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 <u>try to be nice to each other</u>**
- **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)

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

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
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)

18

- 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

19

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

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?

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*

26

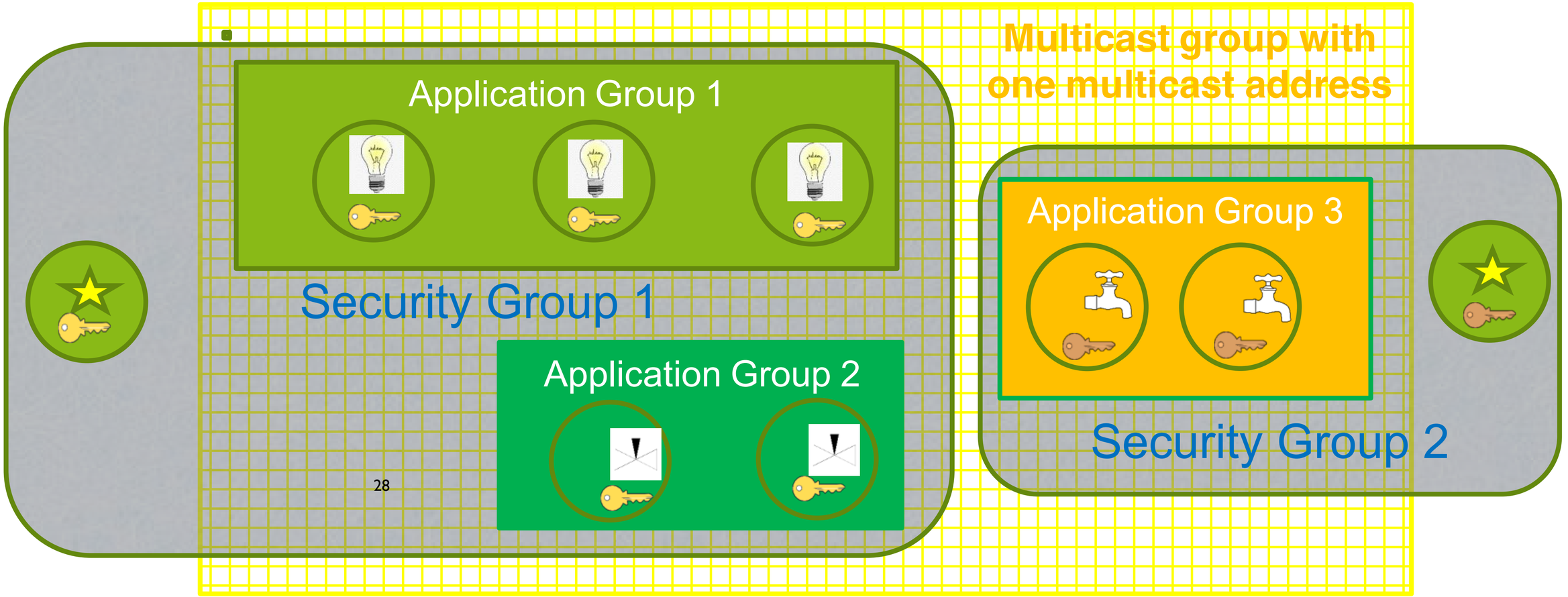
- Use resource lookup, to retrieve especially:
  - A pointer to the join resource at the GM
  - The identifier of the OSCORE group

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

35

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[39]
  - 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

43

Thank you!

Comments/questions?

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

Pub Sub and Multicast

Summary of the CoRE Hallway Discussion @ IETF104 Hackathon

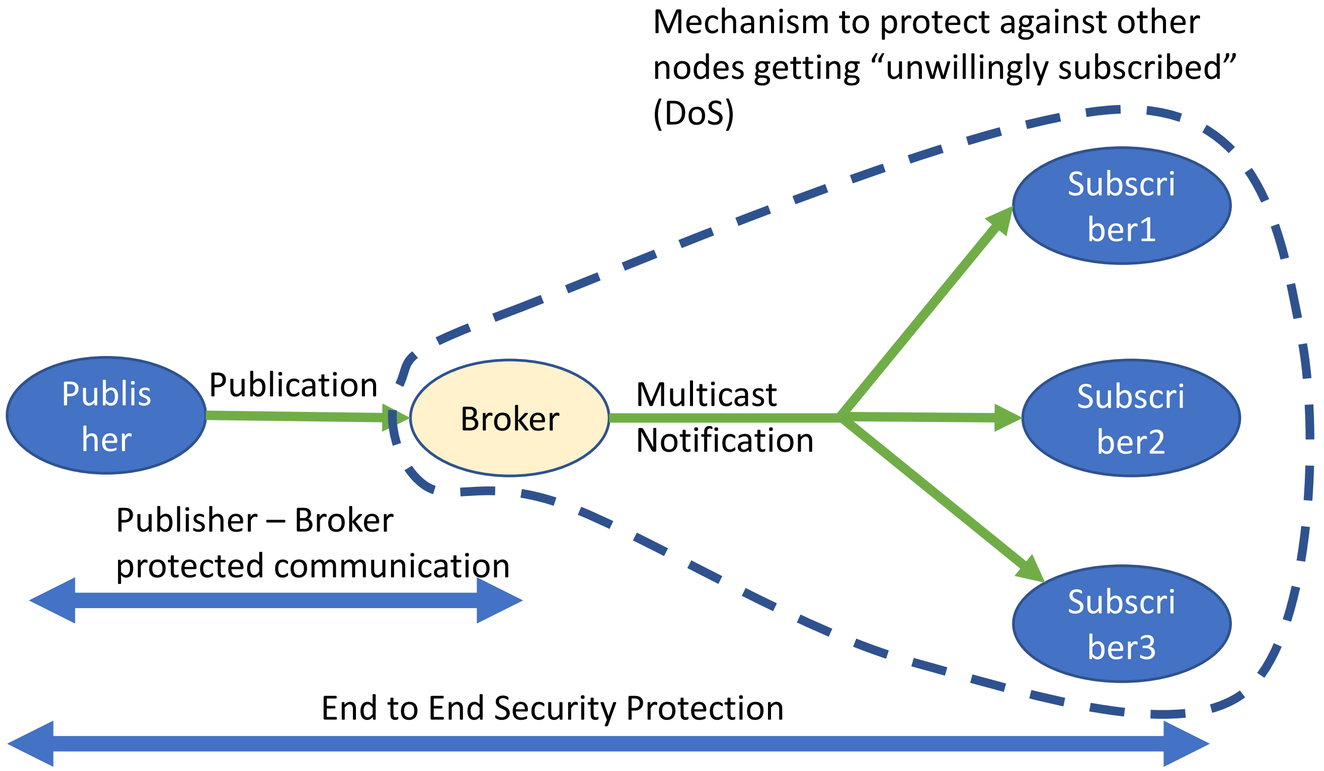
45

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 protection
  - DoS protection



