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 3979 and its updates**

- Blue sheets
- Scribe(s): http://tools.ietf.org/wg/core/minutes

http://www.ietf.org/about/note-well.html

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda Bashing

All times are in time-warped CEST

Tuesday

- **14:00–14:10 Intro, WG status**
- **14:10–14:20 FETCH/PATCH (PV)**
- **14:20–14:30 Links-JSON (CB)**
- **14:30–15:25 CoAP over reliable WG draft (BR)**
- **15:25–15:35 Multiple Transports (BS)**
- **15:35–15:45 Possibly related work (CG, CG, ZC)**
- **15:45–16:00 Resource Directory (MK)**

All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

Milestones (from WG charter page)

http://datatracker.ietf.org/wg/core/charter/

- Done Blockwise transfers in CoAP for PS
- Jul 2016 Best Practices for HTTP-CoAP Mapping Implementation for Info
- Aug 2016 Representing CoRE Link Collections in JSON for PS
- Aug 2016 Patch and Fetch Methods for CoAP for PS
- Aug 2016 Media Types for Sensor Measurement Lists (SenML) for PS
- Aug 2016 WG adoption for Management over CoAP
- Sep 2016 CoRE Resource Directory for PS
- Oct 2016 CoAP over TCP, TLS, and WebSockets for PS
- Dec 2016 CBOR Encoding of Data Modeled with YANG for PS
- Dec 2016 Management over CoAP for PS
- Mar 2017 CoRE Interfaces for Info

All times are in time-warped CEST

Tuesday

- 14:00–14:10 Intro, WG status
- 14:10–14:20 FETCH/PATCH (PV)
- 14:20–14:30 Links-JSON (CB)
- 14:30–15:25 CoAP over reliable WG draft (BR)
- 15:25–15:35 Multiple Transports (BS)
- 15:35–15:45 Possibly related work (CG, CG, ZC)
- 15:45–16:00 Resource Directory (MK)

CoRE working group

Fetch and Patch methods for CoAP

draft-ietf-core-etch-01

P. van der Stok, C. Bormann

Objective:

Payload Reduction

By transporting part(s) of resource(s)

CoAP Methods

Code	Name	Code	Name	safe	idempotent
0.01	GET	0.05	FETCH	yes	yes
0.02	POST	0.06	PATCH	no	no
0.03	PUT	0.07	iPATCH	no	yes
0.04	DELETE			no	yes

Additions since -00

FETCH example added

Excellent exercise, because no Content Format existing

First Customer in queue: CoMI
with list of YANG identifiers

Additions to -02

- Response Code 4.12 for iPatch: not idem-potent request
- admonition not to cache a FETCH result as if it were a GET result.
- Few words about http/coap mapping
- Explain error returns for multiple requests
- Few words on use of “?” in GET URI

All times are in time-warped CEST

Tuesday

- **14:00–14:10 Intro, WG status**
- **14:10–14:20 FETCH/PATCH (PV)**
- **14:20–14:30 Links-JSON (CB)**
- **14:30–15:25 CoAP over reliable WG draft (BR)**
- **15:25–15:35 Multiple Transports (BS)**
- **15:35–15:45 Possibly related work (CG, CG, ZC)**
- **15:45–16:00 Resource Directory (MK)**

Issue #~~403~~

- Q: Should the RFC 7390 part of links-json be split off?
- A: Yes.
- → draft-bormann-core-groupcomm-cbor
- core-links-json now representation of RFC 6690 in JSON and CBOR only

Issue #402

- Q: Should there be a reference implementation?
- A: Yes.
- Appendix A now contains an implementation
  - RFC 6690 parser + JSON/CBOR output plus the inverse

New issue

- Instead of just representing the RFC 6690 structure, should we try to comply to JSON-LD?
- Pro: result conforms to RDF
- Con: result no longer represents RFC 6690 link format

All times are in time-warped CEST

Tuesday

- 14:00–14:10 Intro, WG status
- 14:10–14:20 FETCH/PATCH (PV)
- 14:20–14:30 Links-JSON (CB)
- 14:30–15:25 CoAP over reliable WG draft (BR)
- 15:25–15:35 Multiple Transports (BS)
- 15:35–15:45 Possibly related work (CG, CG, ZC)
- 15:45–16:00 Resource Directory (MK)

coap-tcp-tls @ IETF 96

Brian Raymor

Since IETF 95

- Existing draft and issues transitioned to github repo
- coap-tcp-tls-03 merges:
  - draft-ietf-core-coap-tcp-tls-02
  - draft-savolainen-core-coap-websockets-07
  - draft-bormann-core-coap-sig-02
  - draft-bormann- core-block-bert-01

Pending Issues to Discuss

Require Application Layer Protocol Negotiation (ALPN) for CoAP over TLS?

https://github.com/core-wg/coap-tcp-tls/issues/4

ALPN Refresher

*With ALPN, **the client sends the list of supported application protocols as part of the TLS ClientHello message. The server chooses a protocol and sends the selected protocol as part of the TLS ServerHello message**. The application protocol negotiation can thus be accomplished within the TLS handshake, without adding network round-trips, and allows the server to associate a different certificate with each application protocol, if desired.*

Require ALPN except for port 5684?

Rough consensus was to always require ALPN for CoAP over TLS similar to HTTP/2 over TLS … but …

Strawman: To accommodate TLS implementations that do not (yet) support ALPN, should there be an exception that CoAP over TLS is implied on port 5684 only?

Observing resources over reliable transports

https://github.com/core-wg/coap-tcp-tls/issues/5

Observe: What about Confirmable Notifications?

A notification can be confirmable or non-confirmable … the client MUST acknowledge the message as usual … An acknowledgement message signals to the server that the client is alive and interested in receiving further notifications; **if the server does not receive an acknowledgement in reply to a confirmable notification, it will assume that the client is no longer interested and will eventually remove the associated entry from the list of observers**

Security Considerations: Older versions of TLS

https://github.com/core-wg/coap-tcp-tls/issues/8

“MUST support TLS 1.2 or higher” -but no enforcement details

Strawman: Enforce with the new Abort (7.05) message and indicate reason by either:

- Adding *Inadequate-Security* elective option

OR

- Just using Diagnostic Payload

Security Considerations: Making TLS a MUST

https://github.com/core-wg/coap-tcp-tls/issues/11

Guidance

Security Challenges For the Internet Of Things (2011):

*It is essential that IoT protocol suites specify a **mandatory to implement but optional to use security solution**. This will ensure security is available in all implementations, but configurable to use when not necessary (e.g., in closed environment).*

IAB Statement on Internet Confidentiality (2014):

Newly designed protocols should prefer encryption to cleartext operation.

Mandatory exchange of Capability and Settings after connection setup?

https://github.com/core-wg/coap-tcp-tls/issues/16

New Capability and Settings Messages (CSM) introduce options that may impact how a receiver is expected to communicate with a sender. For example:

- Maximum message size that the sender can receive
- Support for Block-wise Transfer and/or BERT

Strawman: Adopt model similar to HTTP/2 SETTINGS:

- Capability and Settings MUST be sent by both endpoints at the start of a connection and MAY be sent at any other time by either endpoint over the lifetime of the connection.
- Capability and Settings may be empty (contain no options).

WebSocket Ping-Pong versus Signaling Ping-Pong

https://github.com/core-wg/coap-tcp-tls/issues/34

Comparing Ping-Pong(s)

WebSocket Ping-Pong:

- May serve either as a keepalive or as a means to verify that the remote endpoint is still responsive.
- Upon receipt of a Ping, an endpoint MUST send a Pong in response and SHOULD respond with a Pong as soon as is practical

CoAP Ping-Pong Signaling:

- Ping Signaling Message
  - With Custody Option: Explicit request for Pong to return Custody option – this may cause the Pong to be delayed
- Pong Signaling Message
  - With Custody Option: Indicates that all Requests/Responses before Ping have been processed
- Empty messages (Code 0.00) can always be sent and MUST be ignored by the recipient. This provides a basic keep-alive function

Bikeshed: coaps+ws versus coap+wss?

https://github.com/core-wg/coap-tcp-tls/issues/12

Where does the “s” for secure go?

Consistent with the WebSocket secure scheme: coap+wss?

-OR-

Consistent with the CoAP secure schemes: coaps+ws?

- coaps (secure UDP)
- coaps+tcp (secure TCP)

All times are in time-warped CEST

Tuesday

- 14:00–14:10 Intro, WG status
- 14:10–14:20 FETCH/PATCH (PV)
- 14:20–14:30 Links-JSON (CB)
- 14:30–15:25 CoAP over reliable WG draft (BR)
- 15:25–15:35 Multiple Transports (BS)
- 15:35–15:45 Possibly related work (CG, CG, ZC)
- 15:45–16:00 Resource Directory (MK)

CoAP Protocol Negotiation

draft-silverajan-core-coap-protocol-negotiation

Bill Silverajan TUT

Summary of changes from -02

- Restructuring for easier editing
- Scenarios and examples added
- Node classification based on transport types
- CoAP transports can have ”al” (active lifetime) attribute

Forthcoming change:
Usage of URI Templates

- Change this operation:

```
Client ----> GET /.well-known/core?tt=* ---> Server
Client <--- 2.05 Content, tt="tcp sms” <---  Server
```

- Into this operation:

```
Client ---- GET /.well-known/core?rt=core.pn ----> Server
       Content-Format: application/link-format
Client <-- 2.05 Content"</pn>;rt="core.pn";ct=40 <--- Server
```

- Introduce a discovery interface for CoAP transports:

  Method: `GET`
  URI Template: `/.well-known/core`
  URI Template: `/{+pn}{?q*}`

  Example Request: `GET /pn?tt="tcp"`

Proposal:
Client-Initiated Transport Negotiation

- In version -03, waking up an inactive transport is implicit:

```
Client ----> GET coap+sms://0012345/.well-known/core?tt=udp ----> Server
Client <--- 2.05 Content, <coap://example.org/>;rel_"altloc";al=120 <-- Server
```

- Work for version -04: New CoAP option
  - For clients to request activating server's inactive transport
  - Prevent transport from going inactive (eg by extending lifetime)

- Example 1:

```
Client ----> GET coap+sms://001234567/pn?tt=udp ----> Server
Client <--- 4.04 "Not Found" <-- Server
```

- Example 2:

```
Client ----> GET coap+sms://001234567/pn?tt=udp ----> Server
         OPTION ACTIVE_TRANSPORT
Client <-- 2.05 Content <coaps://example.org/>;rel="altloc";al=120;tt=udp <-- Server
```

- Alternatives to above approach?

Session continuation

- Mechanism for client to inform server to continue session over a different CoAP transport
  - Many pitfalls envisaged (Observe, Block Transfers, switching to less secure channel)
- Go/no-go decision to explore?

