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**

✓Blue sheets
✓Scribe(s)

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 8179.

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 8179 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.

I E T F

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

Agenda Bashing

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

All times are in time-warped CEST

Friday (90 min)

- **11:50–11:55 Intro, Agenda**
- **11:55–12:10 Post-WGLC: SenML**
- **12:10–12:40 WG doc: RD, RD-DNS-SD**
- **12:40–12:50 WG doc: pubsub**
- **12:50–13:20 WG doc: oscoap**

draft-ietf-core-etch
→ RFC 8132

Published 2017-04-07

Advertisements

- DNSSD WG today (Wed) 15:20–16:50
- YOT (Yang of Things) Thu 10:00–12:00

Milestones (from WG charter page)

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

Mar 2017	CoRE Interfaces submitted to IESG draft-ietf-core-interfaces
Dec 2016	Management over CoAP submitted to IESG for PS draft-vanderstok-core-comi , draft-veillette-core-cool
Dec 2016	CBOR Encoding of Data Modeled with YANG submitted to IESG for PS draft-ietf-core-yang-cbor
Done	**CoAP over TCP, TLS, and WebSockets submitted to IESG for PS draft-bormann-core-coap-tcp**
Sep 2016	CoRE Resource Directory submitted to IESG for PS draft-ietf-core-resource-directory
Done	**WG adoption for Management over CoAP draft-vanderstok-core-comi draft-veillette-core-cool**
Aug 2016	Media Types for Sensor Measurement Lists (SenML) submitted to IESG for PS draft-ietf-core-senml
Done	**Patch and Fetch Methods for CoAP submitted to IESG for PS draft-ietf-core-etch**
Aug 2016	Representing CoRE Link Collections in JSON submitted to IESG draft-ietf-core-links-json
Done	**Best Practices for HTTP-CoAP Mapping Implementation submitted to IESG — RFC 8075**
Done	**Blockwise transfers in CoAP submitted to IESG — RFC 7959**

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

Using URIs With Multiple Transport Stacks

draft-thaler-appsawg-multi-transport-uris-01

Dave Thaler <dthaler@microsoft.com>

Some Recent Requests for URI Schemes

- CoRE WG (draft-ietf-core-coap-tcp-tls-07) asked for Permanent registration of coap+tcp, coaps+tcp, coap+ws, coaps+ws (in addition to existing coap and coaps)
- Open Connectivity Foundation supported the CoRE WG request, and requested Provisional assignment if IETF declined to register them itself
- OPC Foundation asked for Permanent registration of opc.tcp, opc.amqp, and opc.wss

- Lots of debate ensued around exposing the same resource over multiple transport stacks, especially since HTTP is taking a different approach
  - This draft documents the arguments, tradeoffs, and use cases discussed so far
  - Goal is Informational RFC

The Problem…

- Lots of cases exist today where two URIs for same resource differ only in URI scheme, or authority, or path
- “Architecture of the WWW” argues for minimizing such cases since interferes with valuation and correlation of links/resources
  - But encourages use in some cases (e.g., secured vs unsecured)
- RFC 3986 (URI syntax) similarly argues for minimizing, but does not disallow
  - Indeed, ladder levels of comparison explicitly allow for it
- RFC 7595 (Scheme registration process) gives list of Requirements for Permanent Schemes, but this topic is not one of them (hence implicitly allowed)

Example Use Case

- Application layer protocol supports multiple transports (COAP, HTTP, Bluetooth?, other), and defines a transport-agnostic URI, e.g.
  - **ocf://<hash of public key>/rest/of/uri**
- But need a way to resolve actual transport endpoints
  - Some transports (e.g., websockets, HTTP, coap, …) already have URIs defined
  - For consistency, *convenient* to express them all as URIs
- Resolution might be via some lookup step, or (as in the case of OCF) learned in the same message as the app-layer URI is learned
- But the same thing can happen at multiple layers (OCF over COAP over TCP …) so general problem is not just one id/locator level split
  - OCF defined discovery one level down from ocf: URI, with no hard dependency on DNS or other servers

/oic/res


```
[
 { "href": "/oic/res",
   "anchor": "ocf://dc70373c-1e8d-4fb3-962e-017eaa863989/oic/res",
   "rel": "self",
   "rt": ["oic.wk.res"],
   "if": ["oic.if.ll", "oic.if.baseline"],
   "p": {"bm": 3},
   "eps": [{"ep": "coaps://[fe80::b1d6]:44444"}] },
 { "href": "/oic/p",
   "anchor": "ocf://dc70373c-1e8d-4fb3-962e-017eaa863989",
   "rt": ["oic.wk.p"],
   "if": ["oic.if.r", "oic.if.baseline"],
   "p": {"bm": 3},
   "eps": [{"ep": "coaps://[fe80::b1d6]:44444"}, {"ep": "coaps+tcp://[fe80::b1d6]:11111"} ] },
 { "href": "/oic/d",
   "anchor": "ocf://dc70373c-1e8d-4fb3-962e-017eaa863989",
   "rt": ["oic.wk.d", "oic.d.light"],
   "if": ["oic.if.r", "oic.if.baseline"],
   "p": {"bm": 3},
   "eps": [{"ep": "coaps://[fe80::b1d6]:44444"}, {"ep": "coaps+tcp://[fe80::b1d6]:11111"} ] },
 { "href": "/myLight",
   "anchor": "ocf://dc70373c-1e8d-4fb3-962e-017eaa863989",
   "rt": ["oic.r.switch.binary"],
   "if": ["oic.if.a", "oic.if.baseline"],
   "p": {"bm": 3},
   "eps": [{"ep": "coaps://[fe80::b1d6]:44444"}, {"ep": "coaps+tcp://[fe80::b1d6]:11111"} ] }
]
```


Target URIs do not include locator info

Endpoints for each target resource (in URI syntax)

Discovery vs Selection

- **Discovery:** resolution of a URI to a set of potential transport endpoints
- **Selection:** process of selecting an appropriate endpoint to use from among the discovered set

- Most of the draft is about *discovery*, but also includes a section on *selection* (sorting algorithms, Happy Eyeballs style algorithms, etc.)

Discussion of 4 discovery approaches (1/2)

1. Specified by URI scheme definition, never custom. Example: tftp:
   - Avoids dependency on any other mechanism for discovery
   - No support for non-default endpoint info
   - Adding a transport later might be difficult due to hard coded assumptions
2. Encoded somewhere in a single URI
   - Avoids dependency on any other mechanism for discovery
   - Ports might be problematic:
     - Ephemeral ports (and in theory IANA ports allocated at different times) can vary by transport protocol
     - No natural place to put a transport-agnostic service name in URI
   - If complex stacks or larger or dynamic sets, problematic to try to encode into a common immutable URI

Discussion of 4 discovery approaches (2/2)

3. Use a set of URIs, one per transport stack
   - Results in multiple “equivalent” URIs so often needs a higher layer URI that acts like an ID where the set of URIs are locators
   - Still problematic if can have complex stacks with multiple layers
   - Only “natural” place is to vary by URI scheme
4. Use a locator format that might not be URI and some mechanism to learn them
   - Disadvantage may be lack of consistent syntax across transports, complicating discovery syntax

Next Steps

- AD-sponsored? Some WG? Something else?

- (Currently no plan to update RFC 7595, or requirements for permanent registration)

The coap-tcp URI-Scheme Gordian Knot

- –07: In addition to coap:// (RFC 7252) for UDP, add coap+tcp:// and coap+ws://
  (the analogs for coaps are always implied here).
- –09: Try to appease IESG concerns by mapping coap:// to all three transports
  - Unfortunately: Unworkable
- –10-to-be: Revert to –07, but also add a coap+at://
  (all transports) that plays the role coap:// would have played in –09; define the rules in a bit more detail

CoAP Protocol Negotiation

draft-silverajan-core-coap-protocol-negotiation

Bill Silverajan TUT
Mert Ocak Ericsson

Summary of changes

- Until -03
  - Used .well-known/core to expose CoAP origin server's available alternative transports
- From -04
  - Using .well-known/core was discontinued owing to concerns about CoRE Link format violations
  - Usage of CoRE Resource Directory was proposed, with two new optional RD parameters
  - But WG also asked to explore non-RD scenarios

In -06

- Several ways of achieving that were considered
- Introducing a new CoAP Option was the optimal choice to allow clients to discover alternative transports on origin servers

Proposal in -06:
CoAP Option “Alternative-Transports”

No.	C	U	N	R	Name	Format	Length	Default
66		x	-	x	Alternative-Transports	string	0-1034	(none)

C=Critical, U=Unsafe, N=No-Cache-Key, R=Repeatable

- Used bidirectionally between client and origin server
- Flexible means to discover multiple transports
- Functional equivalence to using an RD for transport discovery

RD Registration and Lookups

- Registration Request from origin server to RD

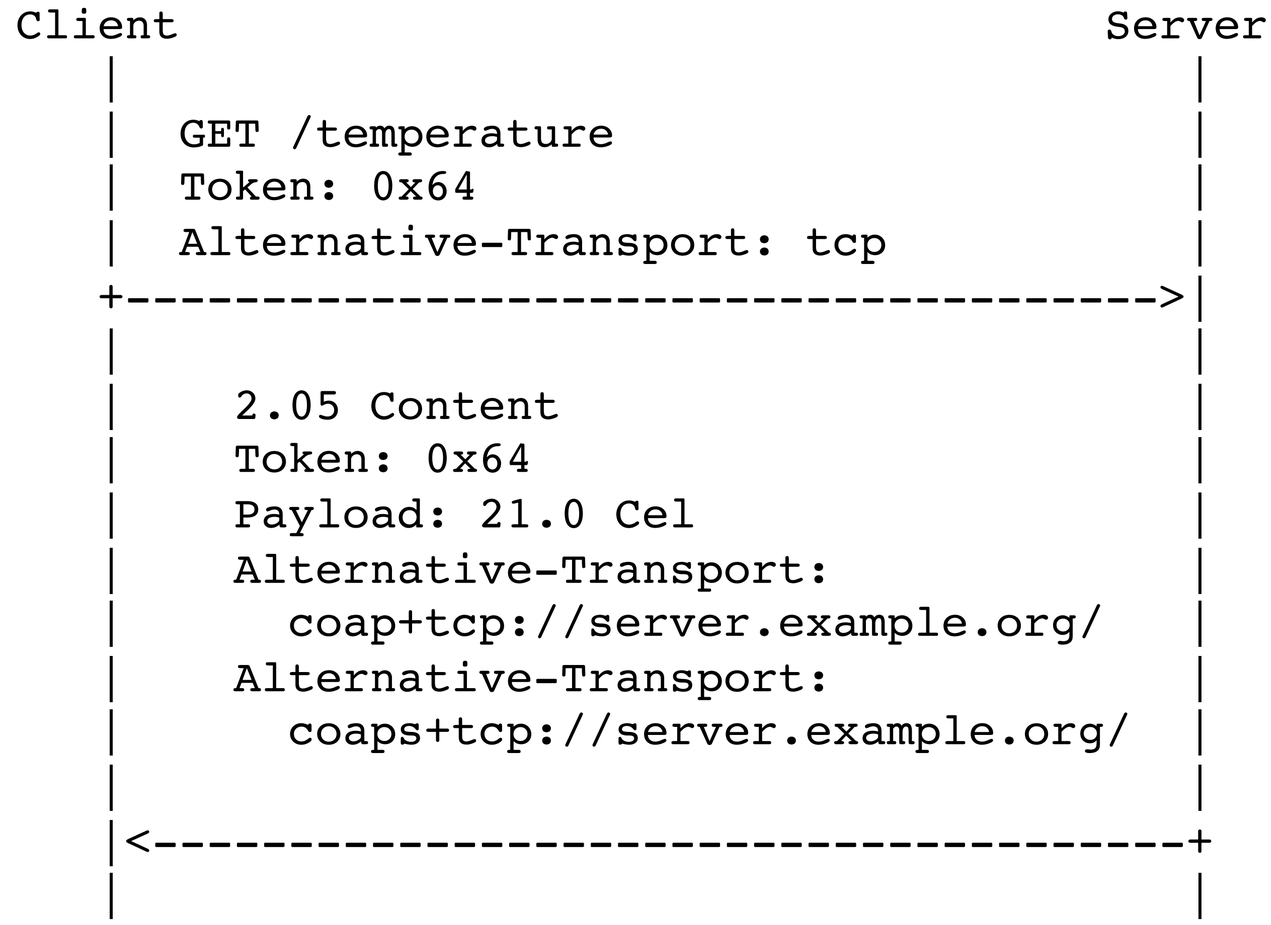
```
POST coap:/rd.example.org/rd?ep=node1
  &at=coap+tcp://server.example.org/,coaps+tcp://
  server.example.org/,coap+ws://server.example.org/
```

