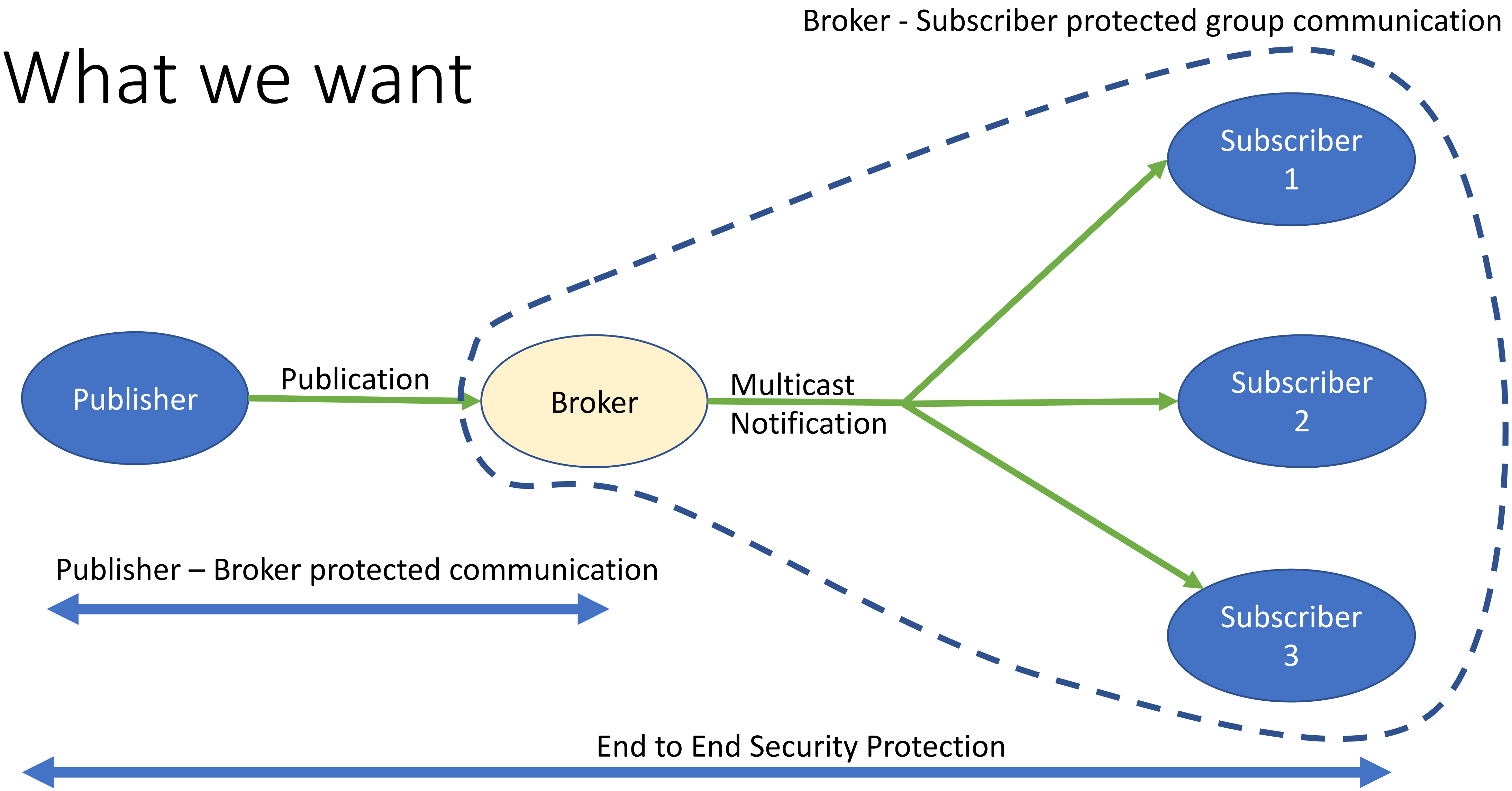
Pub Sub and Multicast

CoRE Hallway Discussion @ IETF104

Francesca Palombini

What we want


Broker - Subscriber protected group communication
Publisher
Publication
Broker
Multicast
Notification
Subscriber
1
Subscriber
2
Subscriber
3
Publisher – Broker protected communication
End to End Security Protection

