# GNAP Interim Meeting

draft-ietf-gnap-core-protocol-05

May 6, 2021

Justin Richer • Aaron Parecki • Fabien Imbault

# Agenda

- Updates since last interim
  - Functional changes
  - Editorial changes
- Discussion Items
  - Cryptographic updates
  - Subject identifier
  - Resource servers
  - AS/RS Relationship
  - Authorization and Consent
- Next topics?
  - Token rotation, key rotation, interim meeting?

# 25 Merged Pull Requests since -04

https://github.com/ietf-wg-gnap/gnap-core-protocol/pulls

?q=is%3Aclosed+merged%3A2021-02-23..2021-05-07

Thank you to contributors!

# Functional Changes

- Cryptographic updates (#250, #232, #226, #209, #208, #207, #202, #195)
- Subject identifiers (#229, #228, #220, #184)
- Interaction & Consent Gathering (#242)
- Extracted RS-AS relationship into its own spec (#246)

# Editorial Changes

- Protocol rationale (#254, #247, #211)
- Minor protocol updates (#199, #194, #183)
- Editorial & fixing typos (#251, #245, #204, #202)

# Discussion Items

# Cryptographic updates

- Aligned with external specs
  - Updated HTTP Message Signatures syntax
  - DPoP ‘ath’ claim (now also used by GNAP JOSE)
  - JOSE ‘typ’ header
- Updated JOSE body signing
  - Uses hash of body instead of detached signature
  - More robust in multi-layer environments
- Updated examples

# Subject identifiers

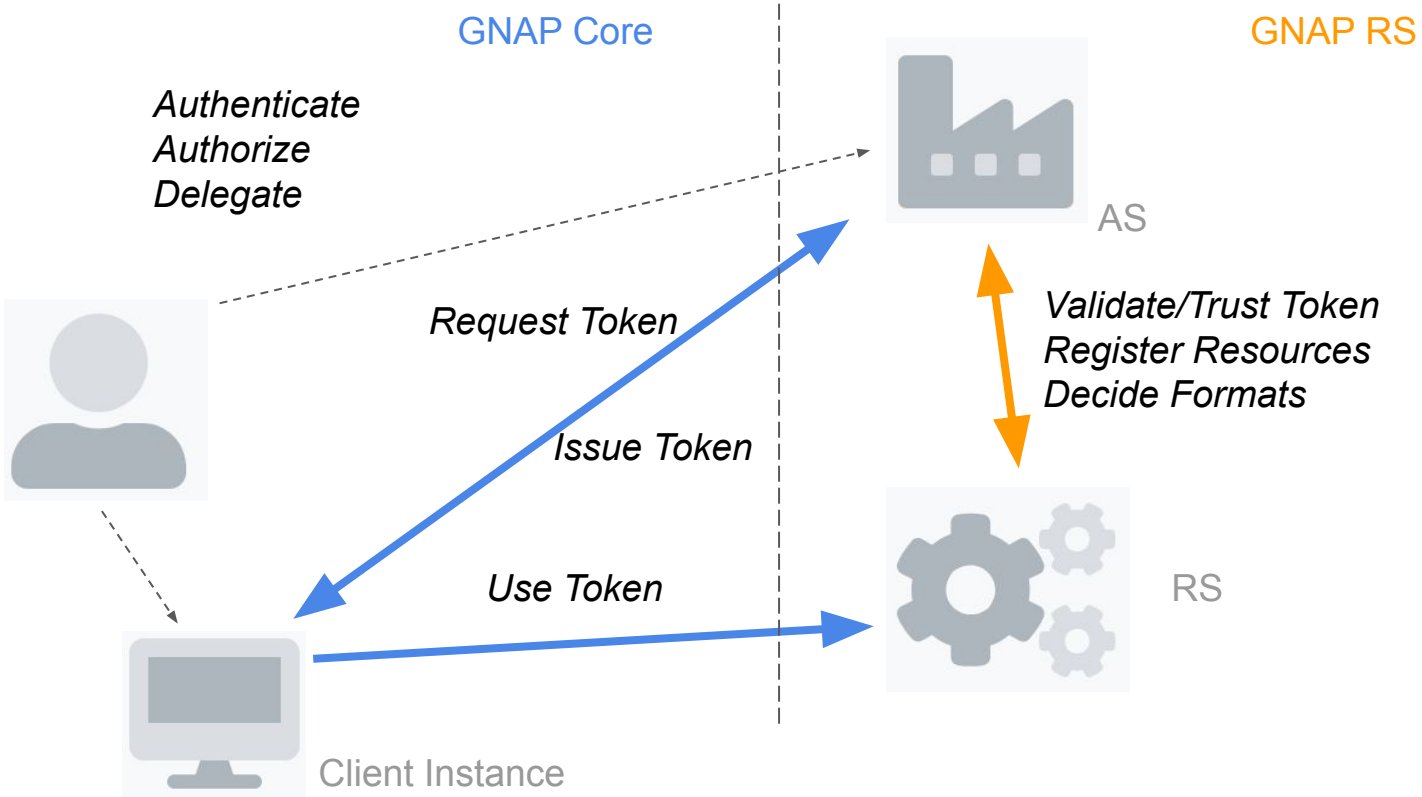
- Subject identifiers
  - Based on feedback received during IETF 110
  - The update on section 4 helps a lot
  - Updated to align with https://www.ietf.org/id/draft-ietf-secevent-subject-identifiers-07.txt
  - Updated all the examples