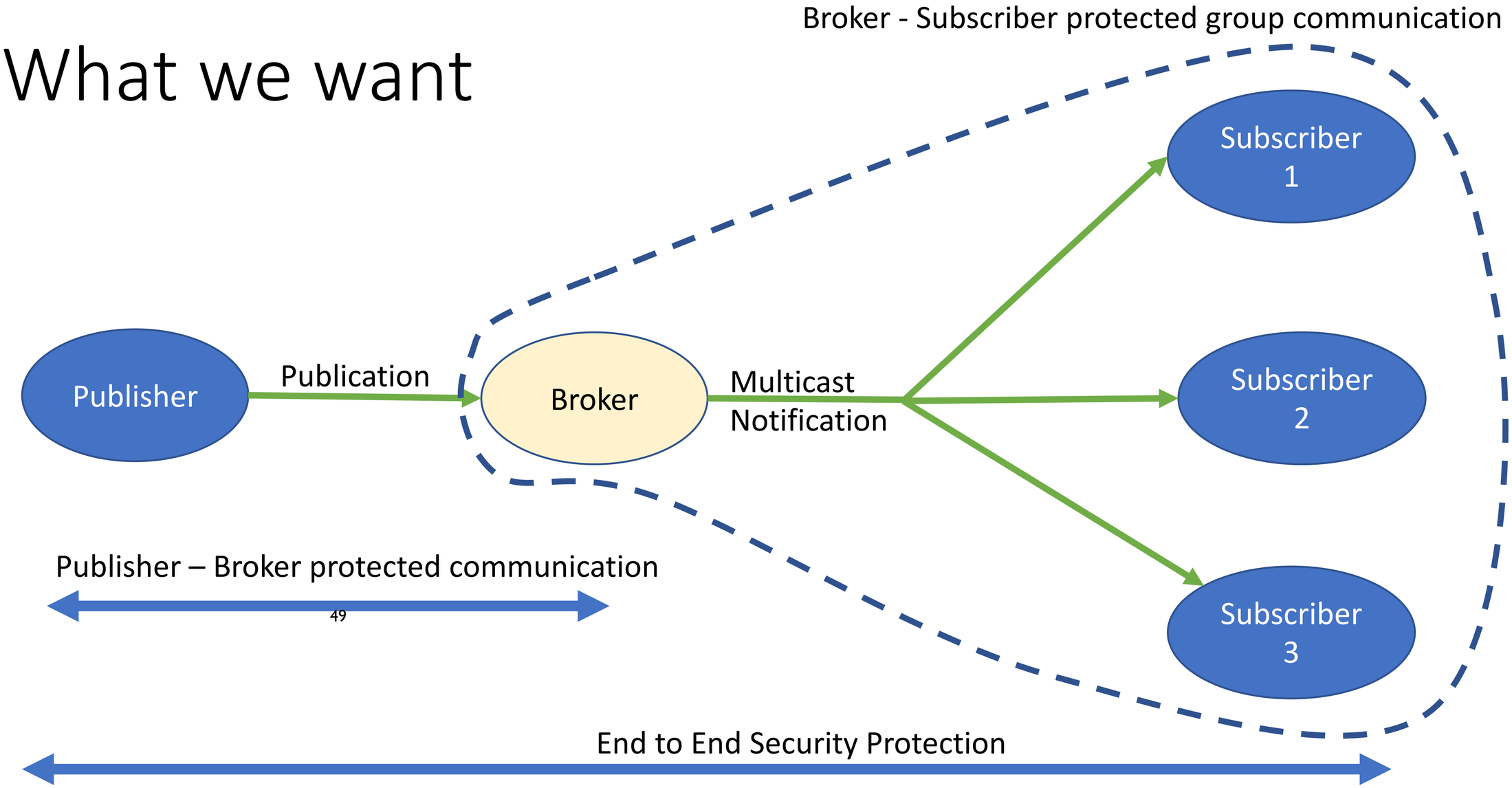
The challenges

- 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

48

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

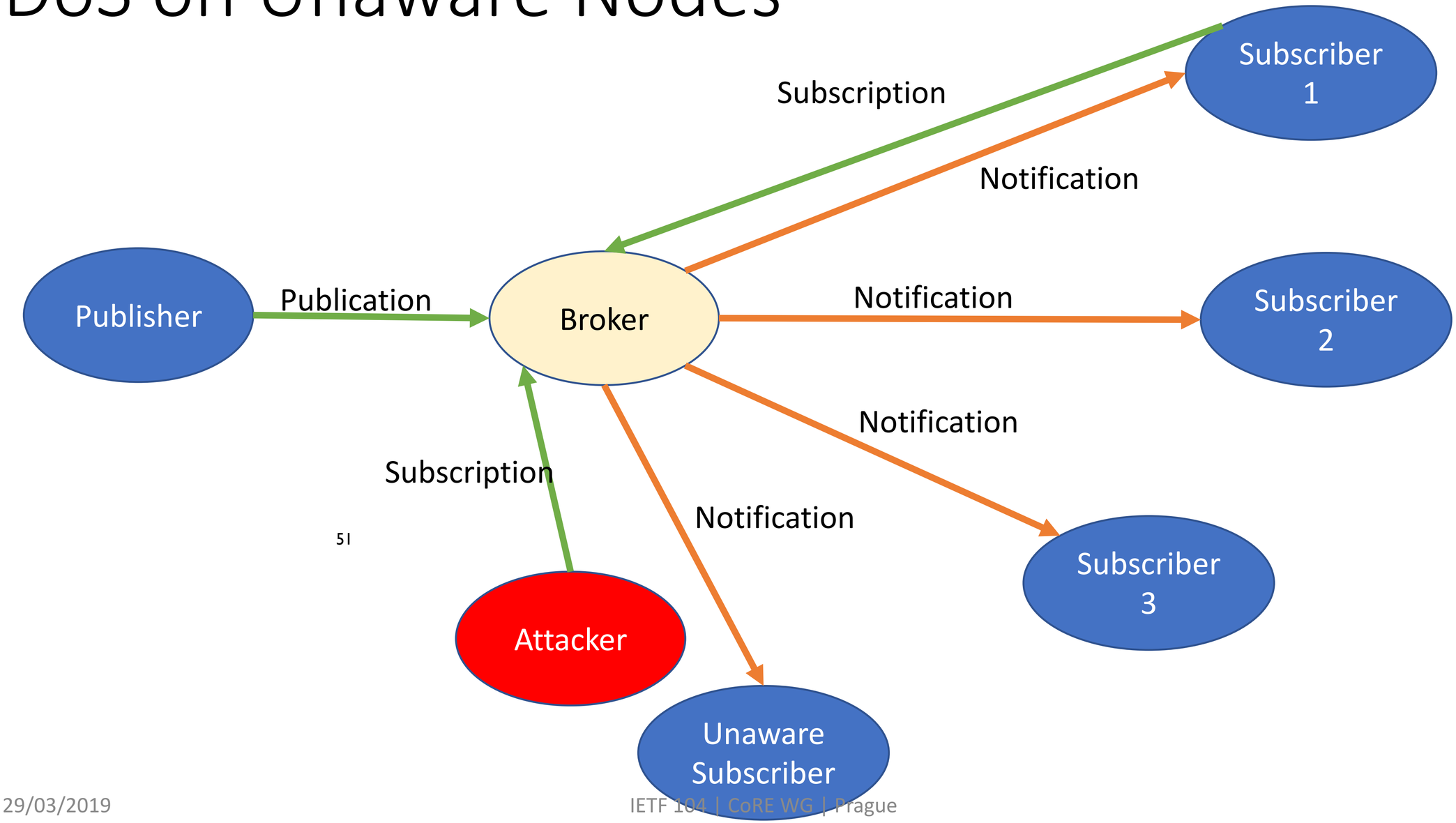
- The Publisher communicates securely with the Broker and must be authorized to publish on the Broker
- The publication is protected (protection of CoAP payload)
- The Subscribers must be authorized to decrypt and verify the publication

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

50

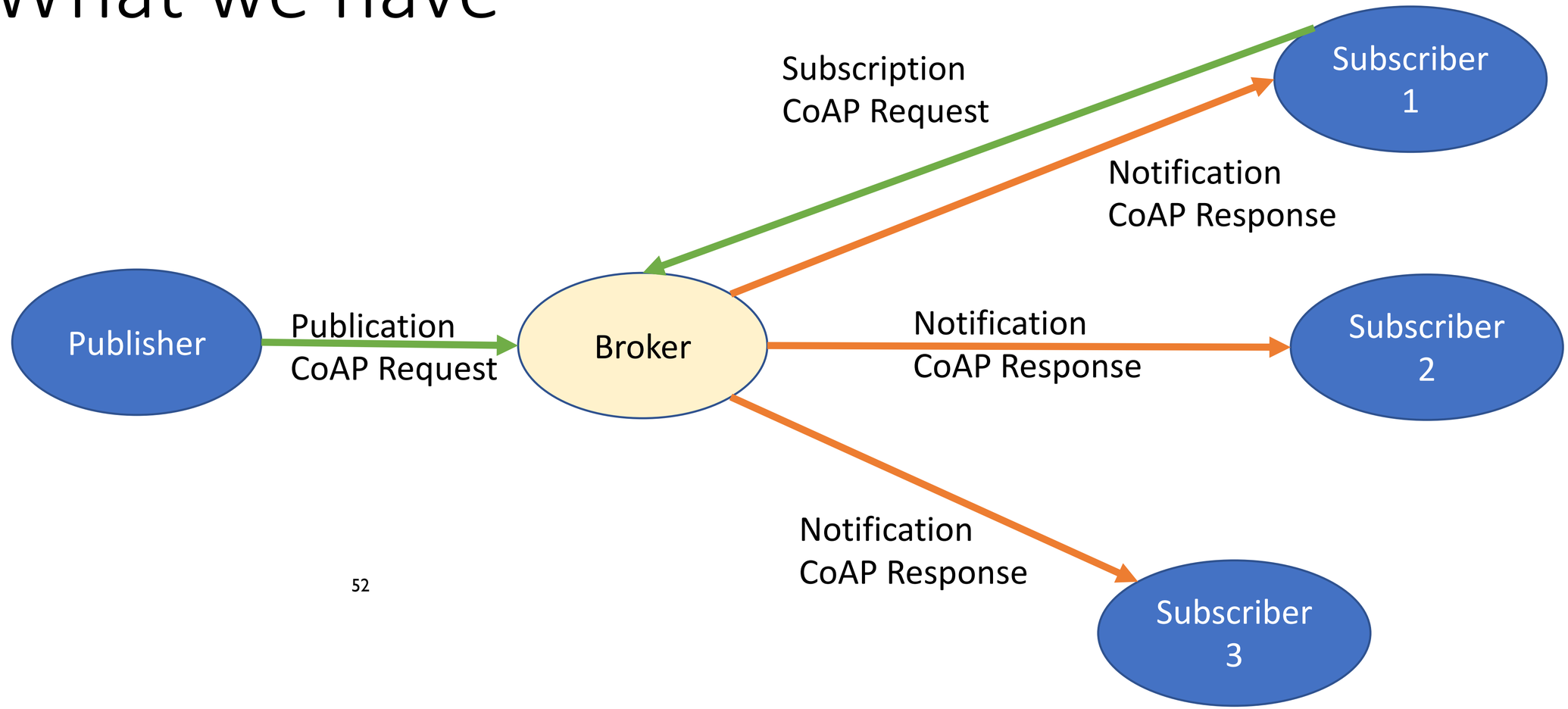
- Additionally, the Subscriber must prove address ownership of a subscription request, otherwise an attacker could DoS external nodes that do not want to receive the publications

