MITRE

Token and Identity Chaining Between Protected Resources in a Single ICAM Ecosystem Using OAuth Token Exchange

Annapolis Junction, MD

Beth Abramowitz
Kelley Burgin
Neil McNab
Michael Peck
Mark Russell
Roger Westman

May 2021

Approved for Public Release; Distribution Unlimited 21-1421

This page intentionally left blank.

Table of Contents

List of Figures

1 Introduction

This document extends the Enterprise Mission Tailored OAuth 2.0 Profile [OAuth-Profile] to enable token and identity chaining in a single Identity, Credential, and Access Management (ICAM) ecosystem by profiling OAuth 2.0 Token Exchange [RFC8693], an Internet Engineering Task Force (IETF) Request for Comments (RFC) that defines a protocol that enables exchanging an access token with an authorization server (AS) for another access token. Readers of this document are expected to have a thorough understanding of the Enterprise Mission Tailored OAuth 2.0 Profile.

All components described in the following are assumed to be profile-compliant with the Enterprise Mission Tailored OAuth 2.0 profile. The requirements in this document assume a single ICAM ecosystem, where all of the involved protected resources (but not necessarily all of the users) are in the same ICAM ecosystem, meaning that they trust the same authorization server. An ICAM ecosystem refers to a system that performs authentication and authorization services within a given security domain (such as a corporation or government organization). A separate profile [Token-Chaining2] provides requirements for a multiple ICAM ecosystem involving protected resources that trust different authorization servers.

The Enterprise Mission Tailored OAuth 2.0 Profile describes use of OAuth 2.0 by an OAuth client to obtain an OAuth access token to access an OAuth protected resource, such as a backend database, on a user's behalf. As described in [OAuth-Profile], the OAuth client may be a web application running on a remote web server, or it may be a native application running on the user's own endpoint system. The type of OAuth client and the method (if any) by which the user authenticates to the OAuth client is out of scope for this profile.

This profile describes how to handle the situation where, in a single ICAM ecosystem, a protected resource (PR1) may need to call a second protected resource (PR2) such as a second backend database in order to satisfy a query received from a client. PR1 cannot simply replay Token1 at PR2 since the Enterprise Mission Tailored OAuth 2.0 Profile requires that the tokens be sender and/or audience constrained, so PR1 must request a new access token, Token2, from an authorization server that is valid for PR1 to use at PR2 (in this usage, PR1 is acting as an OAuth client). If PR2 needs to access a third protected resource (PR3), then PR2 must request a new access token, Token3, and so on. This process of exchanging Token1 (which grants access to PR1) to obtain a new access token, Token2 (which grants access to PR2) is called ***token chaining***. This profile additionally enables ***identity chaining*** by ensuring that the identities of the user, client, and protected resources are propagated in the exchanged tokens, so that each protected resource can, as necessary, use the set of identities to make appropriate access decisions.

This profile describes only the case where an OAuth protected resource receives an OAuth access token and is exchanging it for a new OAuth access token. Another use case may exist where an OAuth client (or protected resource acting as an OAuth client) needs to obtain an access token to act on behalf of a user but does not have an access token to exchange and cannot perform the OAuth authorization code flow as described in OAuth-Profile to obtain an access token. Also, use cases may exist where other types of tokens, such as Security Access Markup

Language tokens, need to be exchanged. This profile does not describe those use cases. Requirements to meet those use cases would need to be specified separately.

1.1 Requirements Notation and Convention

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.2 Terminology

This specification uses the terms "Access Token", "Authorization Server", "Client", "Protected Resource", "Resource Server", and “Token Endpoint” defined by OAuth 2.0 [RFC6749], the term “Token Endpoint” defined by [RFC7662], the term “Token Exchange” defined by [RFC8693], and the terms defined by OpenID Connect Core 1.0 [OIDC-Core].

1.3 Conformance

This specification defines requirements for the following components:

- OAuth 2.0 protected resources.
- OAuth 2.0 authorization servers.

The requirements include details of interaction between these components:

- Protected resource (acting as a client) to authorization server.
- Protected resource (acting as a client) to another protected resource.

When a profile-compliant component is interacting with other profile-compliant components, in any valid combination, all components MUST implement the requirements as stated in this specification. All interaction with non-profile components is outside the scope of this specification.

