private_key_jwt: We have a problem

Joseph Heenan (Authlete)

Mike Jones (Self-Issued Consulting)

Vulnerability identified exploiting ambiguous audience values for AS

- ***Please don't share details of this publicly yet***

- Token replay vulnerability identified by Pedram Hosseyni, Tim Würtele, and Ralf Kuesters of University of Stuttgart
  - During security analysis of OpenID Federation
  - Also applies to several other OAuth and OpenID specs

- Has been extensively discussed among security researchers and affected specification authors

- OpenID Foundation has been proactively notifying owners of affected ecosystems and software

- Today's call part of wider disclosure plan

Link to Vulnerability Disclosure in Chat

- ***Particularly don't share the disclosure doc publicly, including do not put the link in the meeting minutes***

- It contains a sufficiently detailed description of the vulnerability to construct exploits, in some cases

Historic state of private_key_jwt

- Specs historically define audience value sent to AS in different ways & unfortunately vague ways

RFC7523
(JWT Assertions)

> 3. The JWT MUST contain an "aud" (audience) claim containing a value that identifies the authorization server as an intended audience. The token endpoint URL of the authorization server MAY be used as a value for an "aud" element to identify the authorization server as an intended audience of the JWT. The authorization server MUST reject any JWT that does not contain its own identity as the intended audience. In the absence of an

OpenID Connect

aud

REQUIRED. Audience. The `aud` (audience) Claim. Value that identifies the Authorization Server as an intended audience. The Authorization Server MUST verify that it is an intended audience for the token. The Audience SHOULD be the URL of the Authorization Server's Token Endpoint.

Historic state of private_key_jwt

- Specs historically define audience value sent to AS in different ways & unfortunately vague ways

RFC 9126 (PAR):

Due to historical reasons, there is potential ambiguity regarding the appropriate audience value to use when employing JWT client assertion-based authentication (defined in Section 2.2 of [RFC7523] with `private_key_jwt` or `client_secret_jwt` authentication method names per Section 9 of [OIDC]). To address that ambiguity, the issuer identifier URL of the authorization server according to [RFC8414] **SHOULD** be used as the value of the audience. In order to facilitate interoperability, the authorization server **MUST** accept its issuer identifier, token endpoint URL, or pushed authorization request endpoint URL as values that identify it as an intended audience.

More specs using different audience values for authorization server

- Specs historically define audience value sent to AS in different ways & unfortunately vague ways

RFC9101 (JAR):

To sign, JSON Web Signature (JWS) [RFC7515] is used. The result is a JWS-signed JWT [RFC7519]. If signed, the Authorization Request Object **SHOULD** contain the Claims `iss` (issuer) and `aud` (audience) as members with their semantics being the same as defined in the JWT [RFC7519] specification. The value of aud should be the value of the authorization server (AS) `issuer`, as defined in RFC 8414 [RFC8414].¶

