

Backbase

New and Noteworthy in the OAuth World

The Engagement Banking Platform

re-architecting banking around the customer



Leader

FORRESTER® OMDIA

Partner

Microsoft Deloitte. Digital

Experienced

In all lines of business

Trusted by 150+ leading financial institutions

KeyBank 

 BPI

 Discovery

HSBC 

 MCB

 BankUnited

 NAVY FEDERAL
Credit Union

 BRD
GROUPE SOCIETE GENERALE

Goldman Sachs

RAIFFEISEN

 Rabobank

 NBB

State Employees' Credit Union


BKS Bank

Aldermore

VOLKSWAGEN
FINANCIAL SERVICES

 BANQUE DE
LUXEMBOURG

LLOYDS
BANKING
GROUP 

pbb
DEUTSCHE
PFANDBRIEFBANK

 BNP PARIBAS

Deutsche Bank 

WSECU

 Citizens Bank®

 Íslandsbanki

 HDFC BANK

 HISCOX

 Virgin money

200+

Successful projects

17

Offices in the world

2000+

Employees, with over 50% in R&D

Dmitry Telegin



Principal Backend Engineer at Backbase UK



Independent Keycloak expert / consultant / trainer, contributor and SIG member



IETF Contributor



<https://www.linkedin.com/in/d-telegin/>

Agenda

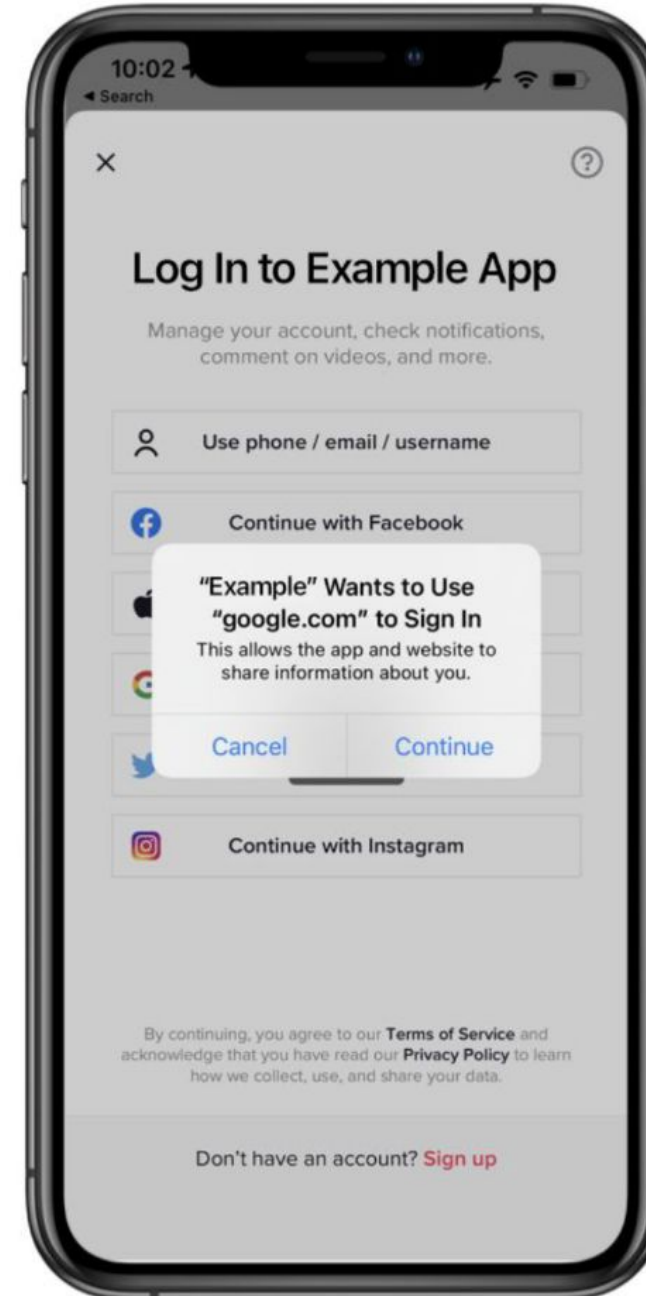
- 1. OAuth 2.0 for First-Party Applications**
- 2. Transaction Tokens**
- 3. Identity and Authorization Chaining Across Domains**
- 4. Client ID Metadata Document**

OAuth 2.0 for First-Party Applications

OAuth 2.0 for First-Party Applications

Why?

