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

http://6lowapp.net

- **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://6lowapp.net

core@IETF97, 2016-11-16..-18

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

2018-08-15 Interim

- **# Status (~ 1505Z)**
  - **multipart-ct and CoAPs-EST early allocation status (Klaus)**
  - **4.29 status (cabo)**
- **# Work by other WGs (~ 1510Z)**
  - **DOTS: Hop-Limit option (Klaus, possibly DOTS people)**
  - **DOTS: Redirect response code (cabo, possibly DOTS people)**
  - **6tisch stateless proxy congestion control (or, CC for proxies in general)**
- **# Progressing our own**
  - **echo/request-tag (chairs)**
- **# And, if there is any time left:**
  - **6tisch minimal security stateless proxy support (cabo)**
- **# Wrapup (~ 1550Z):**
  - **RD interop event: When; details...**
  - **Planning the next interims**

http://6lowapp.net

core@IETF97, 2016-11-16..-18

Status

- **Early Allocations for CoAP EST (Klaus)**
- **4.29 (too-many-reqs) — publication requested**

core@IETF97, 2016-11-16..-18

DOTS: Hop-Limit option

- **draft-ietf-dots-signal-channel-22**
- **Hop-Limit: Option counted down by each proxy forwarding**
- **Zero → error**

- **Would this be a good general addition?**
- **How to make this work for DOTS**
  - **Elective?**
  - **Safe-to-forward?**

DOTS: Redirect response code

- **CoAP does not have redirect — for a reason**
  - Don't want the state machine
  - HTTP redirect is often done in the stack — should be application issue

