OBJECT SECURITY FOR COAP

JOHN MATTSSON, ERICSSON
GÖRAN SELANDER, ERICSSON
LUDWIG SEITZ, SICS

IETF91 HONOLULU

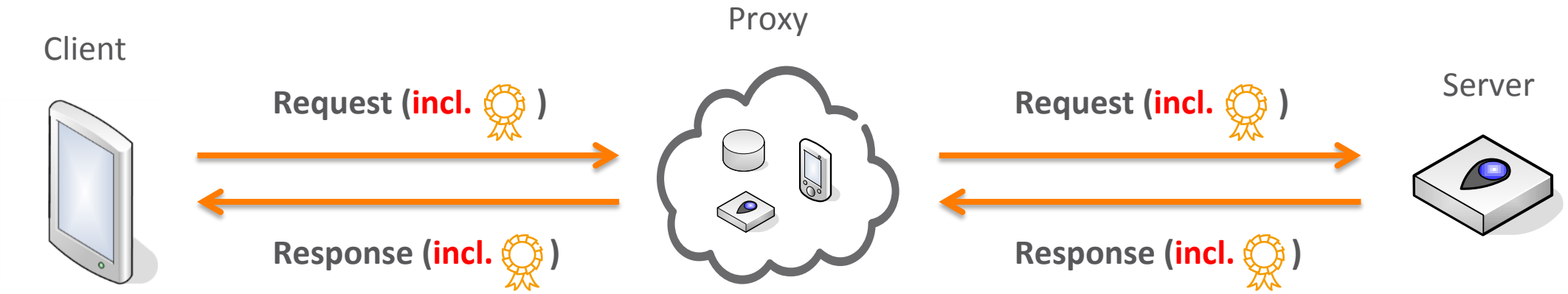
OUTLINE

- Setting described in draft-ace-seitz-usecases
- Tentative requirements in draft-ace-seitz-problem-description, Section 4

- Main objectives:
  - Client-Server end-to-end security in the presence of intermediary nodes (e.g. forward/caching proxies)
  - More lightweight than DTLS when handshake may be redundant
    - E.g. when there is a TTP/ Authorization Server supporting Client and/or Resource Server with key establishment

- Proposal: Secure individual CoAP messages
- Work in progress: Focus on integrity protection in this version

