ACE Working Group
Internet-Draft
Updates: 9200 (if approved)
Intended status: Standards Track
Expires: 7 March 2026

M. Tiloca
RISE AB
G. Selander
Ericsson AB

3 September 2025

Bidirectional Access Control in the Authentication and Authorization for Constrained Environments (ACE) Framework
draft-tiloca-ace-bidi-access-control-01

Abstract

This document updates the Authentication and Authorization for Constrained Environments (ACE) framework, for which it defines a method to enforce bidirectional access control by means of a single access token. Therefore, this document updates RFC 9200.

Discussion Venues

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

Discussion of this document takes place on the Authentication and Authorization for Constrained Environments Working Group mailing list (ace@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ace/.

Source for this draft and an issue tracker can be found at https://gitlab.com/crimson84/draft-tiloca-ace-bidi-access-control.

Status of This Memo

Table of Contents

1. Introduction 3
1.1. Terminology 4
2. New ACE Parameters 6
2.1. rev_audience 6
2.2. rev_scope 7
3. Bidirectional Access Control 7
4. Scenario with One Authorization Server 9
4.1. Access Token Request 9
4.2. Access Token Response 10
4.3. Access to Protected Resources 13
5. Scenario with Two Authorization Servers 13
6. Practical Considerations 13
7. Security Considerations 14
8. IANA Considerations 14
8.1. OAuth Parameters Registry 14
8.2. OAuth Parameters CBOR Mappings Registry 14
8.3. JSON Web Token Claims Registry 15
8.4. CBOR Web Token (CWT) Claims Registry 15
9. References 16
9.1. Normative References 16
9.2. Informative References 17
Appendix A. CDDL Model 19
Acknowledgments 19
Authors' Addresses 19

1. Introduction

The Authentication and Authorization for Constrained Environments (ACE) framework [RFC9200] defines an architecture to enforce access control for constrained devices. A client (C) requests an assertion of granted permissions from an authorization server (AS) in the form of an access token, then uploads the access token to the target resource server (RS), and finally accesses protected resources at the RS according to the permissions specified in the access token.

The framework has as main building blocks the OAuth 2.0 framework [RFC6749], the Constrained Application Protocol (CoAP) [RFC7252] for message transfer, Concise Binary Object Representation (CBOR) [RFC8949] for compact encoding, and CBOR Object Signing and Encryption (COSE) [RFC9052][RFC9053] for self-contained protection of access tokens.

Separate profile documents define in detail how the participants in the ACE architecture communicate, especially as to the security protocols that they use. Profiles of ACE include, for instance, those described in [RFC9202], [RFC9203], [RFC9431], [I-D.ietf-ace-edhoc-oscore-profile], and [I-D.ietf-ace-group-oscore-profile]

In some deployments using the ACE framework, two devices DEV1 and DEV2 might wish to access each other’s protected resources. That is, DEV1 wishes to access protected resources hosted at DEV2 and DEV2 wishes to access protected resources hosted at DEV1.

In such a case, bidirectional access control can clearly be achieved by means of two separate access tokens, each of which is used to enforce access control in one direction. That is:

* A first access token is requested by and issued to DEV1, for accessing protected resources at DEV2. With respect to this access token, DEV1 is an ACE client, while DEV2 is an ACE RS.

* A second access token is requested by and issued to DEV2, for accessing protected resources at DEV1. With respect to this access token, DEV2 is an ACE client, while DEV1 is an ACE RS.

The two access tokens have to be separately requested and handled by DEV1 and DEV2, separately uploaded at DEV1 and DEV2, and separately managed by the AS (e.g., for providing token introspection, retiring access tokens when they become invalid, or notifying about early token revocation [RFC9770]).

While this model results in a clean split between the two directions of access control, it also yields substantial interactions and communication overhead for both DEV1 and DEV2.

Instead, it can be desirable to achieve the same bidirectional access control without such downsides, by means of a single access token that is requested by and issued to a single device.