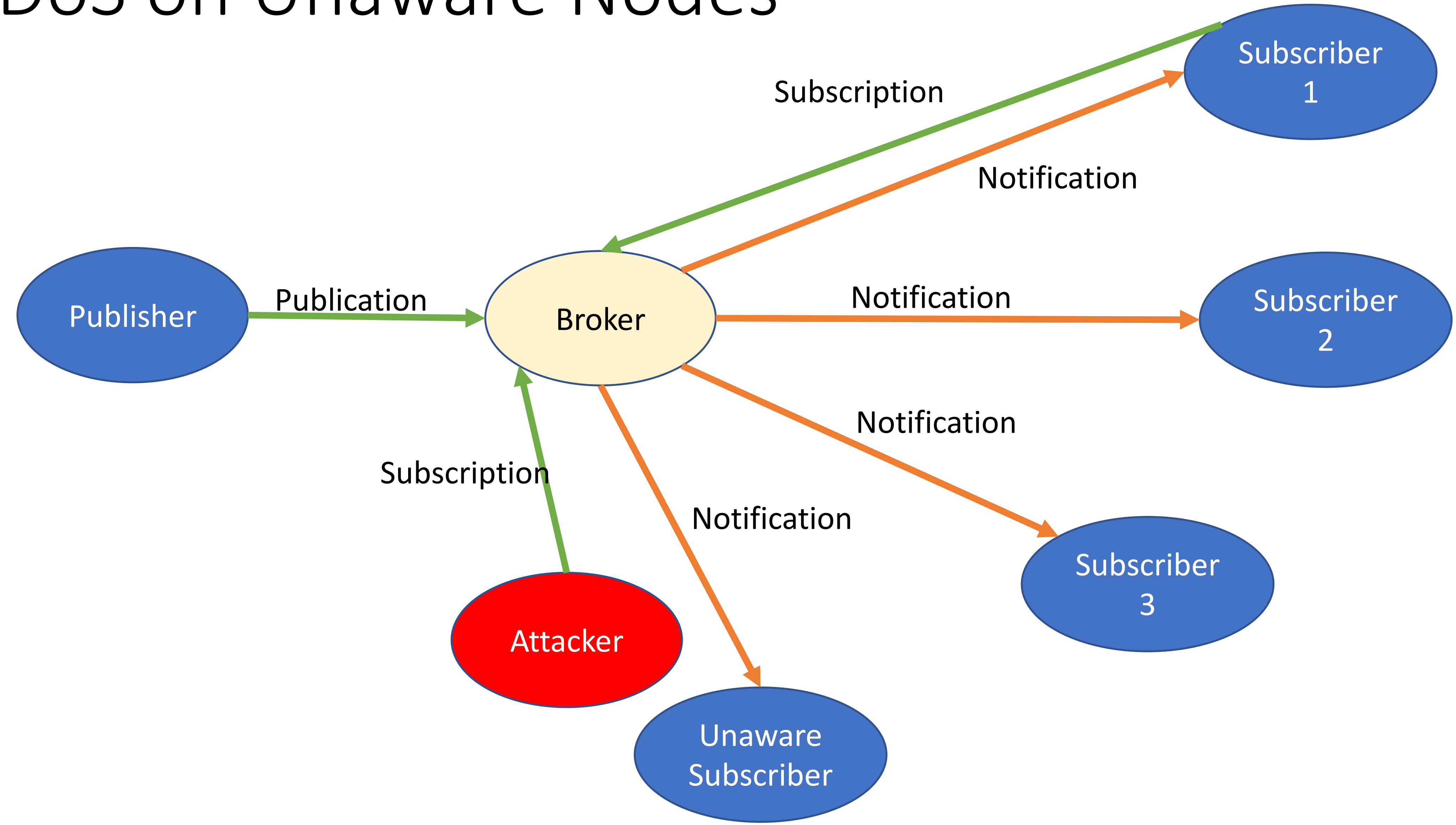
What we want – Sec Requirements

- The Publisher communicates securely with the Broker and must be authorized to publish on the Broker
- The publication is protected (protection of CoAP payload)
- The Subscribers must be authorized to decrypt and verify the publication

