Constrained RESTful Environments WG (core)

Chairs:

Jaime Jiménez <jaime.jimenez@ericsson.com>

Carsten Bormann <cabo@tzi.org>

Mailing List:

core@ietf.org

Jabber:

core@jabber.ietf.org

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

üBlue sheets
üScribe(s)

Note Well

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.

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

Agenda Bashing

All times are in time-warped CEST

Monday (120 min)

- **13:30–13:40 Intro, Agenda, Status**
- **13:40–13:50 Post-WGLC: Links-JSON (chairs)**
- **13:50–14:20 Post-WGLC: OSCORE (GS)**
- **14:20–14:45 Post-WGLC: SenML (AK)**
- **14:45–15:15 Up for WGLC soon: RD/DNS-SD (CA)**
- **15:15–15:30 Up for WGLC soon: COMI (AP)**

All times are in time-warped CEST

Tuesday (150 min)

- **09:30–09:35 Intro, Agenda**
- **09:35–10:00 Post-WGLC: CoCoA (CG)**
- **10:00–10:15 Getting ready: ERT (CA)**
- **10:15–10:25 Getting ready: OSCORE-Group (MT)**
- **10:25–10:40 New response codes (AK)**
- **10:40–10:55 Pending for EST (PV)**
- **10:55–11:05 Pubsub (MK)**
- **11:05–11:15 Dynlink/Interfaces (BS)**
- **11:15–11:25 Negotiation, AT (BS)**
- **11:25–11:35 dev URN (JA)**
- **11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …**

Draft-ietf-coap-tcp-tls → RFC 8323

✓

Published 2018-02-15

Supporting: RFC 8307 (2018-01-03)

Advertisements

- T2TRG Coexistence (see draft-feeney-t2trg-inter-network-01): Mon 17:30..18:00 Waterloo
- 6TiSCH stateless-proxy option (in draft-ietf-6tisch-minimal-security-05): Wed 13:30..15:00 Viscount
- DNSSD: Thu 09:30..12:00 Buckingham

RIOT Summit

September 13 – 14, 2018

Meet in Amsterdam!

We already support the Summit!

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

wolfSSL

Get involved too!

Call for Sponsors & Contributions

https://summit.riot-os.org/

All times are in time-warped CEST

Monday (120 min)

- **13:30–13:40 Intro, Agenda, Status**
- **13:40–13:50 Post-WGLC: Links-JSON (chairs)**
- **13:50–14:20 Post-WGLC: OSCORE (GS)**
- **14:20–14:45 Post-WGLC: SenML (AK)**
- **14:45–15:15 Up for WGLC soon: RD/DNS-SD (CA)**
- **15:15–15:30 Up for WGLC soon: COMI (AP)**

draft-ietf-core-links-json: Status

- Started Feb 2012 as a JSON version of 6690-to-be
  - Avoid the need for another parser
- Added CBOR variants mid-2015
- Focus: roundtrippable with RFC 6690
  - Inherit limitations of RFC 6690 (e.g., percent-encoding)
- Submitted to IESG on 2017-04-02
  - Lots of feedback
  - Related concepts in OCF spec
- Proposed Re-focus:
  - Still cover all of RFC 6690
  - Don’t inherit the limitations

Web Linking: RFC 5988 vs. RFC 8288

- RFC 6690 was based on RFC 5988
- Has since been updated to RFC 8288
  - More conscious use of ABNF
  - Clearer approach to Unicode and language tags
  - Clarifies role of serialization (of which RFC 6690 is one)
- RFC 6690 *not* updated to RFC 8288

- Links-json should use RFC 8288 as a base

Language tags

- **RFC 5988 (and this 8288) defines “starred” attributes**
  - **Encoding Unicode content, language tag**
- **RFC 6690 supports “title*”, but doesn’t do much with that**
- **JSON/CBOR should not be concerned with weird encoding issues**
- **Language tags are useful for human readable values**
- **So: do support them, but get rid of the “*” hack:**

```
{“href”: “…”, “rel”: “…”,
 “title”: {“de_AT”: “Übergrößenträger”}}
```

Is this the right way forward?

- Rebase on RFC 8288
  - Clean up “title*” etc.
- Explain how RFC 6690 documents become Links-json documents
- Otherwise, keep Links-json generally applicable and free of RFC 6690 idiosyncrasies

- Do not change the mandate that “/.well-known/core” is RFC 6690 link-format (!?)

