Token and Identity Chaining Using OAuth 2.0 Token Exchange

November 3, 2021

Kelley Burgin

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

MITRE Enterprise OAuth and OpenID Connect Profiles

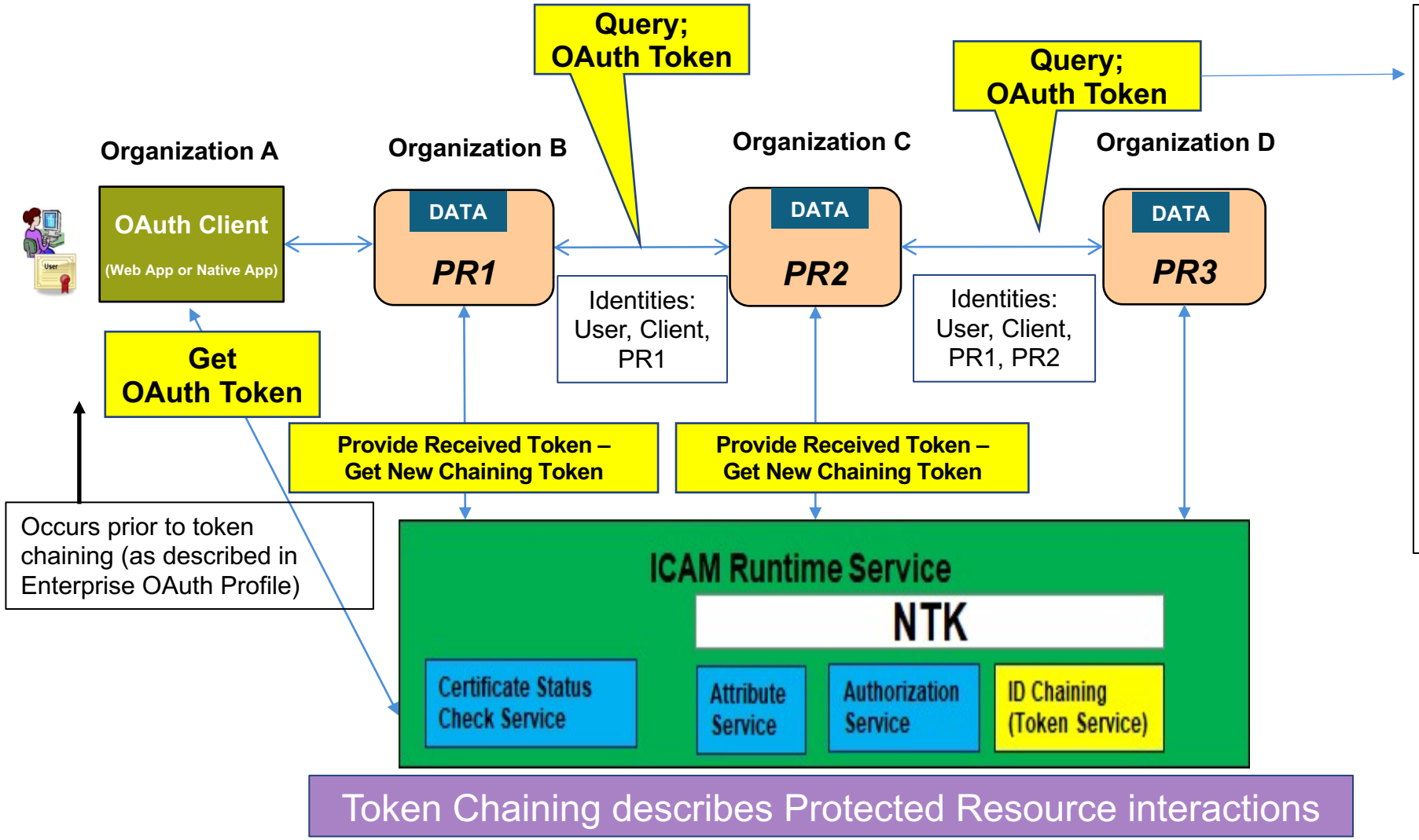
- **Published two profiles to enable "identity bridging" and federated authn**
  - Enterprise Mission Tailored OAuth 2.0 and OpenID Connect Profiles
  - Identity of user and client are bridged to access a resource

- **Goal: Enable secure, interoperable use of OAuth and OpenID Connect in enterprise environments**
  - Details specifics of targeted enterprise use cases
  - Leverages existing enterprise environment (e.g. NPE PKI for servers)
  - Leverages prior work by IETF OAuth WG, OpenID Foundation, etc.