- Lookup Request from client to RD

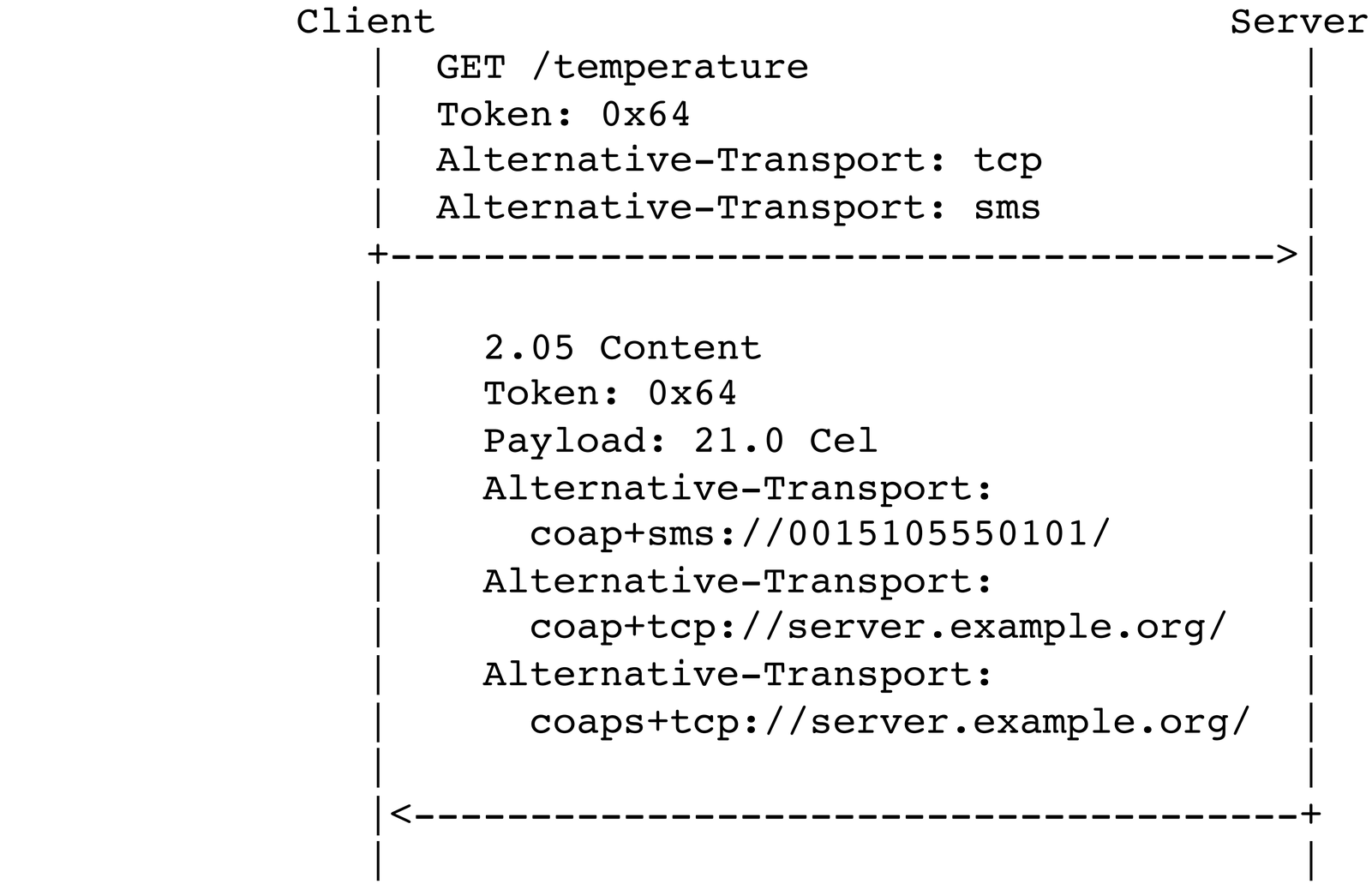
```
 GET /rd-lookup/ep?ep=node1&tt=tcp

Res: 2.05 Content
  <coap+tcp://server.example.org;ep="node1",
  <coaps+tcp://server.example.org;ep="node1"
```

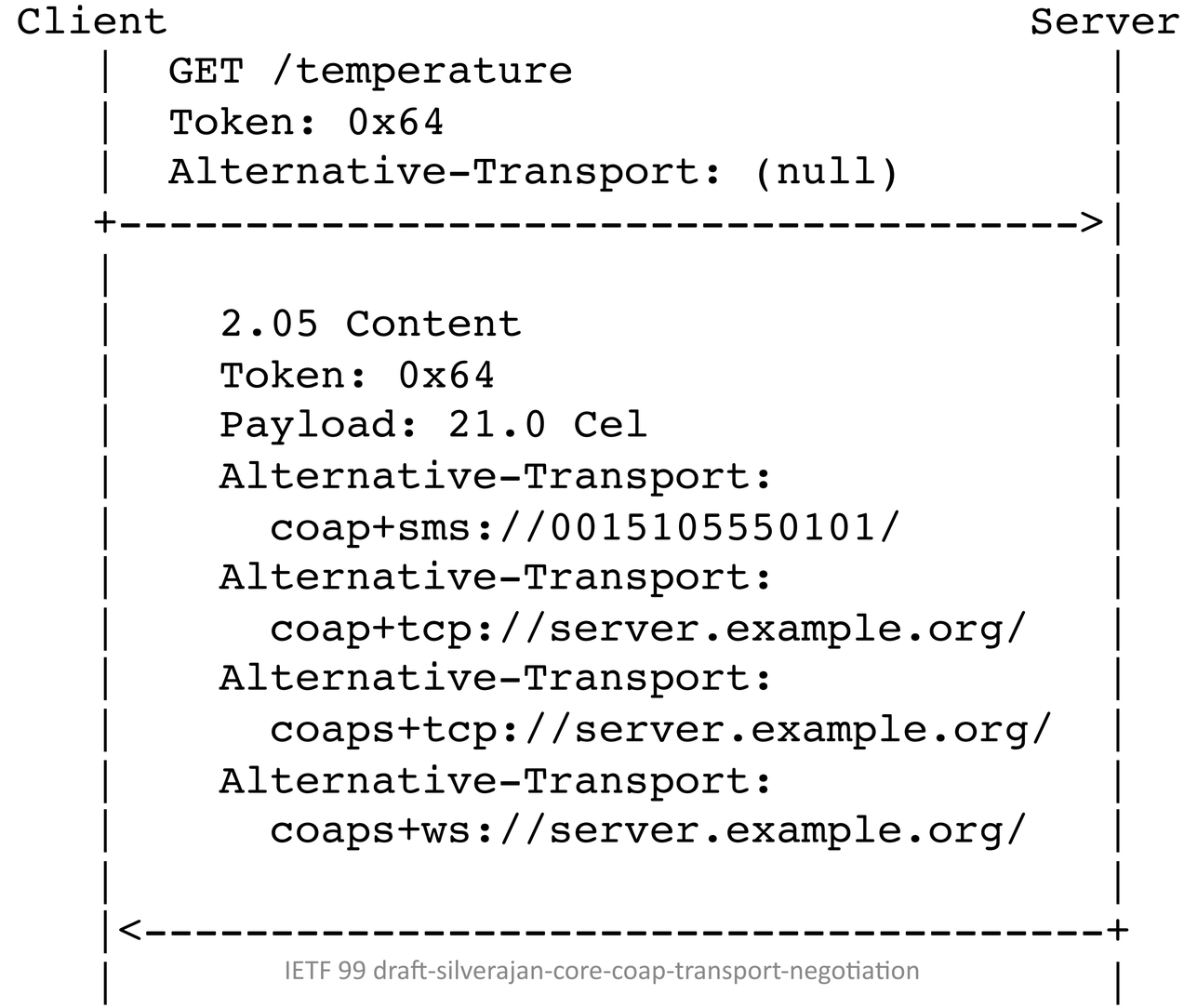
Alternative-Transport CoAP Option



Alternative-Transport CoAP Option



Alternative-Transport CoAP Option



Forthcoming work

- Clients and servers to potentially exchange and agree upon an alternative transport
- Keep in mind (related) effort in
  - SWORN (for securely enabling transports for T1 nodes),
  - CoAP Signalling messages (to exchange capabilities)
  - RFC 7301, RFC 7838
  - Others?

CoAP Communication with Alternative Transports

draft-silverajan-core-coap-alternative-transports

Bill Silverajan TUT
Teemu Savolainen Nokia

Status

- Draft -10 is streamlined
  - directly focus on the URI design work for CoAP over alternative transports
  - Show the technical reasons that if transport information resides in the URI, then the URI scheme provides the best option.

Structure of CoAP URI

scheme://host:port/path/to/resource?query

(CoAP does not support fragments)

- 2 high-level assumptions:
  - WG Consensus was for a CoAP URI which embeds the transport information in one of the URI components above
  - The transport information can be inferred by looking at, or parsing the CoAP URI

Web Linking and Relative URIs

- CoAP Requests can solicit CoAP Response payloads containing relative URIs of the form:
  - **`/3/2024`**
  - **`//host2.org/3/2024`**
- URI relative resolution rules follow RFC 3986
- If the base CoAP URI embeds transport information in the query, path or port components, the target CoAP URI will not retain it.

Guidance in RFC 7320

- The host in a CoAP URI authority component is disqualified for embedding the transport information:

[…] specifications MUST NOT constrain, or define the structure or the semantics for URI authorities […]

For example, an extension or application ought not say that the "foo" prefix in "foo_app.example.com" is meaningful or triggers special handling in URIs.

- In addition to relative URI resolution difficulties, the path component is also disqualifed:

Scheme definitions define the presence, format, and semantic of a path component in URIs; all other specifications MUST NOT constrain, or define the structure or the semantics for any path component. […]

For example, an application ought not specify a fixed URI path "/myapp", since this usurps the host's control of that space.

Design Conclusion

- The URI query, path and authority components can all be disqualified based on RFC 3986 and RFC 7320 rules and recommendations,
- Technical requirements leave only the URI scheme to embed transport identification:
  - **`<coap+transport>`**
  - **`<coaps+transport>`**
- However….

Stumbling blocks

- URI proliferation
  - WG did not see this as an issue, but it was criticised during expert review of core-coap-tcp-tls
- URI aliasing
  - W3C recommendation was also raised about URI aliasing (i.e. Whichever transport is used, the origin server's resource space should not be divided)

Impact

- IESG review: Don't contain any transport information in the CoAP URI at all
  - Prevents URI proliferation (obviously.. ☺)
  - No URI aliasing
  - Use happy eyeballs approach: try every transport until one sticks

Impact

- Implementation issues
  - All CoAP client implementations need to perform recovery and retries for alternative transports for all initial server communication
  - All CoAP client implementations need to perform recovery and retries for alternative transports when relative URIs of the form "`//authority/path/to/resource`" are encountered
  - Dual-stack communication over a NAT or firewall might be significantly affected
  - Energy depletion and performance deterioration for constrained client nodes
- External SDOs and 3rd parties making provisional "coap+foo" IANA registrations to avoid implementation issues
  - Now it might become necessary to have CoAP client nodes implementing both happy eyeballs as well as support for "coap+foo" URI schemes.
  - Brings us back to square 1 with URI proliferation and URI aliasing

Next steps?

- Experts were consulted about how to formulate a URI for CoAP over Alternative Transports, and alot of work was done
- WG consensus was for using the URI scheme
- Adopt as WG document and progress it?
- Or drop some/all of the work?

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

CoAP Simple Congestion Control/Advanced (CoCoA)

draft-ietf-core-cocoa-01

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

Status

- Last revision is -01
  - Presented in IETF 98 (Chicago)
- Heads up before WGLC sent to CoRE, TCPM, ICCRG
  - Two reviews (thanks!)
    - Michael Scharf
    - Ingemar Johansson
- Plan for -02
  - Intended for WGLC

Feedback and plan for -02 (I/IV)

- Weak RTTs
  - RFC 8085:
    - "latency samples MUST NOT be derived from ambiguous transactions"
  - However:
    - We understand that the prohibition applies to **relying** on weak RTTs, not to **extracting information** from them
  - Also, weak RTTs are needed to update the RTO:
    - High link BER
    - Sudden congestion intervals
    - Link/Path RTT larger than default initial RTO

Feedback and plan for -02 (II/IV)

- Tuning the impact of strong and weak estimators

- Current
  - RTO := 0.25 * E_weak_ + 0.75 * RTO (1)
  - RTO := 0.5 * E_strong_ + 0.5 * RTO (2)

- Proposed
  - RTO := w_weak * E_weak_ + (1 – w_weak) * RTO (1)
  - RTO := w_strong * E_strong_ + (1 – w_strong) * RTO (2)

Feedback and plan for -02 (III/IV)

- Editorial improvements
  - Abstract
  - Section 1 almost empty
    - Content from Section 2 may fit Section 1
  - Section 4, “RTO Estimation”
    - Discuss application processing time (and separate responses) vs TCP delayed ACKs
  - Section 4.2, “Measured RTO estimate”
    - Better describe the motivation and properties of the weak estimator
    - Add examples, pseudocode…

Feedback and plan for -02 (IV/IV)

- Editorial improvements:
  - Add references to RFC 7252
    - For readers not so familiar with CoAP
    - Terminology and protocol behavior details
  - Section 7. Security considerations
    - Attacker dropping packets, RTO increase
    - Mitigated by network access control
    - If radio jamming, recovery in reasonable time
      - Weak estimator will help!
- Appendix A. Aggregate Congestion Control
  - To be removed from the document
- Appendix B. Supporting evidence
  - To be kept in the document

Thanks!