All times are in time-warped CEST

Monday (120 min)

- **13:30–13:40 Intro, Agenda, Status**
- **13:40–13:50 Post-WGLC: Links-JSON (chairs)**
- **13:50–14:20 Post-WGLC: OSCORE (GS)**
- **14:20–14:45 Post-WGLC: SenML (AK)**
- **14:45–15:15 Up for WGLC soon: RD/DNS-SD (CA)**
- **15:15–15:30 Up for WGLC soon: COMI (AP)**

OSCORE

draft-ietf-core-object-security-11

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

IETF 101, CoRE WG, London, Mar 19, 2018

Status (v-11)

- Several implementations
  - Java (Californium): https://bitbucket.org/lseitz/oscoap_californium
  - C (Contiki, Erbium): https://github.com/Gunzter/contiki-oscoap
  - Python (aiocoap): https://github.com/chrysn/aiocoap
  - C# (CoAP-CSharp): https://github.com/Com-AugustCellars/CoAP-CSharp
  - Python (CoAP for openwsn): https://github.com/openwsn-berkeley/coap
  - C (openwsn-fw): https://github.com/openwsn-berkeley/openwsn-fw
  - Java (Californium, v-03) https://github.com/lukadschaak/oscore

- Several interops done
  - Spec and reports: https://github.com/EricssonResearch/OSCOAP

Status (v-11)

- IETF Last Call ended: IESG evaluation
- Some post-Last-Call reviews
- Up-to-date handling of review comments on the wiki: https://github.com/core-wg/oscoap/wiki
- All but a few specific review comments addressed.

Review Comments

- “The document needs a security analysis section”
- "implications of modifications of unprotected fields"
- Proposal: Add an appendix describing the security properties of the protocol:
  - Assumptions on intermediaries
  - Protected header fields, security guarantees
  - Unprotected fields, consequences

Review Comments

- "Nonce construction: Why is Sender ID included in the nonce?"
- Answer: Designed for supporting notifications and interchange of client and server roles
- Proposal: Prove (key, nonce) uniqueness in the new appendix

Review Comments

- “But this design actively works against any involvement of intermediaries.”

- Answer: The design supports intermediaries e.g. performing forwarding and translation
- In the general case, proxies can read but not modify without being detected.

- Proposal: Clarify this in the new appendix.

Review Comments

- “neglecting to address important and difficult parts of the problem like key exchange”

- Answer: Key establishment is addressed.
  - The ACE/OAuth 2.0 framework may be used.
  - Some IoT deployments require PSK.

- Key exchange for OSCORE is discussed in ACE since IETF#95.

Review Comments: HTTP 1(2)

- “This protocol abuses HTTP by tunneling over it”
- Answer: Yes. This was requested.

- "Missing [A]BNF"
- Answer: Agreed, included

- "Does the COAP-HTTP gateway understand the significance of the new header field and insert the media type when translating? "
- Answer: Yes

Review Comments: HTTP 2(2)

- "A new media type is defined, but I don't see any mention of a codepoint for use with COAP"
- Proposal: Not needed for this draft, but will include that for other potential use

- "What if the request is redirected by a server that doesn't understand OSCORE?"
- Question for WG: shall we support HTTP redirects?

- Question for WG: Rename HTTP header field:
- 'Object-Security' → 'CoAP-Object-Security'

Reviews Comments: Summary Proposal

- Clarifications of the points brought up
- Editorials
- New appendix:
  - D. Overview of Security Properties
    - D.1. Supporting Proxy Operations
    - D.2. Protected Message Fields
    - D.3. Uniqueness of (key, nonce)
    - D.4. Unprotected Message Fields

- Details on the CoRE WG Github Commits

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:50 Post-WGLC: Links-JSON (chairs)
- 13:50–14:20 Post-WGLC: OSCORE (GS)
- 14:20–14:45 Post-WGLC: SenML (AK)
- 14:45–15:15 Up for WGLC soon: RD/DNS-SD (CA)
- 15:15–15:30 Up for WGLC soon: COMI (AP)

Media Types for Sensor Measurement Lists (SenML)

IETF 101, London

draft-ietf-core-senml-13

Ari Keränen

Status

- Done!
  - IETF LC ongoing
  - IESG Telechat April 19th

- Since -12: "+exi" -> "-exi" & editorial fixes

- Still: could add expert guidance clarification for new values: must have "Value" in the long name

Early assignments

- Suggested CoAP Content-Format IDs
  - XML IDs in 2-byte range

Media type	ID
application/senml+json	110
application/sensml+json	111
application/senml+cbor	112
application/sensml+cbor	113
application/senml-exi	114
application/sensml-exi	115
application/senml+xml	310
application/sensml+xml	311

Early assignments

- How about SenML Fields?

Media types for FETCH & PATCH with SenML

IETF 101, London

draft-keranen-senml-fetch-00

Ari Keränen & Mojan Mohajer

SenML IPSO SO example

```
[ {"bn":"2001:db8::2/3306/0/",
   "n":"5850", "vb":true},
  {"n":"5851", "v":42},
  {"n":"5852", "v":1200},
  {"n":"5750", "vs":"Ceiling light"} ]
```

SenML IPSO SO example

```
[ {"bn":"2001:db8::2/3306/0/",
   "n":"5850", "vb":true},
  {"n":"5851", "v":42},
  {"n":"5852", "v":1200},
  {"n":"5750", "vs":"Ceiling light"} ]
```

- Want to retrieve/change only 5850 **and** 5851
- And want to avoid exchanging full representations or doing multiple requests

CoAP FETCH / PATCH (RFC 8132)

