Constrained RESTful Environments WG (core)

Chairs:

Jaime Jiménez <jaime.jimenez@ericsson.com>

Carsten Bormann <cabo@tzi.org>

Mailing List:

core@ietf.org

Jabber:

core@jabber.ietf.org

- **We assume people have read the drafts**
- **Meetings serve to advance difficult issues by making good use of face-to-face communications**
- **Note Well: Be aware of the IPR principles, according to RFC 8179 and its updates**

üBlue sheets
üScribe(s)

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Agenda Bashing

All times are in time-warped CET (UTC+01:00)

Tuesday (120 min)

- **13:50–13:59 Intro, Agenda, Status**
- **13:59–14:09 ERT (CA)**
- **14:09–14:12 Stateless (KH)**
- **14:12–14:57 Groupcomm/security (MT, FP)**
- **14:57–15:20 SenML (AK)**
- **15:20–15:34 CoRECONF**
- **15:34–15:50 Misc, Pulling items forward from Thu**

All times are in time-warped CET (UTC+01:00)

Friday (90 min)

- **09:00–09:05 Intro, Agenda**
- **09:05–09:35 Core applications (pubsub, dyn, if)**
- **09:35–10:20 Resource-Directory LC, RD & CoRAL**
- **10:20–10:30 New work: speedy-blocktrans**

Hallway discussions and side meetings

- CoRAL: Wednesday 15:00..17:00, Tyrolka
- Protocol Negotiation: _____
- Pubsub Security: @Hackathon, see report
- Observe and Pubsub: _____

OSCORE

draft-ietf-core-object-security

→ RFC editor queue

2019-03-20

Other document status

In IETF Last Call (ends 2019-04-08):

- draft-ietf-core-multipart-ct-03

WGLC completed:

- draft-ietf-core-senml-etch-03

Ready for WGLC:

- draft-ietf-core-hop-limit-03

Ready for chairs' review, WGLC:

- draft-ietf-core-dev-urn-03

All times are in time-warped CET (UTC+01:00)

Tuesday (120 min)

- 13:50–13:59 Intro, Agenda, Status
- 13:59–14:09 ERT (CA)
- 14:09–14:12 Stateless (KH)
- 14:12–14:57 Groupcomm/security (MT, FP)
- 14:57–15:20 SenML (AK)
- 15:20–15:34 CoRECONF
- 15:34–15:50 Misc, Pulling items forward from Thu

Echo and Request Tag

draft-ietf-core-echo-request-tag

Christian Amsüss, John Mattson, Göran Selander

2019-03-26

Token processing

when used with a security protocol prone to request/response mismatch, “client MUST make sure that tokens are not used in a way so that responses risk being associated with the wrong request”

and several of clarification and editorial changes

Working Group Last Call

until 2018-04-17

All times are in time-warped CET (UTC+01:00)

Tuesday (120 min)

- 13:50–13:59 Intro, Agenda, Status
- 13:59–14:09 ERT (CA)
- 14:09–14:12 Stateless (KH)
- 14:12–14:57 Groupcomm/security (MT, FP)
- 14:57–15:20 SenML (AK)
- 15:20–15:34 CoRECONF
- 15:34–15:50 Misc, Pulling items forward from Thu

All times are in time-warped CET (UTC+01:00)

Tuesday (120 min)

- 13:50–13:59 Intro, Agenda, Status
- 13:59–14:09 ERT (CA)
- 14:09–14:12 Stateless (KH)
- 14:12–14:57 Groupcomm/security (MT, FP)
- 14:57–15:20 SenML (AK)
- 15:20–15:34 CoRECONF
- 15:34–15:50 Misc, Pulling items forward from Thu

Group OSCORE - Secure Group Communication for CoAP

draft-ietf-core-oscore-groupcomm-04

Marco Tiloca, RISE
Göran Selander, Ericsson
Francesca Palombini, Ericsson
Jiye Park, Universität Duisburg-Essen

IETF 104, CoRE WG, Prague, March 26th, 2019

Selected points to discuss (1/3)

- Revision mostly based on:
  - A detailed review from Jim – Thanks!
  - More discussions with Jim, John, Rikard, Peter – Thanks!

- “Signature bit” reverted to Reserved and set to 0

- New “Counter Signature Parameters” in the Common Context
  - Structures are from a new IANA Registry. **Move it to COSE-bis?**
  - Need a policy in COSE to always specify signature parameters

Selected points to discuss (2/3)

- Should we have the **Context ID (and more) in the external_aad**?
  - Do we need to integrity-protect the Group ID (and more)?
  - Prevent forged messages to be verified also in a wrong group
  - Value of the OSCORE option in the external_aad of the signature

- Reception of malformed/invalid messages
  - RECOMMENDED to not send error messages back (was MUST)

- Newly created Recipient Contexts
  - MAY be deleted if received message is invalid (up to the application)

Selected points to discuss (3/3)

- Handle replied/repeated responses on clients
  - The same request Token is retained, as per RFC 7390
  - Assumption: at most 1 fresh response from each server
  - Per-request list with Recipient IDs of valid received responses
  - Delete the list when freeing up the Token value

Github issue #6

- Section 3.1
  - Q: Why ‘**request**_kid’ and ‘**request**_iv’ in the external_aad?
  - A: The server uses the very same values for the response
  - Q: Why not also for ‘oscore_version’, ‘algorithms’ and ‘options’?
  - A: Version and algorithms are the same for request and response
  - A: ‘options’ is for the ‘I’ options of either the request or the response

- Section 3.2
  - Q: What is in the ‘unprotected’ field of the message?
  - A: Same as in OSCORE, but the ‘kid’ parameter is always present

Github issues #7 & #8

- #7 What countersignature algorithm?
  - Signature size vs. computing speed
  - ECDSA, Ed25519 (now MTI)

- #8 Use cases with a Gateway
  - (a) Trusted GW as traffic re-writing system (not strictly related)
  - (b) Non trusted GW as verifier and relay (related and interesting)
  - Add (b) to the covered use cases (Appendix B)

Implementation

- Ongoing
  - RISE
  - Peter
  - Jim

- First early tests at IETF 104 Hackathon

Next steps

- Close open points, e.g.:
  - Update (?) external_aad
  - Update (?) IANA actions
  - Extend security and privacy considerations
- Any significant issue remained to address?
- Interop tests
  - 3+ implementations

Thank you!

Comments/questions?

https://github.com/core-wg/oscore-groupcomm

Discovery of OSCORE Groups with the CoRE Resource Directory

draft-tiloca-core-oscore-discovery-02

Marco Tiloca, RISE
Christian Amsüss
Peter van der Stok

IETF 104, CoRE WG, Prague, March 26th, 2019

Recap

- A newly deployed device:
  - May not know the OSCORE groups and their Group Manager (GM)
  - May have to wait GMs to be deployed or OSCORE groups to be created

- Use the CoRE Resource Directory (RD):
  - Discover an OSCORE group and retrieve information to join it
  - CoAP Observe supports early discovery and changes in group information
  - Consistent with the join process in *draft-ietf-ace-key-groupcomm*

