

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**
- **We work as individuals and try to be nice to each other**
- **Note Well: Be aware of the IPR principles, according to RFC 8179 and its updates**
 - ★Blue sheets
 - ★Scribe(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)



I E T F

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 (prepared in T2TRG right after CoRE)
- 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

11

Recent changes, especially since chair review

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”

12

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

¹⁶ 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 Context¹⁷
 - 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)

18

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 ‘l’ options of either the request or the response

20

› 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?

23

- › Interop tests
 - 3+ implementations

Thank you!

Comments/questions?

24

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

Discovery of OSCORE Groups with the CoRE Resource Directory

draft-tiloca-core-oscore-discovery-02

25

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

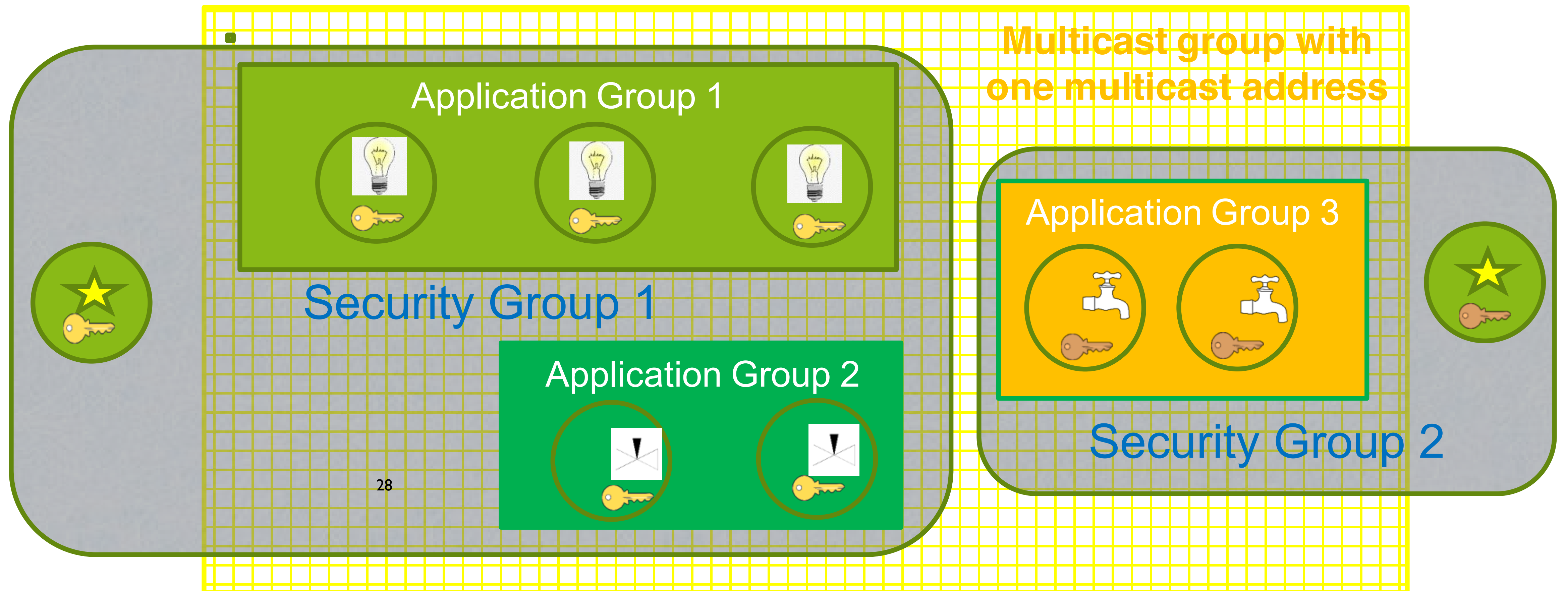
26

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?
- Generalization³² for other group paradigms? A separate document?

› Need for document reviews

Thank you!

Comments/questions?

33

<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

³⁷ 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 cases³⁹
 - 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?

44

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

Pub Sub and Multicast

Summary of the CoRE Hallway Discussion @ IETF104 Hackathon

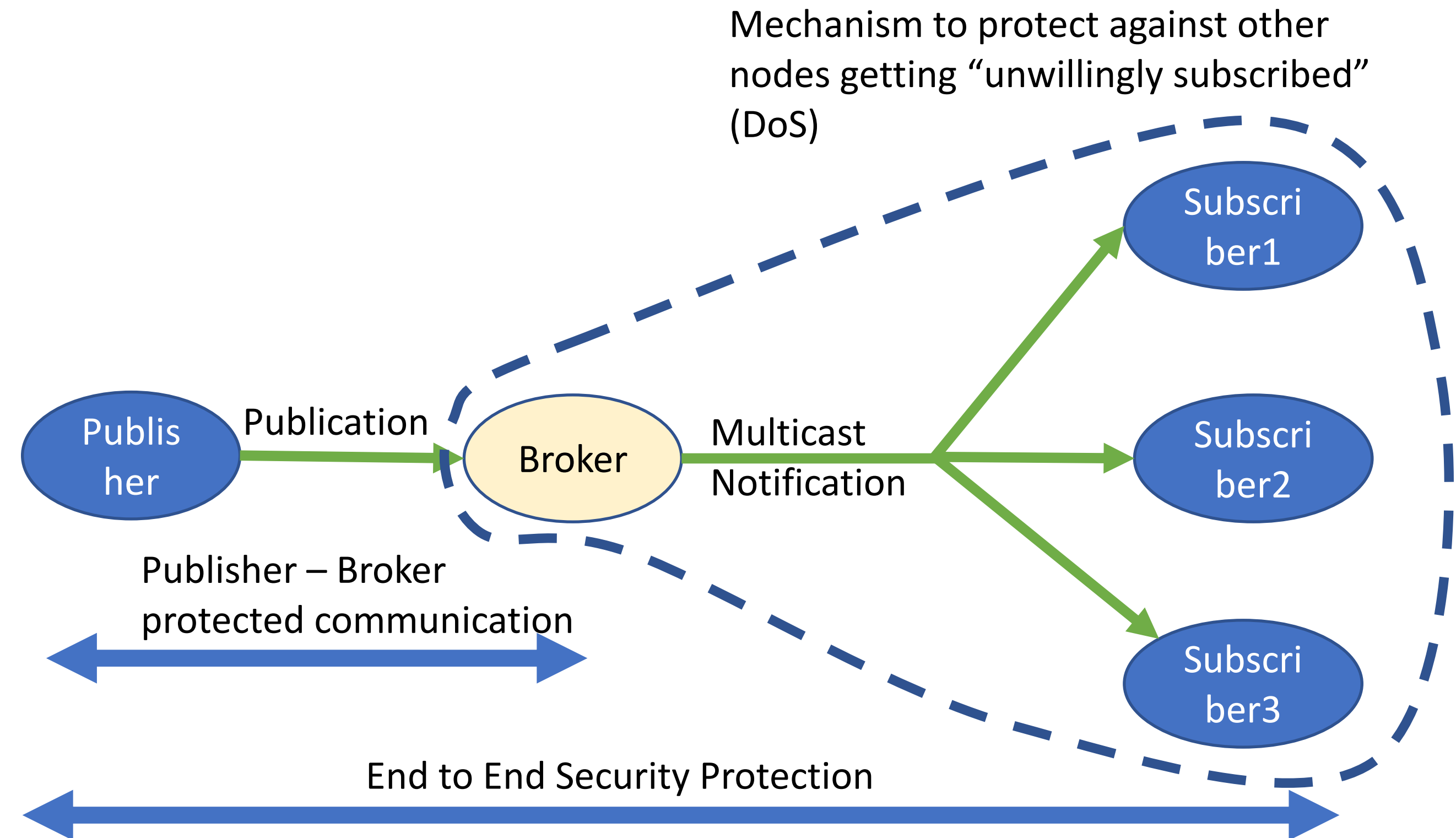
45

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 protection⁴⁶
 - DoS protection