BASIC IDEA: SIGNATURE AS A COAP OPTION

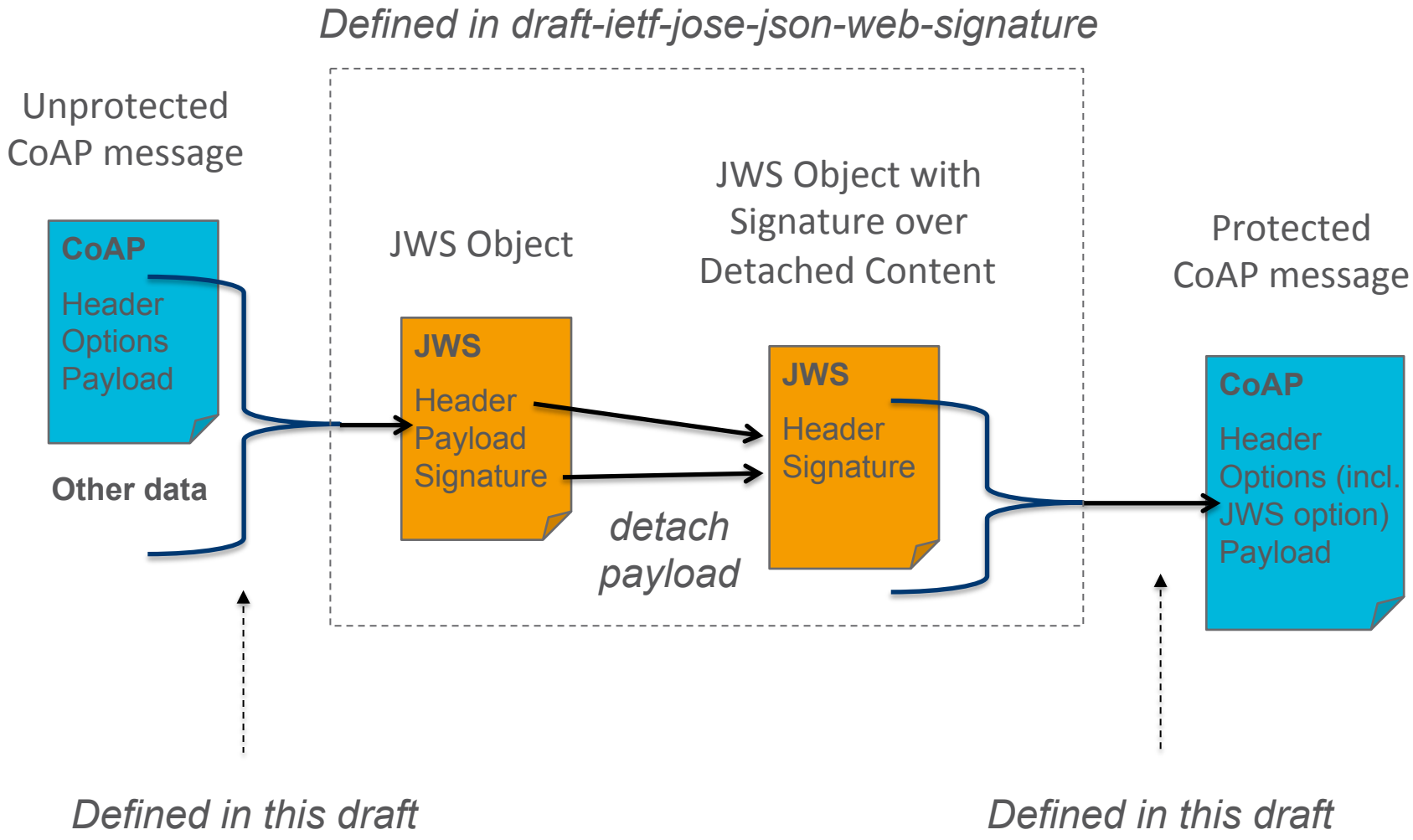


The draft proposes a new CoAP Option called “JWS”, which is a JWS object containing a signature or MAC over the CoAP payload, selected CoAP header fields and options.

Acknowledgement: Klaus Hartke is looking independently at the same problem and a similar solution: establishing end-to-end security across proxies by adding a CoAP option with signature. We encourage other submissions or comments so we can come to a good solution.

HIGH-LEVEL EXPLANATION

- CoAP JWS option:
  JWS Object with Signature over Detached Content
- Other data:
  Used in response to verify freshness



SIGNED PART OF COAP MESSAGE

- Some CoAP header fields or options should be allowed to change between client and server, hence are not integrity protected. The JWS Payload contains what must be integrity protected.

- The JWS Payload is type-value-length encoded and consists of:
  - CoAP header field Code;
  - CoAP options present which are marked as ”signed” (Appendix A)
  - CoAP payload (if any).

- The JWS Payload of a JWS option in a response also contains “other data”
  - See upcoming slide