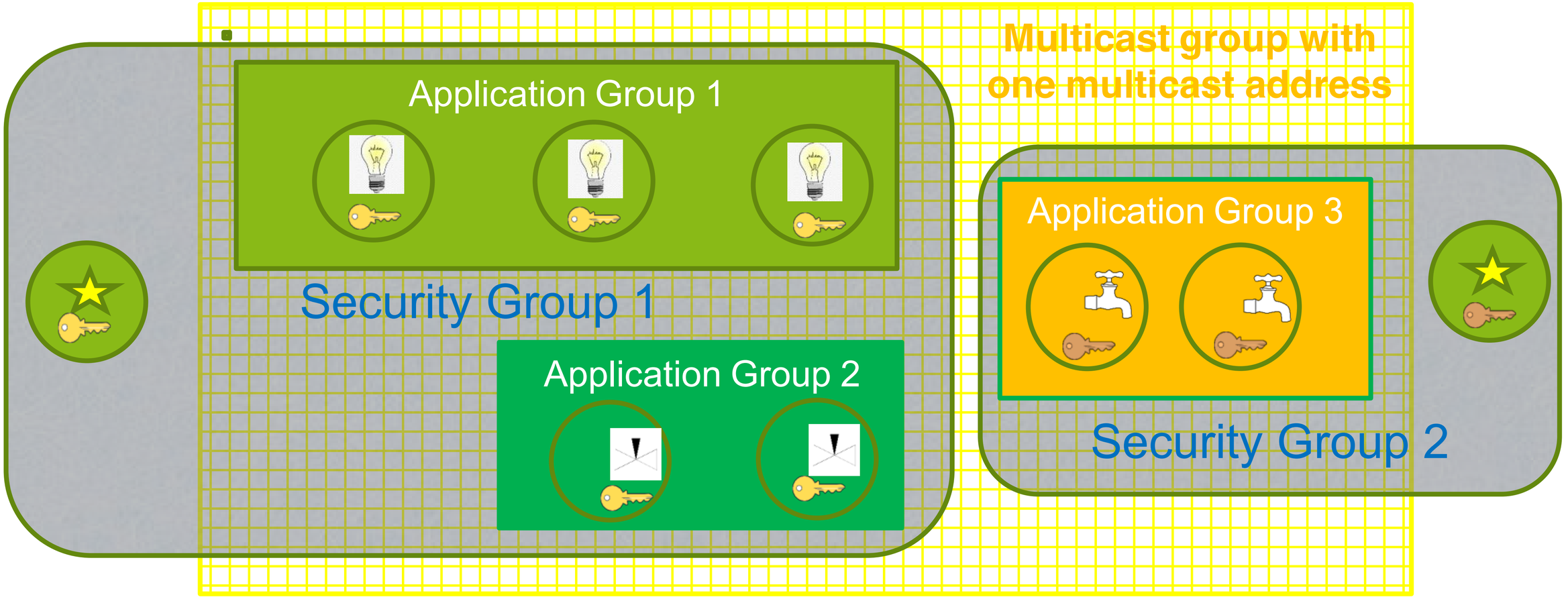
- Use resource lookup, to retrieve especially:
  - A pointer to the join resource at the GM
  - The identifier of the OSCORE group

Updates from -00 (1/2)

- Double update after IETF 103, mostly based on:
  - Latest developments on the RD
  - Discussion at the CoRE interim on 23/01/2019
  - Comments from Jim and Francesca (thanks!)

- Main changes:
  - Now based on the latest RD-group usage pattern
  - Difference between Application Groups and OSCORE Security Groups
  - Renaming: '*oscore-gp*' → '***app-gp***'
  - Clarified parameter semantics
  - Updated registration/discovery examples

Updates from -00 (2/2)



Client of application group

Different key sets

Resources for given function

Registration

- The GM registers itself with the RD
  - MUST include all its join resources, with their link attributes
  - New ‘rt’ value “osc.j” in the CoRE Parameters registry

```
Request: GM -> RD

Req: POST coap://rd.example.com/rd?ep=gm1
Content-Format: 40
Payload:
</join/feedca570000>;ct=41;rt="core.osc.j";
oscore-gid="feedca570000";app-gp="group1"

Response: RD -> GM

Res: 2.01 Created
Location-Path: /rd/4521
```

Discovery (1/2)

- The device performs a resource lookup at the RD
  - Known information: name of the Application Group, i.e. “group1”
  - Need to know: OSCORE Group Identifier; Join resource @ GM; Multicast IP address
  - ‘*app-gp*’ → Name of the Application Group, acting as tie parameter in the RD

```
Request: Joining node -> RD

Req: GET coap://rd.example.com/lookup/res?rt=core.osc.j&app-gp=group1

Response: RD -> Joining node

Res: 2.05 Content
Payload:
<coap://[2001:db8::ab]/join/feedca570000>;rt="core.osc.j";
oscore-gid="feedca570000";app-gp="group1";
anchor="coap://[2001:db8::ab]"
```

Discovery (2/2)

- The device performs an endpoint lookup at the RD
  - Still need to know the Multicast IP address
  - ‘ep’ // Name of the Application Group, value from ‘*app-gp*’
  - ‘base’ // Multicast IP address used in the Application Group

```
Request: Joining node -> RD

Req: GET coap://rd.example.com/lookup/ep?et=core.rd-group&ep=group1

Response: RD -> Joining node

Res: 2.05 Content
Payload:
</rd/501>;ep="group1";et="core.rd-group";\
base="coap://[ff35:30:2001:db8::23]"
```

Summary and next steps

- Main updates
  - Aligned with the latest RD-group usage pattern
  - Distinction between security groups and application groups
  - Update parameter semantics and examples

- Open points for discussion
  - Register '*oscore-gid*' and '*app-gp*'? New "Link Target Attributes" Registry?
  - Generalization for other group paradigms? A separate document?

- Need for document reviews

Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-core-oscore-discovery

Backup

Application & Security Groups

- Application group
  - Defined in {RD} and reused as is
  - Set of CoAP endpoints sharing a pool of resources
  - Registered and looked up just as per Appendix A of {RD}

- OSCORE Security Group
  - Set of CoAP endpoints sharing a common Group OSCORE Security Context
  - A Group Manager registers the join resources for accessing its OSCORE Groups

Semantics updates

- Semantics revision/clarification
  - *oscore-gid* → Identifier of an OSCORE Security Group
  - *app-gp* → Name of an Application Group, tie parameter in 2-step lookups

- *oscore-gid*
  - Single occurrence, with single value

- *app-gp*
  - Used to be *oscore-gp*, but it is not strictly related to oscore
  - Multiple occurrences are possible, each with a single value
  - The same value cannot be repeated in a same request/response

Group Communication for the Constrained Application Protocol (CoAP)

draft-dijk-core-groupcomm-bis-00

Esko Dijk, IoTconsultancy.nl
Chonggang Wang, InterDigital
Marco Tiloca, RISE

IETF 104, CoRE WG, Prague, March 26th, 2019

Motivation

- RFC 7390 was published in 2014
  - CoAP functionalities available by then were covered
  - No group security solution was available to indicate
  - It is an Experimental document (started as Informational)

- What has changed?
  - More CoAP functionalities have been developed (Block-Wise, Observe)
  - RESTful interface for membership configuration is not really used
  - Group OSCORE provides group end-to-end security for CoAP

- Practical considerations
  - Group OSCORE clearly builds on RFC 7390 normatively
  - However, it can refer RFC 7390 only informationally

Goal

- Intended normative update to RFC 7390 (if approved)
  - As a Standards Track document
  - Refer to RFC 7390 when possible
- Standard reference for implementations now based on RFC 7390, e.g.:
  - “Eclipse Californium 2.0.x” (Eclipse Foundation)
  - “Implementation of CoAP Server & Client in Go” (OCF)
- What’s in scope?
  - Updated/new use cases
  - CoAP functionalities in groups, including latest developments
  - Both unsecured and secured CoAP group communication
  - Principles for secure group configurations

Content overview (1/3)

- Compact use case introduction
  - Discovery (3); Operational (3); Software Update
- Communication in CoAP groups
  - Creation and maintenance
  - Usage of CoAP (transport and internetworking still TBD)
- Observing resource
  - Not supported in RFC 7390
  - This document explicitly allows it → Update also RFC 7641
  - A single GET request observes a resource on all group members

Content overview (2/3)

- Unsecured group communication
  - CoAP “NoSec” mode, like in RFC 7390
  - Acceptable for non critical scenarios

- Secured group communication
  - Group OSCORE as security protocol
  - CoAP “network” group ↔ OSCORE “security” group
  - Secure group maintenance upon membership change
  - Key management recommended to follow *ace-key-groupcomm-oscore*

Content overview (3/3)

- Security considerations – “NoSec”
  - SHOULD use only for non-critical applications

- Security considerations – Group OSCORE
  - MUST use for sensitive and critical applications
  - Specific references to *core-oscore-groupcomm*
  - Addressing of security attacks in group (see RFC 7252)
  - Notes on key management as in *ace-key-groupcomm-oscore*

Next steps

- Complete the document
  - Replace TBDs with actual content
  - Add possibly missing points. Any input?