Token Chaining

- **Problem: An OAuth client makes a request to a protected resource (PR1), but PR1 needs to access a second PR (PR2) (which might need to access a third PR, and so on) to answer the client's request.**
- **Two Cases:**
  1. **Single ICAM Ecosystem**: All PRs belong to the same organization and trust the same authorization server (AS).
  2. **Multiple ICAM Ecosystem:** (At least) two of the PRs belong to different organizations and trust different authorization servers.
- **Solution:**
  - PR1, acting as an OAuth client, uses the IETF OAuth Token Exchange protocol to exchange received access token with the AS for a new access token that it can use to access PR2.
- **Relatively simple for single ICAM ecosystem; more complicated for multiple ICAM ecosystem**

Token Chaining in a Single ICAM Ecosystem




```
"sub": "User"
"client_id": "PR2"
"aud": "PR3"
"act": {
    "sub": "PR2"
    "act": {
        "sub": "PR1"
        "act" : {
            "sub": "Client"
        }
    }
}
```

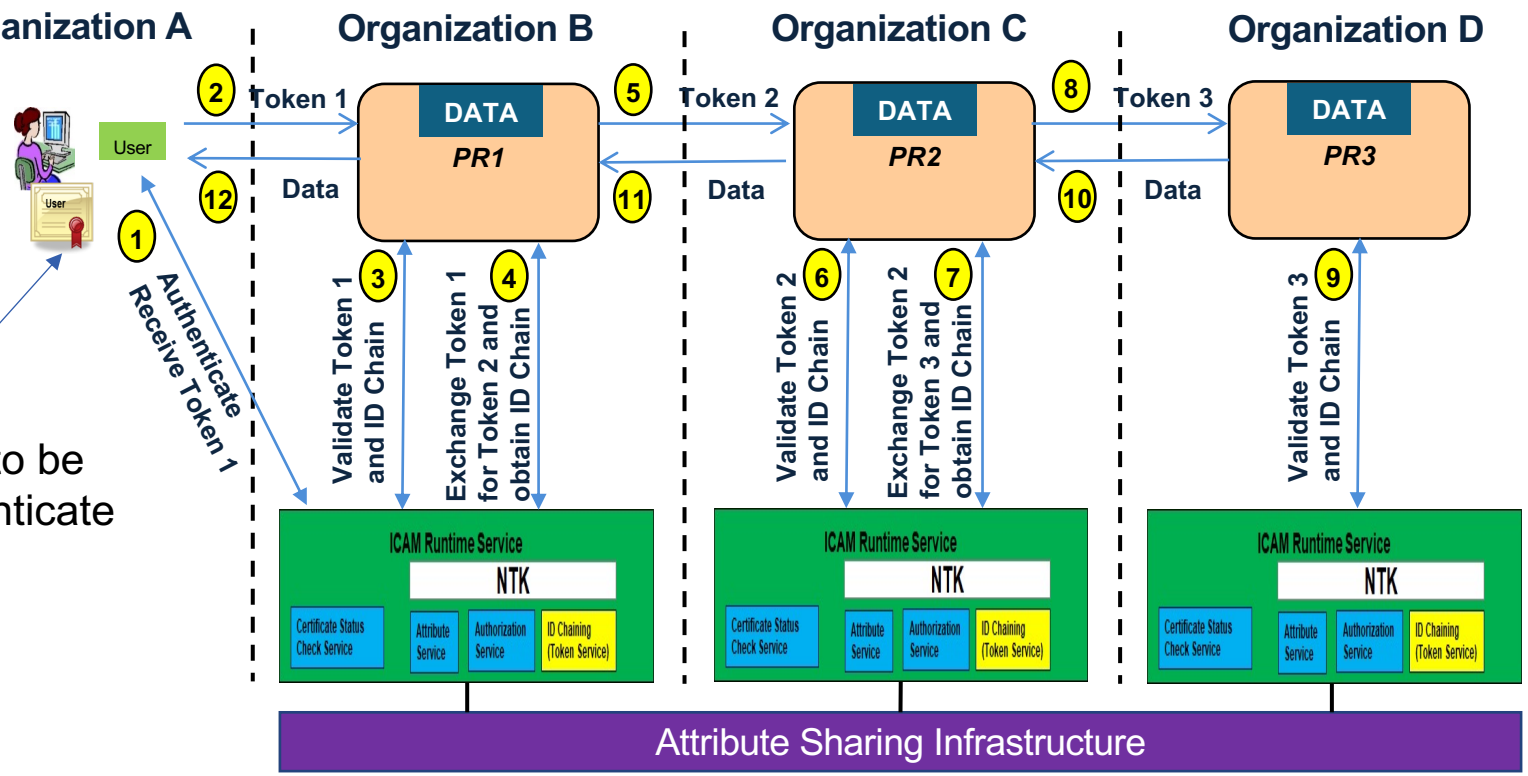
(additional claims not depicted)