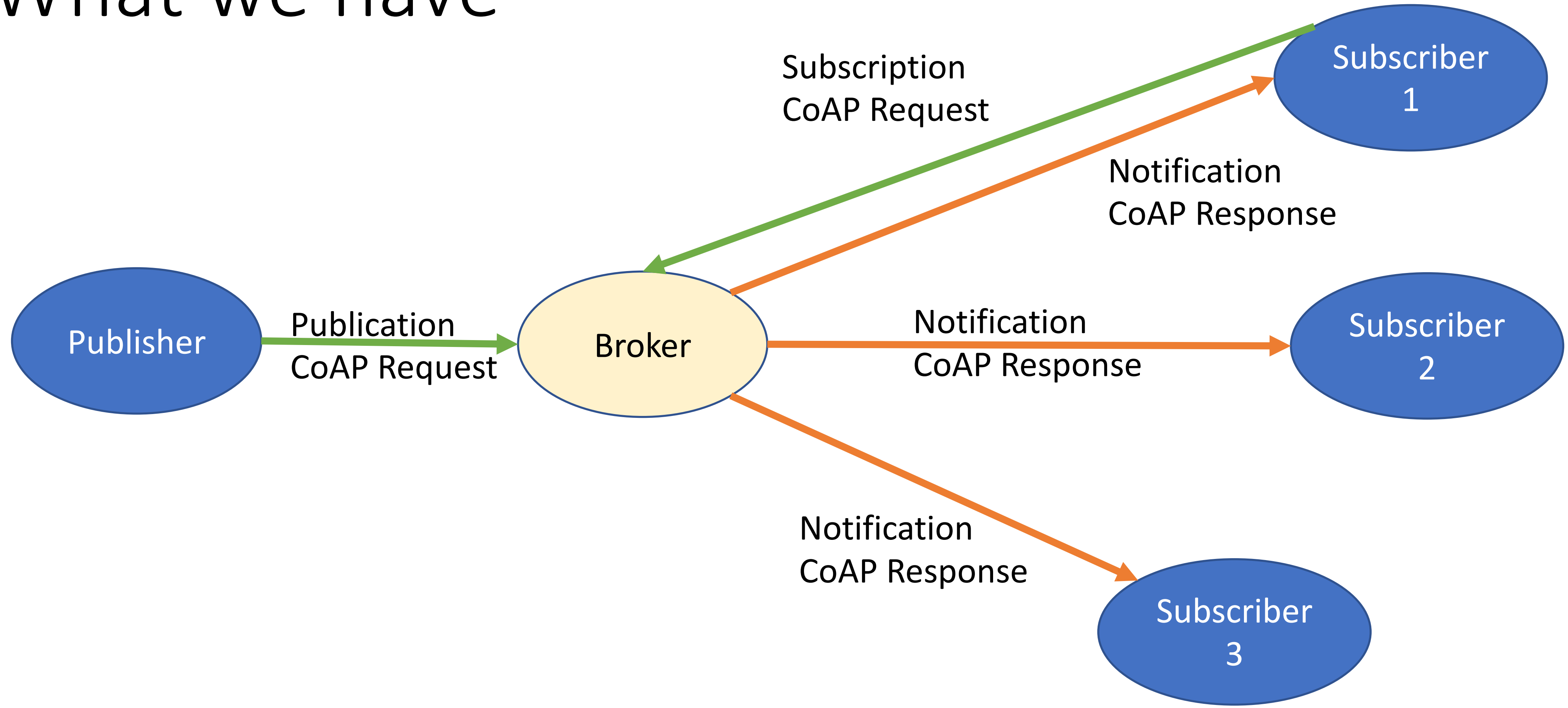
All the above + key distribution is covered by [draft-palombini-ace-coap-pubsub-profile-03]()

- Additionally, the Subscriber must prove address ownership of a subscription request, otherwise an attacker could DoS external nodes that do not want to receive the publications

