ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 26 June 2022

F. Palombini
Ericsson AB
M. Tiloca
RISE AB

23 December 2021

Key Provisioning for Group Communication using ACE draft-ietf-ace-key-groupcomm-15

Abstract

This document defines how to use the Authentication and Authorization for Constrained Environments (ACE) framework to distribute keying material and configuration parameters for secure group communication. Candidate group members acting as Clients and authorized to join a group can do so by interacting with a Key Distribution Center (KDC) acting as Resource Server, from which they obtain the keying material to communicate with other group members. While defining general message formats as well as the interface and operations available at the KDC, this document supports different approaches and protocols for secure group communication. Therefore, details are delegated to separate application profiles of this document, as specialized instances that target a particular group communication approach and define how communications in the group are protected. Compliance requirements for such application profiles are also specified.

Discussion Venues

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

Source for this draft and an issue tracker can be found at https://github.com/ace-wg/ace-key-groupcomm.

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 26 June 2022.

Copyright Notice

Table of Contents

1. Introduction

This document builds on the Authentication and Authorization for Constrained Environments (ACE) framework and defines how to request, distribute and renew keying material and configuration parameters to protect message exchanges in a group communication environment.

Candidate group members acting as Clients and authorized to join a group can interact with the Key Distribution Center (KDC) acting as Resource Server and responsible for that group, in order to obtain the necessary keying material and parameters to communicate with other group members.

In particular, this document defines the operations and interface available at the KDC, as well as general message formats for the interactions between Clients and KDC. At the same time, communications in the group can rely on different approaches, e.g., based on multicast [I-D.ietf-core-groupcomm-bis] or on publish-subscribe messaging [I-D.ietf-core-coap-pubsub], and can be protected in different ways.

Therefore, this document delegates details on the communication and security approaches used in a group to separate application profiles. These are specialized instances of this document, targeting a particular group communication approach and defining how communications in the group are protected, as well as the specific keying material and configuration parameters provided to group members. In order to ensure consistency and aid the development of such application profiles, this document defines a number of related compliance requirements (see Appendix A).

If the application requires backward and forward security, new keying material is generated and distributed to the group upon membership changes (rekeying). A group rekeying scheme performs the actual distribution of the new keying material, by rekeying the current group members when a new Client joins the group, and the remaining group members when a Client leaves the group. This can rely on different approaches, including efficient group rekeying schemes such as [RFC2093], [RFC2094] and [RFC2627].

Consistently with what is recommeded in the ACE framework, this document uses CBOR [RFC8949] for data encoding. However, using JSON [RFC8259] instead of CBOR is possible, by relying on the conversion method specified in Sections 6.1 and 6.2 of [RFC8949].

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 [I-D.ietf-ace-oauth-authz] and in the Authorization Information Format (AIF) [I-D.ietf-ace-aif] to express authorization information. 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).

* The terms and concepts described in CoAP [RFC7252]. Unless otherwise indicated, the term "endpoint" is used here following its OAuth definition, aimed at denoting resources such as /token and /introspect at the AS, and /authz-info at the RS. This document does not use the CoAP definition of "endpoint", which is "An entity participating in the CoAP protocol".

* The terms and concepts described in CBOR [RFC8949] and COSE [I-D.ietf-cose-rfc8152bis-struct] [I-D.ietf-cose-rfc8152bis-algs] [I-D.ietf-cose-countersign].

A principal interested to participate in group communication as well as already participating as a group member is interchangeably denoted as "Client" or "node".

Furthermore, this document uses "names" or "identifiers" for groups and nodes. Their different meanings are summarized below.

* Group: a set of nodes that share common keying material and security parameters used to protect their communications with one another. That is, the term refers to a "security group".

  This is not to be confused with an "application group", which has relevance at the application level and whose members share a common pool of resources or content. Examples of application groups are the set of all nodes deployed in a same physical room, or the set of nodes registered to a pub-sub topic.

  The same security group might be associated to multiple application groups. Also, the same application group can be associated to multiple security groups. Further details and considerations on the mapping between the two types of group are out of the scope of this document.

* Key Distribution Center (KDC): the entity responsible for managing one or multiple groups, with particular reference to the group membership and the keying material to use for protecting group communications.

* Group name: the invariant once established identifier of a group. It is used in the interactions between Client, AS and RS to identify a group. A group name is always unique among the group names of the existing groups under the same KDC.

* GROUPNAME: the invariant once established text string used in URIs. GROUPNAME uniquely maps to the group name of a group, although they do not necessarily coincide.

* Group identifier: the identifier of the group keying material used in a group. Unlike group name and GROUPNAME, this identifier changes over time, when the group keying material is updated.

* Node name: the invariant once established identifier of a node. It is used in the interactions between Client and RS and to identify a member of a group. Within the same group, a node name is always unique among the node names of all the current members of that group.

* NODENAME: the invariant once established text string used in URIs to identify a member a group. Its value coincides with the node name of the associated group member.

This document additionally uses the following terminology:

* Transport profile, to indicate a profile of ACE as per Section 5.8.4.3 of [I-D.ietf-ace-oauth-authz]. A transport profile specifies the communication protocol and communication security protocol between an ACE Client and Resource Server, as well as proof-of-possession methods, if it supports proof-of-possession access tokens, etc. Transport profiles of ACE include, for instance, [I-D.ietf-ace-oscore-profile], [I-D.ietf-ace-dtls-authorize] and [I-D.ietf-ace-mqtt-tls-profile].

* Application profile, that defines how applications enforce and use supporting security services they require. These services may include, for instance, provisioning, revocation and distribution of keying material. An application profile may define specific procedures and message formats.

2. Overview

The full procedure can be separated in two phases: the first one follows the ACE Framework, between Client, AS and KDC; the second one is the key distribution between Client and KDC. After the two phases are completed, the Client is able to participate in the group communication, via a Dispatcher entity.

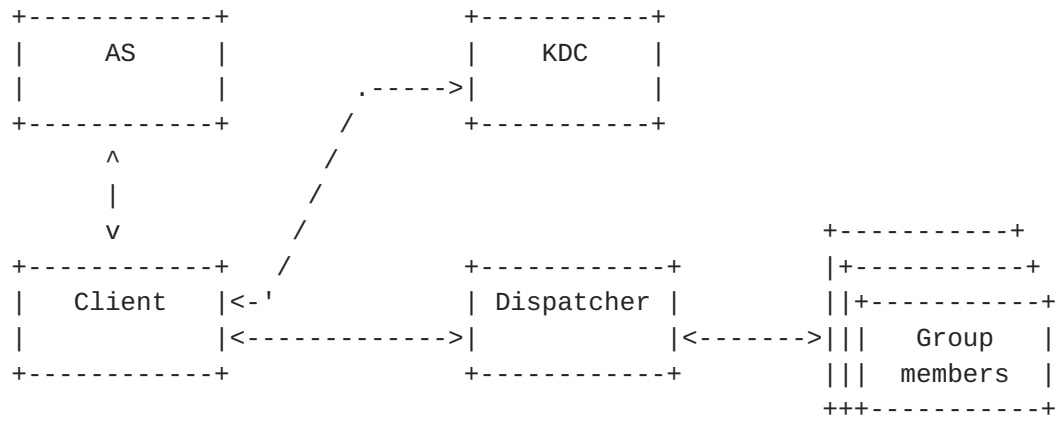


Figure 1: Key Distribution Participants

The following participants (see Figure 1) take part in the authorization and key distribution.

* Client (C): node that wants to join a group and take part in group communication with other group memebrs. Within the group, the Client can have different roles.

* Authorization Server (AS): as per the AS defined in the ACE Framework, it enforces access policies, and knows if a node is allowed to join a given group with write and/or read rights.

* Key Distribution Center (KDC): maintains the keying material to protect group communications, and provides it to Clients authorized to join a given group. During the first part of the exchange (Section 3), it takes the role of the RS in the ACE Framework. During the second part (Section 4), which is not based on the ACE Framework, it distributes the keying material. In addition, it provides the latest keying material to group members when requested or, if required by the application, when membership changes.

* Dispatcher: entity through which the Clients communicate with the group, when sending a message intended to multiple group members. That is, the Dispatcher distributes such a one-to-many message to the group members as intended recipients. A single-recipient message intended to only one group member may be delivered by alternative means, with no assistance from the Dispatcher.

  Examples of a Dispatcher are: the Broker in a pub-sub setting; a relayer for group communication that delivers group messages as multiple unicast messages to all group members; an implicit entity as in a multicast communication setting, where messages are transmitted to a multicast IP address and delivered on the transport channel.

This document specifies a mechanism for:

* Authorizing a Client to join the group (Section 3), and providing it with the group keying material to communicate with the other group members (Section 4).

* Allowing a group member to retrieve group keying material (Section 4.8.1.1 and Section 4.8.2.1).

* Allowing a group member to retrieve public keys of other group members (Section 4.4.1.1) and to provide an updated public key (Section 4.9.1.1).

* Allowing a group member to leave the group (Section 5).

* Evicting a group member from the group (Section 5).

* Renewing and re-distributing the group keying material (rekeying) upon a membership change in the group (Section 4.8.3.1 and Section 5).

Figure 2 provides a high level overview of the message flow for a node joining a group. The message flow can be expanded as follows.

1. The joining node requests an access token from the AS, in order to access one or more group-membership resources at the KDC and hence join the associated groups.

   This exchange between Client and AS MUST be secured, as specified by the transport profile of ACE used between Client and KDC. Based on the response from the AS, the joining node will establish or continue using a secure communication association with the KDC.

2. The joining node transfers authentication and authorization information to the KDC, by transferring the obtained access token. This is typically achieved by including the access token in a request sent to the /authz-info endpoint at the KDC.

   Once this exchange is completed, the joining node MUST have a secure communication association established with the KDC, before joining a group under that KDC.

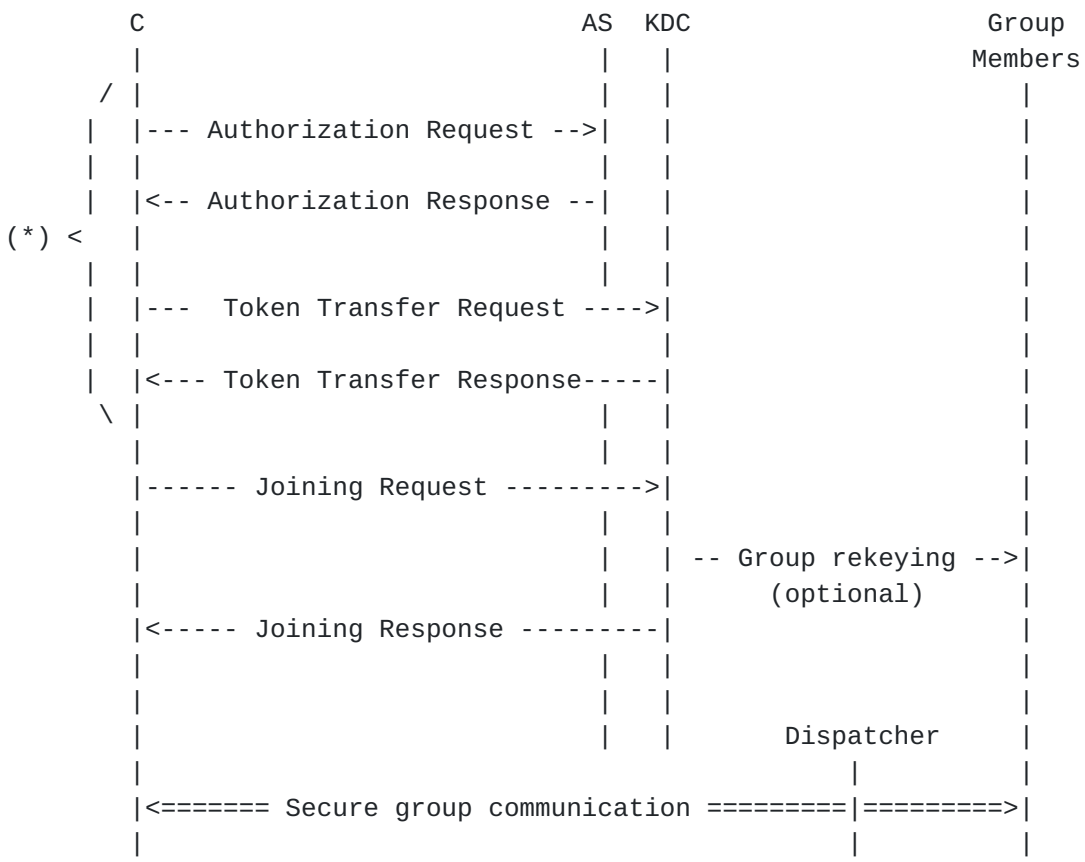
   This exchange and the following secure communications between the Client and the KDC MUST occur in accordance with the transport profile of ACE used between Client and KDC, such as the DTLS transport profile [I-D.ietf-ace-dtls-authorize] and OSCORE transport profile [I-D.ietf-ace-oscore-profile] of ACE.

3. The joining node starts the joining process to become a member of the group, by sending a request to the related group-membership resource at the KDC. Based on the application requirements and policies, the KDC may perform a group rekeying, by generating new group keying material and distributing it to the current group members through the rekeying scheme used in the group.

   At the end of the joining process, the joining node has received from the KDC the parameters and group keying material to securely communicate with the other group members. Also, the KDC has stored the association between the authorization information from the access token and the secure session with the joining node.

4. The joining node and the KDC maintain the secure association, to support possible future communications. These especially include key management operations, such as retrieval of updated keying material or participation to a group rekeying process.

5. The joining node can communicate securely with the other group members, using the keying material provided in step 3.



(*) Defined in the ACE framework

Figure 2: Message Flow Upon New Node's Joining

3. Authorization to Join a Group

This section describes in detail the format of messages exchanged by the participants when a node requests access to a given group. This exchange is based on ACE [I-D.ietf-ace-oauth-authz].

As defined in [I-D.ietf-ace-oauth-authz], the Client requests the AS for the authorization to join the group through the KDC (see Section 3.1). If the request is approved and authorization is granted, the AS provides the Client with a proof-of-possession access token and parameters to securely communicate with the KDC (see Section 3.2).

Communications between the Client and the AS MUST be secured, according to what is defined by the used transport profile of ACE. The Content-Format used in the message also depends on the used transport profile of ACE. For example, it can be application/ace+cbor for the first two messages and application/cwt for the third message, which are defined in the ACE framework.

The transport profile of ACE also defines a number of details such as the communication and security protocols used with the KDC (see Appendix C of [I-D.ietf-ace-oauth-authz]).

Figure 3 gives an overview of the exchange described above.

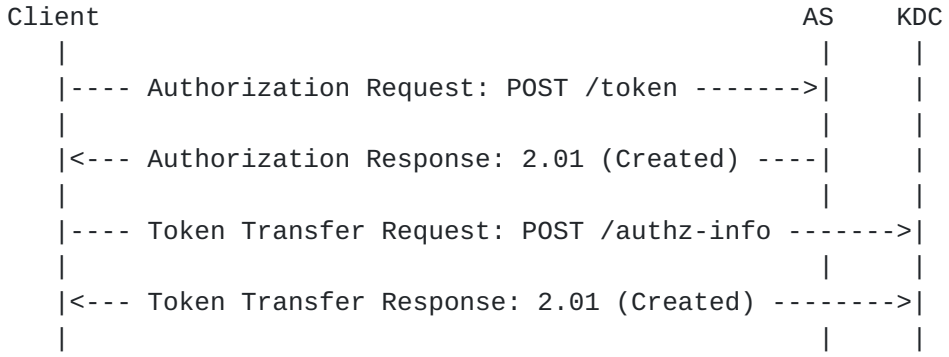


Figure 3: Message Flow of Join Authorization

3.1. Authorization Request

The Authorization Request sent from the Client to the AS is defined in Section 5.8.1 of [I-D.ietf-ace-oauth-authz] and MAY contain the following parameters, which, if included, MUST have format and value as specified below.

* 'scope', specifying the name of the groups that the Client requests to access, and optionally the roles that the Client requests to have in those groups.

  This parameter is encoded as a CBOR byte string, which wraps a CBOR array of one or more scope entries. All the scope entries are specified according to a same format, i.e. either the AIF format or the textual format defined below.

  - If the AIF format is used, each scope entry is encoded as specified in [I-D.ietf-ace-aif]. The object identifier "Toid" corresponds to the group name and MUST be encoded as a CBOR text string. The permission set "Tperm" indicates the roles that the Client wishes to take in the group.

    The AIF format is the default format for application profiles of this specification, and is preferable for those that aim to a compact encoding of scope. This is desirable especially for application profiles defining several roles, with the Client possibly requesting for multiple roles combined.

Figure 4 shows an example in CDDL notation [RFC8610] where scope uses the AIF format.

- If the textual format is used, each scope entry is a CBOR array formatted as follows.

  o As first element, the group name, encoded as a CBOR text string.

  o Optionally, as second element, the role or CBOR array of roles that the Client wishes to take in the group. This element is optional since roles may have been pre-assigned to the Client, as associated to its verifiable identity credentials. Alternatively, the application may have defined a single, well-known role for the target resource(s) and audience(s).

  Figure 5 shows an example in CDDL notation where scope uses the textual format, with group name and role identifiers encoded as CBOR text strings.

  It is REQUIRED of application profiles of this specificaton to specify the exact format and encoding of scope (REQ1). This includes defining the set of possible roles and their identifiers, as well as the corresponding encoding to use in the scope entries according to the used scope format.

  If the application profile uses the AIF format, it is also REQUIRED to register its specific instance of "Toid" and "Tperm", as well as the corresponding Media Type and Content-Format, as per the guidelines in [I-D.ietf-ace-aif] (REQ2).

  If the application profile uses the textual format, it MAY additionally specify CBOR values to use for abbreviating the role identifiers (OPT1).

* 'audience', with an identifier of the KDC.

As defined in [I-D.ietf-ace-oauth-authz], other additional parameters can be included if necessary.

```
gname = tstr

permissions = uint . bits roles

roles = &(
   Requester: 1,
   Responder: 2,
   Monitor: 3,
   Verifier: 4
)

scope_entry = AIF_Generic<gname, permissions>

scope = << [ + scope_entry ] >>
```

Figure 4: Example of scope using the AIF format

```
gname = tstr

role = tstr

scope_entry = [ gname , ? ( role / [ 2*role ] ) ]

scope = << [ + scope_entry ] >>
```

Figure 5: Example of scope using the textual format, with the group name and role identifiers encoded as text strings

3.2. Authorization Response

The AS processes the Authorization Request as defined in Section 5.8.2 of [I-D.ietf-ace-oauth-authz], especially verifying that the Client is authorized to access the specified groups with the requested roles, or possibly a subset of those.

In case of successful verification, the Authorization Response sent from the AS to the Client is also defined in Section 5.8.2 of [I-D.ietf-ace-oauth-authz]. Note that the parameter 'expires_in' MAY be omitted if the application defines how the expiration time is communicated to the Client via other means, or if it establishes a default value.

Additionally, when included, the following parameter MUST have the corresponding values:

* 'scope' has the same format and encoding of 'scope' in the Authorization Request, defined in Section 3.1. If this parameter is not present, the granted scope is equal to the one requested in Section 3.1.

The proof-of-possession access token (in 'access_token' above) MUST contain the following parameters:

* a confirmation claim (see for example 'cnf' defined in Section 3.1 of [RFC8747] for CWT);

* an expiration time claim (see for example 'exp' defined in Section 3.1.4 of [RFC8392] for CWT);

* a scope claim (see for example 'scope' registered in Section 8.14 of [I-D.ietf-ace-oauth-authz] for CWT).

  This claim specifies the same access control information as in the 'scope' parameter of the Authorization Response, if the parameter is present in the message, or as in the 'scope' parameter of the Authorization Request otherwise.

  By default, this claim has the same encoding as the 'scope' parameter in the Authorization Request, defined in Section 3.1.

