OAuth WG Interim Meeting

Date

November 3rd, 2021, 12:00pm EDT

Topic - Token Chaining

Presenter: Kelley Burgin
Draft: Token Chaining - Single ICAM
Draft: Token Chaining - Multiple ICAMs
Slides: Token Chaining

Notes

Note taker: **Justin Richer**

Presentation: Token and Identity Chaining

- MITRE published two profiles for identity briding for OAuth 2.0 & OIDC
- “Enterprise Mission Tailored Profiles”
- Leverage existing environments and previous work

Token Chaining:

- Problem: client calls PR1, PR1 needs to call PR2, etc.
- two cases: all PRs trust one AS, PRs trust different AS’s

Solution in single ICAM:

- PR1 acts as client to get token for PR2 using token exchange
- tokens can be chained through multiple PRs by repeating process
- claims inside token:
  - “aud” is target PR
  - “act” is chain of token history before we got to the current token

Multiple ICAM system:

- More complicated
- user could authenticate in any way, doesn't need to be PKI, just needs to auth to first AS

Multiple ICAM solution options:

- looking for feedback on different options

1. PR1 gets a token from its own AS via token exchange
    - Pros: PR1 doesn't need a relationship w/another AS domain
        - requirements that everyone's registered ahead of time
    - Cons: PR2 needs to trust tokens from AS1
        - has to do token introspection (cross-domain) but through its own AS2

Justin: this isn't off-label use of introspection
Brian: but it's not common to use
Kelley: PR2 calls AS2, not AS1
Justin: that is actually off-label, then

Jeff: is there an assumption of the identifier space being shared?
Kelley: we're assuming there are relationships bbetween parties

Aaron: on introspection, one AS would use introspection of other AS, is that the case?
Kelley: Idea is yes, AS2 validates tokens for PR2, how that happens is outside of scope

2. PR1 gets a token from PR2's AS via token exchange
    - pros: PR2 only needs to validate tokens in its own domain
        - nothing special for PR2
    - cons: PR's need to register across domains in order to get cross-domain tokens
        - registration across all other possible domains where it might need to talk
        - AS2 has to trust tokens from AS1

Brian: in general, token exchange draft defines token exchange URI as particular to the AS you're talking about; something else would need to be used to denote tokens from another AS; profile should add it

3a. PR1 gets a JWT from its own AS that PR2 sends to PR2's AS as an assertion grant
- token exchange can be used to get assertion token (JWT)
- pros: PR2 only sees access tokens from its own AS
- JWTs are meant to be used across domains
- Cons: AS needs to trust assertions from AS1
- AS's need to agree on content/details of assertions, need to communicate & trust
- additional steps; could add latency?

3b. PR1 gets 1nd access token from its own AS using a JWT assertion
- PR1 does token exchange but gets back token, not assertion
- AS1 knows how to make "tokens for outside organizations", contacts/coordinates with AS2
- Pros: PR1 doesn't need to be registered across domain,
- PR2 only gets tokens ussed by AS2
- cons:
- as2 has to trust assertions from AS1
- AS's need to agree on content/details of assertions
- additional steps & latency

Questions / Comments / Discussion

Brian: like model (3b), but it never seems to work out as well as it looks on paper
… all these tokens are bound to the cert of the client making the call, right?
Kelley: yes, we require MTLS with tokens
Brian: that gets problematic b/c you need to issue a token for a client/RS but issued to the AS; binding certificates correctly gets really strange. I'm not sure 3B is even viable w/o a lot more information about certificates.
Kelley: this is the kind of feedback we're looking for, if it's not feasible
Brian: speaking to the logistics of who holds the key; in 3B it doesn't make sense b/c caller isn't entity holding certificate. less about current implementations, more about logistics of the flow.
… in step 4 of diagram for 3b, have one service calling another, but result is token used in (6) but token is bound to certificate in PR1
Kelley: we assume all servers have NPE certs
Brian: even if everybody does have a cert, certs are established btw two entities but

it’s bound to a different certificate
Kelley: hadn’t thought of that

Warren: similar question but to other cases; don’t understand the use cases, how is RS at the end verifying identity that’s coming in?
… is expectation that data w/subs is going to verify each layer? if no, is it only trusting last AS?
… what’s the purpose of stacking? you’re just collecting them, could be a list
Kelley: we want to make sure we know the client and intended recipient, then transferred along in chain
Warren: nothing stops AS3 from lying about what it did to get there
Kelley: last AS signs the token it generates

Beth: we designed this for a very specific environment, there’s an attribute sharing infrastructure underlying the AS’s
… v. strong trust infrastructure, does not work in every environment

WG Call

Dmitry: question on other token binding mechanisms; have mentioned MTLS, might any other mechanisms (Dpop) be relevant here?
Kelley: we’re waiting to see how DPoP turns out
… we like the server nonce, that fixes a lot of issues
… there’s another draft out, asymmetric keypairs

Rifaat: is there interest in solving this problem?

(no +1’s in the chat)

Justin: concerned about scope and unknown assumptions underlying the proposals
… historical chaining draft: https://tools.ietf.org/id/draft-richer-oauth-chain-00.html

Warren: if we treat these as a single AS, then this feels similar to DPoP but only in a way we could stack DPoP on top of each other
… as long as there’s no language about crossing security domains

beth: two different proposals, single and mutli security system
… might have blurred together
… v. interested in making things as standardized as possible
… don’t want specialized solutions if we can avoid it, even thought we have specialized environment

Rifaat: don’t see much support at this stage, but maybe you got good feedback and can try again in the future

Attendees

- Rifaat Shekh-Yusef/Auth0 (chair)
- Hannes Tschofenig/Arm (chair)
- Kelley Burgin/MITRE (Presenter)
- Justin Richer
- Peter Yee, AKAYLA
- Jeff Craig, Google
- Brian Campbell, Ping
- Aaron Parecki, Okta
- Dmitry Telegin, Backbase / Keycloak
- Marie-Helene Bouchard (Government of Canada)
- Beth Abramowitz, MITRE
- Roman Danyliw, CMU SEI
- Warren Parad, Rhosys
- Marius Ciocan
- Vittorio Bertocci (Auth0 | Okta)
- Filip Skokan (Auth0)
- Roberto Polli
- Michael Peck
- Casey Yourman, Ford Credit

Recording

https://ietf.webex.com/recordingservice/sites/ietf/recording/7599b82b1eed103abb7e0050568ced19/playback