Token Chaining describes Protected Resource interactions

Token Chaining in a Multiple ICAM Ecosystem

User may be in the same or different organization as PR1

Does not need to be PKI. Can authenticate any way



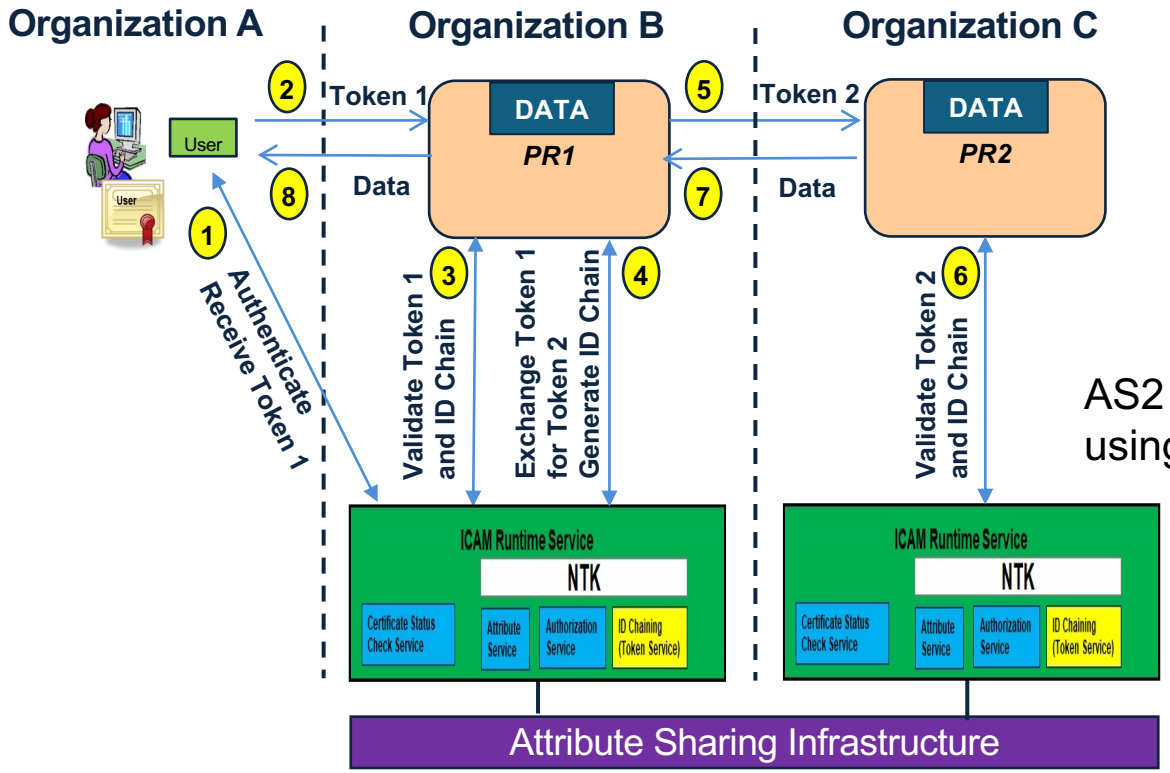
Multiple ICAM Token Chaining Solution Options