- JWS signature and verification is performed as described in the JWS draft

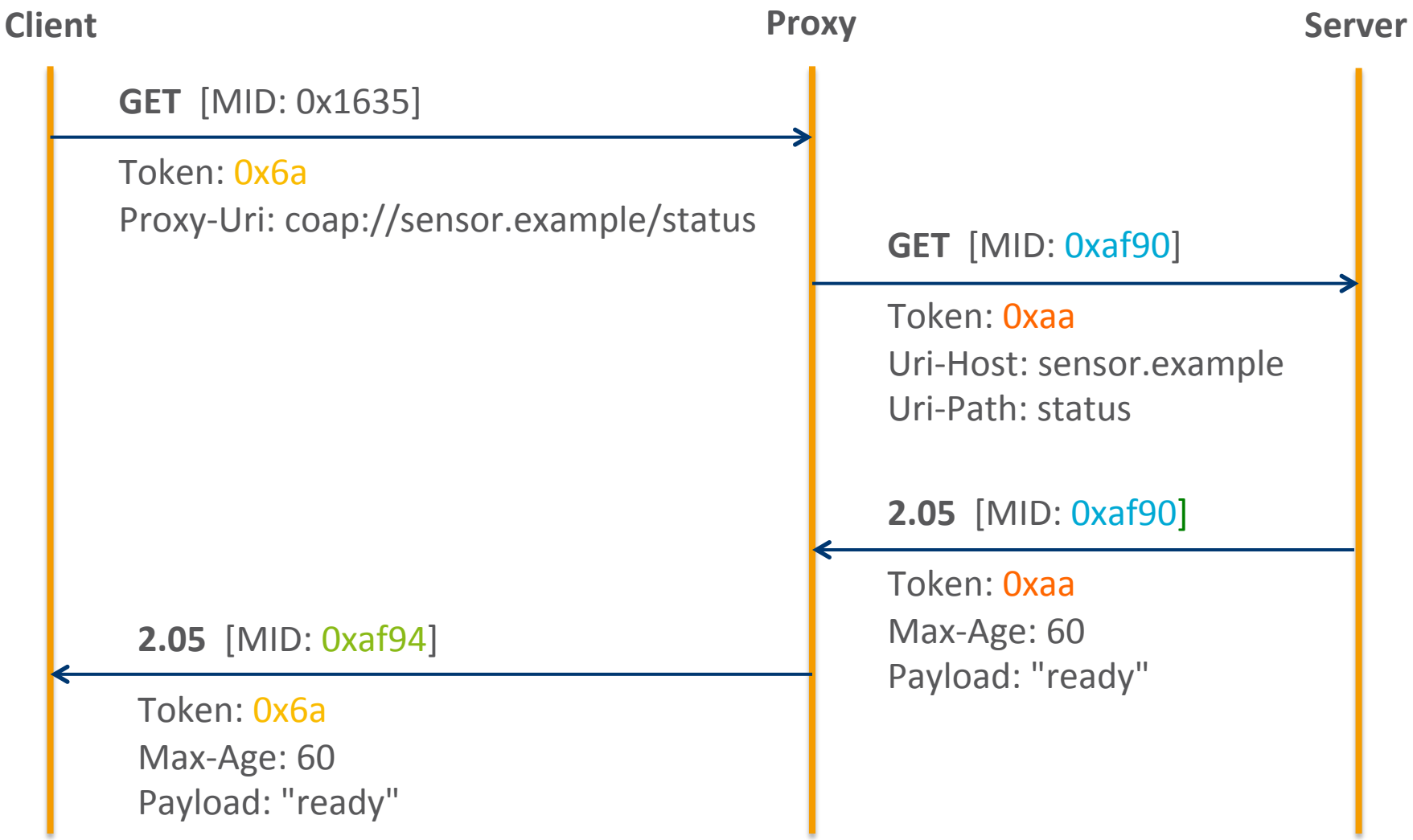
REPLAY PROTECTION 1(3)

- draft-ietf-jose-json-web-signature-36, Section 10.10 “Replay Protection”:
  - *“While not directly in scope for this specification, note that applications using JWS (or JWE) objects can thwart replay attacks by including a unique message identifier as integrity protected content in the JWS (or JWE) message and having the recipient verify that the message has not been previously received or acted upon.”*

- CoAP Message ID and CoAP Token are not persistent end-to-end so we need some other “message identifier”
  - Let’s call it “Transaction ID” to avoid confusion with CoAP Message ID
  - Term not used in 00-version of draft

REPLAY PROTECTION 2(3)

- CoAP Message ID and Token may change
- Thus are not suitable Transaction ID for replay protection