DoS on Unaware Nodes

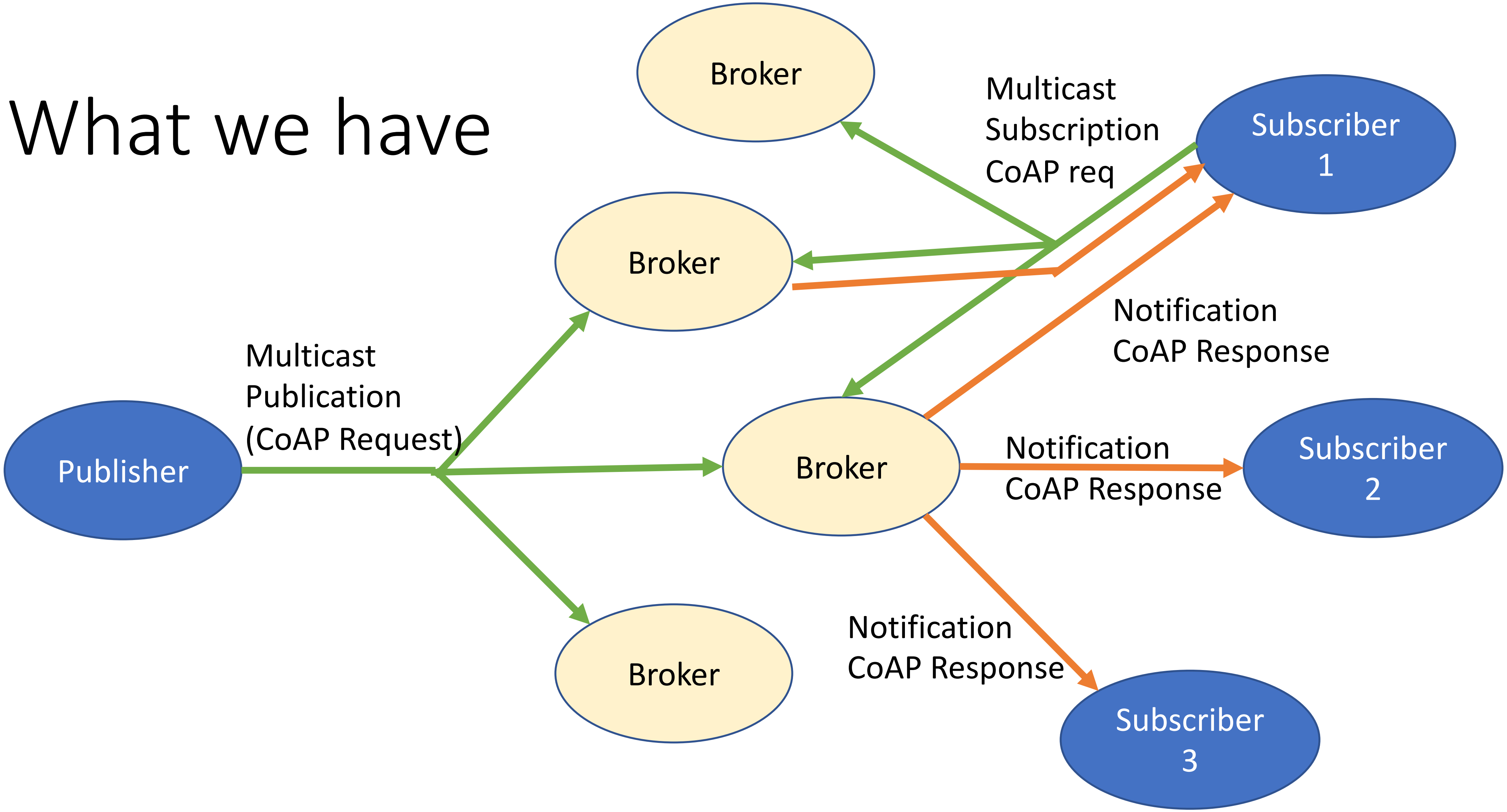


What we have



https://tools.ietf.org/html/draft-ietf-core-coap-pubsub-08

What we have