- Need for document reviews

Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-groupcomm-bis

Pub Sub and Multicast

Summary of the CoRE Hallway Discussion @ IETF104 Hackathon

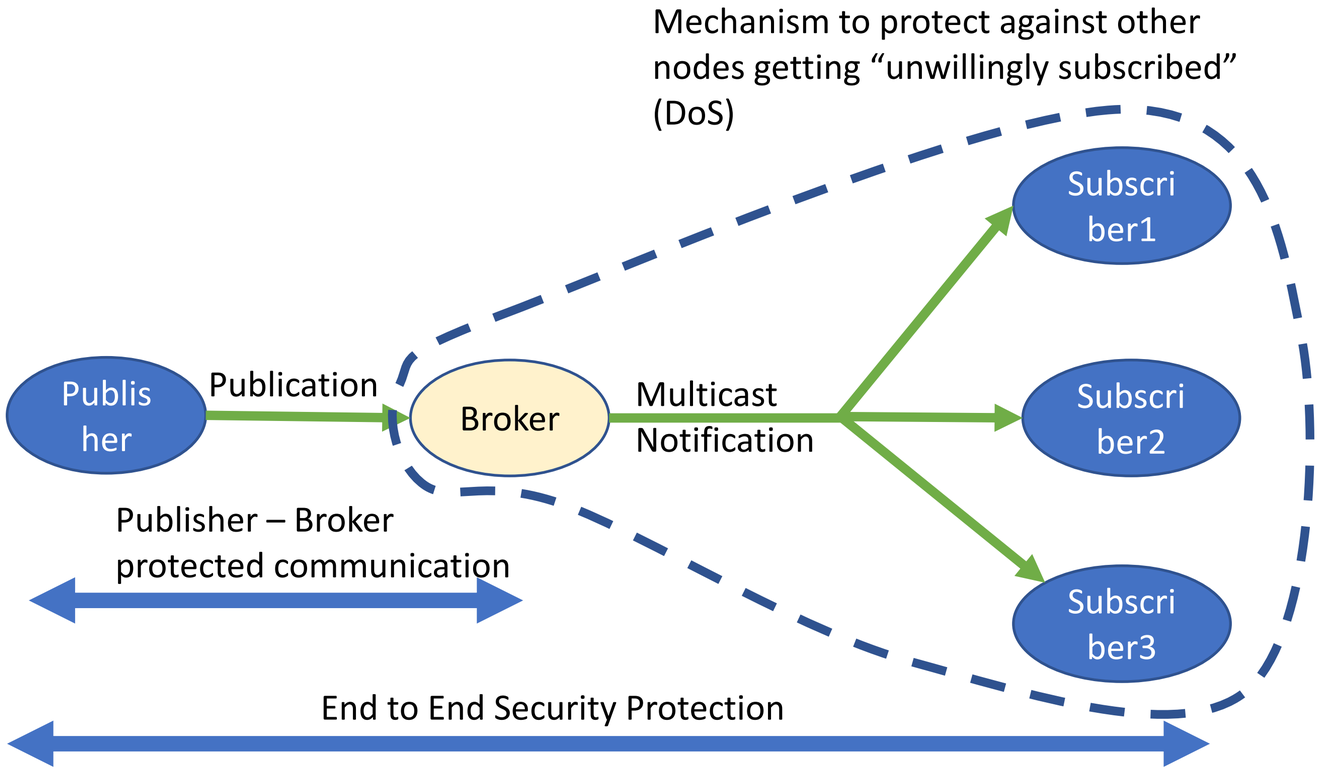
Francesca Palombini

(Jim, John, Carsten, Ari, Klaus, Christian, Marco, Göran, Peter, Ivo, …)

Background and Motivation

- Efficiency goal: sending multicast notifications to subscribers

- Security goals:
  - Authorization and authentication
  - Publications protection
  - DoS protection

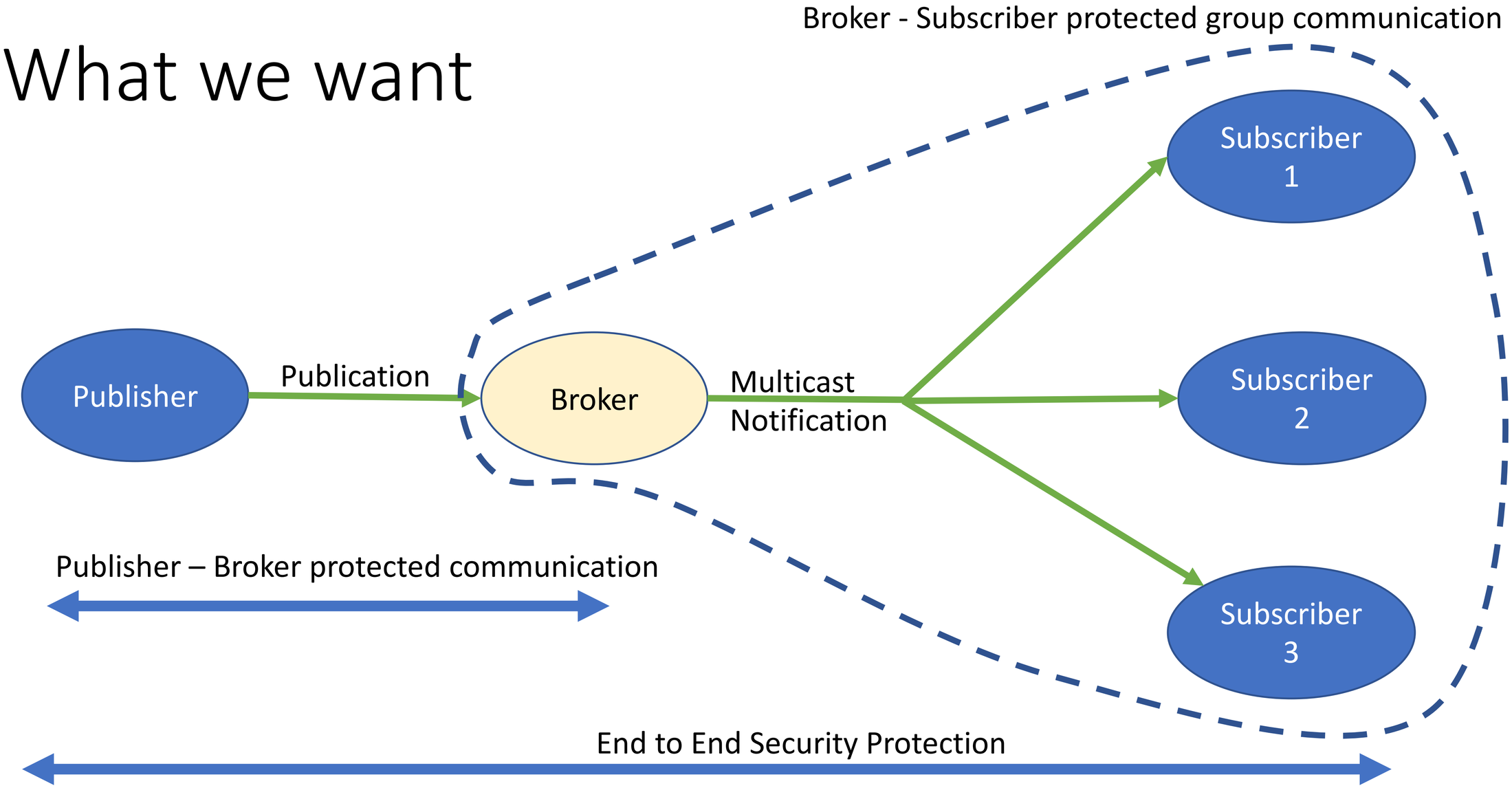


The challenges

- The “plumbing” = how to make the Pub/sub architecture work with multicast delivery of notifications
- How to protect against DoS attacks
- How to protect the communication (Pub-Broker, Pub-Subs, Subs-Broker) and provide authentication and authorization

