

CoAP Publish-Subscribe Profile for Authentication and Authorization for Constrained Environments (ACE)

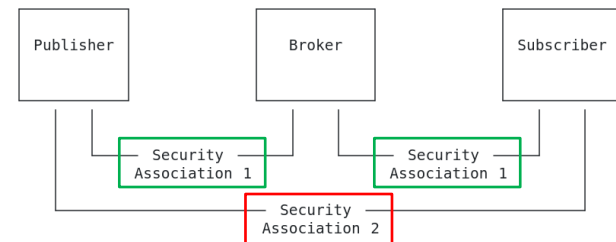
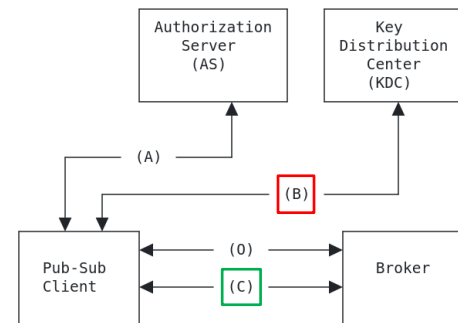
draft-ietf-ace-coap-pubsub-profile-03

Francesca Palombini, Ericsson
Cigdem Sengul, Brunel University
Marco Tiloca, RISE

IETF 125 meeting – Shenzhen – March 17th, 2026

Recap

- › **Application profile of RFC 9594 [1]**
 - Key provisioning for group communication with ACE
- › **Group communication in the CoAP pub-sub architecture [2]**
- › **Mapping with ACE entities and workflows**
 - ACE client: Publisher and/or subscriber node
 - ACE resource server: Broker
 - ACE resource server: Key Distribution Center (KDC)
- › **An access token for ...**
 - Secure and authorized operations at the Broker
- › **Another access token for ...**
 - Secure and authorized operations at the KDC
 - Obtain keying material to protect published data end-to-end with COSE



Latest developments

- › **Version -02 completed WG Last Call in January 2026**
 - Positive feedback, with editorial comments – Thanks!
 - Comments from the authors (see below)

- › **Considered comments received during the IETF Last Call of [3]**
 - Likely to be received later on also for this document

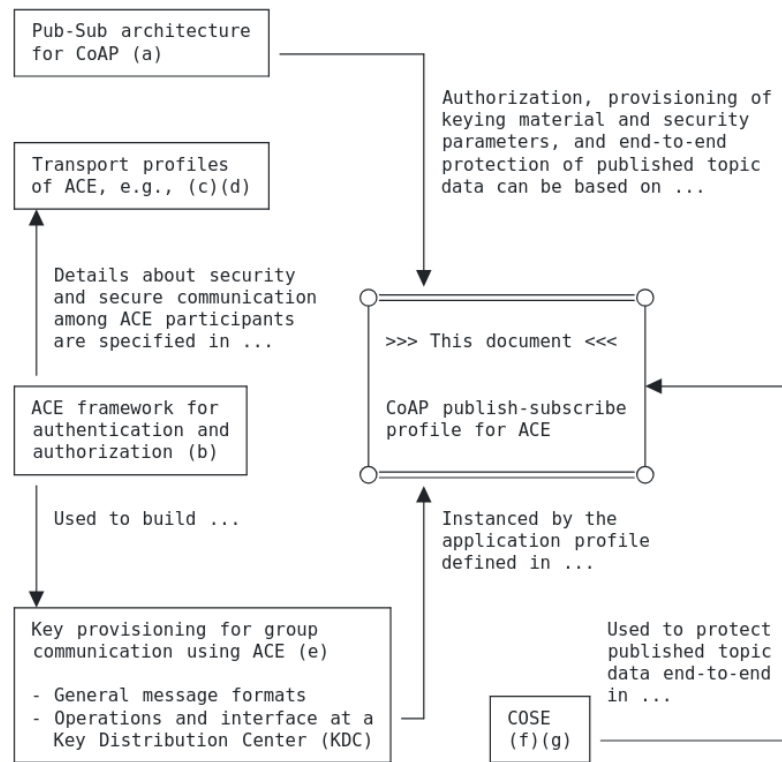
- › **Version -03 submitted in February**
 - Addressed comments to [3] that are also pertaining to this document
 - Fixed an underspecified optimization for the Join Request

From v -02 to v -03

› Editorial fixes and improvements

› Section 1 – Introduction

- Clarified the relationship between this document and the many other documents that it builds on
- Added new text
- Added new figure



(a) : [I-D.ietf-core-coap-pubsub]

(b) : [RFC9200]

(c) : [RFC9202]

(d) : [RFC9203]

(e) : [RFC9594]

(f) : [RFC9052]

(g) : [RFC9053]

From v -02 to v -03

Clarifications

› Section 2 – Application Profile Overview

- What exactly means that communication between parties are protected

“Except for the end-to-end protection of published topic data (see Section 6.1), all communications between the involved entities (Clients, Broker, KDC, Authorization Server) MUST occur and be secured in accordance with the protocol-specific transport profile of ACE used.”

› Multiple sections

- Explicit rationale for computing a proof-of-possession (PoP) evidence
- E.g., Section 4.1.1.2: *The 'client_cred_verify' parameter contains the proof-of-possession (PoP) evidence and is computed by the joining node to prove the possession of its own private key.*

From v -02 to v -03

› Section 8 – Security Considerations

- Clarified reasons for and flexibility of group rekeying

Aligned with Section 5, the KDC performs a group rekeying when one or more members leave the group, According to the specific application requirements, the KDC can also rekey the group upon a new node's joining, The KDC can also rekey the group for further reasons, e.g., according to an application-specific rekeying period or scheduling.

› Section 4.1.1.1 – Fixed underspecified optimization of Join Request

- In a Join Request to the KDC, the client MAY omit its authentication credential ...
- ... if it already provided it to the KDC (e.g., during a previous join)
- Fixed text to comply with RFC 9594 – We cannot just omit the ‘client_cred’ parameter
 - › ‘client_cred’ conveys an empty authentication credential, as an empty CBOR byte string
- Fixed corresponding text in other sections: “absence” → “empty CBOR byte string”

From v -02 to v -03

› Section 7 – Operational Considerations

- Increasingly expected, see <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-rfc5706bis>

› Logging at the KDC

- Events that resulted in an error response
- Events that resulted in a successful operation (e.g., a group joining)
- Execution of a group rekeying
- Change of group membership
- Creation/reconfiguration/termination of a group
- Never log secrets or confidential information
- Logs can be made available to third parties, after removing privacy-sensitive information

› Administration of security groups and application groups is out of scope

Next steps

- › **Good to have a new version -04 – Content already in the GitHub Editor’s Copy**
 1. **Address a point raised by Deb Cooley in her DISCUSS during the IESG evaluation of [3]**
 - Fix the use of the words “nonce” and “challenge”, to be correct and consistent
 2. **Minor clarifications, inspired by the IESG evaluation of [3]**
 - Early statement of compliance with REQ7; group names consistent with semantics of URI path
 3. **Explicitly state an assumption that we have always made and built on**
 - Topic-data resources where to publish/subscribe are hosted precisely at the Broker
 - Alternatives are admitted in the CoAP pub-sub architecture but are out of scope here
- › **One normative reference is an Internet Draft**
 - <https://datatracker.ietf.org/doc/draft-ietf-core-coap-pubsub/>
 - Completed WG Last Call → New version -19 --- To be presented at the CoRE session on Friday
- › **First request publication of the CoRE document and then of this ACE document?**

Thank you!

Comments/questions?

<https://github.com/ace-wg/pubsub-profile>