ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 31, 2020

L. Seitz
Combitech

April 29, 2020

Additional OAuth Parameters for Authorization in Constrained Environments (ACE)
draft-ietf-ace-oauth-params-13

Abstract

This specification defines new parameters and encodings for the OAuth 2.0 token and introspection endpoints when used with the framework for authentication and authorization for constrained environments (ACE). These are used to express the proof-of-possession key the client wishes to use, the proof-of-possession key that the Authorization Server has selected, and the key the Resource Server uses 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 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 October 31, 2020.

Copyright Notice

Table of Contents

1. Introduction

The Authentication and Authorization for Constrained Environments (ACE) specification [I-D.ietf-ace-oauth-authz] requires some new parameters for interactions with the OAuth 2.0 [RFC6749] token and introspection endpoints, as well as some new claims to be used in access tokens. These parameters and claims can also be used in other contexts and have therefore been put into a dedicated document, to facilitate their use in a manner independent of [I-D.ietf-ace-oauth-authz].

Note that although all examples are shown in Concise Binary Object Respresentation (CBOR) [RFC7049], JSON [RFC8259] MAY be used as an alternative for HTTP-based communications, as specified in [I-D.ietf-ace-oauth-authz].

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], especially the terminology for entities in the architecture such as client (C), resource server (RS) and authorization server (AS).

Terminology from [RFC8152] is used in the examples, especially COSE_Key defined in section 7 of [RFC8152].

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 Constrained Application Protocol (CoAP) [RFC7252] definition, which is "An entity participating in the CoAP protocol" is not used in this specification.

3. Parameters for the Token Endpoint

This section defines additional parameters for the interactions with the token endpoint in the ACE framework [I-D.ietf-ace-oauth-authz].

3.1. Client-to-AS Request

This section defines the "req_cnf" parameter allowing clients to request a specific proof-of-possession key in an access token from a token endpoint in the ACE framework [I-D.ietf-ace-oauth-authz]:

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 (kty=Symmetric), since the AS is expected to be able to generate better symmetric keys than a constrained client. The AS MUST verify that the client really is in possession of the corresponding key. Values of this parameter follow the syntax and semantics of the "cnf" claim either from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession] for CBOR-based interactions or from section 3.1 of [RFC7800] for JSON-based interactions.

Figure 1 shows a request for an access token using the "req_cnf" parameter to request a specific public key as proof-of-possession key. The content is displayed in CBOR diagnostic notation, without abbreviations and with line-breaks for better readability.

```
Header: POST (Code=0.02)
Uri-Host: "as.example.com"
Uri-Path: "token"
Content-Format: "application/ace+cbor"
Payload:
{
   "req_cnf" : {
      "COSE_Key" : {
         "kty" : "EC2",
         "kid" : h'11',
         "crv" : "P-256",
         "x" : h'BAC5B11CAD8F99F9C72B05CF4B9E26D24
                 4DC189F745228255A219A86D6A09EFF',
         "y" : h'20138BF82DC1B6D562BE0FA54AB7804A3
                 A64B6D72CCFED6B6FB6ED28BBFC117E'
      }
   }
 }
```

Figure 1: Example request for an access token bound to an asymmetric key.

3.2. AS-to-Client Response

This section 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. Values of this parameter follow the syntax and semantics of the "cnf" claim either from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession] for CBOR-based interactions of from section 3.1 of [RFC7800] for JSON-based interactions. See Section 5 for additional discussion of the usage 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 knows that the RS can authenticate itself to the client without additional information. Values of this parameter follow the syntax and semantics of the "cnf" claim either from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession] for CBOR-based interactions or from section 3.1 of [RFC7800] for JSON-based interactions. See Section 5 for additional discussion of the usage of this parameter.

Figure 2 shows an AS response containing a token and a "cnf" parameter with a symmetric proof-of-possession key.

```
Header: Created (Code=2.01)
Content-Format: "application/ace+cbor"
Payload:
{
  "access_token" : h'4A5015DF686428 ...
   (remainder of CWT omitted for brevity;
   CWT contains COSE_Key in the "cnf" claim)',
  "cnf" : {
    "COSE_Key" : {
      "kty" : "Symmetric",
```

```
      "kid" : h'DFD1AA97',
      "k" : h'849B5786457C1491BE3A76DCEA6C427108'
    }
  }
}
```

Figure 2: Example AS response with an access token bound to a symmetric key.

Figure 3 shows an AS response containing a token bound to a previously requested asymmetric proof-of-possession key (not shown) and a "rs_cnf" parameter containing the public key of the RS.


```
Header: Created (Code=2.01)
Content-Format: "application/ace+cbor"
Payload:
{
  "access_token" : h'D08343A1010AA1054D2A45DF6FBC5A5A ...
   (remainder of CWT omitted for brevity)',
  "rs_cnf" : {
    "COSE_Key" : {
      "kty" : "EC2",
      "kid" : h'12',
      "crv" : "P-256",
      "x" : h'BCEE7EAAC162F91E6F330F5771211E220
              B8B546C96589B0AC4AD0FD24C77E1F1',
      "y" : h'C647B38C55EFBBC4E62E651720F002D5D
              75B2E0C02CD1326E662BCA222B90416'
```

```
      }
    }
  }
```

Figure 3: Example AS response, including the RS's public key.