- 1. PR1 obtains 2nd access token from AS1 via OAuth Token Exchange
- 2. PR1 obtains 2nd access token from AS2 via OAuth Token Exchange
- 3a. PR1 obtains a JWT assertion from AS1 that PR1 sends to AS2 as part of an OAuth assertion grant request to obtain a 2nd access token
- 3b. PR1 obtains 2nd access token from AS1 via JWT assertion grant request by AS1 to AS2

Multiple ICAM Ecosystem – Option 1
PR1 obtains 2nd access token from AS1

PR1 obtains a second access token from its AS1 for use at PR2.

- PR2 asks (using token introspection) its own AS2 to verify the token since PR2 only trust tokens from AS2



AS2 could validate using token signatures

Multiple ICAM Ecosystem – Option 1
PR1 obtains 2nd access token from AS1

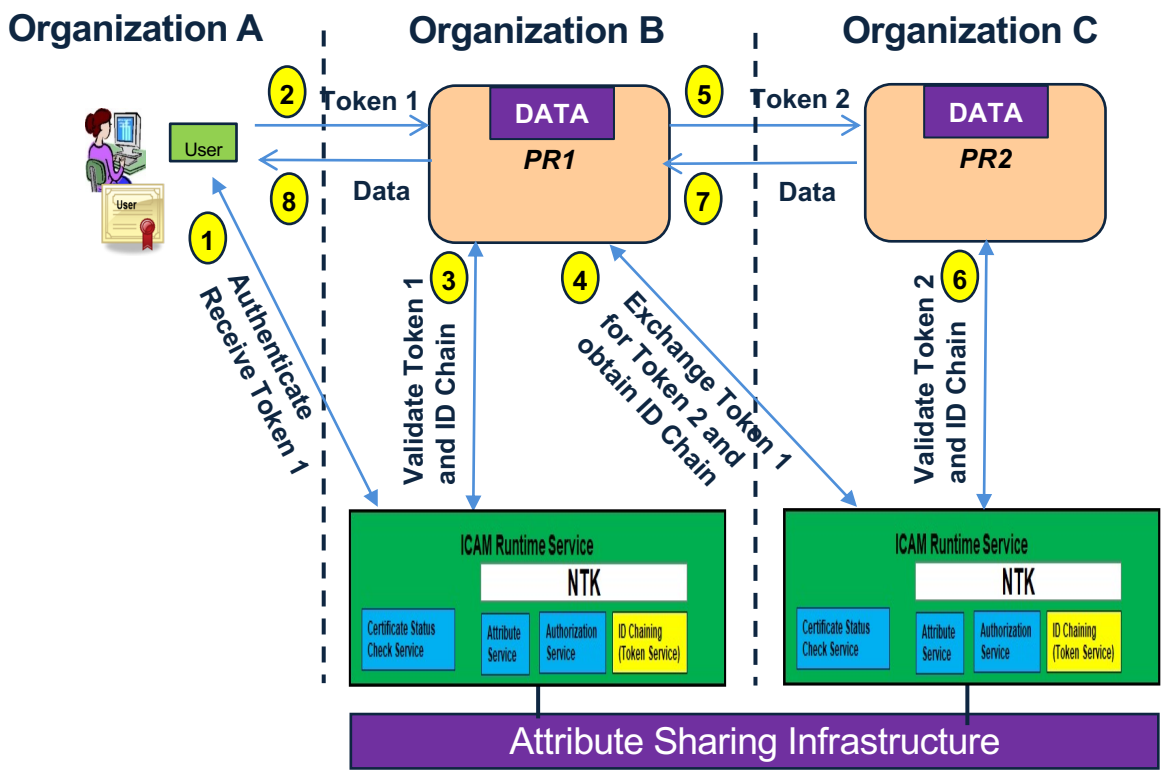
- **Pros**
  - The PRs in one organization do not need to register with the AS of every other organization they may need to access.