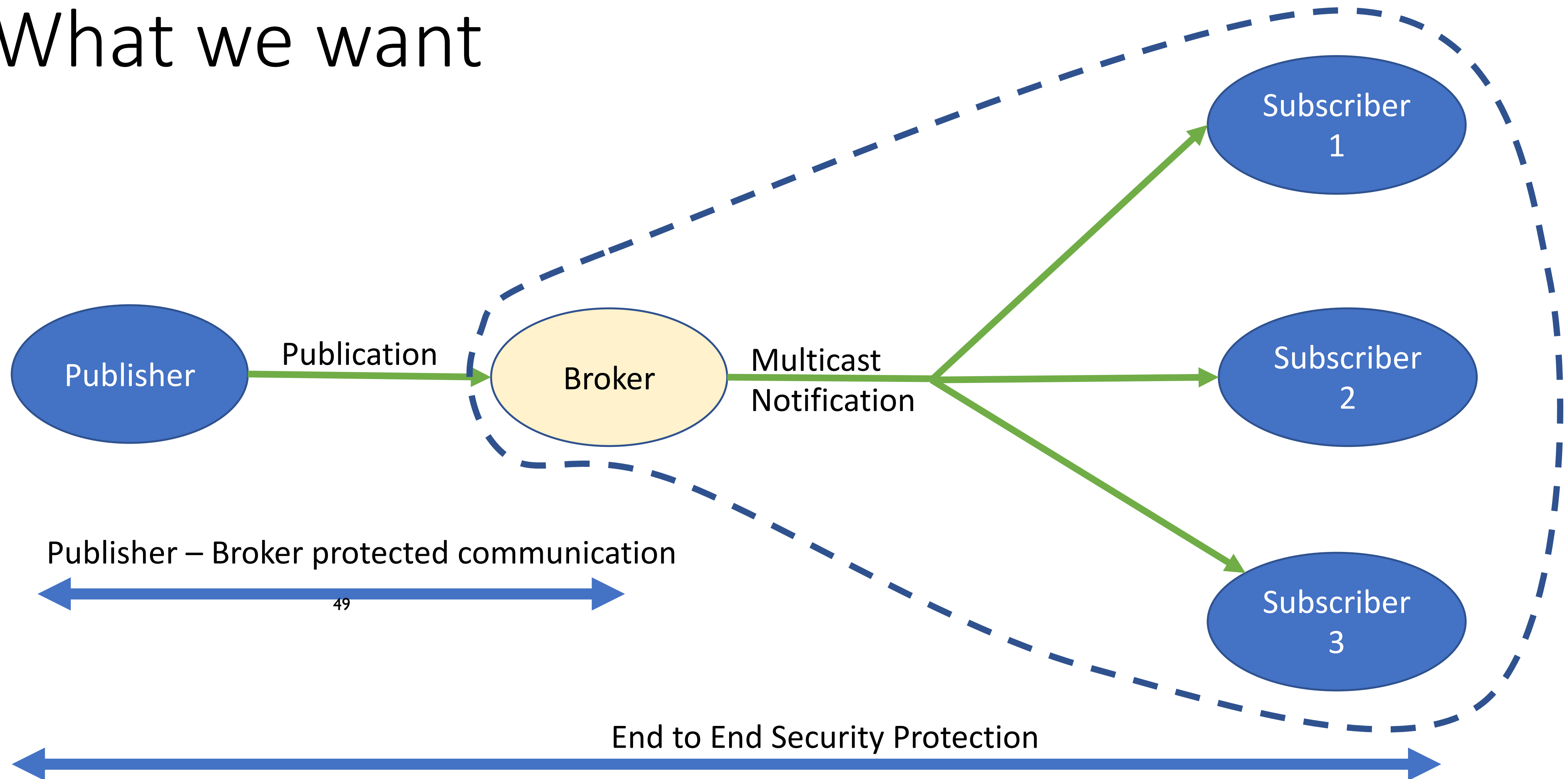
The challenges

- 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

48

What we want



What we want – Sec Requirements

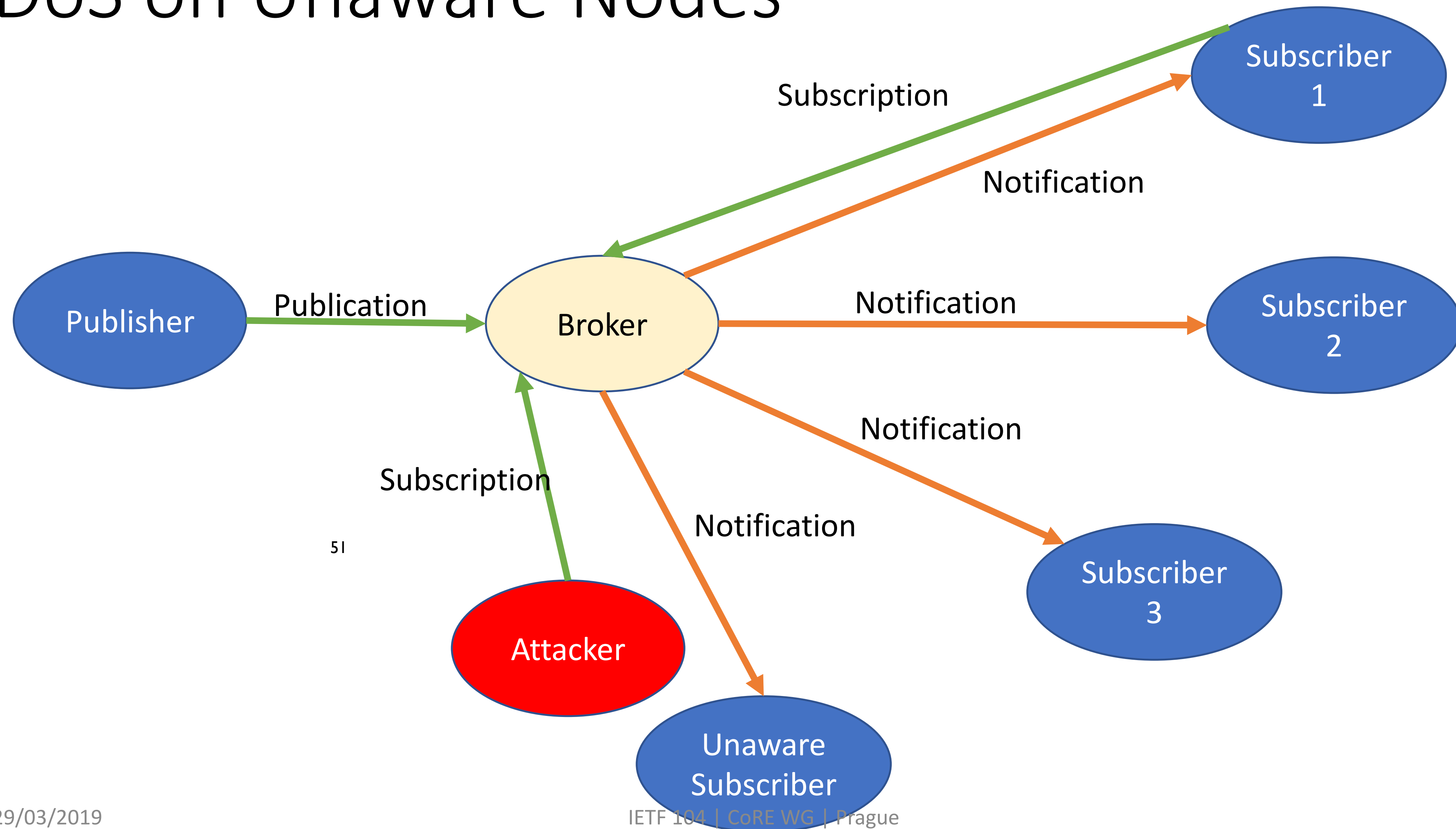
- The Publisher communicates securely with the Broker and must be authorized to publish on the Broker
- The publication is protected (protection of CoAP payload)
- The Subscribers must be authorized to decrypt and verify the publication