Developers want a better user experience for first-party apps



■ OAuth 2.0 for First-Party Applications

What is happening today

People are finding workarounds to avoid RFC8252:

- Custom DIY solutions for native apps
- Using Resource Owner Password Grant
 - (Unable to add MFA)
- OAuth servers creating proprietary APIs to facilitate direct interaction with native apps
- Scripting hidden web views to emulate user interaction with the AS
- (Ab)using Authorization Endpoint with programmatic calls and JSON

■ OAuth 2.0 for First-Party Applications

Goals

- Reuse existing OAuth building blocks as much as possible
- Mirror the web authorization code flow, defining how the client starts and ends the flow
 - Leave the specifics of the user authentication out of the core framework
- Specifics of user authentication can be proprietary to an AS as they are today, or can be defined as extensions
 - Especially if based on standards like FIDO

OAuth 2.0 for First-Party Applications

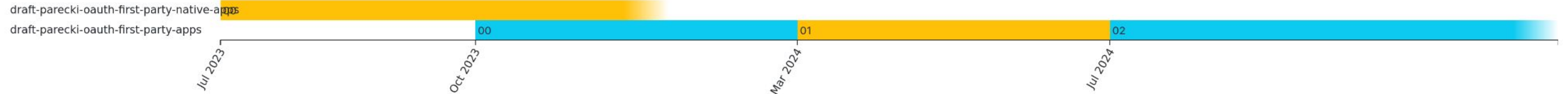
OAuth 2.0 for First-Party Applications draft-parecki-oauth-first-party-apps-02

Status [Email expansions](#) [History](#)

Versions:

[00](#) [01](#) [02](#)

This document is an Internet-Draft (I-D). Anyone may submit an I-D to the IETF. This I-D is **not endorsed by the IETF** and has **no formal standing** in the [IETF standards process](#).



Document	Type	Active Internet-Draft (individual)
	Authors	Aaron Parecki ✉, George Fletcher ✉, Pieter Kasselmann ✉
	Last updated	2024-07-08
	Replaces	draft-parecki-oauth-first-party-native-apps
	RFC stream	(None)
	Intended RFC status	(None)

Link: <https://datatracker.ietf.org/doc/draft-parecki-oauth-first-party-apps/>

Status: **Call for adoption**

OAuth 2.0 for First-Party Applications

Authorization Challenge Endpoint

- New endpoint
 - Accepts parameters that would have been included in the query string to the authorization endpoint
 - including any extensions such as Resource Indicators, OpenID Connect, JAR, etc
- Accepts POST from client to start and continue an authorization
 - The AS defines what the client sends in the requests and defines its own error responses
- Response is an authorization code, error, or redirect
 - The AS may want to interact with the user directly, e.g. based on risk assessment, new authentication method not implemented in the app, or exceptions like account recovery

■ OAuth 2.0 for First-Party Applications

Authorization Challenge Endpoint

Why a new endpoint?

- Existing authorization endpoint is never interacted with by the OAuth client today, only by the browser
- It expects to receive requests from a User Agent, and return HTML
- Feedback has indicated people are unwilling to modify their existing authorization endpoint to accept a direct POST from a client and return JSON
 - CORS at Authorization Endpoint is prohibited by Security BCP

OAuth 2.0 for First-Party Applications

The Protocol

```
> POST /as/challenge HTTP/1.1
> Content-Type: application/x-www-form-urlencoded
>
> login_hint=%2B1-310-123-4567&scope=profile&client_id=bb16c14c73415

< HTTP/1.1 400 Bad Request
< Content-Type: application/json
< {
<   "error": "insufficient_authorization"
< }
```



```
< HTTP/1.1 200 OK
< Content-Type: application/json
< Cache-Control: no-store
< {
<   "authorization_code": "uY29tL2F1dGh1bnRpY"
< }
```