  Optionally, an alternative extended format of scope defined in Section 7 can be used. This format explicitly signals the semantics used to express the actual access control information, and according to which this has to be parsed. This enables a Resource Server to correctly process a received access token, also in case:

  - The Resource Server implements a KDC that supports multiple application profiles of this specification, using different scope semantics; and/or

  - The Resource Server implements further services beyond a KDC for group communication, using different scope semantics.

  If the Authorization Server is aware that this applies to the Resource Server for which the access token is issued, the Authorization Server SHOULD use the extended format of scope defined in Section 7.

The access token MAY additionally contain other claims that the transport profile of ACE requires, or other optional parameters.

When receiving an Authorization Request from a Client that was previously authorized, and for which the AS still owns a valid non-expired access token, the AS MAY reply with that token. Note that it is up to application profiles of ACE to make sure that re-posting the same token does not cause re-use of keying material between nodes (for example, that is done with the use of random nonces in [I-D.ietf-ace-oscore-profile]).

3.3. Token Transferring

The Client sends a Token Transfer Request to the KDC, i.e., a CoAP POST request including the access token and targeting the authz-info endpoint (see Section 5.10.1 of [I-D.ietf-ace-oauth-authz]).

Note that this request deviates from the one defined in [I-D.ietf-ace-oauth-authz], since it allows to ask the KDC for additional information concerning the public keys used in the group to ensure source authentication, as well as for possible additional group parameters.

The joining node MAY ask for this information from the KDC through the same Token Transfer Request. In this case, the message MUST have Content-Format set to application/ace+cbor defined in Section 8.16 of [I-D.ietf-ace-oauth-authz], and the message payload MUST be formatted as a CBOR map, which MUST include the access token. The CBOR map MAY additionally include the following parameter, which, if included, MUST have format and value as specified below.

* 'sign_info' defined in Section 3.3.1, specifying the CBOR simple value 'null' (0xf6) to request information about the signature algorithm, signature algorithm parameters, signature key parameters and about the exact encoding of public keys used in the groups that the Client has been authorized to join.

Alternatively, such information may be pre-configured on the joining node, or may be retrieved by alternative means. For example, the joining node may have performed an early group discovery process and obtained the link to the associated group-membership resource at the KDC, together with attributes descriptive of the group configuration (see, e.g., [I-D.tiloca-core-oscore-discovery]).

After successful verification, the Client is authorized to receive the group keying material from the KDC and join the group. Hence, the KDC replies to the Client with a Token Transfer Response, i.e., a CoAP 2.01 (Created) response.

The Token Transfer Response MUST have Content-Format "application/ace+cbor", and its payload is a CBOR map. Note that this deviates from what is defined in the ACE framework, where the response from the authz-info endpoint is defined as conveying no payload (see Section 5.10.1 of [I-D.ietf-ace-oauth-authz]).

If the access token contains a role that requires the Client to send its own public key to the KDC when joining the group, the CBOR map MUST include the parameter 'kdcchallenge' defined in Section 3.3.2, specifying a dedicated challenge N_S generated by the KDC.

Later, when joining the group (see Section 4.3.1.1), the Client uses the 'kdcchallenge' value and additional information to build a proof-of-possession (PoP) input. This is in turn used to compute a PoP evidence, which the Client also provides to the Group Manager in order to prove possession of its own private key (see the 'client_cred_verify' parameter in Section 4.3.1).

The KDC MUST store the 'kdcchallenge' value associated to the Client at least until it receives a Joining Request from it (see Section 4.3.1.1), to be able to verify the PoP evidence provided during the join process, and thus that the Client possesses its own private key.

The same 'kdcchallenge' value MAY be reused several times by the Client, to generate a new PoP evidence, e.g., in case the Client provides the Group Manager with a new public key while being a group member (see Section 4.9.1.1), or joins a different group where it intends to use a different public key. Therefore, it is RECOMMENDED that the KDC keeps storing the 'kdcchallenge' value after the first join is processed as well. If the KDC has already discarded the 'kdcchallenge' value, that will trigger an error response with a newly generated 'kdcchallenge' value that the Client can use to restart the join process, as specified in Section 4.3.1.1.

If 'sign_info' is included in the Token Transfer Request, the KDC SHOULD include the 'sign_info' parameter in the Token Transfer Response, as per the format defined in Section 3.3.1. Note that the field 'id' of each 'sign_info_entry' specifies the name, or array of group names, for which that 'sign_info_entry' applies to. As an exception, the KDC MAY omit the 'sign_info' parameter in the Token Transfer Response even if 'sign_info' is included in the Token Transfer Request, in case none of the groups that the Client is authorized to join uses signatures to achieve source authentication.

Note that the CBOR map specified as payload of the 2.01 (Created) response may include further parameters, e.g., according to the used transport profile of ACE. Application profiles of this specification MAY define additional parameters to use within this exchange (OPT2).

Application profiles of this specification MAY define alternative specific negotiations of parameter values for the signature algorithm and signature keys, if 'sign_info' is not used (OPT3).

If allowed by the used transport profile of ACE, the Client may provide the Access Token to the KDC by other means than the Token Transfer Request. An example is the DTLS transport profile of ACE, where the Client can provide the access token to the KDC during the secure session establishment (see Section 3.3.2 of [I-D.ietf-ace-dtls-authorize]).

3.3.1. 'sign_info' Parameter

The 'sign_info' parameter is an OPTIONAL parameter of the request and response messages exchanged between the Client and the authz-info endpoint at the RS (see Section 5.10.1. of [I-D.ietf-ace-oauth-authz]).

This parameter allows the Client and the RS to exchange information about a signature algorithm and about public keys to accordingly use for signature verification. Its exact semantics and content are application specific.

In this specification and in application profiles building on it, this parameter is used to exchange information about the signature algorithm and about public keys to be used with it, in the groups indicated by the transferred acces token as per its 'scope' claim (see Section 3.2).

When used in the Token Transfer Request sent to the KDC (see Section 3.3), the 'sign_info' parameter specifies the CBOR simple value 'null' (0xf6). This is done to ask for information about the signature algorithm and about the public keys used in the groups that the Client has been authorized to join - or to have a more restricted interaction as per its granted roles (e.g., the Client is an external signature verifier).

When used in the following Token Transfer Response from the KDC (see Section 3.3), the 'sign_info' parameter is a CBOR array of one or more elements. The number of elements is at most the number of groups that the Client has been authorized to join - or to have a more restricted interaction (see above). Each element contains information about signing parameters and about public keys for one or more groups, and is formatted as follows.

* The first element 'id' is a group name or an array of group names, associated to groups for which the next four elements apply. In the following, each specified group name is referred to as 'gname'.

* The second element 'sign_alg' is an integer or a text string if the POST request included the 'sign_info' parameter with value the CBOR simple value 'null' (0xf6), and indicates the signature algorithm used in the groups identified by the 'gname' values. It is REQUIRED of the application profiles to define specific values that this parameter can take (REQ3), selected from the set of signing algorithms of the COSE Algorithms registry [COSE.Algorithms].

* The third element 'sign_parameters' is a CBOR array indicating the parameters of the signature algorithm used in the groups identified by the 'gname' values. Its content depends on the value of 'sign_alg'. It is REQUIRED of the application profiles to define the possible values and structure for the elements of this parameter (REQ4).

* The fourth element 'sign_key_parameters' is a CBOR array indicating the parameters of the key used with the signature algorithm, in the groups identified by the 'gname' values. Its content depends on the value of 'sign_alg'. It is REQUIRED of the application profiles to define the possible values and structure for the elements of this parameter (REQ5).

* The fifth element 'pub_key_enc' parameter is either a CBOR integer indicating the encoding of public keys used in the groups identified by the 'gname' values, or has value the CBOR simple value 'null' (0xf6) indicating that the KDC does not act as repository of public keys for group members. Its acceptable integer values are taken from the 'Label' column of the "COSE Header Parameters" registry [COSE.Header.Parameters]. It is REQUIRED of the application profiles to define specific values to use for this parameter, consistently with the acceptable formats of public keys (REQ6).

The CDDL notation [RFC8610] of the 'sign_info' parameter is given below.

```
sign_info = sign_info_req / sign_info_resp

sign_info_req  = nil                    ; in the Token Transfer
                                        ; Request to the KDC

sign_info_resp = [ + sign_info_entry ] ; in the Token Transfer
                                        ; Response from the KDC

sign_info_entry =
[
  id : gname / [ + gname ],
  sign_alg : int / tstr,
  sign_parameters : [ any ],
  sign_key_parameters : [ any ],
  pub_key_enc = int / nil
]

gname = tstr
```

This format is consistent with every signature algorithm currently defined in [I-D.ietf-cose-rfc8152bis-algs], i.e., with algorithms that have only the COSE key type as their COSE capability. Appendix B describes how the format of each 'sign_info_entry' can be generalized for possible future registered algorithms having a different set of COSE capabilities.

3.3.2. 'kdcchallenge' Parameter

The 'kdcchallenge' parameter is an OPTIONAL parameter of response message returned from the authz-info endpoint at the RS, as defined in Section 5.10.1 of [I-D.ietf-ace-oauth-authz]. This parameter contains a challenge generated by the RS and provided to the Client.

In this specification and in application profiles building on it, the Client may use this challenge to prove possession of its own private key in the Joining Request (see the 'client_cred_verify' parameter in Section 4.3.1).

4. KDC Functionalities

This section describes the functionalities provided by the KDC, as related to the provisioning of the keying material as well as to the group membership management.

In particular, this section defines the interface available at the KDC; specifies the handlers of each resource provided by the KDC interface; and describes how Clients interact with those resources to join a group and to perform additional operations as group members.

As most important operation after trasferring the access token to the KDC, the Client can perform a "Joining" exchange with the KDC, by specifying the group it requests to join (see Section 4.3.1.1). Then, the KDC verifies the access token and that the Client is authorized to join the specified group. If so, the KDC provides the Client with the keying material to securely communicate with the other members of the group.

Later on as a group member, the Client can also rely on the interface at the KDC to perform additional operations, consistently with the roles it has in the group.

4.1. Interface at the KDC

The KDC provides its interface by hosting the following resources. Note that the root url-path "ace-group" used hereafter is a default name; implementations are not required to use this name, and can define their own instead. The Interface Description (if=) Link Target Attribute value "ace.group" is registered in Section 11.5 and can be used to describe this interface.

If request messages sent to the KDC as well as success response messages from the KDC include a payload and specify a Content-Format, those messages MUST have Content-Format set to application/ace-groupcomm+cbor, defined in Section 11.2. CBOR labels for the message parameters are defined in Section 8.

* /ace-group : this resource is invariant once established, and indicates that this specification is used. If other applications run on a KDC implementing this specification and use this same resource, those applications will collide, and a mechanism will be needed to differentiate the endpoints.

  A Client can access this resource in order to retrieve a set of group names, each corresponding to one of the specified group identifiers. This operation is described in Section 4.2.1.1.

* /ace-group/GROUPNAME : one such sub-resource to /ace-group is hosted for each group with name GROUPNAME that the KDC manages, and contains the symmetric group keying material for that group.

A Client can access this resource in order to join the group with name GROUPNAME, or later as a group member to retrieve the current group keying material. These operations are described in Section 4.3.1.1 and Section 4.3.2.1, respectively.

If the value of the GROUPNAME URI path and the group name in the access token scope ('gname' in Section 3.2) are not required to coincide, the KDC MUST implement a mechanism to map the GROUPNAME value in the URI to the group name, in order to refer to the correct group (REQ7).

* /ace-group/GROUPNAME/pub-key : this resource is invariant once established, and contains the public keys of all the members of the group with name GROUPNAME.

  This resource is created only in case the KDC acts as repository of public keys for group members.

  A Client can access this resource in order to retrieve the public keys of other group members, in addition to when joining the group. That is, the Client can retrieve the public keys of all the current group members, or a subset of them by specifying filter criteria. These operations are described in Section 4.4.2.1 and Section 4.4.1.1, respectively.

  Clients may be authorized to access this resource even without being group members, e.g., if authorized to be external signature verifiers for the group.

* ace-group/GROUPNAME/kdc-pub-key : this resource is invariant once established, and contains the public key of the KDC for the group with name GROUPNAME.

  This resource is created only in case the KDC has an associated public key and this is required for the correct group operation. It is REQUIRED of application profiles to define whether the KDC has such an associated public key (REQ8).

  A Client can interact with this resource in order to retrieve the current public key of the KDC, in addition to when joining the group.

  Clients may be authorized to access this resource even without being group members, e.g., if authorized to be external signature verifiers for the group.

* /ace-group/GROUPNAME/policies : this resource is invariant once established, and contains the group policies of the group with name GROUPNAME.

  A Client can access this resource as a group member in order to retrieve the group policies. This operation is described in Section 4.6.1.1.

* /ace-group/GROUPNAME/num : this resource is invariant once established, and contains the current version number for the symmetric group keying material of the group with name GROUPNAME.

  A Client can access this resource as a group member in order to retrieve the version number of the keying material currently used in the group. This operation is described in Section 4.7.1.1.

* /ace-group/GROUPNAME/nodes/NODENAME : one such sub-resource of /ace-group/GROUPNAME is hosted for each group member of the group with name GROUPNAME. Each of such resources is identified by the node name NODENAME of the associated group member, and contains the group keying material and the individual keying material for that group member.

  A Client as a group member can access this resource in order to retrieve the current group keying material together with its the individual keying material; request new individual keying material to use in the group; and leave the group. These operations are described in Section 4.8.1.1, Section 4.8.2.1, and Section 4.8.3.1, respectively.

* /ace-group/GROUPNAME/nodes/NODENAME/pub-key : this resource is invariant once established, and contains the individual public keying material for the node with name NODENAME, as group member of the group with name GROUPNAME.

  A Client can access this resource in order to upload at the KDC a new public key to use in the group. This operation is described in Section 4.9.1.1.

  This resource is not created if the group member does not have individual public keying material to use in the group, or if the KDC does not store the public keys of group members.

The KDC is expected to fully provide the interface defined above. It is otherwise REQUIRED of the application profiles of this specification to indicate which resources are not hosted, i.e., which parts of the interface defined in this section are not supported by the KDC (REQ9). Application profiles of this specification MAY extend the KDC interface, by defining additional resources and their handlers.

It is REQUIRED of the application profiles of this specification to register a Resource Type for the root url-path (REQ10). This Resource Type can be used to discover the correct url to access at the KDC. This Resource Type can also be used at the GROUPNAME sub-resource, to indicate different application profiles for different groups.

It is REQUIRED of the application profiles of this specification to define what specific actions (e.g., CoAP methods) are allowed on each resource provided by the KDC interface, depending on whether the Client is a current group member; the roles that a Client is authorized to take as per the obtained access token (see Section 3.1); and the roles that the Client has as current group member (REQ11).

4.1.1. Operations Supported by Clients

It is expected that a Client minimally supports the following set of primary operations and corresponding interactions with the KDC.

* FETCH request to ace-group/ , in order to retrieve group names associated to group identifiers.

* POST and GET requests to ace-group/GROUPNAME/ , in order to join a group (POST) and later retrieve the current group key material as a group member (GET).

* GET and FETCH requests to ace-group/GROUPNAME/pub-key , in order to retrieve the public keys of all the other group members (GET) or only some of them by filtering (FETCH). While retrieving public keys remains possible by using GET requests, retrieval by filtering allows to greatly limit the size of exchanged messages.

* GET request to ace-group/GROUPNAME/num , in order to retrieve the current version of the group key material as a group member.

* DELETE request to ace-group/GROUPNAME/nodes/NODENAME , in order to leave the group.

In addition, some Clients may rather not support the following set of secondary operations and corresponding interactions with the KDC. This can be specified, for instance, in compliance documents defining minimalistic Clients and their capabilities in specific deployments. In turn, these might also have to consider the used application profile of this specification.

* GET request to ace-group/GROUPNAME/kdc-pub-key , in order to retrieve the current public key of the KDC, in addition to when joining the group. This is relevant only if the KDC has an associated public key and this is required for the correct group operation.

* GET request to ace-group/GROUPNAME/policies , in order to retrieve the current group policies as a group member, in addition to when joining the group.

* GET request to ace-group/GROUPNAME/nodes/NODENAME, in order to retrieve the current group keying material and individual keying material. The former can also be retrieved through a GET request to ace-group/GROUPNAME/ (see above). The latter would not be possible to re-obtain as a group member.

* PUT request to ace-group/GROUPNAME/nodes/NODENAME , in order to ask for new individual keying material. The Client would have to alternatively re-join the group through a POST request to ace-group/GROUPNAME/ (see above). Furthermore, depending on its roles in the group or on the application profile of this specification, the Client might simply not be associated to any individual keying material.

* POST request to ace-group/GROUPNAME/nodes/NODENAME/pub-key , in order to provide the KDC with a new public key. The Client would have to alternatively re-join the group through a POST request to ace-group/GROUPNAME/ (see above). Furthermore, depending on its roles in the group, the Client might simply not have an associated public key to provide.

It is REQUIRED of application profiles of this specification to categorize possible newly defined operations for Clients into primary operations and secondary operations, and to provide accompanying considerations (REQ12).

4.1.2. Error Handling

Upon receiving a request from a Client, the KDC MUST check that it is storing a valid access token from that Client. If this is not the case, the KDC MUST reply with a 4.01 (Unauthorized) error response.

Unless the request targets the /ace-group resource, the KDC MUST check that it is storing a valid access token from that Client such that:

* The scope specified in the access token includes a scope entry related to the group name GROUPNAME associated to targeted resource; and

* The set of roles specified in that scope entry allows the Client to perform the requested operation on the targeted resource (REQ11).

In case the KDC stores a valid access token but the verifications above fail, the KDC MUST reply with a 4.03 (Forbidden) error response. This response MAY be an AS Request Creation Hints, as defined in Section 5.3 of [I-D.ietf-ace-oauth-authz], in which case the Content-Format MUST be set to application/ace+cbor.

If the request is not formatted correctly (e.g., required fields are not present or are not encoded as expected), the handler MUST reply with a 4.00 (Bad Request) error response.

If the request includes unknown or non-expected fields, the handler MUST silently ignore them and continue processing the request. Application profiles of this specification MAY define optional or mandatory payload formats for specific error cases (OPT4).

Some error responses from the KDC can have Content-Format set to application/ace-groupcomm+cbor. In such a case, the paylod of the response MUST be a CBOR map, which includes the following fields.

* 'error', with value a CBOR integer specifying the error occurred at the KDC. The value is taken from the "Value" column of the "ACE Groupcomm Errors" registry defined in Section 11.13 of this specification. This field MUST be present.

* 'error_description', with value a CBOR text string specifying a human-readable diagnostic description of the error occurred at the KDC, written in English. The diagnostic text is intended for software engineers as well as for device and network operators, in order to aid debugging and provide context for possible intervention. The diagnostic message SHOULD be logged by the KDC. This field MAY be present, and it is unlikely relevant in an unattended setup where human intervention is not expected.

The 'error' and 'error_description' fields are defined as OPTIONAL to support for Clients (see Section 8). A Client supporting the 'error' parameter and able to understand the specified error may use that information to determine what actions to take next.

Section 9 of this specification defines an initial set of error identifiers, as possible values for the 'error' field. Application profiles of this specification inherit this initial set or error identifiers and MAY define additional value (OPT5).

4.2. /ace-group

This resource implements the FETCH handler.

4.2.1. FETCH Handler

The FETCH handler receives group identifiers and returns the corresponding group names and GROUPNAME URIs.

The handler expects a request with payload formatted as a CBOR map, which MUST contain the following fields:

* 'gid', whose value is encoded as a CBOR array, containing one or more group identifiers. The exact encoding of group identifier MUST be specified by the application profile (REQ13). The Client indicates that it wishes to receive the group names and GROUPNAMEs of all groups having these identifiers.

The handler identifies the groups that are secured by the keying material identified by those group identifiers.