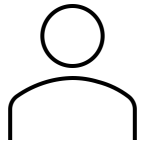
Legitimate Fintech
OAuth Client

Attacker Controlled
Bank AS

1. Publishes in
.well-known/openid-configuration

```
{
  …
  “token_endpoint”:  “https://realbank.com/issuer ”
}
```

Real Bank AS



2. Attacker initiates session

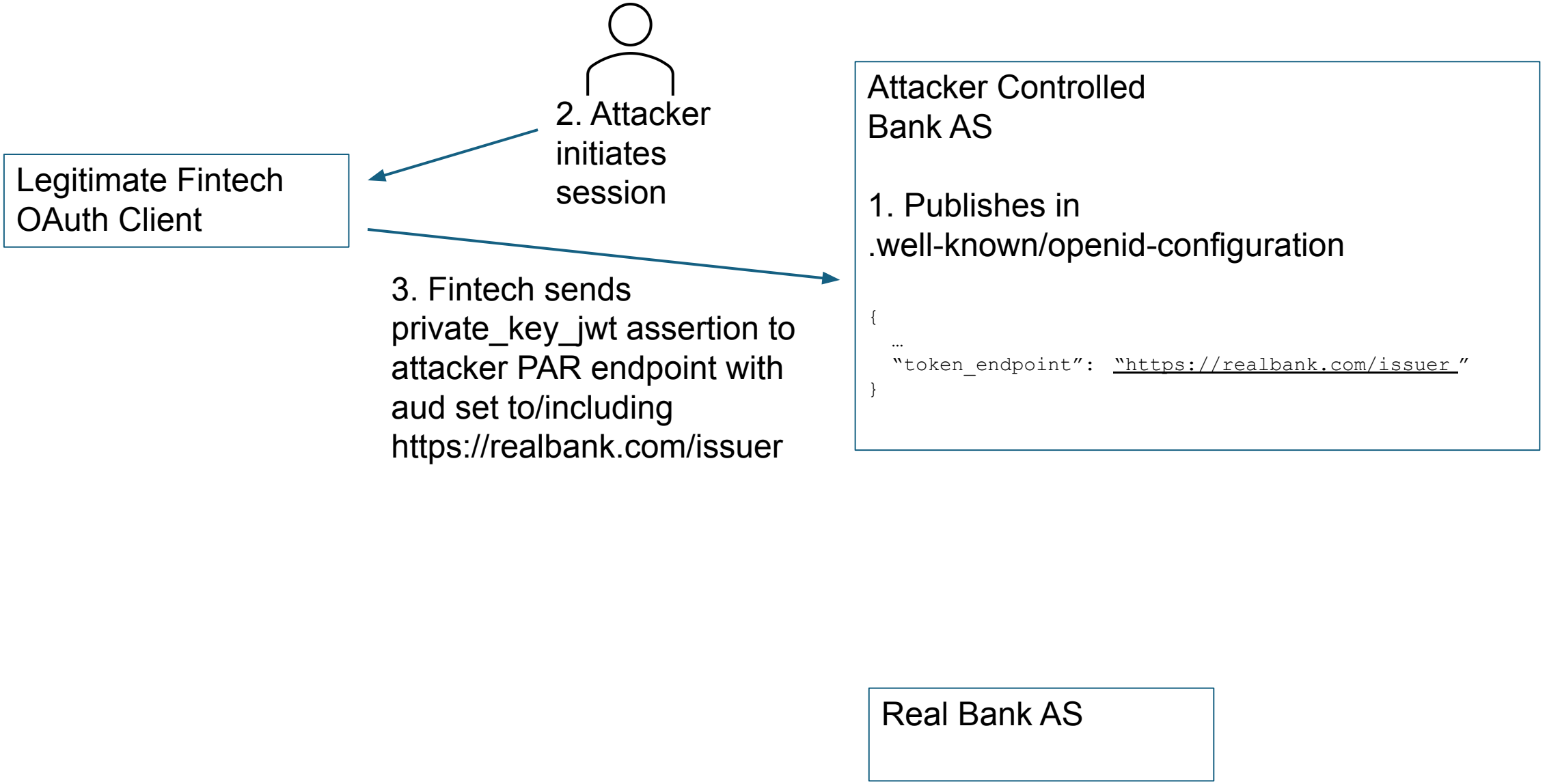
Legitimate Fintech OAuth Client

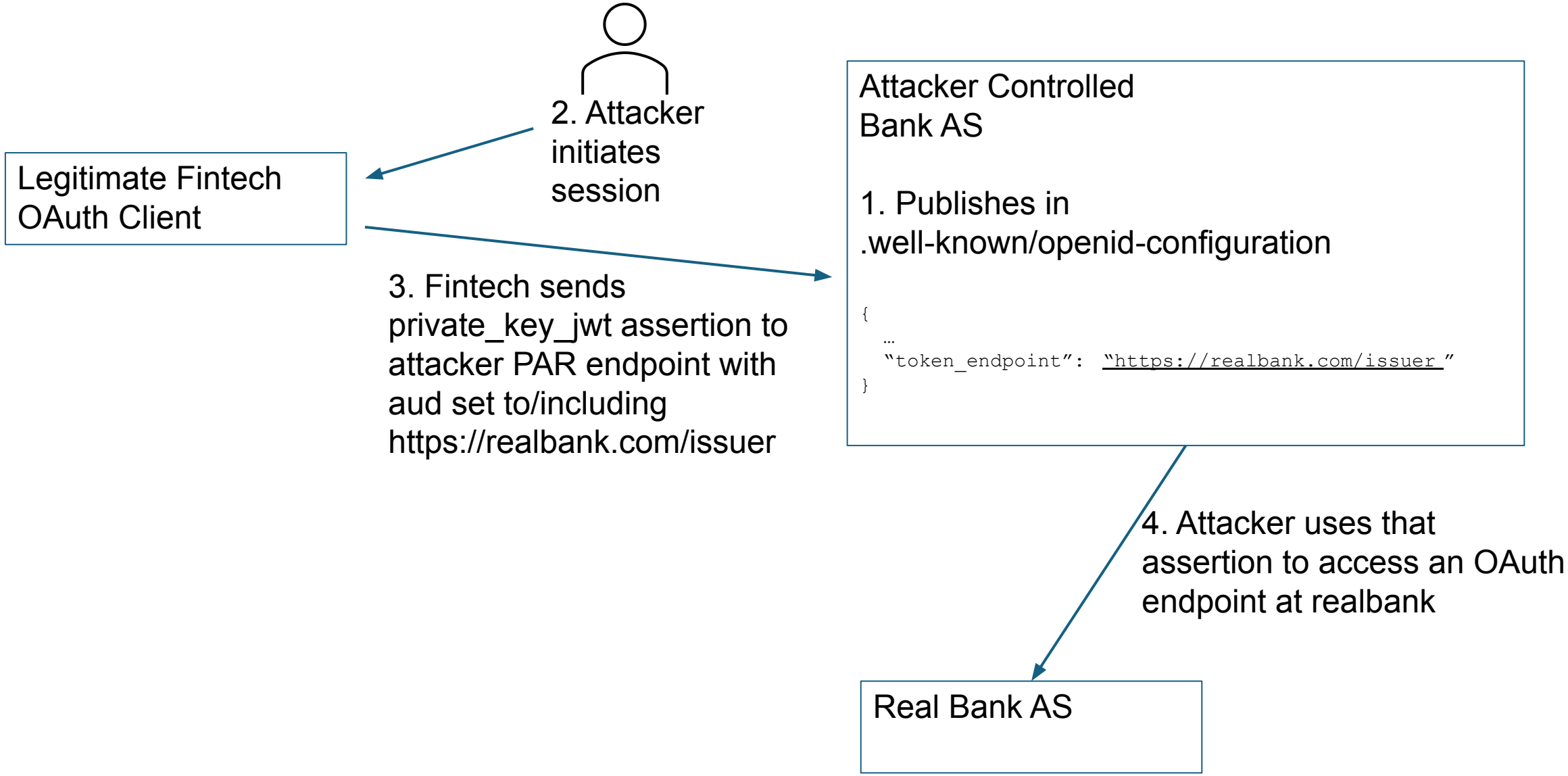
Attacker Controlled Bank AS

1. Publishes in .well-known/openid-configuration

```
{
  …
  “token_endpoint”:  “https://realbank.com/issuer ”
}
```

Real Bank AS


2. Attacker initiates session
Legitimate Fintech OAuth Client
Attacker Controlled Bank AS
1. Publishes in .well-known/openid-configuration
{
…
"token_endpoint": "https://realbank.com/issuer"
}
3. Fintech sends private_key_jwt assertion to attacker PAR endpoint with aud set to/including https://realbank.com/issuer
Real Bank AS


2. Attacker initiates session
Legitimate Fintech OAuth Client
Attacker Controlled Bank AS
1. Publishes in .well-known/openid-configuration
{
…
"token_endpoint": "https://realbank.com/issuer"
}
3. Fintech sends private_key_jwt assertion to attacker PAR endpoint with aud set to/including https://realbank.com/issuer
4. Attacker uses that assertion to access an OAuth endpoint at realbank
Real Bank AS

Requirements to perform attack / mitigations

- Attack should not be possible if MTLS is used and MTLS certificate is required to match client id
- Requires attacker to have registered a bank or gained control of a bank
- Probably requires 2+ endpoints with client authentication (e.g. PAR + token endpoint)