DoS on Unaware Nodes



51

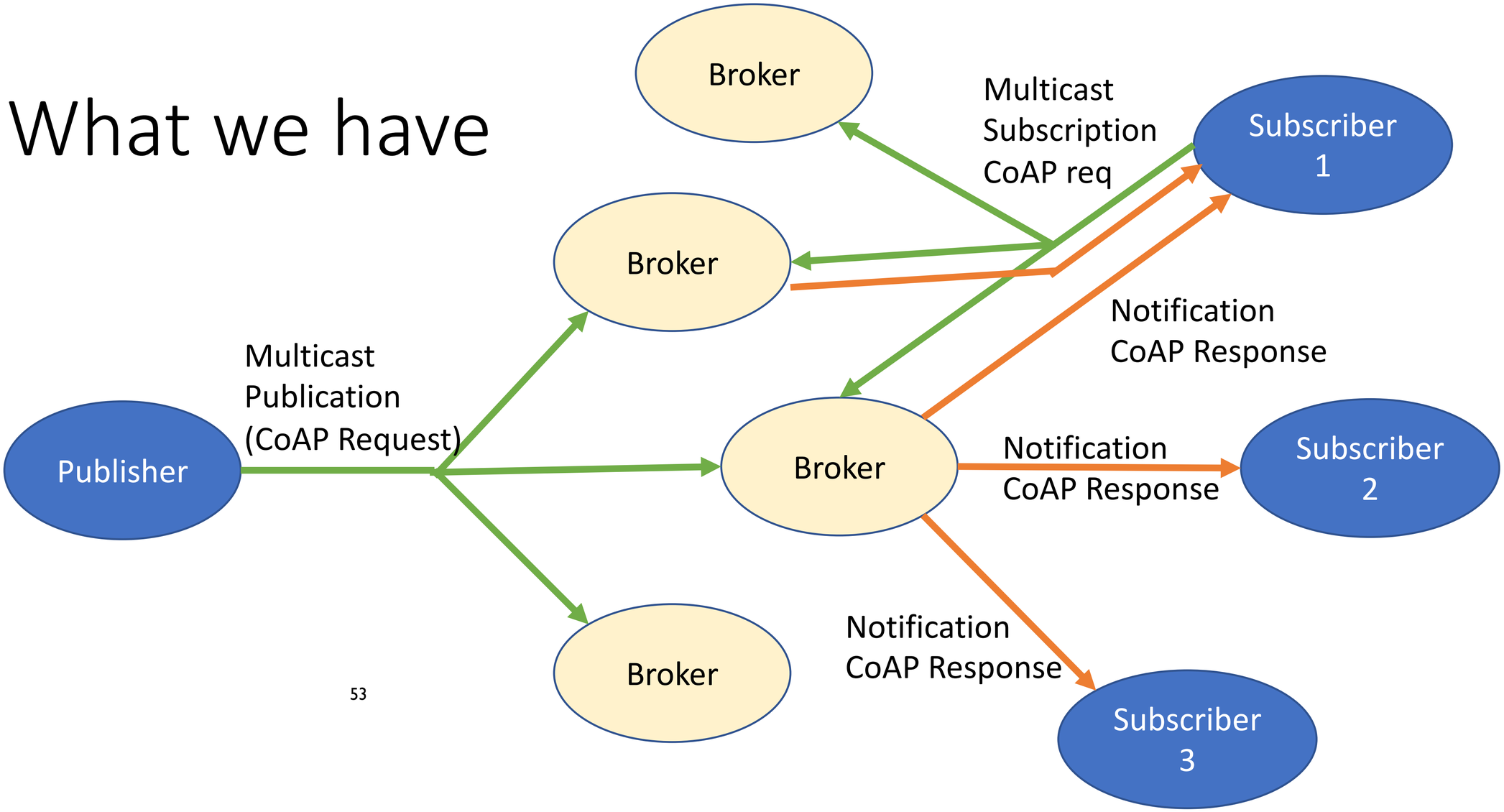
What we have



52

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

What we have



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

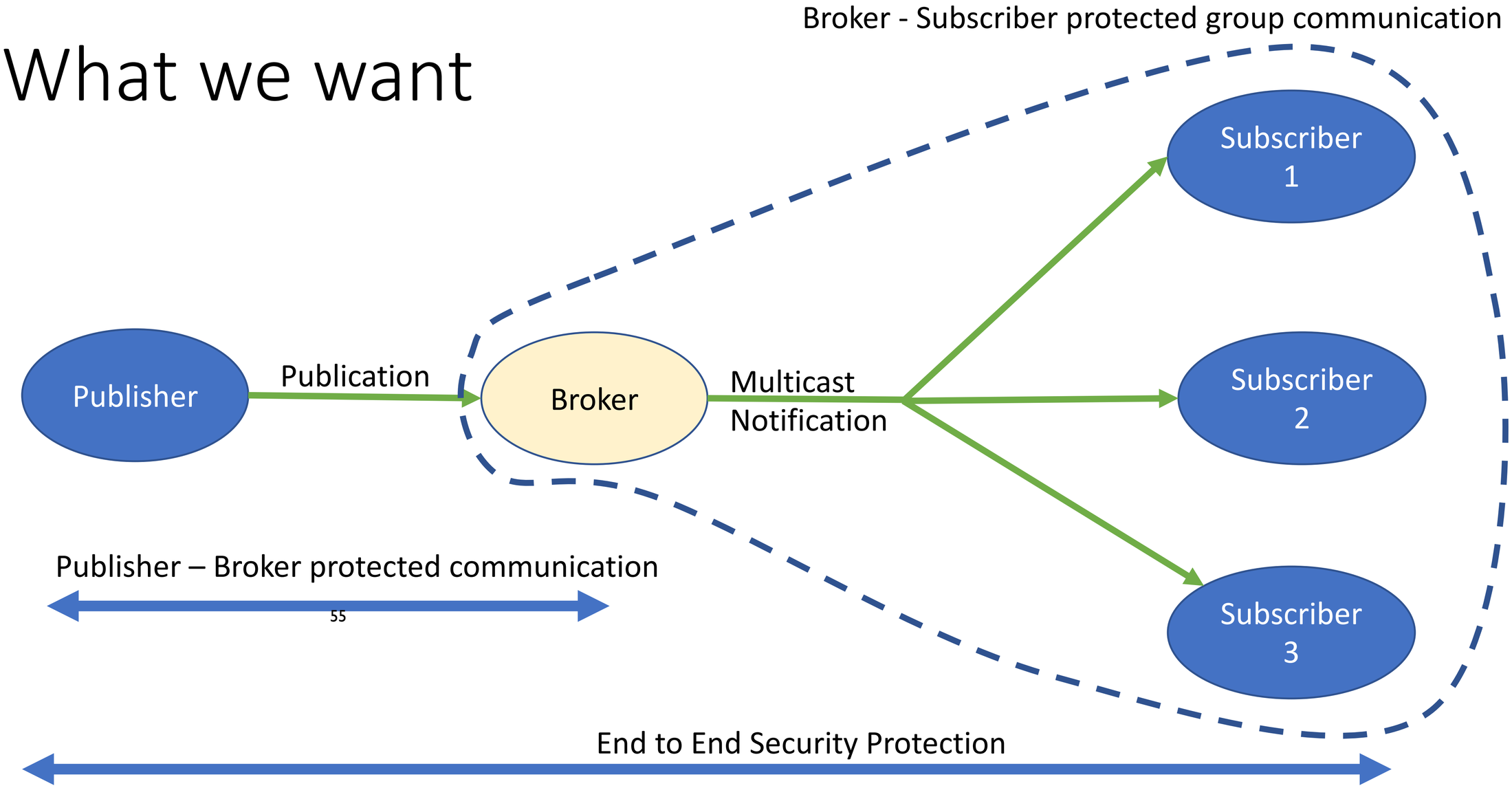
2 Goals

- Performance Goal: Multicasting notifications

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

54

What we want


Broker - Subscriber protected group communication
Publisher
Publication
Broker
Multicast
Notification
Subscriber
1
Subscriber
2
Subscriber
3
Publisher – Broker protected communication
55
End to End Security Protection

How do we get it

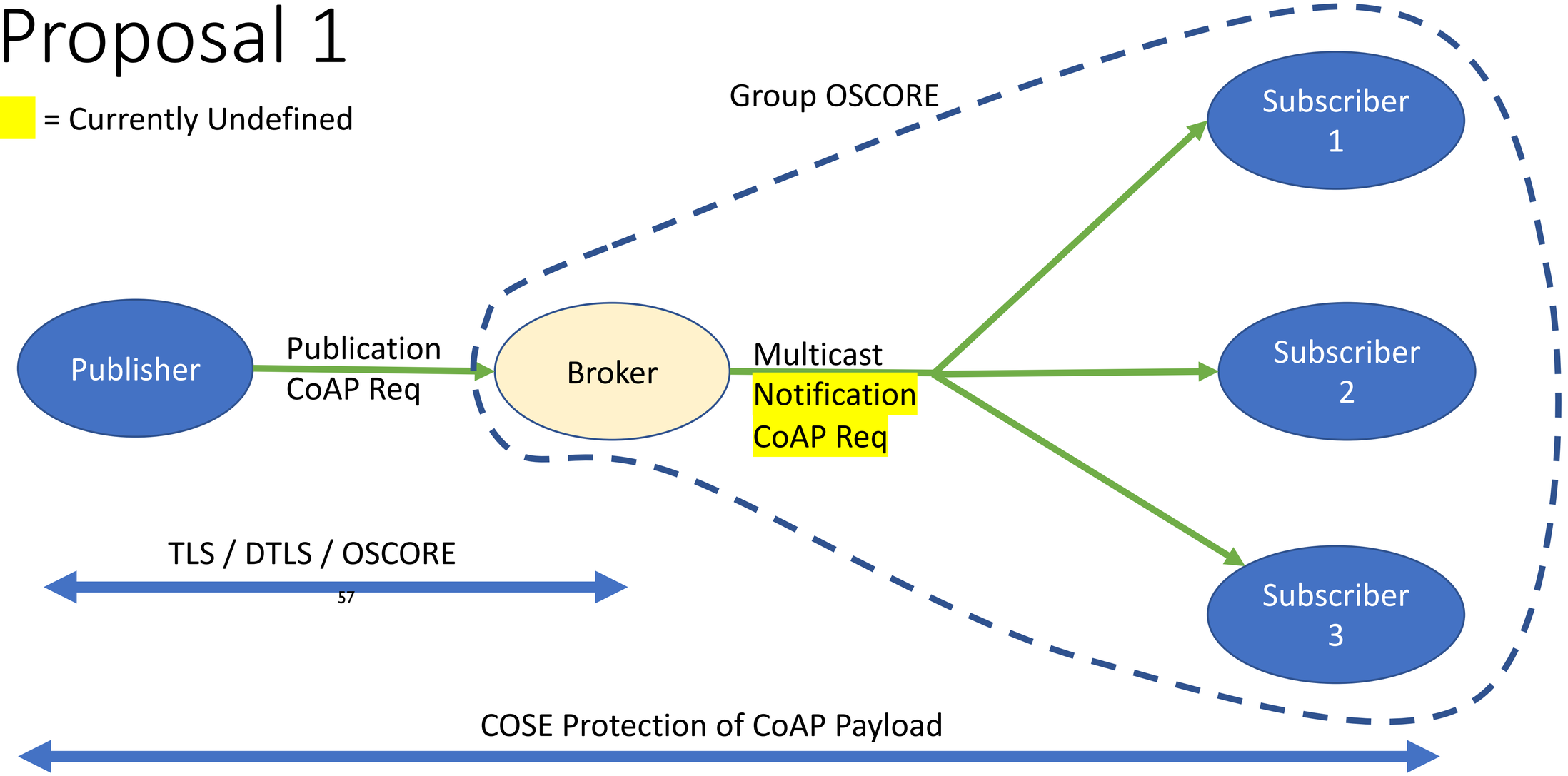
- Notifications as CoAP requests + Multicast the notification +
  1. Group OSCORE (Broker – Subscribers) + Payload protection (Pub – Subscribers)
  2. Group OSCORE (Pub – Subscribers) + additional DoS protection mechanism
  3. Payload protection (Pub – Subscribers) + additional DoS protection mechanism

4. Define multicast responses (how do we deal with the token?) + use multicast notifications to Subscribers + ?? (No secure multicast defined for multicast responses)[56]

- Anything else?