If all verifications succeed, the handler replies with a 2.05 (Content) response, whose payload is formatted as a CBOR map that MUST contain the following fields:

* 'gid', whose value is encoded as a CBOR array, containing zero or more group identifiers. The handler indicates that those are the identifiers it is sending group names and GROUPNAMEs for. This CBOR array is a subset of the 'gid' array in the FETCH request.

* 'gname', whose value is encoded as a CBOR array, containing zero or more group names. The elements of this array are encoded as text strings. Each element of index i of this CBOR array corresponds to the element of group identifier i in the 'gid' array.

* 'guri', whose value is encoded as a CBOR array, containing zero or more URIs, each indicating a GROUPNAME resource. The elements of this array are encoded as text strings. Each element of index i of this CBOR array corresponds to the element of group identifier i in the 'gid' array.

If the KDC does not find any group associated to the specified group identifiers, the handler returns a response with payload formatted as a CBOR byte string of zero length.

Note that the KDC only verifies that the node is authorized by the AS to access this resource. Nodes that are not members of the group but are authorized to do signature verification on the group messages may be allowed to access this resource, if the application needs it.

4.2.1.1. Retrieve Group Names

In case the joining node only knows the group identifier of the group it wishes to join or about which it wishes to get update information from the KDC, the node can contact the KDC to request the corresponding group name and joining resource URI. The node can request several group identifiers at once. It does so by sending a CoAP FETCH request to the /ace-group endpoint at the KDC formatted as defined in Section 4.2.1.

Figure 6 gives an overview of the exchanges described above, and Figure 7 shows an example.

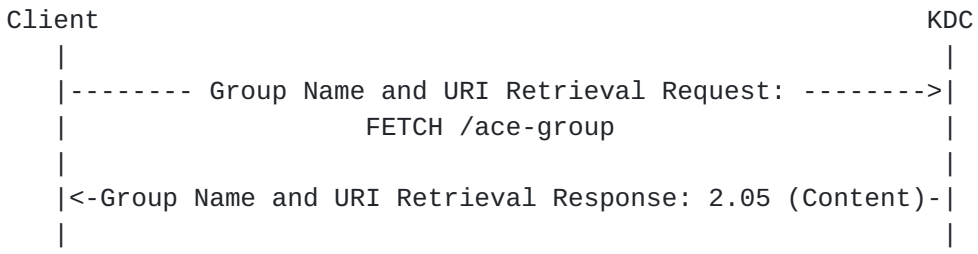


Figure 6: Message Flow of Group Name and URI Retrieval Request-Response

```
Request:

Header: FETCH (Code=0.05)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation):
  { "gid": [01, 02] }

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation):
  { "gid": [01, 02], "gname": ["group1", "group2"],
    "guri": ["ace-group/g1", "ace-group/g2"] }
```

Figure 7: Example of Group Name and URI Retrieval Request-Response

4.3. /ace-group/GROUPNAME

This resource implements the POST and GET and handlers.

4.3.1. POST Handler

The POST handler processes the Joining Request sent by a Client to join a group, and returns a Joining Response as successful result of the joining process (see Section 4.3.1.1). At a high level, the POST handler adds the Client to the list of current group members, adds the public key of the Client to the list of the group members' public keys, and returns the symmetric group keying material for the group identified by GROUPNAME.

The handler expects a request with payload formatted as a CBOR map, which MAY contain the following fields, which, if included, MUST have format and value as specified below.

* 'scope', with value the specific group that the Client is attempting to join, i.e., the group name, and the roles it wishes to have in the group. This value is a CBOR byte string wrapping one scope entry, as defined in Section 3.1.

* 'get_pub_keys', if the Client wishes to receive the public keys of the current group members from the KDC. This parameter may be included in the Joining Request if the KDC stores the public keys of the group members, while it is not useful to include it if the Client obtains those public keys through alternative means, e.g., from the AS. Note that including this parameter might result in a following Joining Response of large size, which can be inconvenient for resource-constrained devices.

  If the Client wishes to retrieve the public keys of all the current group members, the 'get_pub_keys' parameter MUST encode the CBOR simple value 'null' (0xf6). Otherwise, the 'get_pub_keys' parameter MUST encode a non-empty CBOR array, containing the following three elements formatted as defined below.

  - The first element, namely 'inclusion_flag', encodes the CBOR simple value True. That is, the Client indicates that it wishes to receive the public keys of all group members having their node identifier specified in the third element of the 'get_pub_keys' array, namely 'id_filter' (see below).

  - The second element, namely 'role_filter', is a non-empty CBOR array. Each element of the array contains one role or a combination of roles for the group identified by GROUPNAME. That is, when the Joining Request includes a non-Null 'get_pub_keys' parameter, the Client filters public keys based on node identifiers.

    In particular, the Client indicates that it wishes to retrieve the public keys of all the group members having any of the single roles, or at least all of the roles indicated in any combination of roles. For example, the array ["role1", "role2+role3"] indicates that the Client wishes to receive the public keys of all group members that have at least "role1" or at least both "role2" and "role3".

  - The third element, namely 'id_filter', is an empty CBOR array. That is, when the Joining Request includes a non-Null 'get_pub_keys' parameter, the Client does not filter public keys based on node identifiers.

In fact, when first joining the group, the Client is not expected or capable to express a filter based on node identifiers of other group members. Instead, when already a group member and sending a Joining Request to re-join, the Client is not expected to include the 'get_pub_keys' parameter in the Joining Request altogether, since it can rather retrieve public keys associated to specific group identifiers as defined in Section 4.4.1.1.

The CDDL definition [RFC8610] of 'get_pub_keys' is given in Figure 8, using as example encoding: node identifier encoded as a CBOR byte string; role identifier encoded as a CBOR text string, and combination of roles encoded as a CBOR array of roles.

Note that, for this handler, 'inclusion_flag' is always set to true, the array of roles 'role_filter' is always non-empty, while the array of node identifiers 'id_filter' is always empty. However, this is not necessarily the case for other handlers using the 'get_pub_keys' parameter.

```
inclusion_flag = bool

role = tstr
comb_role = [ 2*role ]
role_filter = [ *(role / comb_role) ]

id = bstr
id_filter = [ *id ]

get_pub_keys = null / [ inclusion_flag, role_filter, id_filter]
```

Figure 8: CDLL definition of get_pub_keys, using as example node identifier encoded as bstr and role as tstr

* 'client_cred', encoded as a CBOR byte string, with value the original binary representation of the Client's public key. This parameter is used if the KDC is managing (collecting from/ distributing to the Client) the public keys of the group members, and if the Client's role in the group will require for it to send messages to one or more group members. It is REQUIRED of the application profiles to define the specific formats that are acceptable to use for encoding public keys in the group (REQ6).

* 'cnonce', encoded as a CBOR byte string, and including a dedicated nonce N_C generated by the Client. This parameter MUST be present if the 'client_cred' parameter is present.

* 'client_cred_verify', encoded as a CBOR byte string. This parameter MUST be present if the 'client_cred' parameter is present and no public key associated to the Client's token can be retrieved for that group.

  This parameter contains a proof-of-possession (PoP) evidence computed by the Client over the following PoP input: the scope (encoded as CBOR byte string), concatenated with N_S (encoded as CBOR byte string) concatenated with N_C (encoded as CBOR byte string), where:

  - scope is the CBOR byte string either specified in the 'scope' parameter above, if present, or as a default scope that the handler is expected to understand, if omitted.

  - N_S is the challenge received from the KDC in the 'kdcchallenge' parameter of the 2.01 (Created) response to the Token Transfer Request (see Section 3.3), encoded as a CBOR byte string.

  - N_C is the nonce generated by the Client and specified in the 'cnonce' parameter above, encoded as a CBOR byte string.

  An example of PoP input to compute 'client_cred_verify' using CBOR encoding is given in Figure 9.

  A possible type of PoP evidence is a signature, that the Client computes by using its own private key, whose corresponding public key is specified in the 'client_cred' parameter. Application profiles of this specification MUST specify the exact approaches used to compute the PoP evidence to include in 'client_cred_verify', and MUST specify which of those approaches is used in which case (REQ14).

  If the token was not provided to the KDC through a Token Transfer Request (e.g., it is used directly to validate TLS instead), it is REQUIRED of the specific application profile to define how the challenge N_S is generated (REQ15).

* 'pub_keys_repos', which can be present if the format of the Client's public key in the 'client_cred' parameter is a certificate. In such a case, this parameter has as value the URI of the certificate. This parameter is encoded as a CBOR text string. Alternative specific encodings of this parameter MAY be defined in applications of this specification (OPT6).

* 'control_uri', with value a full URI, encoded as a CBOR text string. A default url-path is /ace-group/GROUPNAME/node, although implementations can use different ones instead. The URI MUST NOT have url-path ace-group/GROUPNAME.

  If 'control_uri' is specified in the Joining Request, the Client acts as a CoAP server and hosts a resource at this specific URI. The KDC MAY use this URI to send CoAP requests to the Client (acting as CoAP server in this exchange), for example for one-to-one provisioning of new group keying material when performing a group rekeying (see Section 4.8.1.1), or to inform the Client of its removal from the group Section 5.

  In particular, this resource is intended for communications concerning exclusively the group whose group name GROUPNAME is specified in the 'scope' parameter. If the KDC does not implement mechanisms using this resource for that group, it can ignore this parameter. Other additional functionalities of this resource MAY be defined in application profiles of this specifications (OPT7).

```
scope, N_S, and N_C expressed in CBOR diagnostic notation:
  scope = h'826667726F7570316673656E646572'
  N_S   = h'018a278f7faab55a'
  N_C   = h'25a8991cd700ac01'


scope, N_S, and N_C as CBOR encoded byte strings:
  scope = 0x4f826667726F7570316673656E646572
  N_S   = 0x48018a278f7faab55a
  N_C   = 0x4825a8991cd700ac01

PoP input:
  0x4f 826667726F7570316673656E646572
    48 018a278f7faab55a 48 25a8991cd700ac01
```

Figure 9: Example of PoP input to compute 'client_cred_verify' using CBOR encoding

If the request does not include a 'scope' field, the KDC is expected to understand with what roles the Client is requesting to join the group. For example, as per the access token, the Client might have been granted access to the group with only one role. If the KDC cannot determine which exact scope should be considered for the Client, it MUST reply with a 4.00 (Bad Request) error response.

The handler considers the scope specified in the access token associated to the Client, and checks the scope entry related to the group with name GROUPNAME associated to the endpoint. In particular,

the handler checks whether the set of roles specified in that scope entry includes all the roles that the Client wishes to have in the group as per the Joining Request. If this is not the case, the KDC MUST reply with a 4.03 (Forbidden) error response.

If the KDC manages the group members' public keys, the handler checks if one is included in the 'client_cred' field. If so, the KDC retrieves the public key and performs the following actions.

* If the access token was provided through a Token Transfer Request (see Section 3.3) but the KDC cannot retrieve the 'kdcchallenge' associated to this Client (see Section 3.3), the KDC MUST reply with a 4.00 Bad Request error response, which MUST also have Content-Format application/ace-groupcomm+cbor. The payload of the error response is a CBOR map including a newly generated 'kdcchallenge' value. This is specified in the 'kdcchallenge' parameter.

* The KDC checks the public key to be valid for the group identified by GROUPNAME. That is, it checks that the public key is encoded according to the format used in the group, is intended for the public key algorithm used in the group, and is aligned with the possible associated parameters used in the group.

  If this verification fails, the handler MUST reply with a 4.00 (Bad Request) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 2 ("Public key incompatible with the group configuration").

* The KDC verifies the PoP evidence contained in the 'client_cred_verify' field. Application profiles of this specification MUST specify the exact approaches used to verify the PoP evidence, and MUST specify which of those approaches is used in which case (REQ14).

  If the PoP evidence does not pass verification, the handler MUST reply with a 4.00 (Bad Request) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 3 ("Invalid Proof-of-Possession evidence").

If no public key is included in the 'client_cred' field, the handler checks if a public key is already associated to the received access token and to the group identified by GROUPNAME (see also Section 4.3.1.1). Note that the same joining node may use different public keys in different groups, and all those public keys would be associate to the same access token.

If an eligible public key for the Client is neither present in the 'client_cred' field nor retrieved from the stored ones at the KDC, it is RECOMMENDED that the handler stops the processing and replies with a 4.00 (Bad Request) error response. Applications profiles MAY define alternatives (OPT8).

If, regardless the reason, the KDC replies with a 4.00 (Bad Request) error response, this response MAY have Content-Format set to application/ace-groupcomm+cbor and have a CBOR map as payload. For instance, the CBOR map can include a 'sign_info' parameter formatted as 'sign_info_res' defined in Section 3.3.1, with the 'pub_key_enc' element set to the CBOR simple value 'null' (0xf6) if the Client sent its own public key and the KDC is not set to store public keys of the group members.

If all the verifications above succeed, the KDC proceeds as follows.

First, only in case the Client is not already a group member, the handler performs the following actions:

* The handler adds the Client to the list of current members of the group.

* The handler assigns a name NODENAME to the Client, and creates a sub-resource to /ace-group/GROUPNAME at the KDC, i.e., "/ace-group/GROUPNAME/nodes/NODENAME".

* The handler associates the node identifier NODENAME to the access token and the secure session for the Client.

Then, the handler performs the following actions.

* If the KDC manages the group members' public keys:

  - The handler associates the retrieved Client's public key to the tuple composed of the node name NODENAME, the group name GROUPNAME and the received access token.

  - The handler adds the retrieved Client's public key to the stored list of public keys stored for the group identified by GROUPNAME. If such list already includes a public key for the Client, but a different public key is specified in the 'client_cred' field, then the handler MUST replace the old public key in the list with the one specified in the 'client_cred' field.

* If the application requires backward security or if the used application profile prescribes so, the KDC MUST generate new group keying material and securely distribute it to the current group members (see Section 6).

* The handler returns a successful Joining Response as defined below, containing the symmetric group keying material; the group policies; and the public keys of the current members of the group, if the KDC manages those and the Client requested them.

The Joining Response MUST have response code 2.01 (Created) if the Client has been added to the list of group members in this joining exchange (see above), or 2.04 (Changed) otherwise, i.e., if the Client is re-joining the group without having left it.

The Joining Response message MUST include the Location-Path CoAP option, specifying the URI path to the sub-resource associated to the Client, i.e. "/ace-group/GROUPNAME/nodes/NODENAME".

The Joining Response message MUST have Content-Format application/ace-groupcomm+cbor. The payload of the response is formatted as a CBOR map, which MUST contain the following fields and values.

* 'gkty', identifying the key type of the 'key' parameter. The set of values can be found in the "Key Type" column of the "ACE Groupcomm Key Types" registry. Implementations MUST verify that the key type matches the application profile being used, if present, as registered in the "ACE Groupcomm Key Types" registry.

* 'key', containing the keying material for the group communication, or information required to derive it.

* 'num', containing the version number of the keying material for the group communication, formatted as an integer. This is a strictly monotonic increasing field. The application profile MUST define the initial version number (REQ16).

The exact format of the 'key' value MUST be defined in applications of this specification (REQ17), as well as values of 'gkty' accepted by the application (REQ18). Additionally, documents specifying the key format MUST register it in the "ACE Groupcomm Key Types" registry defined in Section 11.8, including its name, type and application profile to be used with.

Name	Key Type Value	Profile	Description
Reserved	0		This value is reserved

Figure 10: Key Type Values

The response SHOULD contain the following parameter:

* 'exp', with value the expiration time of the keying material for the group communication, encoded as a CBOR unsigned integer. This field contains a numeric value representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds, analogous to what specified for NumericDate in Section 2 of [RFC7519]. Group members MUST stop using the keying material to protect outgoing messages and retrieve new keying material at the time indicated in this field.

Optionally, the response MAY contain the following parameters, which, if included, MUST have format and value as specified below.

* 'ace-groupcomm-profile', with value a CBOR integer that MUST be used to uniquely identify the application profile for group communication. Applications of this specification MUST register an application profile identifier and the related value for this parameter in the "ACE Groupcomm Profiles" registry (REQ19).

* 'pub_keys', MUST be present if 'get_pub_keys' was present in the request, otherwise it MUST NOT be present. This parameter is a CBOR array specifying the public keys of the group members, i.e., of all of them or of the ones selected according to the 'get_pub_keys' parameter in the request. In particular, each element of the array is a CBOR byte string, with value the original binary representation of a group member's public key. It is REQUIRED of the application profiles to define the specific formats of public keys that are acceptable to use in the group (REQ6).

* 'peer_roles', MUST be present if 'pub_keys' is also present, otherwise it MUST NOT be present. This parameter is a CBOR array of n elements, with n the number of public keys included in the 'pub_keys' parameter (at most the number of members in the group). The i-th element of the array specifies the role (or CBOR array of roles) that the group member associated to the i-th public key in 'pub_keys' has in the group. In particular, each array element is encoded as the role element of a scope entry, as defined in Section 3.1.

* 'peer_identifiers', MUST be present if 'pub_keys' is also present, otherwise it MUST NOT be present. This parameter is a CBOR array of n elements, with n the number of public keys included in the 'pub_keys' parameter (at most the number of members in the group). The i-th element of the array specifies the node identifier that the group member associated to the i-th public key in 'pub_keys' has in the group. In particular, the i-th array element is encoded as a CBOR byte string, with value the node identifier of the group member.

* 'group_policies', with value a CBOR map, whose entries specify how the group handles specific management aspects. These include, for instance, approaches to achieve synchronization of sequence numbers among group members. The elements of this field are registered in the "ACE Groupcomm Policies" registry. This specification defines the three elements "Sequence Number Synchronization Methods", "Key Update Check Interval" and "Expiration Delta", which are summarized in Figure 11. Application profiles that build on this document MUST specify the exact content format and default value of included map entries (REQ20).

Name	CBOR label	CBOR type	Description	Reference
Sequence Number Synchroniza-tion Method	TBD	tstr/int	Method for recipient group members to synchronize with sequence numbers of of sender group members. Its value is taken from the 'Value' column of the Sequence Number Synchronization Method registry	[[this document]]
Key Update Check Interval	TBD	int	Polling interval in seconds, for group members to check at the KDC if the latest group keying material is the one that they own	[[this document]]
Expiration Delta	TBD	uint	Number of seconds from 'exp' until the specified UTC date/time after which group members MUST stop using the group keying material they own to verify incoming messages	[[this document]]

Figure 11: ACE Groupcomm Policies

* 'kdc_cred', encoded as a CBOR byte string, with value the original binary representation of the KDC's public key. This parameter is used if the KDC has an associated public key and this is required for the correct group operation. It is REQUIRED of application profiles to define whether the KDC has a public key and if this has to be provided through the 'kdc_cred' parameter (REQ8).

In such a case, the KDC's public key MUST have the same format used for the public keys of the group members. It is REQUIRED of the application profiles to define the specific formats that are acceptable to use for encoding public keys in the group (REQ6).

* 'kdc_nonce', encoded as a CBOR byte string, and including a dedicated nonce N_KDC generated by the KDC. This parameter MUST be present if the 'kdc_cred' parameter is present.

* 'kdc_cred_verify' parameter, encoded as a CBOR byte string. This parameter MUST be present if the 'kdc_cred' parameter is present.

  This parameter contains a proof-of-possession (PoP) evidence computed by the KDC over the nonce N_KDC, which is specified in the 'kdc_nonce' parameter and taken as PoP input.

  A possible type of PoP evidence is a signature, that the KDC computes by using its own private key, whose corresponding public key is specified in the 'kdc_cred' parameter. Application profiles of this specification MUST specify the exact approaches used by the KDC to compute the PoP evidence to include in 'kdc_cred_verify', and MUST specify which of those approaches is used in which case (REQ21).

* 'rekeying_scheme', identifying the rekeying scheme that the KDC uses to provide new group keying meterial to the group members. This parameter is encoded as a CBOR integer, whose value is taken from the "Value" column of the "ACE Groupcomm Rekeying Schemes" registry defined in Section 11.14 of this specification.