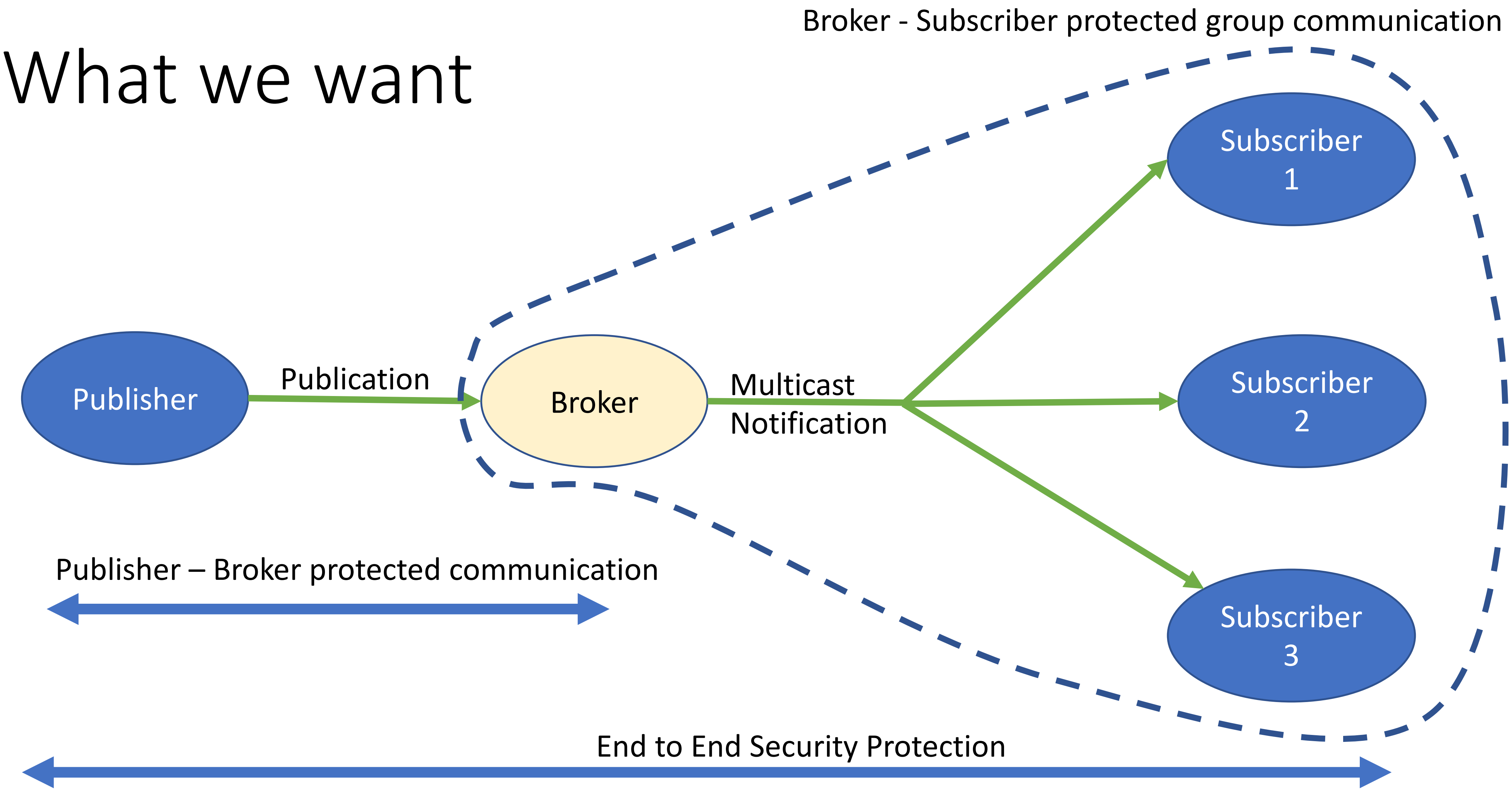
https://tools.ietf.org/html/draft-dijk-core-groupcomm-bis-00
updates multicast with Observe requests