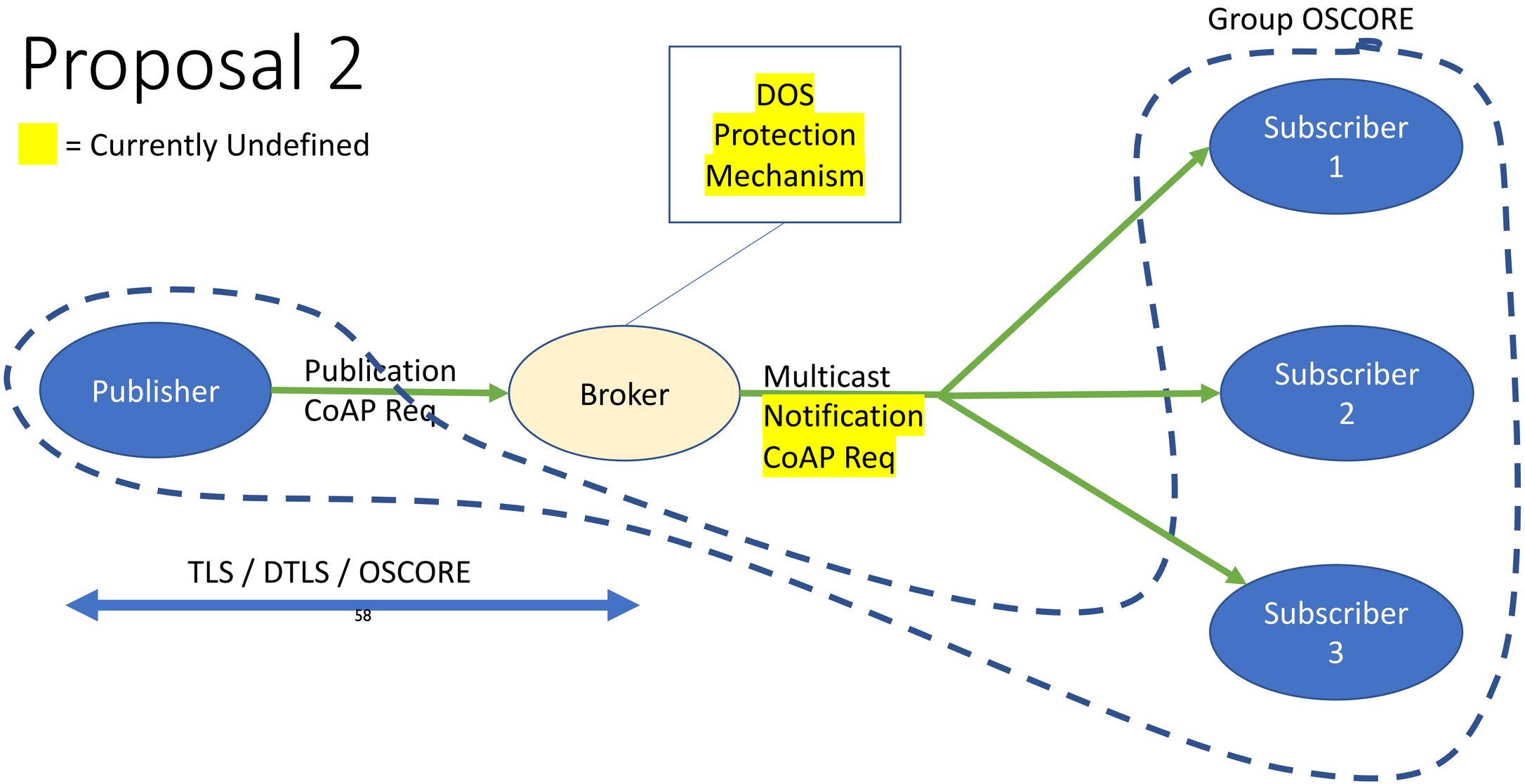
Proposal 1

= Currently Undefined



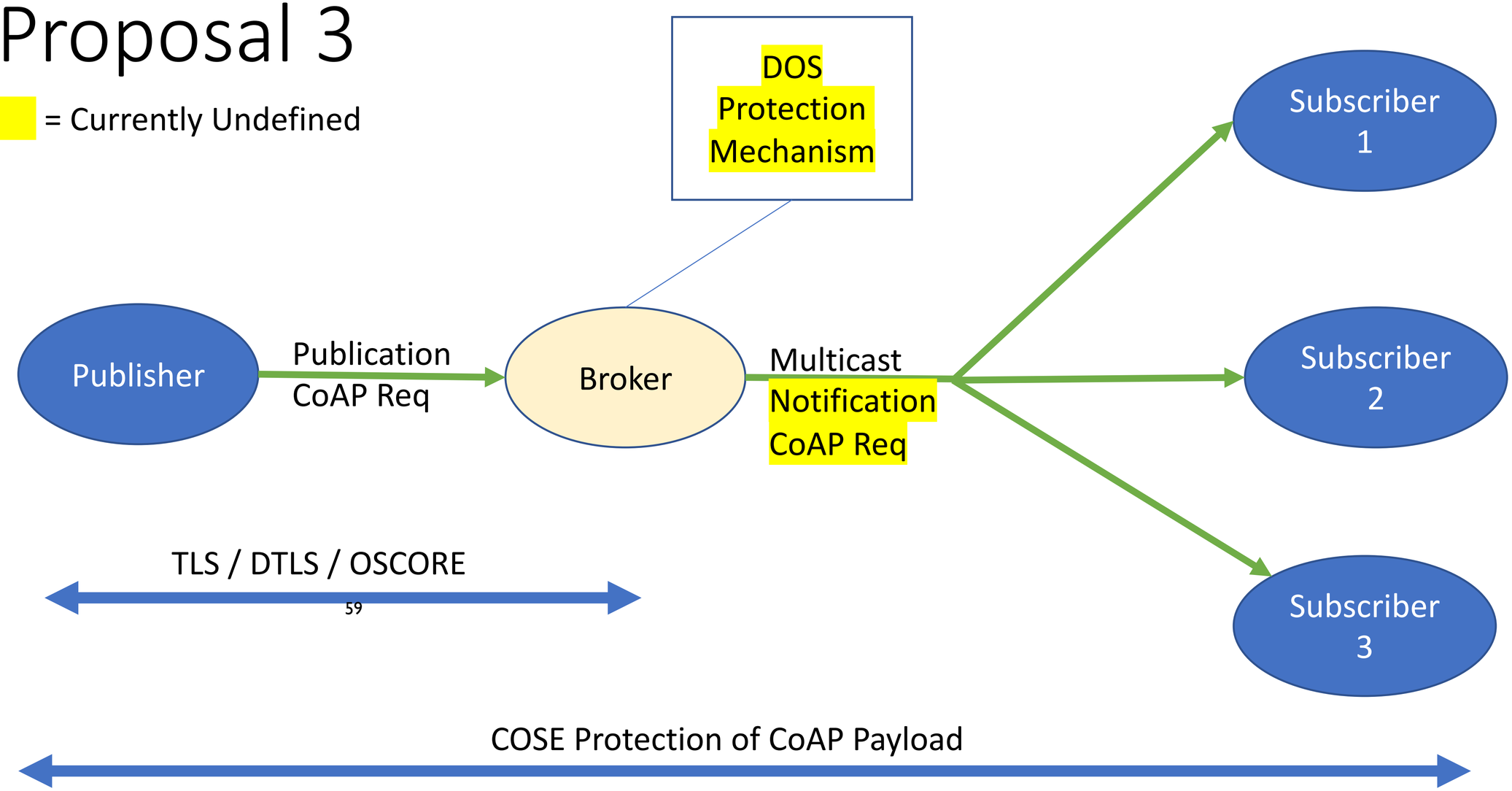
Proposal 2

= Currently Undefined



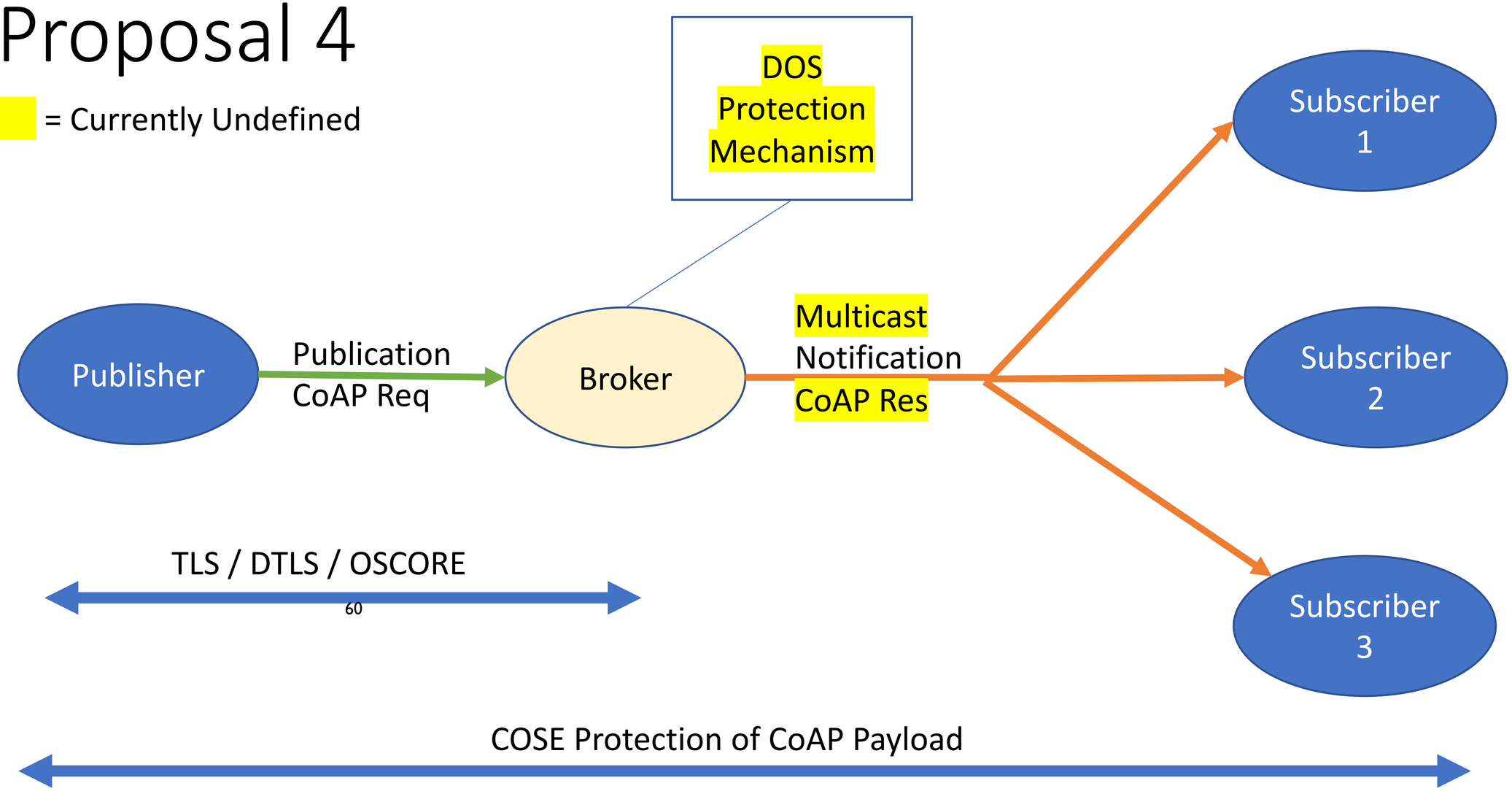
Proposal 3

= Currently Undefined



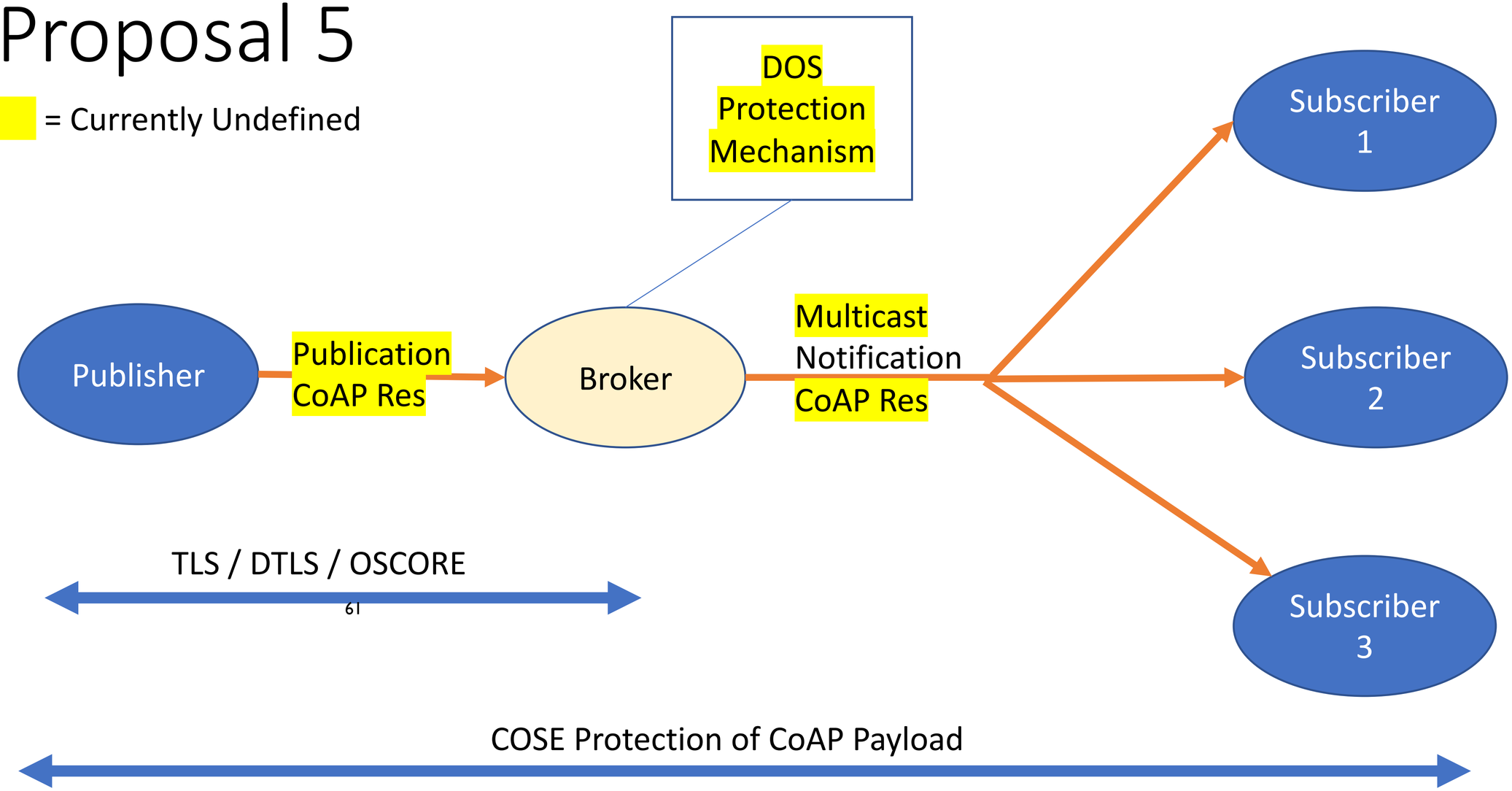
Proposal 4

= 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)"

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

Old

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[88] at all, X.509 rules (but then at least needs to be compressed)

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**

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?

New proposed WG dedicated to EDHOC

- EDHOC [1] is a lightweight [2] security handshake for OSCORE
- SECDISPATCH WG held a virtual interim [3] on EDHOC
- Security ADs yesterday proposed to charter a
  “narrowly scoped, short-lived WG . . . with EDHOC as a starting point” [4]
- If you want this to happen

→ Join Secdispatch WG mailing list now and support this proposal

[1] https://tools.ietf.org/html/draft-selander-ace-cose-ecdhe
[2] https://tools.ietf.org/html/draft-ietf-lwig-security-protocol-comparison
[3] https://mailarchive.ietf.org/arch/msg/secdispatch/9AfqrecZfFMlMGxSXOo4ENZtrVk
[4] https://mailarchive.ietf.org/arch/msg/secdispatch/Kz_6y6Jq4HsWxglsUHafWjXIm0c

Github use on CoRE

Jaime Jiménez

Current Github approaches

- Relationship to existing/future attestation standards
  #12 opened 4 days ago by dthaler
- What should tee "ver" field contain?
  #11 opened 4 days ago by dthaler
- What should tee "name" field contain?
  #10 opened 4 days ago by dthaler
- in dsi.tee, why are cert and cacert separate fields?
  #9 opened 4 days ago by dthaler
- In dsi.sdlist, why is cnt needed?
  #8 opened 4 days ago by dthaler
- Add additional APIs needed by transport
  #7 opened 23 days ago by dthaler
- Specify application/json+otrp as media type
  #6 opened 23 days ago by dthaler
- need appendix of test vectors
  #5 opened on Jan 25 by dthaler
- Clarify how use of "optional to support" algorithms is decided
  #4 opened on Nov 8, 2018 by dthaler
- Clarify uniqueness scope requirement of rid/tid
  #3 opened on Nov 8, 2018 by dthaler
- requestedtalist needs to be added to GetDeviceStateResponse
  #2 opened on Nov 8, 2018 by dthaler
- Unclear what fields are mandatory vs optional
  #1 opened on Nov 8, 2018 by dthaler

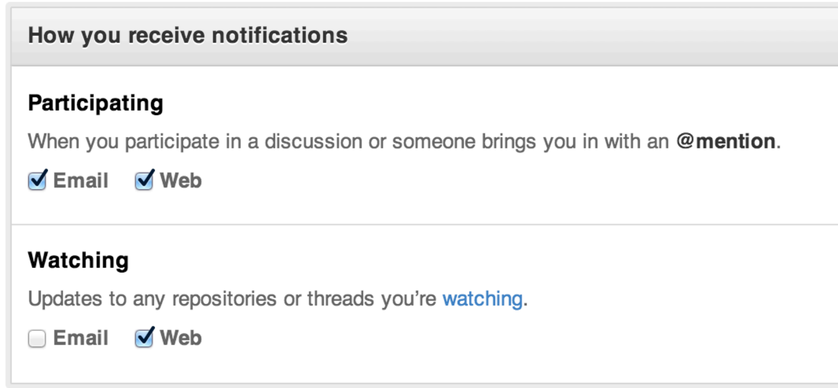
- Enhance simple-registration readability patch available
  #199 by chrysn was closed 23 days ago
- Say something about how limited devices can be expect reporter OK patch available
  #197 by chrysn was closed 22 days ago
- Express registration update parameters as delta to registration parameters
  #196 by chrysn was closed 27 days ago
- One more shifting of heading levels patch available
  #195 by chrysn was closed 22 days ago
- M2M vs IoT patch available
  #194 by chrysn was closed 17 days ago
- Editorial issues from Jaime's comments patch available
  #193 by chrysn was closed 23 days ago
- "NAT gateway": precision patch available
  #192 by chrysn was closed 17 days ago
- Item categories for interactions editorial patch available
  #191 by cabo was closed 17 days ago
- Define structure of an endpoint name patch available
  #190 by cabo was closed 17 days ago
- idnits before –19
  #189 by cabo was closed on Jan 10
- In simple registration, the query of /.well-known/core should be allowed inline
  #186 by jimsch was closed on Dec 17, 2018
- Multiple endpoint types?
  #185 by jimsch was closed on Dec 6, 2018

- semantics: confusing title "Designing New Header Field Values" editorial semantics
  #214 opened 7 hours ago by reschke
- byte-range-set definition allows OWS but probably doesn't work in practice semantics
  #212 opened a day ago by royfielding
- Audit: ABNF exceptions
  #211 opened a day ago by mnot
- unnecessary use of 1#element for header field definitions
  #210 opened a day ago by royfielding
- Expect should be a list header discuss h1-messaging
  #203 opened 3 days ago by mnot
- Tighten language around GET and DELETE request bodies discuss semantics