A profile-compliant OAuth 2.0 protected resource acting in the role of a client to exchange an access token for use at another protected resource MUST support and utilize certain features as described in section 2 of this specification.

A profile-compliant OAuth 2.0 protected resource receiving exchanged access tokens from another entity MUST support and utilize certain features as described in section 2 of this specification.

A profile-compliant OAuth 2.0 authorization server MUST support and utilize certain features as described in section 3 of this specification.

1.4 Single ICAM Ecosystem

The following terms will be used throughout the rest of the document.

PR1	The protected resource receiving the client request and then acting as an OAuth client in OAuth Token Exchange to obtain a new access token to a second protected resource
PR2	The second protected resource being accessed by PR1
AS	The authorization server

Token and identity chaining can take place between two protected resources in the same ICAM ecosystem or between protected resources in different ICAM ecosystems. The focus of this document is on the first case, a single ICAM ecosystem.

The Enterprise Mission Tailored OAuth Profile limits each protected resource to only trust one authorization server. In a single ICAM ecosystem, each protected resource (PR1) will contact its authorization server to obtain an access token that can be used at another protected resource (PR2), and both protected resources (PR1 and PR2) trust the same authorization server.

Token and identity chaining in a single ICAM ecosystem case is described in the following. The client follows the OAuth protocol flow as usual to obtain an access token, Token1, to access PR1. The client presents Token1 to PR1, which in turn needs to access PR2 to satisfy the client query. PR1 (acting as an OAuth client) uses OAuth Token Exchange [RFC8693] to exchange Token1 for a second token, Token2, that PR1 can use to access PR2. PR1 then presents Token2 to PR2 to obtain the data needed to satisfy the client request. Figure 1 shows this process.