Value	Name	Description	Reference
0	Point-to-Point	The KDC individually targets each node to rekey, using the pairwise secure communication association with that node	[this document]

Figure 12: ACE Groupcomm Rekeying Schemes

Application profiles of this specification MAY define a default group rekeying scheme, to refer to in case the 'rekeying_scheme' parameter is not included in the Joining Response (OPT9).

* 'mgt_key_material', encoded as a CBOR byte string and containing the specific administrative keying material that the joining node requires in order to participate in the group rekeying process

performed by the KDC. This parameter MUST NOT be present if the 'rekeying_scheme' parameter is not present and the application profile does not specify a default group rekeying scheme to use in the group. Some simple rekeying scheme may not require specific administrative keying material to be provided, e.g., the basic "Point-to-Point" group rekeying scheme (see Section 6.1).

In more advanced group rekeying schemes, the administrative keying material can be composed of multiple keys organized, for instance, into a logical tree hierarchy, whose root key is the only administrative key shared by all the group members. In such a case, each group member is exclusively associated to one leaf key in the hierarchy, and owns only the administrative keys from the associated leaf key all the way up along the path to the root key. That is, different group members can be provided with a different subset of the overall administrative keying material.

It is expected from separate documents to define how the advanced group rekeying scheme possibly indicated in the 'rekeying_scheme' parameter is used by an application profile of this specification. This includes defining the format of the administrative keying material to specify in 'mgt_key_material', consistently with the group rekeying scheme and the application profile in question.

* 'control_group_uri', with value a full URI, encoded as a CBOR text string. The URI MUST specify addressing information intended to reach all the members in the group. For example, this can be a multicast IP address, optionally together with a port number (which defaults to 5683 if omitted). The URI MUST include GROUPNAME in the url-path. A default url-path is /ace-group/GROUPNAME, although implementations can use different ones instead. The URI MUST NOT have url-path ace-group/GROUPNAME/node.

  If 'control_group_uri' is included in the Joining Response, the Clients supporting this parameter act as CoAP servers, host a resource at this specific URI, and listen to the specified addressing information.

  The KDC MAY use this URI to send one-to-many CoAP requests to the Client group members (acting as CoAP servers in this exchange), for example for one-to-many provisioning of new group keying material when performing a group rekeying (see Section 4.8.1.1), or to inform the Clients of their removal from the group Section 5.

  In particular, this resource is intended for communications concerning exclusively the group whose group name GROUPNAME is specified in the 'scope' parameter. If the KDC does not implement

mechanisms using this resource for that group, it can ignore this parameter. Other additional functionalities of this resource MAY be defined in application profiles of this specifications (OPT10).

If the Joining Response includes the 'kdc_cred_verify' parameter, the Client verifies the conveyed PoP evidence and considers the group joining unsuccessful in case of failed verification. Application profiles of this specification MUST specify the exact approaches used by the Client to verify the PoP evidence in 'kdc_cred_verify', and MUST specify which of those approaches is used in which case (REQ21).

Specific application profiles that build on this document MUST specify the communication protocol that members of the group use to communicate with each other (REQ22) and how exactly the keying material is used to protect the group communication (REQ23).

4.3.1.1. Join the Group

Figure 13 gives an overview of the Joining exchange between Client and KDC, when the Client first joins a group, while Figure 14 shows an example.

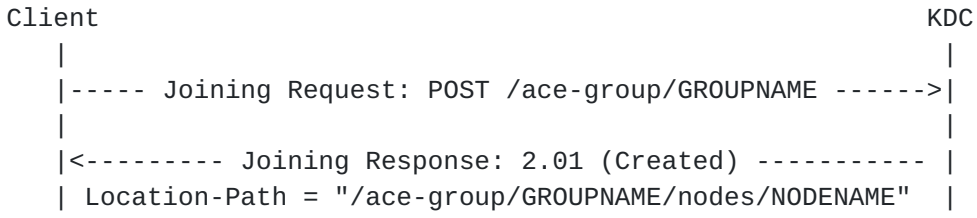


Figure 13: Message Flow of the Joining Exchange

```
 Request:

 Header: POST (Code=0.02)
 Uri-Host: "kdc.example.com"
 Uri-Path: "ace-group"
 Uri-Path: "g1"
 Content-Format: "application/ace-groupcomm+cbor"
 Payload (in CBOR diagnostic notation,
          with PUB_KEY and POP_EVIDENCE being CBOR byte strings):
   { "scope": << [ "group1", ["sender", "receiver"] ] >> ,
     "get_pub_keys": [true, ["sender"], []], "client_cred": PUB_KEY,
     "cnonce": h'6df49c495409a9b5', "client_cred_verify": POP_EVIDENCE }

 Response:

 Header: Created (Code=2.01)
 Content-Format: "application/ace-groupcomm+cbor"
 Location-Path: "kdc.example.com"
 Location-Path: "g1"
 Location-Path: "nodes"
 Location-Path: "c101"
 Payload (in CBOR diagnostic notation,
          with KEY being a CBOR byte strings):
   { "gkty": 13, "key": KEY, "num": 12, "exp": 1609459200,
     "pub_keys": [ PUB_KEY1, PUB_KEY2 ],
     "peer_roles": ["sender", ["sender", "receiver"]],
     "peer_identifiers": [ ID1, ID2 ] }
```

Figure 14: Example of First Exchange for Group Joining

If not previously established, the Client and the KDC MUST first establish a pairwise secure communication channel (REQ24). This can be achieved, for instance, by using a transport profile of ACE. The Joining exchange MUST occur over that secure channel. The Client and the KDC MAY use that same secure channel to protect further pairwise communications that must be secured.

The secure communication protocol is REQUIRED to establish the secure channel between Client and KDC by using the proof-of-possession key bound to the access token. As a result, the proof-of-possession to bind the access token to the Client is performed by using the proof-of-possession key bound to the access token for establishing secure communication between the Client and the KDC.

To join the group, the Client sends a CoAP POST request to the /ace-group/GROUPNAME endpoint at the KDC, where GROUPNAME is the group name of the group to join, formatted as specified in Section 4.3.1. This group name is the same as in the scope entry corresponding to

that group, specified in the 'scope' parameter of the Authorization Request/Response, or it can be retrieved from it. Note that, in case of successful joining, the Client will receive the URI to retrieve individual keying material and to leave the group in the Location-Path option of the response.

If the node is joining a group for the first time, and the KDC maintains the public keys of the group members, the Client is REQUIRED to send its own public key and proof-of-possession (PoP) evidence in the Joining Request (see the 'client_cred' and 'client_cred_verify' parameters in Section 4.3.1). The request is accepted only if both public key is provided and the PoP evidence is successfully verified.

If a node re-joins a group as authorized by the same access token and using the same public key, it can omit the public key and the PoP evidence, or just the PoP evidence, from the Joining Request. Then, the KDC will be able to retrieve the node's public key associated to the access token for that group. If the public key has been discarded, the KDC replies with 4.00 (Bad Request) error response, as specified in Section 4.3.1. If a node re-joins a group but wants to update its own public key, it needs to include both its public key and the PoP evidence in the Joining Request like when it joined the group for the first time.

4.3.2. GET Handler

The GET handler returns the symmetric group keying material for the group identified by GROUPNAME.

The handler expects a GET request.

In addition to what is defined in Section 4.1.2, the handler verifies that the Client is a current member of the group. If the verification fails, the KDC MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 0 ("Operation permitted only to group members").

If all verifications succeed, the handler replies with a 2.05 (Content) response containing the symmetric group keying material. The payload of the response is formatted as a CBOR map which MUST contain the parameters 'gkty', 'key' and 'num' specified in Section 4.3.1.

Each of the following parameters specified in Section 4.3.1 MUST also be included in the payload of the response, if they are included in the payload of the Joining Responses sent for the group: 'rekeying_scheme', 'mgt_key_material'.

The payload MAY also include the parameters 'ace-groupcomm-profile' and 'exp' parameters specified in Section 4.3.1.

4.3.2.1. Retrieve Group Keying Material

A node in the group can contact the KDC to retrieve the current group keying material, by sending a CoAP GET request to the /ace-group/GROUPNAME endpoint at the KDC, where GROUPNAME is the group name.

Figure 15 gives an overview of the Joining exchange between Client and KDC, when the Client first joins a group, while Figure 16 shows an example.

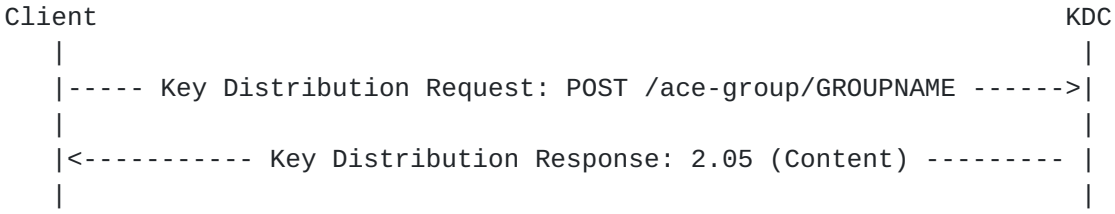


Figure 15: Message Flow of Key Distribution Request-Response

Request:

Header: GET (Code=0.01)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Payload: -

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation,
         with KEY being a CBOR byte strings):
  { "gkty": 13, "key": KEY, "num": 12 }

Figure 16: Example of Key Distribution Request-Response

4.4. /ace-group/GROUPNAME/pub-key

This resource implements the GET and FETCH handlers.

4.4.1. FETCH Handler

The FETCH handler receives identifiers of group members for the group identified by GROUPNAME and returns the public keys of such group members.

The handler expects a request with payload formatted as a CBOR map, that MUST contain the following field.

* 'get_pub_keys', whose value is encoded as in Section 4.3.1 with the following modifications.

  - The arrays 'role_filter' and 'id_filter' MUST NOT both be empty, i.e., in CBOR diagnostic notation: [bool, [ ], [ ]]. If the 'get_pub_keys' parameter has such a format, the request MUST be considered malformed, and the KDC MUST reply with a 4.00 (Bad Request) error response.

    Note that a group member can retrieve the public keys of all the current group members by sending a GET request to the same KDC resource instead (see Section 4.4.2.1).

  - The element 'inclusion_flag' encodes the CBOR simple value True if the third element 'id_filter' specifies an empty CBOR array, or if the Client wishes to receive the public keys of the nodes having their node identifier specified in 'id_filter' (i.e, selection by inclusive filtering). Instead, this element encodes the CBOR simple value False if the Client wishes to receive the public keys of the nodes not having the node identifiers specified in the third element 'id_filter' (i.e., selection by exclusive filtering).

  - The array 'role_filter' can be empty, if the Client does not wish to filter the requested public keys based on the roles of the group members.

  - The array 'id_filter' contains zero or more node identifiers of group members, for the group identified by GROUPNAME. The Client indicates that it wishes to receive the public keys of the nodes having or not having these node identifiers, in case the 'inclusion_flag' element encodes the CBOR simple value True or False, respectively. The array 'id_filter' may be empty, if the Client does not wish to filter the requested public keys based on the node identifiers of the group members.

Note that, in case the 'role_filter' array and the 'id_filter' array are both non-empty:

* If the 'inclusion_flag' encodes the CBOR simple value True, the handler returns the public keys of group members whose roles match with 'role_filter' and/or having their node identifier specified in 'id_filter'.

* If the 'inclusion_flag' encodes the CBOR simple value False, the handler returns the public keys of group members whose roles match with 'role_filter' and, at the same time, not having their node identifier specified in 'id_filter'.

The specific format of public keys as well as identifiers, roles and combination of roles of group members MUST be specified by It is REQUIRED of application profiles of this specification (REQ1, REQ6, REQ25).

The handler identifies the public keys of the current group members for which either:

* the role identifier matches with one of those indicated in the request; note that the request can contain a "combination of roles", where the handler select all group members who have all roles included in the combination.

* the node identifier matches with one of those indicated in the request.

If all verifications succeed, the handler returns a 2.05 (Content) message response with payload formatted as a CBOR map, containing only the following parameters from Section 4.3.1.

* 'num', which encodes the version number of the current group keying material.

* 'pub_keys', which encodes the list of public keys of the selected group members.

* 'peer_roles', which encodes the role (or CBOR array of roles) that each of the selected group members has in the group.

* 'peer_identifiers', which encodes the node identifier that each of the selected group members has in the group.

The specific format of public keys as well as of node identifiers of group members is specified by the application profile (REQ6, REQ25).

If the KDC does not store any public key associated to the specified node identifiers, the handler returns a response with payload formatted as a CBOR byte string of zero length.

The handler MAY enforce one of the following policies, in order to handle possible node identifiers that are included in the 'id_filter' element of the 'get_pub_keys' parameter of the request but are not associated to any current group member. Such a policy MUST be specified by the application profile (REQ26).

* The KDC silently ignores those node identifiers.

* The KDC retains public keys of group members for a given amount of time after their leaving, before discarding them. As long as such public keys are retained, the KDC provides them to a requesting Client.

  If the KDC adopts this policy, the application profile MUST also specify the amount of time during which the KDC retains the public key of a former group member after its leaving, possibly on a per-member basis.

Note that this resource handler only verifies that the node is authorized by the AS to access this resource. Nodes that are not members of the group but are authorized to do signature verifications on the group messages may be allowed to access this resource, if the application needs it.

4.4.1.1. Retrieve a Subset of Public Keys in the Group

In case the KDC maintains the public keys of group members, a node in the group can contact the KDC to request the public keys, roles and node identifiers of a specified subset of group members, by sending a CoAP FETCH request to the /ace-group/GROUPNAME/pub-key endpoint at the KDC, where GROUPNAME is the group name, and formatted as defined in Section 4.4.1.

Figure 17 gives an overview of the exchange mentioned above, while Figure 18 shows an example of such an exchange.

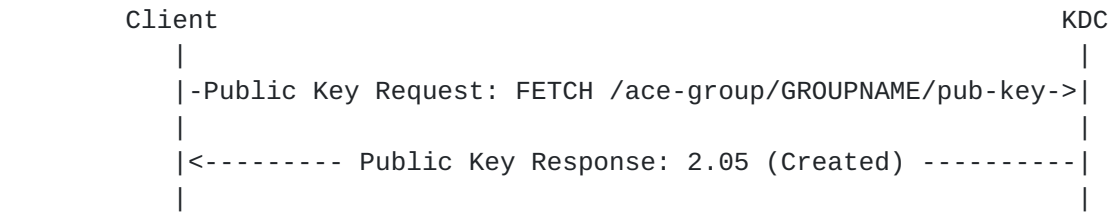


Figure 17: Message Flow of Public Key Exchange to Request the Public Keys of Specific Group Members

```
Request:

Header: FETCH (Code=0.05)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "pub-key"
Content-Format: "application/ace-groupcomm+cbor"
Payload:
  { "get_pub_keys": [true, [], [ ID3 ]] }

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation):
  { "pub_keys": [ PUB_KEY3 ],
    "peer_roles": [ "receiver" ],
    "peer_identifiers": [ ID3 ] }
```

Figure 18: Example of Public Key Exchange to Request the Public Keys of Specific Group Members

4.4.2. GET Handler

The handler expects a GET request.

If all verifications succeed, the KDC replies with a 2.05 (Content) response as in the FETCH handler in Section 4.4.1, but specifying in the payload the public keys of all the group members, together with their roles and node identifiers.

4.4.2.1. Retrieve All Public Keys in the Group

In case the KDC maintains the public keys of group members, a group or an external signature verifier can contact the KDC to request the public keys, roles and node identifiers of all the current group members, by sending a CoAP GET request to the /ace-group/GROUPNAME/pub-key endpoint at the KDC, where GROUPNAME is the group name.

Figure 19 gives an overview of the message exchange, while Figure 20 shows an example of such an exchange.

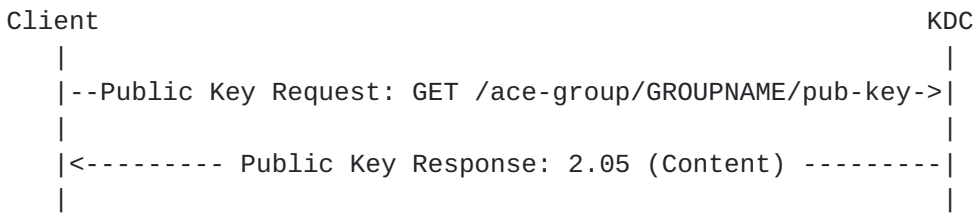


Figure 19: Message Flow of Public Key Exchange to Request the Public Keys of all the Group Members

Request:

Header: GET (Code=0.01)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "pub-key"
Payload: -

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation):

```
{ "num": 5,
  "pub_keys": [ PUB_KEY1, PUB_KEY2, PUB_KEY3 ],
  "peer_roles": ["sender", ["sender", "receiver"], "receiver"],
  "peer_identifiers": [ ID1, ID2, ID3 ] }
```

Figure 20: Example of Public Key Exchange to Request the Public Keys of all the Group Members

4.5. ace-group/GROUPNAME/kdc-pub-key

This resource implements a GET handler.

4.5.1. GET Handler

The handler expects a GET request.

If all verifications succeed, the handler returns a 2.05 (Content) message containing the KDC's public key together with a proof-of-possession (PoP) evidence. The response MUST have Content-Format set to application/ace-groupcomm+cbor. The payload of the response is a CBOR map, which includes the following fields.

* The 'kdc_cred' parameter, specifying the KDC's public key. This parameter is encoded like the 'kdc_cred' parameter in the Joining Response (see Section 4.3.1).

* The 'kdc_nonce' parameter, specifying a nonce generated by the KDC. This parameter is encoded like the 'kdc_nonce' parameter in the Joining Response (see Section 4.3.1).

* The 'kdc_cred_verify' parameter, specifying a PoP evidence computed by the KDC. This parameter is encoded like the 'kdc_cred_verify' parameter in the Joining Response (see Section 4.3.1).

  The PoP evidence is computed over the nonce specified in the 'kdc_nonce' parameter and taken as PoP input, by means of the same method used when preparing the Joining Response (see Section 4.3.1). Application profiles of this specification MUST specify the exact approaches used by the KDC to compute the PoP evidence to include in 'kdc_cred_verify', and MUST specify which of those approaches is used in which case (REQ21).

4.5.1.1. Retrieve the KDC's Public Key

In case the KDC has an associated public key as required for the correct group operation, a group member or an external signature verifier can contact the KDC to request the KDC's public key, by sending a CoAP GET request to the /ace-group/GROUPNAME/kdc-pub-key endpoint at the KDC, where GROUPNAME is the group name.

Upon receiving the 2.05 (Content) response, the Client retrieves the KDC's public key from the 'kdc_cred' parameter, and MUST verify the proof-of-possession (PoP) evidence specified in the 'kdc_cred_verify' parameter. In case of successful verification of the PoP evidence, the Client MUST store the obtained KDC's public key and replace the currently stored one.

The PoP evidence is verified by means of the same method used when processing the Joining Response (see Section 4.3.1). Application profiles of this specification MUST specify the exact approaches used by the Client to verify the PoP evidence in 'kdc_cred_verify', and MUST specify which of those approaches is used in which case (REQ21).

Figure 21 gives an overview of the exchange described above, while Figure 22 shows an example.