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

50

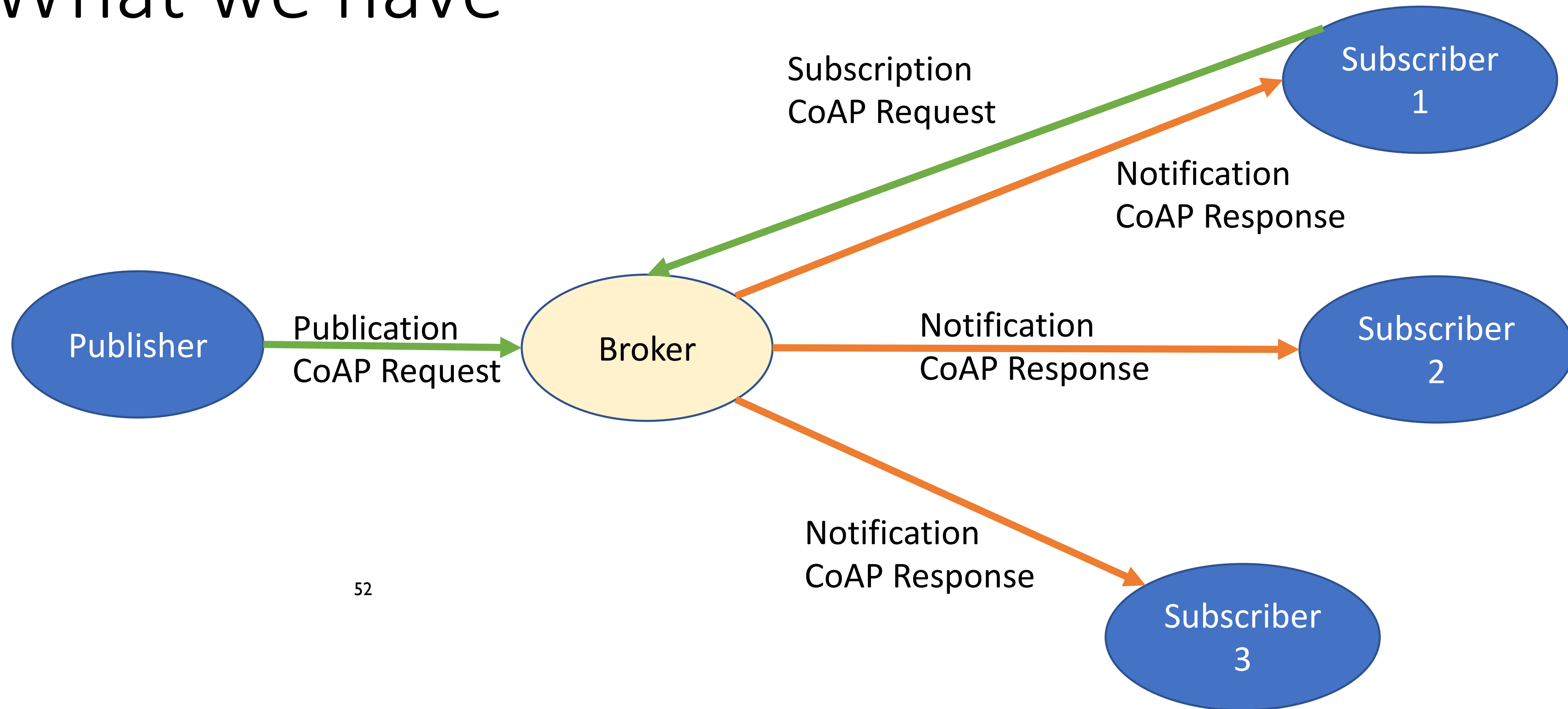
- Additionally, the Subscriber must prove address ownership of a subscription request, otherwise an attacker could DoS external nodes that do not want to receive the publications