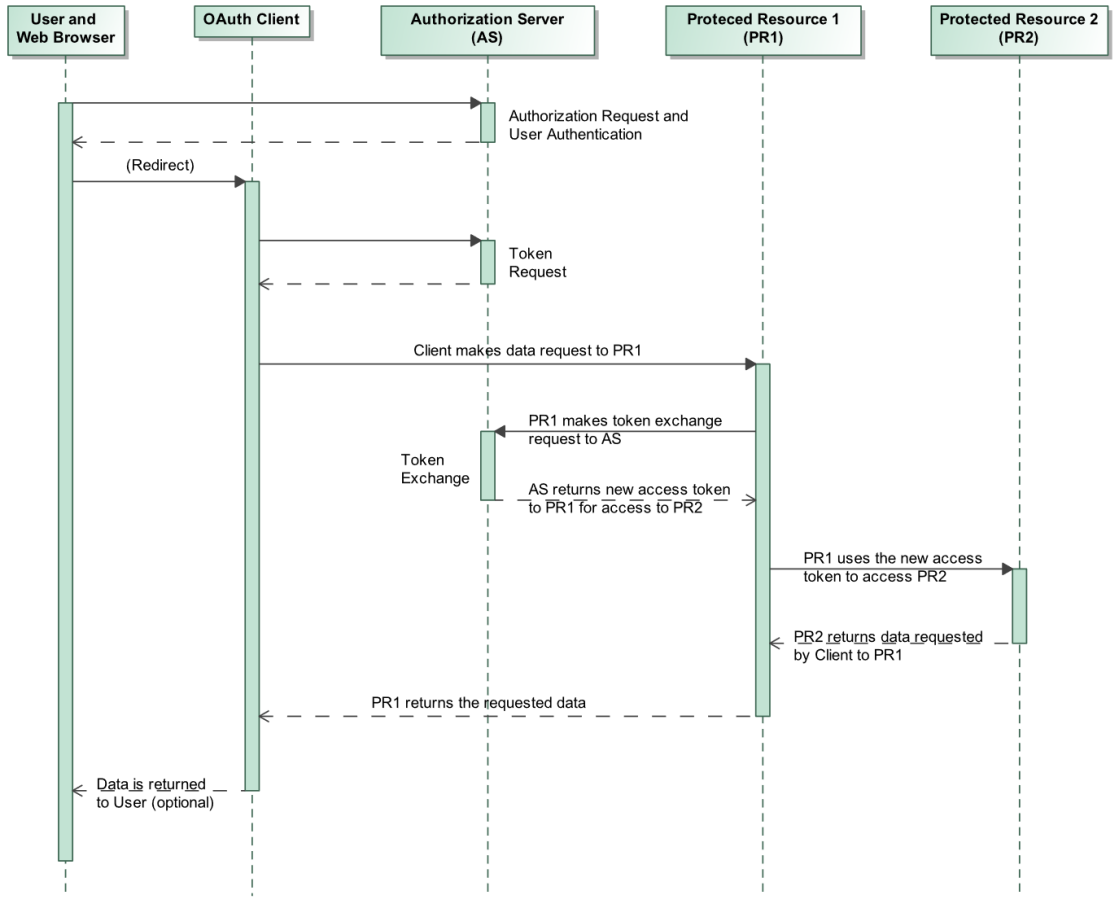

Figure 1: Token Chaining in a Single ICAM Ecosystem Using OAuth Token Exchange

This process may continue if PR2 needs to access a third protected resource, PR3 satisfy the client request. This process may continue further if PR3 needs to access a fourth protected resource, PR4, and so on. In each case, the protected resources (PR2 and PR3, PR3 and PR4) involved satisfy the roles of PR1 and PR2 in the protocol described above. A scenario where PR1 needs to ultimately obtain data from PR5 in order to satisfy the client request is shown in Figure 2.