- client_id needs to be same across both AS (attacker can control if DCR used)
- FAPI2ID2 requires that client send aud == issuer
- Some ecosystems plan to ask AS to reject if aud != issuer

Pros and Cons of Possible Solutions

	"aud" = Issuer Identifier	"aud" = Target Endpoint	New claim like "htu"
Pros	Aligns w/ RFC 9207 "iss" Aligns w/ RFC 8414 issuer Single identifier for each AS Used in FAPI 2 security analysis Used in OpenID Federation	Usable in systems w/o issuer identifier (but not having it seems unlikely when client uses multiple ASs) Aligns w/ part of RFC 7523 token endpoint URL guidance	New claim that we can define however we like Doesn't require updating description of "aud" anywhere
Cons	Requires spec updates Requires updates to some software using private_key_jwt Alternative needed when no issuer in ecosystem (like RFC 9207 "deployment-specific ways" alternative)	Requires spec updates Requires updates to some software using private_key_jwt Many identifiers for same AS (one per endpoint) – confusing *May not solve the security problem* when endpoints shared by multiple ASs	Requires spec updates Requires updates to **all** software using private_key_jwt Gives up on purpose of "aud" Duplicates purpose of "aud"

Solution that Gained Consensus

“aud”=Issuer Identifier

- Issuer Identifier introduced by AS Metadata spec [RFC 8414]
- Single unambiguous identifier for the AS

Already used by most modern specs as AS “aud” value

- Recommended by PAR [RFC 9126]
- Used by JAR [RFC 9101]
- Used by OpenID FAPI 2
- Used by OpenID Federation
- Used by OAuth “iss” Parameter [RFC 9207]