Slides Used at the Hallway Meeting

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

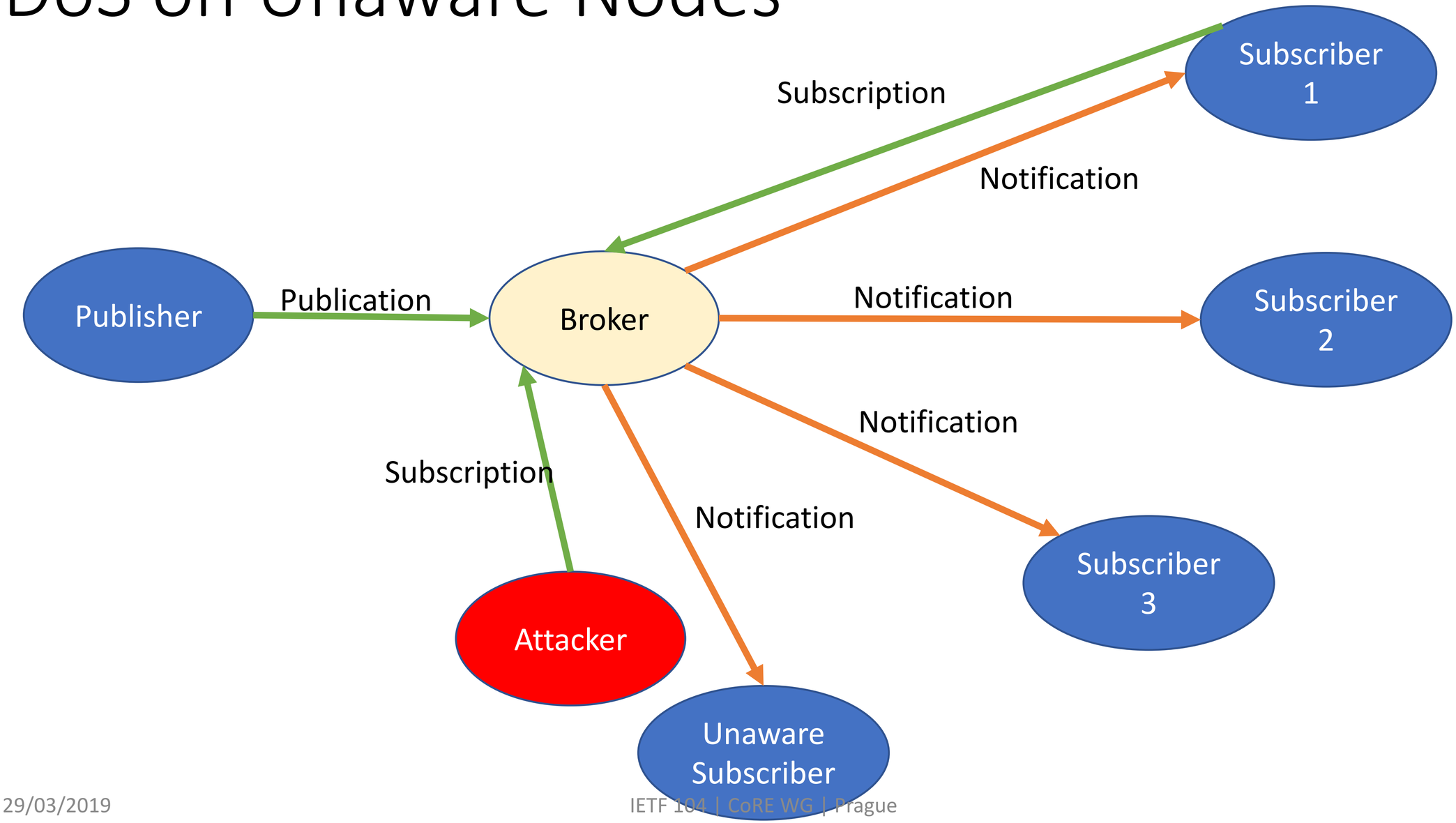
What we want – Sec Requirements

- 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

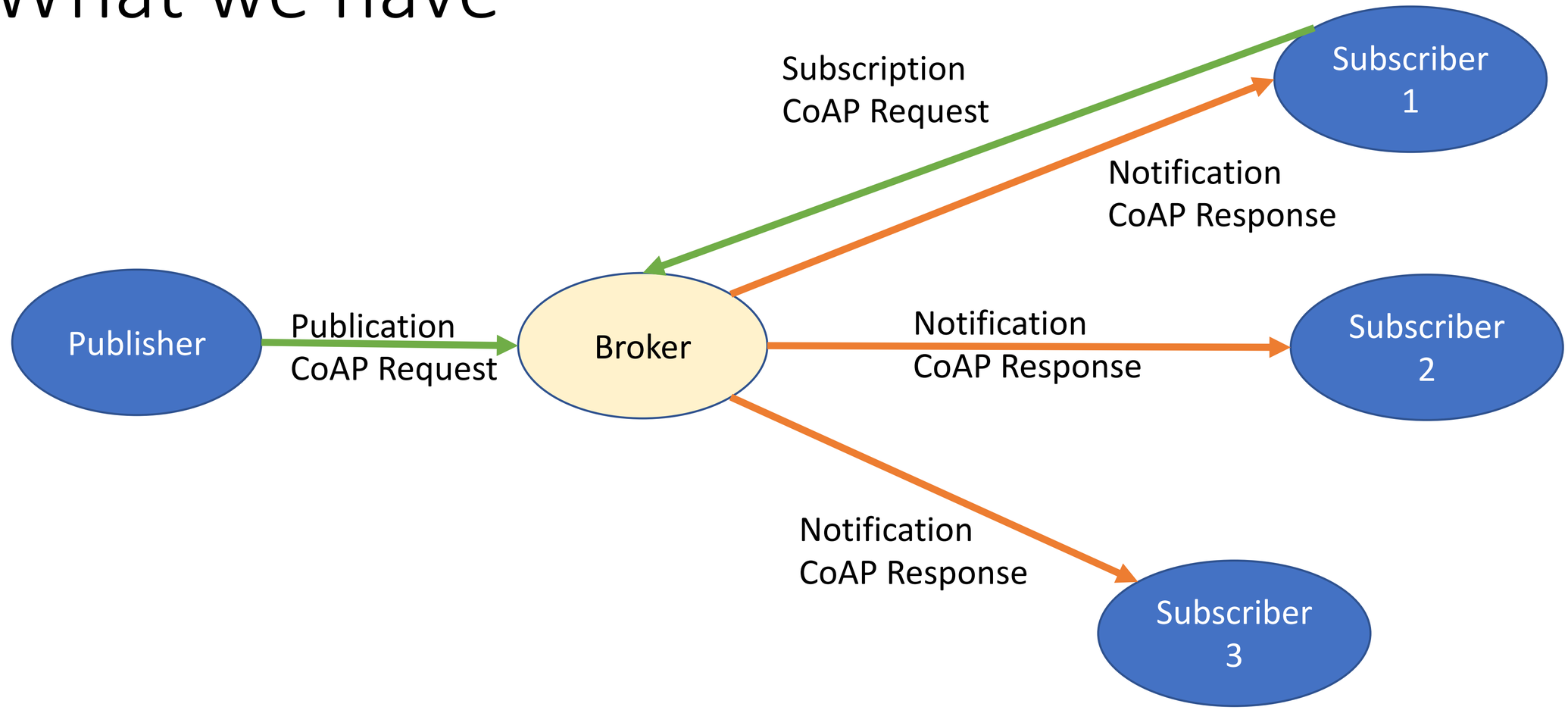
All the above + key distribution is covered by draft-palombini-ace-coap-pubsub-profile-03

