ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 22, 2019

L. Seitz
RISE

September 18, 2018

Additional OAuth Parameters for Authorization in Constrained Environments (ACE)
draft-ietf-ace-oauth-params-00

Abstract

This specification defines new parameters for the OAuth 2.0 token and introspection endpoints when used with framework for authentication and authorization for constrained environments (ACE). These are used to express the desired audience of a requested access token, the desired proof-of-possession key, the proof-of-possession key that the AS has selected, and the key the RS should use to authenticate to the client.

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 March 22, 2019.

Copyright Notice

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The Authorization for the Internet of Things specification [I-D.ietf-ace-oauth-authz] requires some new parameters for requests and responses to the OAuth 2.0 [RFC6749] token and introspection endpoints, as well as some new claims to be used in access tokens. This document specifies these new parameters and claims separately from the framework, so they can be used and updated independently.

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, as shown here.

Readers are assumed to be familiar with the terminology from [I-D.ietf-ace-oauth-authz].

Note that the term "endpoint" is used here following its OAuth 2.0 [RFC6749] definition, which is to denote resources such as token and introspection at the AS and authz-info at the RS. The CoAP [RFC7252]

definition, which is "An entity participating in the CoAP protocol" is not used in this specification.

3. Parameters for the Token Endpoint

3.1. Client-to-AS Request

This document defines the following additional parameters for requesting an access token from a token endpoint in the ACE framework [I-D.ietf-ace-oauth-authz]:

req_aud
: OPTIONAL. Specifies the audience for which the client is requesting an access token. If this parameter is missing, it is assumed that the AS has a default audience for access tokens issued to this client. If a client submits a request for an access token without specifying a "req_aud" parameter, and the AS does not have a default audience value for this client, then the AS MUST respond with an error message using a response code equivalent to the CoAP response code 4.00 (Bad Request).

req_cnf
: OPTIONAL. This field contains information about the key the client would like to bind to the access token for proof-of-possession. It is RECOMMENDED that an AS reject a request containing a symmetric key value in the 'req_cnf' field, since the AS is expected to be able to generate better symmetric keys than a potentially constrained client. See Section 5 for more details on the use of this parameter.

3.2. AS-to-Client Response

This document defines the following additional parameters for an AS response to a request to the token endpoint:

cnf

REQUIRED if the token type is "pop" and a symmetric key is used. MAY be present for asymmetric proof-of-possession keys. This field contains the proof-of-possession key that the AS selected for the token. See Section 5 for details on the use of this parameter.

rs_cnf
OPTIONAL if the token type is "pop" and asymmetric keys are used. MUST NOT be present otherwise. This field contains information about the public key used by the RS to authenticate. If this parameter is absent, either the RS does not use a public key or

the AS assumes that the client already knows the public key of the RS. See Section 5 for details on the use of this parameter.

4. Parameters for the Introspection Endpoint

4.1. AS-to-RS Response

This document defines the following additional parameters for an AS response to a request to the introspection endpoint:

cnf
OPTIONAL. This field contains information about the proof-of-possession key that binds the client to the access token. See Section 5 for more details on the use of the "cnf" parameter.

rs_cnf
OPTIONAL. If the RS has several keys it can use to authenticate towards the client, the AS can give the RS a hint using this parameter, as to which key it should use (e.g., if the AS previously informed the client about a public key the RS is holding). See Section 5 for more details on the use of this parameter.

5. Confirmation Method Parameters

The confirmation method parameters are used as follows:

- "req_cnf" in the token request C -> AS, OPTIONAL to indicate the client's raw public key, or the key-identifier of a previously

established key between C and RS that the client wishes to use for proof-of-possession of the access token.

- "cnf" in the token response AS -> C, OPTIONAL if using an asymmetric key or a key that the client requested via a key identifier in the request. REQUIRED if the client didn't specify a "req_cnf" and symmetric keys are used. Used to indicate the symmetric key generated by the AS for proof-of-possession of the access token.
- "cnf" in the introspection response AS -> RS, REQUIRED if the token that was subject to introspection is a proof-of-possession token, absent otherwise. Indicates the proof-of-possession key bound to the token.
- "rs_cnf" in the token response AS -> C, OPTIONAL to indicate the public key of the RS if it has one.
- "rs_cnf" in the introspection response AS -> RS, OPTIONAL to indicate to the RS which asymmetric key pair to use for authenticating to the client if the RS has several public keys.

