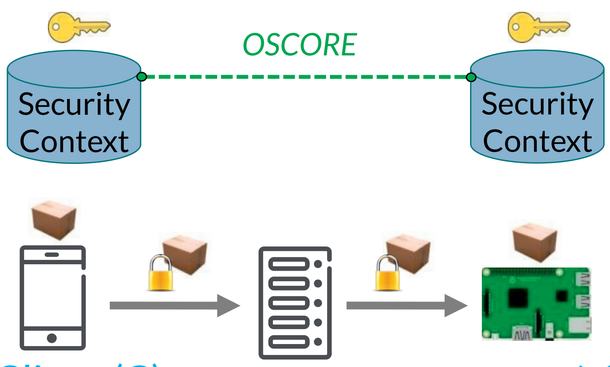
Using the OSCORE Security Protocol at Proxies and for CoAP Secure Tunneling



CoAP (RFC 7252) is a lightweight web-transfer protocol for the IoT. It is based on the client-server model and the REST paradigm, and is extended by *Options* included in the CoAP messages. It natively supports proxies.

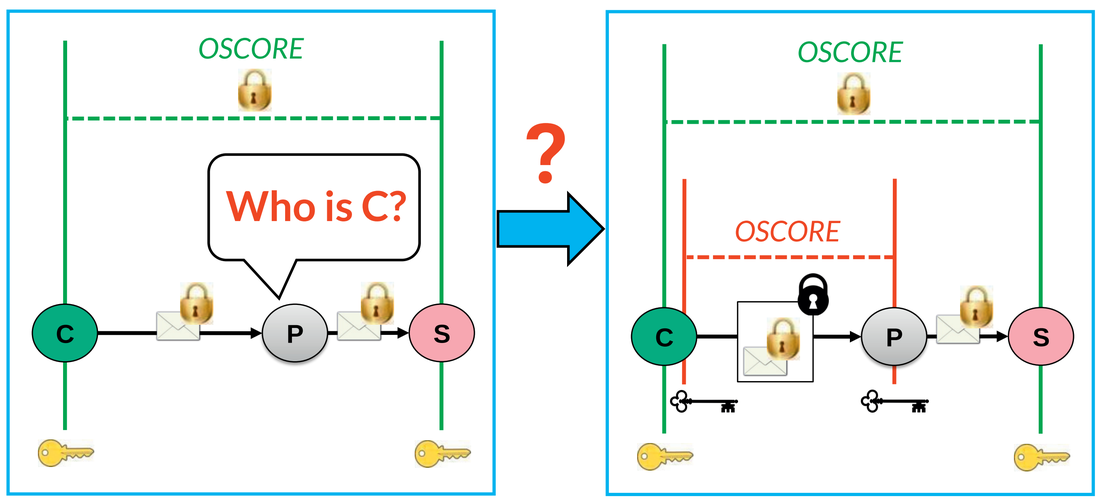
The lightweight security protocol OSCORE (RFC 8613) protects CoAP messages end-to-end at the application layer, through a proxy P.

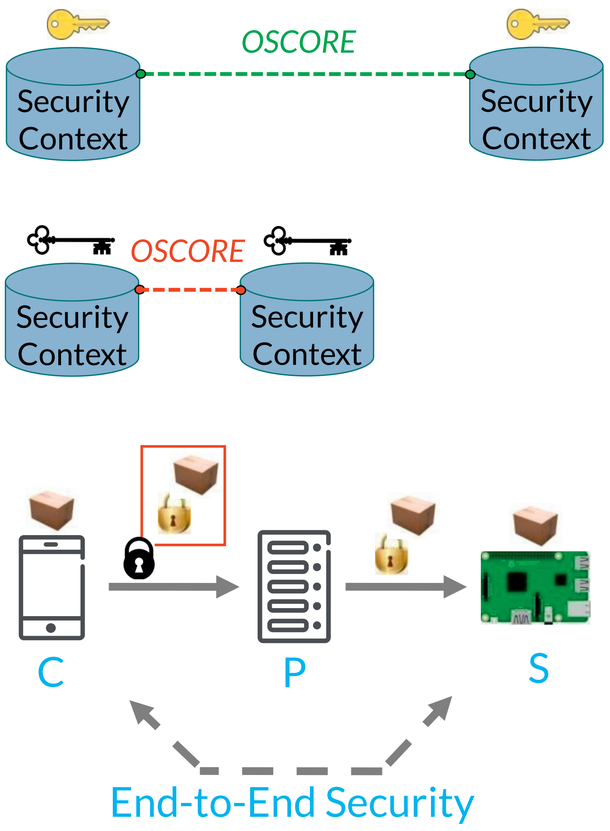
OSCORE was intended to be used only between two origin application endpoints (i.e., C and S), but not to be used at proxies and by proxies.