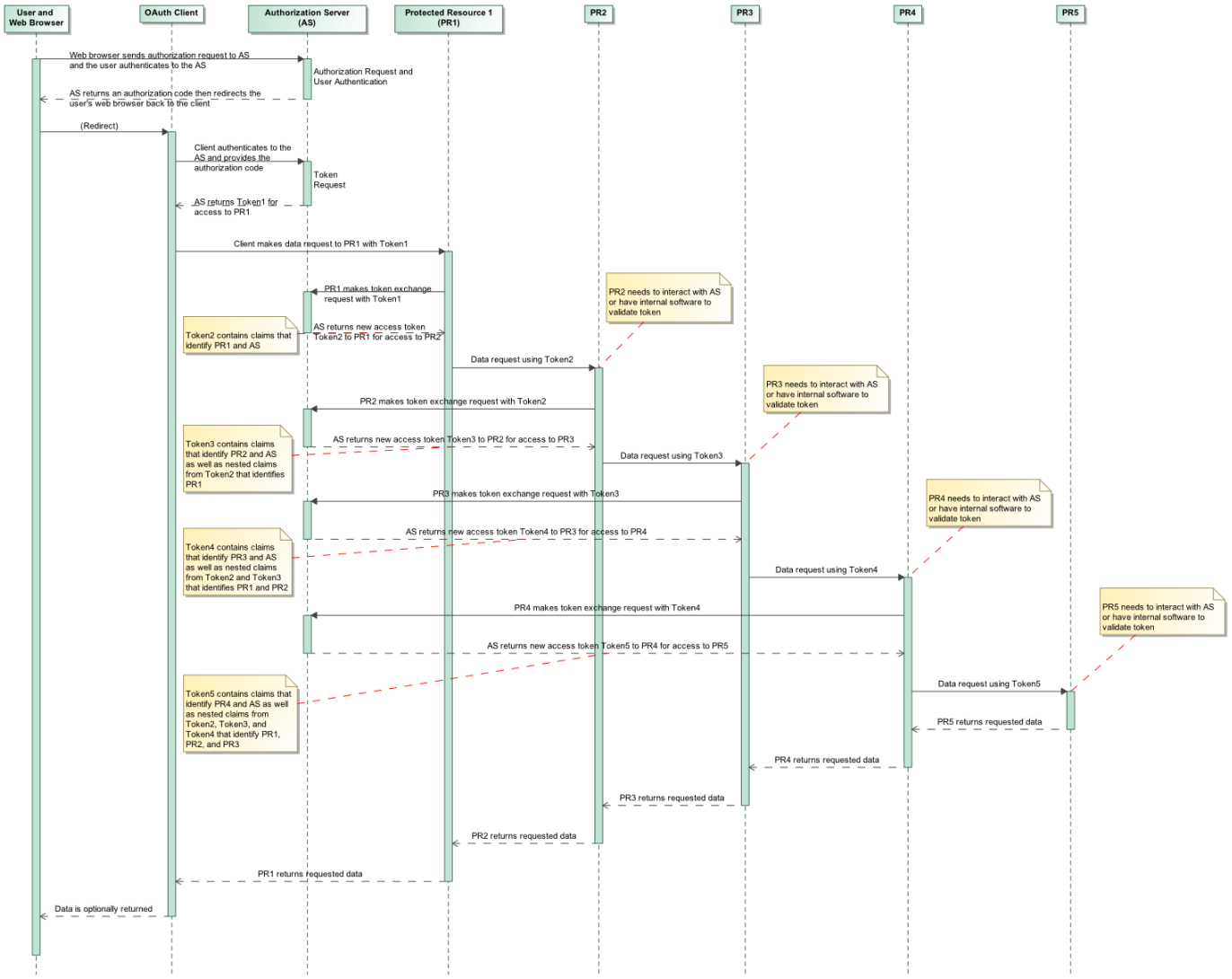

Figure 2: Token Chaining in a Single ICAM Ecosystem with Multiple Protected Resources

Although this profile requires that all protected resources are in the same ICAM ecosystem (trust the same authorization server), since the steps for the OAuth client to obtain the first token (typically based on the authorization server authenticating the user's request) are not part of this profile (they occur before token chaining starts), the user may belong to the same ICAM ecosystem as the protected resources or may be part of a different ICAM ecosystem.

2 Protected Resource Profiles

The protected resources acting in the roles of PR1 and PR2 MUST comply with the requirements described in Section 4 (Protected Resource Profile) of the Enterprise Mission Tailored OAuth 2.0 Profile.

2.1 Protected Resource 1 (PR1) Profile

This section imposes requirements on and describes the actions taken by PR1 to obtain a new access token from an authorization server valid for use by PR1 at PR2. When interacting with the authorization server and with PR2, PR1 is acting in the role of an OAuth client. If PR2 then needs to exchange the access token to access PR3, then PR2 would adopt the role of PR1 as described in this profile, and PR3 would adopt the role of PR2.

2.1.1 Connection to the Authorization Server

When performing token exchange, PR1 MUST authenticate to the token endpoint of the authorization server using mutually authenticated Transport Layer Security (TLS), in compliance with Section 2.1 of RFC8705, using a Public Key Infrastructure (PKI) certificate and corresponding private key.

PR1, when complying with this profile, an organization MUST set the fields of its token exchange requests as follows:

grant_type	REQUIRED	Value set to "urn:ietf:params:oauth:grant-type:token-exchange" as required by Section 2.1 of [RFC8693].
client_id	REQUIRED	Value set to PR1's client_id at the authorization server as required by Section 2 of [RFC8705].
resource	OPTIONAL - at least one of "resource" or "audience" MUST be set	Set as described in [RFC8693]. The requirement that at least one of "resource" or "audience" must be set is per this profile.
audience	OPTIONAL - at least one of "resource" or "audience" MUST be set	Set as described in [RFC8693]. The requirement that at least one of "resource" or "audience" must be set is per this profile.
scope	OPTIONAL	Set as described in [RFC8693].
requested_token_type	REQUIRED	Value set to "urn:ietf:params:oauth:token-type:access_token" as described in Section 3 of [RFC8693]. The requirement that requested_token_type must be set is per this profile.

subject_token	REQUIRED	Value set to the access token sent to PR1 from its client. The requirement to include subject_token is per [RFC8693] Section 2.1. The requirement that it be set to the access token is per this profile.
subject_token_type	REQUIRED	Value set to "urn:ietf:params:oauth:token-type:access_token". The requirement to include subject_token_type is per [RFC8693] Section 2.1. The requirement that it identify an access token is per this profile.
actor_token	NOT ALLOWED	PR1 is the actor and identifies itself to the authorization server through TLS client certificate authentication per [RFC8705]; therefore, this field is not permitted. This field is optional per [RFC8693] Section 2.1 and is prohibited per this profile.
actor_token_type	NOT ALLOWED	PR1 is the actor and identifies itself to the authorization server through TLS client certificate authentication per [RFC8705]; therefore, this field is not permitted. This field is prohibited per [RFC8693] Section 2.1 when actor_token is not present.