- What remains open
  - Include DIDs with sub_ids #221 (needs text)
  - Assertions (array?)

# Resource Servers

- New repository
  - https://github.com/ietf-wg-gnap/gnap-resource-servers
- New draft
  - https://www.ietf.org/archive/id/draft-ietf-gnap-resource-servers-00.html
- Keep issues in their respective repositories
  - e.g. Client-to-AS interaction: core
  - e.g. AS-RS interaction: resource-servers
  - If you don’t know where to file the issue:
    - Open on the main repo
    - The editors will move to RS if needed
- Sets precedent for other extension work

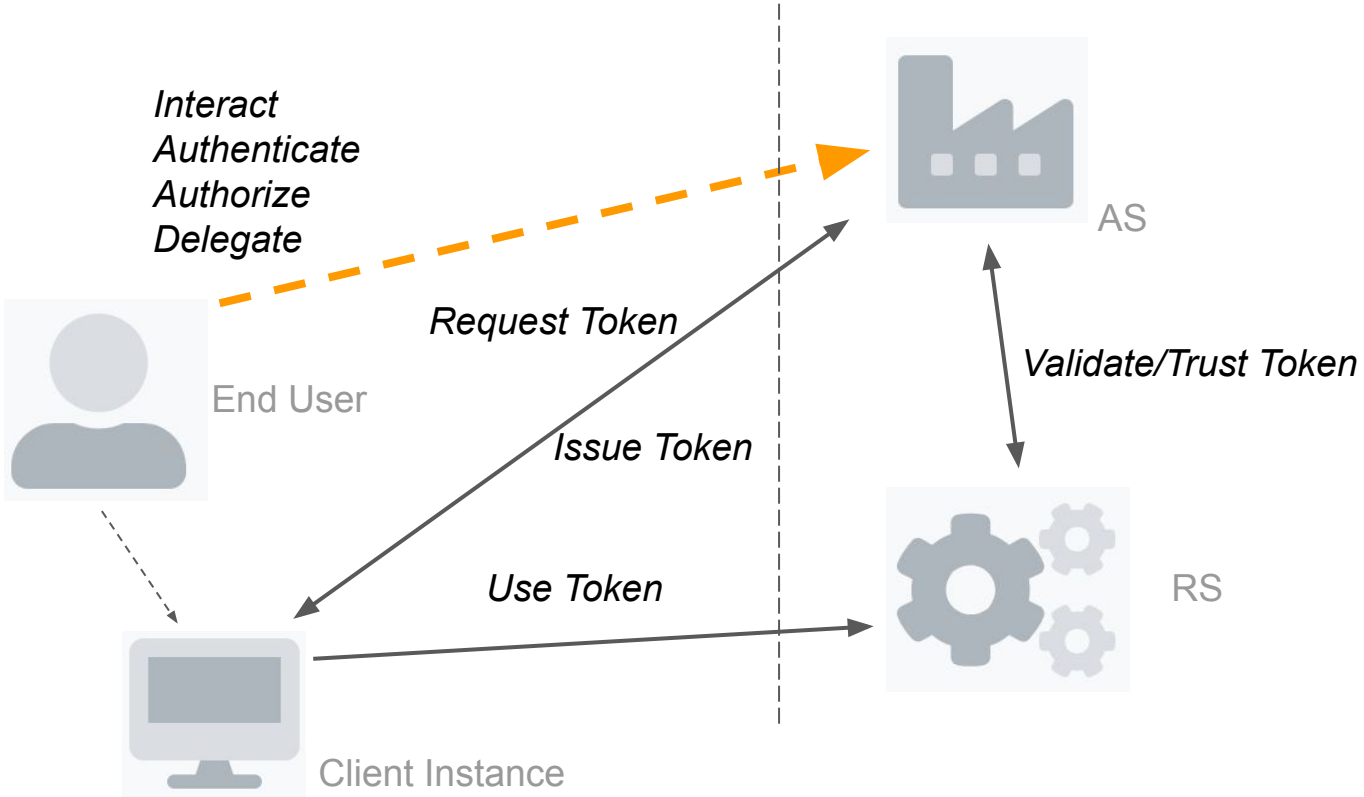
# AS and RS Relationship



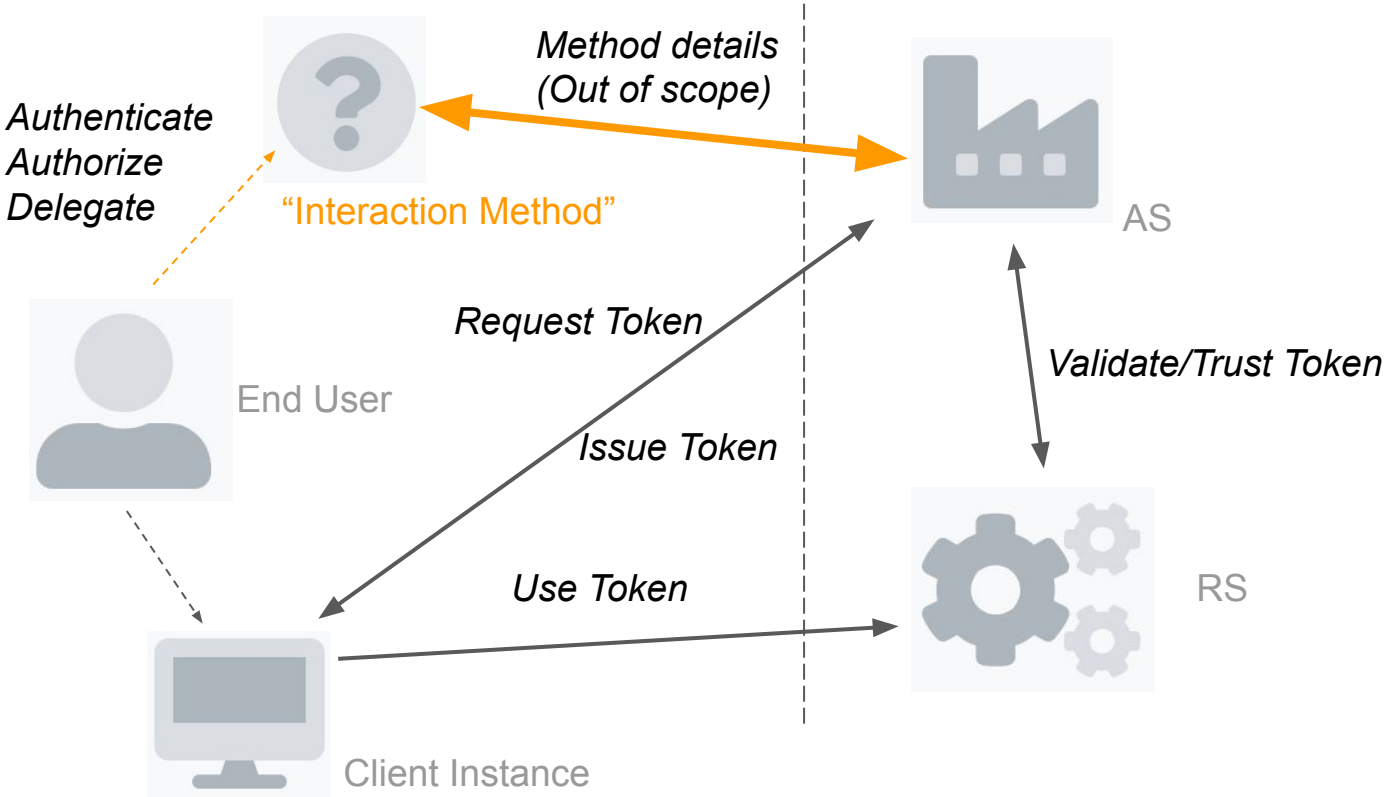
# AS Determining Authorization and Consent

- Rewrite of section 4
- Previously:
  - Accidentally assumed specific model for AS and client instance
  - “Interaction **at the AS**”, “hosted **at the AS**”
- Now:
  - AS has a variety of tools to determine authorization and consent
  - Not just driven by interaction with the “user”
  - Simple redirect-there-and-back case still possible and called out
- Unchanged:
  - Negotiated through “interact” request/response
  - Portions can happen out of band