In order to enable that, this document updates [RFC9200] as follows.

* It defines additional parameters and encodings for the OAuth 2.0 token endpoint at the AS (see Section 2). These parameters include:

  - "rev_audience", used by C to provide the AS with an identifier of itself as a reverse audience and by the AS to possibly confirm that identifier in a response to C.

    A corresponding access token claim, namely "rev_aud", is also defined in this document.

  - "rev_scope", used by C to ask the AS that the requested access token specifies additional access rights as a reverse scope, allowing the access token's audience to accordingly access protected resources at C. This parameter is also used by the AS to provide C with the access rights that are actually granted as reverse scope to the access token's audience.

    A corresponding access token claim, namely "rev_scope", is also defined in this document.

* It defines a method for the ACE framework to enforce bidirectional access control by means of a single access token (see Section 3), building on the two new parameters "rev_audience" and "rev_scope" as well as on the corresponding access token claims "rev_aud" and "rev_scope".

1.1. 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 expected to be familiar with the terms and concepts described in the ACE framework for Authentication and Authorization [RFC9200][RFC9201], as well as with terms and concepts related to CBOR Web Tokens (CWTs) [RFC8392].

The terminology for entities in the considered architecture is defined in OAuth 2.0 [RFC6749]. In particular, this includes client (C), resource server (RS), and authorization server (AS).

Readers are also expected to be familiar with the terms and concepts related to CoAP [RFC7252], Concise Data Definition Language (CDDL) [RFC8610], CBOR [RFC8949], and COSE [RFC9052][RFC9053].

Note that the term "endpoint" is used here following its OAuth definition [RFC6749], aimed at denoting resources such as /token and /introspect at the AS, and /authz-info at the RS. The CoAP definition, which is "[a]n entity participating in the CoAP protocol" [RFC7252], is not used in this document.

Furthermore, this document uses the following term originally defined in [I-D.ietf-ace-workflow-and-params].

* Token series: a set of access tokens, all of which are bound to the same proof-of-possession (PoP) key and are sequentially issued by the same AS for the same pair (client, audience) per the same profile of ACE. A token series ends when the latest access token of that token series becomes invalid (e.g., when it expires or gets revoked).

  Profiles of ACE can provide their extended and specialized definition, e.g., by further taking into account the public authentication credentials of C and the RS.

CBOR [RFC8949] and CDDL [RFC8610] are used in this document. CDDL predefined type names, especially bstr for CBOR byte strings and tstr for CBOR text strings, are used extensively in this document.

Examples throughout this document are expressed in CBOR diagnostic notation as defined in Section 8 of [RFC8949] and Appendix G of [RFC8610]. Diagnostic notation comments are often used to provide a textual representation of the parameters' keys and values.

In the CBOR diagnostic notation used in this document, constructs of the form e'SOME_NAME' are replaced by the value assigned to SOME_NAME in the CDDL model shown in Figure 2 of Appendix A. For example, {e'rev_audience' : "rs1", e'rev_scope_param' : h'00ff'} stands for {56 : "rs1", 57 : h'00ff'}.

Note to RFC Editor: Please delete the paragraph immediately preceding this note. Also, in the CBOR diagnostic notation used in this document, please replace the constructs of the form e'SOME_NAME' with the value assigned to SOME_NAME in the CDDL model shown in Figure 2 of Appendix A. Finally, please delete this note.

2. New ACE Parameters

The rest of this section defines a number of additional parameters and encodings for the OAuth 2.0 token endpoint at the AS.

2.1. rev_audience

The "rev_audience" parameter can be used in an Access Token Request sent by C to the token endpoint at the AS (see Section 5.8.1 of [RFC9200]) as well as in the successful Access Token Response sent as reply by the AS (see Section 5.8.2 of [RFC9200]). In particular, the following applies:

* The "rev_audience" parameter is OPTIONAL in an Access Token Request. The presence of this parameter indicates that C wishes the requested access token to specify additional access rights. These access rights are intended for the access token's audience to access protected resources at C. That is, C is the access token's reverse audience.