  #202 opened 9 days ago by evert
- Range header field ABNF erratum semantics
  #196 opened on Feb 1 by reschke
- QUIC and https:// discuss
  #194 opened on Jan 31 by martinthomson
- Audit: single value header field error handling caching semantics
  #193 opened on Jan 21 by mnot 5 of 25
- Collected ABNF
  #192 opened on Jan 17 by mnot
- Mismatching absolute URI and Host header needs-data semantics
  #191 opened on Jan 17 by mnot 0 of 2
- Privacy considerations section: reference suggestion semantics
  #185 opened on Dec 17, 2018 by rvaneijk

TEEP → CoRE → HTTP

Experimentation with Github

- Document lives on GitHub
  - Individual Submission → WG item → RFC
- Issue Tracker for discussion
  - Email batch once every X weeks.
  - Assigning issues.
  - Milestones.
  - Tagging (**discuss**, **“topic”**, **waiting-OK**, **editorial**, **problem**, **errata**, **patch-available**…).
- Discussion on using Gitlab too (No IETF supported Gitlab atm)



Intended next steps

- Trial with an Individual submission.
- Looking for guinea pigs.

- Comments & Feedback?

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-coap-pubsub-08

IETF 104

March 29, 2019

Open issues

- Don't use a new status code
- Handling empty Topics
- Handling Topic Lifetime
- Handling Data Lifetime

Empty topic

- Created but not published to yet
- What does the broker return in a Subscribe or Read response?
- Response could wait until there is a publish by default
- A multipart content format or response to accept-all could optionally return an empty payload
- Other content formats can return empty payloads
- The publisher would be responsible for sending the null or empty payload

Topics Lifetime

- Can be set using the optional query parameter tlt on creation of the topic
- Alternatively by using a new header option on creation of the topic
- Counter begins to count down at create time
- Publishing to the Topic refreshes the counter
- Repeating the Topic create operation refreshes the counter, optionally with a new supplied tlt option
- When the counter reaches zero, the Topic is removed
- Default is topics live until removed

Data Lifetime (Topic contents)

- Max-Age defaults to 60 seconds and is only in responses
- Default pub/sub behavior would be allow the 60 seconds default Max-Age in all responses
- If we enable a data lifetime option e.g. dlt=xxx as a uri-query option in create or publish, Max-Age would return dlt in notifications and dlt-(tnow-tlastpublish) with Read and Subscribe responses
- data lifetime could also be a header option for push notifications to use in general

Lifetime of topic contents

- Normally Max-Age controls the behavior of a downstream proxy that caches responses
- Sending a Max-Age of 0 in a response doesn't allow the cache to re-use the data
- Likewise, a pub/sub client (library) can behave like a cache and handle the case of Max-Age=0 in responses properly wrt the application
- A cache that subscribes to a Broker could use Max-Age in the usual way, substituting notifications for reads as long as they occur before the Max-Age timeout

Proposed profile (1)

- If a Read or Subscribe is received on a Topic which has been created but data have not been Published, the Broker will not respond until data are Published
- Topic creators are responsible for publishing an empty representation as appropriate for the use case

Proposed profile (2)

- Add tlt and dlt query options on Topic creation
- Default without dlt is to respond without a Max-Age option, allowing the default 60 seconds
- If dlt is included, notifications are sent with Max-Age = dlt, Read and Subscribe responses are sent with Max-Age = dlt-(tnow-tlastpublish)

Proposed profile (3)

- If tlt is included, the topic will be removed if there is no publish activity for a time equal to the tlt value
- Outstanding subscribers and new requests are sent 4.04 responses when the topic is removed

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. lt 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

Burying core-interfaces?

