Internet-Draft   M. Fulz
Intended status: Standards Track   Independent
Expires: May 31, 2026   November 27, 2025

OAuth Trust Binding Extension (OTBE)
draft-fulz-oauth-trust-binding-00

Abstract

This document defines the OAuth Trust Binding Extension (OTBE), a mechanism allowing Resource Owners to explicitly authorize which Authorization Servers may assert their identity towards Relying Parties, mitigating silent impersonation and namespace-based identity capture.

RFC 2119 / RFC 8174 Language

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 and RFC 8174 when, and only when, they appear in all capitals.

1. Introduction

OAuth 2.0 and OpenID Connect are widely deployed for delegated authorization and federated identity. A fundamental, often implicit assumption is that the Authorization Server (AS) and the Resource

Owner (RO) share an established trust relationship before any authorization request is made.

In practice, the current ecosystem assigns implicit trust based solely on possession of an identifier, typically an email address. This creates critical vulnerabilities where:

* any Authorization Server hosting an identity namespace (e.g., *@gmail.com*) can impersonate users who never created an account with that AS;

* Relying Parties (clients) accept identities without any ability to verify whether the RO intentionally approved OAuth-based login for that AS;

* large IdPs (Google, Facebook) gain unilateral access to potentially all RP accounts linked by email identifiers alone.

This document introduces the OAuth Trust Binding Extension (OTBE), a mechanism enabling explicit user-controlled trust binding between an identity namespace and an Authorization Server.

2. Problem Statement

Current OAuth deployments allow the AS to assert identity ownership solely on the basis of email-domain control. This leads to:

2.1. Silent Impersonation Risk

A user who owns "user@example.com" may have no account at Google, but if an RP accepts "Sign in with Google", Google can legitimately assert that identity, creating:

* account takeover potential,

* unobservable impersonation,

* unilateral trust decisions by third parties.

2.2. No User-Driven Consent to Provider-Level Trust

There is currently no mechanism for a user to declare:

> "I trust AS X to authenticate me for RP Y (or globally)."

Instead, trust is assumed, not expressed.

2.3. Centralization and Surveillance Risks

This implicit trust model enables concentrated identity control in dominant AS entities. Under legal compulsion, such providers could impersonate users across the entire ecosystem.

2.4. Namespace Capture

Email domain providers become de facto identity authorities even when users have no intention of delegating authentication to them.

OTBE resolves these issues by introducing explicit Trust Binding Records controlled by the Resource Owner.

3. Terminology

AS

Authorization Server.

RO

Resource Owner (end-user).

RP

Relying Party (Client).

Trust Binding (TB)

A cryptographic or secret-binding record that authorizes a particular AS to authenticate the RO’s identifier.

TB-Record

The stored representation of a Trust Binding at an RP.

4. Protocol Overview

OTBE extends OAuth as follows:

1. Before an RP accepts a login from an AS for identifier "user@example.com", it MUST verify that a Trust Binding exists.

2. Trust Bindings are simple key-value artifacts:

   * either user-generated secrets,

   * or AS-provided cryptographic attestations.

3. Trust Bindings are created by the user, either:

   * manually (copy/paste token),

   * during an enrollment flow,

   * or via a federated mechanism provided by the identity namespace owner.

4. Without a valid Trust Binding, authentication MUST fail.

5. Trust-Binding Registration

5.1. Creating a Trust Binding

An RO creates a random secret or receives a cryptographic token from the AS. Examples:

```
TB-Token = base64url(random(256 bits))
```

5.2. Binding the Token to the RP

The RO stores the TB-Token at the RP during a special "Enable External Login" step:

1. RO authenticates with the RP using primary credentials.

2. RO selects "Enable login with AS X".

3. RP displays a TB-Token (or asks RO to paste one).

4. RP stores: { identifier, AS, TB-Token }.

6. Authorization Flow Modifications

During OAuth login:

1. AS sends authorization assertion to RP.

2. RP extracts RO identifier and AS identity.

3. RP retrieves the stored TB-Token.

4. RP computes verification:

   * If AS supplies a signed TB-Token, RP validates the signature.

   * If AS only supplies identifier, AS must also echo the TB-Token (via standard or extension claim).

5. If no valid TB-Token is presented, RP returns an error such as:

   error = "trust_binding_missing"

7. Security Considerations

* Prevents silent impersonation by AS.

* Reduces impact of AS compromise.

* Prevents surveillance-based identity impersonation.

* Ensures user agency in RPAS trust relationships.

* TB failure forces RP to reject unexpected logins.

8. Privacy Considerations

* OTBE eliminates automatic identity leakage to AS because RPs will no longer accept unsolicited authentication attempts.

* TB-Tokens must be stored securely and treated as secrets.

9. Backward Compatibility

* RPs may operate in compatibility mode where legacy logins still function.

* Deployment SHOULD prefer a "progressive enforcement" model.

10. Deployment Considerations

* Can be implemented without changes to OAuth core specifications.

* AS vendors may gradually adopt TB-token signing for stronger assurances.

* RPs must update user-account-management UIs to allow TB setup.

11. IANA Considerations

This draft requests registration of:

* "trust_binding_token" — OAuth extension claim.

* "trust_binding_required" — OAuth error code.

12. Appendix A — Examples

12.1. Example TB-Record


```
{
  "subject": "user@example.com",
  "as": "https://accounts.example-idp.com",
  "tb": "zY9sD2..."
}
```


13. Appendix B — Threat Model

13.1. Addressed threats

* AS-driven impersonation.

* Government-compelled impersonation.

* Namespace hijacking.

* Centralized identity coercion.

13.2. Out of scope

* Phishing.

* RP credentials compromise.

Authors' Addresses

Matthias Fulz
Independent
Ingolstadt
Germany

Email: mfulz@olznet.de