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

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

CoMI – update

draft-ietf-core-comi-01

Andy Bierman

Michel Veillette <michel.veillette@trilliantinc.com>

Peter van der Stok

Alexander Pelov

Draft status

Draft	Version	Status	
ietf-core-yang-cbor	4	Stable since IETF 97	Ready for WGLC?
ietf-core-sid	1	Stable since IETF 98	More review needed
ietf-core-comi	1	Update this week	More review needed Summary of changes follow
veillette-core-yang-library	0	Stable since IETF 98	More review needed In scope for Core? Normative reference in CoMI

CoMI update - Resource type

Revision 00		Revision 01	
rt	**path**	**rt**	**path**
core.c	/c	core.c.datastore	/c
core.c.data	/c	core.c.datanode	/c/instance-identifier
core.c.moduri	/c/mod.uri	core.c.moduri	/mod.uri
core.c.stream	/c/s	core.c.eventstream	/s

CoMI update - Content-Format

Content-Format	Content	Delta encoding	Reference SID
application/yang-value+cbor	data-node-value	Parent delta	URI
application/yang-values+cbor	CBOR array of data-node-value	Parent delta	Request payload
application/yang-tree+cbor	Ordered map of single-instance-identifier, data-node-value	Sibling delta	Fist SID in map
application/yang-selectors+cbor	CBOR array of instance-identifier	Sibling delta	Fist SID in array
application/yang-patch+cbor	Ordered map of instance-identifier, data-node-value	Sibling delta	Fist SID in map

CoMI update - Content-Format usage

Method	Resource	Content-Format
GET response	data node	/application/yang-value+cbor
PUT request	data node	/application/yang-value+cbor
POST request	data node	/application/yang-value+cbor
DELETE	data node	na
GET response	datastore	/application/yang-tree+cbor
PUT request	datastore	/application/yang-tree+cbor
POST request	datastore	/application/yang-tree+cbor
FETCH request	datastore	/application/yang-selectors+cbor
FETCH response	datastore	/application/yang-values+cbor
iPATCH request	datastore	/application/yang-patch+cbor
GET response	event stream	/application/yang-tree+cbor
POST request	rpc, action	/application/yang-value+cbor
POST response	rpc, action	/application/yang-value+cbor

CoMI update - Ordered map CBOR tag

- Formal definition of this CBOR semantic added to the draft
  - Based on CBOR array
  - Map which allows multiple values per key and preserves order
- Registration of a CBOR tag (Not currently used by CoMI)

Is “Ordered map” the right name?

(deterministic map, multimap, …)

CoMI update - Error payload

RESTCONF		CoMI	
Field name	**Datatype**	**Field name**	**Datatype**
errors			
+---- error*			
+---- error-type	enumeration	error!	
+---- error-tag	string	+---- error-tag	identityref
+---- error-app-tag?	string	+---- error-app-tag?	identityref
+---- error-path?	instance-identifier	+---- data-node-in-error?	instance-identifier
+---- error-message?	string	+---- error-message?	string
+---- error-info?			

1. Single error returned
2. error-type not supported
3. error-info not supported
4. Tag implemented using identityref
5. error-path renamed

CoMI update summary
Error payload

RESTCONF		CoMI	
Field name	**Datatype**	**Field name**	**Datatype**
errors			
+---- error*			
+---- error-type	enumeration	error!	
+---- error-tag	string	+---- error-tag	identityref
+---- error-app-tag?	string	+---- error-app-tag?	identityref
+---- error-path?	instance-identifier	+---- data-node-in-error?	instance-identifier
+---- error-message?	string	+---- error-message?	string
+---- error-info?			

1. Single error returned
2. error-type not supported
3. error-info not supported
4. Tag implemented using identityref
5. error-path renamed

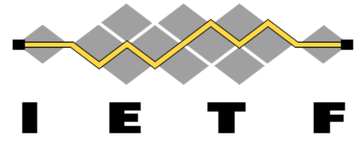
Is "data-node-in-error" the right name? (error-node, …)

CoMI update summary

YANG errors

error-tag	error-app-tag	Defined in YANG 1.1
operation-failed	malformed-message	
	data-not-unique	Yes
	too-many-elements	Yes
	too-few-elements	Yes
	must-violation	Yes
	duplicate	
invalid-value	invalid-datatype	Described
	not-in-range	Described
	invalid-length	Described
	pattern-test-failed	Described
missing-element	missing-key	Described
	missing-input-parameter	Described
unknown-element		Yes
bad-element		Yes
data-missing	instance-required	Yes
	missing-choice	Yes
error		

Next steps - implementations



- Implementations
  - At least 2 independent implementations
    - Go: server+client
    - C: server
    - 2 more partial implementations discussed
  - Open-source implementation planned for next IETF
- Online interop in August
  - In-person interop @IETF100 (Hackathon?)

Next steps

- Review text
  - With gained input from interop
- Goal
  - WGLC for IETF99
- Questions?

CBOR Encoding of Data Modeled with YANG

draft-ietf-core-yang-cbor-04

Andy Bierman

Michel Veillette

Peter van der Stok

Alexander Pelov

Status

- Stable
  - No major modifications on the ML

- Wait for CoMI interop
  - Go for WGLC for IETF100

YANG Schema Item iDentifier (SID)

draft-ietf-core-sid-01

Andy Bierman

Michel Veillette

Peter van der Stok

Alexander Pelov <a@ackl.io>

Status and next steps

Four main topics

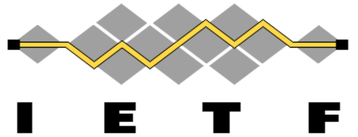
- SID definition (semantic)
  - 64 bit identifier assigned to all YANG identifiers
- SID file format (.sid)
  - YANG Schema -> JSON format
- SID file lifecycle
  - Range registration, .sid generation, .sid update
- Allocation policies
  - Two-tier allocation system
    - MegaRange (1M SIDs) and Range (~1000 SIDs flexible size)
  - Review allocation policy with IANA

Status and next steps

Four main topics

- SID definition (semantic)
  - 64 bit identifier assigned to all YANG identifiers
- SID file format (.sid)
  - YANG Schema -> JSON format
- SID file lifecycle
  - Range registration, .sid generation, .sid update
- Allocation policies
  - Two-tier allocation system
    - MegaRange (1M SIDs) and Range (~1000 SIDs flexible size)
  - Review allocation policy with IANA

Action points from last time



- Modify the current draft: OK?
  - Introduce Mega-Ranges
  - Clarify allocation policy
- Meet @ietf99 with NETMOD
  - 1h meeting, U-shape room
  - Mailing list?
- Detail YANG registration procedure
  - Examples in appendix

Action points from last time

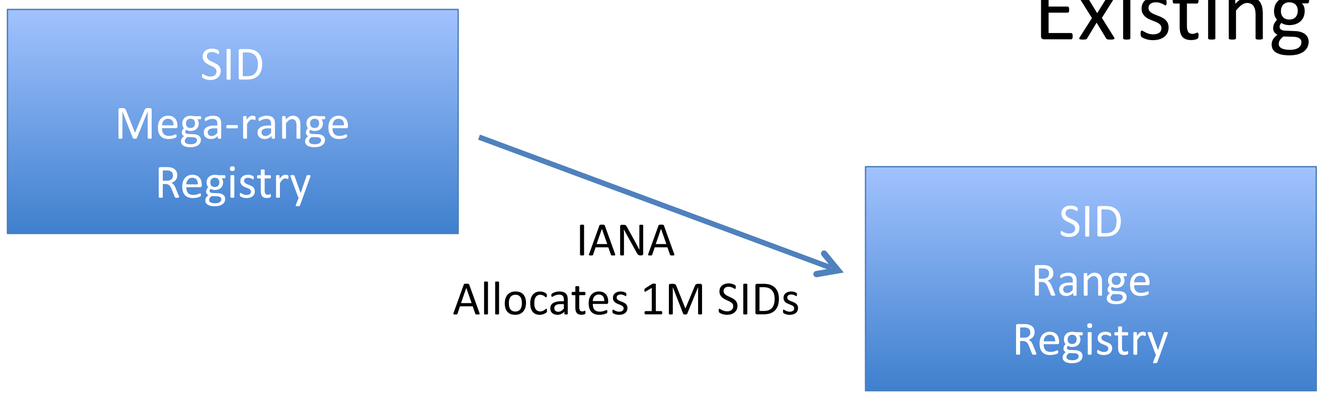
- Modify the current draft: OK?
  - Introduce Mega-Ranges
  - Clarify allocation policy

- Meet @ietf99 with NETMOD
  - 1h meeting, U-shape room
  - Mailing list?

yot@ietf.org
2h - Side-meeting
Thursday, 20th, 10-12am

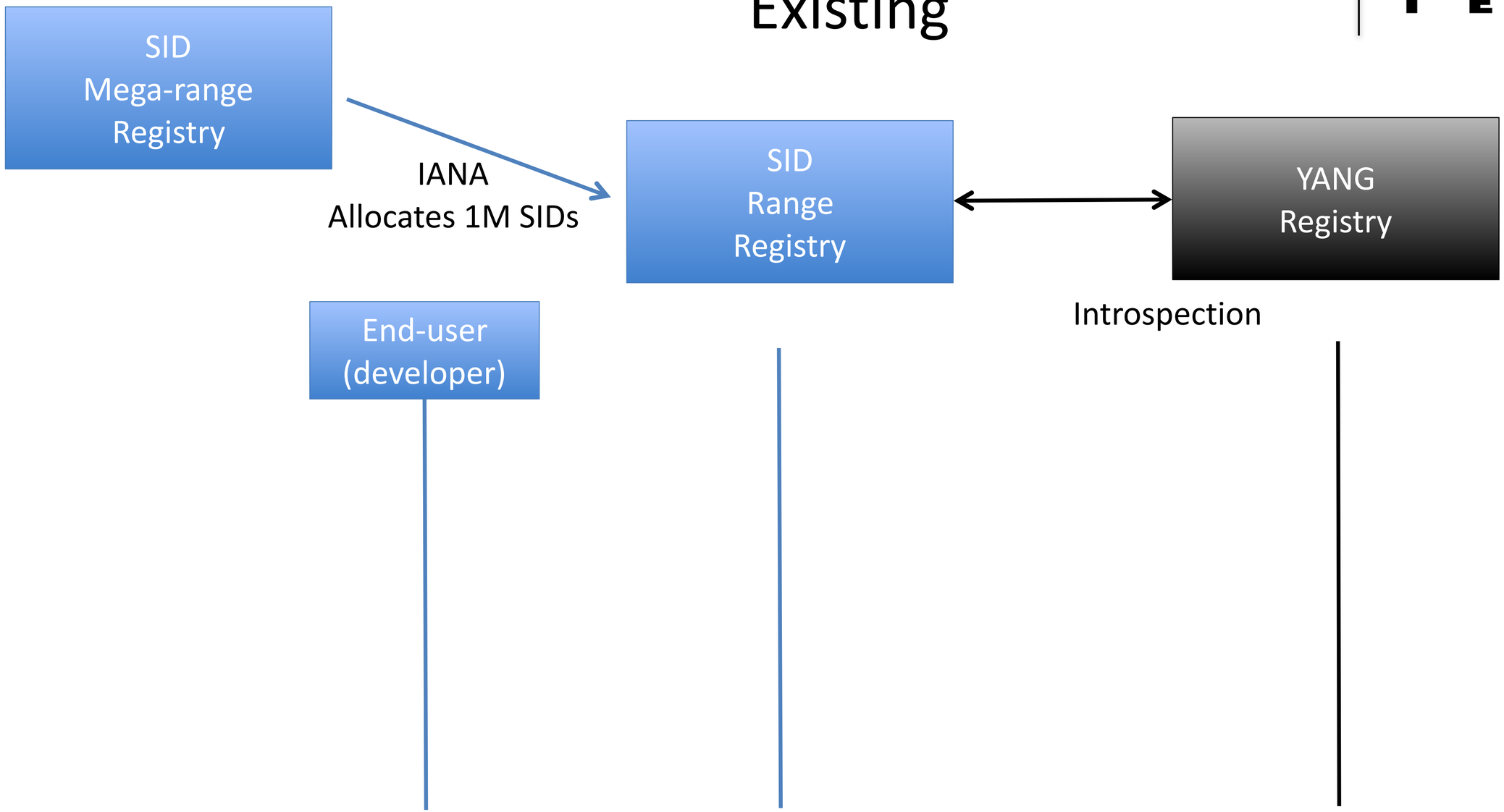
- Detail YANG registration procedure
  - Examples in appendix