■ OAuth 2.0 for First-Party Applications

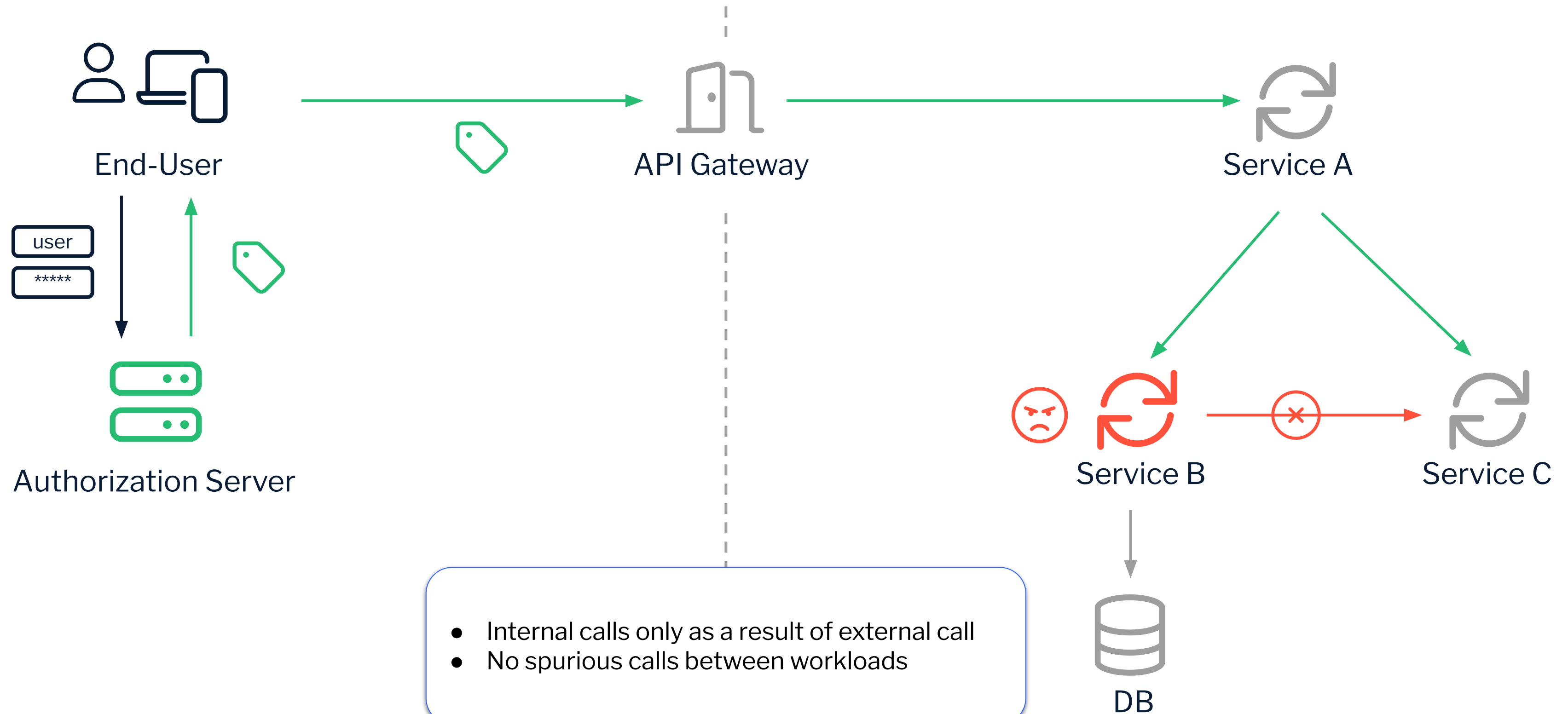
The Keycloak perspective

- Prototype exists (thanks Martin Besozzi)
- Challenge endpoint
 - Moving more code to base class
 - Token Endpoint not affected
- The Back-and-Forth
- Native equivalents for the built-in flows
- Backward compatibility with existing authenticators

