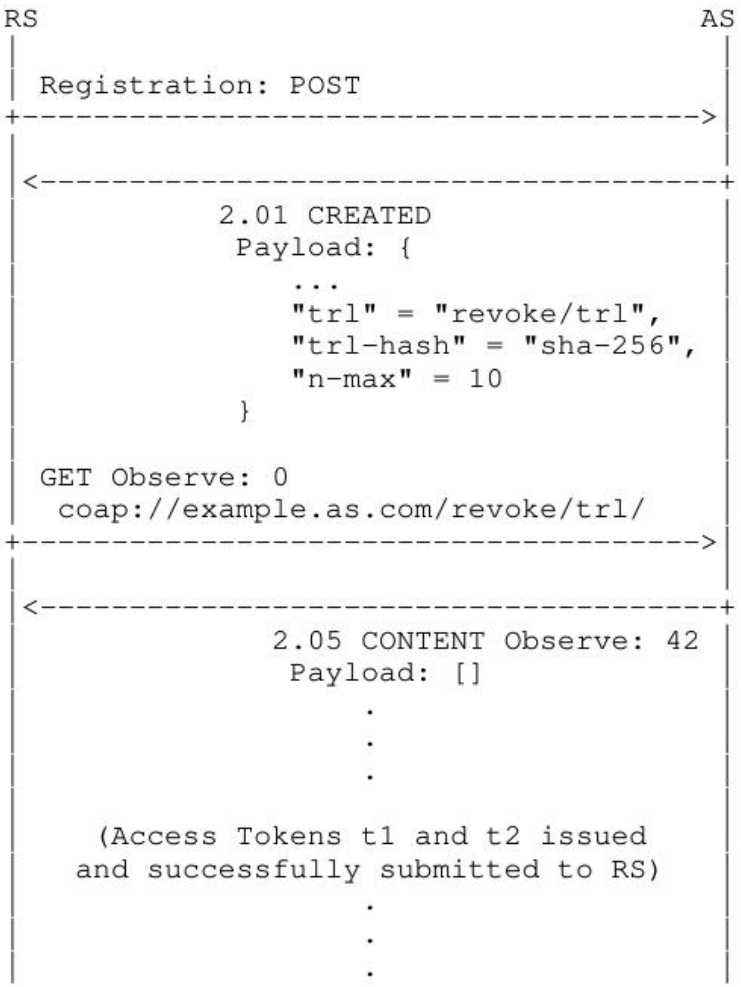
https://gitlab.com/crimson84/draft-tiloca-ace-revoked-token-notification

Backup

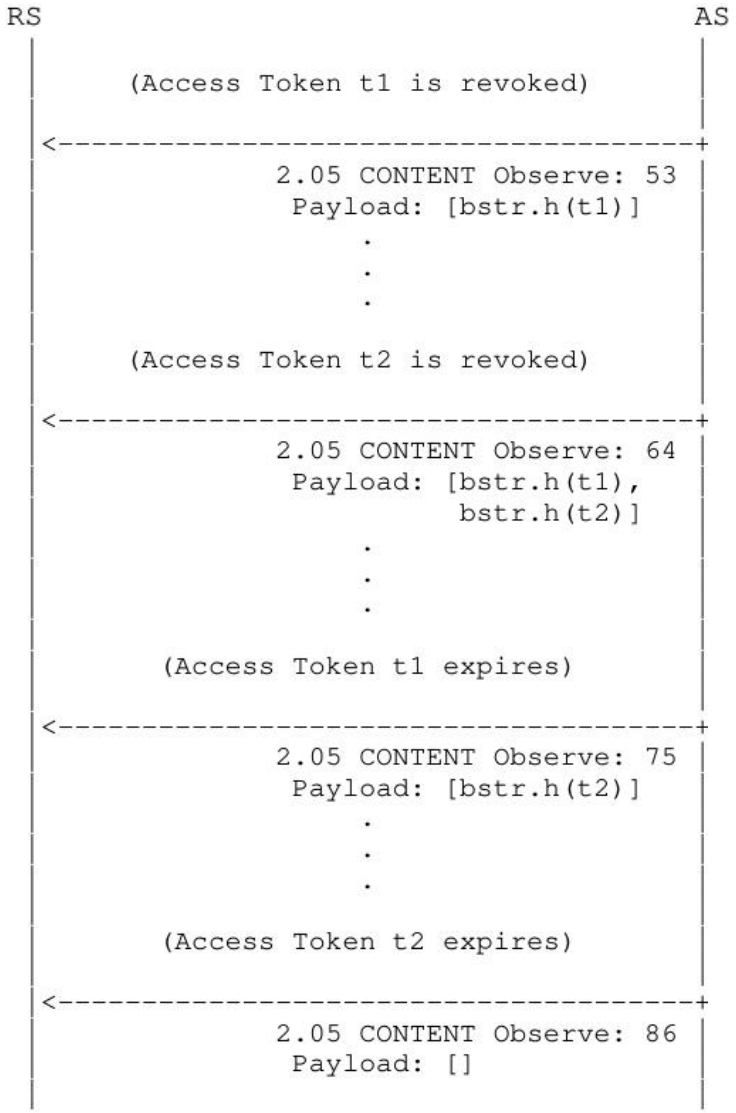
Protocol overview



Example with Full Query



Example with Full Query (ctd.)



Two types of TRL queries

- Common features
  - Limited to the portion of the TRL pertaining the requester
  - TRL filtering based on authenticated identity of the requester (secure session)

- **Full Query – *GET [Observe: 0] coaps://example.as.com/revoke/trl***
  - Request for all pertaining token hashes in the TRL
  - Return a CBOR array, with the Token hashes as elements

- **Diff Query – *GET [Observe: 0] coaps://example.as.com/revoke/trl?diff=3***
  - Request for the latest N updates to the pertaining portion of the TRL list
  - Build N entries as CBOR arrays. Each entry refers to an update and has:
    - An element “deleted”, with a CBOR array of Token hashes.
    - An element “added”, with a CBOR array of Token hashes.
  - Return a CBOR array with the N arrays as element, in reverse chronological order