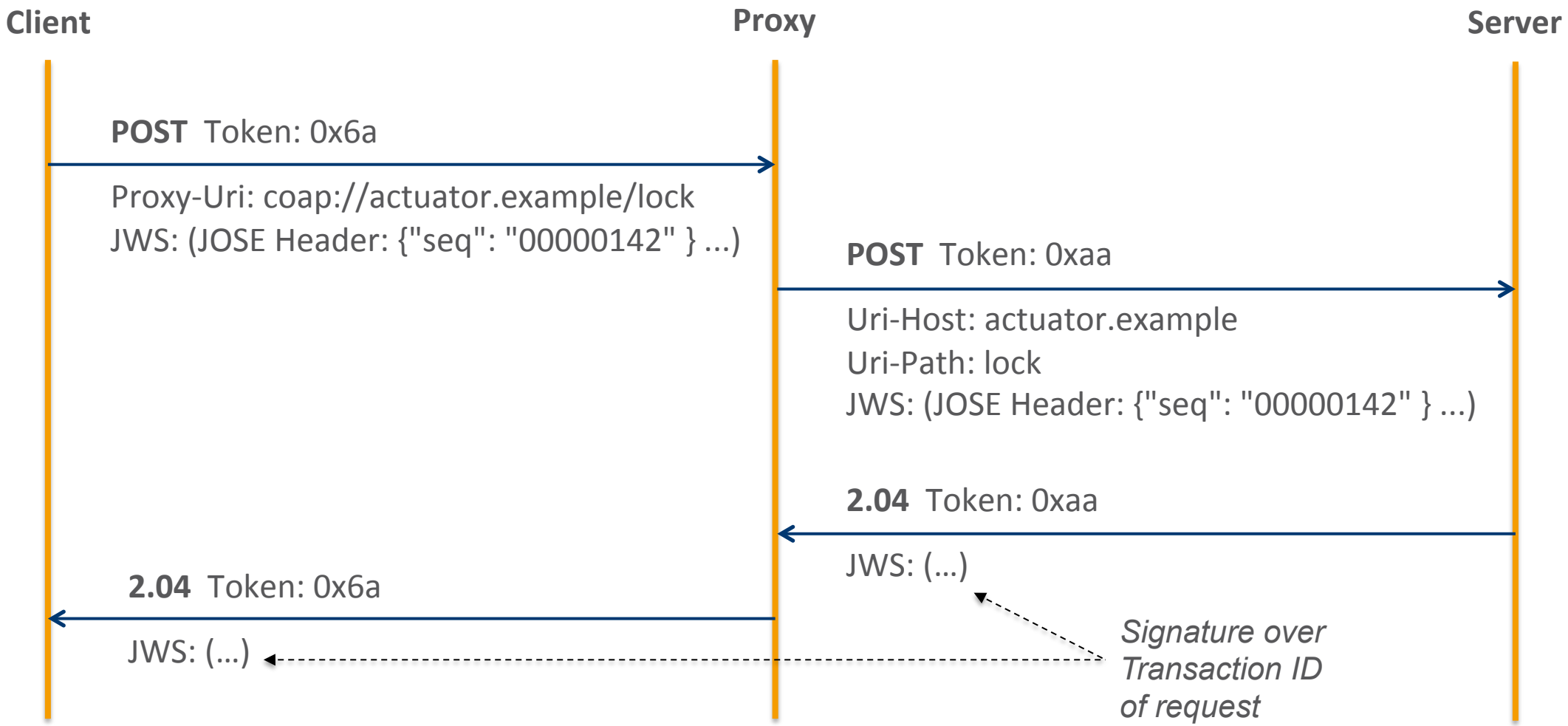
REPLAY PROTECTION 3(3)

- Proposal: Use key identifier and sequence number in JOSE Header as unique Transaction ID (TID)
  - Allows replay protection with limited storage in constrained device
  - Constrained device may not be able to support accurate time or generate random nonces

- Key identifiers already defined in JOSE: "kid", "x5t", "x5t#256"
- Define a new JOSE Header Parameter "seq" (Sequence Number)
  - 32 bits, start from 0, when wraps key must be changed.