Also enable explicit typing (“typ”=”...+jwt”) in updated specs

- Enables participants to know that updated specs being used

Solution Applied: Proposed Spec Updates

- OAuth JWT Assertions [RFC 7523]
- OAuth Assertion Framework [RFC 7521]
- OAuth SAML Assertions [RFC 7522]
- OpenID Connect Core
- OpenID FAPI 1
- OpenID FAPI 2
- OpenID Federation
- OpenID Client-Initiated Backchannel Authentication (CIBA)
- OAuth JWT Authorization Request (JAR) [RFC 9101]
- OAuth Pushed Authorization Request (PAR) [RFC 9126]
- OAuth Security BCP [RFC-to-be 9700]

OAuth JWT Assertions [RFC 7523]

- Defines private_key_jwt and client authentication JWT
- Defines JWT assertion grant
- Audience for both “MAY be token endpoint URL”
- Multiple audiences allowed

Proposed bis document available

- https://selfissued.github.io/draft-jones-oauth-rfc7523bis/draft-jones-oauth-rfc7523bis.html
- Requires that AS issuer identifier be sole audience
- Replaces RFC 7523 and updates several others

OAuth Assertion Framework [RFC 7521]

- Defines assertion framework for assertions sent to authorization server
- Audience as in RFC 7523
- Proposed rfc7523bis updates it to tighten audience

OAuth SAML Assertions [RFC 7522]

- Defines SAML assertions sent to authorization server
- Audience as in RFC 7523
- Proposed rfc7523bis updates it to tighten audience

OpenID Connect Core

- Login protocol layered on OAuth 2.0
- Defines private_key_jwt and client_secret_jwt audience as “SHOULD be the URL of the AS’s Token Endpoint”

Proposed errata update document available

- https://openid.bitbucket.io/connect/openid-connect-core-1_0.html
- Requires that AS issuer identifier be sole audience

OpenID FAPI 1

- Financial-Grade API (FAPI) an OAuth profile providing interop and security guidance
- Requires AS issuer identifier as one of the audience values
- Multiple audiences allowed

Proposed errata update document available

- https://openid.bitbucket.io/fapi/openid-financial-api-part-2-1_0.html
- Requires that AS issuer identifier be sole audience

OpenID FAPI 2

- FAPI 2 a revised OAuth profile providing interop and security guidance
- Spec updated to require that AS issuer identifier be sole audience
- In review to become a final specification
- https://openid.net/specs/fapi-security-profile-2_0.html

OpenID Federation

- Enables multilateral trust establishment
- Security analysis of OpenID Federation revealed vulnerability
- Spec updated to require that AS issuer identifier be sole audience
- https://openid.net/specs/openid-federation-1_0.html

OpenID Client-Initiated Backchannel Authentication (CIBA) Core

- Login protocol layered on OAuth 2 across multiple devices
- Requires accepting any of three different audience values!

Proposed errata update document available

- https://openid.bitbucket.io/modrna/openid-client-initiated-backchannel-authentication-core-1_0.html
- Requires that AS issuer identifier be sole audience

OAuth JWT Authorization Request (JAR) [RFC 9101]

- OAuth Authorization Requests as JWTs
- Says that audience should (lowercase) be AS issuer identifier
- Proposed rfc7523bis updates it to require that AS issuer identifier be sole audience

OAuth Pushed Authorization Request (PAR) [RFC 9126]

- OAuth Authorization Requests pushed to an endpoint
- Like CIBA, currently requires accept three different audience values!
- Proposed rfc7523bis updates it to require that AS issuer identifier be sole audience

OAuth Security BCP [RFC-to-be 9700]

- In RFC Editor queue but waiting for decision on how to handle this OAuth security vulnerability
- Current text https://www.rfc-editor.org/authors/rfc9700.html
- Currently has no guidance on audience for tokens sent to AS
- Propose to short new section along these lines:
  - **4.18. Audience for Tokens Intended for Authorization Server**
  - Describe vulnerabilities enabled by allowing tokens sent to AS to have multiple audiences and ambiguous audiences
  - Describe mitigation by requiring that AS issuer identifier be sole audience value
- Proposed Recommendation text at https://self-issued.info/docs/rfc9700.html#section-4.18

Next Steps

- Plan to publish draft-jones-oauth-rfc7523bis after call
  - Can chairs then please run an adoption call for it?
  - Note this is a starting point for security mitigations - not finished work
- Plan to publish OpenID Connect Core draft after call
- Also publish CIBA Core draft after call?

Questions & Actions for You

- Is there anyone else that needs to be told about this because they might be vulnerable?

- rfc7523bis currently updates all the affected OAuth specs
  - Do people prefer this all-in-one approach or separate docs for each spec being updated?

- Proposed addition to Security BCP
  - We'd like working group approval to add description of vulnerability and mitigation before publishing BCP

Discussion

- Your turn!

Reminder: Please don’t share details of this publicly yet