All confirmation parameters use the same formatting and semantics as the "cnf" claim specified in [I-D.ietf-ace-cwt-proof-of-possession] when used with a CBOR encoding. When these parameters are used with a JSON encoding, the formatting and semantics of the "cnf" claim specified in [RFC7800] is used.

Note that the COSE_Key structure in a confirmation claim or parameter may contain an "alg" or "key_ops" parameter. If such parameters are present, a client MUST NOT use a key that is not compatible with the profile or proof-of-possession algorithm according to those parameters. An RS MUST reject a proof-of-possession using such a key.

If an access token is issued for an audience that includes several RS, the "rs_cnf" parameter MUST NOT be used, since the client cannot determine for which RS the key applies. This document recommends to specify a different endpoint that the client can use to acquire RS authentication keys in such cases. The specification of such an endpoint is out of scope for this document.

6. CBOR Mappings

If CBOR is used, the new parameters and claims defined in this document MUST be mapped to CBOR types as specified in Figure 1, using the given integer abbreviation for the map key.

Parameter name	CBOR Key	Value Type
cnf	8	map
rs_cnf	17	map
req_aud	18	text string
req_cnf	19	map

Figure 1: CBOR mappings for new parameters.

7. Security Considerations

This document is an extension to [I-D.ietf-ace-oauth-authz]. All security considerations from that document apply here as well.

8. Privacy Considerations

This document is an extension to [I-D.ietf-ace-oauth-authz]. All privacy considerations from that document apply here as well.

9. IANA Considerations

9.1. OAuth Parameter Registration

This section registers the following parameters in the "OAuth Parameters" registry [IANA.OAuthParameters]:

- Name: "req_aud"
- Parameter Usage Location: authorization request, token request
- Change Controller: IESG
- Reference: Section 3.1 of [this document]

- Name: "req_cnf"
- Parameter Usage Location: token request
- Change Controller: IESG

- Reference: Section 5 of [this document]

- Name: "rs_cnf"
- Parameter Usage Location: token response
- Change Controller: IESG
- Reference: Section 5 of [this document]

- Name: "cnf"
- Parameter Usage Location: token response
- Change Controller: IESG
- Reference: Section 5 of [this document]

9.2. OAuth Introspection Response Parameter Registration

This section registers the following parameters in the OAuth Token Introspection Response registry [IANA.TokenIntrospectionResponse].

- Name: "cnf"
- Description: Key to prove the right to use a PoP token.
- Change Controller: IESG
- Reference: Section 4.1 of [this document]

- Name: "rs_cnf"
- Description: The key the RS should use to authenticate to the client.
- Change Controller: IESG
- Reference: Section 4.1 of [this document]

10. Acknowledgments

This document is a product of the ACE working group of the IETF.

Ludwig Seitz worked on this document as part of the CelticPlus project CyberWI, with funding from Vinnova.

11. Normative References

[I-D.ietf-ace-cwt-proof-of-possession]
Jones, M., Seitz, L., Selander, G., Erdtman, S., and H. Tschofenig, "Proof-of-Possession Key Semantics for CBOR

Web Tokens (CWTs)", draft-ietf-ace-cwt-proof-of-possession-03 (work in progress), June 2018.

[I-D.ietf-ace-oauth-authz]
Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", draft-ietf-ace-oauth-authz-13 (work in progress), July 2018.

[IANA.OAuthParameters]
IANA, "OAuth Parameters", <https://www.iana.org/assignments/oauth-parameters/oauth-parameters.xhtml#parameters>.

[IANA.TokenIntrospectionResponse]
IANA, "OAuth Token Introspection Response", <https://www.iana.org/assignments/oauth-parameters/oauth-parameters.xhtml#token-introspection-response>.

[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>.

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

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7800] Jones, M., Bradley, J., and H. Tschofenig, "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, DOI 10.17487/RFC7800, April 2016, <https://www.rfc-editor.org/info/rfc7800>.

[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

Ludwig Seitz
RISE
Scheelevaegen 17
Lund 223 70
Sweden

Email: ludwig.seitz@ri.se