ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 3, 2019

L. Seitz
RISE

January 30, 2019

Additional OAuth Parameters for Authorization in Constrained Environments (ACE)
draft-ietf-ace-oauth-params-03

Abstract

This specification defines new parameters 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 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

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 may need to be updated to align them with ongoing OAuth work. Therefore they have been split out into this document, which can be used and updated independently of [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].

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). Values of this parameter follow the syntax of the "aud" claim from section 3.1.3 of [RFC8392].

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. The AS MUST verify that the client really is in possession of the corresponding key. Values of this parameter follow the syntax of the "cnf" claim from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession].

Figure 1 shows a request for an access token using the "req_aud" parameter to request a specific audience and 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 for better readability.

```
Header: POST (Code=0.02)
Uri-Host: "as.example.com"
Uri-Path: "token"
Content-Format: "application/ace+cbor"
Payload:
{
   "req_aud" : "tempSensor4711",
   "req_cnf" : {
      "COSE_Key" : {
         "kty" : "EC",
         "kid" : h'11',
         "crv" : "P-256",
         "x" : b64'usWxHK2PmfnHKwXPS54m0kTcGJ90UiglWiGahtagnv8',
         "y" : b64'IBOL+C3BttVivg+lSreASjpkttcsz+1rb7btKLv8EX4'
      }
   }
 }
```

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

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. Values of this parameter follow the syntax of the "cnf" claim from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession]. 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. Values of this parameter follow the syntax of the "cnf" claim from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession]. See Section 5 for details on the use 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" : b64'SlAV32hkKG ...
   (remainder of CWT omitted for brevity;
   CWT contains COSE_Key in the "cnf" claim)',
  "cnf" : {
    "COSE_Key" : {
      "kty" : "Symmetric",
      "kid" : b64'39Gqlw',
      "k" : b64'hJtXhkV8FJG+Onbc6mxCcQh'
    }
  }
}
```

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" : b64'SlAV32hkKG ...
   (remainder of CWT omitted for brevity;
   CWT contains COSE_Key in the "cnf" claim)',
  "rs_cnf" : {
    "COSE_Key" : {
      "kty" : "EC",
      "kid" : h'12',
      "crv" : "P-256",
      "x" : b64'vO5+qsFi+R5vMw9XcSEeIguLVGyWWJsKxK0P0kx34fE',
      "y" : b64'xkezjFXvu8TmLmUXIPAC1ddbLgwCzRMm5mK8oiK5BBY'
    }
  }
}
```

Figure 3: Example AS response with an access token bound to a symmetric key.

3.3. The Resource Server Confirmation Claim

If the AS needs to convey a hint to the RS about which key it should use to authenticate towards the client, this specification defines the "rs_cnf" claim, which MAY be used in the access token, with the same syntax and semantics as defined in for the "rs_cnf" 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. Values of this parameter follow the syntax of the "cnf" claim from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession]. See Section 5 for more details on the use of the "cnf" parameter.

rs_cnf

OPTIONAL. If the RS uses asymmetric keys to authenticate towards the client (e.g. with a DTLS-RPK handshake) and it has several such keys (e.g. for different elliptic curves), the AS can give the RS a hint using this parameter, as to which key it should use. Values of this parameter follow the syntax of the "cnf" claim from section 3.1 of [I-D.ietf-ace-cwt-proof-of-possession]. See Section 5 for details on the use of this parameter.

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 and the "rs_cnf" parameter to indicate the key the RS is supposed to use to authenticate to the client.

```
   Header: Created Code=2.01)
   Content-Format: "application/ace+cbor"
   Payload:
   {
     "active" : true,
     "scope" : "read",
     "aud" : "tempSensor4711",
     "cnf" : {
       "COSE_Key" : {
         "kty" : "EC",
         "kid" : h'11',
         "crv" : "P-256",
         "x" : b64'usWxHK2PmfnHKwXPS54m0kTcGJ90UiglWiGahtagnv8',
         "y" : b64'IBOL+C3BttVivg+lSreASjpkttcsz+1rb7btKLv8EX4'
       }
     },
     "rs_cnf" : {
       "COSE_Key" : {
         "kty" : "EC",
         "kid" : h'12',
         "crv" : "P-256",
         "x" : b64'vO5+qsFi+R5vMw9XcSEeIguLVGyWWJsKxK0P0kx34fE',
         "y" : b64'xkezjFXvu8TmLmUXIPAC1ddbLgwCzRMm5mK8oiK5BBY'
       }
     }
   }
```

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 to the client.
- "rs_cnf" in the introspection response AS -> RS, OPTIONAL, contains the public key that the RS should use for authenticating to the client (e.g. if the RS has several different public keys).

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

Parameter name	CBOR Key	Value Type
req_aud	3	text string
cnf	8	map
rs_cnf	11	map
req_cnf	12	map

Figure 5: 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.

The audience claim as defined in [RFC7519] and the equivalent "req_aud" parameter are intentionally vague on how to match the audience value to a specific RS. This is intended to allow application specific semantics to be used. This section attempts to

give some general guidance for the use of audiences in constrained environments.