- **Cons**
  - PR2 needs to trust tokens issued by AS1
    - Need to make sure this doesn't introduce security issues
    - Use of token introspection with its AS2 intends to mitigate issues
  - AS2 needs to be able to verify access tokens issued by AS1
  - "Off-label" use of token introspection protocol

Multiple ICAM Ecosystem – Option 2
PR1 obtains 2nd access token from AS2

PR1 performs token exchange with AS2 in PR2's organization to receive a second access token it can use to access PR2

- PR1 acts as an OAuth client using the OAuth Token Exchange protocol to obtain an access token from PR2's AS2 to access PR2



Multiple ICAM Ecosystem – Option 2
PR1 obtains 2nd access token from AS2

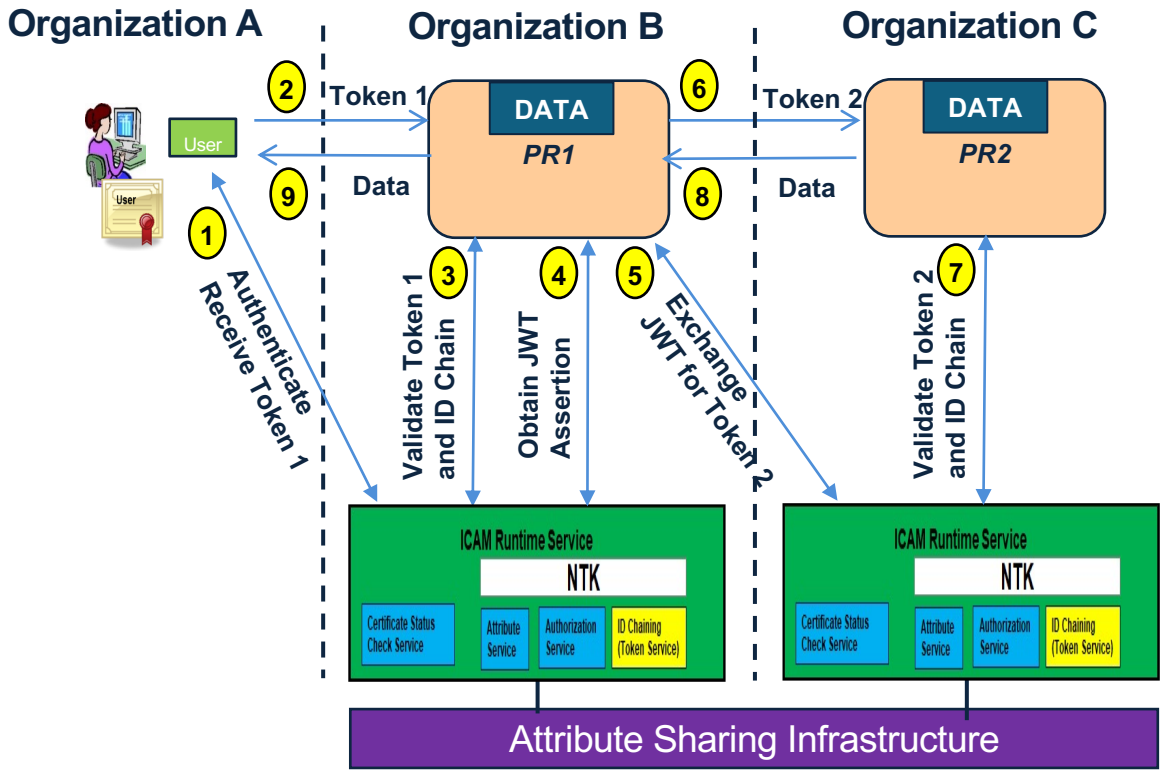
- **Pros**
  - PR2 only needs to be able to validate tokens issued by its own authorization server AS2 rather than tokens issued by other authorization servers.