All times are in time-warped CEST

Tuesday

- **14:00–14:10 Intro, WG status**
- **14:10–14:20 FETCH/PATCH (PV)**
- **14:20–14:30 Links-JSON (CB)**
- **14:30–15:25 CoAP over reliable WG draft (BR)**
- **15:25–15:35 Multiple Transports (BS)**
- **15:35–15:45 Possibly related work (CG, CG, ZC)**
- **15:45–16:00 Resource Directory (MK)**

All times are in time-warped CEST

Tuesday

- **14:00–14:10 Intro, WG status**
- **14:10–14:20 FETCH/PATCH (PV)**
- **14:20–14:30 Links-JSON (CB)**
- **14:30–15:25 CoAP over reliable WG draft (BR)**
- **15:25–15:35 Multiple Transports (BS)**
- **15:35–15:45 Possibly related work (CG, CG, ZC)**
- **15:45–16:00 Resource Directory (MK)**

Resource Directory

draft-ietf-core-resouce-directory

Recent Updates

- Clearly separated resource directory discovery from resource discovery
- Add IPv6 ND Option for discovery of an RD
- Removed option for simple POST of link data, don't require a .well-known/core resource to accept POST data and handle it in a special way
- RD-Look-up text is extended
- Maximum length of domain parameter 63 bytes for consistency with group
- Clarify group configuration section 6.1 that endpoints must be registered before including them in a group
- Removed link target value returned from domain and group lookup types
- Removed all superfluous client-server flow diagrams
- Simplified lighting example
- Introduced Commissioning Tool

Issues

- #372 - use cases (done)
- #398 - lighting example (done)
- #399 - message exchange figures (done)
- #405 - link attribute- link format syntax (missed, do ASAP)
- #406 - RD Enhancements from Rahman (won't do)
- #412 - Discovery text (done)
- #413 - Simple discovery (done)
- #414 – RESTful and parameter changes" (won't do)

Status

- Resolved the issues in issue tracker
- Incorporated comments and suggestions from many people
- 2 rounds of review and revisions in Apirl and July
- No more feature changes or additions
- Preparing for WGLC

All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

CoAP Simple Congestion Control/Advanced (CoCoA)

draft-bormann-core-cocoa-04

Carsten Bormann – Universität Bremen TZI
cabo@tzi.org
August Betzler, Carles Gomez, Ilker Demirkol
Universitat Politècnica de Catalunya (UPC)/Fundació i2cat
carlesgo@entel.upc.edu

With the support of Ministerio de Educación, Cultura y Deporte, through the José Castillejo grant CAS15/00336

Outline

- 1. NONs: performance results

A. Betzler, J. Isern, C. Gomez, I. Demirkol, J. Paradells, "Experimental Evaluation of Congestion Control for CoAP Communications without End-to-End Reliability", Ad-Hoc Networks journal (in press).

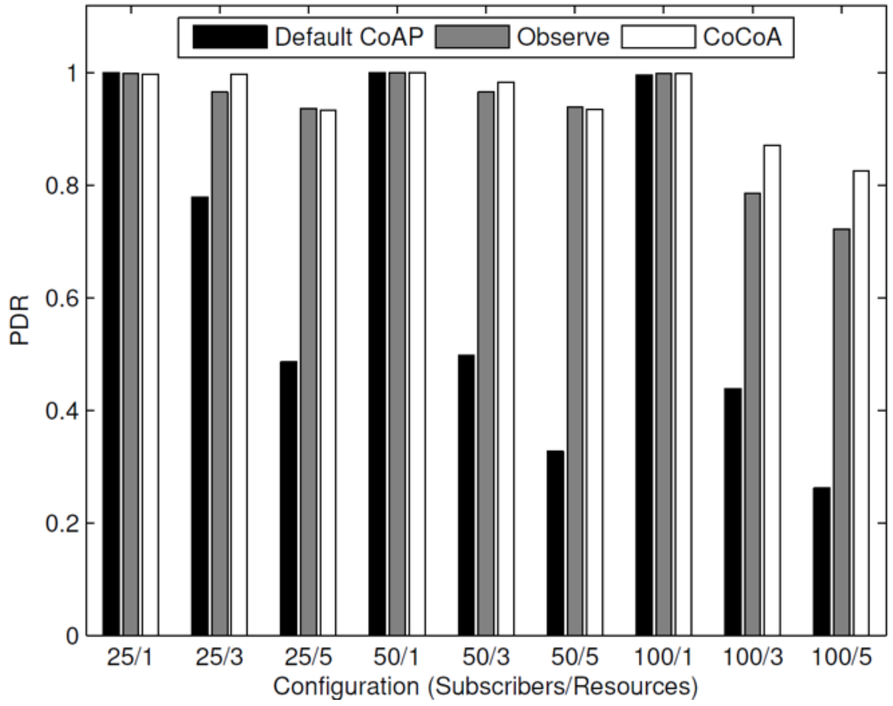
- 2. Updates in -04

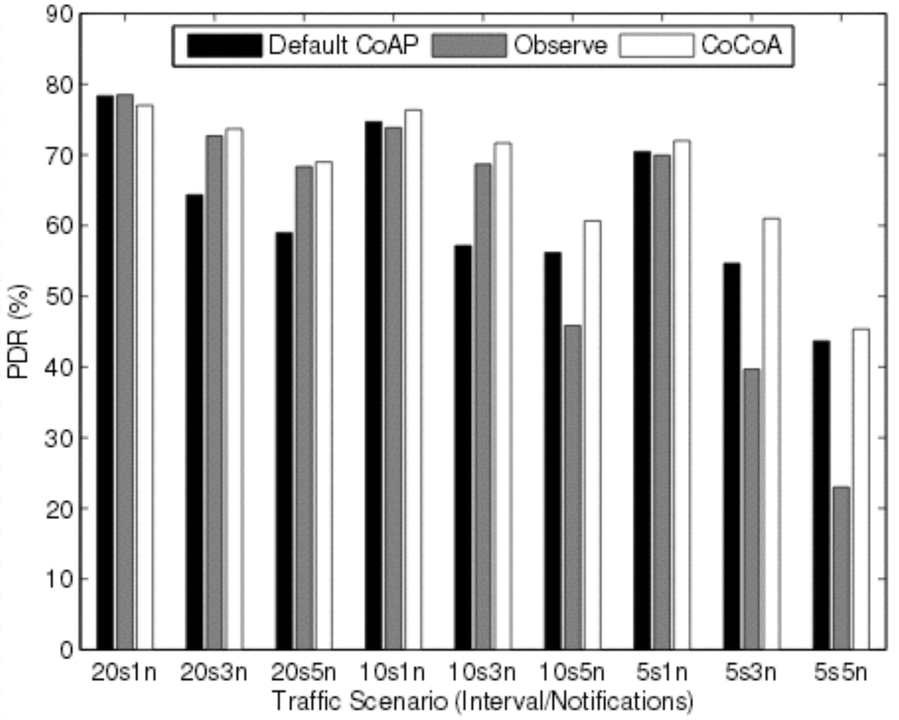
- 3. Aggregate Congestion Control preliminary emulation results

- 4. Ready for WG adoption ?

1. NONs: performance results

- Proxy sending sensor updates to cloud subscribers
  - Emulated GPRS link
- 60-node IEEE 802.15.4 multihop testbed
  - IoT-Lab (Grenoble)





2. Updates in -04

- Aggregate Congestion Control (ACC)
  - LAMBDA modified
    - OLD: constant value of 4
    - NEW: dependent on the number of intended destinations
      - LAMBDA = max(4, KNOWN_DEST_ENDPOINTS/4)
  - Added Example 2
    - To illustrate the effect of the above change
  - Moved ACC to an appendix
    - ACC is probably more interesting on the cloud side
    - Should ACC be a separate document?

3. Preliminary ACC results

- Emulated GPRS scenario
  - Cf client sending messages to several servers
  - Compared to CoCoA (w/o ACC)
    - Similar PDR
      - Slightly higher in „bursty parallel“ scenarios
    - Lower RTT and RTO
    - Significantly lower number of retries
  - More research TBD in other scenarios

4. Ready for WG adoption ?

- CoCoA algorithm is stable, well performing
  - Maturity has been reached
    - Simulation, emulation, experiments
    - IEEE 802.15.4 multihop networks, GPRS, UMTS, Wi-Fi
    - CONs/NONs, different traffic patterns
    - Several alternatives tested (strong-only, PH, Linux TCP…)
- Presentations
  - IETF 87, IETF 89, IETF 90, IETF 91, IETF 92 (ICCRG), IETF 94, IETF 96

4. Ready for WG adoption ?

- Papers or other documents on the topic
  - Evaluation Internet Draft:
    - F. Zheng, B. Fu, Z. Cao, “CoAP Latency Evaluation”, draft-zheng-core-coap-lantency-evaluation-00, 2016 (work in progress)
  - Conferences/workshops

- Bhalerao, Rahul, Sridhar Srinivasa Subramanian, and Joseph Pasquale. "An analysis and improvement of congestion control in the CoAP Internet-of-Things protocol." 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2016.

- I Järvinen, L Daniel, M Kojo, "Experimental evaluation of alternative congestion control algorithms for Constrained Application Protocol (CoAP)", IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015.

- Balandina, Ekaterina, Yevgeni Koucheryavy, and Andrei Gurtov. "Computing the retransmission timeout in coap." Internet of Things, Smart Spaces, and Next Generation Networking. Springer Berlin Heidelberg, 2013. 352-362.

4. Ready for WG adoption ?

- Papers or other documents on the topic
  - Conferences/workshops

- A. Betzler, C. Gomez, I. Demirkol, "Evaluation of Advanced Congestion Control Mechanisms for Unreliable CoAP Communications", ACM PE-WASUN, Cancún, Mexico, 2015.

- A. Betzler, C. Gomez, I. Demirkol, M. Kovatsch, "Congestion Control for CoAP cloud services", 8th International Workshop on Service-Oriented Cyber-Physical Systems in Converging Networked Environments (SOCNE) 2014, Barcelona, Spain, Sept. 2014.

- A. Betzler, C. Gomez, I. Demirkol, J. Paradells, "Congestion Control in Reliable CoAP Communication", 16th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM'13), Barcelona, Spain, Nov. 2013.

4. Ready for WG adoption ?

- Papers or other documents on the topic
  - Journals/magazines

- A. Betzler, J. Isern, C. Gomez, I. Demirkol, J. Paradells, "Experimental Evaluation of Congestion Control for CoAP Communications without End-to-End Reliability", Ad-Hoc Networks journal (in press).

- A. Betzler, C. Gomez, I. Demirkol, J. Paradells, "CoAP congestion control for the Internet of Things", IEEE Communications Magazine (accepted for publication, probably in July 2016).

- A. Betzler, C. Gomez, I. Demirkol, J. Paradells, "CoCoA+: an advanced congestion control mechanism for CoAP", Ad-hoc Networks journal, 2015.