- CoAP methods, FETCH, PATCH, and iPATCH, which are used to access and update parts of a resource
- Needs payload format; dependent on the resource representation format

SenML FETCH format

- Modeled after SenML JSON format: simple parsing on constrained things with SenML support
- Just indicate names, and potentially times, of the SenML records to fetch

```
[ {"bn":"2001:db8::2/3306/0/", "n":"5850"},
  {"n":"5851"} ]
```

SenML PATCH format

- Same as FETCH format, but with the value(s) to set
    - Essentially a subset of the JSON Merge Patch format

```
[ {"bn":"2001:db8::2/3306/0/", "n":"5850", "vb":false},
  {"n":"5851", "v":10} ]
```

Wild cards

- Optimization for selecting many SenML Records with one FETCH/PATCH Record
- Useful with large amounts of SenML Records (e.g., many IPSO objects on a device)
    - "Get all temperature sensor values"
    - "Dim all lights to 10%"

Proposed format

- New SenML Field "ff" ("fetch filter")
  - Used instead of the name field and concatenated to base name like the name field
  - Contains wild card characters "*"
  - Matched to SenML Record Names
- Wild card matches all characters until next "/" or ":"

```
[ {"bn":"2001:db8::2/", "ff":"3306/0/58*"} ]
```

(This matches all records in the example except "3306/0/5750")

(Wild Card) Considerations

- Need something **simple** now: constrained devices
  - Wild card **seemed** most suitable
- Using new Field(s) enables easy extensibility
  - Alternative: re-purpose "n" and "bn" fields
- Should wild card support be MUST?
  - How to indicate "not supporting wild cards"? Now suggesting "4.00 Bad Request" but doesn't seem right
- Regular expressions? New field probably

- PATCH operation codes needed (append, delete, …)?
- Can just re-use SenML content format IDs?
- Interest in CoRE WG to work on this?

All times are in time-warped CEST

Monday (120 min)

- **13:30–13:40 Intro, Agenda, Status**
- **13:40–13:50 Post-WGLC: Links-JSON (chairs)**
- **13:50–14:20 Post-WGLC: OSCORE (GS)**
- **14:20–14:45 Post-WGLC: SenML (AK)**
- **14:45–15:15 Up for WGLC soon: RD/DNS-SD (CA)**
- **15:15–15:30 Up for WGLC soon: COMI (AP)**

Resource Directory

`draft-ietf-core-resource-directory`
`draft-ietf-core-rd-dns-sd`
`draft-amsuess-rd-replication`

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

2018-03-19

Status

pretty much ready

Issue tracker / pull requests

107 down, ~~1 to go~~ 2 to go

Issue #91

plug test upcoming

contact me: `c@amsuess.com`

Changes since -12

- Cleanup and clarification
  - Clarified observation behavior
  - Refer to t2trg-rel-impl for server metadata / versioning
  - Reduced the significance of domains (removed from figure 2)
- Added ”all resource directory” nodes MC address
- Resolve RFC6690-vs-8288 resolution ambiguities
  - Require registered links not to be relative when using anchor
  - Return absolute URIs in resource lookup
- Work with replication without really changing the RD
  - Multiple RDs can be found, and can have absolute addresses
  - Endpoints from other RDs can be members of a group

rd-replication

- Different registration addresses
- Different lookup addresses
- Eventually consistent results

```
      /'''''''\______/'''''\__/''''''''\
   /-                                   -\
   |,                                    |
     \,,,                           ,~''
         \_____/'''\__________/''''   \
          |               |            \
/''''''\  |     /''''''\  |  /''''''\   |  /''''''\
| RD-A |--+     | RD-B |--+--| RD-C |   +--| LP-Z |
| LP-X |  |     | LP-Y |  |  |      |   |  |      |
\_____1/  |     \_____2/  |  \____3/    |  \_____4/
          |               |             |
    +--+--+            +--+--+          +--+
    E  E  C            E  E  E          C  C
```

rd-dns-sd

-01: updated with introduction

`rd-dns-sd`

hooks into RD extension points

Next steps for `resource-directory`

reviews

plug test

All times are in time-warped CEST

Monday (120 min)