- **BE EXPLICIT!?**

Privacy and CoAP Redirects

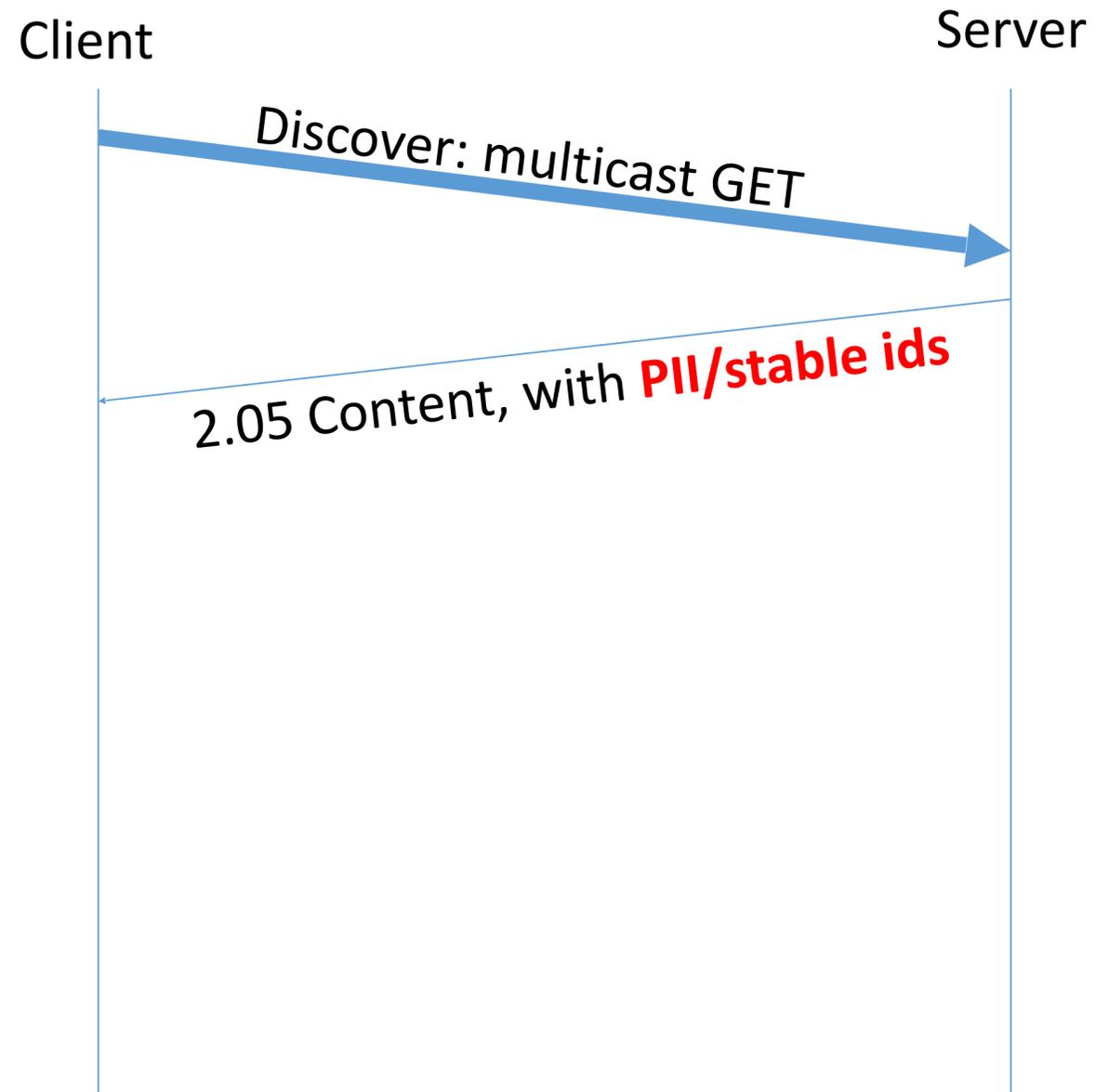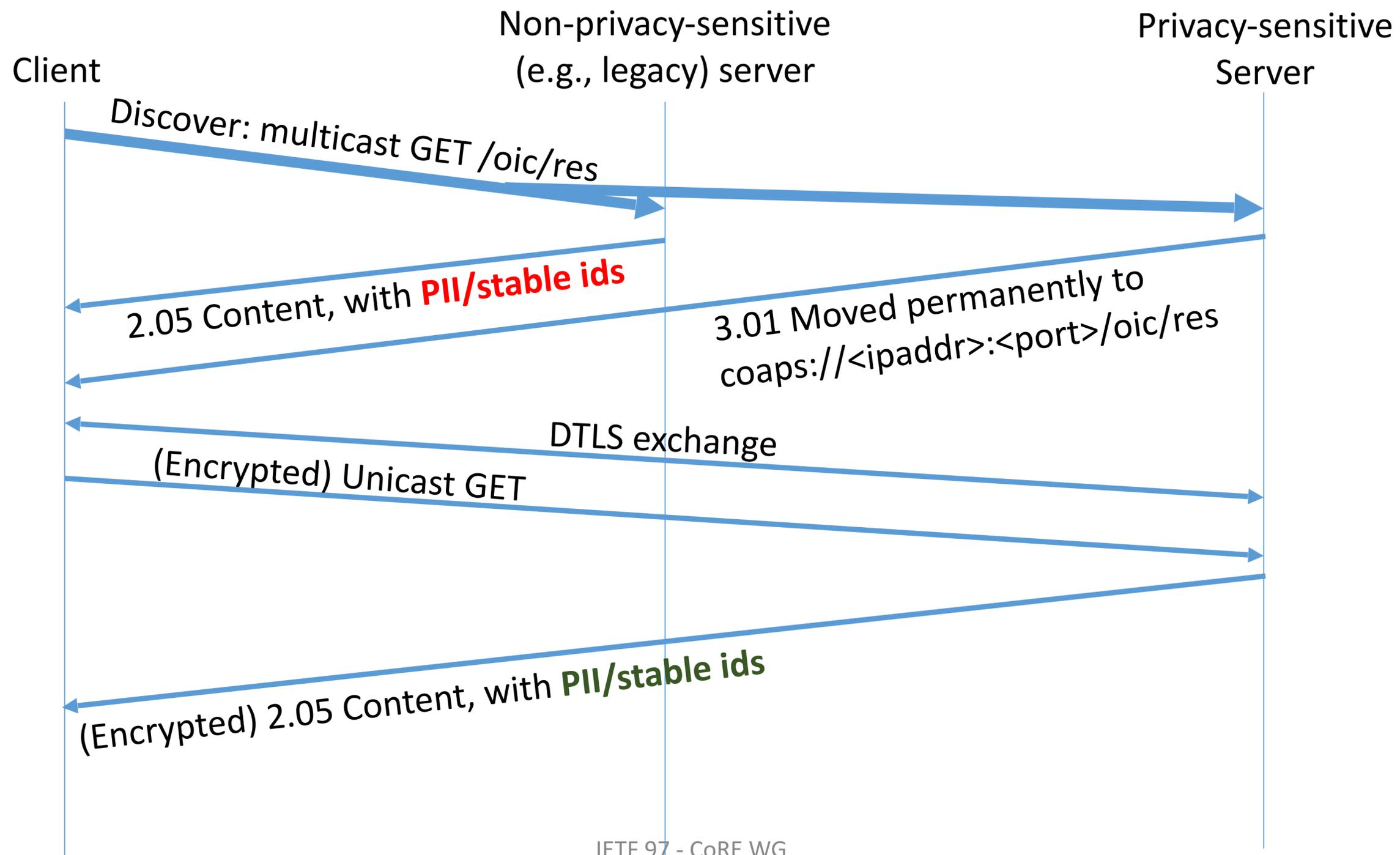https://tools.ietf.org/html/draft-thaler-core-redirect