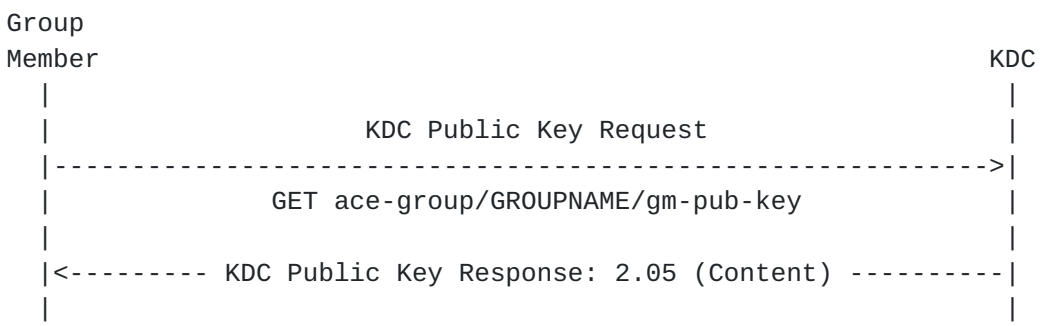


Figure 21: Message Flow of KDC Public Key Request-Response

Request:

Header: GET (Code=0.01)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "kdc-pub-key"
Payload: -

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation, with PUB_KEY_KDC
and POP_EVIDENCE being CBOR byte strings):

```
{
  "kdc_nonce": h'25a8991cd700ac01',
  "kdc_cred": PUB_KEY_KDC,
  "kdc_cred_verify": POP_EVIDENCE
}
```

Figure 22: Example of KDC Public Key Request-Response

4.6. /ace-group/GROUPNAME/policies

This resource implements the GET handler.

4.6.1. GET Handler

The handler expects a GET request.

In addition to what is defined in Section 4.1.2, the handler verifies that the Client is a current member of the group. If the verification fails, the KDC MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 0 ("Operation permitted only to group members").

If all verifications succeed, the handler replies with a 2.05 (Content) response containing the list of policies for the group identified by GROUPNAME. The payload of the response is formatted as a CBOR map including only the parameter 'group_policies' defined in Section 4.3.1 and specifying the current policies in the group. If the KDC does not store any policy, the payload is formatted as a zero-length CBOR byte string.

The specific format and meaning of group policies MUST be specified in the application profile (REQ20).

4.6.1.1. Retrieve the Group Policies

A node in the group can contact the KDC to retrieve the current group policies, by sending a CoAP GET request to the /ace-group/GROUPNAME/policies endpoint at the KDC, where GROUPNAME is the group name, and formatted as defined in Section 4.6.1

Figure 23 gives an overview of the exchange described above, while Figure 24 shows an example.

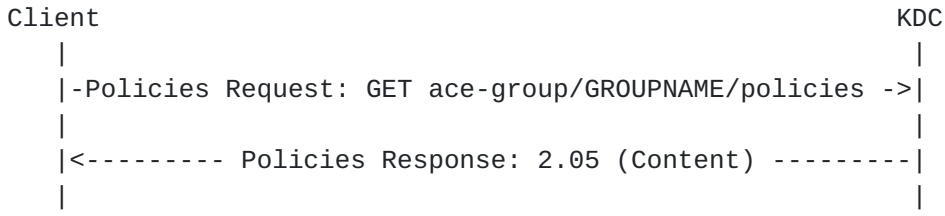


Figure 23: Message Flow of Policies Request-Response

```
Request:

Header: GET (Code=0.01)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "policies"
Payload: -

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload(in CBOR diagnostic notation):
  { "group_policies": {"exp-delta": 120} }
```

Figure 24: Example of Policies Request-Response

4.7. /ace-group/GROUPNAME/num

This resource implements the GET handler.

4.7.1. GET Handler

The handler expects a GET request.

In addition to what is defined in Section 4.1.2, the handler verifies that the Client is a current member of the group. If the verification fails, the KDC MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 0 ("Operation permitted only to group members").

If all verifications succeed, the handler returns a 2.05 (Content) message containing an integer that represents the version number of the symmetric group keying material. This number is incremented on the KDC every time the KDC updates the symmetric group keying material, before the new keying material is distributed. This number is stored in persistent storage.

The payload of the response is formatted as a CBOR integer.

4.7.1.1. Retrieve the Keying Material Version

A node in the group can contact the KDC to request information about the version number of the symmetric group keying material, by sending a CoAP GET request to the /ace-group/GROUPNAME/num endpoint at the KDC, where GROUPNAME is the group name, formatted as defined in Section 4.7.1. In particular, the version is incremented by the KDC every time the group keying material is renewed, before it's distributed to the group members.

Figure 25 gives an overview of the exchange described above, while Figure 26 shows an example.

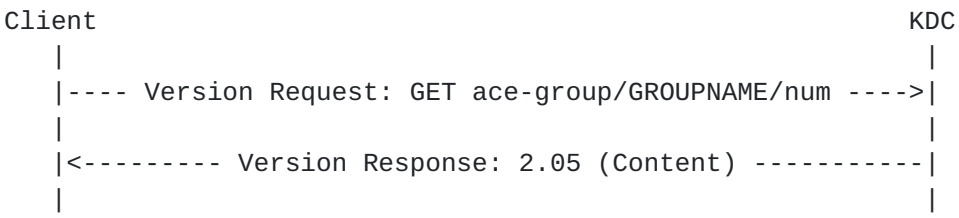


Figure 25: Message Flow of Version Request-Response

Request:

Header: GET (Code=0.01)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "num"
Payload: -

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload(in CBOR diagnostic notation):
  13

Figure 26: Example of Version Request-Response

4.8. /ace-group/GROUPNAME/nodes/NODENAME

This resource implements the GET, PUT and DELETE handlers.

In addition to what is defined in Section 4.1.2, each of the handlers performs the following two verifications.

* The handler verifies that the Client is a current member of the group. If the verification fails, the KDC MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 0 ("Operation permitted only to group members").

* The handler verifies that the node name of the Client is equal to NODENAME used in the url-path. If the verification fails, the handler replies with a 4.03 (Forbidden) error response.

4.8.1. GET Handler

The handler expects a GET request.

If all verifications succeed, the handler replies with a 2.05 (Content) response containing both the group keying material and the individual keying material for the Client, or information enabling the Client to derive it. The payload of the response is formatted as a CBOR map. The format for the group keying material is the same as defined in the response of Section 4.3.2. The specific format of individual keying material for group members, or of the information to derive it, and corresponding CBOR label, MUST be specified in the application profile (REQ27) and registered in Section 11.7.

Optionally, the KDC can make the sub-resource at ace-group/GROUPNAME/nodes/NODENAME also Observable [RFC7641] for the associated node. In case the KDC removes that node from the group without having been explicitly asked for it, this allows the KDC to send an unsolicited 4.04 (Not Found) response to the node as a notification of eviction from the group (see Section 5).

Note that the node could have been observing also the resource at ace-group/GROUPNAME, in order to be informed of changes in the keying material. In such a case, this method would result in largely overlapping notifications received for the resource at ace-group/GROUPNAME and the sub-resource at ace-group/GROUPNAME/nodes/NODENAME.

In order to mitigate this, a node that supports the No-Response option [RFC7967] can use it when starting the observation of the sub-resource at ace-group/GROUPNAME/nodes/NODENAME. In particular, the GET observation request can also include the No-Response option, with value set to 2 (Not interested in 2.xx responses).

4.8.1.1. Retrieve Group and Individual Keying Material

When any of the following happens, a node MUST stop using the owned group keying material to protect outgoing messages, and SHOULD stop using it to decrypt and verify incoming messages.

* Upon expiration of the keying material, according to what indicated by the KDC with the 'exp' parameter in a Joining Response, or to a pre-configured value.

* Upon receiving a notification of revoked/renewed keying material from the KDC, possibly as part of an update of the keying material (rekeying) triggered by the KDC.

* Upon receiving messages from other group members without being able to retrieve the keying material to correctly decrypt them. This may be due to rekeying messages previously sent by the KDC, that the Client was not able to receive or decrypt.

In either case, if it wants to continue participating in the group communication, the node has to request the latest keying material from the KDC. To this end, the Client sends a CoAP GET request to the /ace-group/GROUPNAME/nodes/NODENAME endpoint at the KDC, formatted as specified in Section 4.8.1.

Note that policies can be set up, so that the Client sends a Key Re-Distribution request to the KDC only after a given number of received messages could not be decrypted (because of failed decryption processing or inability to retrieve the necessary keying material).

It is application dependent and pertaining to the particular message exchange (e.g., [I-D.ietf-core-oscore-groupcomm]) to set up these policies for instructing Clients to retain incoming messages and for how long (OPT11). This allows Clients to possibly decrypt such messages after getting updated keying material, rather than just consider them non valid messages to discard right away.

The same Key Distribution Request could also be sent by the Client without being triggered by a failed decryption of a message, if the Client wants to be sure that it has the latest group keying material. If that is the case, the Client will receive from the KDC the same group keying material it already has in memory.

Figure 27 gives an overview of the exchange described above, while Figure 28 shows an example.

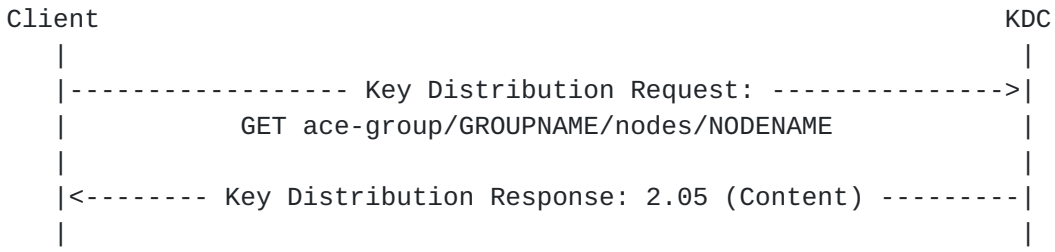


Figure 27: Message Flow of Key Distribution Request-Response

Request:

Header: GET (Code=0.01)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "nodes"
Uri-Path: "c101"
Payload: -

Response:

Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation,
         with KEY and IND_KEY being CBOR byte strings,
         and "ind-key" the profile-specified label
         for individual keying material):
  { "gkty": 13, "key": KEY, "num": 12, "ind-key": IND_KEY }

Figure 28: Example of Key Distribution Request-Response

4.8.2. PUT Handler

The PUT handler processes requests from a Client that asks for new individual keying material, as required to process messages exchanged in the group.

The handler expects a PUT request with empty payload.

In addition to what is defined in Section 4.1.2 and at the beginning of Section 4.8, the handler verifies that this operation is consistent with the set of roles that the Client has in the group (REQ11). If the verification fails, the KDC MUST reply with a 4.00 (Bad Request) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 1 ("Request inconsistent with the current roles").

If the KDC is currently not able to serve this request, i.e., to generate new individual keying material for the requesting Client, the KDC MUST reply with a 5.03 (Service Unavailable) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 4 ("No available node identifiers").

If all verifications succeed, the handler reply with a 2.05 (Content) response containing newly generated, individual keying material for the Client. The payload of the response is formatted as a CBOR map. The specific format of newly-generated individual keying material for group members, or of the information to derive it, and corresponding CBOR label, MUST be specified in the application profile (REQ27) and registered in Section 11.7.

The typical successful outcome consists in replying with newly generated, individual keying material for the Client, as defined above. However, application profiles of this specification MAY also extend this handler in order to achieve different akin outcomes (OPT12), for instance:

* Not providing the Client with newly generated, individual keying material, but rather rekeying the whole group, i.e., providing all the current group members with newly generated group keying material.

* Both providing the Client with newly generated, individual keying material, as well as rekeying the whole group, i.e., providing all the current group members with newly generated group keying material.

In either case, the handler may specify the new group keying material as part of the 2.05 (Content) response.

Note that this handler is not intended to accommodate requests from a group member to trigger a group rekeying, whose scheduling and execution is an exclusive prerogative of the KDC.

4.8.2.1. Request to Change Individual Keying Material

A Client may ask the KDC for new, individual keying material. For instance, this can be due to the expiration of such individual keying material, or to the exhaustion of AEAD nonces, if an AEAD encryption algorithm is used for protecting communications in the group. An example of individual keying material can simply be an individual encryption key associated to the Client. Hence, the Client may ask for a new individual encryption key, or for new input material to derive it.

To this end, the Client performs a Key Renewal Request/Response exchange with the KDC, i.e., it sends a CoAP PUT request to the /ace-group/GROUPNAME/nodes/NODENAME endpoint at the KDC, where GROUPNAME is the group name and NODENAME is its node name, and formatted as defined in Section 4.8.1.

Figure 29 gives an overview of the exchange described above, while Figure 30 shows an example.

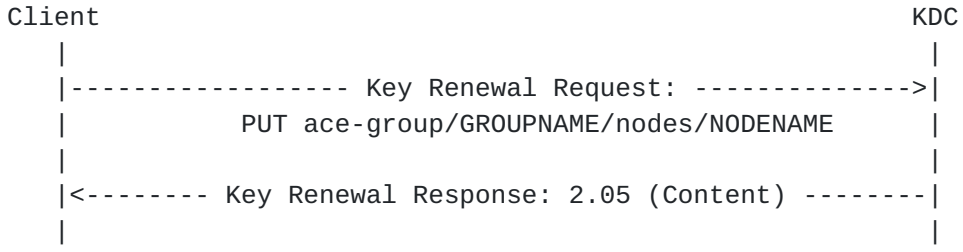


Figure 29: Message Flow of Key Renewal Request-Response

Request:

```
Header: PUT (Code=0.03)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "nodes"
Uri-Path: "c101"
Payload: -
```

Response:

```
Header: Content (Code=2.05)
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation, with IND_KEY being
         a CBOR byte string, and "ind-key" the profile-specified
         label for individual keying material):
  { "ind-key": IND_KEY }
```

Figure 30: Example of Key Renewal Request-Response

Note the difference between the Key Renewal Request in this section and the Key Distribution Request in Section 4.8.1.1. The former asks the KDC for new individual keying material, while the latters asks the KDC for the current group keying material together with the current individual keying material.

As discussed in Section 4.8.2, application profiles of this specification may define alternative outcomes for the Key Renewal Request-Response exchange (OPT12), where the provisioning of new individual keying material is replaced by or combined with the execution of a whole group rekeying.

4.8.3. DELETE Handler

The DELETE handler removes the node identified by NODENAME from the group identified by GROUPNAME.

The handler expects a DELETE request with empty payload.

In addition to what is defined in Section 4.1.2, the handler verifies that the Client is a current member of the group. If the verification fails, the KDC MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 0 ("Operation permitted only to group members").

If all verification succeeds, the handler performs the actions defined in Section 5 and replies with a 2.02 (Deleted) response with empty payload.

4.8.3.1. Leave the Group

A Client can actively request to leave the group. In this case, the Client sends a CoAP DELETE request to the endpoint /ace-group/GROUPNAME/nodes/NODENAME at the KDC, where GROUPNAME is the group name and NODENAME is its node name, formatted as defined in Section 4.8.3

Note that, after having left the group, the Client may wish to join it again. Then, as long as the Client is still authorized to join the group, i.e., the associated access token is still valid, the Client can request to re-join the group directly to the KDC (see Section 4.3.1.1), without having to retrieve a new access token from the AS.

4.9. /ace-group/GROUPNAME/nodes/NODENAME/pub-key

This resource implements the POST handler.

4.9.1. POST Handler

The POST handler is used to replace the stored public key of this Client (identified by NODENAME) with the one specified in the request at the KDC, for the group identified by GROUPNAME.

The handler expects a POST request with payload as specified in Section 4.3.1, with the difference that it includes only the parameters 'client_cred', 'cnonce' and 'client_cred_verify'. In particular, the PoP evidence included in 'client_cred_verify' is computed in the same way considered in Section 4.3.1 and defined by the specific application profile (REQ14), with a newly generated N_C nonce and the previously received N_S. It is REQUIRED of the application profiles to define the specific formats of public keys that are acceptable to use in the group (REQ6).

In addition to what is defined in Section 4.1.2 and at the beginning of Section 4.8, the handler verifies that this operation is consistent with the set of roles that the node has in the group. If the verification fails, the KDC MUST reply with a 4.00 (Bad Request) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 1 ("Request inconsistent with the current roles").

If the KDC cannot retrieve the 'kdcchallenge' associated to this Client (see Section 3.3), the KDC MUST reply with a 4.00 (Bad Request) error response, which MUST also have Content-Format application/ace-groupcomm+cbor. The payload of the error response is a CBOR map including a newly generated 'kdcchallenge' value. This is specified in the 'kdcchallenge' parameter. In such a case the KDC MUST store the newly generated value as the 'kdcchallenge' value associated to this Client, possibly replacing the currently stored value.

Otherwise, the handler checks that the public key specified in the 'client_cred' field is valid for the group identified by GROUPNAME. That is, the handler checks that the public key is encoded according to the format used in the group, is intended for the public key algorithm used in the group, and is aligned with the possible associated parameters used in the group. If that cannot be successfully verified, the handler MUST reply with a 4.00 (Bad Request) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 2 ("Public key incompatible with the group configuration").

Otherwise, the handler verifies the PoP evidence contained in the 'client_cred_verify' field of the request, by using the public key specified in the 'client_cred' field, as well as the same way considered in Section 4.3.1 and defined by the specific application profile (REQ14). If the PoP evidence does not pass verification, the handler MUST reply with a 4.00 (Bad Request) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 3 ("Invalid Proof-of-Possession evidence").

If all verifications succeed, the handler performs the following actions.

* The handler associates the public key from the 'client_cred' field of the request to the node identifier NODENAME and to the access token associated to the node identified by NODENAME.

* In the stored list of group members' public keys for the group identified by GROUPNAME, the handler replaces the public key of the node identified by NODENAME with the public key specified in the 'client_cred' field of the request.

Then, the handler replies with a 2.04 (Changed) response, which does not include a payload.

4.9.1.1. Uploading a New Public Key

In case the KDC maintains the public keys of group members, a node in the group can contact the KDC to upload a new public key to use in the group, and replace the currently stored one.

To this end, the Client performs a Public Key Update Request/Response exchange with the KDC, i.e., it sends a CoAP POST request to the /ace-group/GROUPNAME/nodes/NODENAME/pub-key endpoint at the KDC, where GROUPNAME is the group name and NODENAME is its node name.

The request is formatted as specified in Section 4.9.1.

Figure Figure 31 gives an overview of the exchange described above, while Figure 32 shows an example.

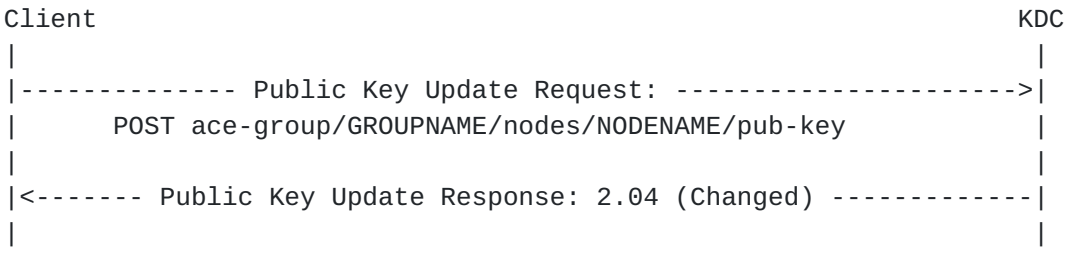


Figure 31: Message Flow of Public Key Update Request-Response

Request:

```
Header: POST (Code=0.02)
Uri-Host: "kdc.example.com"
Uri-Path: "ace-group"
Uri-Path: "g1"
Uri-Path: "nodes"
Uri-Path: "c101"
Uri-Path: "pub-key"
Content-Format: "application/ace-groupcomm+cbor"
Payload (in CBOR diagnostic notation, with PUB_KEY
         and POP_EVIDENCE being CBOR byte strings):
  { "client_cred": PUB_KEY, "cnonce": h'9ff7684414affcc8',
    "client_cred_verify": POP_EVIDENCE }
```

Response:

```
Header: Changed (Code=2.04)
Payload: -
```

Figure 32: Example of Public Key Update Request-Response

Additionally, after updating its own public key, a group member MAY send a number of requests including an identifier of the updated public key, to notify other group members that they have to retrieve it. How this is done depends on the group communication protocol used, and therefore is application profile specific (OPT13).

5. Removal of a Group Member

A Client identified by NODENAME may be removed from a group identified by GROUPNAME where it is a member, due to the following reasons.