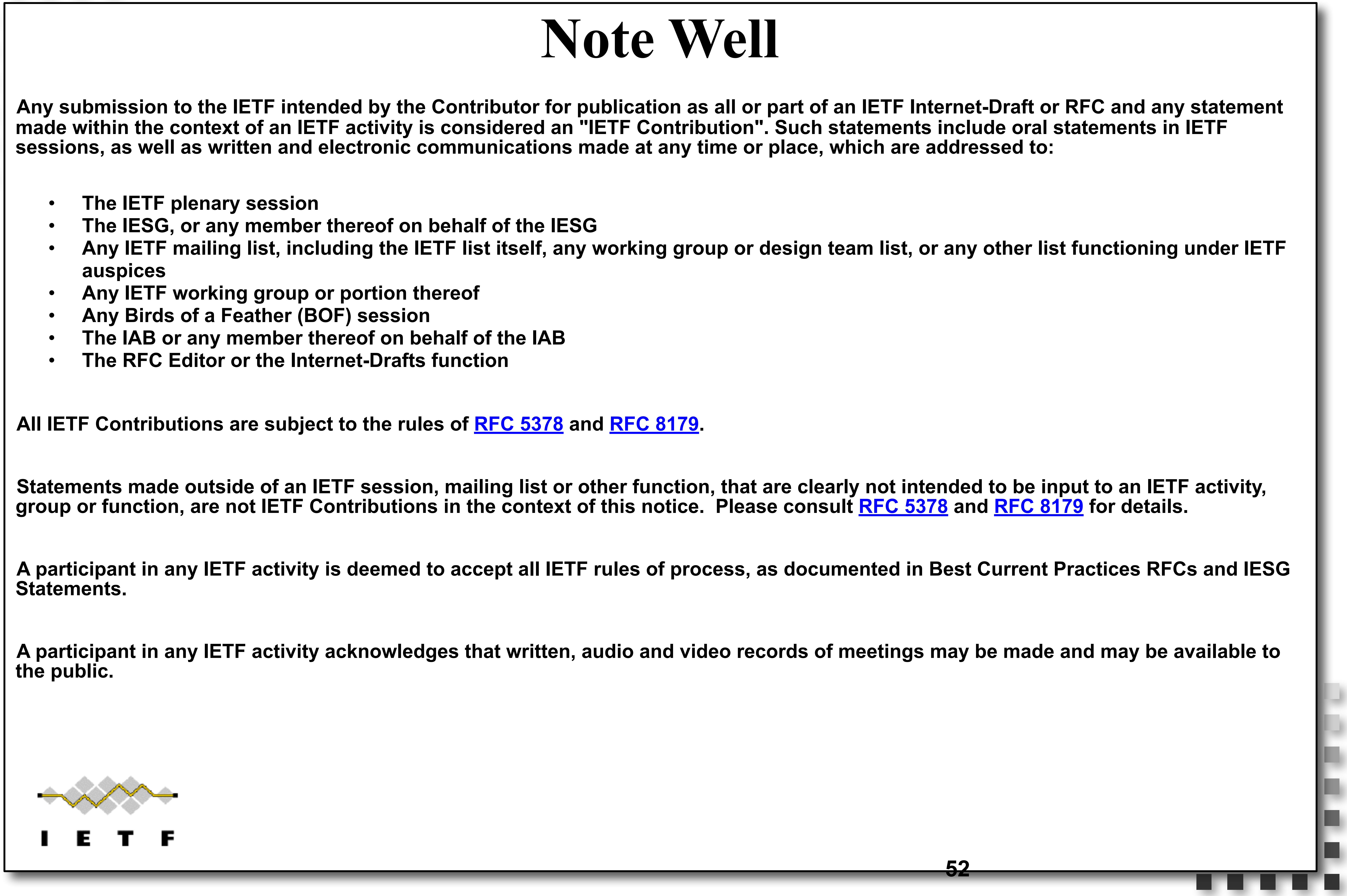
- **13:30–13:40 Intro, Agenda, Status**
- **13:40–13:50 Post-WGLC: Links-JSON (chairs)**
- **13:50–14:20 Post-WGLC: OSCORE (GS)**
- **14:20–14:45 Post-WGLC: SenML (AK)**
- **14:45–15:15 Up for WGLC soon: RD/DNS-SD (CA)**
- **15:15–15:30 Up for WGLC soon: COMI (AP)**

- **We assume people have read the drafts**

- **Meetings serve to advance difficult issues by making good use of face-to-face communications**

- **Note Well: Be aware of the IPR principles, according to RFC 8179 and its updates**

üBlue sheets
üScribe(s)



Note Well

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

Tuesday (150 min)

- **09:30–09:35 Intro, Agenda**
- **09:35–10:00 Post-WGLC: CoCoA (CG)**
- **10:00–10:15 Getting ready: ERT (CA)**
- **10:15–10:25 Getting ready: OSCORE-Group (MT)**
- **10:25–10:40 New response codes (AK)**
- **10:40–10:55 Pending for EST (PV)**
- **10:55–11:05 Pubsub (MK)**
- **11:05–11:15 Dynlink/Interfaces (BS)**
- **11:15–11:25 Negotiation, AT (BS)**
- **11:25–11:35 dev URN (JA)**
- **11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …**

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:35 Intro, Agenda
- 09:35–10:00 Post-WGLC: CoCoA (CG)
- 11:25–11:35 dev URN (JA)
- 10:00–10:15 Getting ready: ERT (CA)
- 10:15–10:25 Getting ready: OSCORE-Group (MT)
- 10:25–10:40 New response codes (AK)
- 10:40–10:55 Pending for EST (PV)
- 10:55–11:05 Pubsub (MK)
- 11:05–11:15 Dynlink/Interfaces (BS)
- 11:15–11:25 Negotiation, AT (BS)
- 11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …

All times are in time-warped CEST

Tuesday (150 min)