Background

Open Connectivity Foundation (OCF) does IoT schemas, certification, etc.

- OCF uses COAP
- OCF does not want to fork COAP
- OCF found privacy issues
- OCF needs some solution regardless of whether IETF or not
- OCF strongly prefers a generic (non-OCF-specific) solution
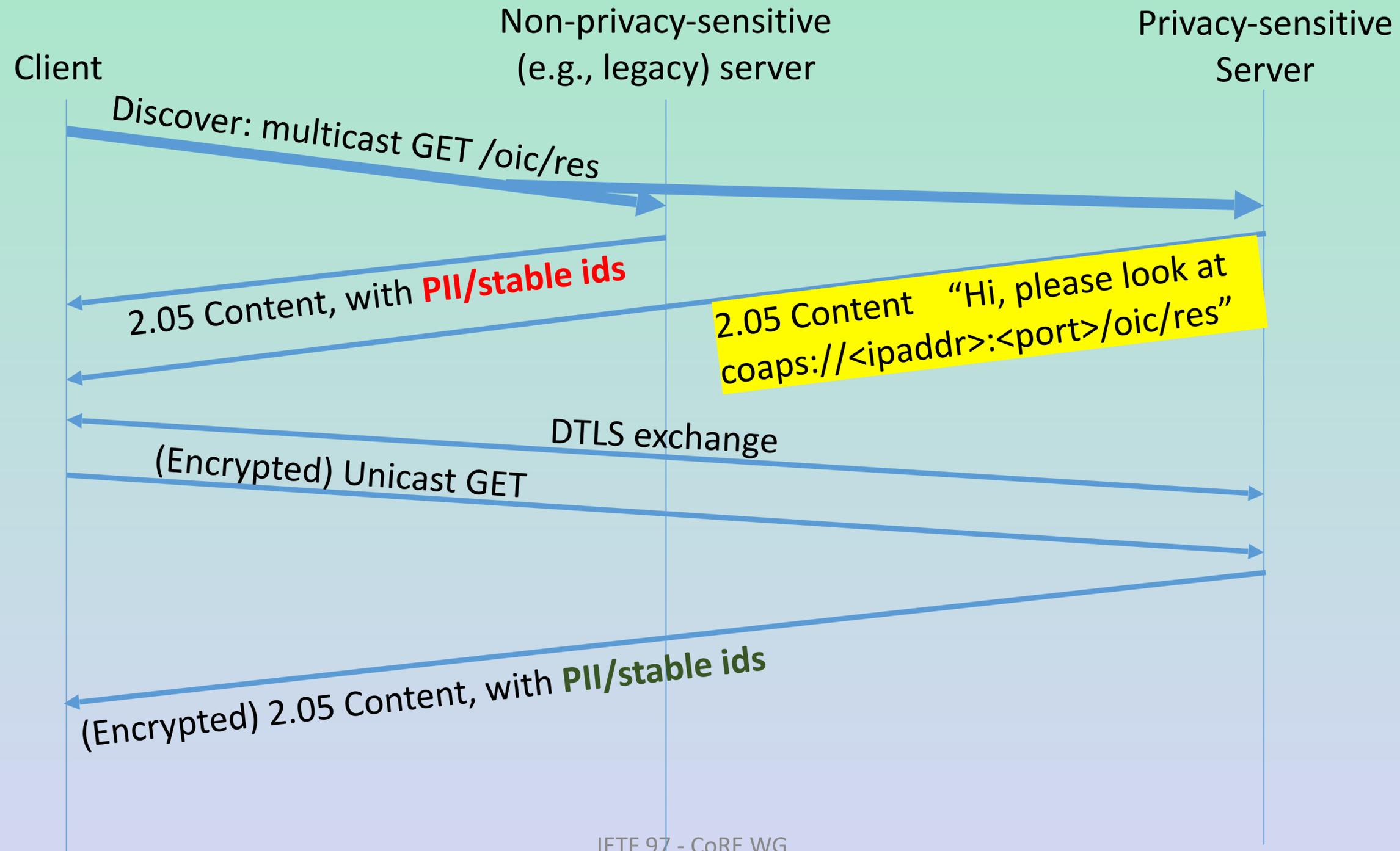- OCF prefers it be done by IETF

