Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 23 October 2026

D. Wiley

21 April 2026

Zero Trust Attribute Assertion Tokens
draft-wiley-ztaaat-00

Abstract

This document defines a mechanism for verifying boolean eligibility claims using cryptographically signed assertion tokens. A relying party can verify authoritative answers to predefined claims without trusting the presenting subject and without learning the subject's identity.

Each assertion token encodes exactly one boolean claim. The system guarantees authenticity and integrity of claim assertions. It does not provide identity, authentication, or subject uniqueness.

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 23 October 2026.

Copyright Notice

Table of Contents

1. Introduction

Many services require verification of user attributes rather than identity. Existing mechanisms frequently disclose unnecessary information and enable cross-service tracking.

This document specifies a zero-trust attribute assertion system in which:

* A relying party requests a single boolean claim.

* An issuer evaluates that claim.

* The issuer produces a signed assertion token.

* The subject presents the token to the relying party.

* The relying party verifies the token without contacting the issuer.

The subject is untrusted. All claim validity derives solely from the issuer’s signature.

2. Terminology

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals.

Subject:
An individual presenting an assertion token.

Issuer:
An authority capable of evaluating and asserting claims.

Relying Party (RP):
An entity requesting verification of claims.

Claim:
A boolean predicate defined by the issuer.

Assertion Token:
A cryptographically signed structure containing one claim result.

3. Privacy Model

3.1. Issuance and Presentation

Token issuance and token presentation are distinct phases.

During issuance, the issuer MAY verify subject identity using authoritative records. The issuer MAY learn that a token is being requested but MUST NOT learn the intended relying party.

During presentation, the relying party MAY learn that a subject is requesting access to a resource but MUST NOT learn the subject’s identity from the token.

The issuer MUST NOT observe token presentation.

3.2. Privacy Invariants

The following invariants are REQUIRED:

1. Assertion tokens MUST NOT contain identifiers, pseudonyms, or stable entropy.

2. Tokens intended for different relying parties MUST be unlinkable.

3. The issuer MUST NOT learn the intended relying party.

4. Tokens MUST reveal only the requested claim.

5. Tokens MUST NOT enable cross-service tracking.

4. Claim Model

4.1. Claim Registry

Claims MUST be defined in an issuer-controlled registry.

Claims:

* MUST be boolean
* MUST be coarse-grained
* MUST NOT encode identifying information

Example claims include:

* is_over_18
* is_us_citizen
* is_us_resident

4.2. Claim Restrictions

Each AssertionToken MUST encode exactly one claim result.

A relying party requiring multiple claims MUST obtain and verify separate tokens for each claim.

Relying parties MUST NOT request arbitrary claims outside the registry.

5. Assertion Token Format

```
AssertionToken = {
   claim: claim_name,
   value: boolean,
   exp: timestamp,
   aud: audience_value,
   iss: issuer_identifier,
   sig: signature
}
```

Field definitions:

claim:
: The requested boolean claim.

value:
: The asserted truth value.

exp:
: Expiration time.

aud:
: An opaque value bound to a single relying party. The value MUST be meaningful only to the relying party and MUST NOT reveal relying party identity to the issuer.

iss:
: Identifier of the issuer.

sig:
: Digital signature over all fields.

Requirements:

* Tokens MUST be audience-bound.

* Tokens MUST be unmodifiable.

* Tokens MUST NOT contain identifiers.

* The expiration time MUST be no more than 10 minutes after issuance.

6. Protocol

6.1. Claim Request

```
ClaimRequest = {
   claim: claim_name,
   audience: audience_value
}
```

The audience value MUST:

* be meaningful only to the relying party

* not reveal relying party identity to the issuer

* not be derivable by the issuer

6.2. Issuance

The issuer evaluates the requested claim and produces a signed assertion token.

The issuance process MUST prevent the issuer from learning the intended relying party.

The issuer MAY learn that a request occurred but MUST NOT learn the audience value.

6.3. Token Presentation

The subject provides the AssertionToken to the relying party.

6.4. Verification

The relying party MUST:

1. Verify the token signature using issuer verification material.

2. Verify expiration.

3. Verify that the audience value matches a relying-party-local value.

4. Apply relying-party replay policy.

5. Evaluate the claim.

Verification MUST NOT require real-time issuer interaction.

6.5. Issuer Trust

Relying parties MUST maintain a local trust configuration of accepted issuers.

Trust MUST be scoped per issuer and per claim. An issuer MUST NOT assert claims outside its authoritative domain.

7. Token Lifetime

Tokens MUST expire within 10 minutes of issuance.

Tokens MUST NOT be renewable.

8. Cryptographic Requirements

Assertion tokens MUST be digitally signed by the issuer.

A relying party MUST verify the issuer signature using trusted verification material.

Issuers MUST make verification material available through a trusted distribution mechanism.

This specification does not mandate specific cryptographic algorithms or key formats.

9. Security Considerations

The primary threat is unauthorized claim assertion.

This protocol mitigates:

* forgery through signature verification
* tampering through integrity checks
* cross-relying-party misuse through audience binding

Replay is handled by relying-party policy.

10. Trust Model

The subject is untrusted.

The issuer is trusted only for correctness of claim evaluation.

The relying party trusts only issuer signatures and local policy.

The protocol guarantees claim authenticity and integrity, but does not guarantee identity or subject uniqueness.

11. IANA Considerations

This document has no IANA actions.

12. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Author’s Address

Devin Wiley
United States of America
Email: devin.d.wiley@gmail.com