- **09:30–09:35 Intro, Agenda**
- **09:35–10:00 Post-WGLC: CoCoA (CG)**
- **10:00–10:15 Getting ready: ERT (CA)**
- **10:15–10:25 Getting ready: OSCORE-Group (MT)**
- **10:25–10:40 New response codes (AK)**
- **10:40–10:55 Pending for EST (PV)**
- **10:55–11:05 Pubsub (MK)**
- **11:05–11:15 Dynlink/Interfaces (BS)**
- **11:15–11:25 Negotiation, AT (BS)**
- **11:25–11:35 dev URN (JA)**
- **11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …**

CoAP Simple Congestion Control/Advanced (CoCoA)

draft-ietf-core-cocoa-03

Carsten Bormann – Universität Bremen TZI

August Betzler – Fundació i2Cat

Carles Gomez, Ilker Demirkol – Univ. Politècnica de Catalunya

Status

- WG state: “Submitted to IESG for publication”
- Last revision is -03
  - Mostly editorial updates
  - Addresses comments by:
    - Wesley Eddy (TSVART Early Review)
    - Mirja Kühlewind (Responsible AD)
- Next revision
  - Needs to address comments by:
    - Scott Bradner (OPSDIR Telechat Review)
    - Vincent Roca (SECDIR Review)
    - Christer Holmberg (Gen-ART Telechat Review)

Updates in -03 (I)

- Section 1
  - Paragraph previously in Section 5, now more general: overview on CoCoA
    - RTO based on (weak or strong) RTTs
    - Weak RTTs: reaction to congestion with a lower sending rate
    - For NONs, sending rate limited to 1/RTO
      - More conservative than RFC 7641 (Observe): 1/RTT

Updates in -03 (II)

- Section 3
  - Added details on scenarios where CoCoA has been found to perform well
    - Latencies: milliseconds to peaks of dozens of seconds
      - Comment from Jaime: which reference contributes to what within this range
    - Single-hop and multihop network topologies
    - Link technologies: IEEE 802.15.4, GPRS, UMTS, Wi-Fi
  - Added that CoCoA is also expected to work suitably across the general Internet

Updates in -03 (III)

- Section 4.2
  - Added that default weight values for strong and weak RTO estimators have been found to work well in evaluations (Appendix A)
- Section 4.2.1
  - Added an explicit note on VBF replacing RFC 6298 simple exponential backoff

Updates in -03 (IV)

- Section 4.3
  - State of RTO estimators for an endpoint
    - Should be kept long enough to avoid frequent returns to inappropriate initial values
    - For default parameters in CoAP, it is RECOMMENDED to keep it for at least 255 s
      - Was a “MUST” in -02

- Minor editorial updates throughout the document

Next revision (I)

- Scott Bradner’s comment
  - The draft makes no reference to RFC 5033…
    - “Specifying New Congestion Control Algorithms”
  - … But we have taken RFC 5033 into account in the design of CoCoA

Next revision (II)

- RFC 5033 guidelines
  - 0. Differences with congestion control principles (RFC 2914)
    - CoCoA design considers such principles (preventing congestion collapse, fairness, optimizing performance)
  - 1. Impact on standard TCP, SCTP, DCCP
    - No negative impact
  - 2. Difficult environments
    - CoCoA has been designed for “difficult environments”
  - 3. Investigating a range of environments
    - Done (see slide 4)

Next revision (III)

- RFC 5033 guidelines
  - 4. Protection against congestion collapse
    - VBF of 1.5, 2 or 3 (always greater than 1)
  - 5. Fairness within the alternate cong. control mech.
    - High fairness measured (thanks to the VBF)
  - 6. Performance with misbehaving nodes
    - Considered. Weak estimator role
  - 7. Responses to sudden or transient events
    - CoCoA restores “normal” network state quickly
  - 8. Incremental deployment
    - CoCoA runs correctly in current CNNs and in CNN-cloud

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)

- 09:30–09:35 Intro, Agenda
- 09:35–10:00 Post-WGLC: CoCoA (CG)
- 10:00–10:15 Getting ready: ERT (CA)
- 10:15–10:25 Getting ready: OSCORE-Group (MT)
- 10:25–10:40 New response codes (AK)
- 10:40–10:55 Pending for EST (PV)
- 10:55–11:05 Pubsub (MK)
- 11:05–11:15 Dynlink/Interfaces (BS)
- 11:15–11:25 Negotiation, AT (BS)
- 11:25–11:35 dev URN (JA)
- 11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:35 Intro, Agenda
- 09:35–10:00 Post-WGLC: CoCoA (CG)
- 10:00–10:15 Getting ready: ERT (CA)
- 10:15–10:25 Getting ready: OSCORE-Group (MT)
- 10:25–10:40 New response codes (AK)
- 10:40–10:55 Pending for EST (PV)
- 10:55–11:05 Pubsub (MK)
- 11:05–11:15 Dynlink/Interfaces (BS)
- 11:15–11:25 Negotiation, AT (BS)
- 11:25–11:35 dev URN (JA)
- 11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …

All times are in time-warped CEST

Tuesday (150 min)

- **09:30–09:35 Intro, Agenda**
- **09:35–10:00 Post-WGLC: CoCoA (CG)**
- **10:00–10:15 Getting ready: ERT (CA)**
- **10:15–10:25 Getting ready: OSCORE-Group (MT)**
- **10:25–10:40 New response codes (AK)**
- **10:40–10:55 Pending for EST (PV)**
- **10:55–11:05 Pubsub (MK)**
- **11:05–11:15 Dynlink/Interfaces (BS)**
- **11:15–11:25 Negotiation, AT (BS)**
- **11:25–11:35 dev URN (JA)**
- **11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …**

Secure group communication for CoAP

draft-ietf-core-oscore-groupcomm-01

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

IETF 101, CoRE WG, London, March 20th, 2018

Updates from -00 (1/2)

- Major updates and restructuring to address reviews
  - Thanks to Esko Dijk and Peter van der Stok

- Section 1.1 – Terminology
  - Added definition of group as “security group”
  - Not to be confused with “network group” or “application group”

- Section 2 – Security Context
  - Clarified establishment/derivation of contexts
  - Added table for additional elements wrt OSCORE

Updates from -00 (2/2)

- Section 3 – COSE Object
  - Examples or request and response (before and after compression)
  - CounterSignature0 is used rather than CounterSignature
  - ‘external_aad’ includes also the signature algorithm
  - ‘external_aad’ does not include the Group Identifier (Gid) any more

- Section 6 – NEW
  - List of responsibilities of the Group Manager

- Appendices
  - Appendix A: assumptions and security objectives (former section)
  - Appendix B: additional details on considered use cases
  - Appendix C: added actual example of Gid format (prefix + epoch)
  - Appendix D: join description aligned with *draft-palombini-ace-key-groupcomm*

Points for discussion (1/2)

- Independence of Security Group from IP addresses
  - Requests may be multicast or unicast (e.g. selective retransmissions)
  - Current context retrieval based on Gid and multicast IP address
  - Change to use only the Gid as kid context for context retrieval ?

- Fixed part of the Gid
  - Currently random and large enough to avoid global collisions
  - Change to neglect randomness and large size ?
  - Tie-breaker can be trying the keying material from multiple contexts

Points for discussion (2/2)

- Current terminology explicitly points at multicast
  - Replace “Multicaster” with “Sender” ?
  - Replace “(Pure) Listener” with “(Pure) Recipient”?
  - This would simplify request/assignment of roles upon joining

- Current description of the join process
  - Appendix D.1: exchanged information
  - Appendix D.2: provisioning/retrieval of public keys
  - Appendix D.3: pointer to the ACE-based approach
  - What should be kept in this document?
  - Should we keep a general description in case ACE is not used?

Implementation

- OSRAM Innovation
  - Developed in C
  - MediaTek LinkIt Smart 7688
  - Aligned with individual submission at IETF99

- Proof-of-concept for Contiki OS
  - Wismote (MSP430; TI CC2520)
  - SmartRF (MSP430; TI CC2538)
  - Aligned with individual submission at IETF99
  - https://github.com/tdrlab/mcast

- Next steps
  - Move forward to interoperability tests
  - Is it feasible already at IETF102?

Related activity

- *draft-tiloca-ace-oscoap-joining*
  - Referred by Appendix D.3

- Join an OSCORE group using the ACE framework
  - Joining node → Client
  - Group Manager → Resource Server
  - Message formats aligned with *draft-palombini-ace-key-groupcomm*

- Leverage protocol-specific profiles of ACE
  - CoAP-DTLS profile *draft-ietf-ace-dtls-authorize*
  - OSCORE profile *draft-ietf-ace-oscore-profile*