Today's problem with PII and stable id's

Client   Server

Discover: multicast GET

2.05 Content, with **PII/stable ids**

With redirect

Client | Non-privacy-sensitive (e.g., legacy) server | Privacy-sensitive Server

Discover: multicast GET /oic/res

2.05 Content, with **PII/stable ids**

3.01 Moved permanently to coaps://<ipaddr>:<port>/oic/res

DTLS exchange

(Encrypted) Unicast GET

(Encrypted) 2.05 Content, with **PII/stable ids**

Sketch for an approach without redirect

Client   Non-privacy-sensitive (e.g., legacy) server   Privacy-sensitive Server

Discover: multicast GET /oic/res

2.05 Content, with **PII/stable ids**

2.05 Content   "Hi, please look at coaps://<ipaddr>:<port>/oic/res"

DTLS exchange

(Encrypted) Unicast GET

(Encrypted) 2.05 Content, with **PII/stable ids**

Alternatives considered

- Use a Resource Directory
  - Same issue can arise with discovering RD to start with
  - Don't want to have to depend on deploying an RD in all cases

- Use a success response with different content
  - More complex & error-prone since requires each relevant entity handler (e.g., app) to be aware rather than base coap layer in one place
  - Different from other protocols (http, etc.)

- Alternative-Address option in coap-tcp-tls
  - Requires same URI scheme, so cannot redirect from coap to coaps

- Use a multicast security mechanism
  - Good if it can exist longer term, but don't see it happening soon

Details

- RFC 7252 today:
  - Location-Path and Location-Query already exist
  - Other values reserved for future Location-* options
- Add Option numbers for Location-Scheme and Location-Authority
- Add Response Code "3.01 Moved Permanently" for parity with HTTP

Redirect alone is not sufficient

There is a separate CFRG problem:

- one must also use an authentication scheme that does not reveal a stable identifier to clients before authentication is complete

- mutual auth schemes exist (e.g., "secret handshake" paper in SOSP 2003) that only reveal the identity of both endpoints if authentication succeeds, but not yet available in current standards and popular code bases

Discussion

- WG adoption?

6tisch stateless proxy congestion control

- **As per CoAP, proxy needs to run congestion control towards origin server (as does any client)**
- **6tisch: proxy is stateless, let the clients do the backoff**

- **How do we do this in general with proxies?**
- **Routers don't do congestion control, either?**

draft-ietf-core-echo-request-tag-02

- **Status: pretty much done**
  - but waiting in the OSCORE cluster (interop next)

- **Where are the reviews?**

- **Should there be common practice to do the same via forms?**

6tisch-minimal stateless proxy support

- **Probably Out of time for today, but remaining issue:**
  - Extending the Token beyond 8 bytes (extending base header)
  - Adding a "token extension" option (normal option registration)
- **Even the option would need to be Critical/Unsafe**
  - So the deployment issues are fundamentally the same
  - Neither is a problem for 6tisch
- **Extending the token is the "clean" option**
  - Little knowledge about interoperability issues
  - Sends wrong signal about stability of RFC 7252
- **"Token Extension" option is tacky**
  - But stays in the frame

Planning

- **RD interop event?**

- **Next interim: 2018-08-29**
  - Carsten on vacation, Jaime on plane
  - Who wants to run this meeting?