DoS on Unaware Nodes



51

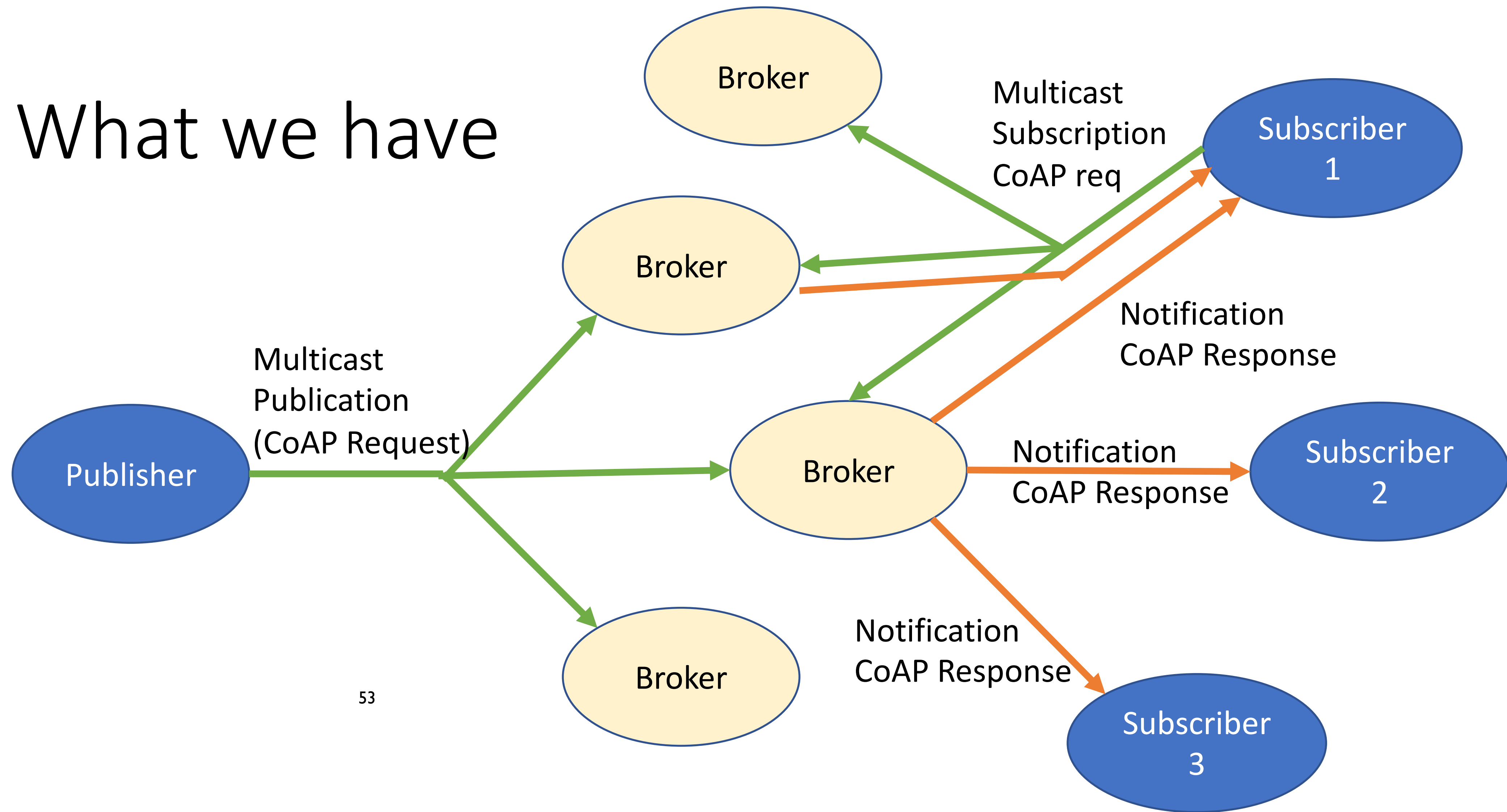
What we have



52

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

What we have



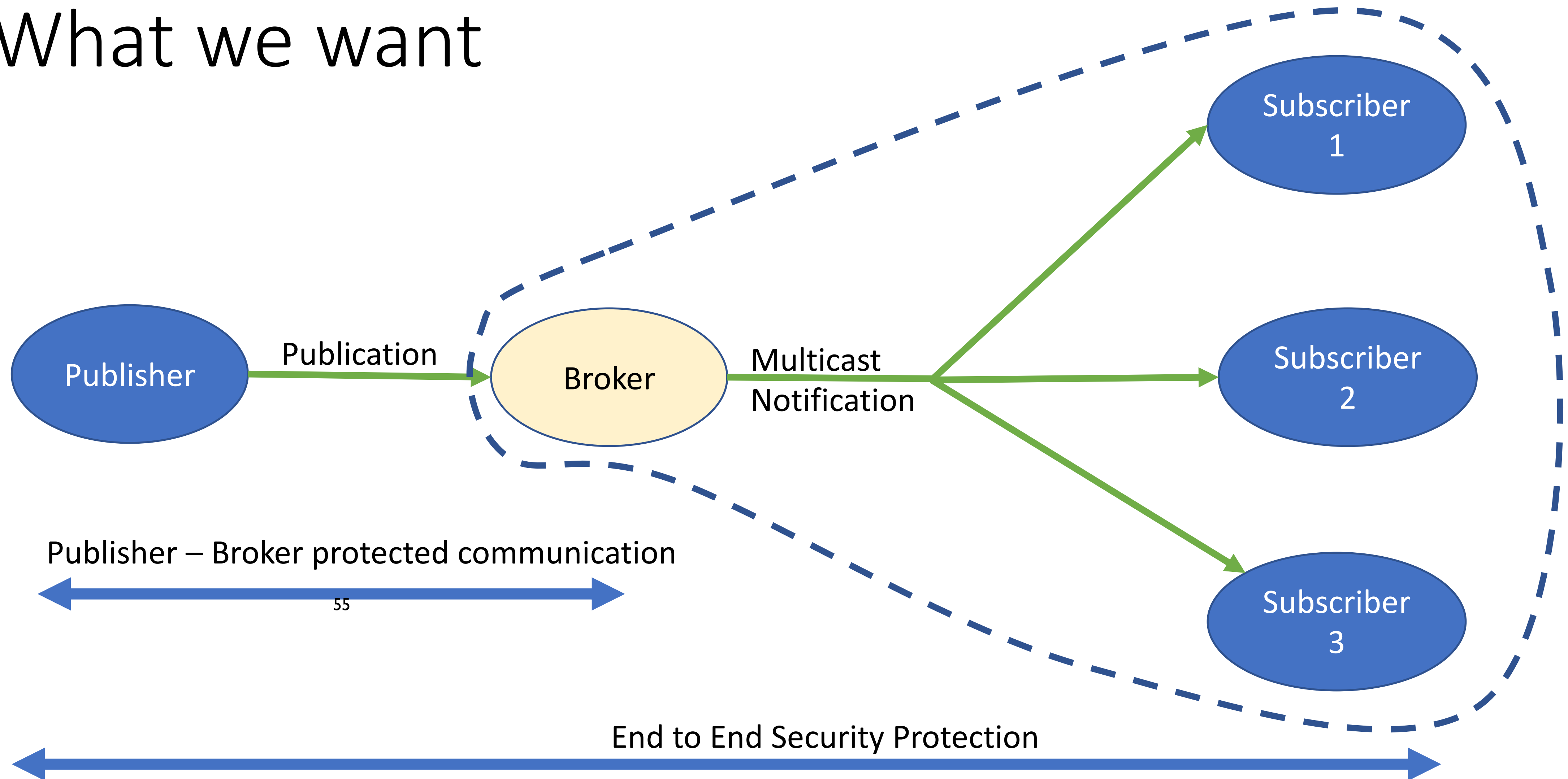
53

<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



How do we get it

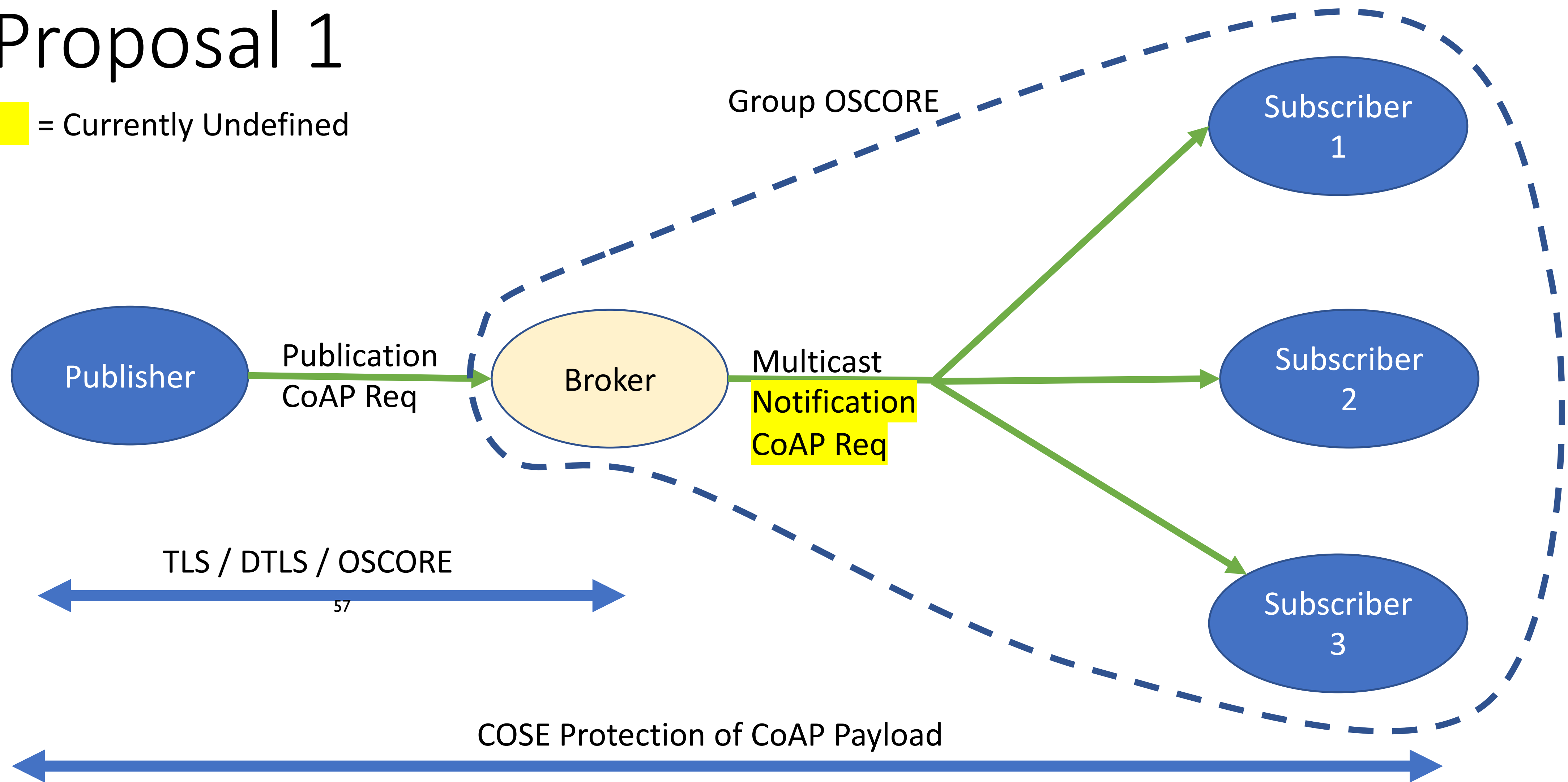
- Notifications as CoAP requests + Multicast the notification +
 1. Group OSCORE (Broker – Subscribers) + Payload protection (Pub – Subscribers)
 2. Group OSCORE (Pub – Subscribers) + additional DoS protection mechanism
 3. Payload protection (Pub – Subscribers) + additional DoS protection mechanism

- 4. Define multicast responses (how do we deal with the token?) + use multicast notifications to Subscribers + ?? (No secure multicast defined for multicast responses⁵⁶)

- Anything else?

