GNAP Meeting
IETF 116

draft-ietf-gnap-core-protocol-13
draft-ietf-gnap-resource-servers-03

March 31, 2023

Justin Richer • Fabien Imbault

Agenda

- Core draft update: changes since IETF115 (from -11 to -13)
- RS draft update: changes since IETF114 (from -02 to -03)
- GNAP Status

Differences since IETF115

https://author-tools.ietf.org/iddiff
?url2=draft-ietf-gnap-core-protocol-13
&url1=draft-ietf-gnap-core-protocol-11

https://author-tools.ietf.org/iddiff
?url2=draft-ietf-gnap-resource-servers-03

Core Draft Changes

- Shift to SHA256 default
- IANA Registry Actions
- Remove “previous_key” from key rotation
- Clarify differences between “new” token and “rotated” token value
- Respond to WGLC comments (mostly editorial, clarification, or consistency)

RS Draft Changes

- Token model
- IANA registry actions

Token Model

- Value
- Issuer
- Audience
- Key Binding
- Flags
- Access Rights
- Time Validity Window
- Authorizing Resource Owner
- Client Instance
- Label
- Parent Grant Request

Current Open Issues on Core

- Token management endpoint access
- Multiple interaction finish methods

Token management endpoint

- Current setup:
  - Present the token being managed as usual
  - ALWAYS sign with the client instance’s key
- Problems with this:
  - Token could be expired (for either rotation or revocation)
  - Prevents use of middleware to check token access here
- Proposed alternative:
  - Pass token value as body parameter (as in introspection)
  - Optional secondary token to protect token management endpoint?
- **Editors opinion: possibly worth the change**
  - Not a lot of deployment experience with token management, might be the time to change it

Multiple finish methods

- Current setup:
  - Client sends only one finish method
  - AS responds to one (or zero)
- Problems with this:
  - Client might not be able to guess which methods are OK ahead of time
  - Not quite in the spirit of “negotiation” elsewhere
- Proposed alternative:
  - Allow client to send multiple finish methods
  - AS still responds to only one (or zero)
- **Editors opinion: defer to an extension**
  - An extension can be defined to handle this behavior without breaking existing code
  - Tagged as “Need Text”

GNAP Status

- WGLC finished on Core
    - We should decide whether to change anything for token rotation
- Ready (soon) for IETF LC