- Early draft with good ideas
- Taken over and adapted by SDOs
- No literal adoption
- Some text may be useful in T2TRG documents
- Cited in the charter as an example for potential cooperation with T2TRG

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

Resource Directory

draft-ietf-core-resource-directory

Zach Shelby, Michael Koster, Carsten Bormann, Peter van der Stok,
Christian Amsüss

2019-03-29

Status

- -20 in WGLC since last Wednesday

Comments coming in

- Additions to security considerations (Klaus)
- Outdated references to other documents (Ted)

  Removing RD discovery via not-yet-spec'd DNS-SD links
- Errors and inconsistencies in examples

Interop status

- 2018-04-12 (-13): Jim's, ackl.io's, RIOT (-11), aiocoap.
  Found several small ambiguities in RD.
- 2018-10-10 (-15): RIOT, aiocoap, Jim's.
  Found IPv6 zone identifier issue.
- 2019-03-23 (-20): Jim's, aiocoap.
  No issues with specification.
  Lookup of link-format registered resources as CoRAL.

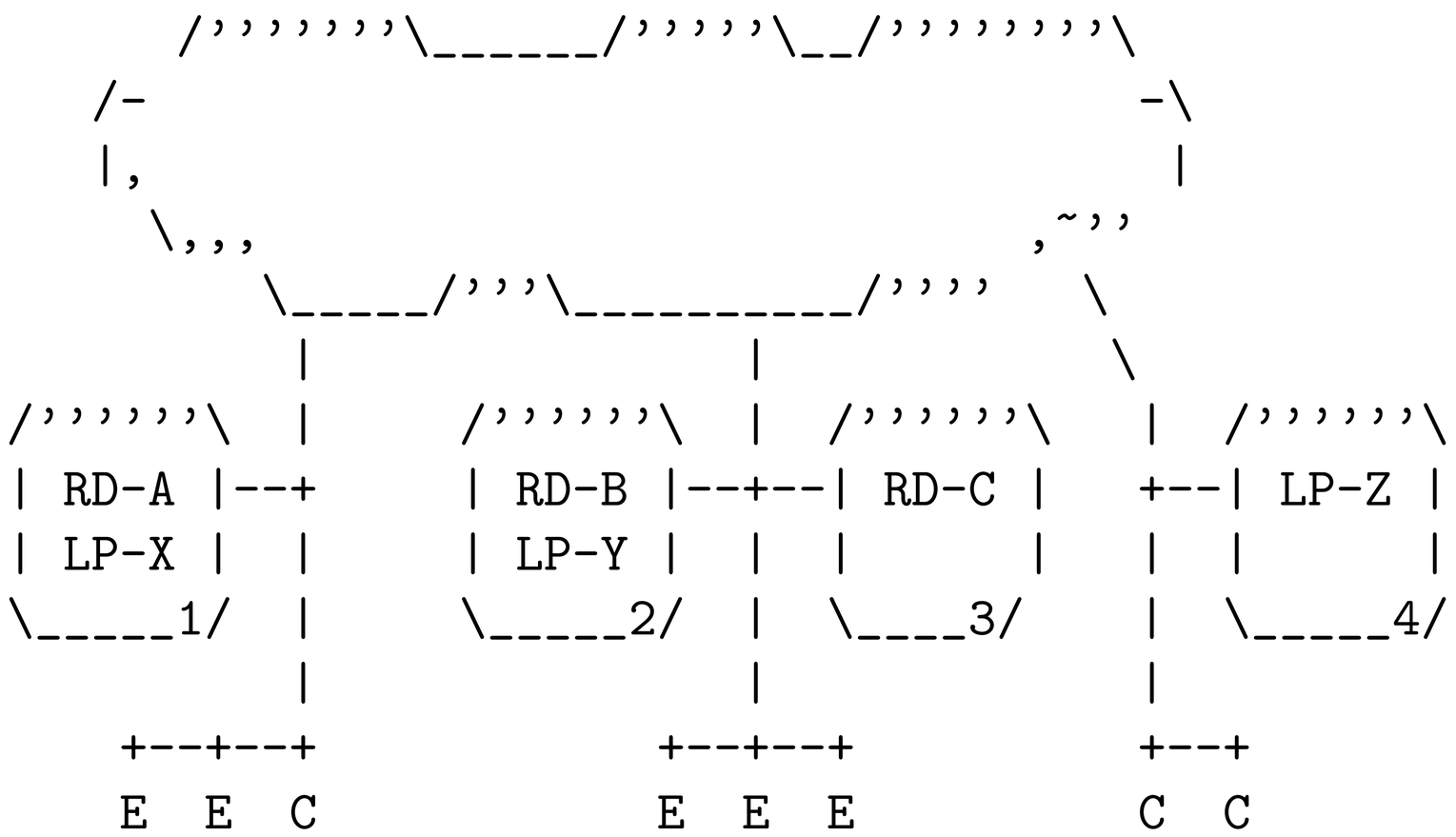
RD replication / rdlink

draft-amsuess-core-rd-replication,
draft-amsuess-t2trg-rdlink

Christian Amsüss

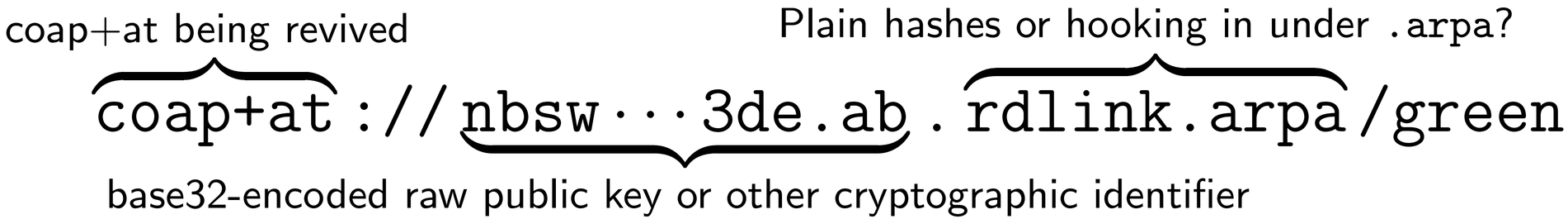
2019-03-29

Recap: RD replication



Moved to T2TRG

rdlink: Addresses



protocol-negotiation and resumed coap+at

- Active work on protocol-negotiation; coap+at resumed
- Requirements and challenges
  - URI aliasing: avoid
  - Trust model: required
- Experimentation
- Parts about to be moved to T2TRG due to experimental nature

CoRAL

CoRE | IETF 104

Drafts

- Constrained Resource Identifiers (CIRIs)
  draft-hartke-t2trg-ciri-02
- Constrained RESTful Application Language (CoRAL)
  draft-hartke-t2trg-coral-08

- Thing-to-Thing Data Hub
  draft-hartke-t2trg-data-hub-03
- CoRE Resource Discovery/Directory with CoRAL
  draft-hartke-t2trg-coral-reef-01

Constrained Resource Identifiers (CIRIs)

- CBOR-based encoding of URIs in the same option-style as CoAP
- Easy, correct implementations of URI arithmetic on constrained devices
- Application outside CoRAL, ex.: SenML, CWT, SUIT, ...

```
[ 1, "coap"
, 2, "example.org"
, 4, 62626
, 6, ".well-known"
, 6, "core"
]
```

```
[?(scheme:    1, text .regexp "[A-Za-z][A-Za-z0-9+.-]*"),
 ?(host.name: 2, text //
   host.ip:   3, bytes .size 4 / bytes .size 16),
 ?(port:      4, 0..65535),
 ?(path.type: 5, 0..127),
 *(path:      6, text),
 *(query:     7, text),
 ?(fragment:  8, text)]
```

Constrained RESTful Application Language (CoRAL)

- Data & interaction model for building M2M applications where machines…
  - navigate between resources by following **links**, and
  - perform operations on resources by submitting **forms**.
- CBOR-based serialization format
  suitable for constrained devices
- Lightweight, textual serialization format
  easy to read and write for humans

"What is the resource?"

"What can you do with the resource?"

"How does the resource relate to other resources?"

IETF 104

- Overall, concepts of CIRIs and CoRAL documents are stable
- Hackathon @ IETF 104
  - Parser for the textual format
  - Basic encoder/decoder for the CBOR format and CIRIs for RIOT OS
  - CoRAL examples and use cases
  - W3C Web of Things (WoT) Thing Description (TD) to CoRAL translation
  - Python CoRAL implementation with visualization updated to latest draft revision
- CoRAL Side-Meeting @ IETF 104
  - CIRIs: Using CIRIs outside CoRAL; Comparing CIRIs
  - Interoperating with CoRAL: Conversion between CoRAL and RDF and Link Format
  - CoRAL data and interaction model: Forms
  - Are real hypermedia applications feasible?
  - Towards working group adoption

.well-known/
core
Link Format

```
#using <http://coreapps.org/core#>
#using iana = <http://www.iana.org/assignments/relation/>

rd-item </sensors> {
  ct 40
  title "Sensor Index"
}
rd-item </sensors/temp> {
  rt "temperature-c"
  if "sensor"
  iana:describedby <http://www.example.com/sensors/t123>
  iana:alternate </t>
}
rd-item </sensors/light> {
  rt "light-lux"
  if "sensor"
}
```

Carsten's Coffee Machine SPLOT Example

```
#using <http://coreschema.org/ccm#>

isBrewing   true
progress    0.5
count       122
readyName   "size 110, strength 50%"
brewingName "size 230, strength 100%"
maxOrders   10
create      -> POST <f/brew?create>
queue-item  <f/brew/2/> {
    state       "paused"
    cancel      -> DELETE <>
    unpause     -> POST <s/order/state> [ payload "brewing" ]
}
queue-item  <f/brew/1/> {
    state       "queued"
    cancel      -> DELETE <>
    pause       -> POST <s/order/state> [ payload "paused" ]
}
queue-item  <f/brew/0/> {
    state       "queued"
    cancel      -> DELETE <>
    pause       -> POST <s/order/state> [ payload "paused" ]
}
```

Michael's Light Switch W3C Thing Description

```
#using  <http://coreapps.org/td#>
#using  iot = <http://iotschema.org/>
#base   <http://159.203.213.90:1880>

id              "urn:uuid:2d5e84f6-85c9-4436-b53f-c0669dfd1603"
type            <http://iotschema.org/Light>
type            <http://iotschema.org/BinarySwitch>
type            <http://iotschema.org/Level>
name            "Lamp"
iot:SwitchState </light> {
    contentType     "application/json"
    writeproperty   -> POST </light> [ contentType "application/json" ]
}
iot:CurrentLevel </light> {
    contentType     "application/json"
    writeproperty   -> POST </light> [ contentType "application/json" ]
}
iot:TurnOn   -> POST </light> [ contentType "application/json" ]
iot:TurnOff  -> POST </light> [ contentType "application/json" ]
iot:SetLevel -> POST </light> [ contentType "application/json" ]
```