Registration procedure
Existing

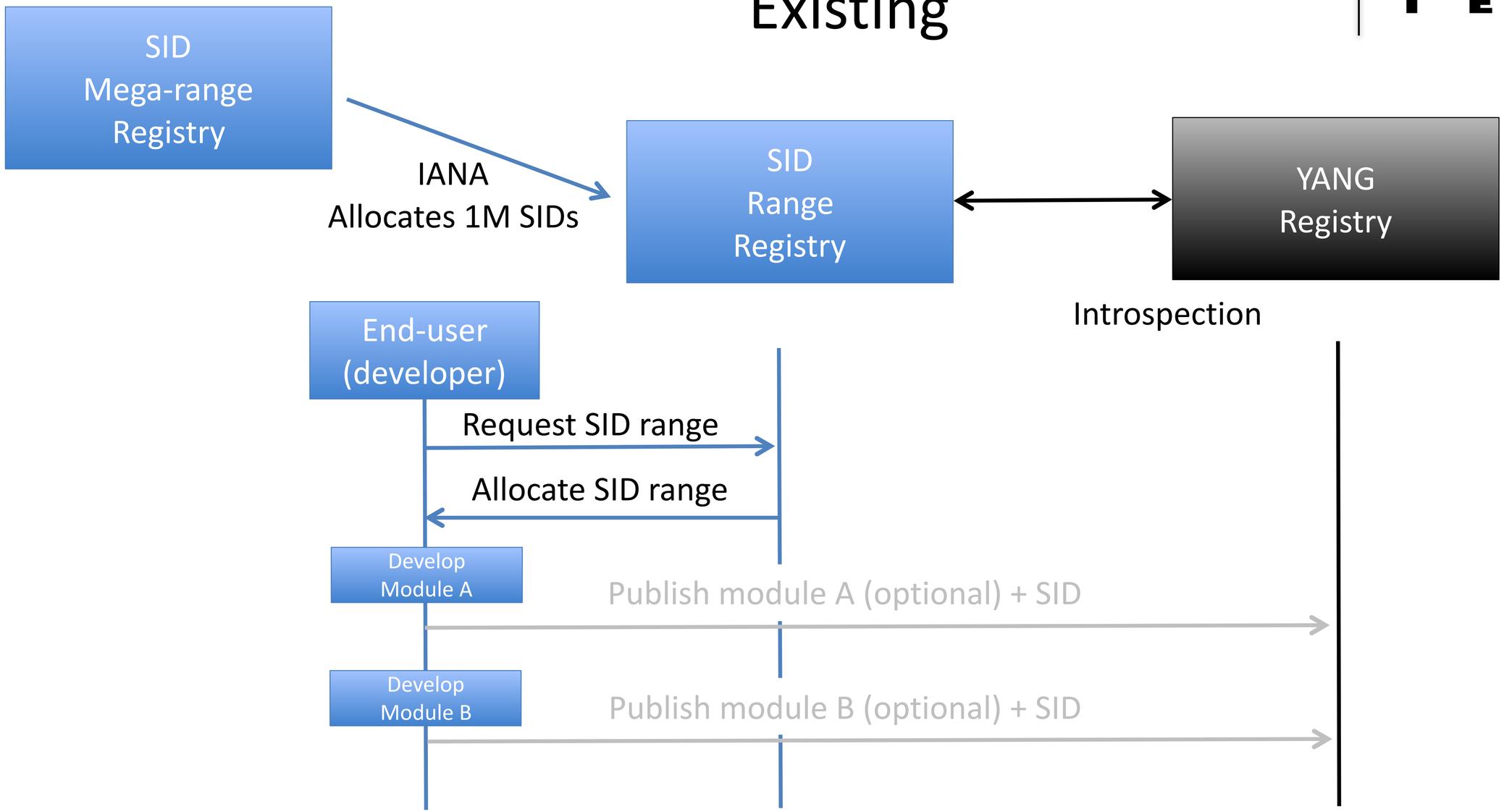


Registration procedure
Existing

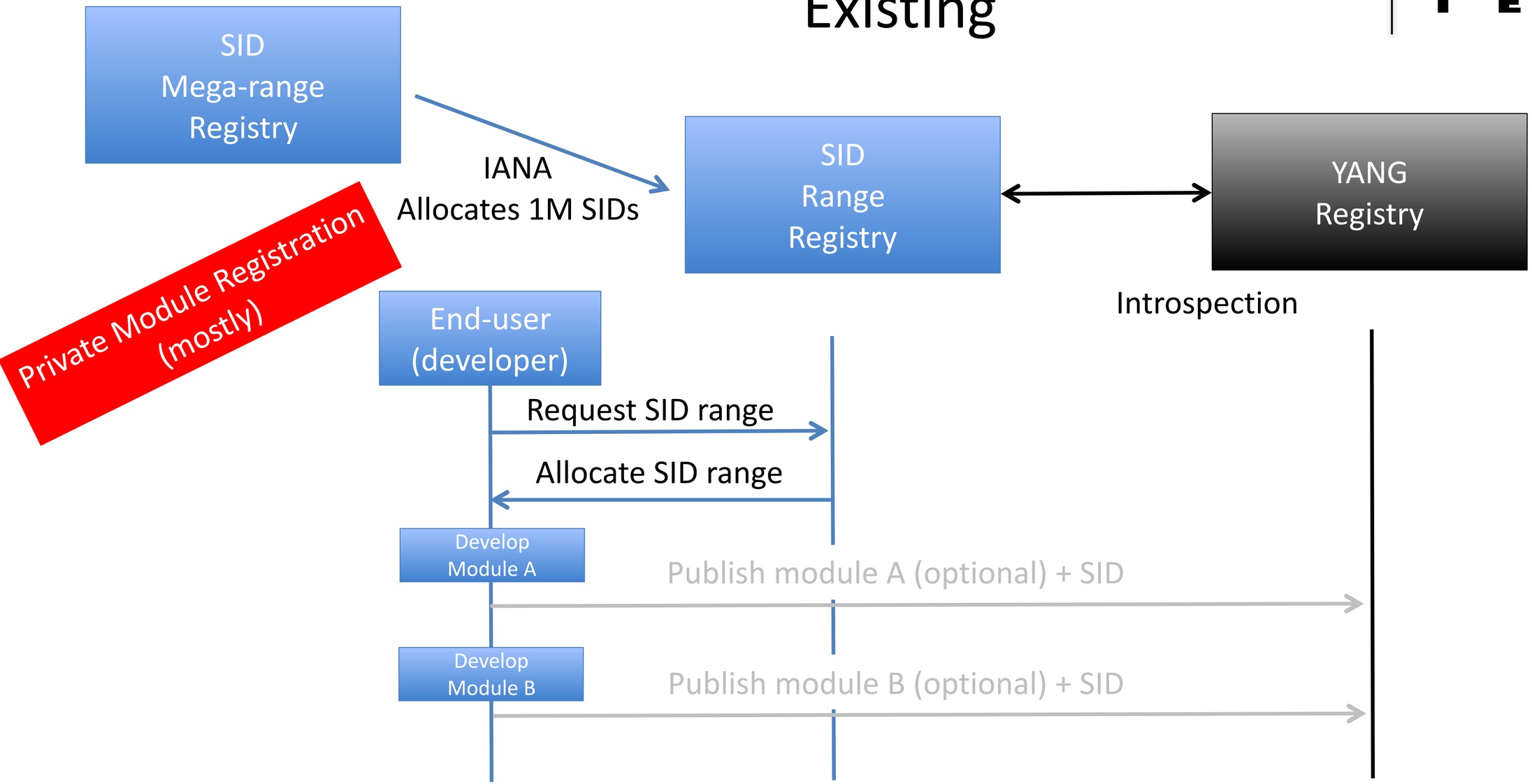
Registration procedure
Existing



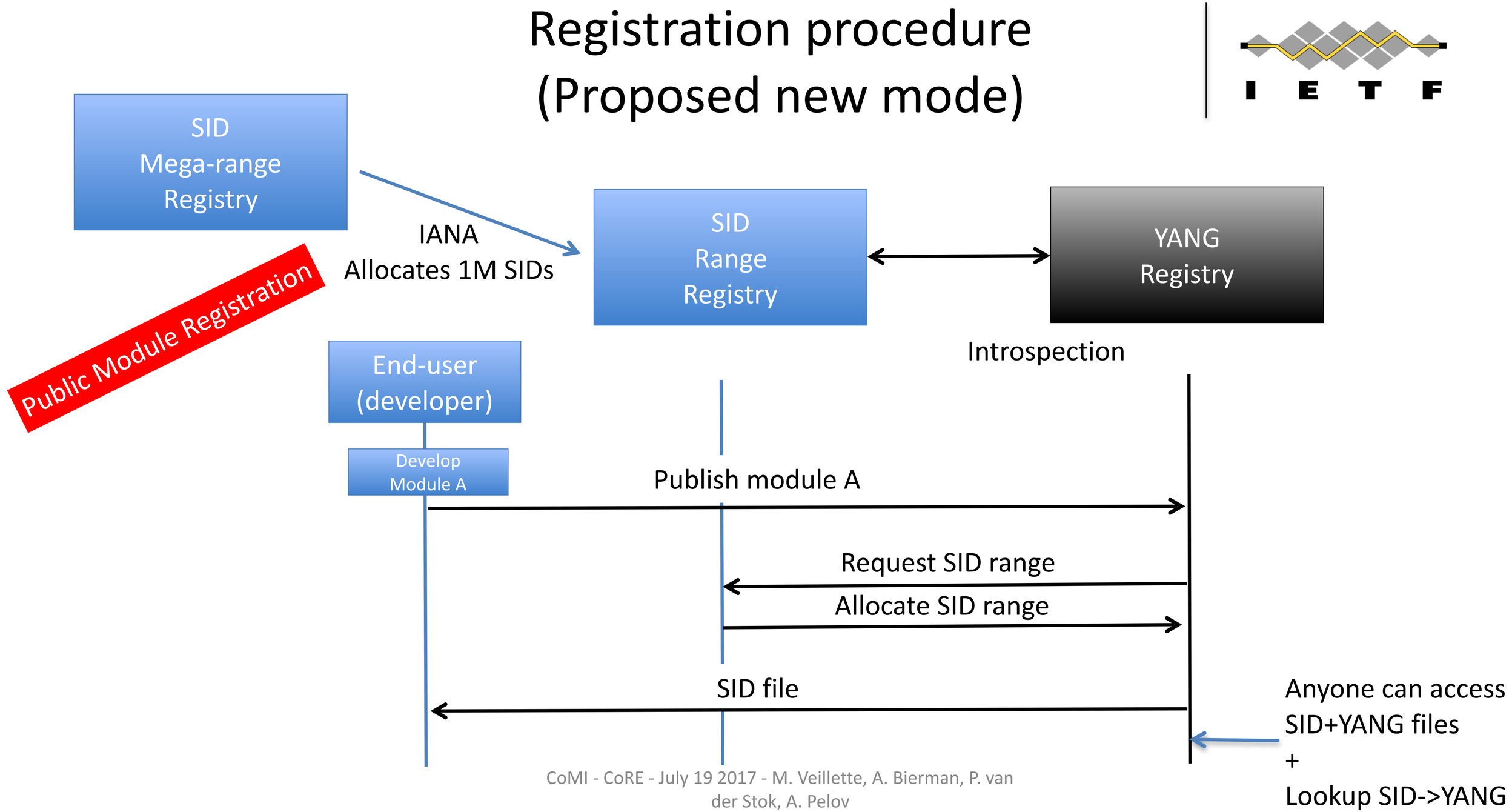
Registration procedure
Existing



Registration procedure
Existing



Registration procedure (Proposed new mode)



Next steps

- Public (one-step) registration

- Introspection - link to YANG file
  - Currently: name
  - Add hash(source)?
    - Optional: URI to stable source?

  - More unclear (v3):
    - Embedding source YANG file to SID file?
    - Add signature to SID file?

IMPLEMENTATION

Currently – git repository

By end of August:
- Private SID registry registration

Proposed action

Make sure one-step registration is not excluded

Add URI+model hash (introspection)

WGLC for IETF100

Extensions could go to other documents (e.g. signing SIDs, etc.)