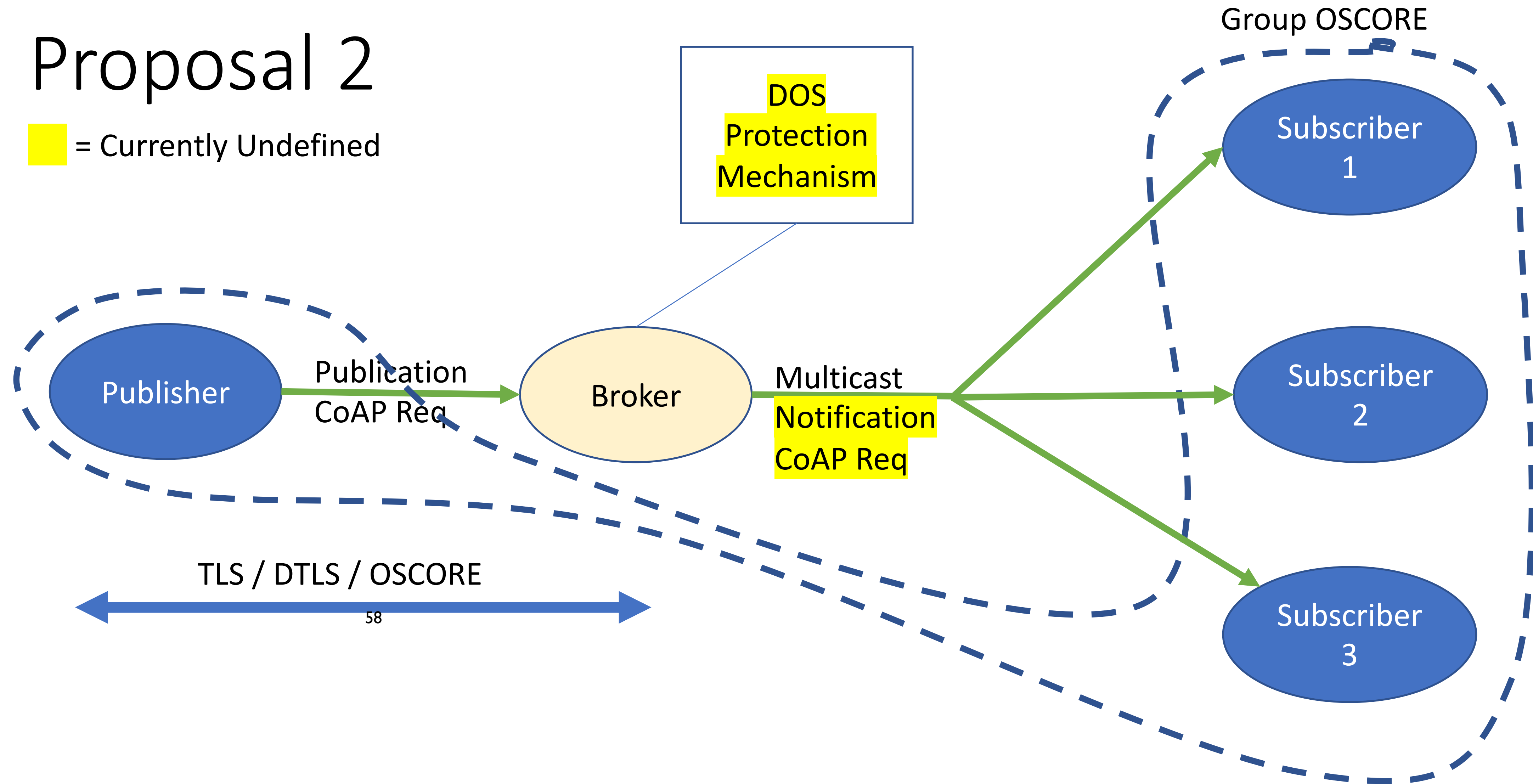
Proposal 1

= Currently Undefined



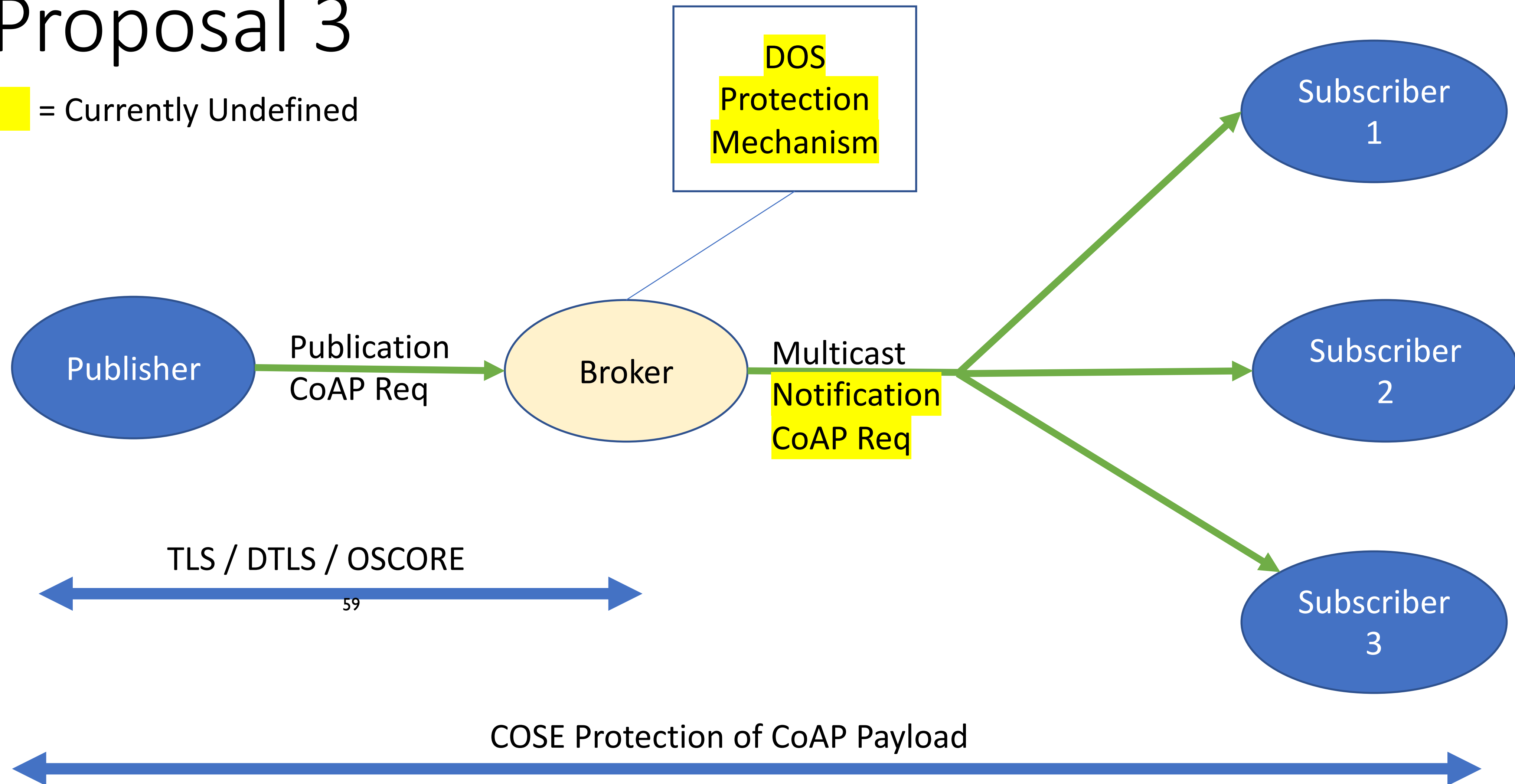
Proposal 2

■ = Currently Undefined



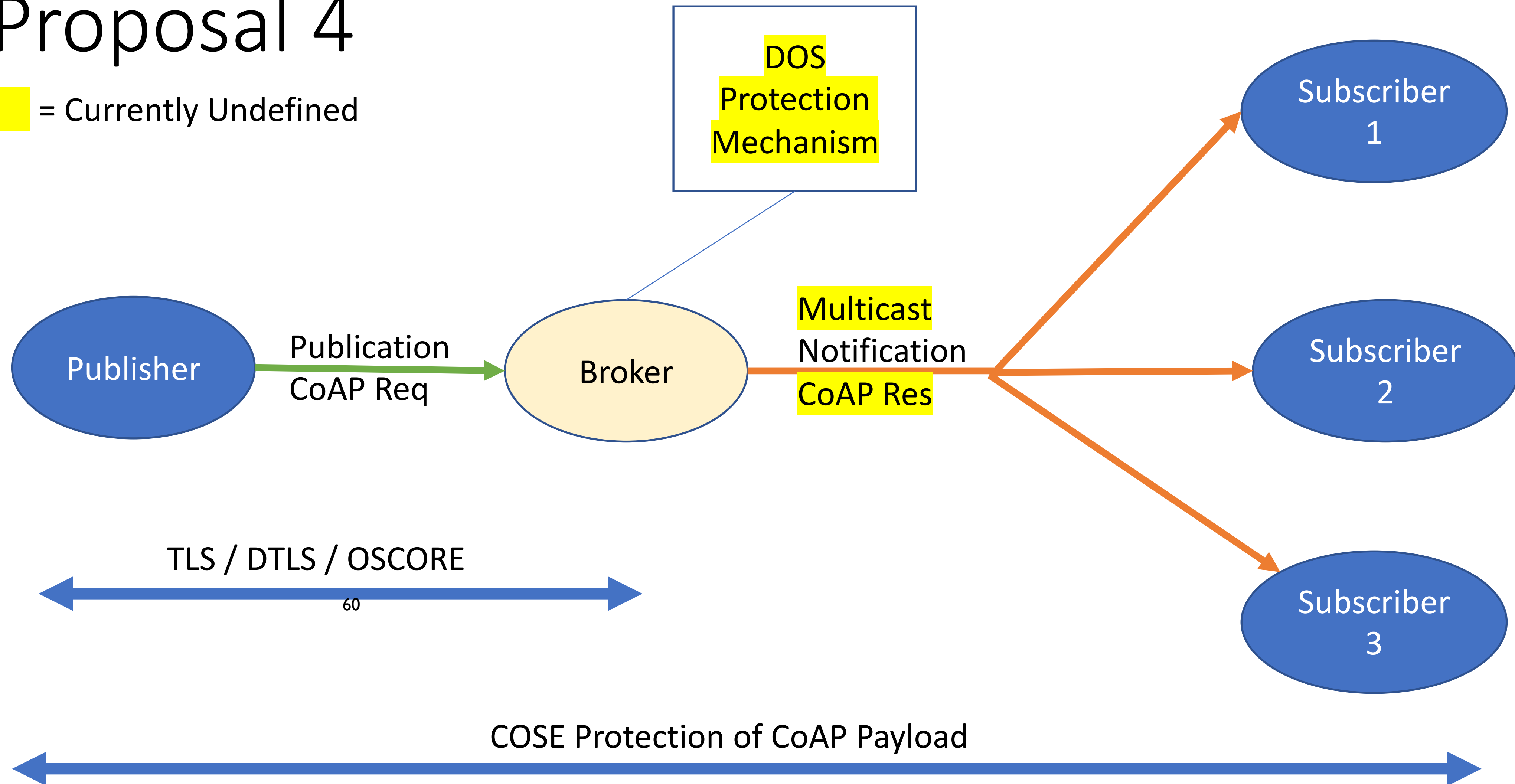
Proposal 3

= Currently Undefined



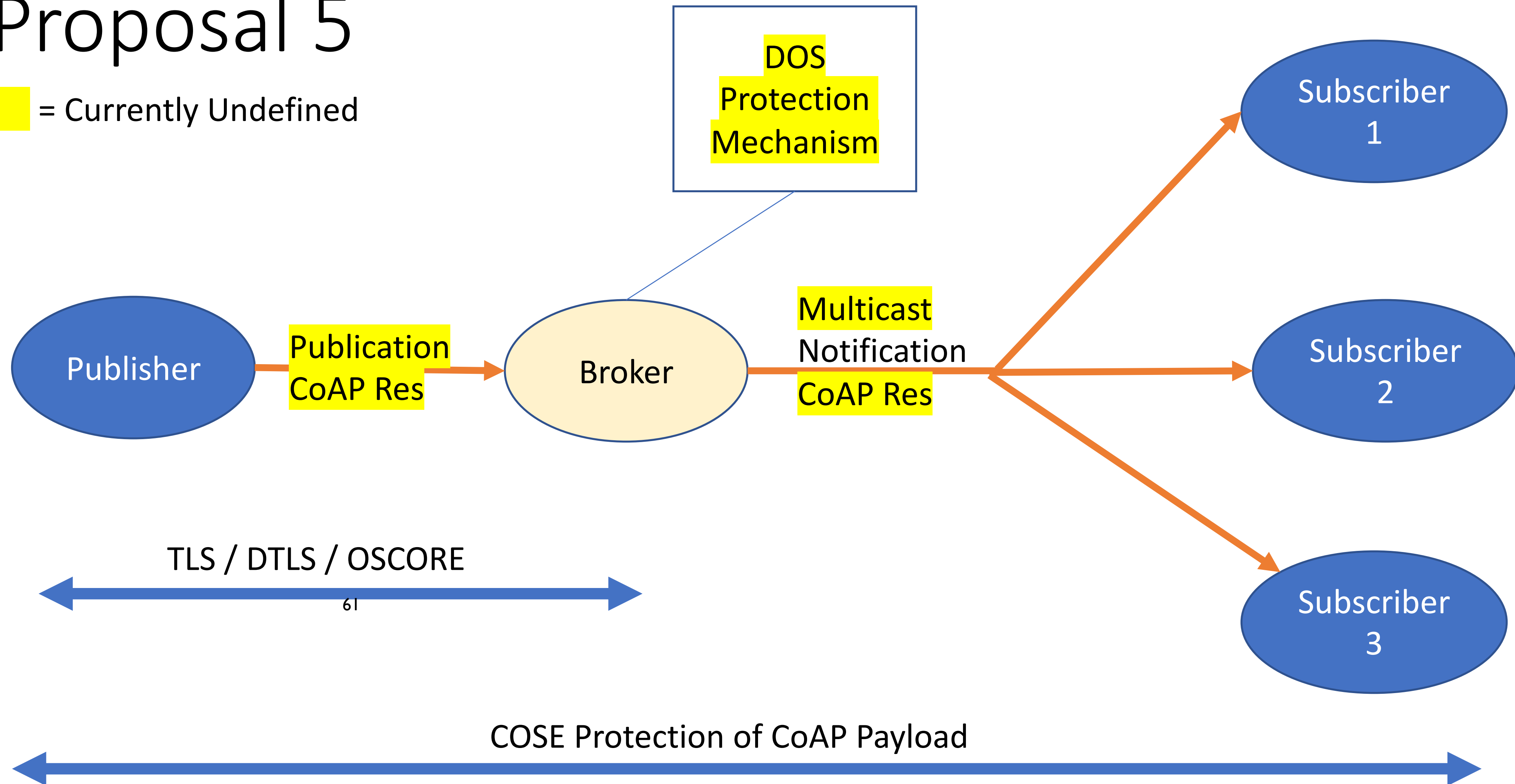
Proposal 4

= 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 }
```

```
base64(      82      # array(2)
              63      # text(3)
              666F6F # "foo"
              18 2A  # unsigned(42)
            )
```

CBOR CoAP
Content Format

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)"

Additional Units for SenML

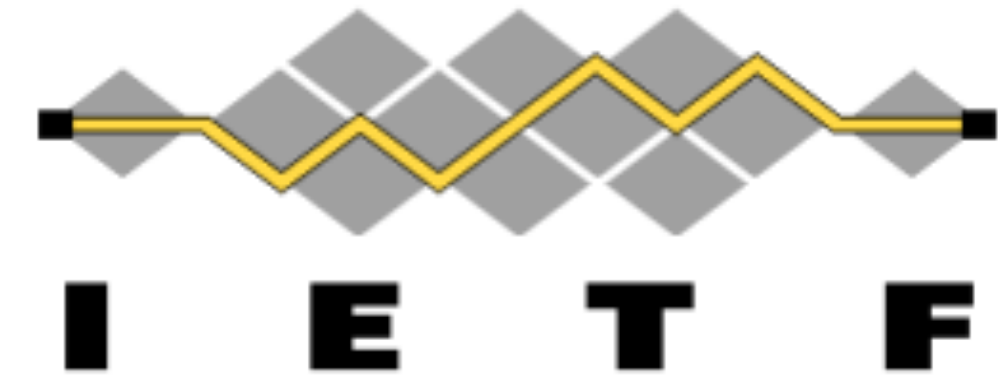
Units for SenML and OMA SpecWorks IPSO/LwM2M models

- All LwM2M/IPSO resources have (optional) unit attribute
 - Some objects have Unit resource
 - Currently no registry for units
- SenML units registry seems like a good fit
 - Already using SenML JSON/CBOR for serialization of objects
 - Just need to add a few new units: draft-bormann-senml-more-units
 - Byte (B), volt-ampere (VA), VA reactive (var), joule per meter (J/m)
 - Degrees (deg) for "compass direction"
- Supports well all other use of SenML

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**



CoRECONF update

Andy Bierman
Michel Veillette
Peter van der Stok
Alexander Pelov
Ivaylo Petrov

CoMI Current status



- Seems rather stable
- Have had interoperable implementations on previous version
- No changes since last IETF

CoMI next steps

- Consider reading again
- WGLC?



YANG-CBOR status

- Rather stable
- Last minute discussions:
 - Discussions over multiple enums inside unions
 - Discussions over yang annotations support



YANG-CBOR next steps

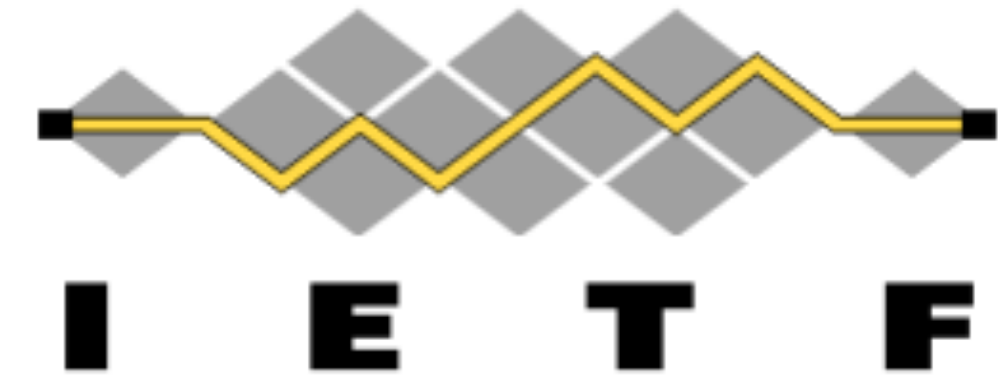
- Resolve those issue
- Issue WGLC



SID draft status



- Very useful discussions with Peter VDS
 - SID pre-allocation
 - Publicly available vs RFC Publication
- Changes between v04 and v05
 - Editorial changes on sid lifecycle
 - Clarifying unclear parts in IANA considerations



SID changes in future v06

- Major editorial changes (moving things around)
 - Lots of input from IANA -> **Simplify**, simplify, simplify
- Moving things into appendix
 - Non-normative -> non-normative
 - SID automatic generation from tools from sec 1.. non-normative
