grow
Internet-Draft
Intended status: Standards Track
Expires: 1 January 2026

Q. Misell
AS207960

30 June 2025

Attesting the Identities of Parties in OpenID Connect (OIDC) using the Resource Public Key Infrastructure (RPKI)

draft-blahaj-grow-rpki-oauth-00

Abstract

The Peering API currently under discussion in the GROW Working Group does not provide a standardised mechanism to authenticate parties engaged in the Peering API. This document specifies a method to attest as to the identities of parties in an OpenID Connect (OIDC) exchange, binding the authentication flow to agents of ASNs.

Discussion

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.molgen.mpg.de/q/rpki-peering-api-discovery.

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 1 January 2026.

Copyright Notice

Table of Contents

1. Introduction

An API allowing programmatic configuration of BGP peering sessions is defined in [I-D.ramseyer-grow-peering-api]. The API defined in that document does not provide a standardised mechanism to authenticate parties engaged in the Peering API. To this end, this documents defines extensions to OpenID Connect to allow verifying an AS's Identity Provider (IdP), its Relying Parties (RP), and agents thereof.

1.1. Requirements 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 [BCP14] when, and only when, they appear in all capitals, as shown here.

2. Problem statement

The Peering API currently under discussion at the Global Routing Operations Working Group [I-D.ramseyer-grow-peering-api]is in need of a way to authenticate parties involved in such API exchanges. The draft, as it is currently conceived, relies on the OAuth service provided by PeeringDB to authenticate Autonomous Systems and their agents. It is undesirable, in the scope of an IETF document to rely on such external parties as a core part of the specification. We therefore set out to define an alternative OAuth federation mechanism based on the RPKI[RFC6480], one that is not tied to one entity, and is usable by anyone within the Internet ecosystem.

The reasons for adapting OAuth and not defining a new authentication mechanism are twofold; firstly, OAuth is a familiar protocol for authentication in application development, and many libraries exist that support it, secondly, and perhaps more crucially, is the large extant deployment of corporate IdPs using OAuth. From discussions from the proponents of the Peering API, the need to identify not only the Autonomous System from which the request originates, but in addition _which agent_ of the AS has made the request. That is, it would be beneficial be able to say not only that AS64496 submitted a peering request, but that John of AS64496 did so.

Given the prevalence of corporate IdPs, specifically those that support OAuth, it seems fitting to extend this to also provide authentication to a peering API. OAuth already provides the dynamic client registration, and token introspection, required to integrate a third party service with a corporate IdP. This document serves to build upon this by creating a tie between resources attested in the RPKI and their IdPs and RPs.

In addition to the peering API, there likely will be other APIs one may wish to establish between ASNs, and this OAuth extensions provides a natual basis for them.

3. Terminology

For brevity, within this document the following terminology is used

Service Provider An AS offering a (e.g. REST API) service to other ASes.

Consumer An AS consuming the service provided by the Service Provider.

4. Endpoint Discovery

All endpoints required for this protocol to function not defined herein, are to be discovered via OpenID Connect Discovery [OpenID.Discovery]

5. Extensions to IdP Metadata

An RP must be able to verify that an IdP is allowed to issue authorization tokens for resources. To this end, the JWK Key Set presented in the OpenID Connect Discovery jwks_url MUST be an RPKI Attested JWK Set. That is, the JWK used to sign the JWTs used in an OAuth exchange is itself signed using the RPKI, attesting that this IdP is authoritative for Internet resources. An IdP is considered authoritative for all resources in the EE Certificate contained in the RSM used to attest the JWK Key Set.

An RP SHOULD regularly check for updates to the JWK Key Set, and its associated attestation, and MUST not cache the attestation and its attested resources beyond the end of the validity of the RSM.

6. Extensions to Dynamic Client Registration

Once the RP of a Service Provider is aware which IdP will be used by the Consumer to authenticate to it, it must register with that IdP, if it hasn’t done so already. This allows it to be issued an authentication token scoped to it, and to engage in Token Introspection [OpenID.Core] to verify tokens given in API requests.

