Network Working Group
Internet-Draft
Intended status: Informational
Expires: 9 February 2026

S. Bou Aram, Ed.

August 2025

OpenID Connect Email Account Linking Extension
draft-bouaram-oidc-email-linking-extension-00

Abstract

This document extends OpenID Connect’s standard email functionality to support secure linking between multiple email accounts. It enables users to associate secondary email addresses with their primary account while maintaining backward compatibility with existing implementations. The extension provides methods for establishing, managing, and utilizing these relationships within the OpenID Connect email scope.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 February 2026.

Table of Contents

1. Core Concepts

The extension operates on these fundamental principles:

1. *Primary Account*: The initial identity that controls all linked accounts

2. *Secondary Accounts*: Additional email identities linked to the primary

3. *Temporal Validity*: Linkages expire after a defined period

4. *Account Resolution*: Secondary logins resolve to the primary identity

2. Protocol Parameters

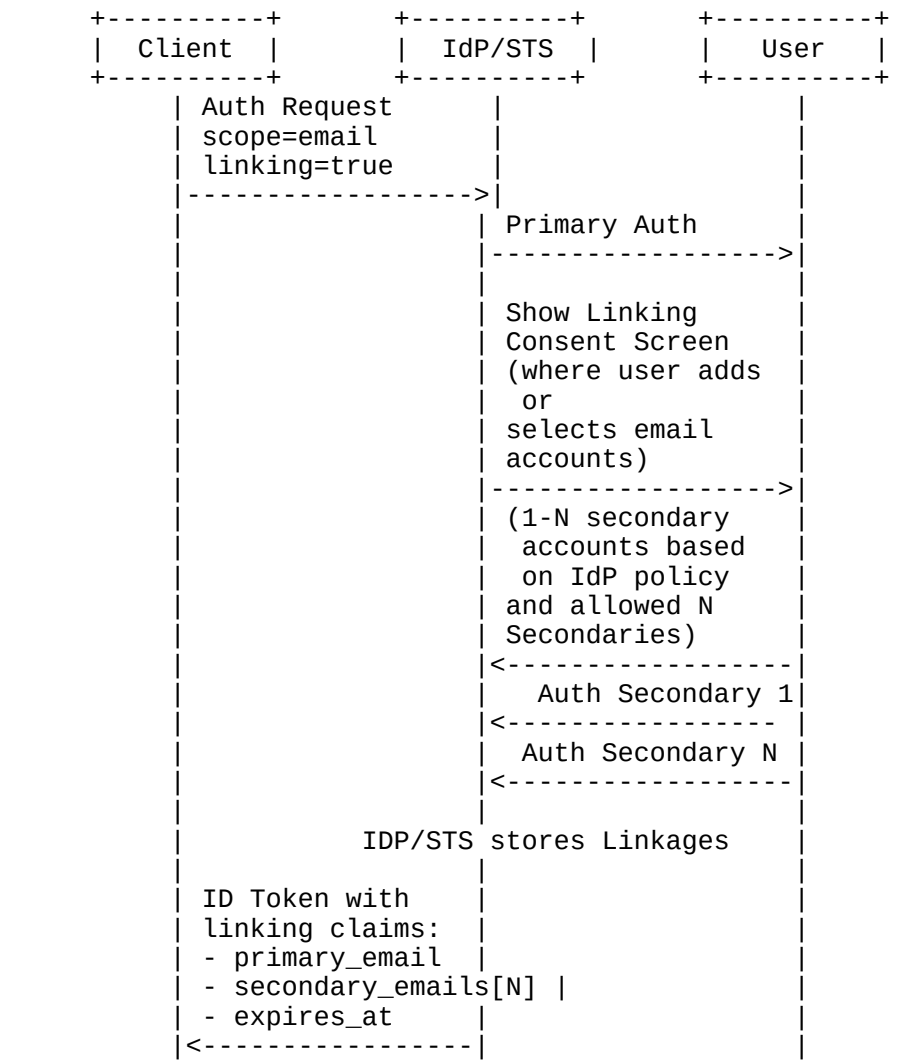
Parameter	Location	Description
linking	Authorization Request	boolean (true/false), initiates linking flow when true
linking_period	Authorization Request	number (seconds), validity duration (default: 2592000)