Transaction Tokens

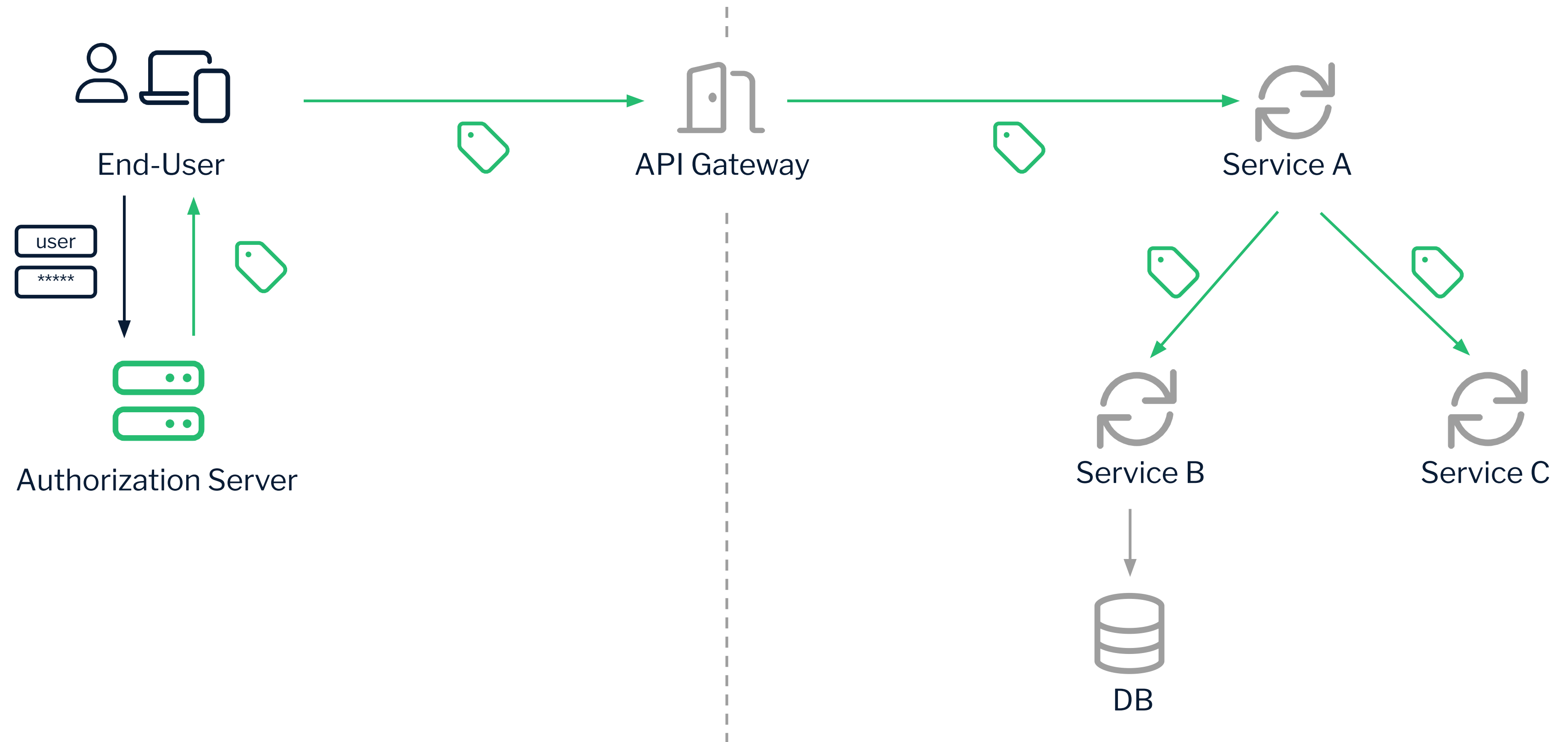
Transaction Tokens

Welcome to the Zero Trust World



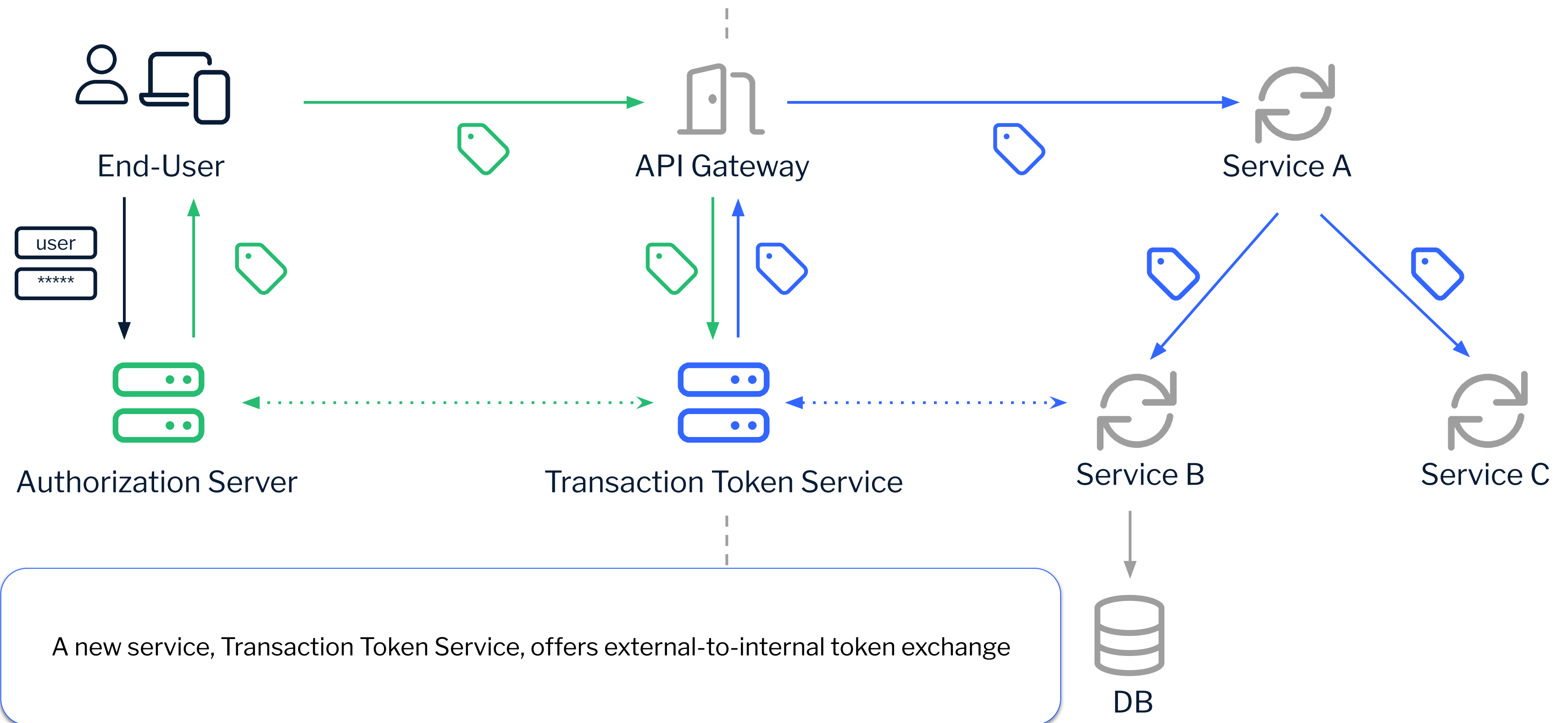
Transaction Tokens

The Naive Approach: Access Token Propagation



Transaction Tokens

A Better Approach: Transaction Token Service



Transaction Tokens

The Document

IETF Datatracker Groups Documents Meetings Other User [Report a bug](#) [Sign in](#)

Transaction Tokens

draft-ietf-oauth-transaction-tokens-03

Status: IESG evaluation record | [IESG writeups](#) | [Email expansions](#) | [History](#)