  - Dr. August Betzler's PhD thesis
    - A. Betzler "Improvements to End-to-End Performance of Low-Power Wireless Networks", 2015

4. Ready for WG adoption ?

- Running code
  - Californium (Cf) with CoCoA is publicly available
    - Cf: CoAP implementation for unconstrained devices
    - https://github.com/eclipse/californium
      - cf-cocoa example
      - org.eclipse.californium.core.network.stack.congestioncontrol
  - CoCoA implementation for Erbium (Er)
    - Er: official CoAP implementation for Contiki OS
  - libcoap ported to Android with CoCoA
    - By Zheng et al

- **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 3979 and its updates**

✓Blue sheets
✓Scribe(s)

http://www.ietf.org/about/note-well.html

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

Core Interfaces Split

draft-ietf-core-interfaces-05

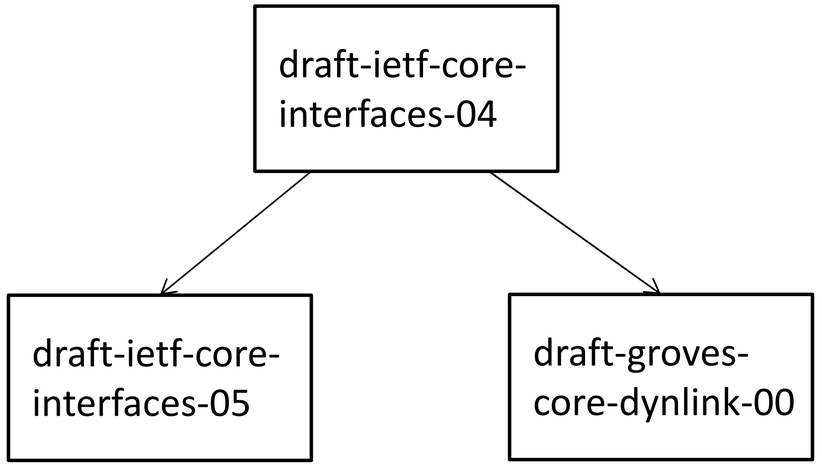
draft-groves-core-dynlink-00

IETF #96 Berlin

Christian Groves

Michael Koster

Split



Principle: KISS

- Split documents without addressing new functionality or changing existing functionality
- Minor errors fixed.
- Subsequent version to introduce technical additions/changes.
- Based on CoRE interfaces draft roadmap email discussion (30/3/2016)

draft-ietf-core-interfaces-05

- Moved:
  - Dynamic linking
  - Conditional Observation attributes
- Removed:
  - Hypermedia Collection and Controls (Topic for T2TRG)
  - WADL descriptions

draft-ietf-core-interfaces-05

- Retained:
  - Interface descriptions: Link List, Batch, Linked Batch, Sensor, Parameter, RO parameter & Actuator
  - Collections: Link List, Batch, Linked Batch
  - Function sets and profiles?

draft-ietf-core-interfaces-05

- Next Steps:
  - Need to indicate that this is not the IETF endorsed way to use REST.
  - Look at alignment with OCF collections to develop BCP guidance.
  - Are function sets and profiles needed? Maybe less formal approach? Is this achieved through removal of WADL?

Dynamic Resource Linking for Constrained RESTful Environments

draft-groves-core-dynlink-00

- Contains:
  - Link Binding (core.bnd)
  - Conditional Observation attributes (bind, pmin, pmax, st, gt, lt)
- Removed:
  - WADL descriptions

draft-groves-core-dynlink-00

- Next steps:
  - Can this become a WG draft?
  - Clarify the usage and behaviour (especially interactions) of existing attributes careful to maintain alignment with LWM2M.
  - New Attributes regarding reporting state, and upper and lower band limits.

  See “Binding Attributes in draft-ietf-core-interfaces” email dicussion 03/2016).

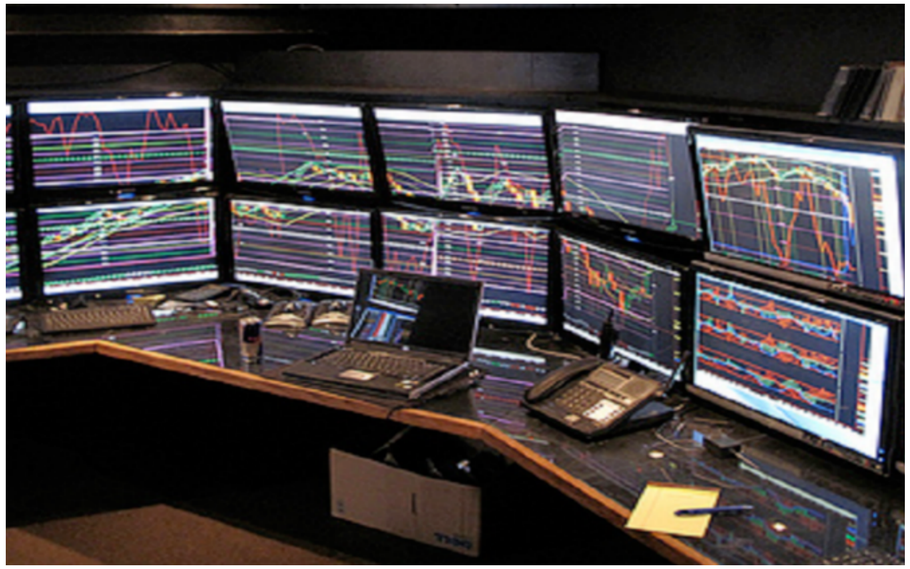
All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

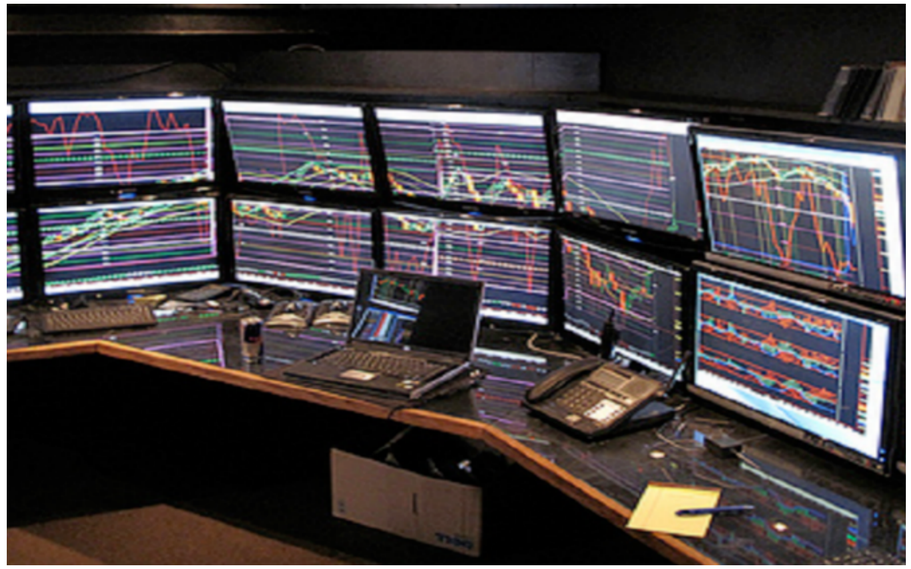
Constrained Management and Objects Language

Michel Veillette
Alexander Pelov
Abhinav Somaraju
Randy Turner
Ana Minaburo
Laurent Toutain
Peter Van der Stok
Andy Biermann



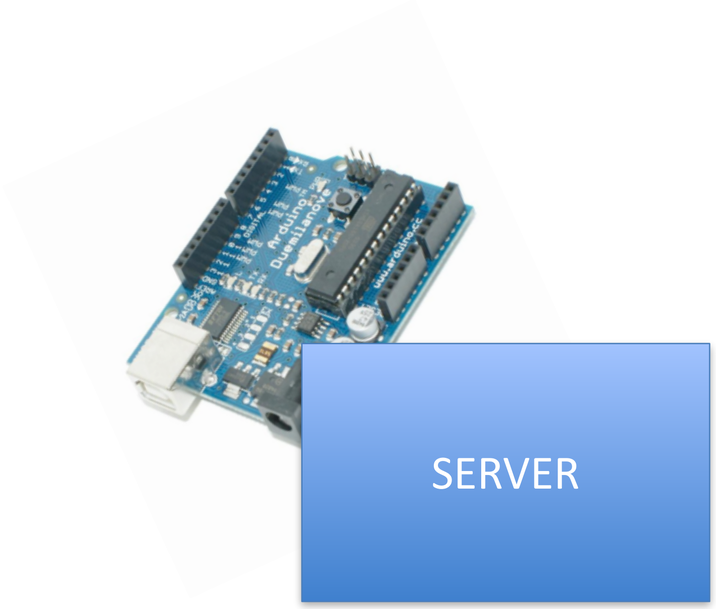
Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander
Pelov <a@ackl.io>

SERVER



Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

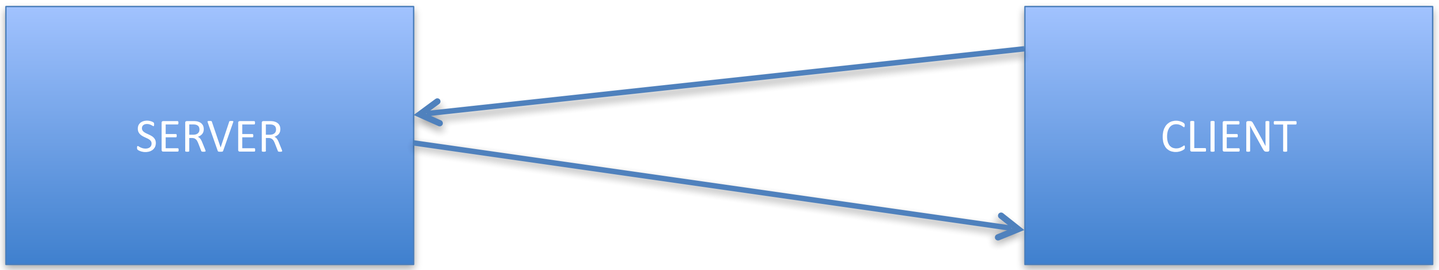
Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>