 - SID file lifecycle (most of sec 3) -> very 3rd party registry related, lots of prose.. Non-normative
- Removed Section 5 - 3 lines to say 3rd party registries are out of scope
- 0..999 and 100 000..1000 000 SIDs - RFU



SID changes in future v06

- Move sid type definition from comi yang file to ietf-sid-file.yang
- SID files are added to Yang Name Registry and sec 7.3 is deleted
 - Much simpler
 - The two are very inter-connected
- Section titles are being updated
 - Module registration -> SID File Format Module Registration
 - "SID Mega-Range" registry -> Create new IANA Registry: "SID- Mega-Range" registry
 - "IANA SID Mega-Range" -> Create a new IANA Registry: IETF SID Mega-Range Registry (managed by IANA)
- Registry sections are split into structure, policy and initial values sections
- Other smaller clarifications

SID next steps

- Publish v06 by end of the week with all the input from IANA
- Issue WGLC



Questions and answers



Thank you!

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**

draft-bormann-core- media-content-type-format

- **What is a**
 - **Media type**
 - **Content type**
 - **Content format**

OID

84

Signed assertions are expressed as X.509 certificates

NEW

Authenticated assertions are expressed as
CWTs (RFC 8392) protected by COSE (RFC 8152)

COIDS

CoIDs (Concise IDs): Profile CWT/COSE to take over from X.509, fill in any gaps left: [draft-birkholz-core-coid-01](#)

86

— (Contributions by Henk Birkholz, Carsten Bormann, Max Pritikin, Robert Moskowitz)

Related Work, outside scope of CoIDs

Re-encoding X.509 certificates in CBOR ([draft-raza-ace-cbor-certificates-01](#))

- More streamlined encoding
- Signature is still on equivalent ASN.1 DER byte string

Inherits semantic baggage and uncertainties of X.509

87

Not applicable to constrained environments that directly want to validate CWTs

Profiling CWT for authenticated assertions

- Do it in ACE:
Owner of CWTs and CWT Proof of Possession
- Do it in CoRE:
Has requirements for concise authenticated assertions
- Do in other existing WG: ???
- Create a new WG
- Don't do this at all, X.509 rules (but then at least needs to be compressed)

88

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)