2.1.2 Connection to PR2

For connections between PR1 and PR2, where PR1 is acting in an OAuth Client role, PR1 MUST comply with the requirements described in Section 2.3 (Client Connection to the Protected Resource) of the Enterprise Mission Tailored OAuth 2.0 Profile.

2.2 Protected Resource 2 (PR2) Profile

As described by Section 3.9 of the Enterprise Mission Tailored OAuth 2.0 Profile, PR2 (the recipient of an access token presented by PR1) may directly make authorization decisions based on the scopes or other claims that are optionally found in the access token. Alternatively, PR2 can make use of applicable enterprise authorization services to determine the allowed access. This access determination can be based on the user's identity (as asserted by the "sub" claim), PR1's identity (as asserted by the "client_id" claim), and the identity of the original client and any other protected resources involved in the token exchange (as asserted by the "act" claim).

If the protected resource acting in the role of PR2 needs to make a request to an additional protected resource, this initiates a new token chaining transaction. Such protected resources that both receive and request chained tokens must comply with the PR1 profile in the context of requesting new tokens for further resource access, and with the PR2 profile in the context of receiving tokens from the prior protected resource in the chain. No additional requirements are imposed on protected resources that perform both roles.

However, risks exist that must be accepted if PR2 chooses to use identities asserted by nested "act" claims within the access token. [RFC8693] states, "[f]or the purpose of applying access control policy, the consumer of a token MUST only consider the token's top-level claims and the party identified as the current actor by the ‘act’ claim. Prior actors identified by any nested ‘act’ claims are informational only and are not to be considered in access control decisions."

3 Authorization Server (AS) Profile

The authorization server MUST comply with the requirements described in Section 3 (Authorization Server Profile) of the Enterprise Mission Tailored OAuth 2.0 Profile.

This section imposes requirements on and describes the actions taken by the authorization server when performing token exchange with PR1 so that PR1 can obtain a new access token valid for use by PR1 at PR2.

The authorization server MUST allow token exchange only if it has authenticated PR1 using mutually authenticated TLS in compliance with Section 2.1 of [RFC8705]. PR1 MUST be registered as an OAuth client at the AS, with the subject distinguished name of PR1’s PKI certificate associated with that client’s registration for authentication purposes.

The authorization server MUST ensure before allowing token exchange that the subject_token field in the token exchange request contains a valid, unexpired OAuth access token (compliant with the format specified in Section 3.3 of the Enterprise Mission Tailored OAuth 2.0 Profile). This access token to be exchanged MUST contain an “aud” claim, and the claim MUST specifically identify PR1 as a valid recipient of the token.

The authorization server MUST provide the ability to set and enforce an authorization policy that determines under what conditions token exchange is permitted and how claims will be populated in the issued token. The authorization policy MUST specify which protected resources are allowed to perform token exchange. If tokens issued as a result of token exchange are to contain “scope”, “resource”, “aud” or similar claims, the authorization policy MUST specify the allowed values for these claims. For example, in most cases it would be desired that a new access token’s “scope” claim must contain a subset of the values in the access token to be exchanged, not new values, as PR1 should not be able to obtain new authorizations that were not originally granted by the user to the client. **It is critical that each authorization server’s administrators appropriately configure the token exchange authorization policy to meet the organization’s security objectives; otherwise, serious privilege escalation threats may be introduced.**

Note that Section 3.9 of the Enterprise Mission Tailored OAuth 2.0 Profile states that issued access tokens “are not required to contain scopes or other claims conveying detailed authorization information.” If they do not, the protected resource (PR2) consuming the newly issued token can make use of applicable enterprise authorization services to determine the allowed access. This access can be based on the user’s identity (as asserted by the “sub” claim), PR1’s identity (as asserted by the “client_id” claim), and the identity of the original client and any other protected resources involved in the token exchange chain (as asserted by the “act” claim described below).

If the token exchange request passes the authorization server's checks, the authorization server will generate a new access token compliant with section 3.3 of the Enterprise Mission Tailored OAuth 2.0 Profile. If the "amr" or "auth_time" fields are present in the access token to be exchanged, the authorization server MUST place the field in the new access token and populate it with the same value (to indicate the properties of the initial authentication to the authorization server).