- **Cons**
  - The protected resources in one organization must register with the authorization server of every other organization it may need to access.
  - AS2 must be able to trust, interpret, and verify access tokens issued by AS1 (and all other relevant organizations) in order to complete token exchange.

Multiple ICAM Ecosystem – Option 3a
PR1 obtains 2nd access token from AS2 using a JWT Assertion

PR1 performs token exchange with AS1 in its organization to receive a JWT assertion [RFC7523] that it sends to AS2 as part of an OAuth assertion grant request.

- AS2 then returns an access token to PR1 that it can use to access PR2



Multiple ICAM Ecosystem – Option 3a
PR1 obtains 2nd access token from AS2 using a JWT Assertion

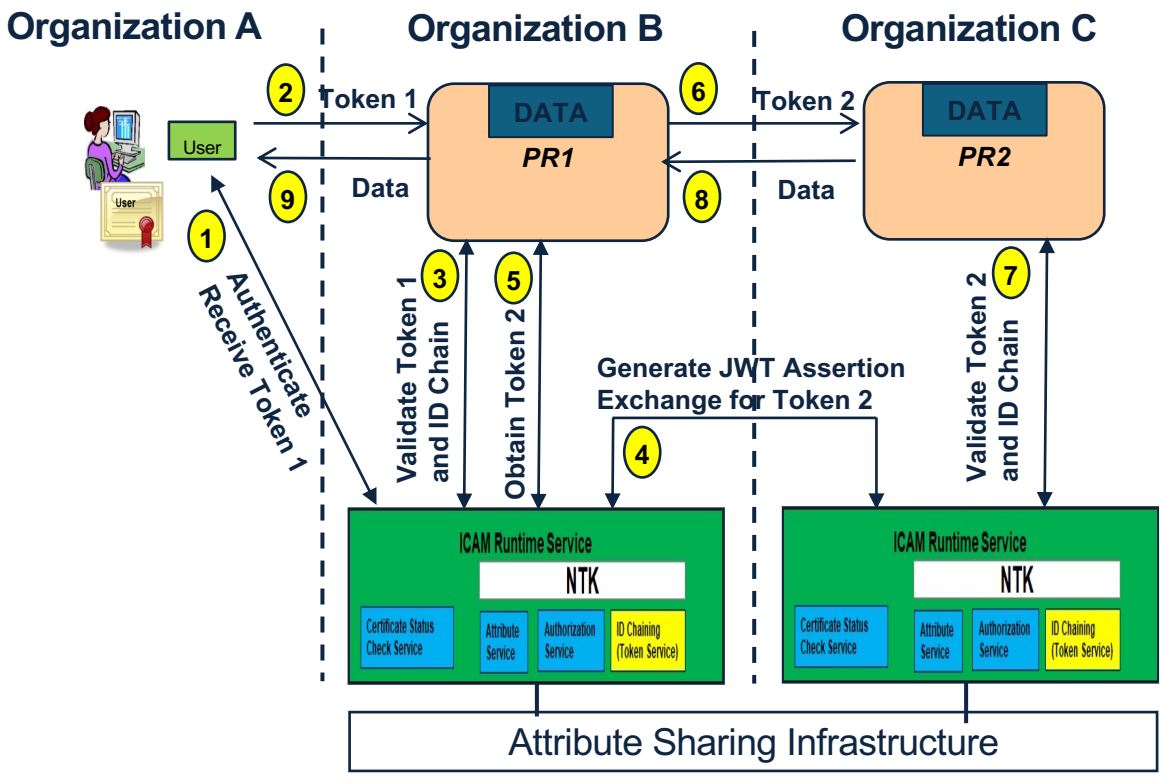
- **Pros**
  - PR2 only receives access tokens issued by its authorization server AS2
  - JWT Assertions are intended to be used ”across security domains” [RFC 7521]