  This parameter specifies such reverse audience as a text string identifier of C. When the Access Token Request is encoded in CBOR, the value of this parameter is encoded as a CBOR text string.

* The "rev_audience" parameter is OPTIONAL in an Access Token Response. If present, it has the same meaning and encoding that it has in the Access Token Request.

Fundamentally, this parameter has the same semantics of the "audience" parameter used in the ACE framework, with the difference that it conveys an identifier of C as a host of protected resources to access, according to the access rights granted as reverse scope to the access token's audience.

The use of this parameter is further detailed in Section 3.

2.2. rev_scope

The "rev_scope" parameter can be used in an Access Token Request sent by C to the token endpoint at the AS (see Section 5.8.1 of [RFC9200]) as well as in the successful Access Token Response sent as reply by the AS (see Section 5.8.2 of [RFC9200]). In particular, the following applies:

* The "rev_scope" parameter is OPTIONAL in an Access Token Request. The presence of this parameter indicates that C wishes the requested access token to specify additional access rights. These access rights are intended for the access token's audience to access protected resources at C. That is, C is the access token's reverse audience.

  This parameter specifies such access rights as a reverse scope. When the Access Token Request is encoded in CBOR, the value of this parameter is encoded as a CBOR text string or a CBOR byte string.

* The "rev_scope" parameter is OPTIONAL in an Access Token Response. If present, this parameter specifies the access rights that the AS has actually granted as a reverse scope to the access token's audience, for accessing protected resources at C (i.e., at the access token's reverse audience).

Fundamentally, this parameter has the same semantics of the "scope" parameter used in the ACE framework, with the difference that it conveys the access rights requested/granted as reverse scope for/to the access token's audience to access protected resources at the access token's reverse audience.

The use of this parameter is further detailed in Section 3.

3. Bidirectional Access Control

The rest of this document considers two devices DEV1 and DEV2 that wish to access each other's protected resources, and it defines a method that DEV1 and DEV2 can use to enforce bidirectional access control by means of a single access token.

It is assumed that the access token is requested by and issued to DEV1 acting as ACE client. The access token is intended to specify access rights concerning both the access of DEV1 to protected resources hosted at DEV2 and the access of DEV2 to protected resources hosted at DEV1. In particular:

* The access token expresses access rights according to which the requesting ACE client DEV1 can access protected resources hosted at the ACE RS DEV2.

  For this first direction of access control, the target DEV2 is specified by means of the "audience" parameter and the corresponding access token claim "aud", while the access rights are specified by means of the "scope" parameter and the corresponding access token claim "scope".

  This is the original, primary direction of access control, where the ACE client DEV1 that requests the access token wishes to obtain access rights for accessing protected resources at the ACE RS DEV2.

* The same access token additionally expresses access rights according to which the ACE RS DEV2 can access protected resources hosted at the ACE client DEV1.

  For this second direction of access control, the target DEV1 is specified by means of the "rev_audience" parameter defined in Section 2.1 and the corresponding access token claim "rev_aud" (see Section 4.2), while the access rights are specified by means of the "rev_scope" parameter defined in Section 2.2 and the corresponding access token claim "rev_scope" (see Section 4.2).

  This is the new, secondary direction of access control, where the ACE client DEV1 that requests the access token also wishes that access rights are granted for the ACE RS DEV2 to access resources at DEV1.

  Clearly, this requires the ACE client DEV1 to also act as CoAP server, and the ACE RS DEV2 to also act as CoAP client.

Like for the original case with a single access control direction, the access token is uploaded to the ACE RS DEV2, which processes the access token as per Section 5.10 of [RFC9200] and according to the profile of ACE used by DEV1 and DEV2.

The protocol workflow is detailed in the following Section 4 and Section 5, in case only one authorization server or two authorization servers are involved, respectively.