Versions: 00 | 01 | 02 | 03

draft-oauth-transaction-tokens 00

draft-ietf-oauth-transaction-tokens 00 01 02 03

Nov 2023 Mar 2024 Jun 2024 Jul 2024

Document	Type	Active Internet-Draft (oauth WG)
	Authors	Atul Tulshibagwale ✉, George Fletcher ✉, Pieter Kasselmann ✉
	Last updated	2024-07-03
	Replaces	draft-oauth-transaction-tokens
	RFC stream	Internet Engineering Task Force (IETF)
	Intended RFC status	(None)
	Formats	txt html xml htmlized bibtex bibxml
	Additional resources	Mailing list discussion

Link: <https://datatracker.ietf.org/doc/draft-ietf-oauth-transaction-tokens/>

Status: **Adopted (Active Internet-Draft)**

Transaction Tokens

Features

- Token internal to a given trust boundary
- Maintains the immutable context of a Transaction
 - Subject
 - Context
 - Authorization Details
- Shared across multiple workloads
- Allows for “down-scoping” a transaction at the edge
- Supports finer-grained authorization
- Built on top of OAuth 2.0 (RFC 6749), Token Exchange (RFC 8693) and JSON Web Token (RFC 7519)

Transaction Tokens

The Token

Example: transaction token body

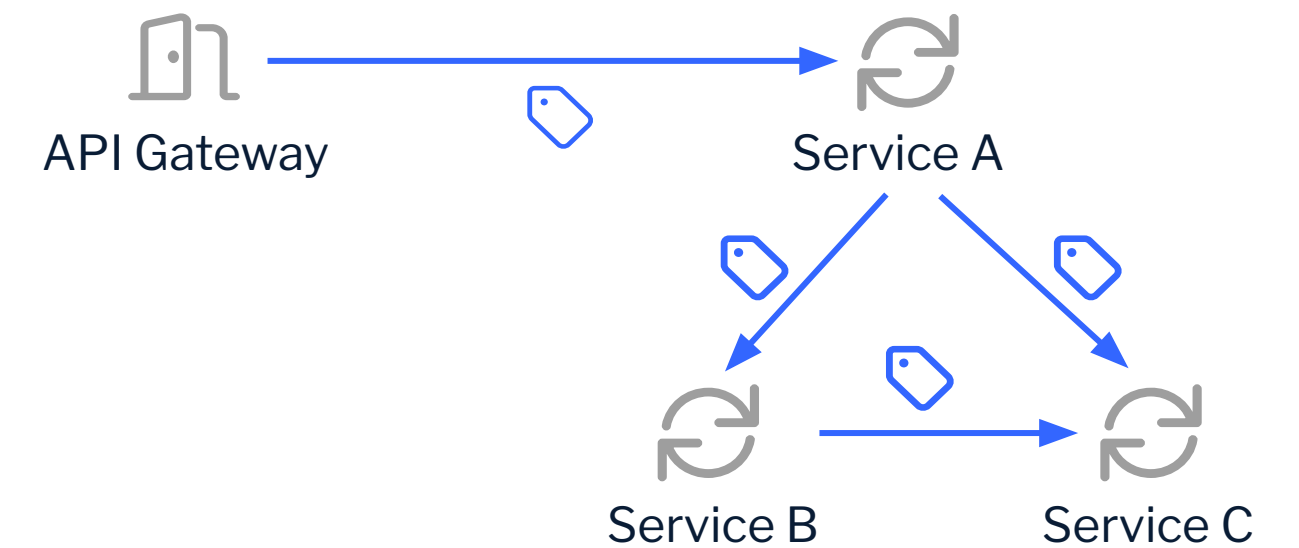
```
{
  "iat": "1686536226000",
  "aud": "trust-domain.example",
  "exp": "1686536526000",
  "txn": "97053963-771d-49cc-a4e3-20aad399c312",
  "sub": "d084sdrt234fsaw34tr23t",
  "rctx": {
    "req_ip": "69.151.72.123", // env context of external call
    "authn": "urn:ietf:rfc:6749", // env context of the external call
    "req_wl": "apigateway.trust-domain.example" // the internal entity that requested the Txn-Token
  },
  "purp": "trade.stocks",
  "azd": {
    "action": "BUY", // parameter of external call
    "ticker": "MSFT", // parameter of external call
    "quantity": "100", // parameter of external call
    "user_level": "vip" // computed value not present in external call
  }
}
```


Transaction Tokens

The Use

Example: transaction token use

```
> GET /workload/api/foo HTTP 1.1
> Host: workload-a.trust-domain.example
> Txn-Token: eyJCI6IjllciJ9...Qedw6rx
< HTTP/1.1 200 OK
```



Transaction Tokens

The Keycloak perspective

Presentation: “Securing Workloads with Transaction Tokens and Minicloak” @ Open Source Summit 2024

Keycloak TTS: <https://github.com/dteleguin/keycloak-tts>

Keycloak TTS Demo: <https://github.com/dteleguin/tts-demo>

- Token Exchange
 - Custom Token Exchange Provider
 - Relax client_id requirement
 - Promote to stable
- ? SPIFFE/WIMSE integration - obtaining WL ID
- ? Trusted Party