1. The Client explicitly asks to leave the group, as defined in Section 4.8.3.1.

2. The node has been found compromised or is suspected so.

3. The Client's authorization to be a group member with the current roles is not valid anymore, i.e., the access token has expired or has been revoked. If the AS provides token introspection (see Section 5.9 of [I-D.ietf-ace-oauth-authz]), the KDC can optionally use it and check whether the Client is still authorized.

In either case, the KDC performs the following actions.

* The KDC removes the Client from the list of current members or the group.

* In case of forced eviction, i.e., for cases 2 and 3 above, the KDC deletes the public key of the removed Client, if it acts as repository of public keys for group members.

* If the removed Client is registered as an observer of the group-membership resource at ace-group/GROUPNAME, the KDC removes the Client from the list of observers of that resource.

* If the sub-resource nodes/NODENAME was created for the removed Client, the KDC deletes that sub-resource.

  In case of forced eviction, i.e., for cases 2 and 3 above, the KDC MAY explicitly inform the removed Client, by means of the following methods.

  - If the evicted Client implements the 'control_uri' resource specified in Section 4.3.1, the KDC sends a DELETE request, targeting the URI specified in the 'control_uri' parameter of the Joining Request (see Section 4.3.1).

  - If the evicted Client is observing its associated sub-resource at ace-group/GROUPNAME/nodes/NODENAME (see Section 4.8.1), the KDC sends an unsolicited 4.04 (Not Found) error response, which does not include the Observe option and indicates that the observed resource has been deleted (see Section 3.2 of [RFC7641]).

    The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 5 ("Group membership terminated").

* If the application requires forward security or the used application profile requires so, the KDC MUST generate new group keying material and securely distribute it to all the current group members except the leaving node (see Section 6).

6. Group Rekeying Process

A group rekeying is started and driven by the KDC. The KDC is not intended to accommodate explicit requests from group members to trigger a group rekeying. That is, the scheduling and execution of a group rekeying is an exclusive prerogative of the KDC. Reasons that can trigger a group rekeying are a change in the group membership, the current group keying material approaching its expiration time, or a regularly scheduled update of the group keying material.

The KDC MUST increment the version number NUM of the current keying material, before distributing the newly generated keying material with version number NUM+1 to the group. Once completed the group rekeying, the KDC MUST delete the old keying material and SHOULD store the newly distributed keying material in persistent storage.

Distributing the new group keying material requires the KDC to send multiple rekeying messages to the group members. Depending on the rekeying scheme used in the group and the reason that has triggered the rekeying process, each rekeying message can be intended to one or multiple group members, hereafter referred to as target group members. The KDC MUST support at least the "Point-to-Point" group rekeying scheme in Section 6.1 and MAY support additional ones.

Each rekeying message MUST have Content-Format set to application/ace-groupcomm+cbor and its payload formatted as a CBOR map, which MUST include at least the information specified in the Key Distribution Response message (see Section 4.3.2), i.e., the parameters 'gkty', 'key' and 'num' defined in Section 4.3.1. The CBOR map MAY include the parameter 'exp', as well as the parameter 'mgt_key_material' specifying new administrative keying material for the target group members, if relevant for the used rekeying scheme.

A rekeying message may include additional information, depending on the rekeying scheme used in the group, the reason that has triggered the rekeying process and the specific target group members. In particular, if the group rekeying is performed due to one or multiple Clients that have joined the group and the KDC acts as repository of public keys of the group members, then a rekeying message MAY also include the public keys that those Clients use in the group, together with the roles and node identifier that the corresponding Client has in the group. It is RECOMMENDED to specify this information by means of the parameters 'pub_keys', 'peer_roles' and 'peer_identifiers', like done in the Joining Response message (see Section 4.3.1).

The complete format of a rekeying message, including the encoding and content of the 'mgt_key_material' parameter, has to be defined in separate specifications aimed at profiling the used rekeying scheme in the context of the used application profile of this specification. As a particular case, an application profile of this specification MAY define additional information to include in rekeying messages for the "Point-to-Point" group rekeying scheme in Section 6.1 (OPT14).

Consistently with the used group rekeying scheme, the actual delivery of rekeying messages can occur through different approaches, as discussed in the following.

6.1. Point-to-Point Group Rekeying

This approach consists in the KDC sending one individual rekeying message to each target group member. In particular, the rekeying message is protected by means of the security association between the KDC and the target group member in question, as per the used application profile of this specification and the used transport profile of ACE.

This is the approach taken by the basic "Point-to-Point" group rekeying scheme, that the KDC can explicitly signal in the Joining Response (see Section 4.3.1), through the 'rekeying_scheme' parameter specifying the value 0.

When taking this approach in the group identified by GROUPNAME, the KDC can practically deliver the rekeying messages to the target group members in different, co-existing ways.

* The KDC SHOULD make the ace-group/GROUPNAME resource Observable [RFC7641]. Thus, upon performing a group rekeying, the KDC can distribute the new group keying material through individual notification responses sent to the target group members that are also observing that resource.

In case the KDC deletes the group, this also allows the KDC to send an unsolicited 4.04 (Not Found) response to each observer group member, as a notification of group termination. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4. The value of the 'error' field MUST be set to 6 ("Group deleted").

* If a target group member specified a URI in the 'control_uri' parameter of the Joining Request upon joining the group (see Section 4.3.1), the KDC can provide that group member with the new group keying material by sending a unicast POST request to that URI.

  A Client that does not plan to observe the ace-group/GROUPNAME resource at the KDC SHOULD provide a URI in the 'control_uri' parameter of the Joining Request upon joining the group.

If the KDC has to send a rekeying message to a target group member, but this did not include the 'control_uri' parameter in the Joining Request and is not a registered observer for the ace-group/GROUPNAME resource, then that target group member would not be able to participate to the group rekeying. Later on, after having repeatedly failed to successfully exchange secure messages in the group, that group member can retrieve the current group keying material from the KDC, by sending a GET request to ace-group/GROUPNAME or ace-group/GROUPNAME/nodes/NODENAME (see Section 4.3.2 and Section 4.8.1, respectively).

6.2. One-to-Many Group Rekeying

This section provides high-level recommendations on how the KDC can rekey a group by means of a more efficient and scalable group rekeying scheme, e.g., [RFC2093][RFC2094][RFC2627]. That is, each rekeying message might be, and likely is, intended to multiple target group members, and thus can be delivered to the whole group, although possible to decrypt only for the actual target group members.

This yields an overall lower number of rekeying messages, thus potentially reducing the overall time required to rekey the group. On the other hand, it requires the KDC to provide and use additional administrative keying material to protect the rekeying messages, and to additionally sign them to ensure source authentication (see Section 6.2.1). Typically, this pays off in large-scale groups, where the introduced performance overhead is less than what experienced by rekeying the group in a point-to-point fashion (see Section 6.1).

The exact set of rekeying messages to send, their content and format, the administrative keying material to use to protect them, as well as the set of target group members depend on the specific group rekeying scheme, and are typically affected by the reason that has triggered the group rekeying. Details about the data content and format of rekeying messages have to be defined by separate documents profiling the use of the group rekeying scheme, in the context of the used application profile of this specification.

When one of these group rekeying schemes is used, the KDC provides a number of related information to a Client joining the group in the Joining Response message (see Section 4.3.1). In particular, 'rekeying_scheme' identifies the rekeying scheme used in the group (if no default can be assumed); 'control_group_uri', if present, specifies a URI with a multicast address where the KDC will send the rekeying messages for that group; 'mgt_key_material' specifies a subset of the administrative keying material intended for that particular joining Client to have, as used to protect the rekeying messages sent to the group when intended also to that joining Client.

Rekeying messages can be protected at the application layer, by using COSE and the administrative keying material as prescribed by the specific group rekeying scheme (see Section 6.2.1). After that, the delivery of protected rekeying messages to the intended target group members can occur in different ways, such as the following ones.

* Over multicast - In this case, the KDC simply sends a rekeying message as a CoAP request addressed to the multicast URI specified in the 'control_group_uri' parameter of the Joining Response (see Section 4.3.1).

  If a particular rekeying message is intended to a single target group member, the KDC may alternatively protect the message using the security association with that group member, and deliver the message like when using the "Point-to-Point" group rekeying scheme (see Section 6.1).

* Through a pub-sub communication model - In this case, the KDC acts as publisher and publishes each rekeying message to a specific "rekeying topic", which is associated to the group and is hosted at a broker server. Following their group joining, the group members subscribe to the rekeying topic at the broker, thus receiving the group rekeying messages as they are published by the KDC.

  In order to make such message delivery more efficient, the rekeying topic associated to a group can be further organized into subtopics. For instance, the KDC can use a particular subtopic to

address a particular set of target group members during the rekeying process, as possibly aligned to a similar organization of the administrative keying material (e.g., a key hierarchy).

The setup of rekeying topics at the broker as well as the discovery of the topics at the broker for group members are application specific. A possible way is for the KDC to provide such information in the Joining Response message (see Section 4.3.1), by means of a new parameter analogous to 'control_group_uri' and specifying the URI(s) of the rekeying topic(s) that a group member has to subscribe to at the broker.

Regardless the specifically used delivery method, the group rekeying scheme can perform a possible roll-over of the administrative keying material through the same sent rekeying messages. Actually, such a roll-over occurs every time a group rekeying is performed upon the leaving of group members, which have to be excluded from future communications in the group.

From a high level point of view, each group member owns only a subset of the overall administrative keying material, obtained upon joining the group. Then, when a group rekeying occurs:

* Each rekeying message is protected by using a (most convenient) key from the administrative keying material such that: i) the used key is not owned by any node leaving the group, i.e. the key is safe to use and does not have to be renewed; and ii) the used key is owned by all the target group members, that indeed have to be provided with new group keying material to protect communications in the group.

* Each rekeying message includes not only the new group keying material intended to all the rekeyed group members, but also any new administrative keys that: i) are pertaining to and supposed to be owned by the target group members; and ii) had to be updated since leaving group members own the previous version.

Further details depend on the specific rekeying scheme used in the group.

6.2.1. Protection of Rekeying Messages

When using a group rekeying scheme relying on one-to-many rekeying messages, the actual data content of each rekeying message is prepared according to what the rekeying scheme prescribes.

Then, the KDC can protect the rekeying message as defined below. The used encryption algorithm which SHOULD be the same one used to protect communications in the group. The method defined below assumes that the following holds for the management keying material specified in the 'mgt_key_material' parameter of the Joining Response (see Section 4.3.1).

* The included symmetric encryption keys are accompanied by a corresponding and unique key identifier assigned by the KDC.

* A Base IV is also included, with the same size of the AEAD nonce considered by the encryption algorithm to use.

First, the KDC computes a COSE_Encrypt0 object as follows.

* The encryption key to use is selected from the administrative keying material, as defined by the rekeying scheme used in the group.

* The plaintext is the actual data content of the rekeying message.

* The Additional Authenticated Data (AAD) is empty, unless otherwise specified by separate documents profiling the use of the group rekeying scheme.

* Since the KDC is the only sender of rekeying messages, the AEAD nonce can be computed as follows, where NONCE_SIZE is the size in bytes of the AEAD nonce. Separate documents profiling the use of the group rekeying scheme may define alternative ways to compute the AEAD nonce.

  The KDC considers the following values.

  - COUNT, as a 1-byte unsigned integer associated to the used encryption key. Its value is set to 0 when starting to perform a new group rekeying instance, and is incremented after each use of the encryption key.

  - NEW_NUM, as the version number of the new group keying material to distribute in this rekeying instance, left-padded with zeroes to exactly NONCE_SIZE - 1.

  Then, the KDC computes a Partial IV as the byte string concatenation of COUNT and NEW_NUM, in this order. Finally, the AEAD nonce is computed as the XOR between the Base IV and the Partial IV.

* The protected header of the COSE_Encrypt0 object MUST include the following parameters.

  - 'alg', specifying the used encryption algorithm.

  - 'kid', specifying the identifier of the encryption key from the administrative keying material used to protect this rekeying message.

* The unprotected header of the COSE_Encrypt0 object MUST include the 'Partial IV' parameter, with value the Partial IV computed above.

In order to ensure source authentication, each rekeying message protected with the administrative keying material MUST be signed by the KDC. To this end, the KDC computes a countersignature of the COSE_Encrypt0 object, as described in Sections 3.2 and 3.3 of [I-D.ietf-cose-countersign]. In particular, the following applies when computing the countersignature.

* The Countersign_structure contains the context text string "CounterSignature0".

* The private key of the KDC is used as signing key.

* The payload is the ciphertext of the COSE_Encrypt0 object.

* The Additional Authenticated Data (AAD) is empty, unless otherwise specified by separate documents profiling the use of a group rekeying scheme.

* The protected header of the signing object MUST include the parameter 'alg', specifying the used signature algorithm.

If source authentication of messages exchanged in the group is also ensured by means of signatures, then rekeying messages MUST be signed using the same signature algorithm and related parameters. Also, the KDC's public key used for signature verification MUST me provided in the Joining Response through the 'kdc_cred' parameter, together with the corresponding proof-of-possession (PoP) evidence in the 'kdc_cred_verify' parameter.

If source authentication of messages exchanged in the group is not ensured by means of signatures, then the KDC MUST provide its public key together with a corresponding PoP evidence as part of the management keying material specified in the 'mgt_key_material' parameter of the Joining Response (see Section 4.3.1). It is RECOMMENDED to specify this information by using the same format and

encoding used for the parameters 'kdc_cred', 'kdc_nonce' and 'kdc_cred_verify' in the Joining Response. It is up to separate documents profiling the use of the group rekeying scheme to specify such details.

After that, the KDC specifies the computed countersignature in the 'COSE_Countersignature0' header parameter of the COSE_Encrypt0 object.

Finally, the KDC specifies the COSE_Encrypt0 object as payload of a CoAP request, which is sent to the target group members as per the used message delivery method.

7. Extended Scope Format

This section defines an extended format of binary encoded scope, which additionally specifies the semantics used to express the same access control information from the corresponding original scope.

As also discussed in Section 3.2, this enables a Resource Server to unambiguously process a received access token, also in case the Resource Server runs multiple applications or application profiles that involve different scope semantics.

The extended format is intended only for the 'scope' claim of access tokens, for the cases where the claim takes as value a CBOR byte string. That is, the extended format does not apply to the 'scope' parameter included in ACE messages, i.e., the Authorization Request and Authorization Response exchanged between the Client and the Authorization Server (see Sections 5.8.1 and 5.8.2 of [I-D.ietf-ace-oauth-authz]), the AS Request Creation Hints message from the Resource Server (see Section 5.3 of [I-D.ietf-ace-oauth-authz]), and the Introspection Response from the Authorization Server (see Section 5.9.2 of [I-D.ietf-ace-oauth-authz]).

The value of the 'scope' claim following the extended format is composed as follows. Given the original scope using a semantics SEM and encoded as a CBOR byte string, the corresponding extended scope is encoded as a tagged CBOR byte string, wrapping a CBOR sequence [RFC8742] of two elements. In particular:

* The first element of the sequence is a CBOR integer, and identifies the semantics SEM used for this scope. The value of this element has to be taken from the "Value" column of the "ACE Scope Semantics" registry defined in Section 11.12 of this specification.

When defining a new semantics for a binary scope, it is up to the applications and application profiles to define and register the corresponding integer identifier (REQ28).

* The second element of the sequence is the original scope using the semantics SEM, encoded as a CBOR byte string.

Finally, the CBOR byte string wrapping the CBOR sequence is tagged, and identified by the CBOR tag TBD_TAG "ACE Extended Scope Format", defined in Section 11.6 of this specification.

The resulting tagged CBOR byte string is used as value of the 'scope' claim of the access token.

The usage of the extended scope format is not limited to application profiles of this specification or to applications based on group communication. Rather, it is generally applicable to any application and application profile where access control information in the access token is expressed as a binary encoded scope.

Figure 33 and Figure 34 build on the examples in Section 3.2, and show the corresponding extended scopes.

```
gname = tstr

permissions = uint . bits roles

roles = &(
   Requester: 1,
   Responder: 2,
   Monitor: 3,
   Verifier: 4
)

scope_entry = AIF_Generic<gname, permissions>

scope = << [ + scope_entry ] >>

semantics = int

; This defines an array, the elements
; of which are to be used in a CBOR Sequence:
sequence = [semantics, scope]

extended_scope = #6.TBD_TAG(<< sequence >>)
```

Figure 33: Example CDLL definition of scope, using the default Authorization Information Format

```
gname = tstr

role = tstr

scope_entry = [ gname , ? ( role / [ 2*role ] ) ]

scope = << [ + scope_entry ] >>

semantics = int

; This defines an array, the elements
; of which are to be used in a CBOR Sequence:
sequence = [semantics, scope]

extended_scope = #6.TBD_TAG(<< sequence >>)
```

Figure 34: CDLL definition of scope, using as example group name encoded as tstr and role as tstr

8. ACE Groupcomm Parameters

This specification defines a number of parameters used during the second part of the message exchange, after the exchange of Token Transfer Request and Response. The table below summarizes them, and specifies the CBOR key to use instead of the full descriptive name.

Note that the media type application/ace-groupcomm+cbor MUST be used when these parameters are transported in the respective message fields.

Name	CBOR Key	CBOR Type	Reference
error	TBD	int	[this document]
error_description	TBD	tstr	[this document]
gid	TBD	array	[this document]
gname	TBD	array of tstr	[this document]
guri	TBD	array of tstr	[this document]
scope	TBD	bstr	[this document]
get_pub_keys	TBD	array / nil	[this document]

client_cred	TBD	bstr	[this document]
cnonce	TBD	bstr	[this document]
client_cred_verify	TBD	bstr	[this document]
pub_keys_repos	TBD	tstr	[this document]
control_uri	TBD	tstr	[this document]
gkty	TBD	int / tstr	[this document]
key	TBD	See the "ACE Groupcomm Key Types" registry	[this document]
num	TBD	int	[this document]
ace-groupcomm-profile	TBD	int	[this document]
exp	TBD	int	[this document]
pub_keys	TBD	array	[this document]
peer_roles	TBD	array	[this document]
peer_identifiers	TBD	array	[this document]
group_policies	TBD	map	[this document]
kdc_cred	TBD	bstr	[this document]
kdc_nonce	TBD	bstr	[this document]
kdc_cred_verify	TBD	bstr	[this document]
rekeying_scheme	TBD	int	[this document]
mgt_key_material	TBD	bstr	[this document]
control_group_uri	TBD	tstr	[this document]
sign_info	TBD	array	[this document]
kdcchallenge	TBD	bstr	[this document]

Figure 35: ACE Groupcomm Parameters

The KDC is expected to support and understand all the parameters above. Instead, a Client can support and understand only a subset of such parameters, depending on the roles it expects to take in the joined groups or on other conditions defined in application profiles of this specification.

In the following, the parameters are categorized according to the support expected by Clients. That is, a Client that supports a parameter is able to: i) use and specify it in a request message to the KDC; and ii) understand and process it if specified in a response message from the KDC. It is REQUIRED of application profiles of this specification to sort their newly defined parameters according to the same categorization (REQ29).

Note that the actual use of a parameter and its inclusion in a message depends on the specific exchange, the specific Client and group involved, as well as what is defined in the used application profile of this specification.

A Client MUST support the following parameters.

* 'scope', 'gkty', 'key', 'num', 'exp', 'gid', 'gname', 'guri', 'pub_keys', 'peer_identifiers', 'ace_groupcomm_profile', 'control_uri', 'rekeying_scheme'.

A Client SHOULD support the following parameter.

* 'get_pub_keys'. That is, not supporting this parameter would yield the inconvenient and undesirable behavior where: i) the Client does not ask for the other group members' public keys upon joining the group (see Section 4.3.1.1); and ii) later on as a group member, the Client only retrieves the public keys of all group members (see Section 4.4.2.1).

A Client MAY support the following optional parameters. Application profiles of this specification MAY define that Clients must or should support these parameters instead (OPT15).

* 'error', 'error_description'.

The following conditional parameters are relevant only if specific conditions hold. It is REQUIRED of application profiles of this specification to define whether Clients must, should or may support these parameters, and under which circumstances (REQ30).