- 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

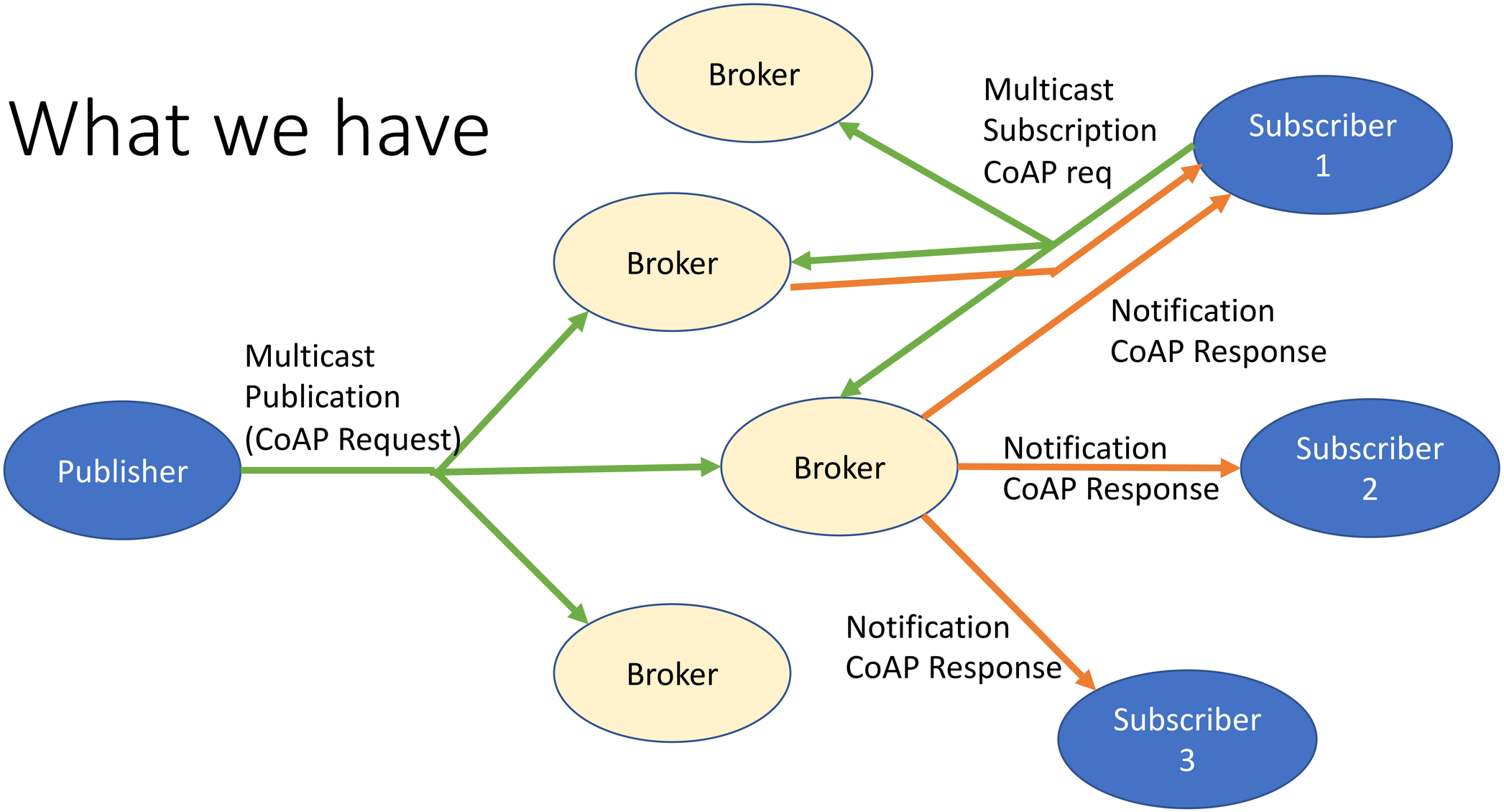


What we have



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

What we have



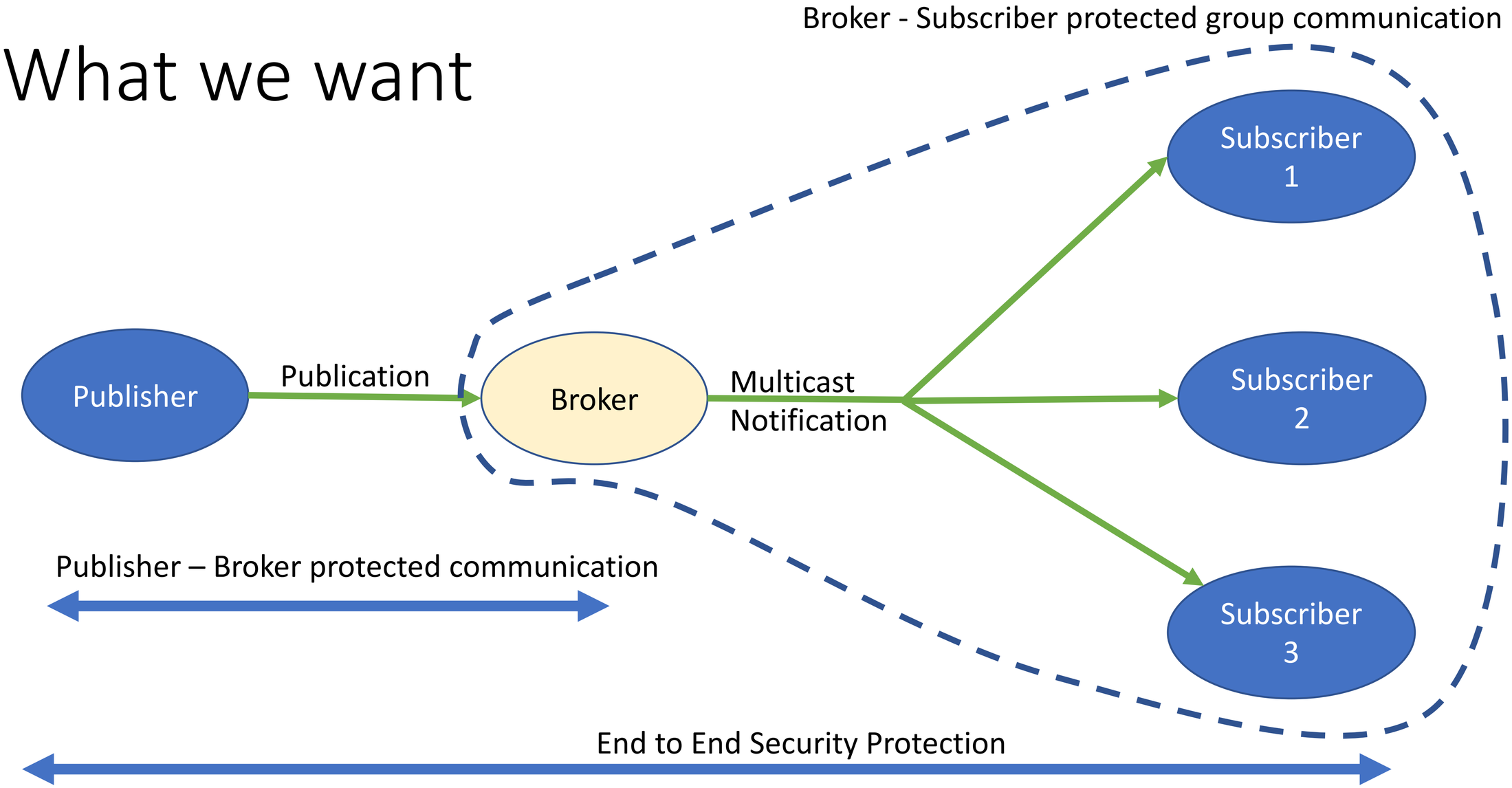
https://tools.ietf.org/html/draft-dijk-core-groupcomm-bis-00
updates multicast with Observe requests