4. Scenario with One Authorization Server

This section considers the scenario shown in Figure 1, with a single authorization server AS. Both devices DEV1 and DEV2 are registered at AS, with permissions to access protected resources at the other device. In the following, DEV1 acts as ACE client by requesting an access token from AS.

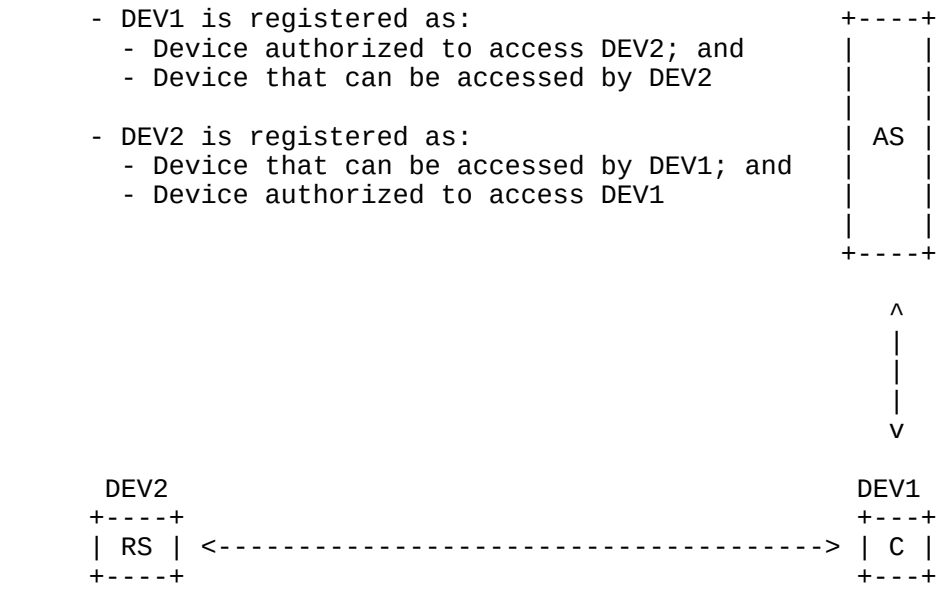

Figure 1: Bidirectional Access Control with One Authorization Server.

4.1. Access Token Request

As to the Access Token Request that DEV1 sends to AS, the following applies.

* The "audience" and "scope" parameters are used as defined in [RFC9200], according to the profile of ACE used by DEV1 and DEV2.

  In particular, "audience" specifies an identifier of DEV2, while "scope" specifies access rights that DEV1 wishes to obtain for accessing protected resources at DEV2.

  That is, the two parameters pertain to the primary direction of access control.

* The "req_cnf" parameter defined in [RFC9201] can be included. When present, it specifies the key that DEV1 wishes to bind to the requested access token.

* The "rev_audience" and "rev_scope" parameters defined in Section 2.1 and Section 2.2 can be included.

  In particular, "rev_audience" specifies an identifier of DEV1, while "rev_scope" specifies access rights that DEV1 wishes DEV2 to obtain for accessing protecting resources at DEV1.

  That is, the two parameters pertain to the secondary direction of access control.

If DEV1 wishes that the requested access token also provides DEV2 with access rights pertaining to the secondary direction of access control, then the Access Token Request has to include at least one of the two parameters "rev_audience" and "rev_scope".

4.2. Access Token Response

When receiving an Access Token Request that includes at least one of the two parameters "rev_audience" and "rev_scope", AS processes it as defined in Section 5.8.2 of [RFC9200], with the following additions:

* If the Access Token Request includes the "rev_scope" parameter but not the "rev_audience" parameter, then AS assumes that the identifier of DEV1 (i.e., the access token’s reverse audience) is the default one, if any is defined.

* If the Access Token Request includes the "rev_audience" parameter but not the "rev_scope" parameter, then AS assumes that the access rights requested as reverse scope for DEV2 (i.e., the access token’s audience) to access DEV1 are the default ones, if any are defined.