* 'client_cred', 'cnonce', 'client_cred_verify'. These parameters are relevant for a Client that has a public key to use in a joined group.

* 'kdcchallenge'. This parameter is relevant for a Client that has a public key to use in a joined group and that provides the access token to the KDC through a Token Transfer Request (see Section 3.3).

* 'pub_keys'repo'. This parameter is relevant for a Client that has a public key to use in a joined group and that makes it available from a key repository different than the KDC.

* 'group_policies'. This parameter is relevant for a Client that is interested in the specific policies used in a group, but it does not know them or cannot become aware of them before joining that group.

* 'peer_roles'. This parameter is relevant for a Client that has to know about the roles of other group members, especially when retrieving and handling their corresponding public keys.

* 'kdc_nonce', 'kdc_cred', 'kdc_cred_verify'. These parameters are relevant for a Client that joins a group for which, as per the used application profile of this specification, the KDC has an associated public key and this is required for the correct group operation.

* 'mgt_key_material'. This parameter is relevant for a Client that supports an advanced rekeying scheme possibly used in the group, such as based on one-to-many rekeying messages sent over IP multicast.

* 'control_group_uri'. This parameter is relevant for a Client that supports the hosting of local resources each associated to a group (hence acting as CoAP server) and the reception of one-to-many requests sent to those resources by the KDC (e.g., over IP multicast), targeting multiple members of the corresponding group. Examples of related management operations that the KDC can perform by this means are the eviction of group members and the execution of a group rekeying process through an advanced rekeying scheme, such as based on one-to-many rekeying messages.

9. ACE Groupcomm Error Identifiers

This specification defines a number of values that the KDC can include as error identifiers, in the 'error' field of an error response with Content-Format application/ace-groupcomm+cbor.

Value	Description
0	Operation permitted only to group members
1	Request inconsistent with the current roles
2	Public key incompatible with the group configuration
3	Invalid proof-of-possession evidence
4	No available node identifiers
5	Group membership terminated
6	Group deleted

Figure 36: ACE Groupcomm Error Identifiers

A Client supporting the 'error' parameter (see Section 4.1.2 and Section 8) and able to understand the specified error may use that information to determine what actions to take next. If it is included in the error response and supported by the Client, the 'error_description' parameter may provide additional context.

In particular, the following guidelines apply, and application profiles of this specification can define more detailed actions for the Client to take when learning that a specific error has occurred.

* In case of error 0, the Client should stop sending the request in question to the KDC. Rather, the Client should first join the targeted group. If it has not happened already, this first requires the Client to obtain an appropriate access token authorizing access to the group and provide it to the KDC.

* In case of error 1, the Client as a group member should re-join the group with all the roles needed to perform the operation in question. This might require the Client to first obtain a new access token and provide it to the KDC, if the current access token does not authorize to take those roles in the group. For operations admitted to a Client which is not a group member (e.g., an external signature verifier), the Client should first obtain a new access token authorizing to also have the missing roles.

* In case of error 2, the Client has to obtain or self-generate a different asymmetric key pair, as aligned to the publick key algorithms, parameters and encoding used in the targeted group. After that, the Client should provide its new consistent public key to the KDC.

* In case of error 3, the Client should ensure to be computing its proof-of-possession evidence by correctly using the parameters and procedures defined in the used application profile of this specification. In an unattended setup, it might be not possible for a Client to autonomously diagnose the error and take an effective next action to address it.

* In case of error 4, the Client should wait for a certain (pre-configured) amount of time, before trying re-sending its request to the KDC.

* In case of error 5, the Client may try joining the group again. This might require the Client to first obtain a new access token and provide it to the KDC, e.g., if the current access token has expired.

* In case of error 6, the Client should clean up its state regarding the group, just like if it has left the group with no intention to re-join it.

10. Security Considerations

Security considerations are inherited from the ACE framework [I-D.ietf-ace-oauth-authz], and from the specific transport profile of ACE used between the Clients and the KDC, e.g., [I-D.ietf-ace-dtls-authorize] and [I-D.ietf-ace-oscore-profile].

Furthermore, the following security considerations apply.

10.1. Secure Communication in the Group

When a group member receives a message from a certain sender for the first time since joining the group, it needs to have a mechanism in place to avoid replayed messages, e.g., Appendix B.2 of [RFC8613] or Appendix E of [I-D.ietf-core-oscore-groupcomm]. Such a mechanism aids the recipient group member also in case it has rebooted and lost the security state used to protect previous group communications with that sender.

By its nature, the KDC is invested with a large amount of trust, since it acts as generator and provider of the symmetric keying material used to protect communications in each of its groups. While

details depend on the specific communication and security protocols used in the group, the KDC is in the position to decrypt messages exchanged in the group as if it was also a group member, as long as those are protected through commonly shared group keying material.

A compromised KDC would thus put the attacker in the same position, which also means that:

* The attacker can generate and control new group keying material, hence possibly rekeying the group and evicting certain group members as part of a broader attack.

* The attacker can actively participate to communications in a group even without been authorized to join it, and can allow further unauthorized entities to do so.

* The attacker can build erroneous associations between node identifiers and group members' public keys.

On the other hand, as long as the security protocol used in the group ensures source authentication of messages (e.g., by means of signatures), the KDC is not able to impersonate group members since it does now own their private keys.

Further security considerations are specific of the communication and security protocols used in the group, and thus have to be provided by those protocols and complemented by the application profiles of this specification using them.

10.2. Update of Group Keying Material

Due to different reasons, the KDC can generate new group keying material and provide it to the group members (rekeying) through the rekeying scheme used in the group, as discussed in Section 6.

In particular, the KDC must renew the group keying material latest upon its expiration. Before then, the KDC may also renew the group keying material on a regular or periodical fashion.

The KDC should renew the group keying material upon a group membership change. Since the minimum number of group members is one, the KDC should provide also a Client joining an empty group with new keying material never used before in that group. Similarly, the KDC should provide new group keying material also to a Client that remains the only member in the group after the leaving of other group members.

Note that the considerations in Section 10.1 about dealing with replayed messages still hold, even in case the KDC rekeys the group upon every single joining of a new group member. However, if the KDC has renewed the group keying material upon a group member's joining, and the time interval between the end of the rekeying process and that member's joining is sufficiently small, then that group member is also on the safe side, since it would not accept replayed messages protected with the old group keying material previous to its joining.

The KDC may enforce a rekeying policy that takes into account the overall time required to rekey the group, as well as the expected rate of changes in the group membership. That is, the KDC may not rekey the group at each and every group membership change, for instance if members' joining and leaving occur frequently and performing a group rekeying takes too long. Instead, the KDC might rekey the group after a minimum number of group members have joined or left within a given time interval, or after a maximum amount of time since the last group rekeying was completed, or yet during predictable network inactivity periods.

However, this would result in the KDC not constantly preserving backward and forward security in the group. That is:

* Newly joining group members would be able to access the keying material used before their joining, and thus they could access past group communications if they have recorded old exchanged messages. This might still be acceptable for some applications and in situations where the new group members are freshly deployed through strictly controlled procedures.

* The leaving group members would remain able to access upcoming group communications, as protected with the current keying material that has not been updated. This is typically undesirable, especially if the leaving group member is compromised or suspected to be, and it might have an impact or compromise the security properties of the protocols used in the group to protect messages exchanged among the group member.

The KDC should renew the group keying material in case it has rebooted, even in case it stores the whole group keying material in persistent storage. This assumes that the secure associations with the current group members as well as any administrative keying material required to rekey the group are also stored in persistent storage.

However, if the KDC relies on Observe notifications to distribute the new group keying material, the KDC would have lost all the current ongoing Observations with the group members after rebooting, and the

group members would continue using the old group keying material. Therefore, the KDC will rather rely on each group member asking for the new group keying material (see Section 4.3.2.1 and Section 4.8.1.1), or rather perform a group rekeying by actively sending rekeying messages to group members as discussed in Section 6.

The KDC needs to have a mechanism in place to detect DoS attacks from nodes repeatedly performing actions that might trigger a group rekeying. Such actions can include leaving and/or re-joining the group at high rates, or often asking the KDC for new indidivual keying material. Ultimately, the KDC can resort to removing these nodes from the group and (temperorarily) preventing them from joining the group again.

The KDC also needs to have a congestion control mechanism in place, in order to avoid network congestion upon distributing new group keying material. For example, CoAP and Observe give guidance on such mechanisms, see Section 4.7 of [RFC7252] and Section 4.5.1 of [RFC7641].

A node that has left the group should not expect any of its outgoing messages to be successfully processed, if received by other nodes after its leaving, due to a possible group rekeying occurred before the message reception.

10.2.1. Misalignment of Group Keying Material

A group member can receive a message shortly after the group has been rekeyed, and new keying material has been distributed by the KDC (see Section 6). In the following two cases, this may result in misaligned keying material between the group members.

In the first case, the sender protects a message using the old group keying material. However, the recipient receives the message after having received the new group keying material, hence not being able to correctly process it. A possible way to ameliorate this issue is to preserve the old, recent group keying material for a maximum amount of time defined by the application, during which it is used solely for processing incoming messages. By doing so, the recipient can still temporarily process received messages also by using the old, retained group keying material. Note that a former (compromised) group member can take advantage of this by sending messages protected with the old, retained group keying material. Therefore, a conservative application policy should not admit the storage of old group keying material. Eventually, the sender will have obtained the new group keying material too, and can possibly re-send the message protected with such keying material.

In the second case, the sender protects a message using the new group keying material, but the recipient receives that message before having received the new group keying material. Therefore, the recipient would not be able to correctly process the message and hence discards it. If the recipient receives the new group keying material shortly after that and the application at the sender endpoint performs retransmissions, the former will still be able to receive and correctly process the message. In any case, the recipient should actively ask the KDC for the latest group keying material according to an application-defined policy, for instance after a given number of unsuccessfully decrypted incoming messages.

10.3. Block-Wise Considerations

If the Block-Wise CoAP options [RFC7959] are used, and the keying material is updated in the middle of a Block-Wise transfer, the sender of the blocks just changes the group keying material to the updated one and continues the transfer. As long as both sides get the new group keying material, updating group the keying material in the middle of a transfer will not cause any issue. Otherwise, the sender will have to transmit the message again, when receiving an error message from the recipient.

Compared to a scenario where the transfer does not use Block-Wise, depending on how fast the group keying material is changed, the group members might consume a larger amount of the network bandwidth by repeatedly resending the same blocks, which might be problematic.

11. IANA Considerations

This document has the following actions for IANA.

11.1. Media Type Registrations

This specification registers the 'application/ace-groupcomm+cbor' media type for messages of the protocols defined in this document following the ACE exchange and carrying parameters encoded in CBOR. This registration follows the procedures specified in [RFC6838].

Type name: application

Subtype name: ace-groupcomm+cbor

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Must be encoded as CBOR map containing the protocol parameters defined in [this document].

Security considerations: See Section 10 of this document.

Interoperability considerations: n/a

Published specification: [this document]

Applications that use this media type: The type is used by Authorization Servers, Clients and Resource Servers that support the ACE groupcomm framework as specified in [this document].

Fragment identifier considerations: N/A

Additional information: N/A

Person & email address to contact for further information: iesg@ietf.org (mailto:iesg@ietf.org)

Intended usage: COMMON

Restrictions on usage: None

Author: Francesca Palombini francesca.palombini@ericsson.com (mailto:francesca.palombini@ericsson.com)

Change controller: IESG

11.2. CoAP Content-Formats

IANA is asked to register the following entry to the "CoAP Content-Formats" registry within the "CoRE Parameters" registry group.

Media Type: application/ace-groupcomm+cbor

Encoding: -

ID: TBD

Reference: [this document]

11.3. OAuth Parameters

IANA is asked to register the following entries in the "OAuth Parameters" registry following the procedure specified in Section 11.2 of [RFC6749].

* Parameter name: sign_info

* Parameter usage location: client-rs request, rs-client response

* Change Controller: IESG

* Specification Document(s): [[This specification]]

* Parameter name: kdcchallenge

* Parameter usage location: rs-client response

* Change Controller: IESG

* Specification Document(s): [[This specification]]

11.4. OAuth Parameters CBOR Mappings

IANA is asked to register the following entries in the "OAuth Parameters CBOR Mappings" registry following the procedure specified in Section 8.10 of [I-D.ietf-ace-oauth-authz].

* Name: sign_info

* CBOR Key: TBD (range -256 to 255)

* Value Type: Simple value null / array

* Reference: [[This specification]]

* Name: kdcchallenge

* CBOR Key: TBD (range -256 to 255)

* Value Type: Byte string

* Reference: [[This specification]]

11.5. Interface Description (if=) Link Target Attribute Values

IANA is asked to register the following entry in the "Interface Description (if=) Link Target Attribute Values" registry within the "CoRE Parameters" registry group.

* Attribute Value: ace.group

* Description: The 'ace group' interface is used to provision keying material and related information and policies to members of a group using the Ace framework.

* Reference: [This Document]

11.6. CBOR Tags

IANA is asked to register the following entry in the "CBOR Tags" registry.

* Tag : TBD_TAG

* Data Item: byte string

* Semantics: Extended ACE scope format, including the identifier of the used scope semantics.

* Reference: [This Document]

11.7. ACE Groupcomm Parameters

This specification establishes the "ACE Groupcomm Parameters" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15.

The columns of this registry are:

* Name: This is a descriptive name that enables easier reference to the item. The name MUST be unique. It is not used in the encoding.

* CBOR Key: This is the value used as CBOR key of the item. These values MUST be unique. The value can be a positive integer, a negative integer, or a string.

* CBOR Type: This contains the CBOR type of the item, or a pointer to the registry that defines its type, when that depends on another item.

* Reference: This contains a pointer to the public specification for the item.

This registry has been initially populated by the values in Section 8. The Reference column for all of these entries refers to sections of this document.

11.8. ACE Groupcomm Key Types

This specification establishes the "ACE Groupcomm Key Types" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15.

The columns of this registry are:

* Name: This is a descriptive name that enables easier reference to the item. The name MUST be unique. It is not used in the encoding.

* Key Type Value: This is the value used to identify the keying material. These values MUST be unique. The value can be a positive integer, a negative integer, or a text string.

* Profile: This field may contain one or more descriptive strings of application profiles to be used with this item. The values should be taken from the Name column of the "ACE Groupcomm Profiles" registry.

* Description: This field contains a brief description of the keying material.

* References: This contains a pointer to the public specification for the format of the keying material, if one exists.

This registry has been initially populated by the values in Figure 10. The specification column for all of these entries will be this document.

11.9. ACE Groupcomm Profiles

This specification establishes the "ACE Groupcomm Profiles" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15. It should be noted that, in addition to the expert review, some portions of the registry require a specification, potentially a Standards Track RFC, to be supplied as well.

The columns of this registry are:

* Name: The name of the application profile, to be used as value of the profile attribute.

* Description: Text giving an overview of the application profile and the context it is developed for.

* CBOR Value: CBOR abbreviation for the name of this application profile. Different ranges of values use different registration policies [RFC8126]. Integer values from -256 to 255 are designated as Standards Action. Integer values from -65536 to -257 and from 256 to 65535 are designated as Specification Required. Integer values greater than 65535 are designated as Expert Review. Integer values less than -65536 are marked as Private Use.

* Reference: This contains a pointer to the public specification of the abbreviation for this application profile, if one exists.

11.10. ACE Groupcomm Policies

This specification establishes the "ACE Groupcomm Policies" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15. It should be noted that, in addition to the expert review, some portions of the registry require a specification, potentially a Standards Track RFC, to be supplied as well.

The columns of this registry are:

* Name: The name of the group communication policy.

* CBOR label: The value to be used to identify this group communication policy. Key map labels MUST be unique. The label can be a positive integer, a negative integer or a string. Integer values between 0 and 255 and strings of length 1 are designated as Standards Track Document required. Integer values from 256 to 65535 and strings of length 2 are designated as Specification Required. Integer values greater than 65535 and strings of length greater than 2 are designated as expert review. Integer values less than -65536 are marked as private use.

* CBOR type: the CBOR type used to encode the value of this group communication policy.

* Description: This field contains a brief description for this group communication policy.

* Reference: This field contains a pointer to the public specification providing the format of the group communication policy, if one exists.

This registry will be initially populated by the values in Figure 11.

11.11. Sequence Number Synchronization Methods

This specification establishes the "Sequence Number Synchronization Methods" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15. It should be noted that, in addition to the expert review, some portions of the registry require a specification, potentially a Standards Track RFC, to be supplied as well.

The columns of this registry are:

* Name: The name of the sequence number synchronization method.

* Value: The value to be used to identify this sequence number synchronization method.

* Description: This field contains a brief description for this sequence number synchronization method.

* Reference: This field contains a pointer to the public specification describing the sequence number synchronization method.

11.12. ACE Scope Semantics

This specification establishes the "ACE Scope Semantics" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15. It should be noted that, in addition to the expert review, some portions of the registry require a specification, potentially a Standards Track RFC, to be supplied as well.

The columns of this registry are:

* Value: The value to be used to identify this scope semantics. The value MUST be unique. The value can be a positive integer or a negative integer. Integer values between 0 and 255 are designated as Standards Track Document required. Integer values from 256 to 65535 are designated as Specification Required. Integer values greater than 65535 are designated as expert review. Integer values less than -65536 are marked as private use.

* Description: This field contains a brief description of the scope semantics.

* Reference: This field contains a pointer to the public specification defining the scope semantics, if one exists.

11.13. ACE Groupcomm Errors

This specification establishes the "ACE Groupcomm Errors" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15. It should be noted that, in addition to the expert review, some portions of the registry require a specification, potentially a Standards Track RFC, to be supplied as well.

The columns of this registry are:

* Value: The value to be used to identify the error. The value MUST be unique. The value can be a positive integer or a negative integer. Integer values between 0 and 255 are designated as Standards Track Document required. Integer values from 256 to 65535 are designated as Specification Required. Integer values greater than 65535 are designated as expert review. Integer values less than -65536 are marked as private use.

* Description: This field contains a brief description of the error.

* Reference: This field contains a pointer to the public specification defining the error, if one exists.

This registry has been initially populated by the values in Section 9. The Reference column for all of these entries refers to this document.

11.14. ACE Groupcomm Rekeying Schemes

This specification establishes the "ACE Groupcomm Rekeying Schemes" IANA registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 11.15. It should be noted that, in addition to the expert review, some portions of the registry require a specification, potentially a Standards Track RFC, to be supplied as well.

The columns of this registry are:

* Value: The value to be used to identify the group rekeying scheme. The value MUST be unique. The value can be a positive integer or a negative integer. Integer values between 0 and 255 are designated as Standards Track Document required. Integer values

from 256 to 65535 are designated as Specification Required. Integer values greater than 65535 are designated as expert review. Integer values less than -65536 are marked as private use.

* Name: The name of the group rekeying scheme.

* Description: This field contains a brief description of the group rekeying scheme.

* Reference: This field contains a pointer to the public specification defining the group rekeying scheme, if one exists.

This registry has been initially populated by the value in Figure 12.

11.15. Expert Review Instructions

The IANA Registries established in this document are defined as expert review. This section gives some general guidelines for what the experts should be looking for, but they are being designated as experts for a reason so they should be given substantial latitude.

Expert reviewers should take into consideration the following points:

* Point squatting should be discouraged. Reviewers are encouraged to get sufficient information for registration requests to ensure that the usage is not going to duplicate one that is already registered and that the point is likely to be used in deployments. The zones tagged as private use are intended for testing purposes and closed environments, code points in other ranges should not be assigned for testing.

* Specifications are required for the standards track range of point assignment. Specifications should exist for specification required ranges, but early assignment before a specification is available is considered to be permissible. Specifications are needed for the first-come, first-serve range if they are expected to be used outside of closed environments in an interoperable way. When specifications are not provided, the description provided needs to have sufficient information to identify what the point is being used for.