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

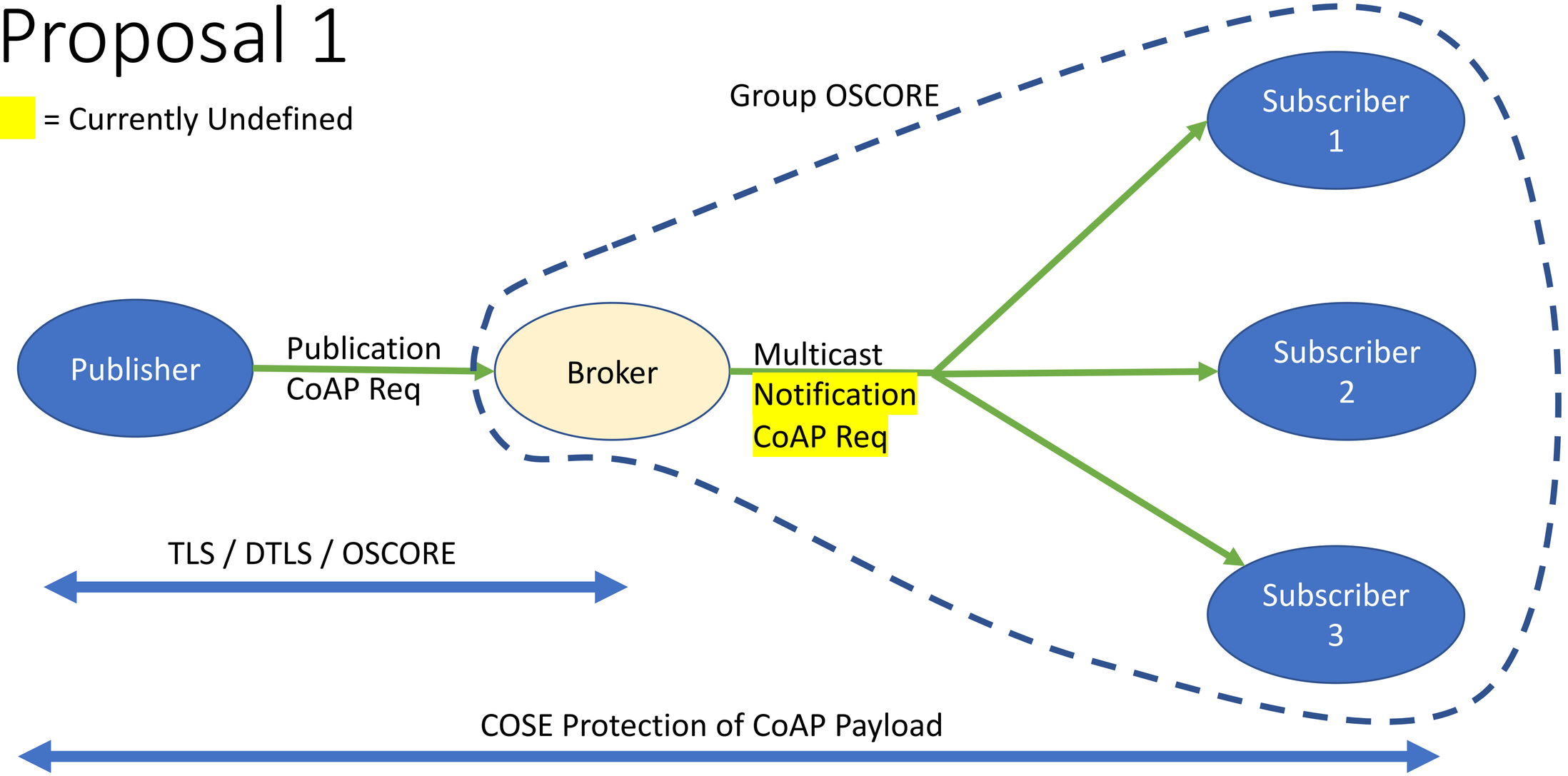
- Notifications as CoAP requests + Multicast the notification +
  1. Group OSCORE (Broker – Subscribers) + Payload protection (Pub – Subscribers)
  2. Group OSCORE (Pub – Subscribers) + additional DoS protection mechanism
  3. Payload protection (Pub – Subscribers) + additional DoS protection mechanism

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?