* AS checks whether the access rights requested as reverse scope for DEV2 can be at least partially granted, in accordance with the installed access policies pertaining to the access from DEV2 to protected resources at DEV1.

  That is, AS performs the same evaluation that it would perform if DEV2 sent an Access Token Request acting as an ACE client, with the intent to access protected resources at DEV1 that acts as an ACE RS.

It is REQUIRED that such evaluation succeeds, in order for AS to issue an access token and reply to DEV1 with a successful Access Token Response.

As to the successful Access Token Response that AS sends to DEV1, the following applies:

* The "audience" and "scope" parameters are used as defined in [RFC9200] and according to the profile of ACE used by DEV1 and DEV2.

  In particular, "audience" specifies an identifier of DEV2, while "scope" specifies the access rights that AS has granted to DEV1 for accessing protected resources at DEV2.

  The "scope" parameter has to be present if: i) it was present in the Access Token Request and the access rights granted to DEV1 are different from the requested ones; or ii) it was not present in the Access Token Request and the access rights granted to DEV1 are different from the default ones.

  If the "scope" parameter is not present, then the granted access rights are those requested by the "scope" parameter in the Access Token Request if present therein, or the default access rights otherwise.

* The "rs_cnf" parameter defined in [RFC9201] can be included. When present, it specifies information about the public key that DEV2 uses to authenticate.

* The "rev_audience" parameter defined in Section 2.1 can be included and specifies an identifier of DEV1 (i.e., the access token’s reverse audience).

  If the "rev_audience" parameter is present in the Access Token Response and it was also present in the Access Token Request, then the parameter in the Access Token Response MUST have the same value specified by the parameter in the Access Token Request.

* The "rev_scope" parameter defined in Section 2.2 can be included and specifies the access rights that AS has granted to DEV2 (i.e., the access token’s audience) for accessing protected resources at DEV1.

The "rev_scope" parameter MUST be present if: i) it was present in the Access Token Request and the access rights granted to DEV2 are different from the requested ones; or ii) it was not present in the Access Token Request and the access rights granted to DEV2 are different from the default ones.

If the "rev_scope" parameter is not present, then the access rights granted to DEV2 are those requested by the "rev_scope" parameter in the Access Token Request if present therein, or the default access rights otherwise.

The issued access token MUST include information about the reverse audience and reverse scope pertaining to the secondary access control direction. In particular:

* The access token MUST contain a claim specifying the identifier of DEV1 (i.e., the access token’s reverse audience).

  If the Access Token Response includes the "rev_audience" parameter, then the claim specifies the same information conveyed by that parameter.

  If this is not the case, then the claim specifies the same information conveyed by the "rev_audience" parameter of the Access Token Request if present therein, or the default identifier of DEV1 otherwise.

  When CWTs are used as access tokens, this information MUST be transported in the "rev_aud" claim registered in Section 8.4.

* The access token MUST contain a claim specifying the access rights that AS has granted to DEV2 (i.e., the access token’s audience) for accessing protected resources at DEV1.

  If the Access Token Response includes the "rev_scope" parameter, then the claim specifies the same information conveyed by that parameter.

  If this is not the case, then the claim specifies the same information conveyed by the "rev_scope" parameter of the Access Token Request if present therein, or the default access rights for DEV2 to access DEV1 otherwise.

  When CWTs are used as access tokens, this information MUST be transported in the "rev_scope" claim registered in Section 8.4.

4.3. Access to Protected Resources

As to the secure communication association between DEV1 and DEV2, its establishment and maintenance do not deviate from what is defined in the profile of ACE used by DEV1 and DEV2.

Furthermore, communications between DEV1 and DEV2 MUST rely on such secure communication association for both directions of access control, i.e., when DEV1 accesses protected resources at DEV2 and vice versa.

After having received a successful Access Token Response from AS, DEV1 MUST maintain and enforce the information about the access rights granted to DEV2 and pertaining to the secondary access control direction.