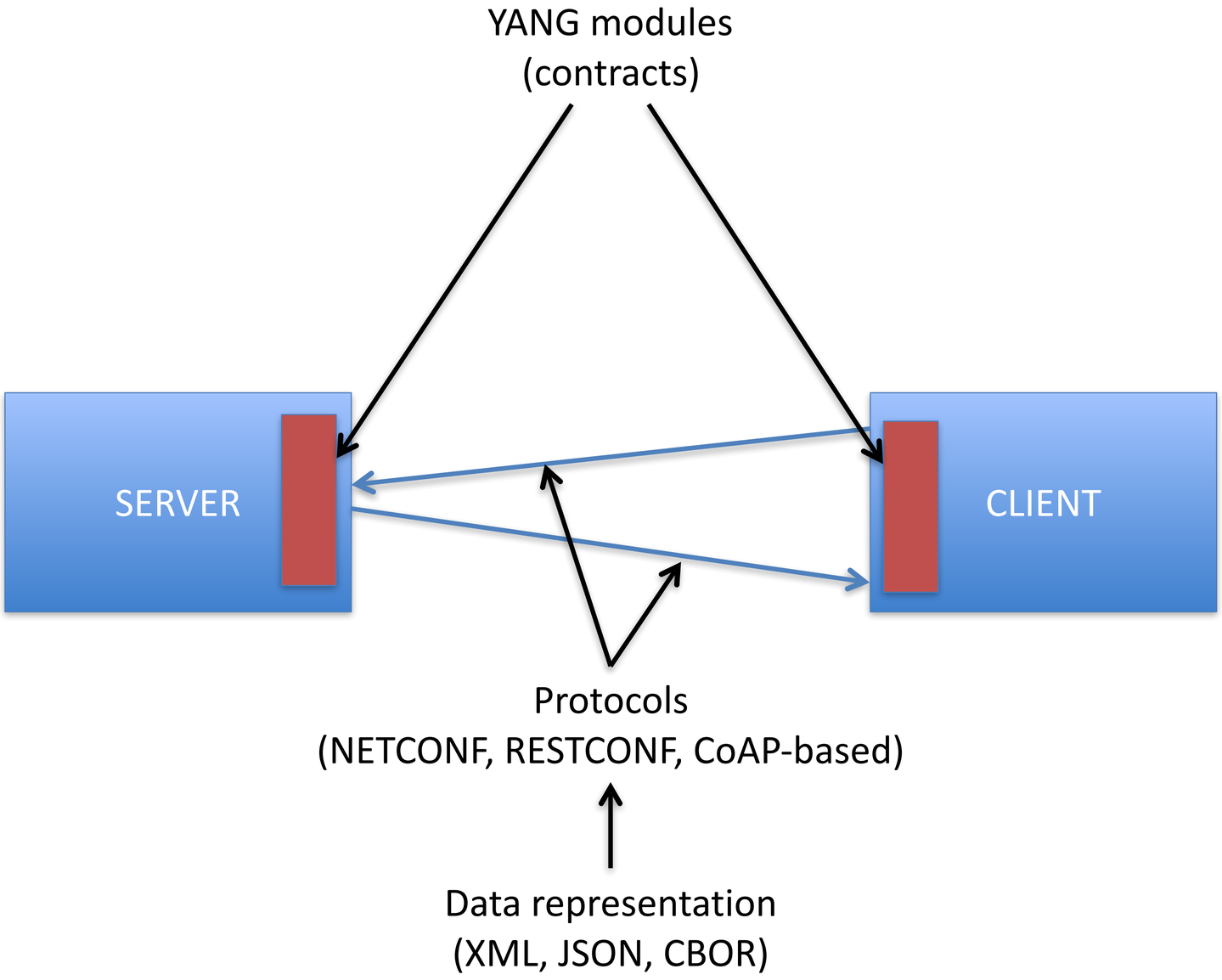
SERVER

CLIENT

Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

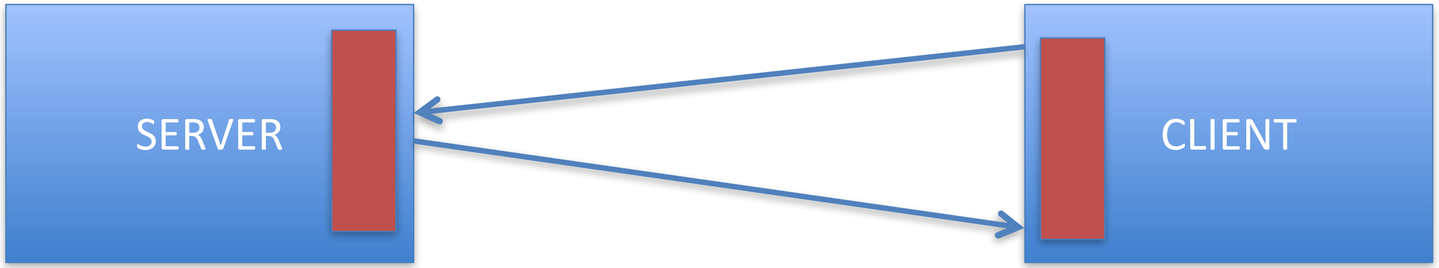


Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander
Pelov <a@ackl.io>



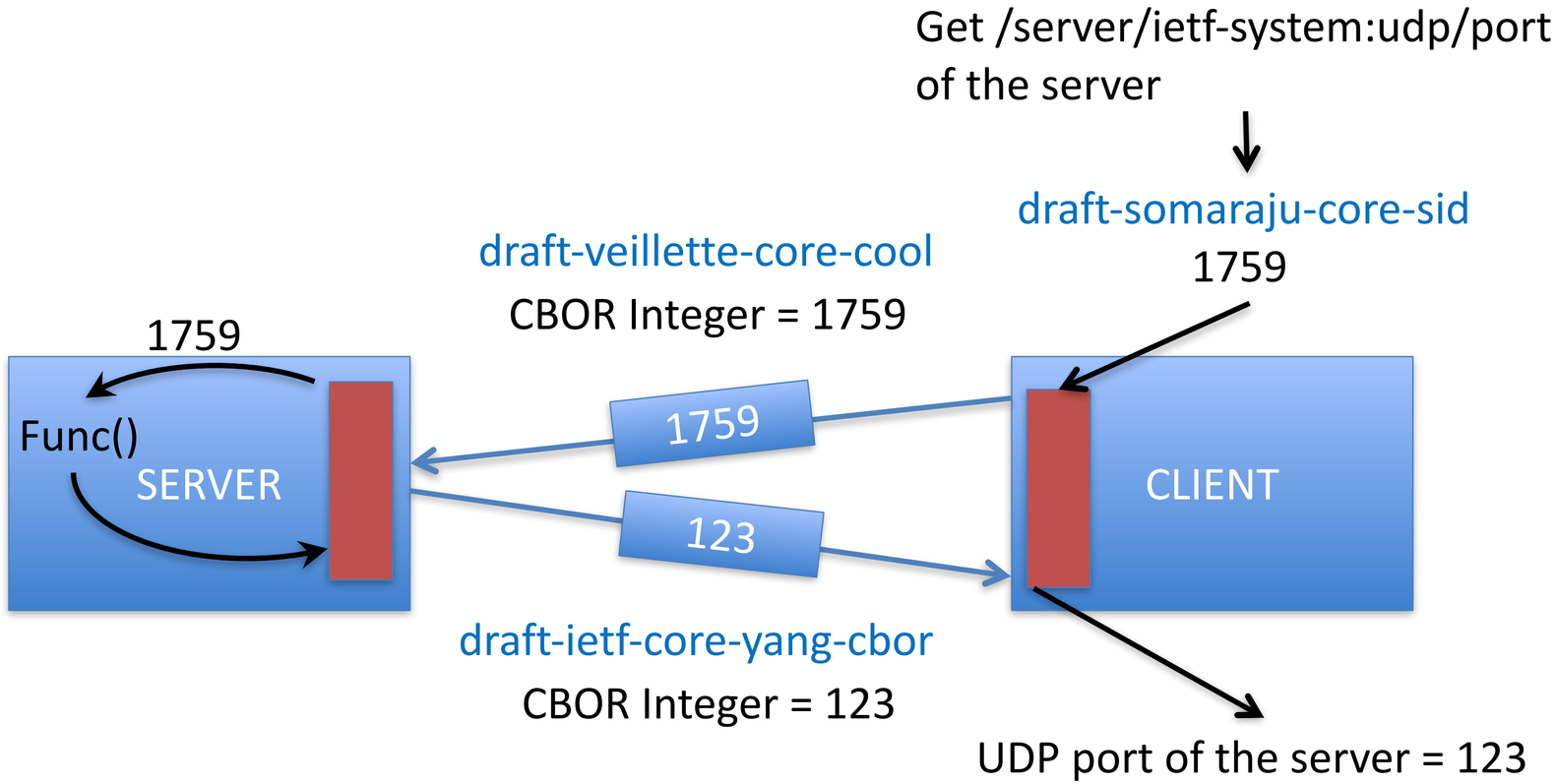
Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

1. Write your YANG module (contract) → YANG ecosystem
2. Compile to stub/lib, write your functional code → Implementation in progress
3. From YANG generate IDs (SID) for compression → Existing tools (e.g. pyang)
4. Deploy on servers and clients



5. Client discovers server, CoOL/CoMI root resource → /.well-known/core
6. Client discovers YANG modules on the server → I-D.veillette-core-cool-library
7. Normal operations (Commissioning, decommissioning, configuration update, notification, statistic gathering, logging, ad-hoc verification) → I-D.veillette-core-cool

Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>



Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander
Pelov <a@ackl.io>

Roadmap

Current targets

Encoding
I-D.ietf-core-yang-cbor

Identifiers
I-D.somaraju-core-sid

Protocol operations
I-D.veillette-core-cool

Discovery
I-D.veillette-core-cool-library

Registry, implementations

Future works

Security
- Boot strapping
- Authorization
(Profile of existing methods)

Protocol extensions
- Multicast
- Binding table
- Application management
- OTA upgrade

Support for LWM2M

Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

Questions #1

- What should be the name of the Protocol document?
  - CoOL (Constrained Objects Language)
  - CoMI (CoAP Management Interface)

Questions #2

- Should we remove the following items already present in I-D.veillette-core-cool-02 to address them in a future draft targeting protocol enhancements?
  - Support of multiple end points within the same server?
    Allows support of multiple entities accessed using a common server.
  - Support of a confirmed commit?
    Allows the automatic rollback of a configuration change if a confirmation is not performed within the specified delay.
  - Support of a scheduled commit?
    Allows a synchronized update of multiple network elements.

Thank you!

Michel Veillette

Alexander Pelov

Abhinav Somaraju

Randy Turner

Ana Minaburo

Laurent Toutain

Andy Biermann

Peter van der Stok

CBOR Encoding of Data Modeled with YANG

I-D.ietf-core-yang-cbor

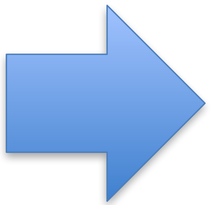
Michel Veillette
Alexander Pelov
Abhinav Somaraju
Randy Turner
Ana Minaburo

Goal

- To define the serialization rules to encode YANG data nodes in CBOR

YANG

Data model



CBOR

- I-D. ietf-netmod-yang-json performs the same task for JSON. The table of content of both drafts are similar.

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Data node encoding

YANG data node	Encoding
leaf	CBOR type as listed on next slide
container	CBOR map
leaf-list	CBOR array of CBOR type as listed on next slide
list	CBOR array of CBOR map
anydata	Any CBOR content conform to these rules
anyxml	Any CBOR content

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Data type encoding

YANG data node	Encoding
uint8, uint16, uint32 and uint64	CBOR unsigned integer
int8, int16, int32 and int64	CBOR unsigned integer / signed integer
decimal64	CBOR unsigned integer / signed integer
string	CBOR text string
boolean	CBOR simple value 'true' or 'false'
enumeration	CBOR unsigned integer
bits	CBOR byte string
binary	CBOR byte string
leafref	As specified by the 'path' YANG statement
identityref	CBOR unsigned integer OR CBOR text string
empty	CBOR simple value 'null'
union	bits, decimal64, enumeration, identityref and instance-identifier are tag to avoid ambiguities
instance-identifier	CBOR unsigned integer / array OR CBOR text string

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Delta encoding

- Use in YANG container and YANG list
- Allow reduction of message size

Delta = Current SID value – Base value

Base value = Parent in CBOR map | Previous sibling in CBOR array | 0

SID	Delta
{ 5243 : "v", 5245 : [{ 5246 : "v", 5251 : "v" }, { 5246 : "v", 5247 : "v", 5251 : "v" },], }	{ 5243 : "v", 5245 : [{ +1 : "v", +6 : "v" }, { +1 : "v", +2 : "v", +6 : "v" }], }

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Questions #1

- The fix decimal point datatype (decimal64) is currently encoded as a CBOR signed/unsigned integer.
  Should we use the CBOR Decimal Fractions?

```
273.15 encoded as :
   19 6ab3                 # 27315

or encoded as :
   C4                      # Tag 4
    82                     # Array of length 2
     21                    # -2
     19 6ab3               # 27315
```

- CBOR Decimal Fractions required 3 bytes or overhead
- The position decimal point is part of the YANG definition and may be considered unnecessary meta data.

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Questions #2

- The current draft support two types of identifiers, SID and name. For example:
  - an identityref can be set to either:

    "iana-if-type:ethernetCsmacd"

    1180
  - an instance-identifier can be set to either:

    "/ietf-system:system/authentication/user[name='bob']"

    [1726, "bob"]
- Should we keep only one type of identifier (SID)?

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Question #3

- A union of multiple enumeration or bits with overlapping values or positions won't work if they don't have the same meaning.
  Is it an issue?

```
leaf answer {
  type union {
    type enumeration { enum no { value 0; }  enum yes { value 1; } }
    type enumeration { enum non { value 0; }  enum oui { value 1; } }
    type enumeration { enum nein { value 0; }  enum ja { value 1; } }
  }
}
```

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Thank you!