Table 1: Parameters

3. Protocol Flows

3.1. Linking Flow

Complete sequence for establishing account linkages:



1. Client initiates with parameters:

```
GET /authorize?response_type=code
  &client_id=client123
  &scope=openid%20email
  &linking=true
  &linking_period=604800
```

2. IdP authenticates primary account, the account should be primary or normal (not linked) email account

3. User authenticates 1-N secondary accounts (IdP-defined limit)

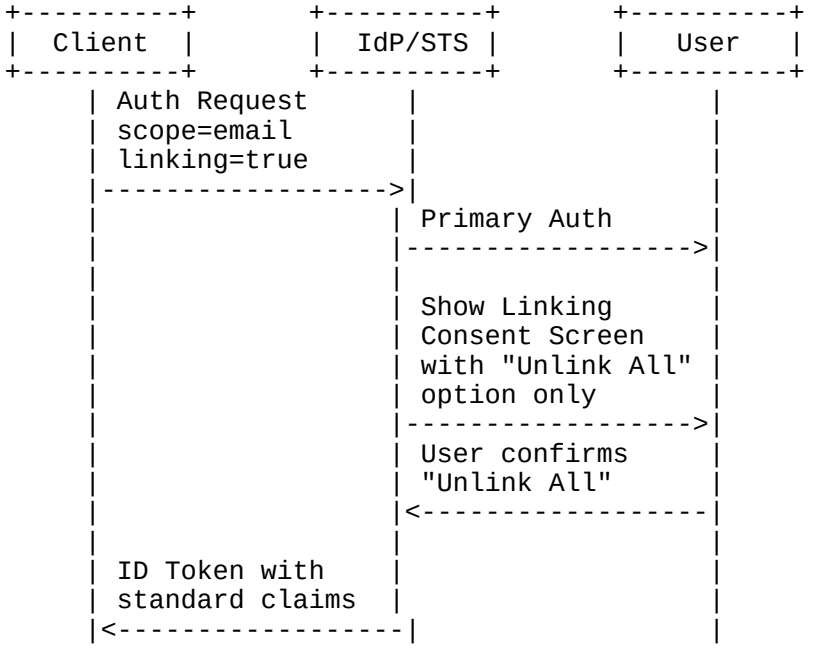
4. IdP stores linkages with desired expiration timestamp

5. IdP returns ID token containing:

```
{
  "email": "main@example.com",
  "primary": true,
  "linking": {
    "secondary_emails": ["alt1@example.com", "alt2@example.org"],
    "expires_at": 1735689600
  }
}
```

3.2. Unlinking Flow

Unlinking occurs through the standard linking interface when initiated by primary accounts:



1. User authenticates with primary account credentials

2. IdP displays linking consent screen with:

* List of currently linked accounts

* Single "Unlink All" option

* No account selection options

3. User confirms by clicking "Unlink All"

4. IdP completely removes all linkages

5. Standard ID token returned with empty linkage:

```
{
  "email": "main@example.com",
  "linking": {}
}
```

3.3. Secondary Account Authentication

When authenticating with an email account that is linked to a primary account:

1. Client initiates standard OIDC authentication:

```
GET /authorize?response_type=code
  &client_id=client123
  &scope=openid%20email
```

2. IdP/STS performs normal authentication flow

3. After successful authentication, system checks for account linkages

4. For secondary accounts, ID token contains:

```
{
  "email": "secondary@example.com",
  "linking": {
    "is_primary": false,
    "primary_email": "main@example.com",
    "expires_at": 1735689600
  }
}
```

Applications must process the token as follows:

* Use primary_email as the canonical user identifier

* Verify expires_at is in the future

* Treat permissions/access identical to primary account login

* Include secondary email in audit logs only

4. Security Considerations

Key security requirements:

1. *Authentication Requirements*:

    * All accounts must complete full authentication during linking

    * Secondary accounts cannot initiate linking/unlinking

2. *Token Validation*:

    * Linking expiry must always be validated

3. *Account Resolution*:

* Always resolve secondary logins to primary email account

4. *Audit Logging*:

* Log all linking/unlinking events

* Record both primary and secondary emails in logs

5. IANA Considerations

This document has no IANA actions.

Author’s Address

Salim BOU ARAM (editor)
Beirut
Lebanon
Email: salimbouaram12@gmail.com