Since PR1 was identified using mutually authenticated TLS, the authorization server MUST populate a "cnf" claim in the new access token as specified by section 3.3 of the Enterprise Mission Tailored OAuth 2.0 Profile.

Each organization should perform a risk analysis to determine an appropriate policy for populating the "exp" (expiration) claim of new access token. Authorization servers SHOULD make the token expiration behavior configurable. In some cases, the appropriate position would be to ensure that the "exp" claim's value is less than or equal to the "exp" claim of the access token to be exchanged, to prevent the token exchange process from being abused to create new access tokens with longer validity than the original access token. However, there may be cases where an operation takes a lengthy amount of time and potentially involves a chain of many protected resources, where it may be necessary to extend the lifetime of exchanged tokens beyond the original token's expiration.

The authorization server MUST populate an "act" claim in the new access token as specified by Section 4.1 of [RFC8693]. The "act" claim MUST contain a "sub" claim identifying PR1 and an "iss" claim identifying the AS. If an "act" claim is present in the access token to be exchanged, the AS MUST copy it into the new access token as a nested claim within the new access token's outer "act" claim. If an "act" claim is not present in the access token to be exchanged, the AS MUST add a nested "act" claim containing a "sub" claim with the identity of the client that presented the access token to be exchanged to PR1 (found in the access token's "client_id" claim) and an "iss" claim identifying the AS..

Informative examples of "act" contents within issued access tokens are as follows.

If an "act" claim is present in the access token to be exchanged:

```
{
  ...
  "act":
  {
    "sub":"PR1",
    "iss":"AS1",
    "act":
    {
      "sub":"[client_id2]",
      "iss":"AS1",
      "act":
      {
        "sub":"[client_id1]",
        "iss":"AS1"
```

```
      }
    }
  }
}
```

If an "act" claim is not present in the access token to be exchanged:

```
{
  ...
  "act":
  {
    "sub":"PR1",
    "iss":"AS1",
    "act":
    {
      "sub":"[client_id from access token to be exchanged]",
      "iss":"AS1"
    }
  }
}
```

The authorization server, when complying with this profile, MUST set the fields of successful token exchange responses as follows:

access_token	REQUIRED	Value set to the access token issued in response to the token exchange request. Note the requirements above on the contents of the access token. Requirement to include this field is per [RFC8693]; requirement to set it to an access token is per this profile.
issued_token_type	REQUIRED	Value set to "urn:ietf:params:oauth:token-type:access_token". Requirement to include this field is per [RFC8693]; requirement to set it to the particular value is per this profile.
token_type	REQUIRED	Value set to “Bearer”. Even though the issued access token must be sender constrained per [RFC8705], the RFC does not define a distinct OAuth Access Token Type in the Internet Assigned Numbers Authority (IANA) registry.

		Requirement to include this field is per [RFC8693]; requirement to set it to "Bearer" is per this profile.
expires_in	RECOMMENDED	As specified by [RFC8693].
scope	OPTIONAL or REQUIRED depending upon request	As specified by [RFC8693], this field is OPTIONAL if the scope is identical to the scope in the request; otherwise, this field is REQUIRED. It is acceptable for this field to be either omitted or set to an empty value if it was not present in the request or was set to an empty value in the request and is not present or is empty in the issued access token.
refresh_token	NOT ALLOWED	Token exchange pursuant to this profile cannot be used to obtain refresh tokens. If the issued access token expires and a new access token is needed, another token exchange can be performed. Expiration times in access tokens issued from a token exchange can be lengthened when necessary to minimize the need to obtain new access tokens. Future guidance may be provided on obtaining refresh tokens if warranted. This field is OPTIONAL in [RFC8693] and per this profile is NOT ALLOWED.

3.1 Example Protocol Interactions

This section is non-normative and provides examples of protocol interactions involving token exchange. These steps occur after the client obtains an access token for use at PR1.