IPSO Reuseable Resources

```
<http://coreapps.org/ipso#digital-input-state>              // The current state of a digital input.
<http://coreapps.org/ipso#digital-input-counter>            // The cumulative value of active state detected.
<http://coreapps.org/ipso#digital-input-polarity>           // The polarity of a digital input as a Boolean (0 = Normal, 1= Reversed)
<http://coreapps.org/ipso#digital-input-debounce>           // The debounce period in ms.
<http://coreapps.org/ipso#digital-input-edge-selection>     // The edge selection as an integer (1 = Falling edge, 2 = Rising edge, 3 = Both Rising and Falling edge)
<http://coreapps.org/ipso#digital-input-counter-reset>      // Reset the Counter value
<http://coreapps.org/ipso#current-time>                     // Unix Time. A signed integer representing the number of seconds since Jan 1st, 1970 in the UTC time zone.
<http://coreapps.org/ipso#fractional-time>                  // For shorter times of a fraction of a second (i.e. 0.23).
<http://coreapps.org/ipso#min-x-value>                      // The minimum measured value along the X axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#max-x-value>                      // The maximum measured value along the X axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#min-y-value>                      // The minimum measured value along the Y axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#max-y-value>                      // The maximum measured value along the Y axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#min-z-value>                      // The minimum measured value along the Z axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#max-z-value>                      // The maximum measured value along the Z axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#latitude>                         // The decimal notation of latitude, e.g. -43.5723 (World Geodetic System 1984).
<http://coreapps.org/ipso#longitude>                        // The decimal notation of longitude, e.g. 153.21760 (World Geodetic System 1984).
<http://coreapps.org/ipso#uncertainty>                      // The accuracy of the position in meters.
<http://coreapps.org/ipso#velocity>                         // The velocity of the device as defined in 3GPP 23.032 GAD specification. This set of values may not be available if the device is static.
<http://coreapps.org/ipso#timestamp>                        // The timestamp of when the location measurement was performed.
<http://coreapps.org/ipso#min-limit>                        // The minimum value that can be measured by the sensor.
<http://coreapps.org/ipso#max-limit>                        // The maximum value that can be measured by the sensor.
<http://coreapps.org/ipso#delay-duration>                   // The duration of the time delay.
<http://coreapps.org/ipso#clip>                             // Audio Clip that is playable (i.e. short audio recording indicating the floor in an elevator).
<http://coreapps.org/ipso#trigger>                          // Trigger initiating actuation.
<http://coreapps.org/ipso#duration>                         // The duration of the sound once tripper.
<http://coreapps.org/ipso#minimum-off-time>                 // The off time when On/Off control remains on.
<http://coreapps.org/ipso#timer-mode>                       // Type of timer pattern used by the timer. 1: One-shot, 2: On-Time or Interval, 3: Time delay on pick-up, 4: Time Delay on Drop-Out, 0: disables the timer.
<http://coreapps.org/ipso#text>                             // A string of text.
<http://coreapps.org/ipso#x-coordinate>                     // X Coordinate.
<http://coreapps.org/ipso#y-coordinate>                     // Y Coordinate.
<http://coreapps.org/ipso#clear-display>                    // Command to clear the display.
<http://coreapps.org/ipso#contrast>                         // Proportional control, integer value between 0 and 100 as a percentage.
<http://coreapps.org/ipso#increase-input-state>             // Indicates an increase control action.
<http://coreapps.org/ipso#decrease-input-state>             // Indicates a decrease control action.
<http://coreapps.org/ipso#counter>                          // Counts the number of times the timer output transitions from 0 to 1.
<http://coreapps.org/ipso#calibration-offset>               // Calibration offset value to be used to additively correct the measured value of the sensor.
<http://coreapps.org/ipso#current-position>                 // Current position or desired position of a positioner actuator.
<http://coreapps.org/ipso#transition-time>                  // The time expected to move the actuator to the new position.
<http://coreapps.org/ipso#remaining-time>                   // The time remaining in an operation.
<http://coreapps.org/ipso#up-counter>                       // Counts the number of times the increase control has been operated. Writing a 0 resets the counter.
<http://coreapps.org/ipso#down-counter>                     // Counts the times the decrease control has been operated. Writing a 0 resets the counter.
<http://coreapps.org/ipso#digital-state>                    // The current state of the timer output.
<http://coreapps.org/ipso#cumulative-time>                  // The total time in seconds that the timer input is true. Writing a 0 resets the time.
<http://coreapps.org/ipso#max-x-coordinate>                 // The highest X coordinate the display supports before wrapping to the next line.
<http://coreapps.org/ipso#max-y-coordinate>                 // The highest Y coordinate the display supports before wrapping to the next line.
<http://coreapps.org/ipso#multi-state-input>                // The current state of a Multi-state input or selector.
<http://coreapps.org/ipso#level>                            // Used to represent a level control such as audio volume.
<http://coreapps.org/ipso#digital-output-state>             // The current state of a digital output
<http://coreapps.org/ipso#digital-output-polarity>          // The polarity of a digital input as a Boolean (False = Normal, True = Reversed)
<http://coreapps.org/ipso#analog-input-current-value>       // The current value of the analog input.
<http://coreapps.org/ipso#min-measured-value>               // The minimum value measured by the sensor since it is ON or Reset, expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#max-measured-value>               // The maximum value measured by the sensor since it is ON or Reset, expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#min-range-value>                  // The minimum value that can be measured by the sensor, expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#max-range-value>                  // The maximum value that can be measured by the sensor, expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#reset-min-and-max-measured-values> // Reset the Min and Max Measured Values to current value.
<http://coreapps.org/ipso#analog-output-current-value>      // The current value of the analog output.
<http://coreapps.org/ipso#sensor-value>                     // Last or Current Measured Value from the Sensor expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#sensor-units>                     // Measurement Units Definition e.g. "Cel" for Temperature in degrees Celsius.
<http://coreapps.org/ipso#x-value>                          // The measured value along the X axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#y-value>                          // The measured value along the Y axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#z-value>                          // The measured value along the Z axis expressed in the unit defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#compass-direction>                // The compass direction.
<http://coreapps.org/ipso#colour>                           // A string representing a value in the color space defined by the "Sensor Units" resource if present.
<http://coreapps.org/ipso#application-type>                 // The application type of the sensor or actuator as a string, for instance "Air Pressure".
<http://coreapps.org/ipso#sensor-type>                      // The type of the sensor (for instance PIR type)
<http://coreapps.org/ipso#instantaneous-active-power>       // The current active power
<http://coreapps.org/ipso#min-measured-active-power>        // The minimum active power measured by the sensor since it is ON
<http://coreapps.org/ipso#max-measured-active-power>        // The maximum active power measured by the sensor since it is ON
<http://coreapps.org/ipso#min-range-active-power>           // The minimum active power that can be measured by the sensor
<http://coreapps.org/ipso#max-range-active-power>           // The maximum active power that can be measured by the sensor
<http://coreapps.org/ipso#cumulative-active-power>          // The cumulative active power since the last cumulative energy reset or device start
<http://coreapps.org/ipso#active-power-calibration>         // Request an active power calibration by writing the value of a calibrated load.
<http://coreapps.org/ipso#instantaneous-reactive-power>     // The current reactive power
<http://coreapps.org/ipso#min-measured-reactive-power>      // The minimum reactive power measured by the sensor since it is ON
<http://coreapps.org/ipso#max-measured-reactive-power>      // The maximum reactive power measured by the sensor since it is ON
<http://coreapps.org/ipso#min-range-reactive-power>         // The minimum active power that can be measured by the sensor
<http://coreapps.org/ipso#max-range-reactive-power>         // The maximum reactive power that can be measured by the sensor
<http://coreapps.org/ipso#cumulative-reactive-power>        // The cumulative reactive power since the last cumulative energy reset or device start
<http://coreapps.org/ipso#reactive-power-calibration>       // Request a reactive power calibration by writing the value of a calibrated load.
<http://coreapps.org/ipso#power-factor>                     // If applicable, the power factor of the current consumption.
<http://coreapps.org/ipso#current-calibration>              // Read or Write the current calibration coefficient
<http://coreapps.org/ipso#reset-cumulative-energy>          // Reset both cumulative active/reactive power
<http://coreapps.org/ipso#event-identifier>                 // The event identifier as a string.
<http://coreapps.org/ipso#start-time>                       // Time when the load control event will start started.
<http://coreapps.org/ipso#duration-in-min>                  // The duration of the load control event.
<http://coreapps.org/ipso#criticality-level>                // The criticality of the event. The device receiving the event will react in an appropriate fashion for the device.
<http://coreapps.org/ipso#avg-load-adjpct>                  // Defines the maximum energy usage of the receiving device, as a percentage of the device's normal maximum energy usage.
<http://coreapps.org/ipso#duty-cycle>                       // Defines the duty cycle for the load control event, i.e, what percentage of time the receiving device is allowed to be on.
<http://coreapps.org/ipso#on-off>                           // This resource represents an on/off actuator, which can be controlled, the setting of which is a Boolean value where True is On and False is Off.
<http://coreapps.org/ipso#dimmer>                           // This resource represents a light dimmer setting, which has an Integer value between 0 and 100 as a percentage.
<http://coreapps.org/ipso#on-time>                          // The time in seconds that the device has been turned on. Writing a value of 0 resets the counter.
<http://coreapps.org/ipso#muti-state-output>                // A string describing a state for multiple level output such as Pilot Wire
<http://coreapps.org/ipso#off-time>                         // The time in seconds since the Off command was sent. Writing a value of 0 resets the counter.
<http://coreapps.org/ipso#set-point-value>                  // The setpoint value expressed in the unit defined by the "Sensor Units" resource if present..
<http://coreapps.org/ipso#busy-to-clear-delay>              // Delay from the detection state to the clear state in ms
<http://coreapps.org/ipso#clear-to-busy-delay>              // Delay from the clear state to the busy state in ms.
<http://coreapps.org/ipso#bitmap-input>                     // Integer in which each of the bits are associated with specific digital input value.  Represented as a binary signed integer in network byte order, and in two's complement representation.
<http://coreapps.org/ipso#bitmap-input-reset>               // Reset the Bitmap Input value
<http://coreapps.org/ipso#element-description>              // The semantics / description of each bit as a string. First instance describes the least significant bit, second instance the second least significant bit, etc
```

IETF 104

- CoRAL works!
  for resource discovery and beyond
- GitHub repository with companion material
  https://github.com/ektrah/coral
  - CDDL, ABNF grammars
  - Code extracted from the drafts
  - Test vectors
- 10+ GitHub issues that would benefit from WG input

https://datatracker.ietf.org/doc/draft-hartke-t2trg-coral/

https://datatracker.ietf.org/doc/draft-hartke-t2trg-ciri/

https://datatracker.ietf.org/doc/draft-hartke-t2trg-coral-reef/

https://datatracker.ietf.org/doc/draft-hartke-t2trg-data-hub/

https://github.com/ektrah/coral

WGA CoRAL+CIRI

- Do we want to adopt (part of) the CoRAL work?
  - CIRI
  - CoRAL
  - Not CoRAL-Reef at this time?