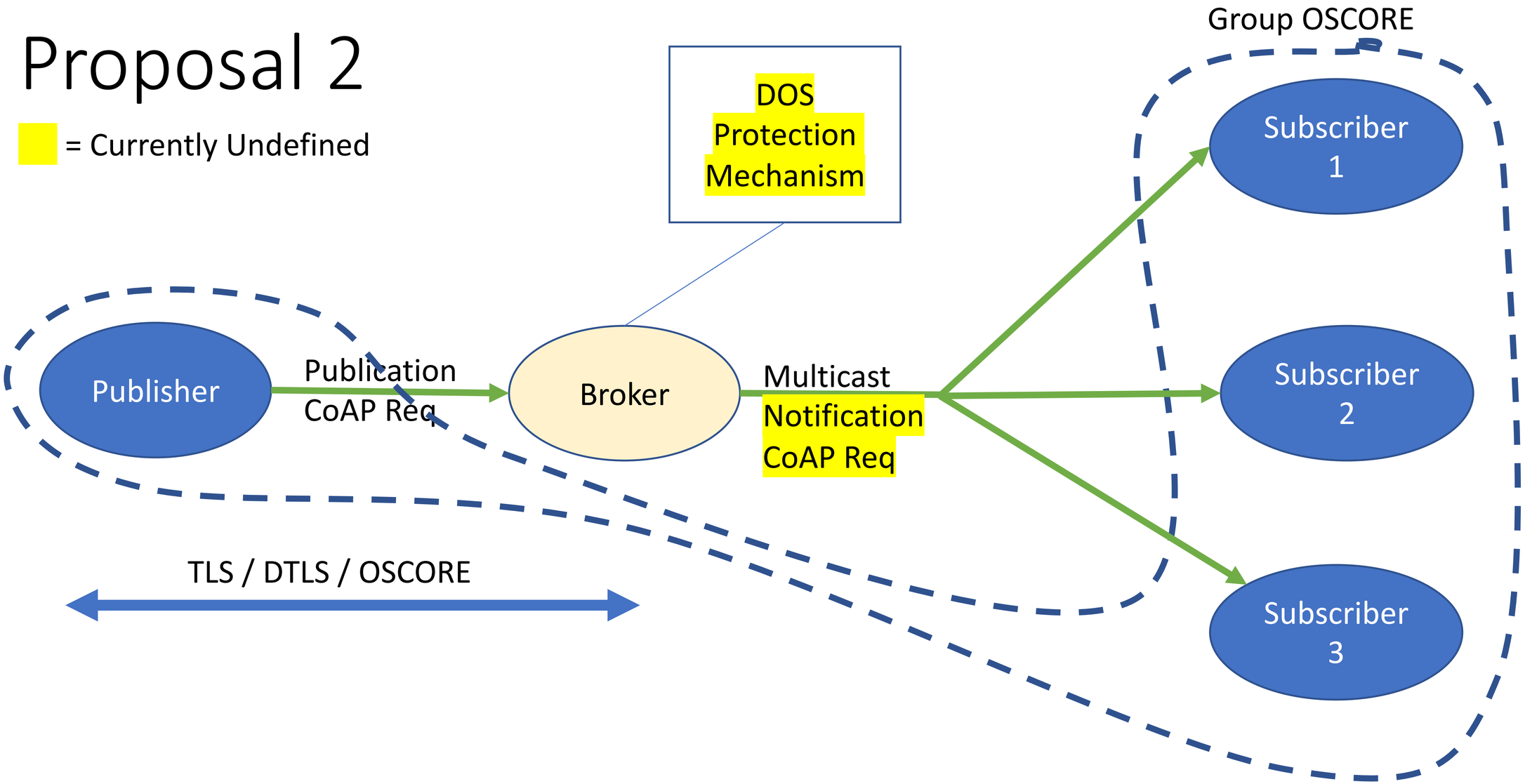
Proposal 1

= Currently Undefined



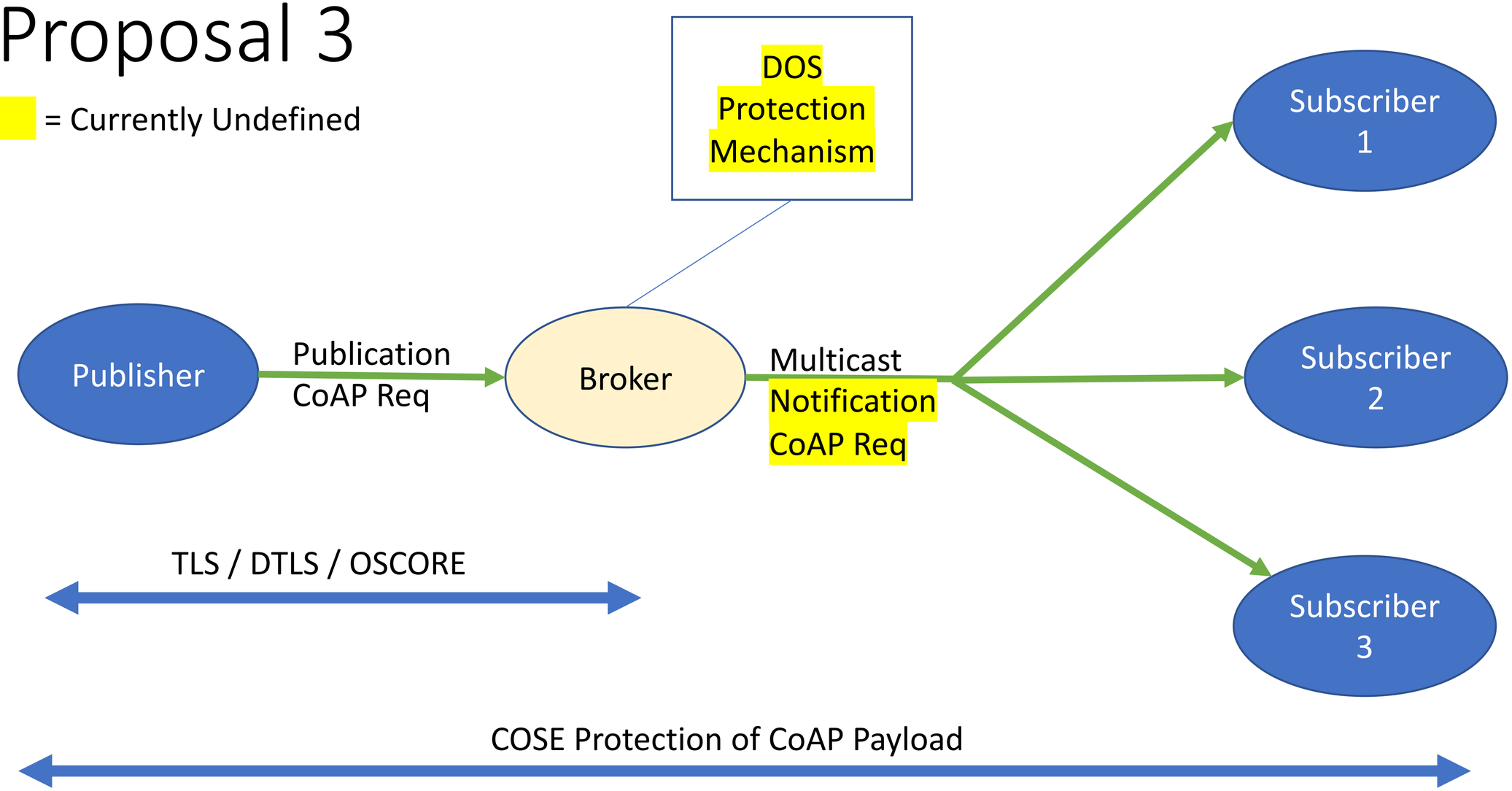
Proposal 2

= Currently Undefined



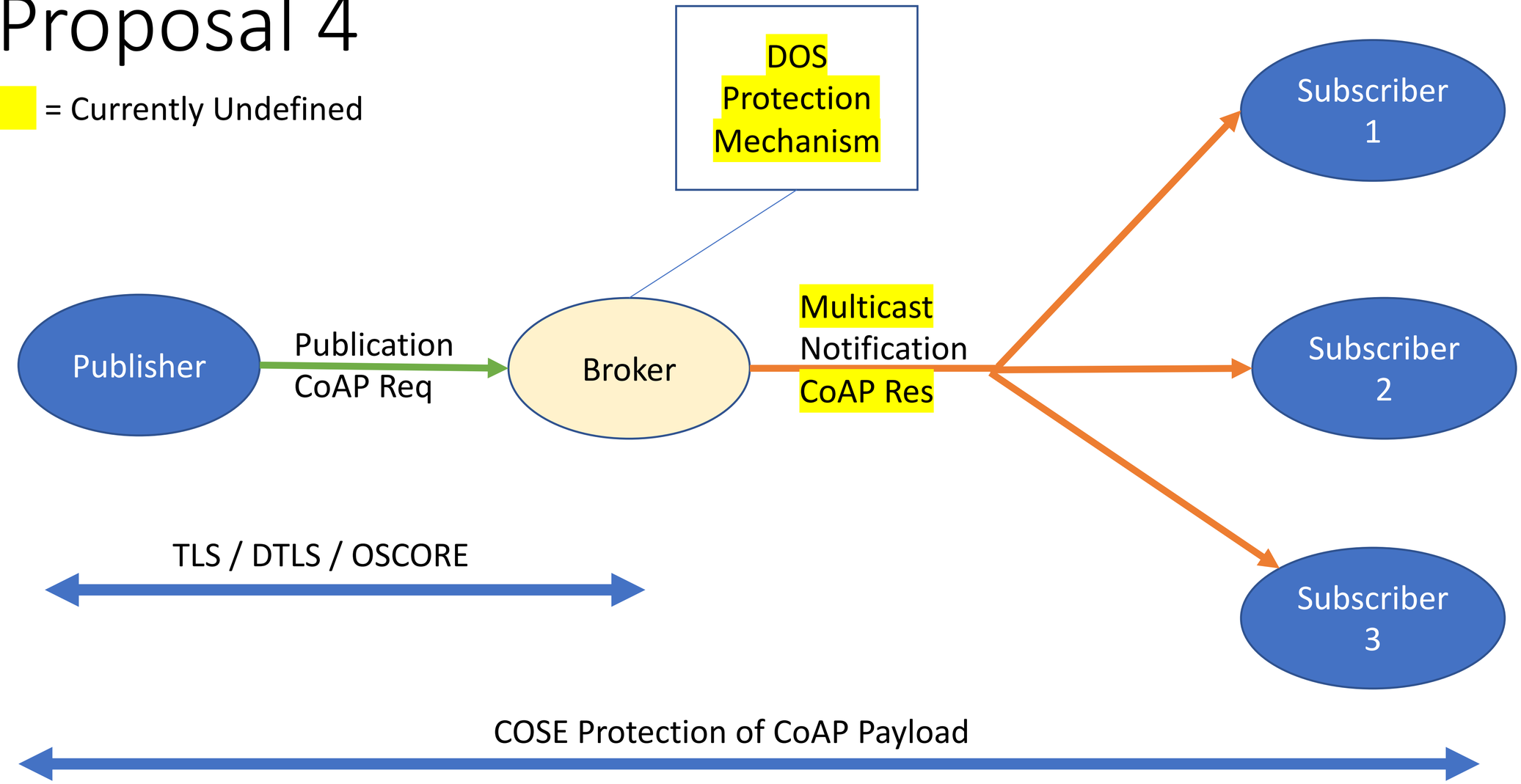
Proposal 3

= Currently Undefined



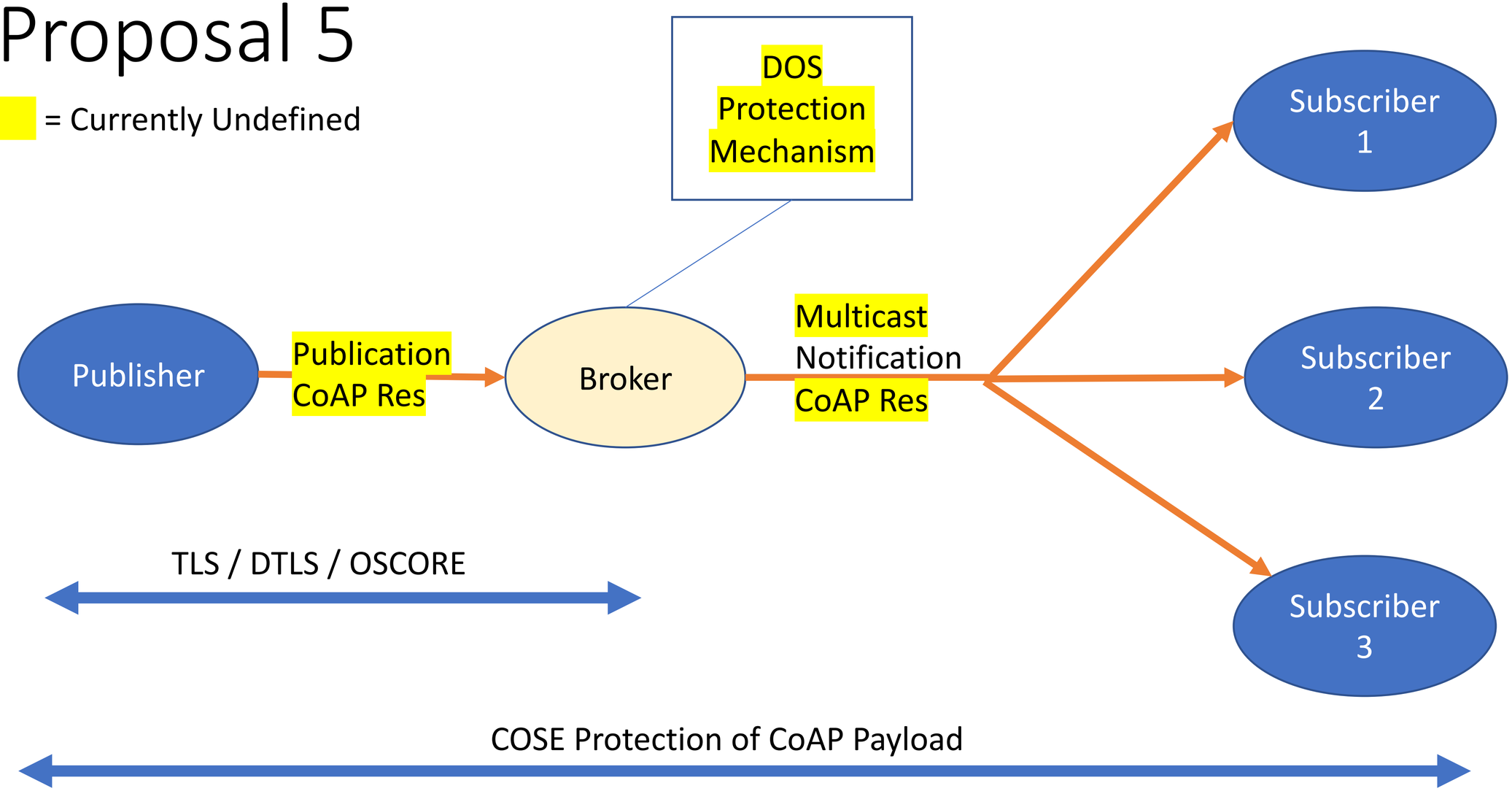
Proposal 4

= Currently Undefined



Proposal 5

= Currently Undefined



All times are in time-warped CET (UTC+01:00)

Tuesday (120 min)

- 13:50–13:59 Intro, Agenda, Status
- 13:59–14:09 ERT (CA)
- 14:09–14:12 Stateless (KH)
- 14:12–14:57 Groupcomm/security (MT, FP)
- 14:57–15:20 SenML (AK)
- 15:20–15:34 CoRECONF
- 15:34–15:50 Misc, Pulling items forward from Thu

SenML Data Value Content-Format Indication

draft-keranen-core-senml-data-ct-01

Ari Keränen

IETF 104

Content-Format indication

- SenML Records can contain (binary) "data values" in a "vd" field
- Information how to decode the value established out of band

```
[
 {"bn":"urn:dev:ow:10e2073a01080063:", "n":"temp", "v":7.1},
  {"n":"open", "vb":false},
  {"n":"nfc-reader", "vd":"aGkgCg"}
]
```

- Proposal: Content-Format indication ("ct") field to indicate the Content-Format of the data in the SenML Record

Example SenML Record with data value and Content-Format indication

```
{"n":"nfc-reader", "vd":"gmNmb28YKg", "ct":60}
```

Example SenML Record with data value and Content-Format indication

```
{"n":"nfc-reader", "vd":"gmNmb28YKg", "ct":60}
```

CBOR CoAP Content Format

base64(

```
82          # array(2)
  63        # text(3)
    666F6F  # "foo"
  18 2A     # unsigned(42)
```

)

Content-Type and Content-Coding

- Not all Media-Types and Content-Coding alternatives (will) have CoAP Content-Format IDs assigned
  - Some may not even make sense for CoAP in general
- Proposal:
  - "content-type" field for Content-Type as a string
  - "content-coding" field for Content-Coding as a string

```
{"n":"nfc-reader-42",
 "vd":"H4sIAA+dmFwAAzMx0jEZMAQALnH8Yn0AAAA",
 "content-type":"text/csv", "content-coding":"gzip"}
```

Base value challenge(s)

- Draft proposes base values for all fields (b + field name)
  - "bct", "bcontent-type", "bcontent-coding"
  - Applies to all values with "vd" without specific "ct", "content-type" or "content-coding"
- Should not mix "ct" and "content-type/coding" fields