2 Goals

- Performance Goal: Multicasting notifications

- Security Goal: DoS protection for unauthorized subscribers
    - Performance Goal: Setting up many Broker-Subscriber DTLS connection is not optimal…

What we want


Broker - Subscriber protected group communication
Publisher
Publication
Broker
Multicast
Notification
Subscriber
1
Subscriber
2
Subscriber
3
Publisher – Broker protected communication
End to End Security Protection

How do we get it

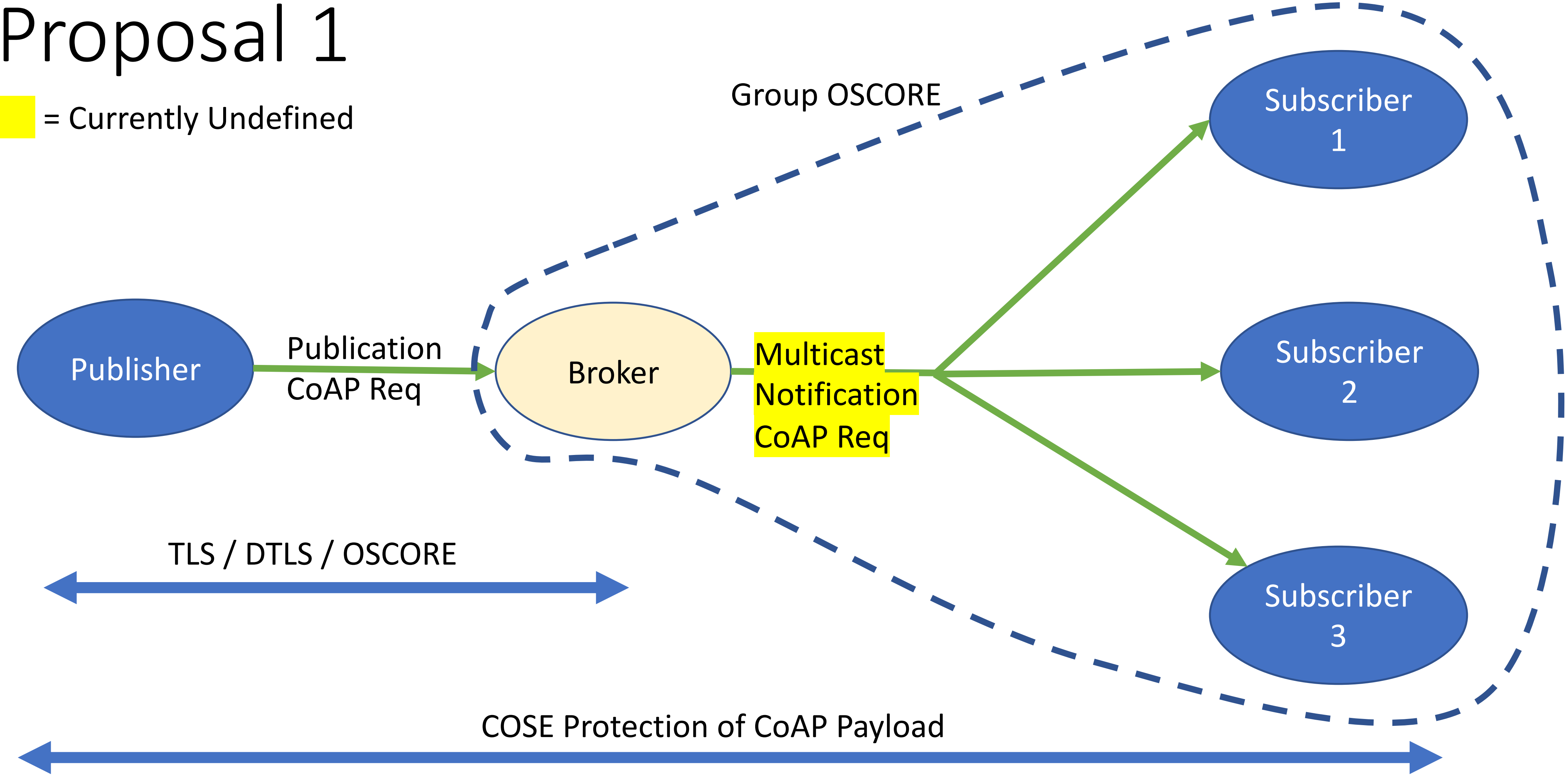
- Notifications as CoAP requests + Multicast the notification +
  1. Group OSCORE (Broker – Subscribers) + Payload protection (Pub – Subscribers)
  2. Group OSCORE (Pub – Subscribers) + additional DoS protection mechanism
  3. Payload protection (Pub – Subscribers) + additional DoS protection mechanism

