Notification of Revoked Access Tokens in the Authentication and Authorization for Constrained Environments (ACE) Framework

draft-ietf-ace-revoked-token-notification-04

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

IETF 116 meeting – Yokohama – March 30th, 2023

Since IETF 115

- **Ongoing work presented during two ACE interim meetings**
  - On 2022-12-19 and 2023-02-20

- **Version -04 submitted before the cut-off**
  - All remaining open points have been addressed
  - No changes in the protocol mechanics and rationale

- **Started and completed WG Last Call on version -04**
  - Received reviews from Marco Rasori and Rikard Höglund – Thanks a lot!
  - https://mailarchive.ietf.org/arch/msg/ace/nxpyDRldkxgNSqXY-QGZp-3kbkI/
  - https://mailarchive.ietf.org/arch/msg/ace/al6Ta1iRRMHOuAsIy7GAUwW4MwM/

Update summary

- **Clarified details on handling token hashes (Section 10.1)**
  - C/RS: Expunge a stored access token when receiving its token hash
  - RS: Don't accept an access token if currently storing its token hash
  - RS: Clear rules on when it is safe to delete a stored token hash
    - Handling also late-uploaded access tokens with the EXI claim
- **Extended and improved security considerations**
  - Content Retrieval from the TRL Resource
  - Size of the TRL resource
  - Communication patterns
  - Request of new access tokens after 4.01 (NEW)
  - Dishonest clients (NEW)
- **New Appendix B overviewing parameters of the TRL endpoint at the AS**

Update summary

- **Examples of message exchange are now all collected in Appendix C**
  - Added new examples with the "Cursor" extension (Appendices C.4 and C.5)
- **Influencing the AS on sending observe notifications**
  - The use of the "c.pmax" conditional attribute is just an example
  - *draft-ietf-core-conditional-attributes* is now an informative reference
- **Clarifications and editorial improvements**
  - Improved presentation of pre- and post-registration operations
  - Removed moot processing cases with the "Cursor" extension
  - Access Tokens are not necessarily uploaded through /authz-info
  - Renamed the parameter N_MAX as MAX_N
  - Positive integers as CBOR abbreviations of message parameters
  - Fixed details in IANA considerations

Summary of WGLC reviews

- **From Marco Rasori**
  - Mention the features of the diff query upfront
  - Merge the handling of two similar error conditions
  - Improve security considerations on Clients requesting a new access token
  - Clarify that a TRL update can involve more access tokens at once
  - Editorial improvements and fixes

- **From Rikard Höglund**
  - Mention CoAP earlier
  - “TRL resource” → “TRL endpoint” ; “Portion of the TRL” → “Subset of the TRL”
  - “Caller of the TRL endpoint” → “Requester towards the TRL endpoint”
  - Rewrite the computing of the Token Hash using one less symbolic definition
  - Clarifications, editorial improvements and fixes

The reviews have requested clarifications and minor fixes – No controversial issues to discuss

Next steps

- **Submit version -05 addressing the WG Last Call comments**

Thank you!

Comments/questions?

https://github.com/ace-wg/ace-revoked-token-notification