- **Cons**
  - AS2 must trust assertions issued by AS1 in order to respond successfully to the assertion grant request
  - AS1 and AS2 need to agree on content of JWT Assertions
  - Multiple interactions needed; may introduce latency delays

Multiple ICAM Ecosystem – Option 3b
PR1 obtains 2nd access token from AS1 using a JWT Assertion

PR1 performs token exchange with the authorization server AS1 in its organization to receive a new access token it can use to access PR2.

- AS1 generates a JWT assertion and issues an assertion grant request to AS2 using the assertion AS1 generated to receive a new access token generated by AS2 that PR1 can use to access PR2



Multiple ICAM Ecosystem – Option 3b
PR1 obtains 2nd access token from AS1 using a JWT Assertion

- **Pros**
  - PR1 does not need to be registered at AS2
  - PR2 only receives access tokens issued by its authorization server AS2
  - JWT Assertions are intended to be used ”across security domains” [RFC 7521]

- **Cons**
  - AS2 must trust assertions issued by AS1 (to respond to the assertion grant request)
  - AS1 and AS2 need to agree on content of JWT Assertions
  - Multiple interactions needed; may introduce latency delays

Token Chaining Profile Security Requirements

- **All PRs and ASs are profile-compliant with Enterprise OAuth Profile**
- **The token being exchanged must contain an "aud" field, and it must identify PR1**
  - Ensures PR1 is the intended recipient of an access token in order to exchange it for another access token
  - Intended to prevent stolen access tokens from being exchanged for new access tokens by an unauthorized entity
  - [RFC8693] does not contain this explicit requirement.
- **Access tokens obtained through token exchange must identify the entire chain of clients and PRs that held previously exchanged access tokens.**
- **The newly issued access token must contain an "act" claim that identifies the PR that exchanged the token, the client that sent the token to the PR, and any other entities involved in exchanges of other access tokens in the chain**
  - Enables the PR consuming the access token to look up authorizations or privileges associated with each entity in the chain as part of deciding what access to allow

Backup

Token Chaining Profile Requirements (1)

- **PR1, PR2, AS1, and AS2 are profile-compliant with Enterprise OAuth Profile**
- **PRs connect to Authorization Servers over mutually authenticated TLS**
- **PR1 provides to-be-exchanged access token and requests new token**
  - PR1 specifies scope, resource, and/or audience for new token
- **AS authenticates PRs (using PR's PKI certificate)**
- **AS verifies that the to-be-exchanged access token is valid and that PR1 is the token's intended audience**
- **AS verifies that PR1 is authorized to exchange for the requested token**
  - Details of how are out-of-scope of the profile
- **AS provides new access token to PR1**
  - Details of how scopes, etc. are populated are out-of-scope (just as they are in the Enterprise Mission Tailored OAuth Profile)

Token Chaining Profile Requirements (2)

- **New access token has PR1 as the client_id and is sender-constrained to PR1's PKI certificate**
- **New access token contains "act" claim**
  - Contains "sub" claim identifying PR1, "iss" claim identifying AS, and all previous "act" claims from previous tokens to show entire history of token holders back to the original client
- **"act" claim could be used by PR2 for authorization**
  - PR2 could use it to determine intersection of allowed accesses of entire token chain
  - However, Section 4.1 of OAuth Token Exchange says not to consider anything besides the newest (outer) "act" claim (unsafe in multiple ICAM ecosystem?)
- **Or, other methods can be used by PR2 for authorization instead**
  - "scope", "resource" or other claims within access token, with AS configured to appropriately populate the claims (e.g. by considering authorizations held by the entities involved in the token exchange)