Michel Veillette

Alexander Pelov

Abhinav Somaraju

Randy Turner

Ana Minaburo

Laurent Toutain

Andy Biermann

Peter van der Stok

Michel Veillette
<Michel.Veillette@trilliantinc.com>

Structured Identifier
draft-somaraju-core-sid

Abhinav Somaraju
Michel Veillette
Alexander Pelov
Randy Turner
Ana Minaburo

Structured Identifier (SID)

- Compact, globally unique identifier
- Fix, unaltered by revisions (modules, includes, imports)
- Assigned to YANG items
  - Modules & Submodules
  - Features
  - Data nodes
  - RPCs & Actions
  - Notifications
  - Identities
- Allocated by range
- Multiple disjoint ranges can be assigned to a module.

Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

.SID file

- Contain the list of SIDs assigned to a YANG module
- Used to maintain already assigned SIDs between revisions
- Used to share / publish SIDs
- Automated generation

```
> pyang --update-sid-file  toaster@2009-11-20.sid  toaster@2009-12-28.yang
File toaster@2009-12-28.sid updated
Number of SIDs available : 100
Number of SIDs assigned : 19
```

- Automated update

```
> pyang --generate-sid-file  20000:100  toaster@2009-11-20.yang
File toaster@2009-11-20.sid created
Number of SIDs available : 100
Number of SIDs assigned : 17
```

- Automated consistency check

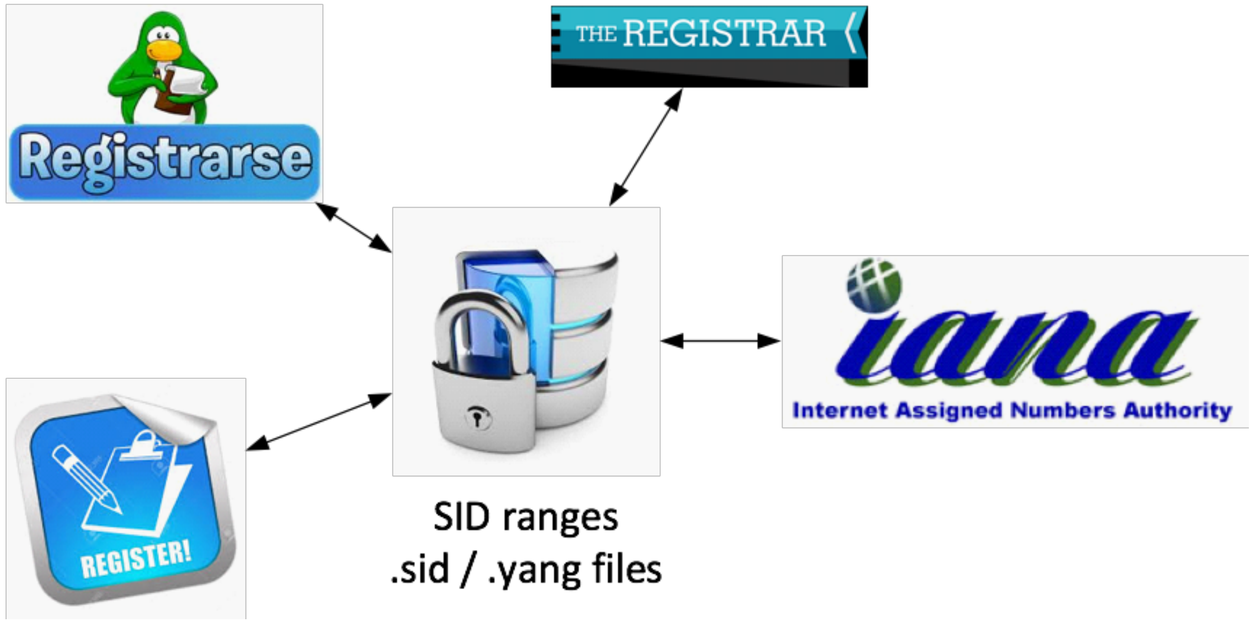
.SID file example

```
toaster@2009-12-28.sid
{
  "assignment-ranges": [
    { "entry-point": 20000, "size": 100 }
  ],
  "module-name": "toaster",
  "module-revision": "2009-12-28",
  "items": [
    { "type": "identity", "label": "toaster:frozen-bagel", "sid": 20000 },
    { "type": "identity", "label": "toaster:frozen-waffle", "sid": 20001 },
    { "type": "identity", "label": "toaster:hash-brown", "sid": 20002 },
    { "type": "identity", "label": "toaster:toast-type", "sid": 20003 },
    { "type": "identity", "label": "toaster:wheat-bread", "sid": 20004 },
    { "type": "identity", "label": "toaster:white-bread", "sid": 20005 },
    { "type": "identity", "label": "toaster:wonder-bread", "sid": 20006 },
    { "type": "identity", "label": "toaster:sourdough", "sid": 20017 },
    { "type": "node", "label": "/toaster", "sid": 20007 },
    { "type": "node", "label": "/toaster/toaster-manufacturer", "sid": 20008 },
    { "type": "node", "label": "/toaster/toaster-model-number", "sid": 20009 },
    { "type": "node", "label": "/toaster/toaster-status", "sid": 20010 },
    { "type": "node", "label": "/toaster/power-source/electric/voltage", "sid": 20018 },
    { "type": "notification", "label": "/toast-done", "sid": 20011 },
    { "type": "notification", "label": "/toast-done/toast-status", "sid": 20012 },
    { "type": "rpc", "label": "/cancel-toast", "sid": 20013 },
    { "type": "rpc", "label": "/make-toast", "sid": 20014 },
    { "type": "rpc", "label": "/make-toast/input/toaster-doneness", "sid": 20015 },
    { "type": "rpc", "label": "/make-toast/input/toaster-toast-type", "sid": 20016 }
  ]
}
```

Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

Proposed registration model

- Two registries
  - SID range
  - .sid and .yang files (Optional, to promote interoperability)
- Three layers or assignment (IANA, Registrar, Developer)
- Share registry information and validation using Blockchain?



Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

Question #1

- Is it ready for working group adoption?

Constrained Objects Language
Constrained Management Interface

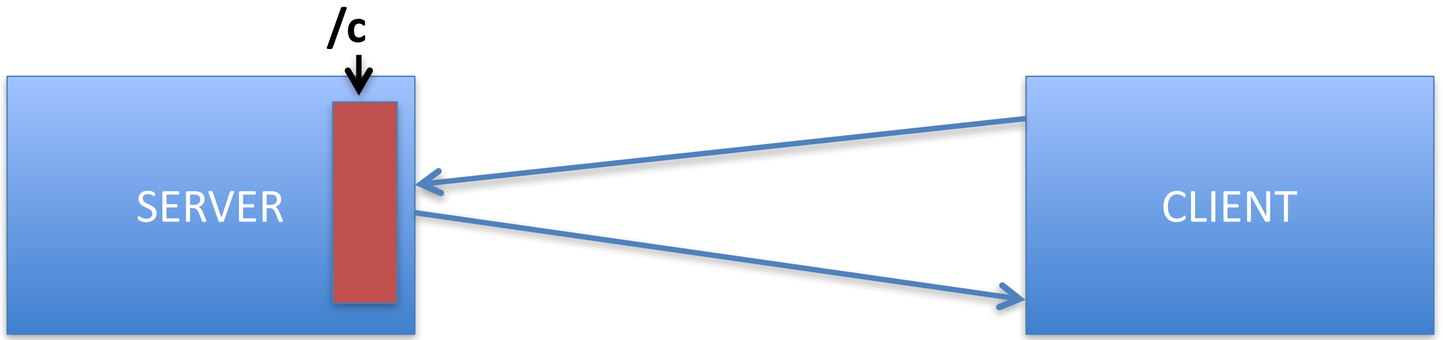
draft-veillette-core-cool

draft-vanderstok-comi

Michel Veillette
Alexander Pelov
Abhinav Somaraju
Randy Turner
Ana Minaburo
Peter van der Stok
Andy Biermann

Summary

	Description	**Use cases**
GET /c	Retrieve config, non-config or all	Backup, walk all available info
PUT /c	Set configuration	Restore, Provisioning
FETCH /c	Retrieve specific data nodes	Statistic gathering, Diagnostic
iPATCH /c	Update specific data nodes	Configuration update
POST /c	Execute RPC or Action	Complex operations not efficiently implementable using FETCH and iPATCH
GET /e	Notification	Event or alarm



Default handling

- Normal behaviour (trim)
  Defaults are not transmitted
- Query parameter 'a' (report-all)
  Force transmission of all instances

Observe

- 'observe' CoAP option is supported to retrieve a time series of a specific data node.
- Coincidental values may be included in each report.

```
FETCH /c Content-Format(application/cool-instance-id-list+cbor) Observe(0)
[ [1751, "tic.nrc.ca"], -3 ]

2.05 Content Content-Format(application/cool-value-pairs+cbor) Observe(2631)
[
  false,                # enabled (SID 1751)
  "tic"                 # hostname (SID 1748)
]
```

Observed

Coincidental

Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

Content-Format

- Four Content-Format are supported

Content-Format	Description
application/cool-value+cbor	value
application/cool-value-list+cbor	CBOR array [value]
application/cool-instance-id-list+cbor	CBOR array [instance-identifier]
application/cool-value-pairs+cbor	CBOR array [instance-identifier, value]

Note:
"value" and "instance-identifier" are serialized based on the rules defined in I-D.ietf-core-yang-cbor

Content-Format

- Context of use

	Request	**Response**
GET /c		application/cool-value-pairs+cbor
PUT /c	application/cool-value-pairs+cbor	
FETCH /c	application/cool-instance-id-list+cbor	application/cool-value+cbor application/cool-value-list+cbor
iPATCH /c	application/cool-value-pairs+cbor	
POST /c	application/cool-value-pairs+cbor	application/cool-value+cbor
GET /e		application/cool-value-pairs+cbor

GET example

GET /c

```
2.05 Content Content-Format(application/cool-value-pairs+cbor)
[
  1533,                                    # interface (SID 1533)
    {
     +4 : "eth0",                          # name (SID 1537)
     +1 : "Ethernet adaptor",              # description (SID 1534)
     +5 : 1179,                            # type (SID 1538), identity ethernetCsmacd
     +2 : true                             # enabled (SID 1535)
    },
  +184,                                    # clock (SID 1717)
    {
      +1 : "2015-02-08T14:10:08Z09:00",    # boot-datetime (SID 1718)
      +2 : "2015-04-04T09:32:51Z09:00"     # current-datetime (SID 1719)
    },
  +19, 60                                  # timezone-utc-offset (SID 1736)
]
```

FETCH example

FETCH /c Content-Format(application/cool-instance-id-list+cbor)
[[1534, "eth0"]]

2.05 Content Content-Format(application/cool-value+cbor)
"Ethernet adaptor"

Michel Veillette <Michel.Veillette@trilliantinc.com> Alexander Pelov <a@ackl.io>

Question #1

- The last version proposes four Content-Formats instead of a single one.

Right approach?

Question #2

- In order to minimize the payload size of FETCH responses
  - instance-identifiers requested are elided, those need to be maintained in the context of the client
  - CBOR array is not used for single values

Acceptable optimization?