OAuth Identity and Authorization Chaining Across Domains

OAuth Identity and Authorization Chaining Across Domains

Why Identity Chaining Across Trust Domains

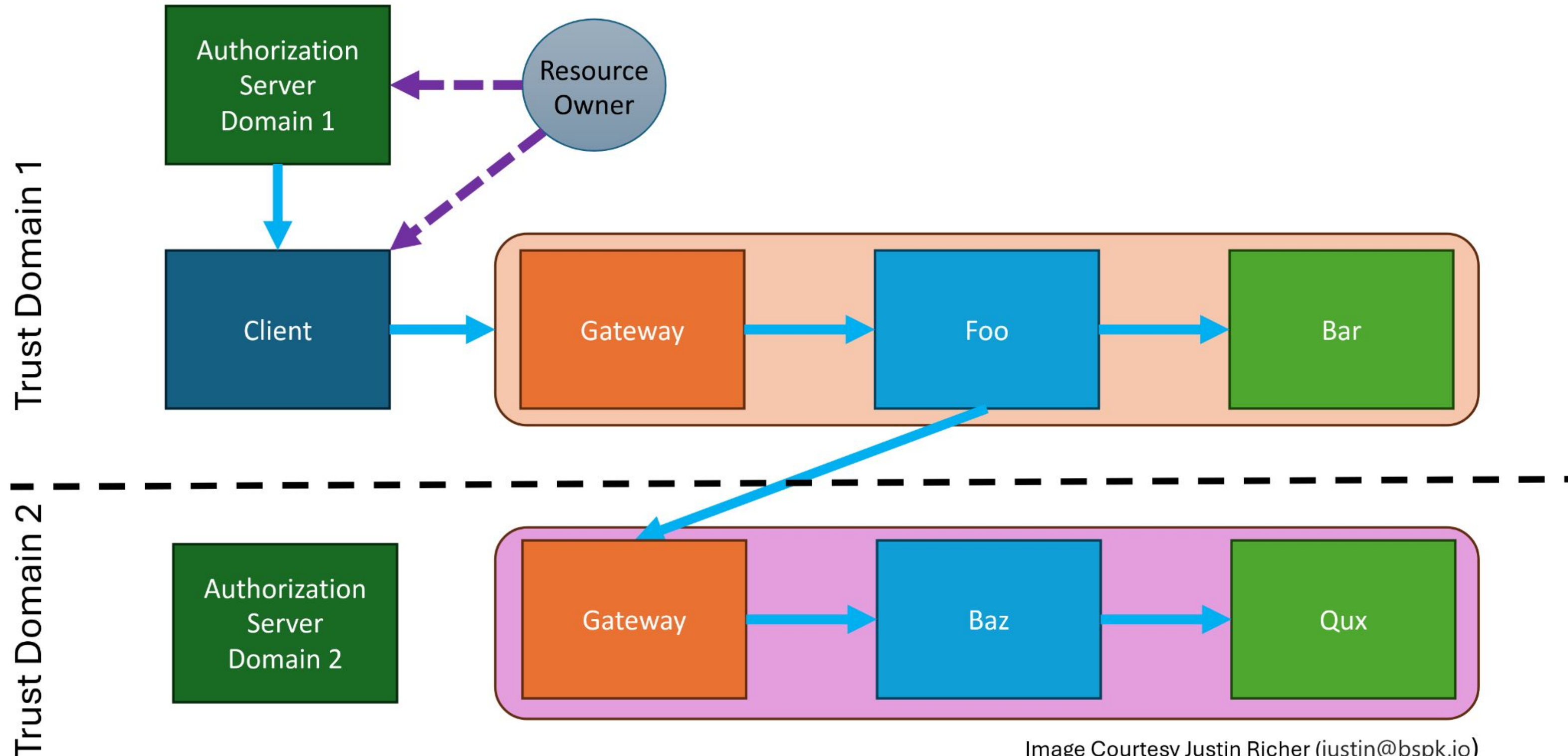
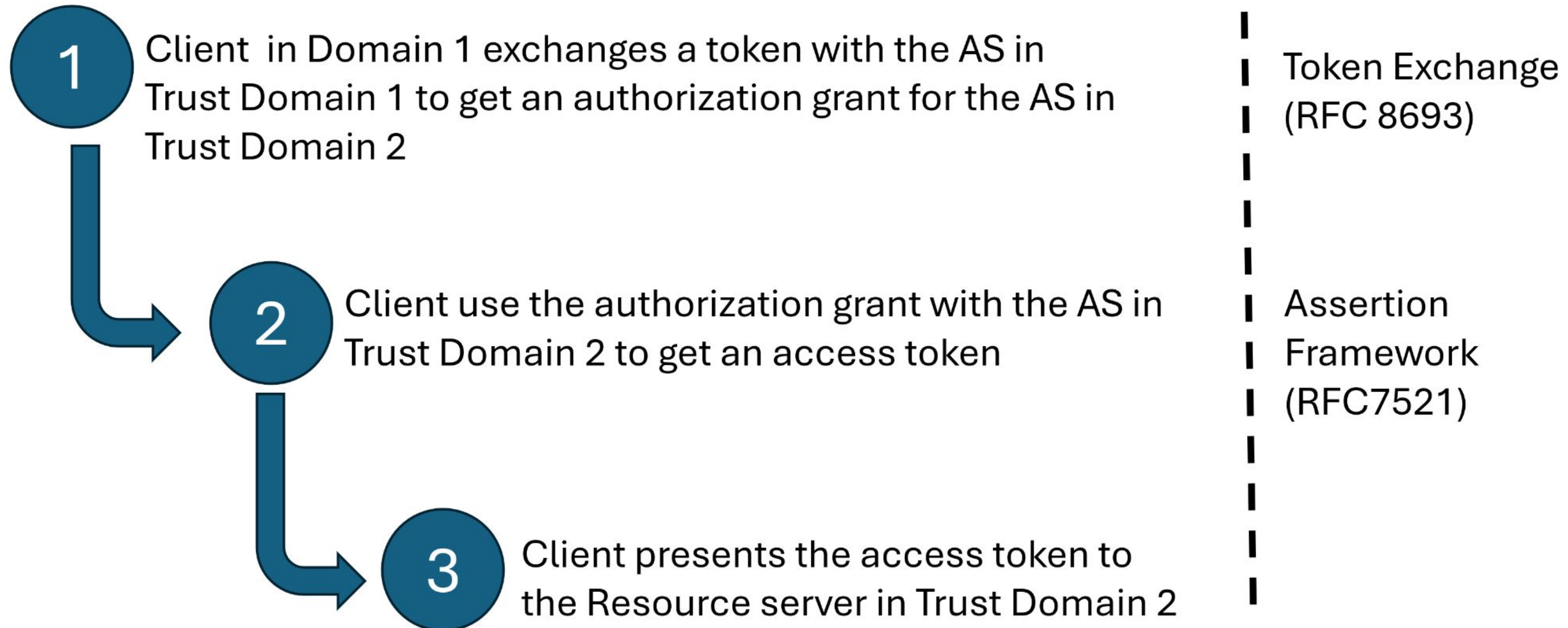


