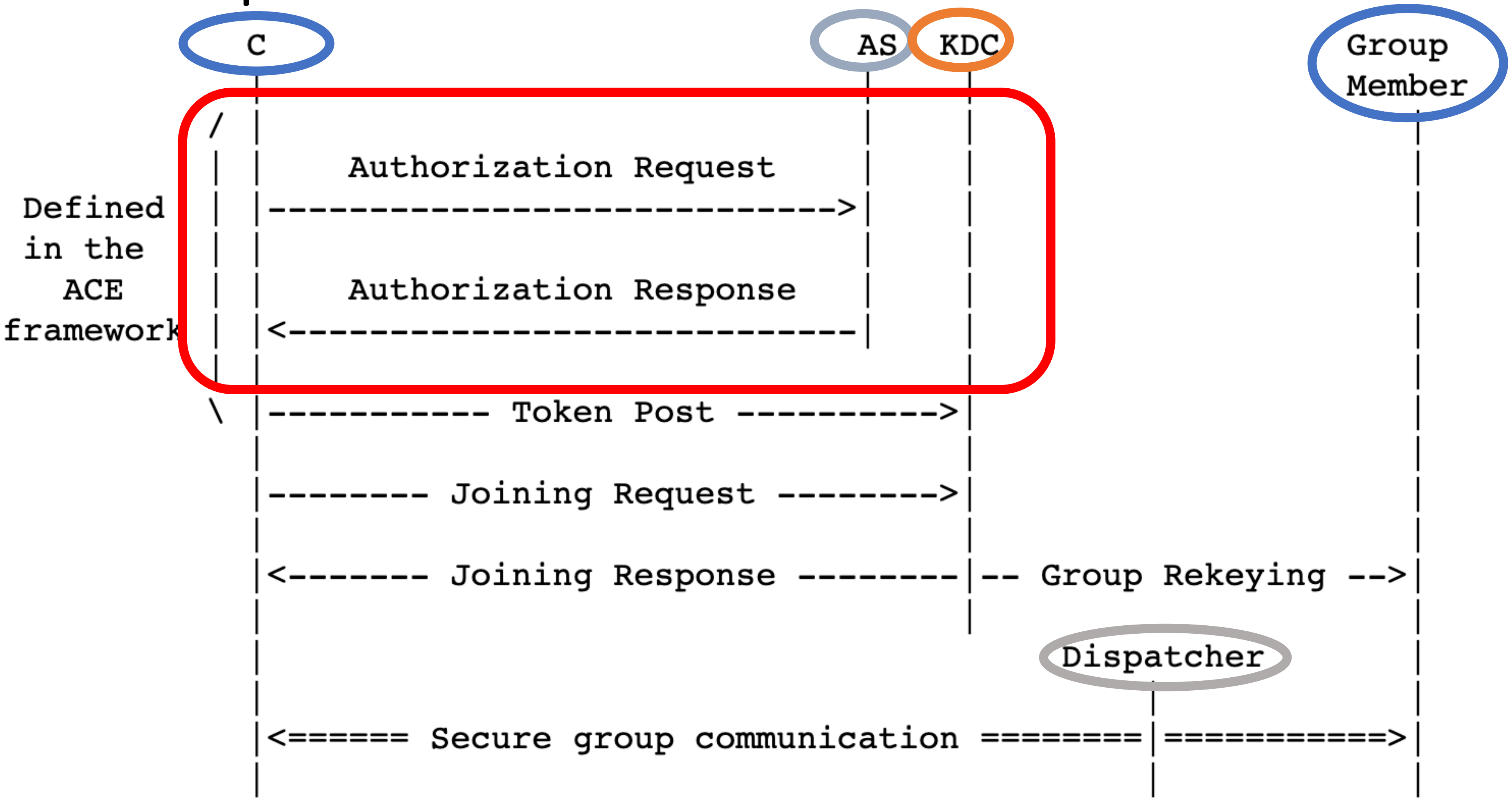
Key Provisioning for Group Communication using ACE