- The TID can also be used in a challenge-response protocol for the client to verify freshness of the response
  - TID of the request included in the JWS Payload associated to the response
  - This is the previously mentioned “other data”

EXAMPLE: NEW JOSE HEADER PARAMETER "SEQ"



SUMMARY

We propose: a CoAP option called “JWS” containing essentially a signature over selected parts of the CoAP message

- This option provides end-to-end integrity protection and replay protection through proxies
- This is particularly favorable in situations where an initial security handshake between client and server is not necessary, such as in the ACE multiparty setting

Ongoing work: caching and observe (Appendix B)

Future work: encryption

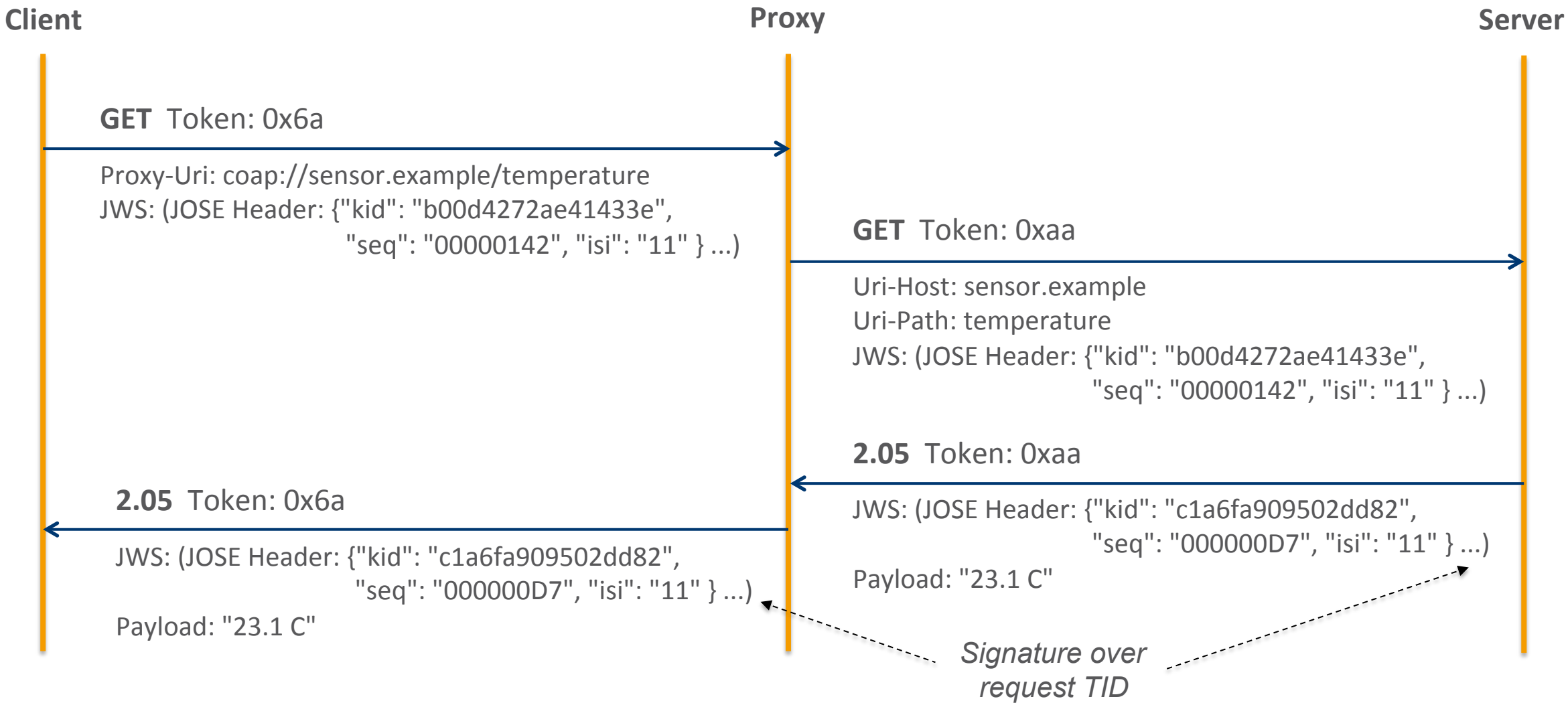
ADDITIONAL SLIDES

ONGOING WORK: CACHING AND OBSERVE

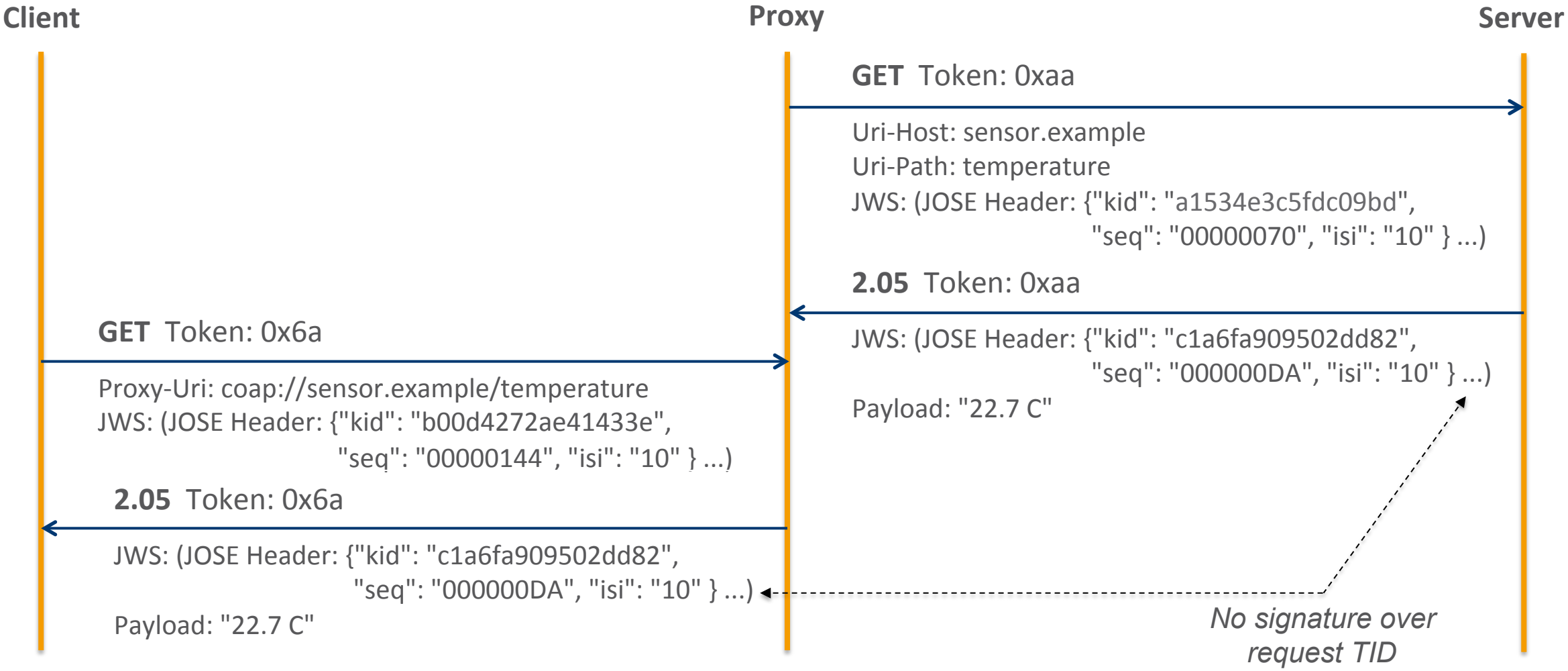
- Current proposal provides challenge-response based freshness for requesting client.
- In order to serve multiple clients cached responses and to handle multiple responses to one request, one needs to do the following change:
- Need to allow Transaction ID (TID) in response message

- Proposal: Define new JOSE Header Parameter: "isi" (Integrity Scope Indication):
  - "01": TID from request message (i.e. "other data") included in the JWS Payload of the response
  - "10": TID included in the JOSE Header of the response
  - "11": Both the previous