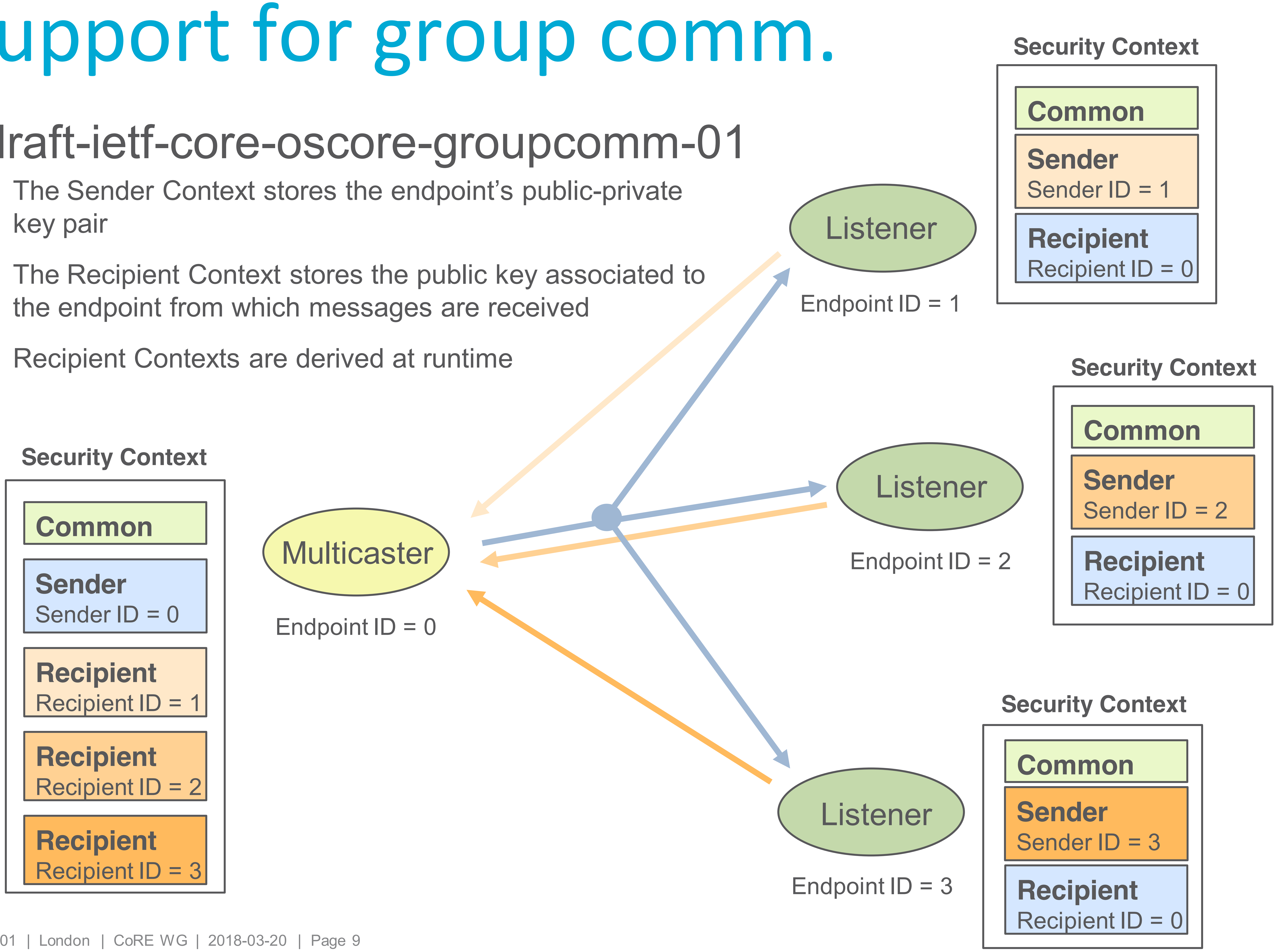
Thank you!

Comments/questions?

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

Support for group comm.

- draft-ietf-core-oscore-groupcomm-01
  - 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



All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:35 Intro, Agenda
- 09:35–10:00 Post-WGLC: CoCoA (CG)
- 10:00–10:15 Getting ready: ERT (CA)
- 10:15–10:25 Getting ready: OSCORE-Group (MT)
- 10:25–10:40 New response codes (AK)
- 10:40–10:55 Pending for EST (PV)
- 10:55–11:05 Pubsub (MK)
- 11:05–11:15 Dynlink/Interfaces (BS)
- 11:15–11:25 Negotiation, AT (BS)
- 11:25–11:35 dev URN (JA)
- 11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …

Too Many Requests Response Code for CoAP

IETF 101, London

draft-keranen-core-too-many-reqs-00

Ari Keränen

Background

- CoAP client can cause overload in server with too frequent requests
- How can server tell client to back off
- HTTP error code 429 “Too many requests”
- Proposal: register 4.29 for CoAP
  - With MaxAge to indicate when it’s OK to request again
- Originally part of CoAP Pub/sub Broker draft; also OCF interest

What requests are OK?

- Current text: Client “SHOULD NOT send the same request to the server before the time indicated in the Max-Age option has passed”
- Other requests? Should server be able to give guidance what else is (not) OK during this time?
  - Example: GET instead of PUBLISH
- Sounds like a generic problem worth a generic solution; probably out of scope for this draft

Next steps

- Bundle with other non-controversial Response Codes?
- WG item?

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:35 Intro, Agenda
- 09:35–10:00 Post-WGLC: CoCoA (CG)
- 10:00–10:15 Getting ready: ERT (CA)
- 10:15–10:25 Getting ready: OSCORE-Group (MT)
- 10:25–10:40 New response codes (AK)
- 10:40–10:55 Pending for EST (PV)
- 10:55–11:05 Pubsub (MK)
- 11:05–11:15 Dynlink/Interfaces (BS)
- 11:15–11:25 Negotiation, AT (BS)
- 11:25–11:35 dev URN (JA)
- 11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …

‘Pending’ response code

Peter van der Stok, Klaus Hartke

IETF 101 - CoRE Working Group

Motivation

RFC 7030:
Enrollment over Secure Transport (EST)
uses http response 202 when result is not
immediately available (say: 3 hours) in
response to GET or POST.

