OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 13, 2017

B. Campbell
J. Bradley
Ping Identity

October 10, 2016

Mutual X.509 Transport Layer Security (TLS) Authentication for OAuth Clients
draft-campbell-oauth-tls-client-auth-00

Abstract

This document describes X.509 certificates as OAuth client credentials using Transport Layer Security (TLS) mutual authentication as a mechanism for client authentication to the authorization server's token endpoint.

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 http://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 April 13, 2017.

Copyright Notice

Table of Contents

1. Introduction

The OAuth 2.0 Authorization Framework [RFC6749] defines a shared secret method of client authentication but also allows for the definition and use of additional client authentication mechanisms when interacting with the authorization server's token endpoint. This document describes an additional mechanism of client authentication utilizing mutual TLS [RFC5246] certificate-based authentication.

1.1. Requirements Notation and Conventions

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 [RFC2119].

2. Mutual TLS for Client Authentication

The following section defines, as an extension of OAuth 2.0, Section 2.3 [RFC6749], the use of mutual TLS as client credentials. OAuth 2.0 requires that access token requests by the client to the token endpoint use TLS. In order to utilize TLS for client authentication, the TLS connection MUST have been established or

reestablished with mutual X.509 certificate authentication (i.e. the Client Certificate and Certificate Verify messages are sent during the TLS Handshake [RFC5246]).

For all access token requests to the token endpoint, regardless of the grant type used, the client MUST include the "client_id" parameter, described in OAuth 2.0, Section 2.2 [RFC6749]. The presence of the "client_id" parameter enables the authorization server to easily identify the client independently from the content of the certificate and allows for trust models to vary as appropriate for a given deployment. The authorization server can locate the client configuration by the client identifier and check the certificate presented in the TLS Handshake against the expected credentials for that client.

3. Metadata

The value "tls_client_auth" is used to indicate mutual TLS as an authentication method to the token endpoint for the "token_endpoint_auth_methods_supported" client metadata field defined in [RFC7591], Section 2.

The same "tls_client_auth" value can also indicate server support for mutual TLS as a client authentication method in authorization server metadata such as [OpenID.Discovery] and [I-D.ietf-oauth-discovery].

4. IANA Considerations

4.1. Token Endpoint Authentication Method Registration

This specification requests registration of the following value in the IANA "OAuth Token Endpoint Authentication Methods" registry [IANA.OAuthTEAuthnMeths] established by [RFC7591].

4.1.1. Registry Contents

- Token Endpoint Authentication Method Name: "tls_client_auth"
- Change Controller: IESG
- Specification Document(s): [[this specification]]

5. Security Considerations

5.1. TLS Versions and Best Practices

TLS 1.2 [RFC5246] is cited in this document because, at the time of writing, it is latest version that is widely deployed. However, this document is applicable with other TLS versions supporting certificate-based client authentication. Implementation security considerations for TLS, including version recommendations, can be found in Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) [BCP195].

5.2. Client Identity Binding

No specifc method of binding a certificate to a client identifier is prescribed by this document. However, some method should employed so that, in addition to proving possession of the private key corresponding to the certificate, the client identity is also bound to the certificate. One such binding would be to configure for the client a value that the certificate must contain in the subject field or the subjectAltName extension and possibly a restricted set of trust anchors. An alternative method would be to configure a public key for the client directly that would have to match the subject public key info of the certificate.

6. References

6.1. Normative References

[BCP195] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <http://www.rfc-editor.org/info/bcp195>.

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

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security

(TLS) Protocol Version 1.2", RFC 5246,
DOI 10.17487/RFC5246, August 2008,
<http://www.rfc-editor.org/info/rfc5246>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework",
RFC 6749, DOI 10.17487/RFC6749, October 2012,
<http://www.rfc-editor.org/info/rfc6749>.

6.2. Informative References

[I-D.ietf-oauth-discovery]
Jones, M., Sakimura, N., and J. Bradley, "OAuth 2.0
Authorization Server Metadata", draft-ietf-oauth-
discovery-04 (work in progress), August 2016.

[IANA.OAuthTEAuthnMeths]
IANA, "OAuth Token Endpoint Authentication Methods",
<http://www.iana.org/assignments/oauth-parameters/
oauth-parameters.xhtml#token-endpoint-auth-method>.

[OpenID.Discovery]
Sakimura, N., Bradley, J., Jones, M., and E. Jay, "OpenID
Connect Discovery 1.0", February 2014.

[RFC7591] Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and
P. Hunt, "OAuth 2.0 Dynamic Client Registration Protocol",
RFC 7591, DOI 10.17487/RFC7591, July 2015,
<http://www.rfc-editor.org/info/rfc7591>.

Appendix A. Acknowledgements

Scott "not Tomlinson" Tomilson and Matt Peterson were involved in the original design and implementation work that informed the content of this document.

Appendix B. Document History

[[to be removed by the RFC Editor before publication as an RFC]]

-00

- Initial draft.

Authors' Addresses

Brian Campbell
Ping Identity

Email: brian.d.campbell@gmail.com

John Bradley
Ping Identity

Email: ve7jtb@ve7jtb.com
URI: http://www.thread-safe.com/