In particular, DEV1 MUST prevent DEV2 from accessing protected resources at DEV1, in case access requests from DEV2 are not authorized as per the reverse scope specified by the issued access token, or after having purged the issued access token (e.g., following its expiration of revocation).

As to maintaining and enforcing the information about the access rights granted to DEV1 and pertaining to the primary access control direction, there is no deviation from what is defined in the ACE framework and the profile of ACE used by DEV1 and DEV2.

5. Scenario with Two Authorization Servers

TBD

6. Practical Considerations

When enforcing bidirectional access control by means of a single access token, the following considerations hold.

* The access token can be uploaded to the ACE RS DEV2 by the ACE client DEV1 per the original ACE workflow, or instead by the AS that has issued the access token per the Short Distribution Chain (SDC) workflow defined in [I-D.ietf-ace-workflow-and-params].

* Since the access token is requested by the ACE client DEV1, only DEV1 can request for a new access token in the same token series, in order to dynamically update the access rights concerning its own access to protected resources hosted by DEV2 (on the primary access control direction) and/or the access rights concerning the access of DEV2 to protected resources hosted by DEV1 (on the secondary access control direction).

7. Security Considerations

The same security considerations from the ACE framework for Authentication and Authorization [RFC9200] apply to this document, together with those from the specific profile of ACE used.

Editor’s note: add more security considerations.

8. IANA Considerations

This document has the following actions for IANA.

Note to RFC Editor: Please replace all occurrences of "[RFC-XXXX]" with the RFC number of this specification and delete this paragraph.

8.1. OAuth Parameters Registry

IANA is asked to add the following entries to the "OAuth Parameters" registry within the "OAuth Parameters" registry group.

* Name: rev_audience
* Parameter Usage Location: token request and token response
* Change Controller: IETF
* Reference: [RFC-XXXX]

* Name: rev_scope
* Parameter Usage Location: token request and token response
* Change Controller: IETF
* Reference: [RFC-XXXX]

8.2. OAuth Parameters CBOR Mappings Registry

IANA is asked to add the following entries to the "OAuth Parameters CBOR Mappings" registry within the "Authentication and Authorization for Constrained Environments (ACE)" registry group, following the procedure specified in [RFC9200].

* Name: rev_audience
* CBOR Key: TBD

* Value Type: text string
* Reference: [RFC-XXXX]
* Original Specification: [RFC-XXXX]

* Name: rev_scope
* CBOR Key: TBD
* Value Type: text string or byte string
* Reference: [RFC-XXXX]
* Original Specification: [RFC-XXXX]

8.3. JSON Web Token Claims Registry

IANA is asked to add the following entries to the "JSON Web Token Claims" registry within the "JSON Web Token (JWT)" registry group, following the procedure specified in [RFC7519].

* Claim Name: rev_aud
* Claim Description: The reverse audience of an access token
* Change Controller: IETF
* Reference: [RFC-XXXX]

* Claim Name: rev_scope
* Claim Description: The reverse scope of an access token
* Change Controller: IETF
* Reference: [RFC-XXXX]

8.4. CBOR Web Token (CWT) Claims Registry

IANA is asked to add the following entries to the "CBOR Web Token (CWT) Claims" registry within the "CBOR Web Token (CWT) Claims" registry group, following the procedure specified in [RFC8392].

* Claim Name: rev_aud
* Claim Description: The reverse audience of an access token
* JWT Claim Name: rev_aud
* Claim Key: TBD
* Claim Value Type: text string
* Change Controller: IETF
* Reference: Section 3 of [RFC-XXXX]

* Claim Name: rev_scope
* Claim Description: The reverse scope of an access token
* JWT Claim Name: rev_scope
* Claim Key: TBD
* Claim Value Type: text string or byte string
* Change Controller: IETF
* Reference: Section 3 of [RFC-XXXX]

9. References

9.1. Normative References

[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/rfc/rfc2119>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/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/rfc/rfc7252>.