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

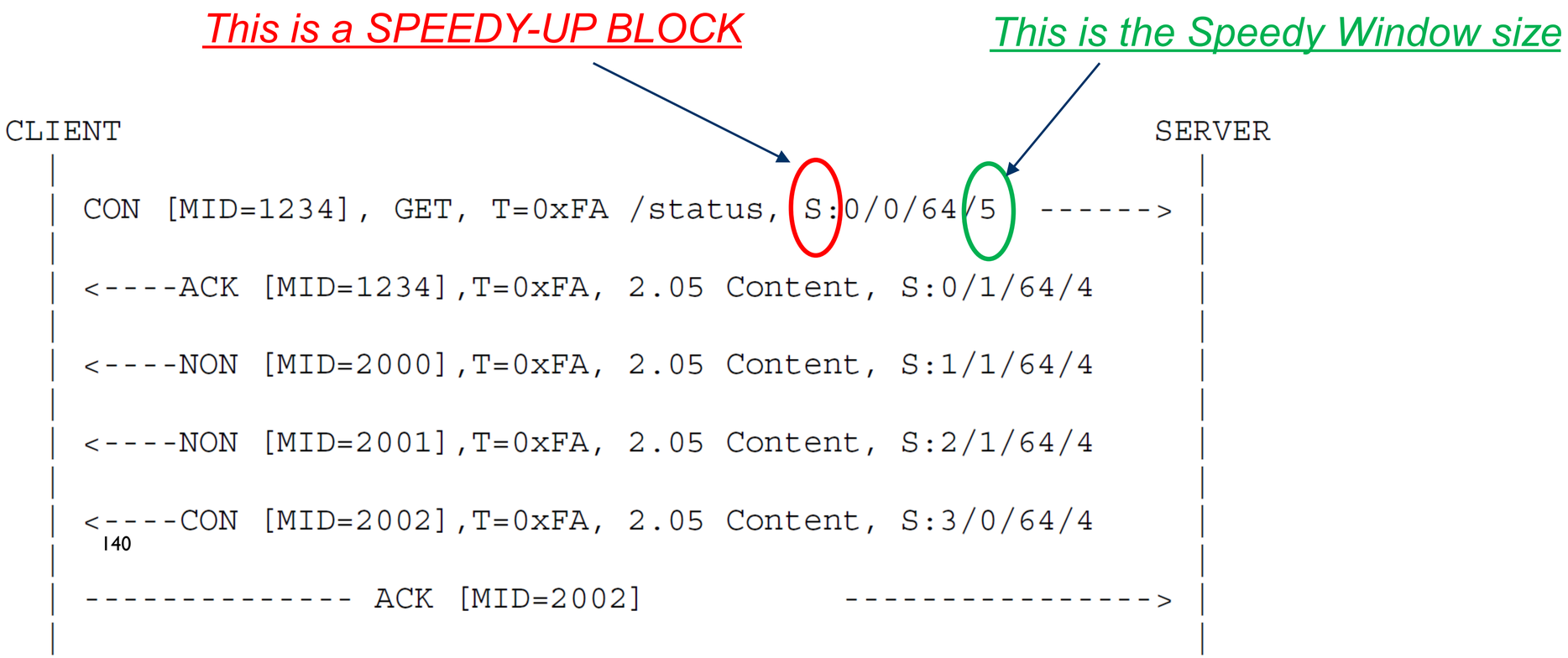
The State of The Art

- 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;

139

Example Conversation using the Speedy-up Block Transfer



Another example conversation

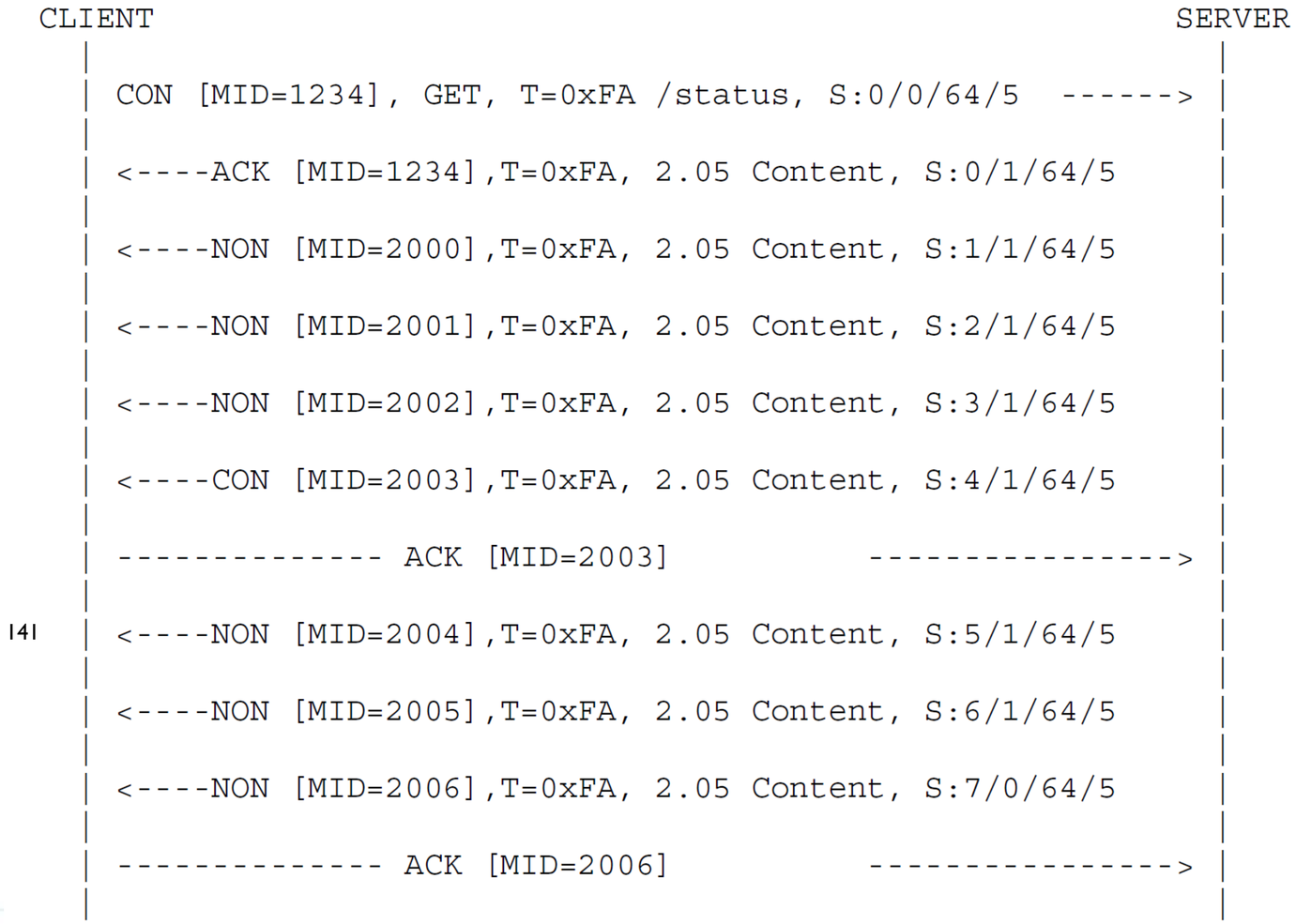
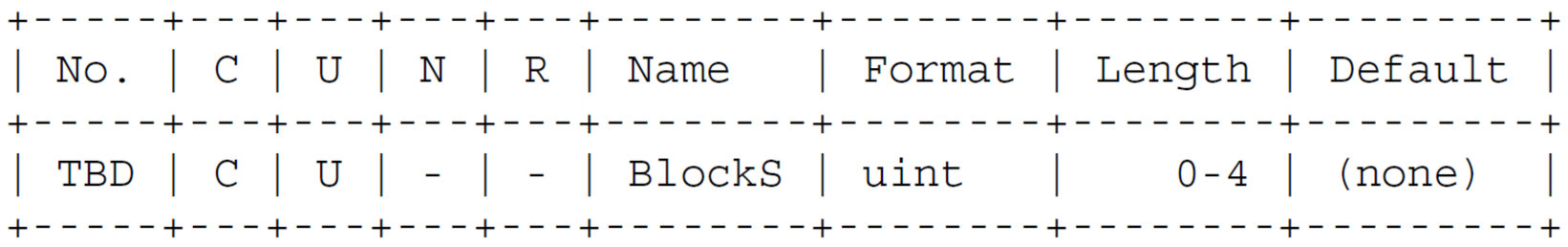


Figure 3: Speedy Blockwise GET with Early Negotiation

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

142

There are some other considerations for Retransmission and etc.

Next Steps

This is a small fix ;

Any interests in this WG?

Slides lost on the way (not shown)

RD-DNS-SD

draft-ietf-core-rd-dns-sd-04

Kerry Lynn, Peter van der Stok, Michael Koster, Christian Amsuess

IETF 104 - CoRE Working Group

-04 Updates to -03

- Text is restructured:
  - Merged sections 2 and 4
  - Removed automatic mapping “rt-> ServiceType”
  - Added ‘st’ attribute section
  - Removed hierarchical (_sub) DNS-SD Service Instance Names for simplicity

- General rephrasing of Introduction
- Examples adapted with ‘st’ parameter

- IANA considerations: addition of ‘st’, ‘ins’ and ‘exp’ parameters to registry “RD parameters” <specified in RD>

Thanks to Ted Lemon and Stuart Cheshire for their thorough reviews.

‘st’ parameter

‘st‘ attribute maps directly to the <Service> part of a DNS-SD Service Instance Name.

- Value of 'st' attribute is pre-specified.
- Registered in the IANA Service Name and Transport Protocol Port Number Registry
- Conforms to the syntax defined in RFC 6335 Section 5.

Example

Req: GET /rd-lookup/res?exp
Res: 2.05 Content
<coap://[FDFD::1234]:5683/light/1>;
exp;st='oic-light';rt='oic.d.light';ins='Spot'; d='office';ep='node1'

An agent registers the following DNS-SD RRs, assuming a derived DNS zone name "office.example.com"

```
_oic-light._udp.office.example.com  IN PTR
        Spot._oic-light._udp.office.example.com
Spot._oic-light._udp.office.example.com. IN TXT
        txtver=1;path=/light/1;rt=oic.d.light
Spot._oic-light._udp.office.example.com. IN SRV
        0 0 5683 node1.office.example.com.
node1.office.example.com.  IN AAAA  FDFD::1234
```

TODO

- Work out hierarchical (_sub) form of DNS-SD naming, if required

- Explain how to derive <Domain> part of DNS-SD Service Instance Name