* Experts should take into account the expected usage of fields when approving point assignment. The fact that there is a range for standards track documents does not mean that a standards track document cannot have points assigned outside of that range. The length of the encoded value should be weighed against how many code points of that length are left, the size of device it will be used on, and the number of code points left that encode to that size.

12. References

12.1. Normative References

[COSE.Algorithms]
IANA, "COSE Algorithms", <https://www.iana.org/assignments/cose/cose.xhtml#algorithms>.

[COSE.Header.Parameters]
IANA, "COSE Header Parameters", <https://www.iana.org/assignments/cose/cose.xhtml#header-parameters>.

[I-D.ietf-ace-aif]
Bormann, C., "An Authorization Information Format (AIF) for ACE", Work in Progress, Internet-Draft, draft-ietf-ace-aif-03, 24 June 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-aif-03.txt>.

[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)", Work in Progress, Internet-Draft, draft-ietf-ace-oauth-authz-46, 8 November 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-oauth-authz-46.txt>.

[I-D.ietf-core-oscore-groupcomm]
Tiloca, M., Selander, G., Palombini, F., Mattsson, J. P., and J. Park, "Group OSCORE - Secure Group Communication for CoAP", Work in Progress, Internet-Draft, draft-ietf-core-oscore-groupcomm-13, 25 October 2021, <https://www.ietf.org/archive/id/draft-ietf-core-oscore-groupcomm-13.txt>.

[I-D.ietf-cose-countersign]
Schaad, J. and R. Housley, "CBOR Object Signing and Encryption (COSE): Countersignatures", Work in Progress, Internet-Draft, draft-ietf-cose-countersign-05, 23 June 2021, <https://www.ietf.org/archive/id/draft-ietf-cose-countersign-05.txt>.

[I-D.ietf-cose-rfc8152bis-algs]
Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", Work in Progress, Internet-Draft, draft-ietf-cose-rfc8152bis-algs-12, 24 September 2020, <https://www.ietf.org/archive/id/draft-ietf-cose-rfc8152bis-algs-12.txt>.

[I-D.ietf-cose-rfc8152bis-struct]
Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", Work in Progress, Internet-Draft, draft-ietf-cose-rfc8152bis-struct-15, 1 February 2021, <https://www.ietf.org/archive/id/draft-ietf-cose-rfc8152bis-struct-15.txt>.

[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>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/info/rfc6838>.

[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>.

[RFC7967] Bhattacharyya, A., Bandyopadhyay, S., Pal, A., and T. Bose, "Constrained Application Protocol (CoAP) Option for No Server Response", RFC 7967, DOI 10.17487/RFC7967, August 2016, <https://www.rfc-editor.org/info/rfc7967>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[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/info/rfc8610>.

[RFC8742] Bormann, C., "Concise Binary Object Representation (CBOR) Sequences", RFC 8742, DOI 10.17487/RFC8742, February 2020, <https://www.rfc-editor.org/info/rfc8742>.

[RFC8747] Jones, M., Seitz, L., Selander, G., Erdtman, S., and H. Tschofenig, "Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)", RFC 8747, DOI 10.17487/RFC8747, March 2020, <https://www.rfc-editor.org/info/rfc8747>.

[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/info/rfc8949>.

12.2. Informative References

[I-D.ietf-ace-dtls-authorize]
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)", Work in Progress, Internet-Draft, draft-ietf-ace-dtls-authorize-18, 4 June 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-dtls-authorize-18.txt>.

[I-D.ietf-ace-mqtt-tls-profile]
Sengul, C. and A. Kirby, "Message Queuing Telemetry Transport (MQTT)-TLS profile of Authentication and Authorization for Constrained Environments (ACE) Framework", Work in Progress, Internet-Draft, draft-ietf-ace-mqtt-tls-profile-13, 23 October 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-mqtt-tls-profile-13.txt>.

[I-D.ietf-ace-oscore-profile]
Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "OSCORE Profile of the Authentication and Authorization for Constrained Environments Framework", Work in Progress, Internet-Draft, draft-ietf-ace-oscore-profile-19, 6 May 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-oscore-profile-19.txt>.

[I-D.ietf-core-coap-pubsub]
Koster, M., Keranen, A., and J. Jimenez, "Publish-Subscribe Broker for the Constrained Application Protocol (CoAP)", Work in Progress, Internet-Draft, draft-ietf-core-coap-pubsub-09, 30 September 2019, <https://www.ietf.org/archive/id/draft-ietf-core-coap-pubsub-09.txt>.

[I-D.ietf-core-groupcomm-bis]
Dijk, E., Wang, C., and M. Tiloca, "Group Communication for the Constrained Application Protocol (CoAP)", Work in Progress, Internet-Draft, draft-ietf-core-groupcomm-bis-05, 25 October 2021, <https://www.ietf.org/archive/id/draft-ietf-core-groupcomm-bis-05.txt>.

[I-D.tiloca-core-oscore-discovery]
Tiloca, M., Amsuess, C., and P. V. D. Stok, "Discovery of OSCORE Groups with the CoRE Resource Directory", Work in Progress, Internet-Draft, draft-tiloca-core-oscore-discovery-10, 25 October 2021, <https://www.ietf.org/archive/id/draft-tiloca-core-oscore-discovery-10.txt>.

[RFC2093] Harney, H. and C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification", RFC 2093, DOI 10.17487/RFC2093, July 1997, <https://www.rfc-editor.org/info/rfc2093>.

[RFC2094] Harney, H. and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094, DOI 10.17487/RFC2094, July 1997, <https://www.rfc-editor.org/info/rfc2094>.

[RFC2627] Wallner, D., Harder, E., and R. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, DOI 10.17487/RFC2627, June 1999, <https://www.rfc-editor.org/info/rfc2627>.

[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>.

[RFC7641] Hartke, K., "Observing Resources in the Constrained Application Protocol (CoAP)", RFC 7641, DOI 10.17487/RFC7641, September 2015, <https://www.rfc-editor.org/info/rfc7641>.

[RFC7959] Bormann, C. and Z. Shelby, Ed., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)", RFC 7959, DOI 10.17487/RFC7959, August 2016, <https://www.rfc-editor.org/info/rfc7959>.

[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>.

[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>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

Appendix A. Requirements on Application Profiles

This section lists the requirements on application profiles of this specification, for the convenience of application profile designers.

A.1. Mandatory-to-Address Requirements

* REQ1: Specify the format and encoding of 'scope'. This includes defining the set of possible roles and their identifiers, as well as the corresponding encoding to use in the scope entries according to the used scope format (see Section 3.1).

* REQ2: If the AIF format of 'scope' is used, register its specific instance of "Toid" and "Tperm", as well as the corresponding Media Type and Content-Format, as per the guidelines in [I-D.ietf-ace-aif].

* REQ3: If used, specify the acceptable values for 'sign_alg' (see Section 3.3).

* REQ4: If used, specify the acceptable values for 'sign_parameters' (see Section 3.3).

* REQ5: If used, specify the acceptable values for 'sign_key_parameters' (see Section 3.3).

* REQ6: Specify the acceptable formats for encoding public keys and, if used, the acceptable values for 'pub_key_enc' (see Section 3.3).

* REQ7: If the value of the GROUPNAME URI path and the group name in the access token scope (gname in Section 3.2) are not required to coincide, specify the mechanism to map the GROUPNAME value in the URI to the group name (see Section 4.1).

* REQ8: Define whether the KDC has a public key and if this has to be provided through the 'kdc_cred' parameter, see Section 4.3.1.

* REQ9: Specify if any part of the KDC interface as defined in this document is not supported by the KDC (see Section 4.1).

* REQ10: Register a Resource Type for the root url-path, which is used to discover the correct url to access at the KDC (see Section 4.1).

* REQ11: Define what specific actions (e.g., CoAP methods) are allowed on each resource provided by the KDC interface, depending on whether the Client is a current group member; the roles that a Client is authorized to take as per the obtained access token (see Section 3.1); and the roles that the Client has as current group member.

* REQ12: Categorize possible newly defined operations for Clients into primary operations expected to be minimally supported and secondary operations, and provide accompanying considerations (see Section 4.1.1).

* REQ13: Specify the encoding of group identifier (see Section 4.2.1).

* REQ14: Specify the approaches used to compute and verify the PoP evidence to include in 'client_cred_verify', and which of those approaches is used in which case (see Section 4.3.1).

* REQ15: Specify how the nonce N_S is generated, if the token is not provided to the KDC through the Token Transfer Request to the authz-info endpoint (e.g., if it is used directly to validate TLS instead).

* REQ16 Define the initial value of the 'num' parameter (see Section 4.3.1).

* REQ17: Specify the format of the 'key' parameter (see Section 4.3.1).

* REQ18: Specify the acceptable values of the 'gkty' parameter (see Section 4.3.1).

* REQ19: Specify and register the application profile identifier (see Section 4.3.1).

* REQ20: If used, specify the format and content of 'group_policies' and its entries. Specify the policies default values (see Section 4.3.1).

* REQ21: Specify the approaches used to compute and verify the PoP evidence to include in 'kdc_cred_verify', and which of those approaches is used in which case (see Section 4.3.1).

* REQ22: Specify the communication protocol the members of the group must use (e.g., multicast CoAP).

* REQ23: Specify the security protocol the group members must use to protect their communication (e.g., group OSCORE). This must provide encryption, integrity and replay protection.

* REQ24: Specify how the communication is secured between Client and KDC. Optionally, specify transport profile of ACE [I-D.ietf-ace-oauth-authz] to use between Client and KDC (see Section 4.3.1.1.

* REQ25: Specify the format of the identifiers of group members (see Section 4.3.1).

* REQ26: Specify policies at the KDC to handle ids that are not included in 'get_pub_keys' (see Section 4.4.1).

* REQ27: Specify the format of newly-generated individual keying material for group members, or of the information to derive it, and corresponding CBOR label (see Section 4.8.1).

* REQ28: Specify and register the identifier of newly defined semantics for binary scopes (see Section 7).

* REQ29: Categorize newly defined parameters according to the same criteria of Section 8.

* REQ30: Define whether Clients must, should or may support the conditional parameters defined in Section 8, and under which circumstances.

A.2. Optional-to-Address Requirements

* OPT1: Optionally, if the textual format of 'scope' is used, specify CBOR values to use for abbreviating the role identifiers in the group (see Section 3.1).

* OPT2: Optionally, specify the additional parameters used in the exchange of Token Transfer Request and Response (see Section 3.3).

* OPT3: Optionally, specify the negotiation of parameter values for signature algorithm and signature keys, if 'sign_info' is not used (see Section 3.3).

* OPT4: Optionally, specify possible or required payload formats for specific error cases.

* OPT5: Optionally, specify additional identifiers of error types, as values of the 'error' field in an error response from the KDC.

* OPT6: Optionally, specify the encoding of 'pub_keys_repos' if the default is not used (see Section 4.3.1).

* OPT7: Optionally, specify the functionalities implemented at the 'control_uri' resource hosted at the Client, including message exchange encoding and other details (see Section 4.3.1).

* OPT8: Optionally, specify the behavior of the handler in case of failure to retrieve a public key for the specific node (see Section 4.3.1).

* OPT9: Optionally, define a default group rekeying scheme, to refer to in case the 'rekeying_scheme' parameter is not included in the Joining Response (see Section 4.3.1).

* OPT10: Optionally, specify the functionalities implemented at the 'control_group_uri' resource hosted at the Client, including message exchange encoding and other details (see Section 4.3.1).

* OPT11: Optionally, specify policies that instruct Clients to retain messages and for how long, if they are unsuccessfully decrypted (see Section 4.8.1.1). This makes it possible to decrypt such messages after getting updated keying material.

* OPT12: Optionally, specify for the KDC to perform group rekeying (together or instead of renewing individual keying material) when receiving a Key Renewal Request (see Section 4.8.2.1).

* OPT13: Optionally, specify how the identifier of a group members's public key is included in requests sent to other group members (see Section 4.9.1.1).

* OPT14: Optionally, specify additional information to include in rekeying messages for the "Point-to-Point" group rekeying scheme (see Section 6).

* OPT15: Optionally, specify if Clients must or should support any of the parameters defined as optional in this specification (see Section 8).

Appendix B. Extensibility for Future COSE Algorithms

As defined in Section 8.1 of [I-D.ietf-cose-rfc8152bis-algs], future algorithms can be registered in the "COSE Algorithms" registry [COSE.Algorithms] as specifying none or multiple COSE capabilities.

To enable the seamless use of such future registered algorithms, this section defines a general, agile format for each 'sign_info_entry' of the 'sign_info' parameter in the Token Transfer Response, see Section 3.3.1.

If any of the currently registered COSE algorithms is considered, using this general format yields the same structure of 'sign_info_entry' defined in this document, thus ensuring retro-compatibility.

B.1. Format of 'sign_info_entry'

The format of each 'sign_info_entry' (see Section 3.3.1) is generalized as follows. Given N the number of elements of the 'sign_parameters' array, i.e., the number of COSE capabilities of the signature algorithm, then:

* 'sign_key_parameters' is replaced by N elements 'sign_capab_i', each of which is a CBOR array.

* The i-th array following 'sign_parameters', i.e., 'sign_capab_i' (i = 0, ..., N-1), is the array of COSE capabilities for the algorithm capability specified in 'sign_parameters'[i].

```
sign_info_entry =
[
  id : gname / [ + gname ],
  sign_alg : int / tstr,
  sign_parameters : [ alg_capab_1 : any,
                      alg_capab_2 : any,
                      ...,
                      alg_capab_N : any],
  sign_capab_1 : [ any ],
  sign_capab_2 : [ any ],
  ...,
  sign_capab_N : [ any ],
  pub_key_enc = int / nil
]

gname = tstr
```

Figure 37: 'sign_info_entry' with general format

Appendix C. Document Updates

RFC EDITOR: PLEASE REMOVE THIS SECTION.

C.1. Version -14 to -15

* Fixed nits.

C.2. Version -13 to -14

* Clarified scope and goal of the document in abstract and introduction.

* Overall clarifications on semantics of operations and parameters.

* Major restructuring in the presentation of the KDC interface.

* Revised error handling, also removing redundant text.

* Imported parameters and KDC resource about the KDC's public key from draft-ietf-ace-key-groupcomm-oscore.

* New parameters 'group_rekeying_scheme' and 'control_group_uri'.

* Provided example of administrative keying material transported in 'mgt_key_material'.

* Reasoned categorization of parameters, as expected support by ACE Clients.

* Reasoned categorization of KDC functionalities, as minimally/ optional to support for ACE Clients.

* Guidelines on enhanced error responses using 'error' and 'error_description'.

* New section on group rekeying, discussing at a high-level a basic one-to-one approach and possible one-to-many approaches.

* Revised and expanded security considerations, also about the KDC.

* Updated list of requirements for application profiles.

* Several further clarifications and editorial improvements.

C.3. Version -05 to -13

* Incremental revision of the KDC interface.

* Removed redundancy in parameters about signature algorithm and signature keys.

* Node identifiers always indicated with 'peer_identifiers'.

* Format of public keys changed from raw COSE Keys to be certificates, CWTs or CWT Claims Set (CCS). Adapted parameter 'pub_key_enc'.

* Parameters and functionalities imported from draft-ietf-key-groupcomm-oscore where early defined.

* Possible provisioning of the KDC's Diffie-Hellman public key in response to the Token transferring to /authz-info.

* Generalized proof-of-possession evidence, to be not necessarily a signature.

* Public keys of group members may be retrieved filtering by role and/or node identifier.

* Enhanced error handling with error code and error description.

* Extended "typed" format for the 'scope' claim, optional to use.

* Editorial improvements.

C.4. Version -04 to -05

* Updated uppercase/lowercase URI segments for KDC resources.

* Supporting single Access Token for multiple groups/topics.

* Added 'control_uri' parameter in the Joining Request.

* Added 'peer_roles' parameter to support legal requesters/ responders.

* Clarification on stopping using owned keying material.

* Clarification on different reasons for processing failures, related policies, and requirement OPT11.

* Added a KDC sub-resource for group members to upload a new public key.

* Possible group rekeying following an individual Key Renewal Request.

* Clarified meaning of requirement REQ3; added requirement OPT12.

* Editorial improvements.

C.5. Version -03 to -04

* Revised RESTful interface, as to methods and parameters.

* Extended processing of joining request, as to check/retrieval of public keys.

* Revised and extended profile requirements.

* Clarified specific usage of parameters related to signature algorithms/keys.

* Included general content previously in draft-ietf-ace-key-groupcomm-oscore

* Registration of media type and content format application/ace-group+cbor

* Editorial improvements.

C.6. Version -02 to -03

* Exchange of information on the signature algorithm and related parameters, during the Token POST (Section 3.3).

* Restructured KDC interface, with new possible operations (Section 4).

* Client PoP signature for the Joining Request upon joining (Section 4.1.2.1).

* Revised text on group member removal (Section 5).

* Added more profile requirements (Appendix A).

C.7. Version -01 to -02

* Editorial fixes.

* Distinction between transport profile and application profile (Section 1.1).

* New parameters 'sign_info' and 'pub_key_enc' to negotiate parameter values for signature algorithm and signature keys (Section 3.3).

* New parameter 'type' to distinguish different Key Distribution Request messages (Section 4.1).

* New parameter 'client_cred_verify' in the Key Distribution Request to convey a Client signature (Section 4.1).

* Encoding of 'pub_keys_repos' (Section 4.1).

* Encoding of 'mgt_key_material' (Section 4.1).

* Improved description on retrieval of new or updated keying material (Section 6).

* Encoding of 'get_pub_keys' in Public Key Request (Section 7.1).

* Extended security considerations (Sections 10.1 and 10.2).

* New "ACE Public Key Encoding" IANA registry (Section 11.2).

* New "ACE Groupcomm Parameters" IANA registry (Section 11.3), populated with the entries in Section 8.

* New "Ace Groupcomm Request Type" IANA registry (Section 11.4), populated with the values in Section 9.

* New "ACE Groupcomm Policy" IANA registry (Section 11.7) populated with two entries "Sequence Number Synchronization Method" and "Key Update Check Interval" (Section 4.2).

* Improved list of requirements for application profiles (Appendix A).

C.8. Version -00 to -01

* Changed name of 'req_aud' to 'audience' in the Authorization Request (Section 3.1).

* Defined error handling on the KDC (Sections 4.2 and 6.2).

* Updated format of the Key Distribution Response as a whole (Section 4.2).

* Generalized format of 'pub_keys' in the Key Distribution Response (Section 4.2).

* Defined format for the message to request leaving the group (Section 5.2).

* Renewal of individual keying material and methods for group rekeying initiated by the KDC (Section 6).

* CBOR type for node identifiers in 'get_pub_keys' (Section 7.1).

* Added section on parameter identifiers and their CBOR keys (Section 8).

* Added request types for requests to a Join Response (Section 9).

* Extended security considerations (Section 10).

* New IANA registries "ACE Groupcomm Key registry", "ACE Groupcomm Profile registry", "ACE Groupcomm Policy registry" and "Sequence Number Synchronization Method registry" (Section 11).

* Added appendix about requirements for application profiles of ACE on group communication (Appendix A).

Acknowledgments

The following individuals were helpful in shaping this document: Christian Amsuess, Carsten Bormann, Rikard Hoeglund, Ben Kaduk, Watson Ladd, John Mattsson, Daniel Migault, Jim Schaad, Ludwig Seitz, Goeran Selander, Cigdem Sengul and Peter van der Stok.

The work on this document has been partly supported by VINNOVA and the Celtic-Next project CRITISEC; by the H2020 project SIFIS-Home (Grant agreement 952652); and by the EIT-Digital High Impact Initiative ACTIVE.

Authors' Addresses

Francesca Palombini
Ericsson AB
Torshamnsgatan 23
SE-16440 Stockholm Kista
Sweden

Email: francesca.palombini@ericsson.com

Marco Tiloca
RISE AB
Isafjordsgatan 22
SE-16440 Stockholm Kista
Sweden

Email: marco.tiloca@ri.se