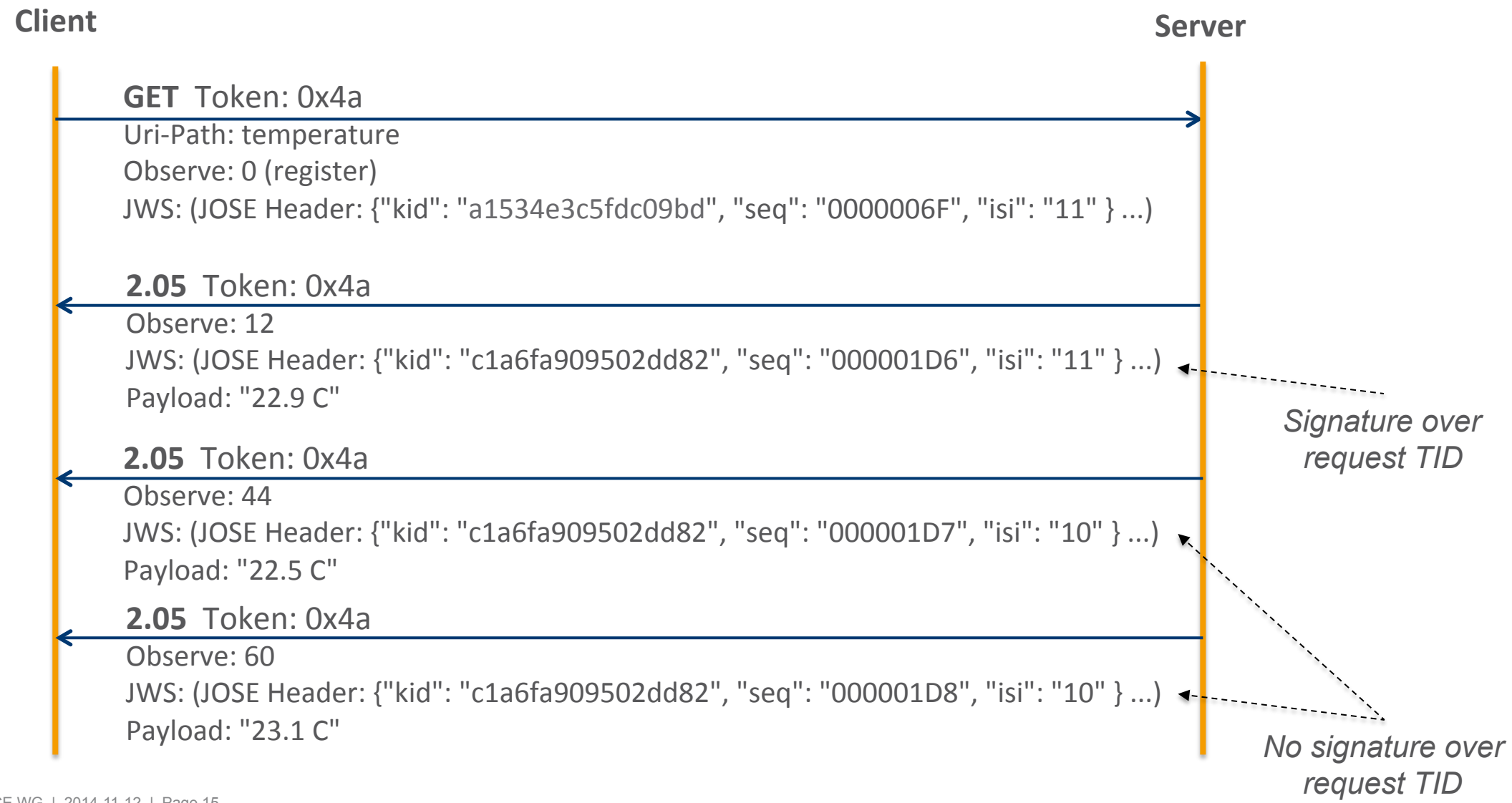
ONGOING WORK: CACHING 1(2)



ONGOING WORK: CACHING 2(2)



ONGOING WORK: OBSERVE



EXAMPLE: ACCESS TOKEN PROVISIONING PRIOR TO RESOURCE ACCESS

- Access_Token object secured on top of CoAP (end-to-end between AS and RS)
- In the resource access, DLTS would secure the payload hop-by-hop between Client and RS