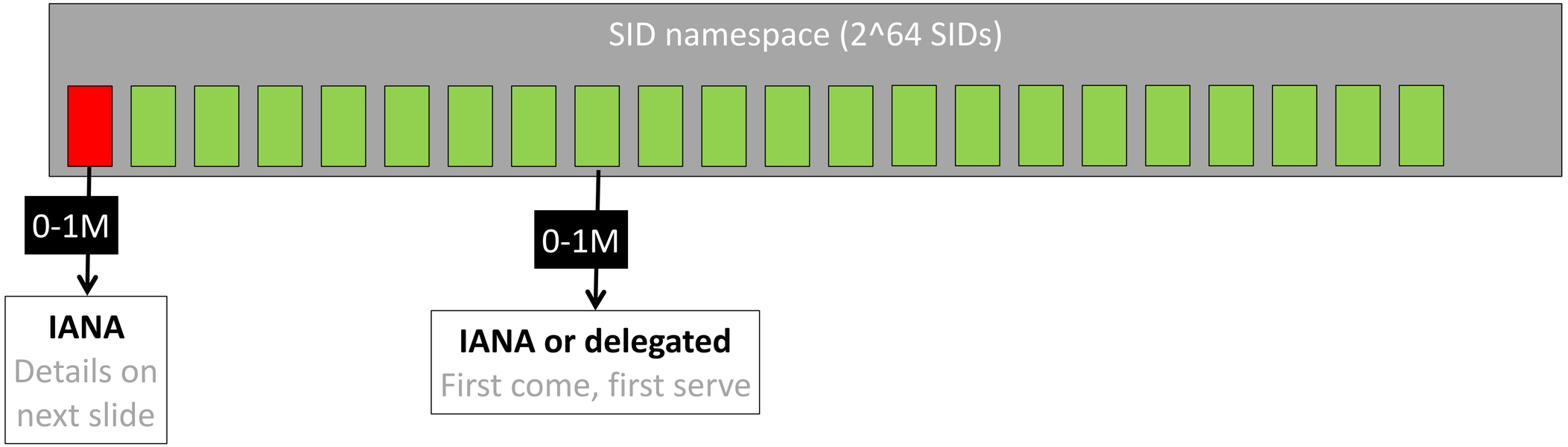
Backup slides

draft-ietf-core-sid-01

Mega-range Registry

- Allocated by : IANA
- Policy : Hierarchical Allocation / Expert Review
  - Who the assignee is, change controller
- Conditions :
  - Demonstration of a functional SID allocation infrastructure
  - Upon repeated request, demonstrate exhaustion of range
  - Supply contact information
  - Supply registry entry point (URI of the registry)

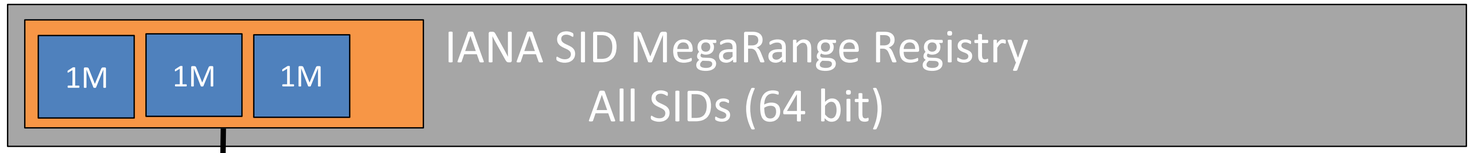
SID Mega-range Registry



SID Mega-range Registry

Hierarchical Allocation - 0-100M

Reserved >100M



<IANA Expert Review>

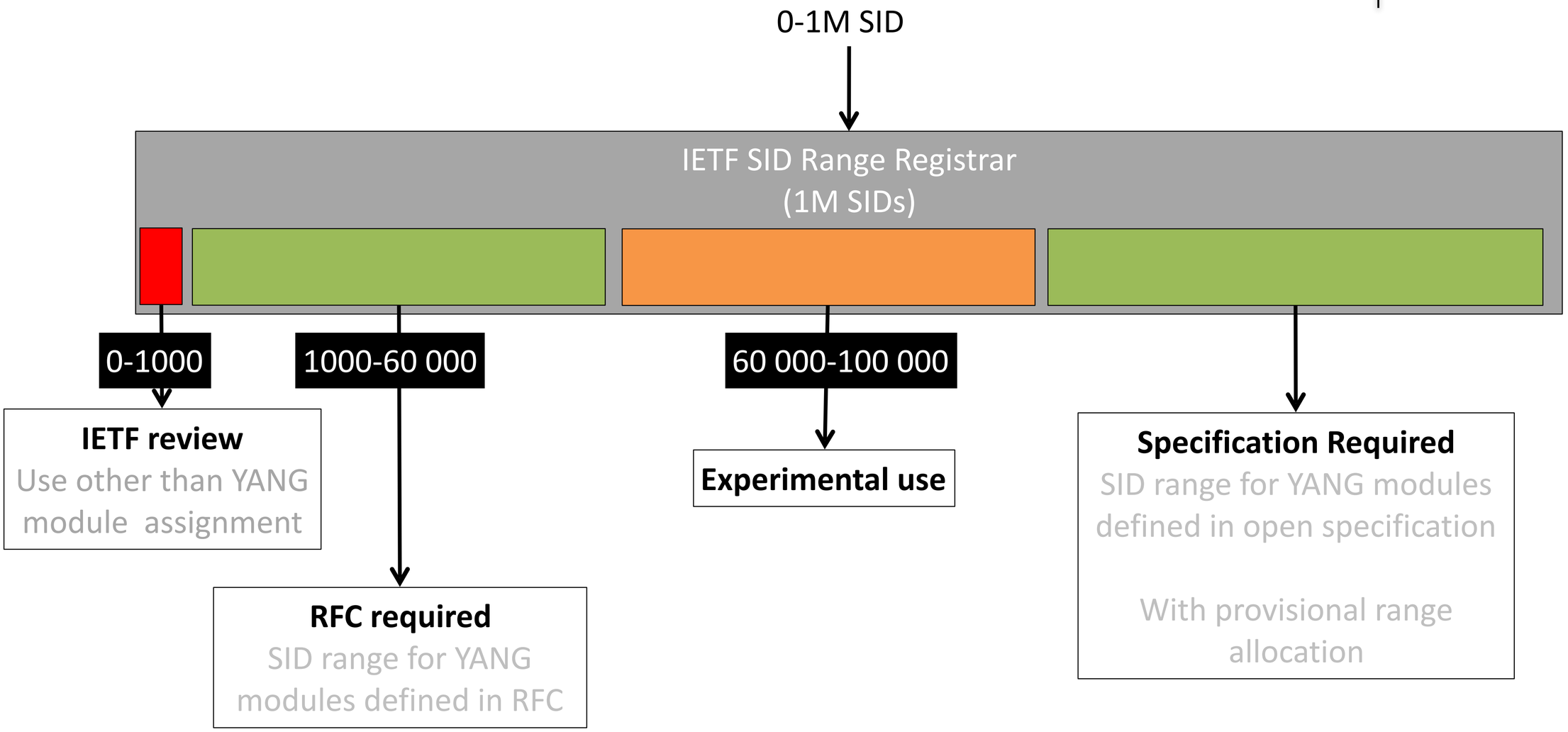
- Requester must:
  - Specify internal SID range allocation policy
  - Demonstrate a functional SID allocation infrastructure
  - Supply contact name, who the assignee is, change controller
  - Supply registry entry point
- Upon repeated request, demonstrate exhaustion of range

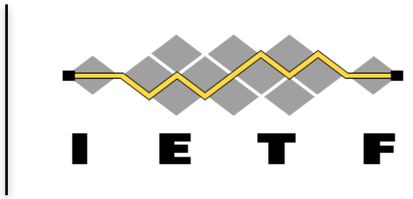
SID Range Registrar
(1M SIDs)

- A permanent HTTP URL which allows to retrieve all YANG definitions

SID Range
(policy depending registrar)

IETF SID Mega-range Registry

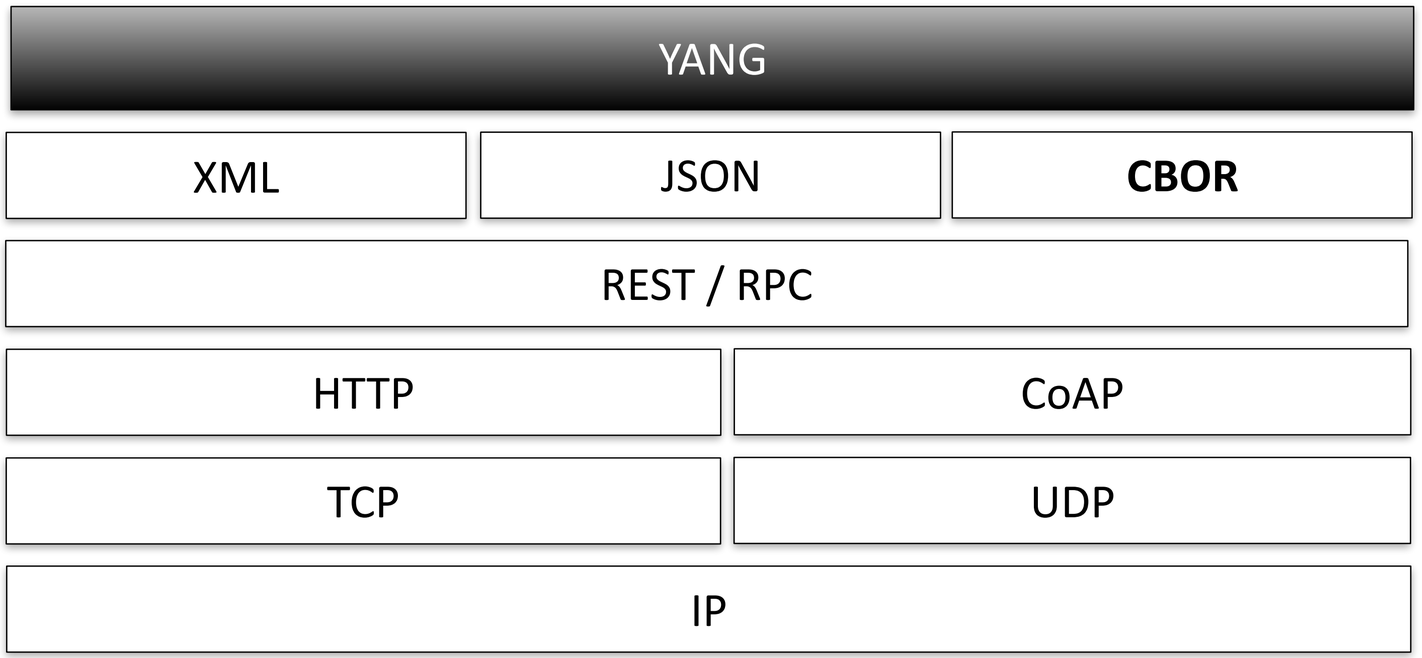




YANG of Things

Alexander Pelov <a@ackl.io>

The YANG Stack



Data Model

Data Representation

Interaction Model

Protocol Bindings

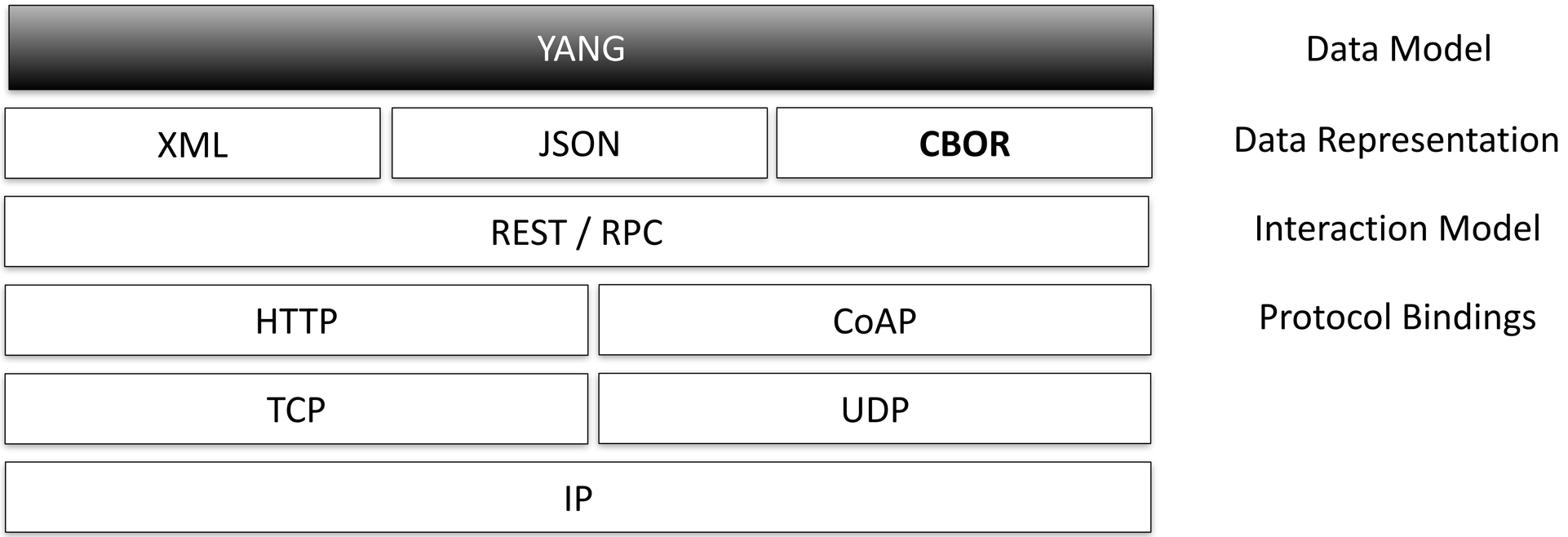
Features (small sample)