- Need a way to "undo" base content-type/coding and bct
  - Currently no method for inter-dependent field values with base fields
  - For example, "if both present, ct wins, except if it's -1 (undefined)"

All times are in time-warped CET (UTC+01:00)

Tuesday (120 min)

- 13:50–13:59 Intro, Agenda, Status
- 13:59–14:09 ERT (CA)
- 14:09–14:12 Stateless (KH)
- 14:12–14:57 Groupcomm/security (MT, FP)
- 14:57–15:20 SenML (AK)
- 15:20–15:34 CoRECONF
- 15:34–15:50 Misc, Pulling items forward from Thu

All times are in time-warped CET (UTC+01:00)

Tuesday (120 min)

- 13:50–13:59 Intro, Agenda, Status
- 13:59–14:09 ERT (CA)
- 14:09–14:12 Stateless (KH)
- 14:12–14:57 Groupcomm/security (MT, FP)
- 14:57–15:20 SenML (AK)
- 15:20–15:34 CoRECONF
- 15:34–15:50 Misc, Pulling items forward from Thu

Constrained RESTful Environments WG (core)

Chairs:

Jaime Jiménez <jaime.jimenez@ericsson.com>

Carsten Bormann <cabo@tzi.org>

Mailing List:

core@ietf.org

Jabber:

core@jabber.ietf.org

- **We assume people have read the drafts**
- **Meetings serve to advance difficult issues by making good use of face-to-face communications**
- **Note Well: Be aware of the IPR principles, according to RFC 8179 and its updates**

üBlue sheets
üScribe(s)

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

All times are in time-warped CET (UTC+01:00)

Friday (90 min)

- **09:00–09:05 Intro, Agenda**
- **09:05–09:35 Core applications (pubsub, dyn, if)**
- **09:35–10:20 Resource-Directory LC, RD & CoRAL**
- **10:20–10:30 New work: speedy-blocktrans**

All times are in time-warped CET (UTC+01:00)

Friday (90 min)

- 09:00–09:05 Intro, Agenda
- 09:05–09:35 Core applications (pubsub, dyn, if)
- 09:35–10:20 Resource-Directory LC, RD & CoRAL
- 10:20–10:30 New work: speedy-blocktrans

All times are in time-warped CET (UTC+01:00)

Friday (90 min)

- 09:00–09:05 Intro, Agenda
- 09:05–09:35 Core applications (pubsub, dyn, if)
- 09:35–10:20 Resource-Directory LC, RD & CoRAL
- 10:20–10:30 New work: speedy-blocktrans

All times are in time-warped CET (UTC+01:00)

Friday (90 min)

- **09:00–09:05 Intro, Agenda**
- **09:05–09:35 Core applications (pubsub, dyn, if)**
- **09:35–10:20 Resource-Directory LC, RD & CoRAL**
- **10:20–10:30 New work: speedy-blocktrans**