4. Define multicast responses (how do we deal with the token?) + use multicast notifications to Subscribers + ?? (No secure multicast defined for multicast responses)

- Anything else?

Proposal 1

🟨 = Currently Undefined



Group OSCORE

Publisher

Publication
CoAP Req

Broker

Multicast
Notification
CoAP Req

Subscriber
1

Subscriber
2

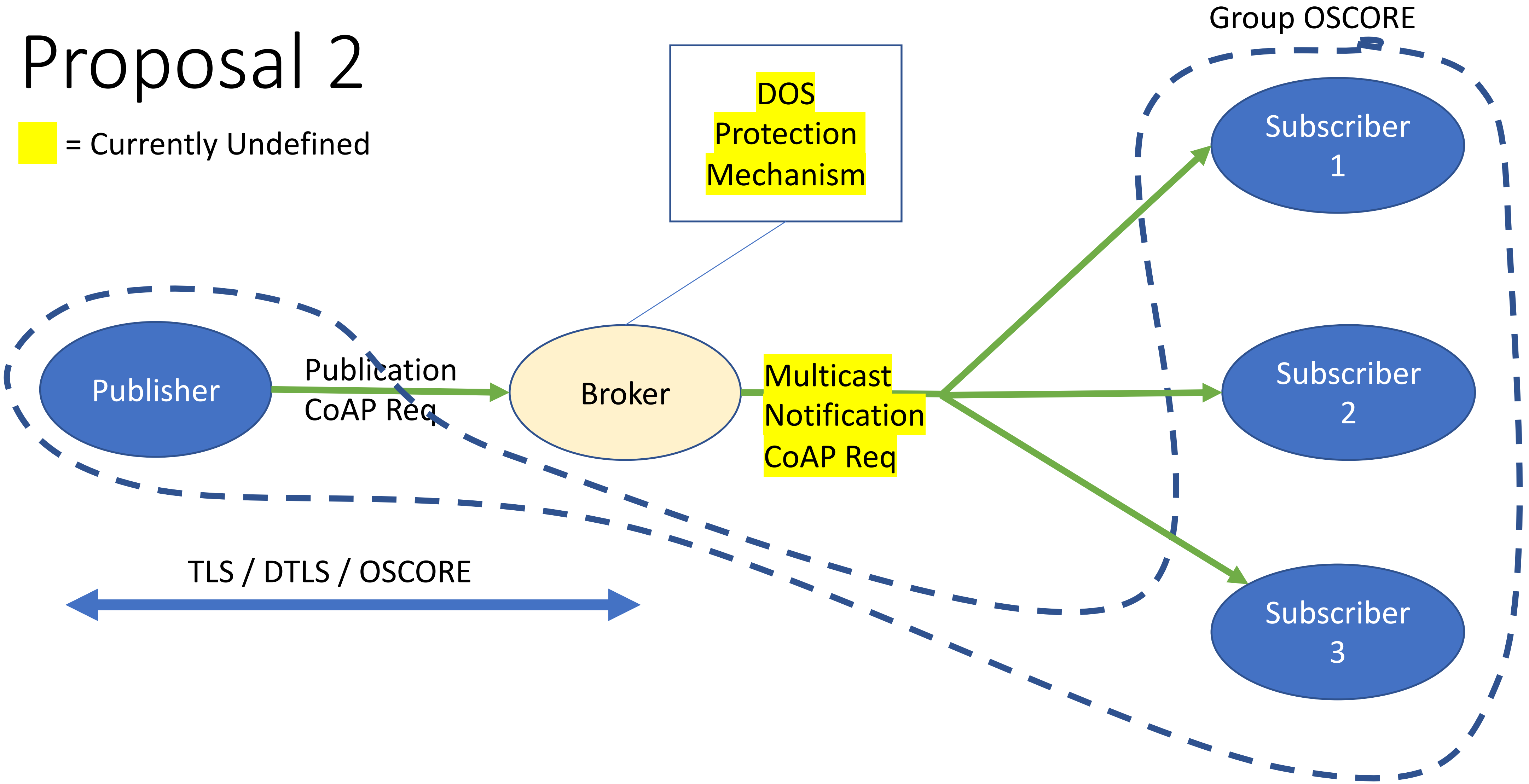
Subscriber
3

TLS / DTLS / OSCORE

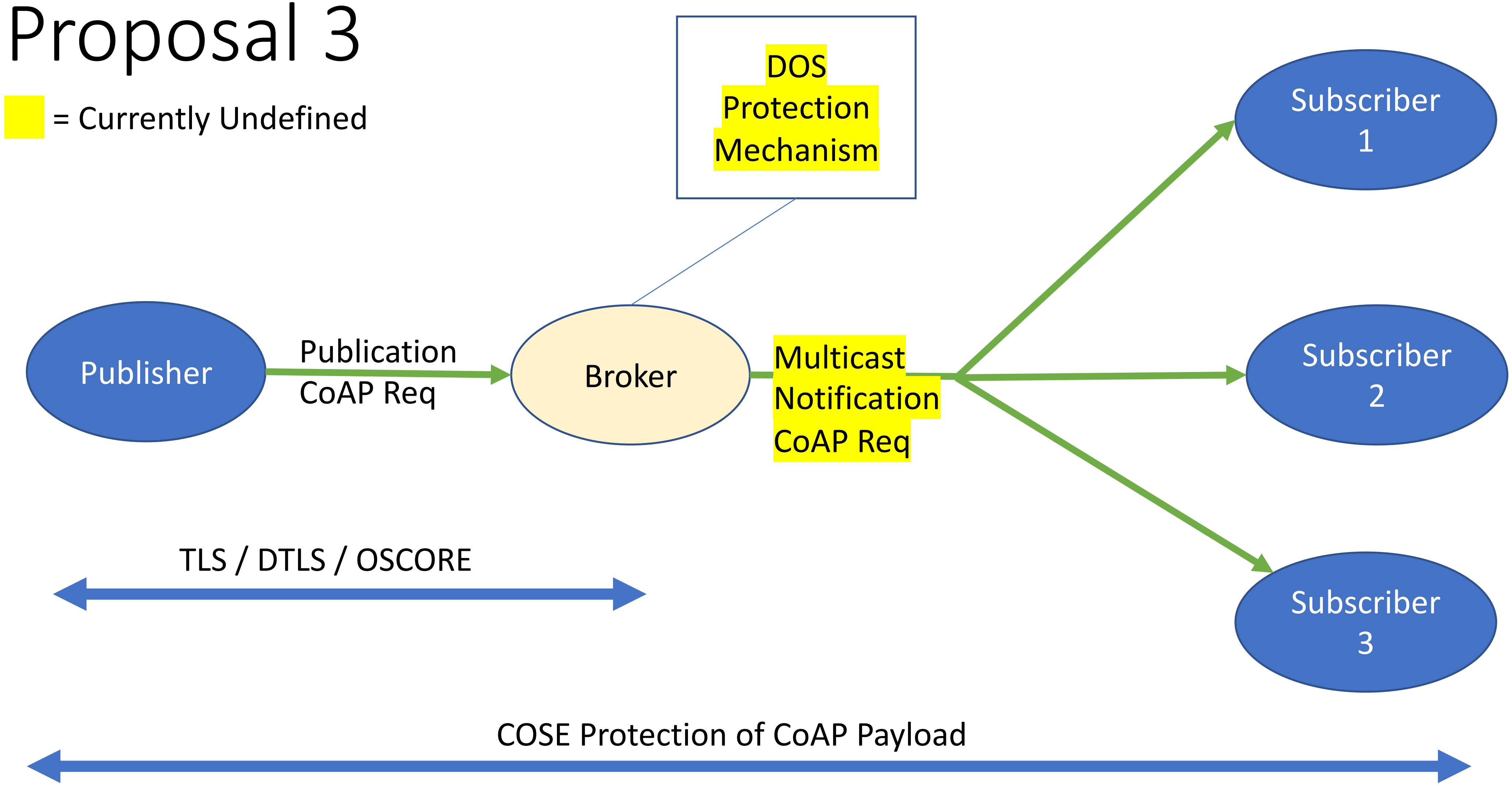
COSE Protection of CoAP Payload

Proposal 2

🟨 = Currently Undefined