The proxy P might have to identify C, before forwarding a message to S. Since C and S use OSCORE, it would be convenient and efficient that also C and P use OSCORE.

Q: Can OSCORE be used at P?
A: No, it is not defined.

Q: But if it was possible, would it be fine?
A: No, the message from C would be protected two times (between C-S and between C-P). This is forbidden!



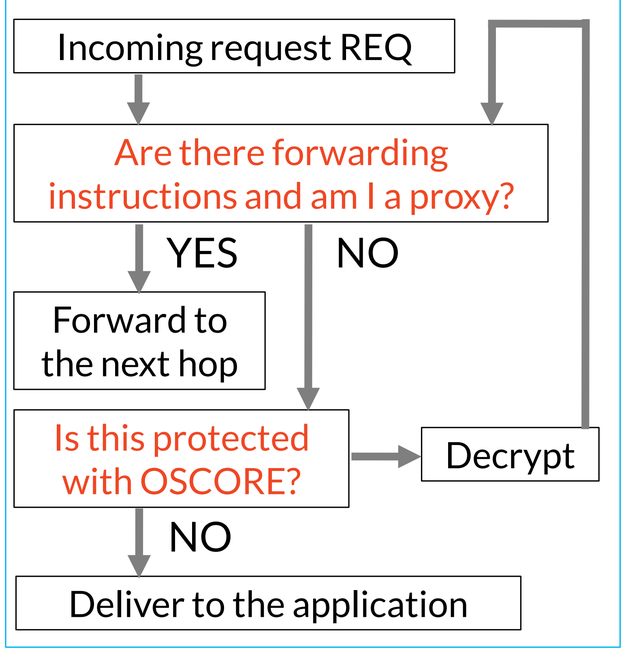


Features and benefits

- Any hop in a transport chain can use OSCORE, including proxies
- No max number of OSCORE nested protections (layers) for the same CoAP message
- When applying an OSCORE layer, as much information as possible is encrypted
- It works as-is also for Group OSCORE (OSCORE for CoAP group communication)
- Backward compatible
- Conducive to code reuse

Processing of incoming requests (simplified)

Same state machine at each hop in the chain



Selected use cases

- Proxies for group communication: P identifies C before forwarding a request over IP multicast
- OMA LwM2M: LwM2M Clients use the LwM2M Server as a proxy, to reach an external Application Server
- Proxy as first barrier between CoAP clients and an HTTP server (certificate enrollment with EST)

Ongoing standardization work in the CoRE Working Group of the IETF:
M. Tiloca and R. Höglund, “OSCORE-capable Proxies” (work in progress)
https://datatracker.ietf.org/doc/draft-ietf-core-oscore-capable-proxies/

This work has been partially funded by: the Sweden's Innovation Agency VINNOVA through the Celtic-Next projects CRITISEC and CYPRESS; and the H2020 projects SIFIS-Home (Grant agreement 952652).

RISE Research Institutes of Sweden
www.ri.se / info@ri.se

CONTACT
Marco Tiloca - marco.tiloca@ri.se
Rikard Höglund - rikard.hoglund@ri.se