4. Parameters for the Introspection Endpoint

This section defines the use of CBOR instead of JSON for the "cnf" introspection response parameter specified in section 9.4 of [I-D.ietf-oauth-mtls].

If CBOR is used instead of JSON in an interaction with the introspection endpoint, the AS MUST use the parameter mapping specified in Figure 5 and the value must follow the syntax of "cnf" claim values from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession].

Figure 4 shows an AS response to an introspection request including the "cnf" parameter to indicate the proof-of-possession key bound to the token.


```
Header: Created Code=2.01)
Content-Format: "application/ace+cbor"
Payload:
{
  "active" : true,
  "scope" : "read",
  "aud" : "tempSensor4711",
  "cnf" : {
```

```
      "COSE_Key" : {
        "kty" : "EC2",
        "kid" : h'11',
        "crv" : "P-256",
        "x" : h'BAC5B11CAD8F99F9C72B05CF4B9E26D24
                4DC189F745228255A219A86D6A09EFF',
        "y" : h'20138BF82DC1B6D562BE0FA54AB7804A3
                A64B6D72CCFED6B6FB6ED28BBFC117E'
      }
    }
  }
```

Figure 4: Example introspection response.

5. Confirmation Method Parameters

The confirmation method parameters are used as follows:

- "req_cnf" in the access 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 access token that was subject to introspection is a proof-of-possession token, absent otherwise. Indicates the proof-of-possession key bound to the access token.

- "rs_cnf" in the token response AS -> C, OPTIONAL to indicate the public key of the RS, if it uses one to authenticate itself to the client and the binding between key and RS identity is not established through other means.

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 incompatible 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 5, using the given integer abbreviation for the map key.

Name	CBOR Key	Value Type	Usage
req_cnf	TBD (4)	map	token request
cnf	TBD (8)	map	token response
cnf	TBD (8)	map	introspection response
rs_cnf	TBD (41)	map	token response

Figure 5: CBOR mappings for new parameters and claims.

7. Requirements when using asymmetric keys

An RS using asymmetric keys to authenticate to the client MUST NOT hold several different asymmetric key pairs, applicable to the same authentication algorithm. For example when using DTLS, the RS MUST NOT hold several asymmetric key pairs applicable to the same cipher suite. The reason for this restriction is that the RS has no way of determining which key to use before the client's identity is established. Therefore authentication attempts by the RS could randomly fail based on which key the RS selects, unless the algorithm negotiation produces a unique choice of key pair for the RS.

8. Security Considerations

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

9. Privacy Considerations

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

10. IANA Considerations

10.1. OAuth Parameter Registration

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

- 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]

10.2. OAuth Parameters CBOR Mappings Registration

This section registers the following parameter mappings in the "OAuth Parameters CBOR Mappings" registry established in section 8.9. of [I-D.ietf-ace-oauth-authz].

- Name: "req_cnf"
- CBOR key: TBD (suggested: 4)
- Change Controller: IESG
- Reference: Section 3.1 of [this document]

- Name: "cnf"
- CBOR key: TBD (suggested: 8)
- Change Controller: IESG
- Reference: Section 3.2 of [this document]

- Name: "rs_cnf"
- CBOR key: TBD (suggested: 41)
- Change Controller: IESG

- Reference: Section 3.2 of [this document]

10.3. OAuth Token Introspection Response CBOR Mappings Registration

This section registers the following parameter mapping in the "OAuth Token Introspection Response CBOR Mappings" registry established in section 8.11. of [I-D.ietf-ace-oauth-authz].

- Name: "cnf"
- CBOR key: TBD (suggested: 8)
- Change Controller: IESG
- Reference: Section 4 of [this document]

11. Acknowledgments

This document is a product of the ACE working group of the IETF. Special thanks to Brian Campbell for his thorough review of this document.

Ludwig Seitz worked on this document as part of the CelticNext projects CyberWI, and CRITISEC with funding from Vinnova.

12. References

12.1. 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-11 (work in progress), October 2019.

[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-33 (work in progress), February 2020.

[I-D.ietf-oauth-mtls]
Campbell, B., Bradley, J., Sakimura, N., and T.

Lodderstedt, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens", draft-ietf-oauth-mtls-17 (work in progress), August 2019.

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

[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>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[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>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[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>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

12.2. Informative References

[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>.

Author's Address

Ludwig Seitz
Combitech
Djaeknegatan 31
Malmoe 211 35
Sweden

Email: ludwig.seitz@combitech.se