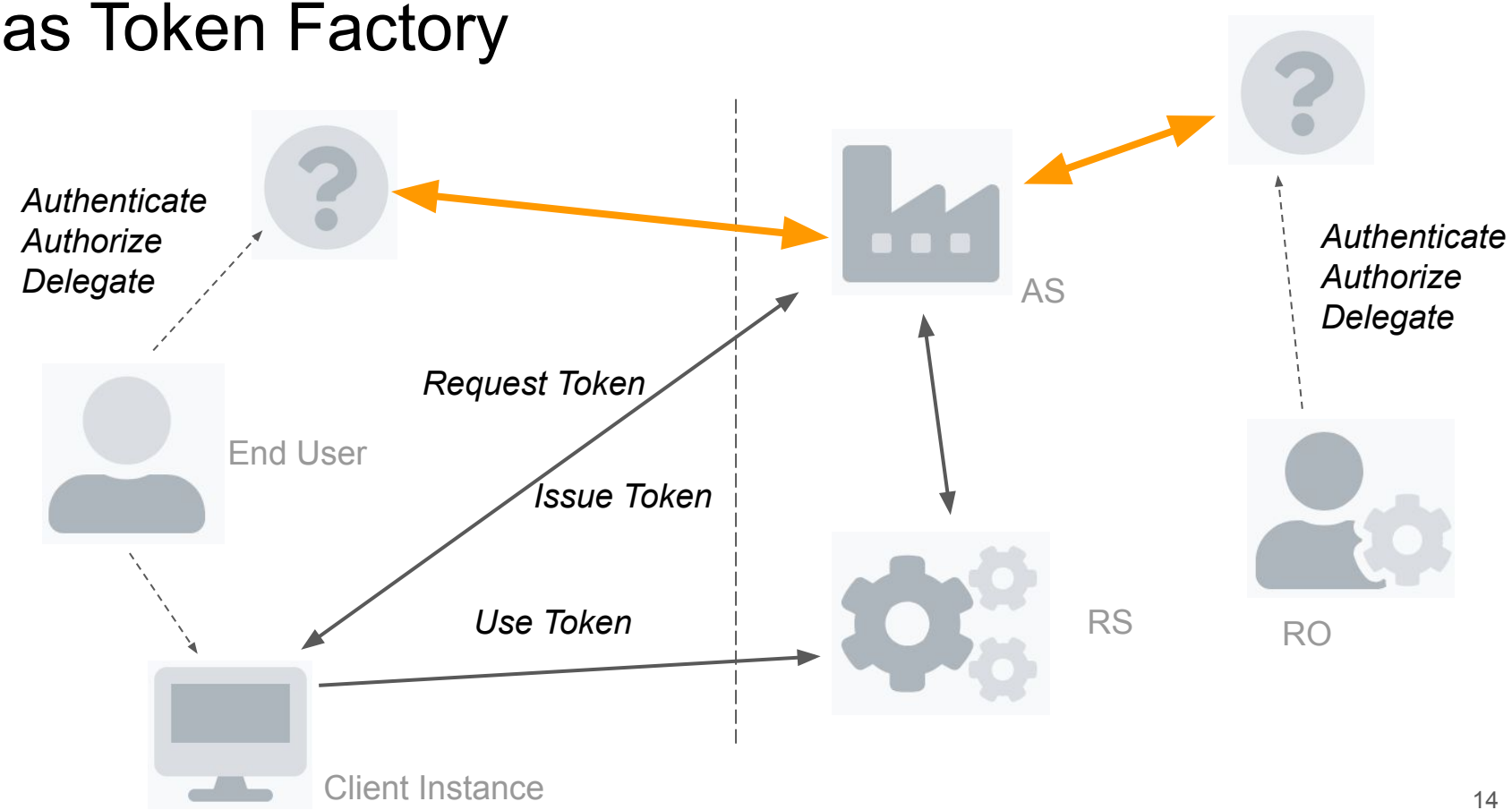
# AS as Previously Assumed



# AS as Token Factory



# AS as Token Factory



# Going forward

# Current state

- Reasonably stable core
- Plenty to discuss and define around all the edges
- We need to implement and deploy

# Next Topics

- Token rotation
  - What to do with old tokens during rotation?
- Signature methods
  - Which ones do we keep in core?
  - What’s an extension?
  - What should be dropped?
- Key rotation
  - Rotate keys for client instances and tokens
- Access request internals (#244)
- Interim: Mid-June?