[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/rfc/rfc7519>.

[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/rfc/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/rfc/rfc8392>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

[RFC9200] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth)", RFC 9200, DOI 10.17487/RFC9200, August 2022, <https://www.rfc-editor.org/rfc/rfc9200>.

[RFC9201] Seitz, L., "Additional OAuth Parameters for Authentication and Authorization for Constrained Environments (ACE)", RFC 9201, DOI 10.17487/RFC9201, August 2022, <https://www.rfc-editor.org/rfc/rfc9201>.

9.2. Informative References

[I-D.ietf-ace-edhoc-oscore-profile] Selander, G., Mattsson, J. P., Tiloca, M., and R. H旦glund, "Ephemeral Diffie-Hellman Over COSE (EDHOC) and Object

Security for Constrained Environments (OSCORE) Profile for Authentication and Authorization for Constrained Environments (ACE)", Work in Progress, Internet-Draft, draft-ietf-ace-edhoc-oscore-profile-08, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-edhoc-oscore-profile-08>.

[I-D.ietf-ace-group-oscore-profile] Tiloca, M., H旦glund, R., and F. Palombini, "The Group Object Security for Constrained RESTful Environments (Group OSCORE) Profile of the Authentication and Authorization for Constrained Environments (ACE) Framework", Work in Progress, Internet-Draft, draft-ietf-ace-group-oscore-profile-04, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-group-oscore-profile-04>.

[I-D.ietf-ace-workflow-and-params] Tiloca, M. and G. Selander, "Short Distribution Chain (SDC) Workflow and New OAuth Parameters for the Authentication and Authorization for Constrained Environments (ACE) Framework", Work in Progress, Internet-Draft, draft-ietf-ace-workflow-and-params-05, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-workflow-and-params-05>.

[RFC9202] Gerdes, S., Bergmann, O., Bormann, C., Selander, G., and L. Seitz, "Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)", RFC 9202, DOI 10.17487/RFC9202, August 2022, <https://www.rfc-editor.org/rfc/rfc9202>.

[RFC9203] Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "The Object Security for Constrained RESTful Environments (OSCORE) Profile of the Authentication and Authorization for Constrained Environments (ACE) Framework", RFC 9203, DOI 10.17487/RFC9203, August 2022, <https://www.rfc-editor.org/rfc/rfc9203>.

[RFC9431] Sengul, C. and A. Kirby, "Message Queuing Telemetry Transport (MQTT) and Transport Layer Security (TLS) Profile of Authentication and Authorization for Constrained Environments (ACE) Framework", RFC 9431, DOI 10.17487/RFC9431, July 2023, <https://www.rfc-editor.org/rfc/rfc9431>.

[RFC9770] Tiloca, M., Palombini, F., Echeverria, S., and G. Lewis, "Notification of Revoked Access Tokens in the Authentication and Authorization for Constrained Environments (ACE) Framework", RFC 9770, DOI 10.17487/RFC9770, June 2025, <https://www.rfc-editor.org/rfc/rfc9770>.

Appendix A. CDDL Model

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

```
; OAuth Parameters CBOR Mappings
rev_audience = 56
rev_scope_param = 57

; CBOR Web Token (CWT) Claims
rev_aud = 43
rev_scope_claim = 44
```

Figure 2: CDDL Model

Acknowledgments

The authors sincerely thank Rikard H旦glund and Dave Robin for their comments and feedback.

This work was supported by the Sweden’s Innovation Agency VINNOVA within the EUREKA CELTIC-NEXT project CYPRESS.

Authors’ Addresses

Marco Tiloca
RISE AB
Isafjordsgatan 22
SE-164 40 Kista
Sweden
Email: marco.tiloca@ri.se

G旦ran Selander
Ericsson AB
Torshamnsgatan 23
SE-164 40 Kista
Sweden
Email: goran.selander@ericsson.com