The manner in which the base URL of an IdP is communicated to an RP is out of the scope of this document, and is intended to be defined in subservient documents.

The RP submits an OIDC Dynamic Client Registration request to the Consumer’s IdP [OpenID.Registration], containing any well-known scopes as defined in subservient specifications required for which services the RP provides. Updates to these scopes in future may be made via the Client Configuration Endpoint.

Such that the Idp can validate the identity of the RP making the registration request, the request MUST be signed using HTTP signatures[RFC9421]. The signature keyid parameter MUST be URL to an RPKI Attested JWK Set. The fragment of such a URL is used to identify the exact kid used to sign the request.

This signature MUST be over at least the following components:

* @method

* @target-uri

* content-digest

The body of the HTTP request MUST be included in the signature by the use of a HTTP Digest [RFC9530].

This signature MUST contain at least the following parameters:

* @created

* @nonce

* @keyid

The response to such a registration request need not be signed, as the identity of the IdP is validated via its TLS domain identity and its attested discovery metadata.

7. RPKI Attested JWK Set

An RPKI Attested JWK Set is as a normal JWK Set[RFC7517], that MUST contain an rpki_attestation parameter. The construction of such a parameter is the base64url encoding [RFC7515] of an RPKI Signed Message over the JWK Set without the rpki_attestation parameter, using the JWK Thumbprint JSON hash input calculation algorithm[RFC7638].

The audience field for such an RSM MUST be the Global Audience (1.3.6.1.5.5.TBD.0.0).

The purpose field for such an RSM MUST be the OAuth Attestation Audience (1.3.6.1.5.5.TBD.1.1).

8. Security Considerations

The security considerations of this protocol have been left until the protocol proper is further refined.

9. IANA Considerations

9.1. RPKI Signed Message well-known purposes

The IANA is requested to allocate a new OID under the "RPKI Signed Message well-known purposes" registry:

Decimal	Description	References
1	OAuth Attestation	This document

Table 1

10. References

10.1. Normative References

[BCP14] Best Current Practice 14, <https://www.rfc-editor.org/info/bcp14>. At the time of writing, this BCP comprises the following:

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>.

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>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7638] Jones, M. and N. Sakimura, "JSON Web Key (JWK) Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September 2015, <https://www.rfc-editor.org/info/rfc7638>.

[RFC9421] Backman, A., Ed., Richer, J., Ed., and M. Sporny, "HTTP Message Signatures", RFC 9421, DOI 10.17487/RFC9421, February 2024, <https://www.rfc-editor.org/info/rfc9421>.

[RFC9530] Polli, R. and L. Pardue, "Digest Fields", RFC 9530, DOI 10.17487/RFC9530, February 2024, <https://www.rfc-editor.org/info/rfc9530>.

[I-D.ramseyer-grow-peering-api]
Aguado, C., Griswold, M., Ramseyer, J., Servin, A., and T. Strickx, "Peering API", Work in Progress, Internet-Draft, draft-ramseyer-grow-peering-api-05, 30 May 2024, <https://datatracker.ietf.org/doc/html/draft-ramseyer-grow-peering-api-05>.

[OpenID.Core]
Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0 incorporating errata set 2", The OpenID Foundation, 15 December 2023, <https://openid.net/specs/openid-connect-core-1_0.html>.

[OpenID.Discovery]
Sakimura, N., Bradley, J., Jones, M., and E. Jay, "OpenID Connect Discovery 1.0 incorporating errata set 2", The OpenID Foundation, 15 December 2023, <https://openid.net/specs/openid-connect-discovery-1_0.html>.

[OpenID.Registration]
Sakimura, N., Bradley, J., and M. Jones, "OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 2", The OpenID Foundation, 15 December 2023, <https://openid.net/specs/openid-connect-registration-1_0.html>.

Author’s Address

Q Misell
AS207960 Cyfyngedig
13 Pen-y-lan Terrace
Caerdydd
CF23 9EU
United Kingdom
Email: q@as207960.net, q@magicalcodewit.ch
URI: https://magicalcodewit.ch