No such response code exists for coap.
This functionality is needed for EST over coap.

HTTP 202

The request has been accepted for processing, but the processing has not been completed. The request might or might not eventually be acted upon, as it might be disallowed when processing actually takes place.
The representation sent with this response ought to describe the request's current status and point to (or embed) a status monitor that can provide the user with an estimate of when the request will be fulfilled.

Use cases

draft-ietf-ace-coap-est specifies requests to servers to verify a node’s identity; this may need manual intervention and takes a minimum response time

draft-ietf-core-coap-pubsub specifies a server to send a response to the client to indicate a valid request but may contain an empty payload.

draft-keranen-core-too-many-reqs specifies that response is available after minimum response time

History

A new response code (e.g. 2.06) was deemed harmful for proxies. (They will return 5.01 (Not Implemented))

An extension to response code 5.03 “Service Unavailable” does not cover the case because service is available

This draft specifies a content format “60001” extension to existing response codes

Details

- Pending response indicates that target resource exists, but no representation is available yet.
- Location may be specified where result will become available.
- Allows multiple clients to have multiple concurrent requests open at the server.
- Client has to retry with GET request after Max-Age.
- Can be used in conjunction with “observe”

Pushing application-specific state machines into CoAP?

- How should application-specific state machines be added to CoAP applications?
- REST approach: transfer **representations**
- Need to define **media types** for those application states
- Related trial balloon: draft-bormann-core-maybe-00

All times are in time-warped CEST

Tuesday (150 min)

- 09:30–09:35 Intro, Agenda
- 09:35–10:00 Post-WGLC: CoCoA (CG)
- 10:00–10:15 Getting ready: ERT (CA)
- 10:15–10:25 Getting ready: OSCORE-Group (MT)
- 10:25–10:40 New response codes (AK)
- 10:40–10:55 Pending for EST (PV)
- 10:55–11:05 Pubsub (MK)
- 11:05–11:15 Dynlink/Interfaces (BS)
- 11:15–11:25 Negotiation, AT (BS)
- 11:25–11:35 dev URN (JA)
- 11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …

All times are in time-warped CEST

Tuesday (150 min)

- **09:30–09:35 Intro, Agenda**
- **09:35–10:00 Post-WGLC: CoCoA (CG)**
- **10:00–10:15 Getting ready: ERT (CA)**
- **10:15–10:25 Getting ready: OSCORE-Group (MT)**
- **10:25–10:40 New response codes (AK)**
- **10:40–10:55 Pending for EST (PV)**
- **10:55–11:05 Pubsub (MK)**
- **11:05–11:15 Dynlink/Interfaces (BS)**
- **11:15–11:25 Negotiation, AT (BS)**
- **11:25–11:35 dev URN (JA)**
- **11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …**

All times are in time-warped CEST

Tuesday (150 min)

- **09:30–09:35 Intro, Agenda**
- **09:35–10:00 Post-WGLC: CoCoA (CG)**
- **10:00–10:15 Getting ready: ERT (CA)**
- **10:15–10:25 Getting ready: OSCORE-Group (MT)**
- **10:25–10:40 New response codes (AK)**
- **10:40–10:55 Pending for EST (PV)**
- **10:55–11:05 Pubsub (MK)**
- **11:05–11:15 Dynlink/Interfaces (BS)**
- **11:15–11:25 Negotiation, AT (BS)**
- **11:25–11:35 dev URN (JA)**
- **11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …**

All times are in time-warped CEST

Tuesday (150 min)

- **09:30–09:35 Intro, Agenda**
- **09:35–10:00 Post-WGLC: CoCoA (CG)**
- **10:00–10:15 Getting ready: ERT (CA)**
- **10:15–10:25 Getting ready: OSCORE-Group (MT)**
- **10:25–10:40 New response codes (AK)**
- **10:40–10:55 Pending for EST (PV)**
- **10:55–11:05 Pubsub (MK)**
- **11:05–11:15 Dynlink/Interfaces (BS)**
- **11:15–11:25 Negotiation, AT (BS)**
- **11:25–11:35 dev URN (JA)**
- **11:35–12:00 Flextime: OPC/UA (CP), Time scale (LT), …**

OPC UA Message Transmission Method over CoAP

draft-wang-core-opcua-transmission-03

Ping Wang, Chenggen Pu,
Heng Wang, Junrui Wu, Yi Yang,
Lun Shao, Jianqiang Hou

London, March 20, 2018

Status

- Last version is 02.
- Made some meaningful changes according to the last meeting comments.
- Keep the draft updated.

What We Have Updated

Three use cases:

Offline/Online diagnostic system for resource-constrained factories,
Factory data monitoring based on web pages,
Factory data analysis based on cloud.

Consolidate two transmission schemes into one:

Consolidate the proxy for OPC UA-CoAP and the direct transmission into one to realize better transmission performance.

Next Steps

Contact with OPC Foundation to get feedback.

Implement the transmission schemes mentioned above over a reasonable architecture.

Comments or Questions?

Thank you!