

Key Provisioning for Group Communication using ACE

[draft-ietf-ace-key-groupcomm-01](#)

Francesca Palombini, Ericsson

Marco Tiloca, RISE

draft-ietf-ace-key-groupcomm-01

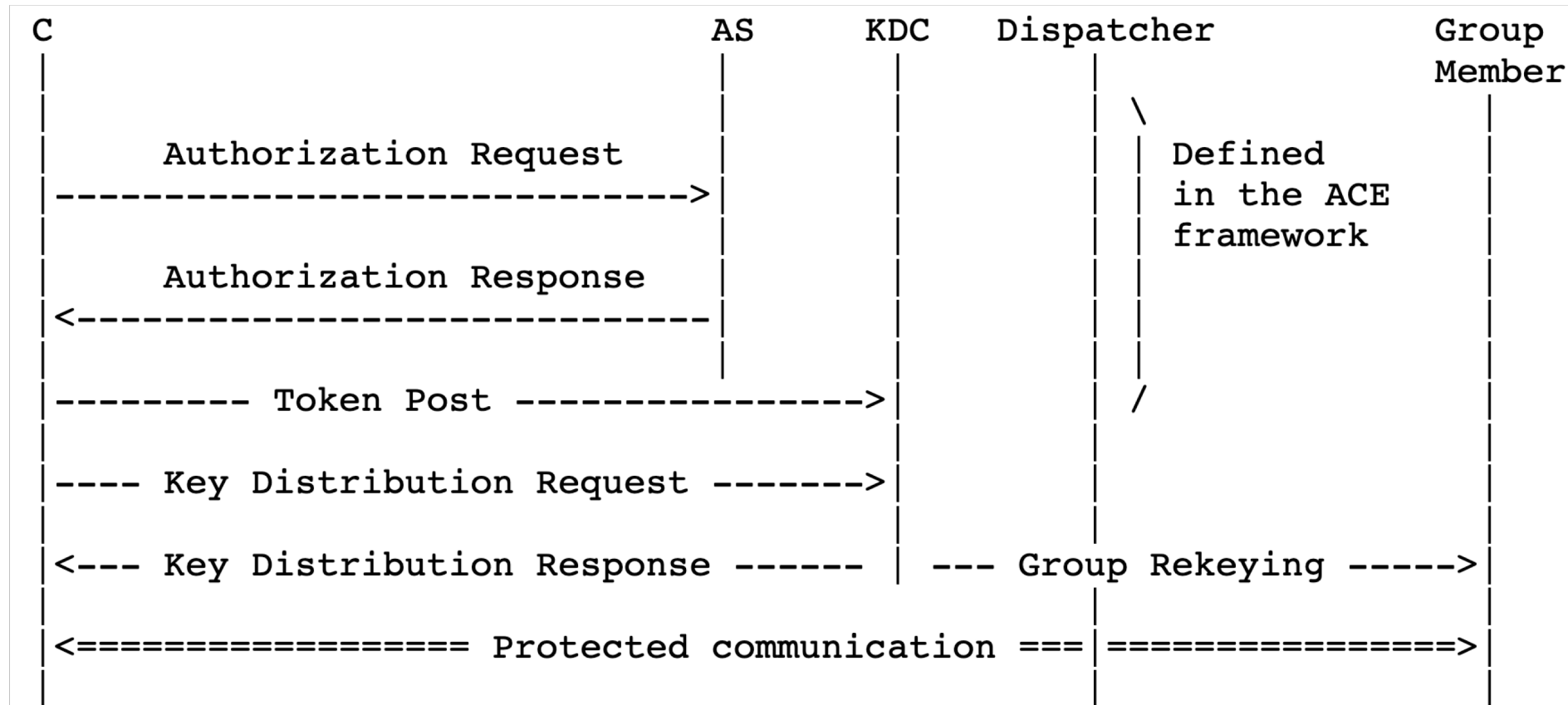


Figure 2: Message Flow Upon New Node's Joining

IANA

- Key Distribution Response contains a general “key” field, its type is defined by the new “kty” field, to be registered in a new “Ace Groupcomm Key” registry:

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

- Key Distribution Response contains a new “profile”, to be registered in a new “Ace Groupcomm Profile” registry (NOT the same profile as Ace!)
- Key Distribution Response contains a new “exp” field (expiration of the keying material)

Errors Definition

- KDC error on Requests:
 - If verification fails, the KDC MUST respond with a 4.01 (Unauthorized) error message.
 - If the Request is not formatted correctly (e.g. no 'scope' field present while expected, or unknown fields present), the KDC MUST respond with 4.00 (Bad Request) error message.

Request To Leave the Group

- CoAP POST to /resource associated with group at KDC
Payload: { 'leave':[], ~~'scope':["group1"]~~, ?'client_cred': pubkey_id1}
- Leave the group altogether, not role based
- A client can re-request to join a group without contacting AS as long as token is valid

Key Redistribution Initiated by KDC (examples)

KDC can distribute keying material by:

- Using unicast requests to each Client over a secure channel
- Using Observe (members = observers)
- Using Pub/Sub (KDC = publisher, members = subscribers)
- Using Multicast (KDC = multicaster)

“different security properties and require different security associations.”