Image Courtesy Justin Richer (justin@bspk.io)

OAuth Identity and Authorization Chaining Across Domains

Getting an Authorization Grant for another Trust Domain



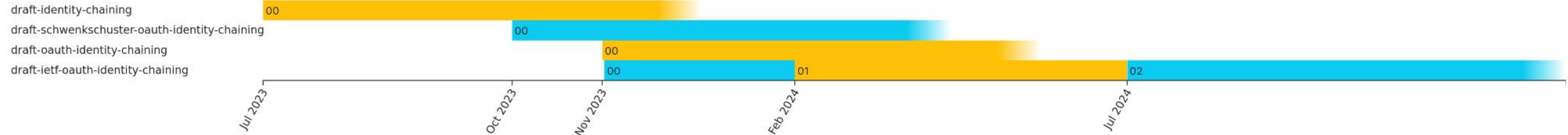
OAuth Identity and Authorization Chaining Across Domains

OAuth Identity and Authorization Chaining Across Domains draft-ietf-oauth-identity-chaining-02

Status IESG evaluation record IESG writeups Email expansions History

Versions:

00 01 02



Document	Type	Active Internet-Draft (oauth WG)
	Authors	Arndt Schwenkschuster ✉, Pieter Kasselmann ✉, Kelley Burgin ✉, Michael J. Jenkins ✉, Brian Campbell ✉
	Last updated	2024-07-08
	Replaces	draft-oauth-identity-chaining
	RFC stream	Internet Engineering Task Force (IETF)
	Intended RFC status	(None)

Link: <https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-chaining/>




Status: **Adopted (Active Internet-Draft)**

Complimentary draft: Identity Assertion Authorization Grant aka ID-JAG (Individual)

Link: <https://datatracker.ietf.org/doc/draft-parecki-oauth-identity-assertion-authz-grant/>