I E T F

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**

draft-jarvinen-core-fasor “IPR”

- For draft-jarvinen-core-fasor, patent claims were laid out in <https://datatracker.ietf.org/ipr/3227/>
- At IETF103, we said that the information given might not be sufficient to make a WG decision on its impact
- The statement has since been updated: <https://datatracker.ietf.org/ipr/3346/>
 - Not asserted for “essential” part of IETF *standard*
 - But under reciprocity (“defensive patent”)
 - (FRAND available, too)
- Do we now have sufficient information, to discuss, e.g., working group adoption?

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**

draft-ietf-core-dynlink

IETF 104

Recent Activity

- Core-dynlink was discussed during a joint IETF-OMA conf call at the end of Feb
 - Reorganized the draft to introduce Conditional Notification Attributes at the beginning
 - Made pmin and pmax type xsd:decimal to accommodate fractional second timing
 - Updated the attribute descriptions. It and gt notify on all crossings, both directions
- Updated Binding Table description, removed interface description but introduced core.bnd rt attribute value

Binding Table in -07

```
Req: POST /bnd/ (Content-Format: application/link-format)
<coap://sensor.example.com/s/light>;
  rel="boundto";anchor="/a/light";bind="obs";pmin="10";pmax="60"
Res: 2.04 Changed
```

```
Req: GET /bnd/
Res: 2.05 Content (application/link-format)
<coap://sensor.example.com/s/light>;
  rel="boundto";anchor="/a/light";bind="obs";pmin="10";pmax="60"
```

```
Req: DELETE /bnd/a/light
Res: 2.04 Changed
```

```
Req: DELETE /bnd/
Res: 2.04 Changed
```

Binding Table in -08

```
Req: GET /.well-known/core?rt=core.bnd (application/link-format)
Res: 2.05 Content (application/link-format)
</bnd/>;rt=core.bnd;ct=40
```

```
Req: GET /bnd/
Res: 2.05 Content (application/link-format)
<coap://sensor.example.com/a/switch1/>;
    rel=boundto;bind=obs;anchor=/a/fan,;bind="obs",
<coap://sensor.example.com/a/switch2/>;
    rel=boundto;bind=obs;anchor=/a/light;bind="obs"
```

```
Req: PUT /bnd/ (Content-Format: application/link-format)
<coap://sensor.example.com/s/light>;
    rel="boundto";anchor="/a/light";bind="obs";pmin="10";pmax="60"
Res: 2.04 Changed
```