draft-ietf-ace-key-groupcomm-08

Francesca Palombini, Ericsson
Marco Tiloca, RISE

ACE WG, IETF 108, July 29, 2020

Quick Recap



```
                 C                           AS  KDC              Group
                 |                            |   |               Member
               / |                            |   |                 |
               | |   Authorization Request    |   |                 |
    Defined    | |--------------------------->|   |                 |
    in the     | |                            |   |                 |
      ACE      | |   Authorization Response   |   |                 |
    framework  | |<---------------------------|   |                 |
               | |                                |                 |
               \ |---------- Token Post --------->|                 |
                 |                                |                 |
                 |------- Joining Request ------->|                 |
                 |                                |                 |
                 |<------ Joining Response -------|-- Group Rekeying -->|
                 |                                |                 |
                 |                            Dispatcher            |
                 |                                |                 |
                 |<===== Secure group communication =======|==========>|
                 |                                |                 |
```

Figure 2: Message Flow Upon New Node's Joining

What happened since last interim (22/06/2020)

- Version -08 was submitted:
  - Based on review from Jim: https://mailarchive.ietf.org/arch/msg/ace/VGbRA3XPLJE5n3TrQElhjFtq3q0/
  - Mostly editorial changes and clarifications
  - Details at: https://github.com/ace-wg/ace-key-groupcomm/pull/97

- 24 issues created as a result of Jim’s follow up review –> v-09 planned

- Of these, 4 are discussed today

Remove default URIs + application profiles can define their own

- Right now we leave to application profiles to define their URIs:
  - e.g. “/oscore-group” or “/pubsub”

- We propose to remove that, all application profiles can use the same, ex “ace-group”
  - The KDC needs to save for each group itself the information about what application profile it’s using (ex: “group1” uses encodings from “coap_group_oscore_app” profile)

- 2 options:
  1. Register the URI “ace-group” as a well-known URI
  2. Register one resource type for “/ace-group” and describe resource directory use to find this URI (same as Ace framework for /authz-info)
     - Needs to define a new target attribute for each application profile to do filtering?
     - We already register the interface… can we use that?
  3. Register a different resource type for each application profile

Clarify ”group name” ≠ “GROUPNAME” ≠ “group identifier”

- Group name is the “invariant once established” identifier of the group
  - Used in the scope to identify the group between AS, Client, KDC
  - Right now it can be encoded as anything, we propose to change to tstr for simplicity

- GROUPNAME is the value used in the URI (tstr)
  - Group name maps to GROUPNAME

- Group identifier is the identifier of the group keying material
  - Changes with rekeys

  (not in v-08 but asked to be included in v-09)

Add a PUT handler at the root of the interface at the KDC

- Sends a list of group identifiers and get back the the corresponding group names and URIs at the KDC for those identifiers

- Useful when there is a rekey, the node gets a group identifier it does not recognize, and wants to know where to do the rekey:

  For example needs to know "/ace-group/g1" where g1 is the GROUPNAME for "group1"

- Example:

  PUT { gid: [h'12', h'34'] } returns

  2.05 { gid: [h'12', h'34'], gname: ["group1", "group2"], guri: ["/ace-group/g1", "/ace-group/g1"]

  - Both have content-format "ace-groupcomm+cbor"
  - The new parameters **gname** and **guri** need to be registered.

Individual keying material

- From the review, it’s not clear how PUT /ace-group/GROUPNAME/nodes/NODENAME is used

- Nodes can use it to renew individual keying material (= input to derive keying material to protect outgoing messages to the group, different for each member of the group, e.g. sender Id in OSCORE groups)

- Some application profiles may not implement individual keying material
- Proposal: Profiles <u>MAY</u>(*) additionally use this handler to rekey the whole group

- Up to the application profiles to specify if they support renew of individual keying material and/or rekey of the whole group via this handler

(*) Note: we probably don’t want MUST here….

Plan forward

- Submit v-09

- WGLC?