Constraints on data

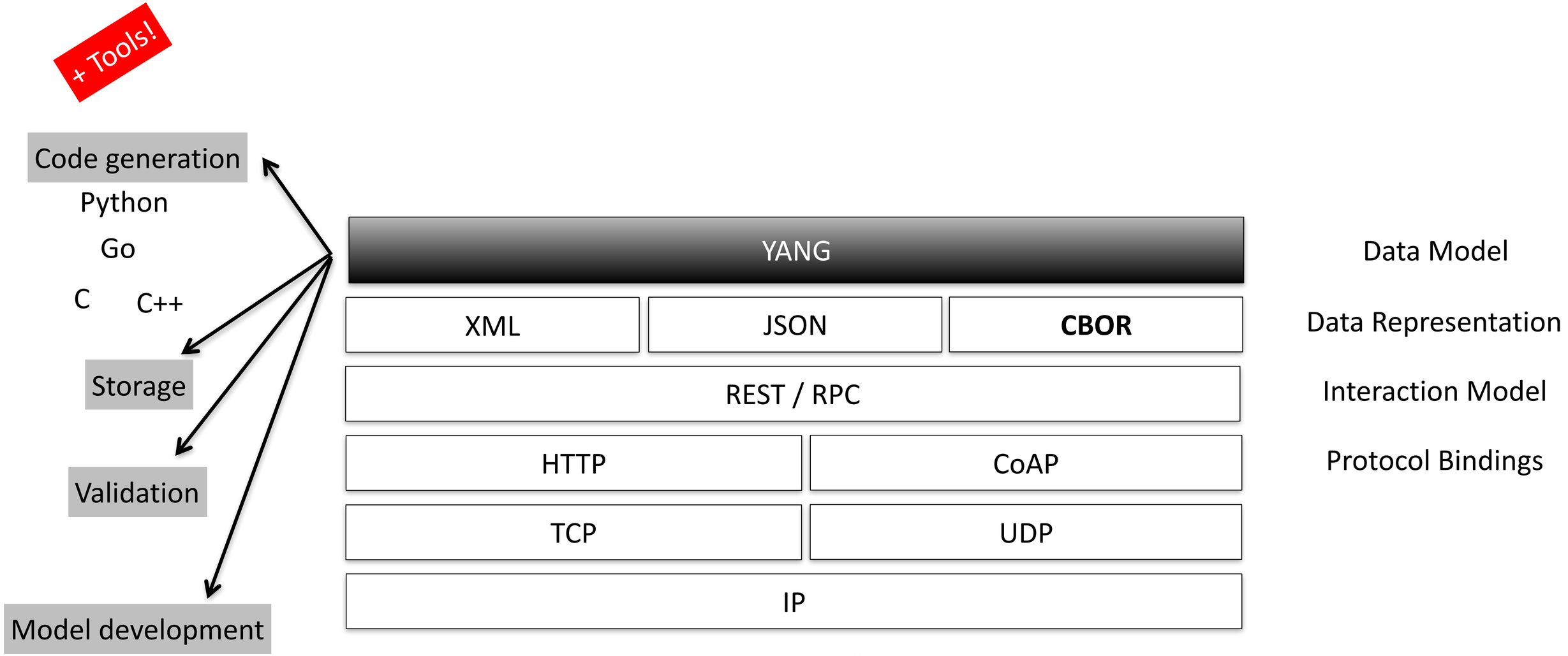
Rich built-in data + Rich extension mechanism

Transactions

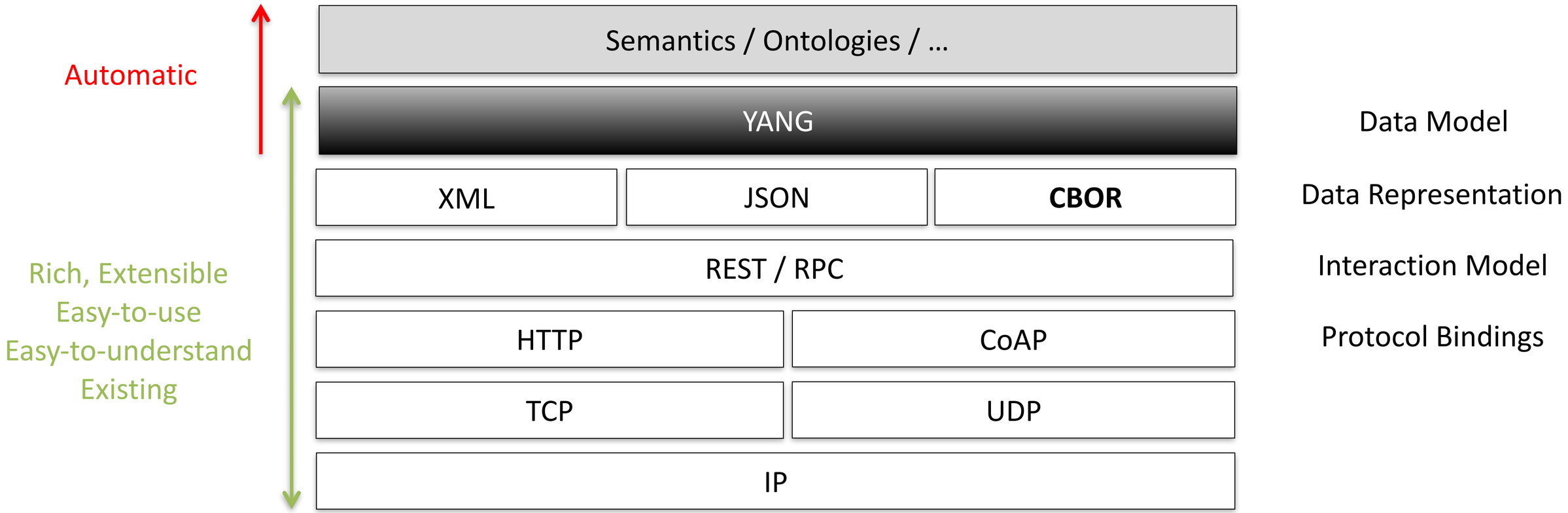
Balance between high-level data modeling and low-level bits-on-the-wire encoding



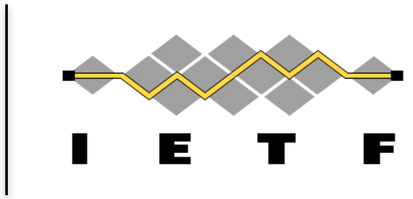
Rich ecosystem



A way into WoT



YANG for IoT (YoT)



IETF

6TiSCH

LPWAN

(Side meetings)

YANG models

Manufacturer Usage Description (MUD)

LWM2M – CoMI mapping

RD

Decentralized Registry

SID

YANG for IoT (YoT)

IETF
6TiSCH
LPWAN
(Side meetings)

YANG models
Manufacturer Usage Description (MUD)
LWM2M – CoMI mapping
RD

Decentralized Registry
SID

Non-WG ML created: yot@ietf.org

Best practices for using YANG-based data modeling for the management of networks with constrained devices and constrained networks

How to make use of properties of the combination of technologies involved (YANG, CBOR, SID, CoAP, RESTCONF, …)

Side-meeting @ IETF: Thursday, 20th, 10am-12pm

Thanks!

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

All times are in time-warped CEST

Tuesday (150 min)

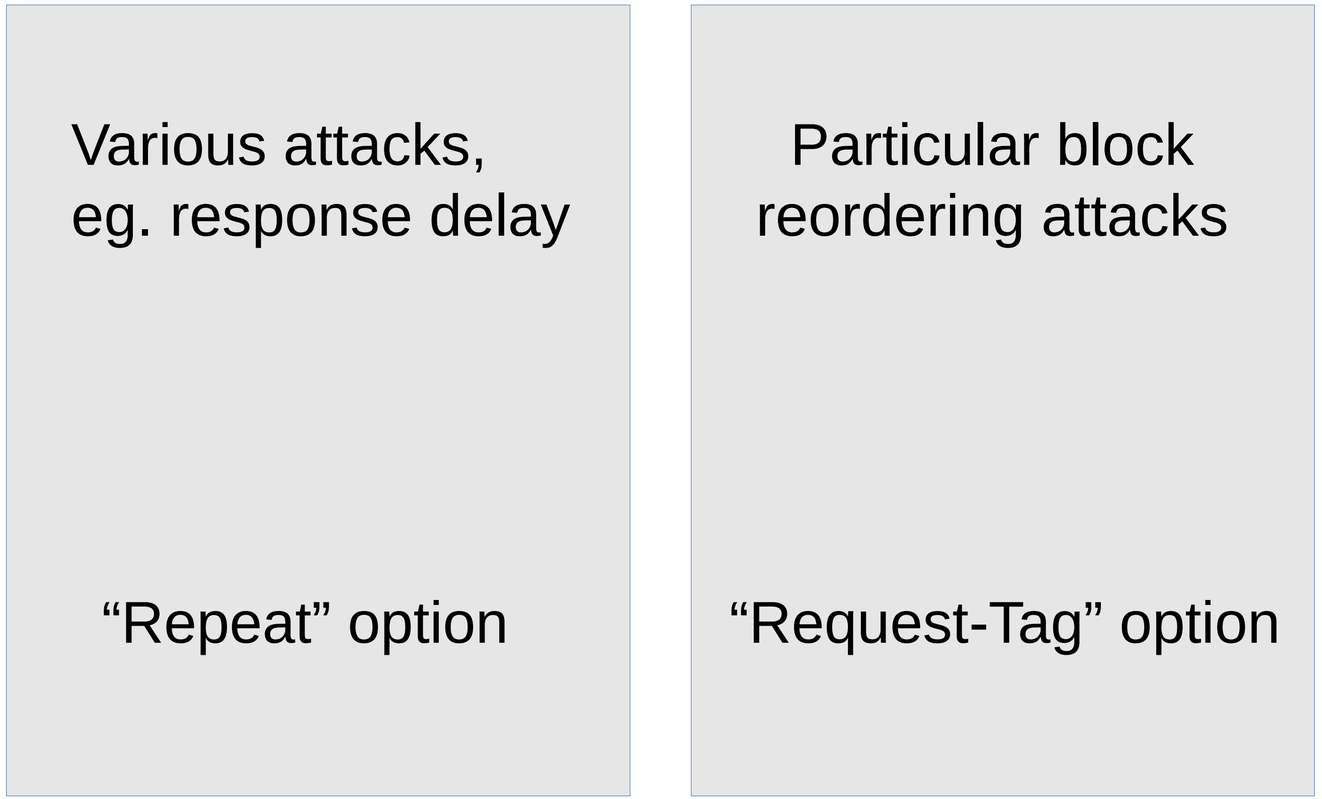
- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

repeat-request-tag

Utility options for CoAP security

Christian Amsüss, John Mattson, Göran Selander

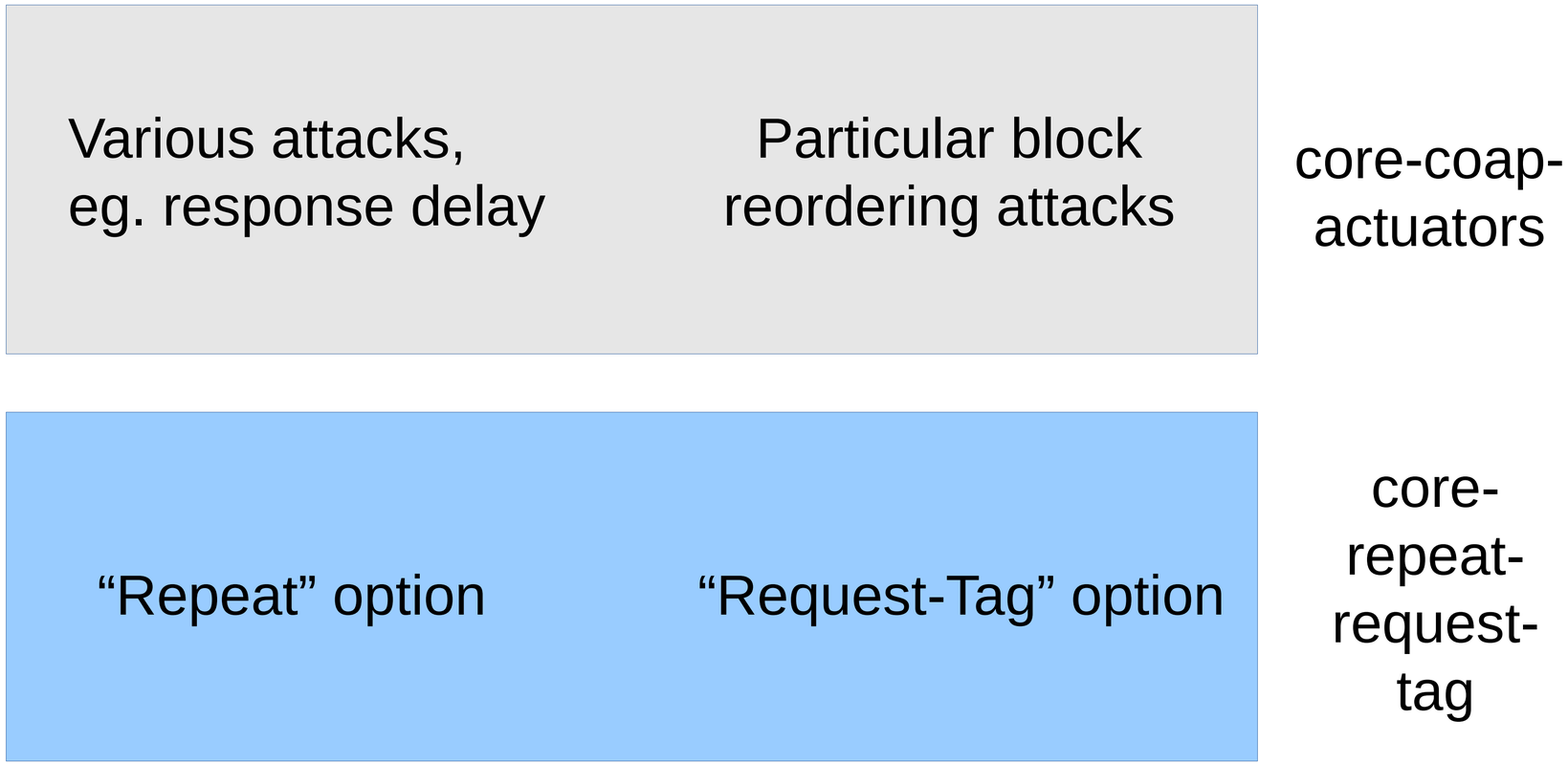
Document History



core-coap-actuators

core-request-tag

Document History



Issue: Freshness

- No freshness guarantees in CoAP
  - Affects all security modes
  - User presses “unlock” button, attacker delays package until user went to get a physical key.
- Solution: “Repeat” option
  - POST /lock “open” → 4.xx Retry, Repeat “0123cafe”
  - POST /lock, Repeat “0123cafe”, “open” → 2.04 Changed
- Other applications
  - OSCOAP: synchronize the receive window states after power loss or when entering a multicast

Issue: Freshness

- No freshness guarantees in CoAP
  - Affects all security modes
  - User presses “unlock” button, attacker delays package until user went to get a physical key.