OAuth Identity and Authorization Chaining Across Domains

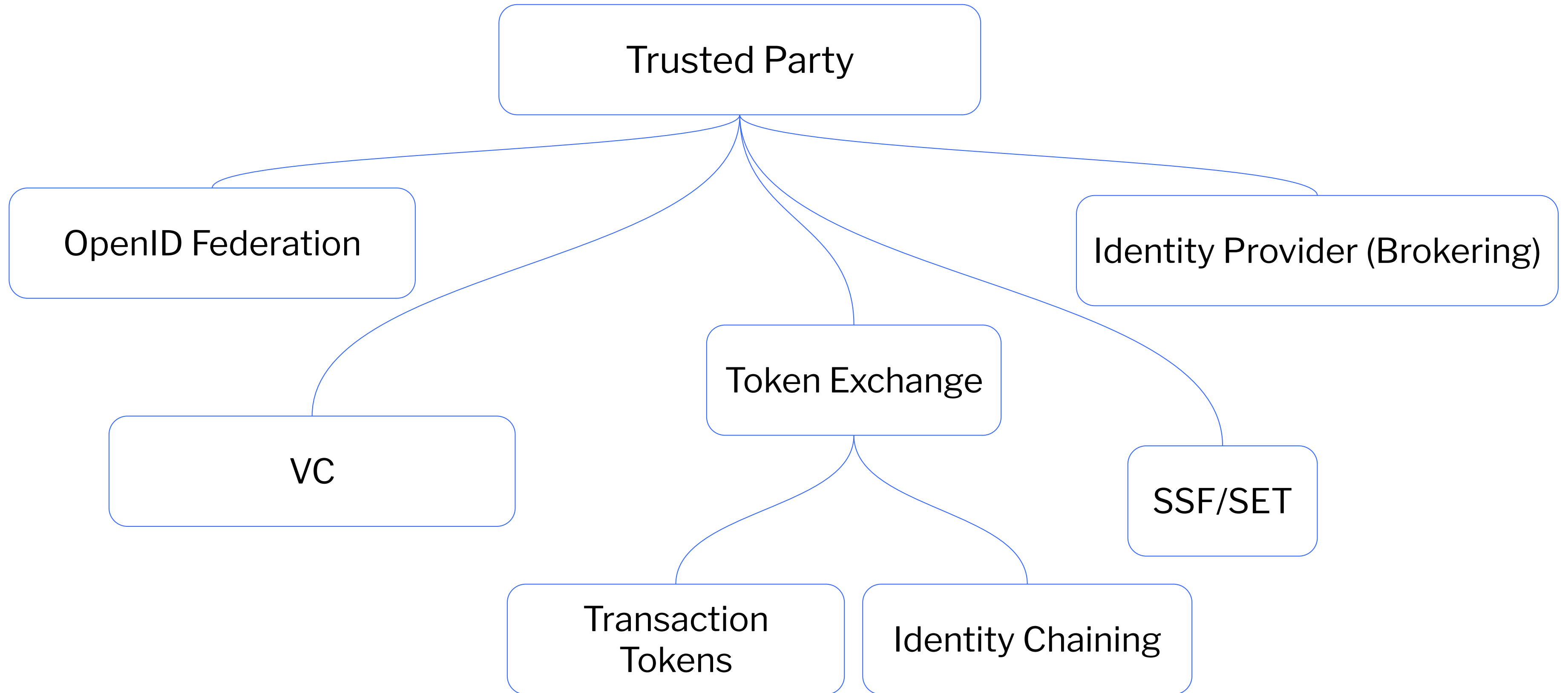
The Keycloak perspective

- Source:
 -  Custom Token Exchange Provider
- Target:
 -  JWT Assertion Grant ([#24509](#))
-  Trusted Party

Trusted Party

Identity Provider

Trusted Party



Client ID Metadata Document

Client ID Metadata Document

Static/dynamic client registration

```
POST /as/authorize HTTP/1.1
Content-Type: application/x-www-form-urlencoded

redirect_uri=...&response_mode=...&client_id=bb16c14c73415
```

Client ID Metadata Document

Automatic client registration

```
POST /as/authorize HTTP/1.1
Content-Type: application/x-www-form-urlencoded

redirect_uri=...&response_mode=...&client_id=https://app.example/id
```

```
GET https://app.example/id HTTP/1.1
Content-Type: application/json

{
  "client_id": "https://app.example/id",
  "client_name": "Solid Application Name",
  "redirect_uris": ["https://app.example/callback"],
  "post_logout_redirect_uris": ["https://app.example/logout"],
  "client_uri": "https://app.example/",
  "logo_uri": "https://app.example/logo.png",
  "tos_uri": "https://app.example/tos.html",
  "scope": "openid profile offline_access webid",
  "grant_types": ["refresh_token", "authorization_code"],
  "response_types": ["code"],
  "default_max_age": 3600,
  "require_auth_time": true
}
```

Client ID Metadata Document

Automatic client registration

Used by:

- OpenID Federation
- Solid-OIDC
- IndieAuth
- ...

Client ID Metadata Document

OAuth Client ID Metadata Document

draft-parecki-oauth-client-id-metadata-document-01

Status [Email expansions](#) [History](#)

Versions:

00 01

This document is an Internet-Draft (I-D). Anyone may submit an I-D to the IETF. This I-D is **not endorsed by the IETF** and has **no formal standing** in the [IETF standards process](#).

draft-parecki-oauth-client-id-metadata-document-00 01

Jul 2024

Document	Type	Active Internet-Draft (individual)
	Authors	Aaron Parecki ✉, Emelia Smith ✉
	Last updated	2024-07-08
	RFC stream	(None)
	Intended RFC status	(None)

Link: <https://datatracker.ietf.org/doc/draft-parecki-oauth-client-id-metadata-document/>

Status: **Individual Internet-Draft**

Client ID Metadata Document

The Keycloak perspective

- ? Client Policy
 - ✓ PreAuthorization
- Metadata retrieval and caching
 - Overlap with Trusted Party
 - ? Document storage

Q&A

Thank You!