1. Request from Client to PR1 with access token Token1 (Step 6 in Figure 1):

```
GET /resource_PR1 HTTP/1.1
Host: rs1.example.com
Authorization: Bearer [client-to-PR1-access-token]
```

2. Token Exchange request from PR1 to the authorization server (Step 7 in Figure 1):

(Request must be sent over a mutually authenticated TLS connection, with PR1 using its PKI certificate to authenticate itself to the authorization server.)

```
POST /as/token.oauth2 HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Atoken-
exchange&client_id=[PR1's client_id]&audience=[PR2]
&requested_token_type=urn%3Aietf%3Aparams%3Aoauth%3Atoken-
type%3Aaccess_token&subject_token=[client-to-PR1-access-token]
&subject_token_type=urn%3Aietf%3Aparams%3Aoauth%3Atoken-
type%3Aaccess_token
```

3. Successful token exchange response from the authorization server to PR1 (Step 7 in Figure 1):

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

{
"access_token":"[PR1-to-PR2-access-token]",
"issued_token_type":"urn:ietf:params:oauth:token-
type:access_token",
"token_type":"Bearer",
"expires_in":60
}
```

4. Data request from PR1 to PR2 (Step 8 in Figure 1):
(Request must be sent over a mutually authenticated TLS connection, with PR2 using its PKI certificate to authenticate itself to PR2.)

```
GET /resource_PR2 HTTP/1.1
Host: rs2.example.com
Authorization: Bearer [PR1-to-PR2-access-token]
```

4 Security Rationale for Profile Requirements

This section is intended to provide the rationale behind the requirements in this profile to help the reader understand the reason(s) certain decisions were made.

This profile requires that the token being exchanged must contain an "aud" field, and it must identify PR1 (the entity exchanging the token). This ensures that PR1 is the intended recipient of an access token in order to exchange it for another access token. This requirement is intended to

prevent stolen access tokens from being exchanged for new access tokens by an unauthorized entity. [RFC8693] does not contain this explicit requirement.

This profile requires that access tokens obtained through token exchange must identify the entire chain of clients and protected resources that held previously exchanged access tokens. The newly issued access token must contain an "act" claim that identifies the protected resource that exchanged the token, the client that sent the token to the protected resource, and any other entities involved in exchanges of other access tokens in the chain. This enables the protected resource consuming the access token to, if desired, look up authorizations or privileges associated with each entity in the chain as part of deciding what access to allow. The access tokens can still include specific authorization information (e.g. in its scope claim, resource claim, or other environment-specific claim) that protected resources could use instead of or in addition to the chain information. [RFC8693] defines the "act" claim but does not explicitly require its use.

5 Normative Reference

[RFC6749]	Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", IETF RFC 6749, October 2012, <http://www.rfc-editor.org/info/rfc6749>.
[RFC7662]	Richer, J., Ed., “OAuth 2.0 Token Introspection”, IETF RFC 7662, October 2015, <http://www.rfc-editor.org/info/rfc7662>.
[RFC8693]	M. Jones, A. Nadalin, B. Campbell, J. Bradley, and C. Mortimore, "OAuth 2.0 Token Exchange”, IETF RFC 8693, January 2020, <https://tools.ietf.org/html/rfc8693>.
[RFC8705]	B. Campbell, J. Bradley, N. Sakimura, and T. Lodderstedt, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens", IETF RFC 8705, February 2020, <https://tools.ietf.org/html/rfc8705>.
[OIDC-Core]	OpenID Foundation. "OpenID Connect Core 1.0 incorporating errata set 1”, November 2014, <https://openid.net/specs/openid-connect-core-1_0.html>.

6 Informative Reference

[OAuth-Profile]	B. Abramowitz et al., "Enterprise Mission Tailored OAuth 2.0 Profile.", The MITRE Corporation, February 2020, <https://www.mitre.org/sites/default/files/publications/pr_19-3213_enterprise_tailored_oauth_profile.pdf>.
[Token-Chaining2]	B. Abramowitz, et al. "Token and Identity Chaining Between OAuth Protected Resources in a Multiple ICAM Ecosystem using OAuth Token Exchange.”, Draft.

Appendix A Acronyms

AS	Authorization Server
IANA	Internet Assigned Numbers Authority
ICAM	Identity, Credential, and Access Management
IETF	Internet Engineering Task Force
PKI	Public Key Infrastructure
PR1	The protected resource initiating the token exchange protocol
PR2	The protected resource containing the data requested by the client
RFC	Request For Comments
TLS	Transport Layer Security
Claims	
act	actor
aud	audience
cnf	confirmation
exp	expiration time
iss	issuer