Proposal 3



🟨 = Currently Undefined

DOS Protection Mechanism

Publisher

Publication CoAP Req

Broker

Multicast Notification CoAP Req

Subscriber 1

Subscriber 2

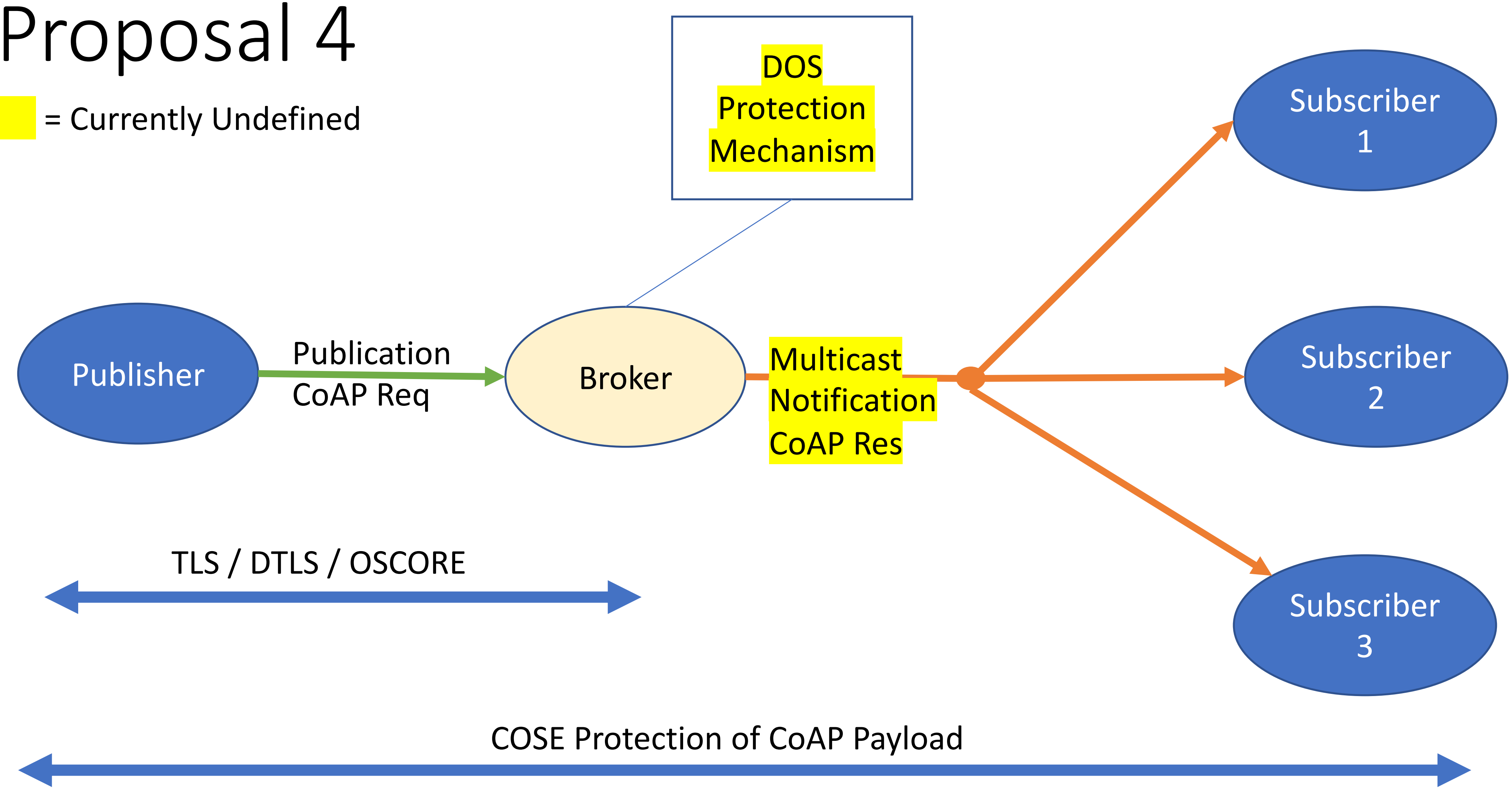
Subscriber 3

TLS / DTLS / OSCORE

COSE Protection of CoAP Payload

Proposal 4

🟨 = Currently Undefined



DOS Protection Mechanism

Publisher

Publication CoAP Req

Broker

Multicast Notification CoAP Res

Subscriber 1

Subscriber 2

Subscriber 3

TLS / DTLS / OSCORE

COSE Protection of CoAP Payload