```
Req: GET /bnd/
Res: 2.05 Content (application/link-format)
<coap://sensor.example.com/s/light>;
    rel="boundto";anchor="/a/light";bind="obs";pmin="10";pmax="60"
```

Next

- Conditional notifications are completed
 - Use of pmin, pmax and band clarified
- Work on Link bindings completed
- Binding table needs support for partial changes

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**

- **Slides following...**
- **Objectives include:**
 - **Do we want to adopt (part of) the CoRAL work?**
 - **CIRI**
 - **CoRAL**
 - **Not CoRAL-Reef?**

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**

Speedy CoAP Blockwise Transfer

draft-zcao-core-speedy-blocktran-00

Presented by Zhen Cao
Joint work of Baicheng, Jinke

IETF 104 CORE , March 2019

The State of The Art

- The Client needs to continuously send requests to the Server, using the BLOCK options to specify the exact segment that is expected each time;
- Such a design was a reasonable choice since the server can be implemented to be truly stateless and lightweight.
- There are some scenarios that need to speeding up :
 - Firmware update;
 - To conduct a critical mission conversation;
 - More capable servers;

104

Example Conversation using the Speedy-up Block Transfer

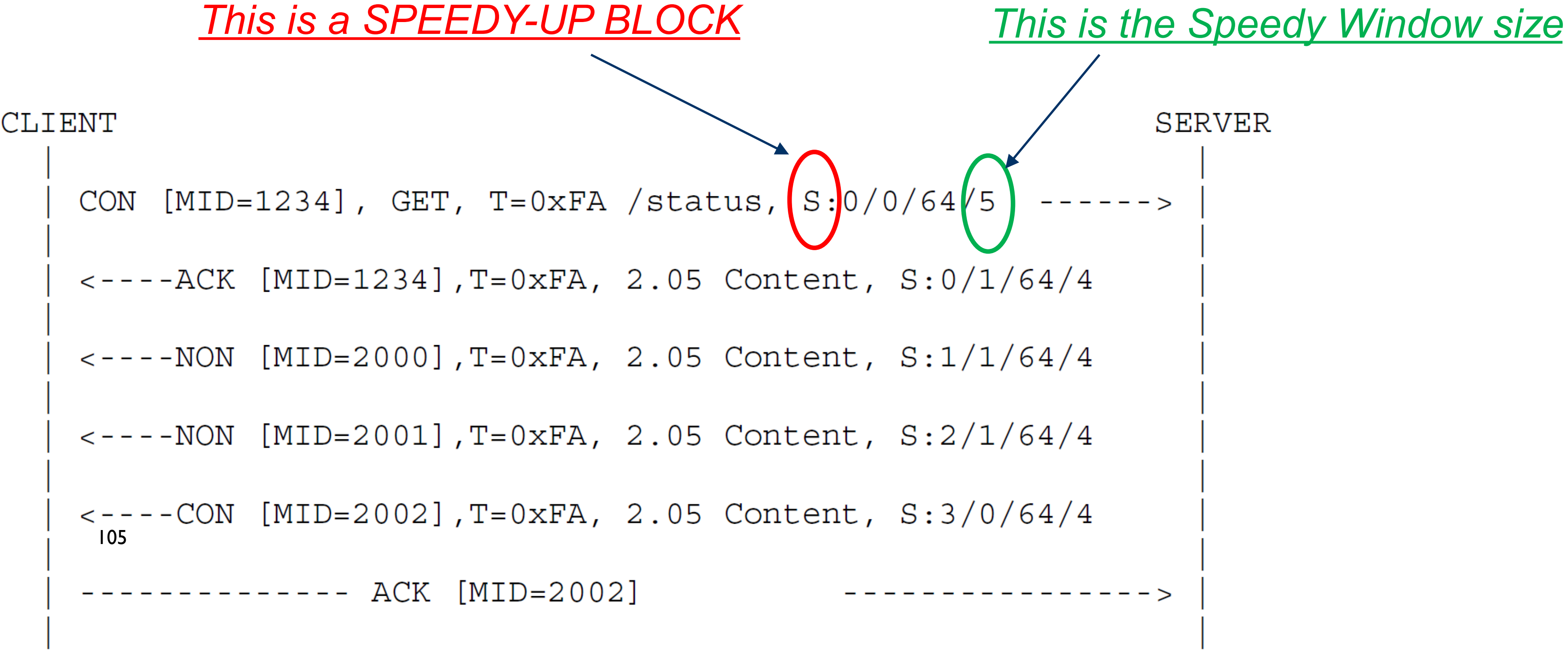


Figure 2: Speedy Blockwise GET with Early Negotiation

Another example conversation

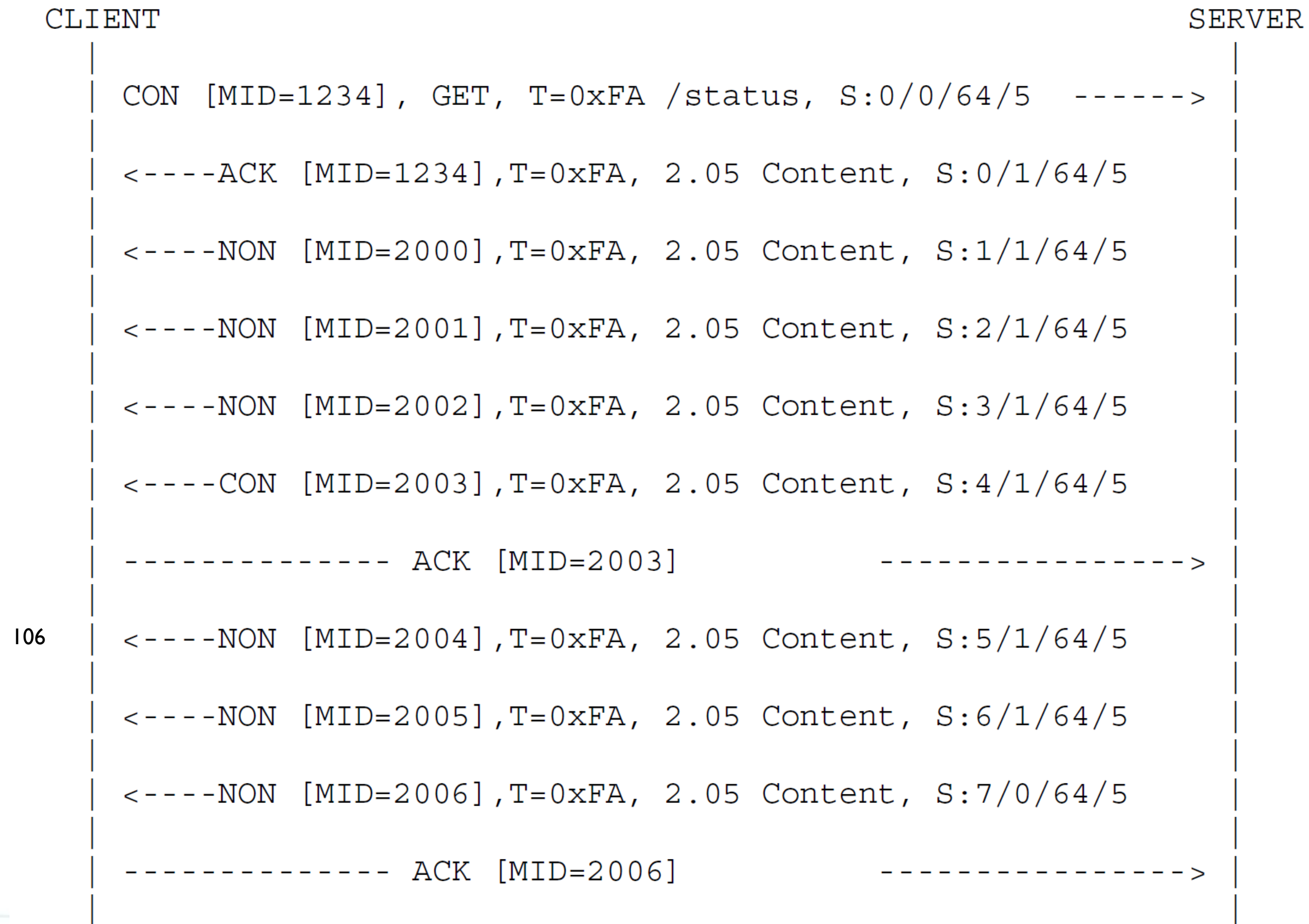


Figure 3: Speedy Blockwise GET with Early Negotiation

The Speedy Block Option

No.	C	U	N	R	Name	Format	Length	Default
TBD	C	U	-	-	BlockS	uint	0-4	(none)

Figure 1: The Speedy Block Option

107

There are some other considerations for Retransmission and etc.

Next Steps

This is a small fix ;

Any interests in this WG?