URLs are not a good way of identifying mobile devices that can switch networks and thus be associated with new URLs. If the audience represents a single RS, and asymmetric keys are used, the RS can be uniquely identified by a hash of its public key. If this approach is used this framework RECOMMENDS to apply the procedure from section 3 of [RFC6920].

If the audience addresses a group of resource servers, the mapping of group identifier to individual RS has to be provisioned to each RS before the group-audience is usable. Managing dynamic groups could be an issue, if the RS is not always reachable when the group memberships change. Furthermore issuing access tokens bound to symmetric proof-of-possession keys that apply to a group-audience is problematic, as an RS that is in possession of the access token can impersonate the client towards the other RSs that are part of the group. It is therefore NOT RECOMMENDED to issue access tokens bound to a group audience and symmetric proof-of possession keys.

Even the client must be able to determine the correct values to put into the "req_aud" parameter, in order to obtain a token for the intended RS. Errors in this process can lead to the client inadvertantly communicating with the wrong RS. The correct values for "req_aud" can either be provisioned to the client as part of its configuration, or dynamically looked up by the client in some directory. In the latter case the integrity and correctness of the directory data must be assured.

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. JSON Web Token Claims

This specification registers the following new claim in the JSON Web Token (JWT) registry of JSON Web Token Claims [IANA.JsonWebTokenClaims]:

- Claim Name: "rs_cnf"
- Claim Description: The public key the RS is supposed to use to authenticate to the client wielding this token.
- Change Controller: IESG
- Reference: Section 3.3 of [this document]

9.2. CBOR Web Token Claims

This specification registers the following new claim in the "CBOR Web Token (CWT) Claims" registry [IANA.CborWebTokenClaims].

- Claim Name: "rs_cnf"
- Claim Description: The public key the RS is supposed to use to authenticate to the client wielding this token.
- JWT Claim Name: rs_cnf
- Claim Key: TBD (suggested: 40)
- Claim Value Type(s): map
- Change Controller: IESG
- Specification Document(s): Section 3.3 of [this document]

9.3. 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]

9.4. 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]

9.5. Token Endpoint CBOR Mappings Registraton

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

- Name: "req_aud"
- CBOR key: 18
- Change Controller: IESG
- Reference: Section 3.1 of [this document]

- Name: "req_cnf"
- CBOR key: 19
- Change Controller: IESG
- Reference: Section 3.1 of [this document]

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

- Name: "rs_cnf"
- CBOR key: 17
- Change Controller: IESG
- Reference: Section 3.2 of [this document]

9.6. Introspection Endpoint CBOR Mappings Registraton

This section registers teh following parameter mappings in the "Introspection Endpoint CBOR Mappings" registry established in section 8.11. of [I-D.ietf-ace-oauth-authz].

- Name: "cnf"
- CBOR key: 8
- Change Controller: IESG
- Reference: Section 4.1 of [this document]

- Name: "rs_cnf"
- CBOR key: 17
- 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. References

11.1. 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-05 (work in progress), November 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-18 (work in progress), January 2019.

[IANA.CborWebTokenClaims]
IANA, "CBOR Web Token (CWT) Claims", <https://www.iana.org/assignments/cwt/cwt.xhtml#claims-registry>.

[IANA.JsonWebTokenClaims]
IANA, "JSON Web Token Claims", <https://www.iana.org/assignments/jwt/jwt.xhtml#claims>.

[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>.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <https://www.rfc-editor.org/info/rfc6920>.

[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>.

[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>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

11.2. Informative References

[I-D.ietf-oauth-pop-key-distribution]
Bradley, J., Hunt, P., Jones, M., Tschofenig, H., and M. Mihaly, "OAuth 2.0 Proof-of-Possession: Authorization Server to Client Key Distribution", draft-ietf-oauth-pop-key-distribution-04 (work in progress), October 2018.

[I-D.ietf-oauth-resource-indicators]
Campbell, B., Bradley, J., and H. Tschofenig, "Resource Indicators for OAuth 2.0", draft-ietf-oauth-resource-indicators-02 (work in progress), January 2019.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

Appendix A. Overlap with OAuth work

This document overlaps with draft work from OAuth, namely [I-D.ietf-oauth-pop-key-distribution] and [I-D.ietf-oauth-resource-indicators].

The former specifies the use of "req_cnf" and "cnf" for requesting proof-of-possession tokens and indicating the key that the AS has selected. It it was initially deemed that the work at OAuth had been

discontinued and therefore equivalent functionality was defined here. Work in OAuth has since resumed, but it is lagging behind the planned milestones of the ACE working group. We have therefore split this work out into a separate document so that it can later be updated or obsoleted to align it with the final result of the OAuth work, without affecting [I-D.ietf-ace-oauth-authz].

The latter defines the use of the "resource" parameter, allowing to indicate the location fo the target service or resource where access is being requested. This partially overlaps with the "req_aud" parameter specified here, however the definition of "req_aud" is more broad, since it can be used in an application specific way that is not necessarily bound to the location of the target audience (e.g. a group identifier referring to several resource servers, or the public key of a resource server).

Author's Address

Ludwig Seitz
RISE
Scheelevaegen 17
Lund 223 70
Sweden

Email: ludwig.seitz@ri.se