- Solution: “Repeat” option
  - POST /lock “open” → 4.xx Retry, Repeat “0123cafe”
  - POST /lock, Repeat “0123cafe”, “open” → 2.04 Changed

Freshness Challenge Echo

- Other applications
  - OSCOAP: synchronize the receive window states after power loss or when entering a multicast

Issue: Blockwise

- Request body correlation is weak
  - Affects all security modes
  - unlikely to occur “naturally”
- Solution: “Request-Tag” option
  - Similar to ETag
  - Client-chosen, single-use with defined recycling
  - Zero overhead in OSCOAP most of the time
  - Server must not combine payloads across request tags
  - Extends protection from payloads to bodies
- Other applications
  - Concurrent blockwise operations (relevant to proxies transporting OSCOAP)

Blockwise attack: Firmware

- PUT /firmware/baseband, payload=v10, 2 blocks
  - First block gets through
  - Second block stored by attacker, attacker creates network outage
- later: PUT /firmware/baseband, payload=v11, 2 blocks
  - First block let through
  - Second block injected from earlier → new operation
  - Atomic PUT successful with mixed content. Device bricked from secure operation.

Questions to the WG

- Can we update RFC7959 with this?

- Did we miss more lightweight alternatives? (candidates:)
  - Deeper integration of sequence numbers (visible in DTLS?)
  - Have the server set a nonce (bigger overhead)
  - Option to discriminate within endpoint / security context
  - Alternatives must still allow random access

- Who has read the document?
- Can we adopt it as a WG document?

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:40 Intro, Agenda, Status
- 09:40–09:50 Post-WGLC: Links-json direction (CB)
- 09:50–10:35 Post-WGLC: CoAP-TCP (DT, chairs)
- 10:35–10:45 Up for WGLC: CoCoA (CG)
- 10:45–11:20 Up for WGLC: COMI (AP)
- 11:20–12:00 Anticipate Friday:
  - 11:20–11:30 dev URN (JA)
  - 11:30–11:45 Request Tag (CA)
  - 11:45–11:55 Multicast-OSCOAP (MT)

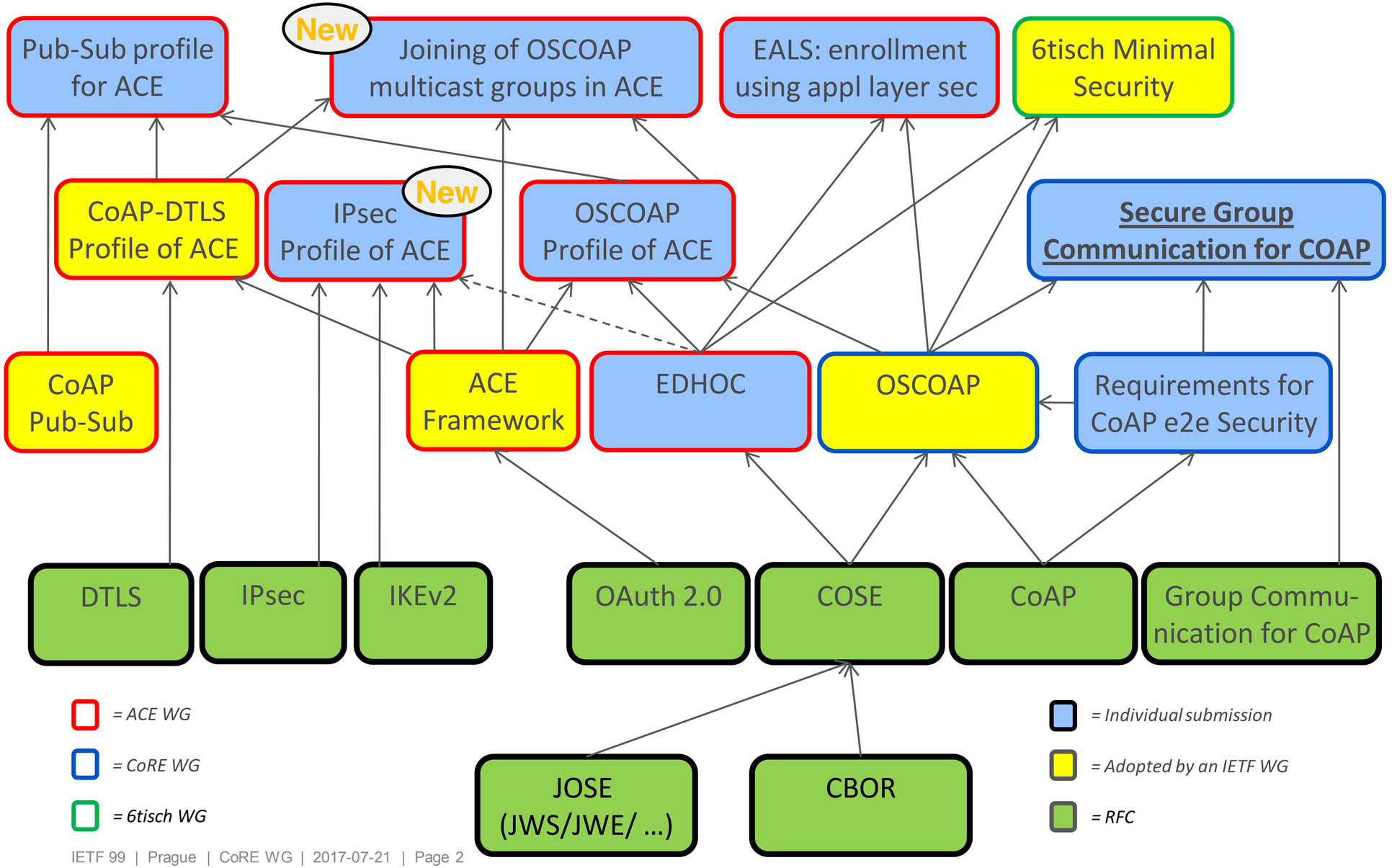
Secure group communication for CoAP

draft-tiloca-core-multicast-oscoap-02

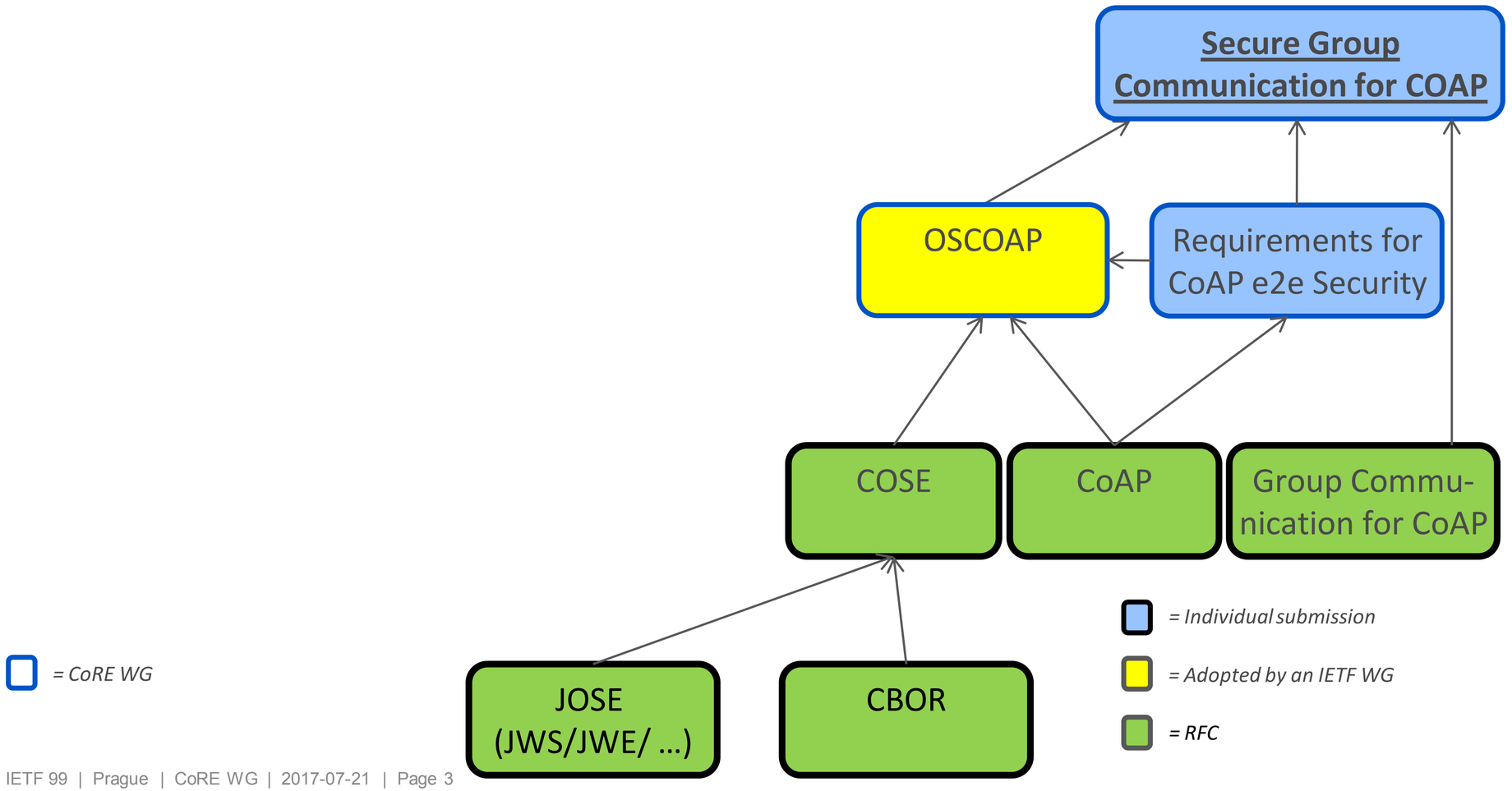
Marco Tiloca, RISE SICS
Göran Selander, Ericsson
Francesca Palombini, Ericsson