All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

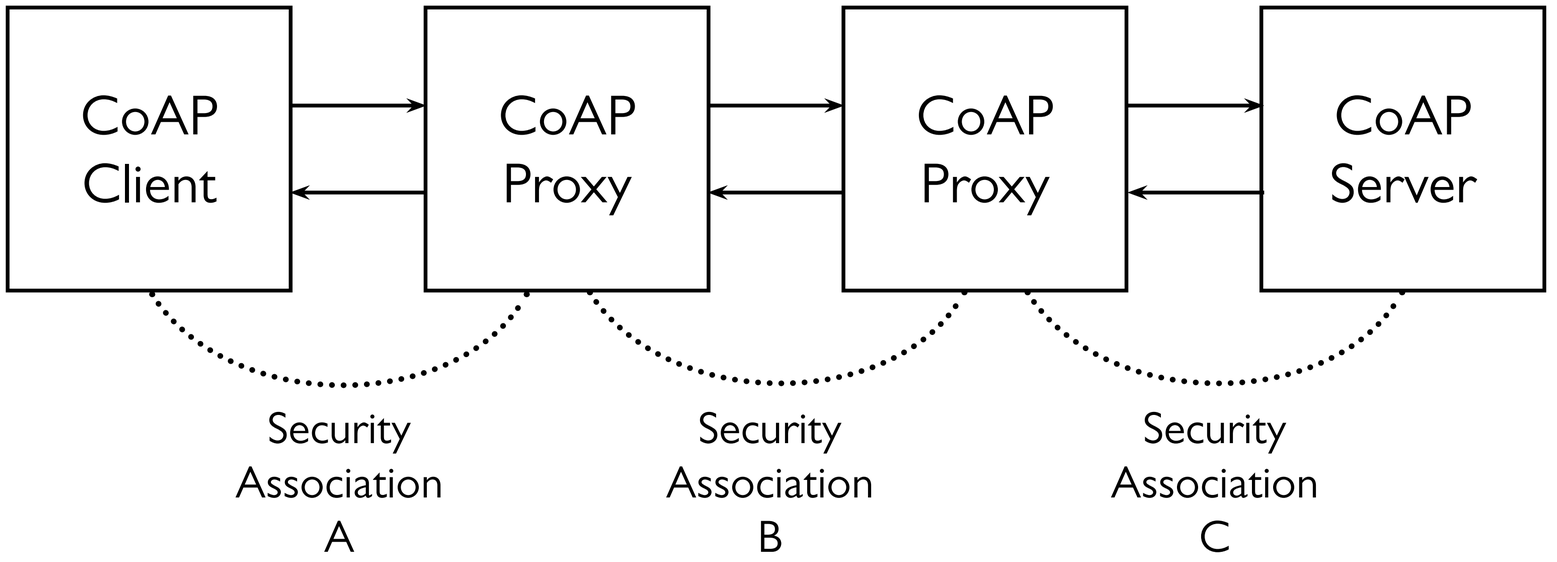
Requirements for CoAP End-To-End Security

draft-hartke-core-e2e-security-reqs

Göran Selander
Francesca Palombini
Klaus Hartke

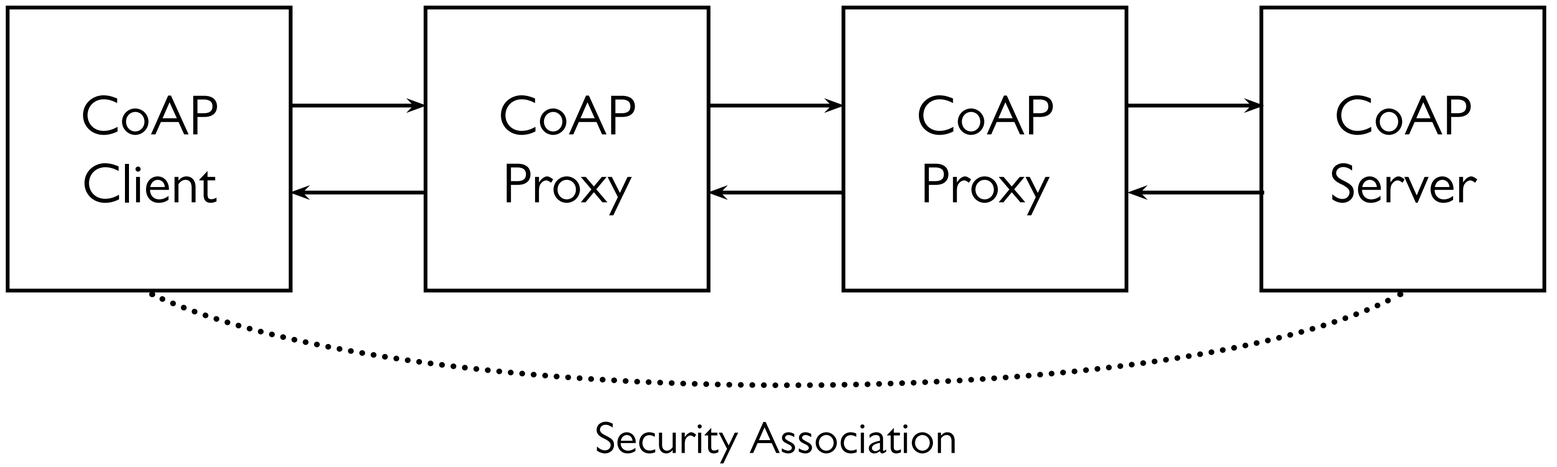
IETF 96 • 2016/07/21

Hop-by-Hop Security:



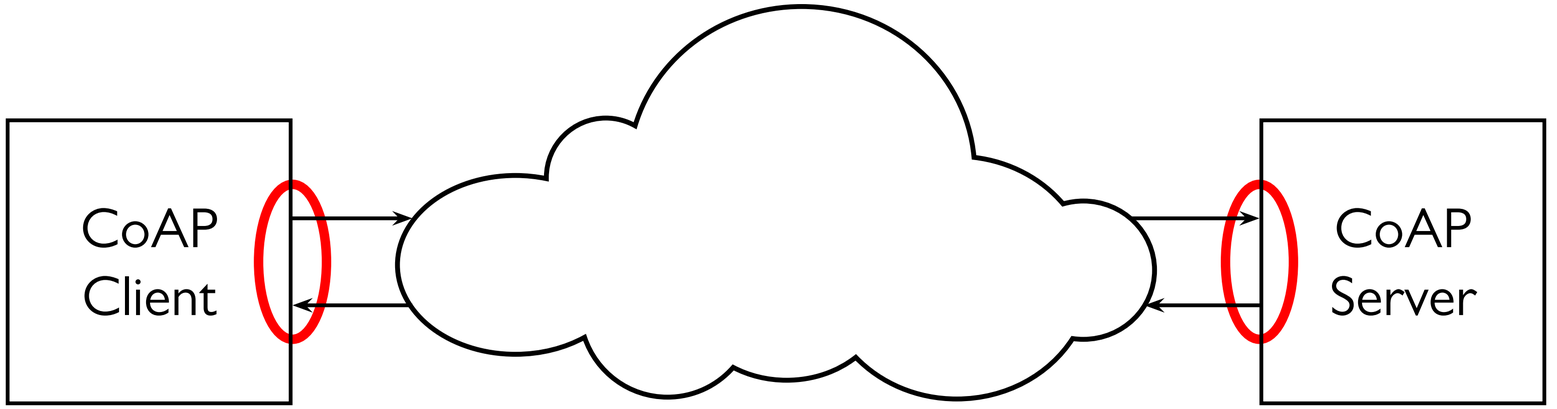
- DTLS provides hop-by-hop security at the application layer
- The communication between each pair of hops is secured, but each hop can arbitrarily create, read, modify, delete messages

End-to-End Security:



- The communication between client and server is secured, but messages are exchanged through proxies as usual
- Each proxy must create, read, modify, delete messages only as required, but not more

Threats and Security Requirements



Threat	*Mitigation*
• Spoofing	REQUIRED
• Delaying	REQUIRED
• Withholding	OPTIONAL
• Flooding	OPTIONAL
• Eavesdropping	REQUIRED *
• Traffic Analysis	OPTIONAL

Security Solutions

* Solutions need to find a **trade-off** between proxy functionality (such as caching) and the level of protection (i.e., what parts of messages can be integrity- and confidentiality-protected)

The draft presents two exemplary choices:

- The first provides a high protection level by tying requests and responses uniquely together and confidentiality-protecting as much as possible, at the cost of reduced proxy functionality.
- The second preserves proxy functionality as much as possible, at the cost of reduced confidentiality protection.

Next Steps

- Need reviews
  - Did we get it right?
  - Is something missing?
- Adoption as a working group document

Object Security of CoAP (OSCOAP)

draft-selander-ace-object-security-05

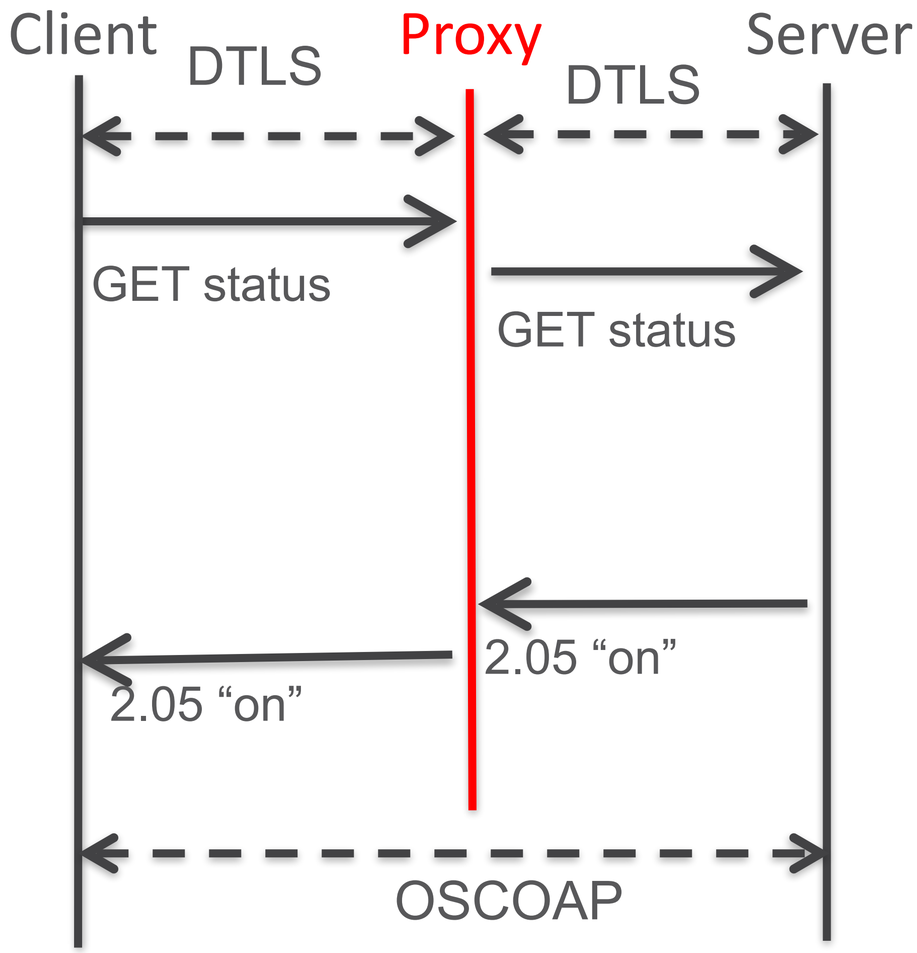
CAPITALS

Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

IETF 96, CORE WG, Berlin, Jul 21, 2016

OSCOAP

- OSCOAP defines a method for in-layer security of CoAP message exchanges using the COSE format.
- Independent of how CoAP is transported (UDP, TCP, Bluetooth, 802.15.4 IE, foo…)
- OSCOAP protects CoAP end-to-end and can be used instead of DTLS
  - Allows legitimate proxy operations
  - Detects illegitimate proxy operations
- Requirements: draft-hartke-core-e2e-security-reqs



What’s next

From IETF 95 – Buenos Aires

- Include Blockwise
- CoAP over TCP
- New implementations in progress
- Release as open source
- ACE profiles based on OSCOAP

for Embedded font:
,-./0123456789:;<=>?
GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
wxyz{|}~¡¢£¤¥¦§¨©ª«¬®¯°±²³
ÁÂÃÄÅÆÇÈËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâã
íîïðñòóôõö÷øùúûüýþÿĀāĂăąĆćĊċČĎďĐđĒĖėĘ
ġĪīĮįİıĶķĹĺĻļĽľŁłŃńŅņŇňŌŐőŒœŔŕŖŗŘřŚśŞşŠ
ŰűŲųŴŵŶŷŸŹźŻżŽžƒȘșˆˇ˘˙˚˛˜˝ẀẁẃẄẅỲỳ–
‰‹›⁄
ĄĆĆĊĊČČĎĎĐĐĒĒĖĖĘĘĚĚĞĞĠĠĢĢĪĪĮĮİĶĶ
ŅŅŇŇŌŌŐŐŔŔŖŖŘŘŚŚŞŞŢŢŤŤŪŪŮŮŰŰŲŲ
ŻȘș−≤≥fifl
ΩΐΑΒΓΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΪΫΆΈΉΊΰα
λνξορςΣΤΥΦΧΨΩΪΫΌΎΏ
ьЊЋЌЎЏАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЁЂЃЄЅІЇЈЉЊЋЌЎЏѢѣѲѳѴѵҐґəǽẀẁẂẃẄẅ

What’s done

› Include Blockwise ✓

as described at IETF95.

for Embedded font:
,-./0123456789:;<=>?
GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
wxyz{|}~¡¢£¤¥¦§¨©ª«¬¬®¯°±²³
ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâã
ïïðñòóôõö÷øùúûüýþÿĀāĂăĄąĆćĈĉĊċČčĎďĐđĒēĖęĚ
ĞğĠġĢģĤĥĦħĨĩĪīĬĭĮįİıĲĳĴĵĶķĹĺĻļĽľĿŀŁłŃńŅņŇňŊŋŌōŎŏŐőŒœŔŕŖŗŘřŚśŞşŠ
ŰúŲųŴŵŶŷŸŹźŻżŽžƒˆˇ˘˙˚˛˜˝‘’‚“”„‹›
‰∞‹›∕
ĄĆĈĊČĎĐĒĖĘĚĜĞĠĢĤĦĨĪĬĮİĲĴĶĸ
ŃŅŇŊŌŎŐŔŖŘŚŜŞŠŢŤŦŨŪŬŮŰŲ
ŹŻŞş−≤≥fiflˆ

ΩΐΑΒΓΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΪΫΆΈΉΊΰα
λνξορςΣΤΥΦΧΨΩΪΫΟΥΩ

ЬЊЋЎЏАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЁЂЃЄЅІЇЈЉЊЋЎЏЪЂЄΘVVΓΎəæŴŵẂẁẄẅ

What’s done

› Include Blockwise ✓
› (OS)CoAP over TCP ✓

Complies with [draft-ietf-core-coap-tcp-tls-03]

for Embedded font:
,-./0123456789:;<=>?
GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
wxyz{|}~¡¢£¤¥¦§¨©ª«¬®¯°±²³
ÁÂÃÄÅÆÇÈËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâã
íîïðñòóôõö÷øùúûüýþÿĀāĂăąĆćĊċČĎďĐđĒĖėĘ
ġĪīĮįİıĶķĹĺĻļĽľŁłŃńŅņŇňŌŐőŒœŔŕŖŗŘřŚśŞşŠ
ŰűŲųŴŵŶŷŸŹźŻżŽžƒȘșˆˇ˘˙˚˛˜˝ẀẁẃẄẅỲỳ–
‰‹›⁄
ĄĆĆĊĊČČĎĎĐĐĒĒĖĖĘĘĚĚĞĞĠĠĢĪĪĮĮİĶ
ŅŅŇŇŌŌŐŐŔŔŖŖŘŘŚŚŞŞŢŢŤŤŪŪŮŮŰŰŲŲ
ŻȘș−≤≥ﬁﬂ

ΏΐΑΒΓΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΪΫΆΈΉΊΰα
λνξορςΣΤΥΦΧΨΩΪΫΌΎΏ
ЊЋЌЎЏАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЁЂЃЄЅІЇЈЉЊЋЌЎЏѢѣѲѳѴѵҐґәǽẀẁẂẃẄẅ

What’s done

- Include Blockwise ✓
- OSCOAP over TCP ✓
- New implementations in progress ✓
- Release as open source ✗✓

https://github.com/joakimb/OSCoAP

for Embedded font:
,-./0123456789:;<=>?
GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
wxyz{|}~¡¢£¤¥¦§¨©ª«¬¬®¯°±²³
ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâã
ïîïðñòóôõö÷øùúûüýþÿĀāĂăĄąĆćĈĉĊċČčĎďĐđĒēĔĕĖ
ĜĝĞğĠġĢģĤĥĦħĨĩĪīĬĭĮįİıĲĳĴĵĶķĹĺĻļĽľĿŀŁłŃńŅņŇňŊŋŌōŎŏŐőŒœŔŕŖŗŘřŚśŞşŠ
ŰúŲųŴŵŶŷŸŹźŻżŽžƒˆˇ˘˙˚˛˜˝‘’‚“”„‹›⁄
‰∂∆∏∑−√≈∙
ĄĆĈĊČĎĐĒĔĖĘĚĜĞĠĢĤĦĨĪĬĮİĲĴĶĸĹĻĽĿŁŃŅŇŊŌŎŐŒŔŖŘŚŜŞŠŢŤŦŨŪŬŮŰŲ
ŹŻŽŞ–≤≠fifl

ΩΐΑΒΓΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΪΫΆΈΉΊΰα
λνξορςΣΤΥΦΧΨΩΪΫΟΥΩ

ЬЊЋЎЏАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЁЂЃЄЅІЇЈЉЊЋЎЏЪЂЄΘVVΓΎəæŴŵẂẁẄẅ

What’s done

- Include Blockwise ✓
- OSCOAP over TCP ✓
- New implementations in progress ✓
- Release as open source ✗✓
- ACE profiles based on OSCOAP ✓

draft-seitz-ace-ocsoap-profile-00

Where are we now

- Draft is stable
  - https://github.com/EricssonResearch/OSCOAP
- Positive feedback
  - Considered for use in 6tisch and for secure multicast
- More reviews committed
- Implementation in progress
- WG support?

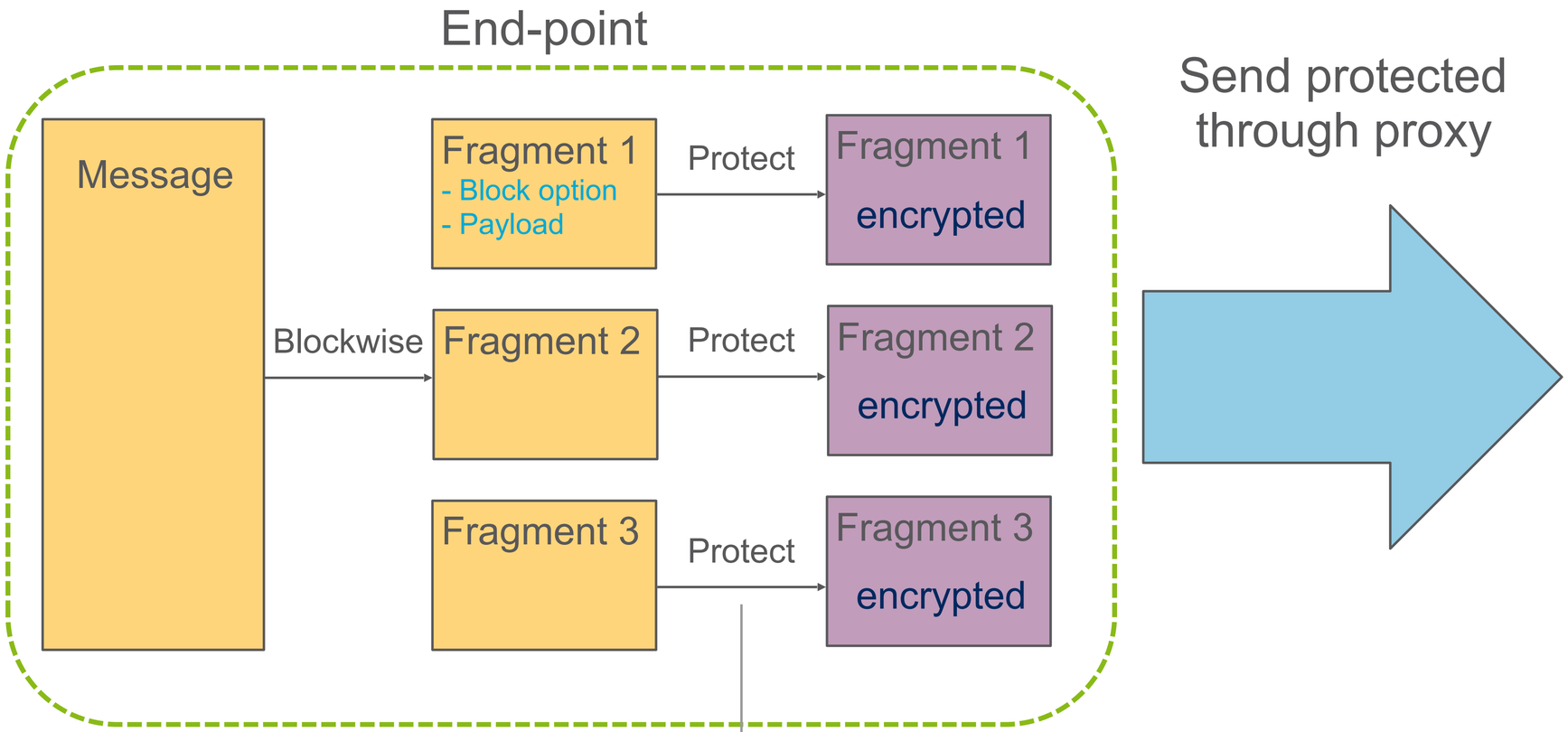
Thank you!

Comments/questions?