IETF 99, CoRE WG, Prague, July 21st, 2017

Related Work

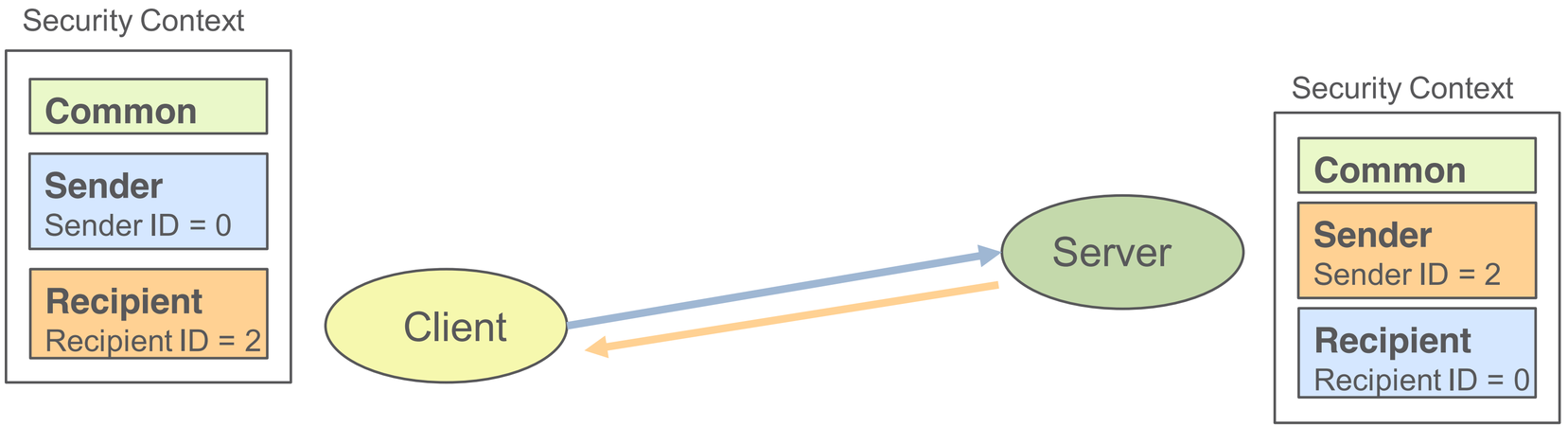


Related Work



OSCOAP

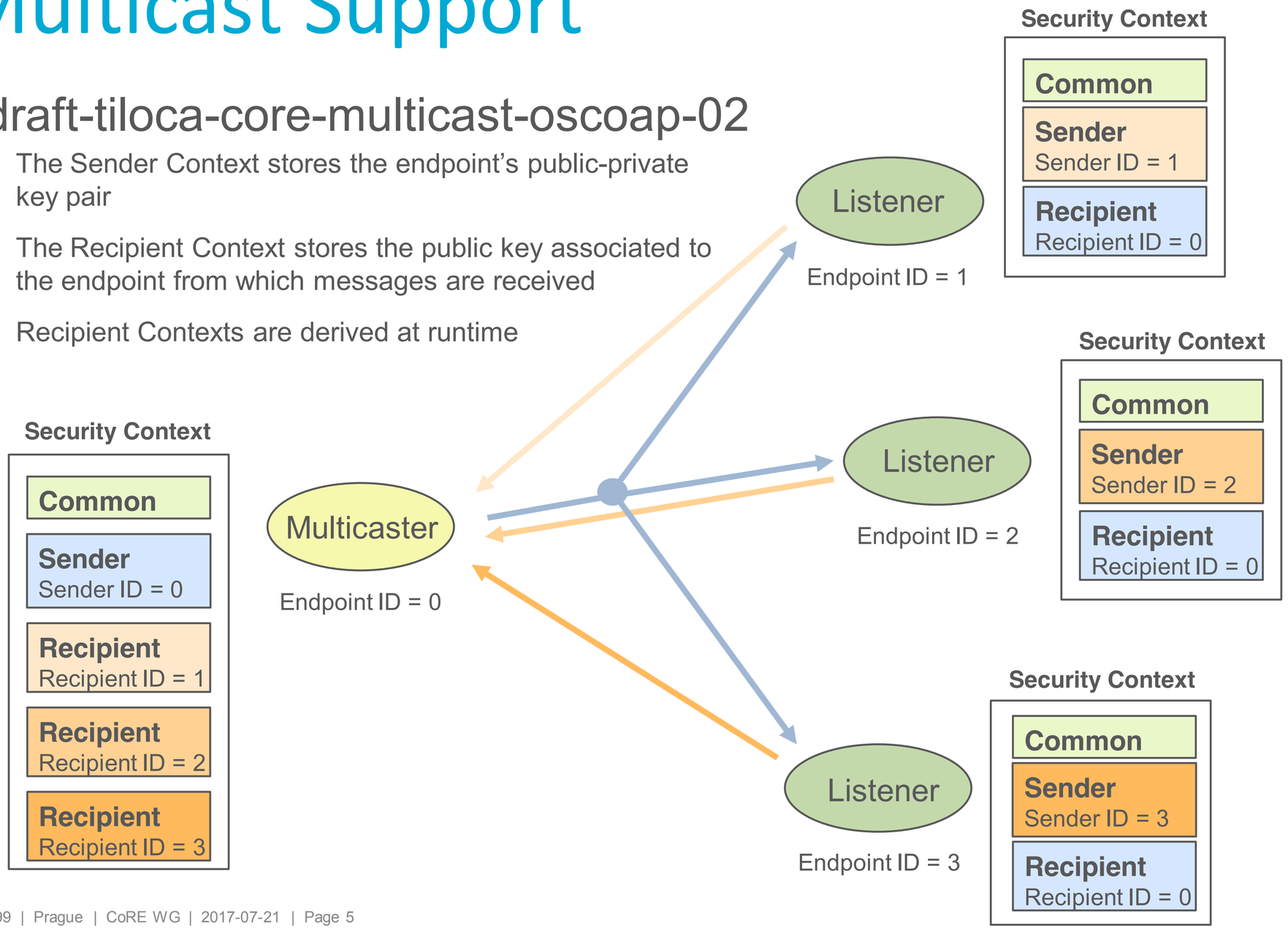
› draft-ietf-core-object-security-03



- Secure end-to-end communication in the presence of intermediaries (Protection against replay included)
- Uniquely bind the CoAP response to the CoAP request
- Protects payload and parts of CoAP metadata (header, options ...)

Multicast Support

- draft-tiloca-core-multicast-oscoap-02
  - The Sender Context stores the endpoint's public-private key pair
  - The Recipient Context stores the public key associated to the endpoint from which messages are received
  - Recipient Contexts are derived at runtime



Main Features

- How to use OSCOAP in group communication
  - Same structures, constructs, mechanisms of OSCOAP
- Confidentiality, integrity, replay protection, req-resp binding
  - Shared keying material to protect communications within the group
  - Locally-derived keying material to protect communications in the group
- Source authentication
  - Asymmetric-key counter signatures
  - Embedded in the COSE object (“countersign” field)
- Group Manager
  - Responsible for the multicast group (join process, group rekeying)
  - Ensures uniqueness of Endpoint IDs within a same group

Draft Update (v-02) (1/3)

- Adapted to OSCOAP v-03

- New concept: “pure-listener”
  - Listener that never replies to a group request
  - Easier to initialize and manage

- Revised requirements

- Revised security contexts
  - “Pure-listener” case
  - Considerations on Context ID
  - EdDSA signature algorithm ed25519 mandatory to implement

Draft Update (v-02) (2/3)

- Compressed COSE object (from OSCOAP v-03)
  - Updated/extended use from OSCOAP
  - Usage of “countersign” field for counter signatures
  - New field “gid” for the Context ID

- Security considerations
  - Synchronization of sequence numbers based on Repeat Option (*)
  - Revision of public key provisioning upon joining

* *draft-amsuess-core-repeat-request-tag-00*

Draft Update (v-02) (3/3)

- Group-authentication only (Appendix C)
  - Disable counter signatures for a purely symmetric solution
  - Intended for use cases with low-message latency (*)

- Unicast OSCOAP with signatures (Appendix D)
  - In some scenarios, E2E-confidentiality may not be required
  - Then proxies can fully inspect, process and aggregate messages
  - How to build the COSE object accordingly
  - Better to cover it in this draft than in OSCOAP

* *draft-somaraju-ace-multicast-02*

Implementation

- First proof-of-concept up and running
  - Contiki OS
  - Wismote (MSP430; TI CC2520)
  - SmartRF (MSP430; TI CC2538)

- Planned next steps
  - Harmonize implementation with latest OSCOAP
  - Compute digital signatures in Hardware on SmartRF nodes
  - Experimental evaluation

https://github.com/tdrlab/mcast

Related activity

- draft-tiloca-ace-oscoap-joining-00
  - Related to Appendix A of Group OSCOAP v-02
  - Following comments at IETF97

- Join an OSCOAP multicast group over the ACE framework
  - Joining node → Client
  - Group Manager → Resource Server

- Leverage protocol-specific profiles of ACE
  - CoAP-DTLS profile *draft-ietf-ace-dtls-authorize-01*
  - OSCOAP profile *draft-seitz-ace-oscoap-profile-03*

Wrap-up and next steps

- v-02 is the result of several reviews
- Several updates from v-01, including:
  - Pure-listener endpoints
  - Compressed COSE object
  - SN synchronization with Repeat Option
  - Group-authentication only (appendix)
  - Unencrypted unicast w/ signatures (appendix)
- First proof-of-concept implementation up-and-running
  - Plan for improvements and evaluation
- Authors think it is ready for WG adoption

Thank you!

Comments/questions?

https://ericssonresearch.github.io/Multicast-OSCOAP/

Motivation

- RFC7390* Section 5.3.3 : ” In the future, to further mitigate the threats, security enhancements need to be developed at the IETF for group communications.”
- CoRE WG requested Multicast OSCOAP (IETF95, mailing list, …)
- draft-somaraju-ace-multicast relies on OSCOAP to secure group messages, but does not define how.
- Multicast OSCOAP fills this gap and is use case independent

* RFC7390: Group Communication for the Constrained Application Protocol (CoAP)

What's Different from OSCOAP v-03

- Defines Context ID (oscoap-03 does not have it)
- ContextID added to the COSE object (new "gid" field)
- Sender ID is always sent in the message (optional in oscoap-03)
- Counter Signature added to COSE object ("countersign" field)
- Transaction ID includes also Context ID (in oscoap: {sid , seqn})
- Recipient Contexts created at runtime upon receiving the first message from the respective endpoint
- Additional asymmetric key(s) in Sender/Recipient Contexts

- **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**

✓Blue sheets
✓Scribe(s)

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 8179.

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 8179 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.

I E T F

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

All times are in time-warped CEST

Friday (90 min)

- **11:50–11:55 Intro, Agenda**
- **11:55–12:10 Post-WGLC: SenML**
- **12:10–12:40 WG doc: RD, RD-DNS-SD**
- **12:40–12:50 WG doc: pubsub**
- **12:50–13:20 WG doc: oscoap**

All times are in time-warped CEST

Friday (90 min)

- 11:50–11:55 Intro, Agenda
- 11:55–12:10 Post-WGLC: SenML
- 12:10–12:40 WG doc: RD, RD-DNS-SD
- 12:40–12:50 WG doc: pubsub
- 12:50–13:20 WG doc: oscoap

All times are in time-warped CEST

Friday (90 min)

- 11:50–11:55 Intro, Agenda
- 11:55–12:10 Post-WGLC: SenML
- 12:10–12:40 WG doc: RD, RD-DNS-SD
- 12:40–12:50 WG doc: pubsub
- 12:50–13:20 WG doc: oscoap

All times are in time-warped CEST

Friday (90 min)

- 11:50–11:55 Intro, Agenda
- 11:55–12:10 Post-WGLC: SenML
- 12:10–12:40 WG doc: RD, RD-DNS-SD
- 12:40–12:50 WG doc: pubsub
- 12:50–13:20 WG doc: oscoap

All times are in time-warped CEST

Friday (90 min)

- 11:50–11:55 Intro, Agenda
- 11:55–12:10 Post-WGLC: SenML
- 12:10–12:40 WG doc: RD, RD-DNS-SD
- 12:40–12:50 WG doc: pubsub
- 12:50–13:20 WG doc: oscoap

Object Security of CoAP (OSCOAP)

draft-ietf-core-object-security-04

CAPITALS

Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, RISE SICS

IETF 99, CoRE WG, Prague, Jul 19, 2017

Draft Status (v-04)

- https://github.com/core-wg/oscoap

- Minor editorial changes
- Blockwise uses draft-amsuess-core-repeat-request-tag-00

Issues left

- Check the issue tracker!
  https://github.com/core-wg/oscoap/issues

- Observe option processing simplification
- Remove OSCON
- Minor edits (replay window…)
- Test vectors

for Embedded font:
,-./0123456789:;<=>?
GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
wxyz{|}~¡¢£¤¥¦§¨©ª«¬¬®¯°±²³
ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâã
ïîïðñòóôõö÷øùúûüýþÿĀāĂăĄąĆćĈĉĊċČčĎďĐđĒēĔĕĖ
ĝĞğĠġĢģĤĥĦħĨĩĪīĬĭĮįİıĲĳĴĵĶķĹĺĻļĽľĿŀŁłŃńŅņŇňŊŋŌōŎŏŐőŒœŔŕŖŗŘřŚśŞşŠ
ŰúŲųŴŵŶŷŸŹźŻżŽžƒˆˇ˘˙˚˛˜˝‐–
‰‹›⁄
ĄĆĈĊČĎĐĒĔĖĘĚĜĞĠĢĤĦĨĪĬĮİĲĴĶĸĹĻĽĿŁŃŅŇŊŌŎŐŒŔŖŘŚŜŞŠŢŤŦŨŪŬŮŰŲ
ŽŞş–≤≠fifl

ΩΐΑΒΓΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΪΫΆΈΉΊΰα
λνξορςΣΤΥΦΧΨΩΪΫΟΥΩ

ЬЊЋЎЏАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЁЂЃЄЅІЇЈЉЊЋЎЏЪЂЄΘVVΓΎəæŴŵẂẁẄẅ

Interop Report

- Test specifications, reports, captures: https://github.com/EricssonResearch/OSCOAP

- 4 Interop (Feb, March, May, July)
- 6 implementations tested (C, python, java, C#, …)
- 15 tests on succeeding and failing OSCOAP processing

- Successfully interoperated

Next Steps

› One more update covering the remaining issues

› WGLC

for Embedded font:
,-./0123456789:;<=>?
GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
wxyz{|}~¡¢£¤¥¦§¨©ª«¬¬®¯°±²³
ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâã
ïîïðñòóôõö÷øùúûüýþÿĀāĂăĄąĆćĈĉĊċČčĎďĐđĒēĔĕĖ
ĜĝĞğĠġĢģĤĥĦħĨĩĪīĬĭĮįİıĲĳĴĵĶķĸĹĺĻļĽľĿŀŁłŃńŅņŇňŉŊŋŌōŎŏŐőŒœŔŕŖŗŘřŚśŜŝŞşŠ
ŰűŲųŴŵŶŷŸŹźŻżŽžƒˆˇ˘˙˚˛˜˝‐–—‘’‚“”„†‡•…‰‹›⁄
₣₤₧₫€™Ω∂∆∏∑−√∞∫≈≠≤≥◊fifl

ΩΐΑΒΓΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΪΫΆΈΉΊΰα
λνξορςΣΤΥΦΧΨΩΪΫΌΎΩ

ЬЊЋЎЏАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЁЂЃЄЅІЇЈЉЊЋЎЏЪЪΘΘѴѴҐґәæŴŵẀẁẂẃ

Thank you!

Comments/questions?

CAPITALS