What’s done

› Include Blockwise ✓

Duplicate options:
- **End-to-end protected within the COSE object**
- Proxy-generated unprotected

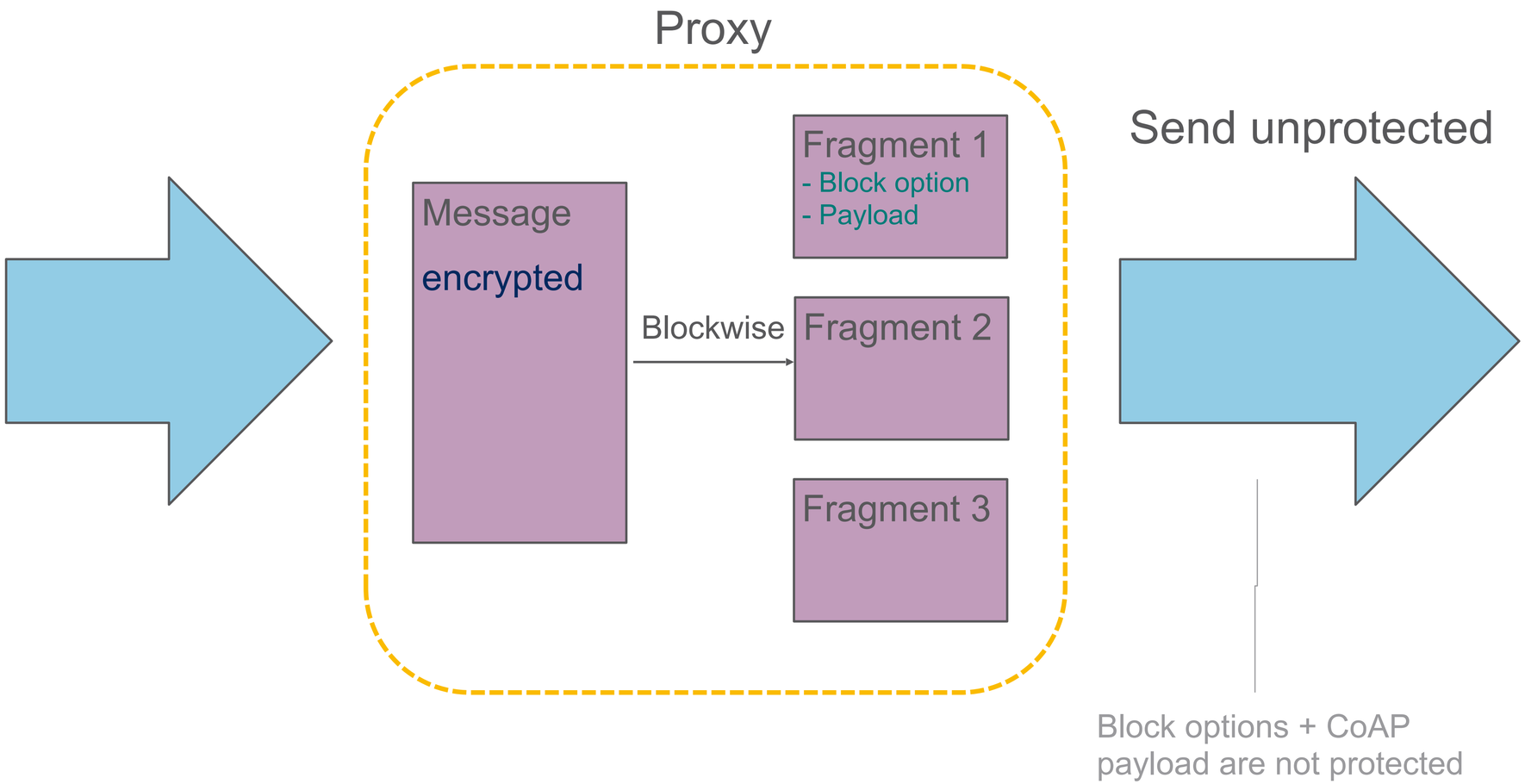


- Block options + CoAP payload are protected within the COSE object.
- The fragments are cryptographically linked.
- Applications must define a policy for maximum size of Fragments.

What’s done

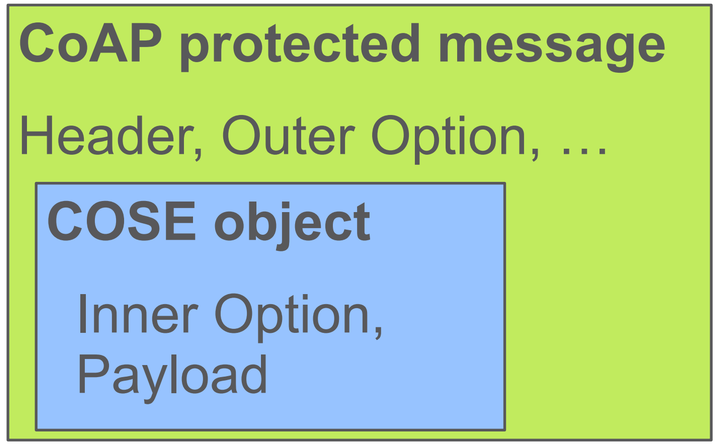
› Include Blockwise ✓

Duplicate options:
- End-to-end protected within the COSE object
- **Proxy-generated unprotected**



Duplicate options

- Encrypted options are carried in the COSE object
- We introduce **Duplicate of an option** which is in the Options part of the CoAP protected message.



- In version -05:
  - Max-age
  - Observe
  - Block* and Size*

- One instance is sent encrypted (“Inner” option) the other in clear (“Outer” option)
  - “Inner” and “Outer” relative to the secure COSE object
- The Inner option value is intended for the end-point, the Outer option value is intended for the proxy

Blockwise

Block* and Size* are Duplicate options

- The endpoint can fragment and protect each block with OSCOAP. The Block* option are encrypted (Inner Block* option)
- A proxy can fragment each protected OSCOAP message, thus adding an unprotected option (Outer Block* option)
- The “Inner” and “Outer” options are **independent**

- Adding a policy for maximum size of the inner fragments prevents an adversary from adding outer options and sending fragments ad infinitum.
- The inner blocks need to be cryptographically linked

for Embedded font:
,-./0123456789:;<=>?
GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
wxyz{|}~¡¢£¤¥¦§¨©ª«¬®¯°±²³
ÁÂÃÄÅÆÇÈËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâã
íîïðñòóôõö÷øùúûüýþÿĀāĂăąĆćĊċČĎďĐđĒĖėĘ
ġĪīĮįİıĶķĹĺĻļĽľŁłŃńŅņŇňŌŐőŒœŔŕŖŗŘřŚśŞşŠ
ŰűŲųŴŵŶŷŸŹźŻżŽžƒȘș˘˙˚˛˜˝ẀẁẃẄẅỲỳ–
‰‹›⁄
ĄĆĆĊĊČČĎĎĐĐĒĒĖĖĘĘĚĚĞĞĠĠĢĢĪĪĮĮİĶĶ
ŅŅŇŇŌŌŐŐŔŔŖŖŘŘŚŚŞŞŢŢŤŤŪŪŮŮŰŰŲŲ
ŻŞș–≤≥ﬁﬂ
ΏΐΑΒΓΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΪΫΆΈΉΊΰα
λνξορςΣΤΥΦΧΨΩΪΫΌΎΏ
ЉЊЋЌЎЏАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЁЂЃЄЅІЇЈЉЊЋЌЎЏѢѣѲѳѴѵҐґәӕẀẁẂẃẄẅ

Alignment with existing work:

- Alignment with COSE (draft-ietf-cose-msg-14)
  - COSE object
  - Security Context derivation
  - AEAD ciphers, nonce construction

Java implementation

- Californium: a CoAP Java implementation*
- OSCOAP: patch for Californium, easy to maintain
  https://github.com/joakimb/OSCoAP
- Dependencies: COSE Java implementation (that uses CBOR and tinyDTLS)

* http://www.eclipse.org/californium/

C implementation

- Erbium CoAP: a CoAP library in Contiki OS*
- OSCOAP: new App for Contiki

- Implementation based on v-04, with some differences:
  - No protected Observe option
  - No sliding window for sequence numbers

- Dependencies: COSE-C implementation (that uses CN-CBOR and adapted to use mbedTLS AES-CCM-64-64-128)
  - COSE-C is not optimized for embedded devices: large buffers are used. Some optimizations was done, to use one buffer only.

* http://people.inf.ethz.ch/mkovatsc/erbium.php

All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

SenML

draft-ietf-core-senml-02

V2

Changes since draft-jennings-core-senml-06

- Significant clean up of units registry
- For ratios from 0 to 1, recommend a unit of / not %. Kept old symbol but it is not recommended for future use
- Changed the prefered unit of mass from g to kg to match SI

Extensibility

- Need to ensure we have adequate extensibility
- Need to check that extensibility allows what we want to do with links

SenML value extensions

- Currently: must be exactly one of the defined value labels {v, vb, vd, vs}
- New v* values can not exist alone in SenML Record
- Proposal: relax that rule to say that "**at most** one value label must be in each record"
  - The label may be defined in some future document
  - In the Label registry defines if a label is "value label"; starts with "v"?
- Or even: Exclusively only value or base values in the first Record? Same as "optional base record"

Metadata

- Free-form UTF-8 text, like string value (sv)
- Unlike sv, you can have this **and** a value

- Original proposal: new "m" and "bm" Labels with UTF-8
- Or: no metadata in-line, only e.g. web-links that describe the resources
  - Metadata is much more static than values

URI Semantics for (base)names

- Currently: simple string concatenation
- Proposal: URI semantics for names
  - "/b" + "thing" -> "/thing"
  - "/b/" + "my/thing" -> "/b/my/thing"
  - "/b/" + "/name" -> "/name"
  - "/b/" + "coap://x/" -> "coap://x/"
  - "http://otherdevice/" + "/p/t" -> "http://otherdevice/p/t"

Base Stride

- Elide time value for measurements that have been done at equal intervals

Current

```
"bt": 1320067464,
"bu": "%RH",
"v": 21.2, "t": 0 },
{ "v": 21.3, "t": 10 },
{ "v": 21.4, "t": 20 },
{ "v": 21.4, "t": 30 },
```

Proposed

```
"bt": 1320067464,
"bs": 10,
"bu": "%RH",
 "v": 21.2},
 { "v": 21.3},
 { "v": 21.4},
 { "v": 21.4},
 ...
```

Other issues

- Content types per Record?
- Object values?
  - Do we want to have extensibility to nested objects?

Minor Open Issue

Do we have different types of counts in the units “rpm” & “bpm” are both a rate count widely used

Proposal: Would “measure” would be a better name than “Units”

Other Work Needed

- Normalize JSON formatting in examples
- Add a few missing example to illustrate bulk of features
- Various small fixes at https://github.com/core-wg/senml-spec/issues
- Update relaxNG to support extensibility
- Example(s) with an actuator

All times are in time-warped CEST

Thursday

- 16:20–16:25 Intro
- 16:25–16:40 Core Interfaces (CG/MK)
- 16:40–17:25 Management over CoAP (COMI/COOL)
  - 16:40–16:50 Roadmap
  - 16:50–17:05 YANG over CBOR
  - 17:05–17:15 SIDs
  - 17:15–17:25 COMI/COOL
- 17:25–17:45 Object Security 2 (KH, GS)
- 17:45–17:55 SenML (AK)
- 17:55–18:05 Pubsub (MK)
- 18:05–18:15 Congestion Control (CG)

draft-core-koster-coap-pubsub

Publish/Subscribe Broker for CoAP

Recent Updates

- Defined "brokerless" pubsub
  - Two or more nodes may directly communicate with each other using CoAP Pubsub
  - Pubsub nodes may assume both client and broker roles
  - A node exposing a broker may have internal access to create, publish, and subscribe to its own topics
  - Initial definition, may need more description
- Added topic discovery methods
  - Broker may expose topics in .well-known/core
  - Broker may register topics to a resource directory using "pull" pattern triggered by an empty POST to the RD .well-known/core location

Possible Future Extensions

- Add support for PATCH
  - Use pubsub to forward PATCH payloads
  - Clients use a patch content format
- Add queueing of messages using POST
  - Add representations to a collection for queuing
  - Define behavior using an Interface Type (?if=)
- Optional, server could return 4.xx code if not supported

Status

- Good interest, many requests for information from large service providers, etc.
- A few implementations exist
- A few open conversations: OCF Cloud, Amazon, others
- Good time to look at stabilizing the draft, limit new features, and drive toward completion