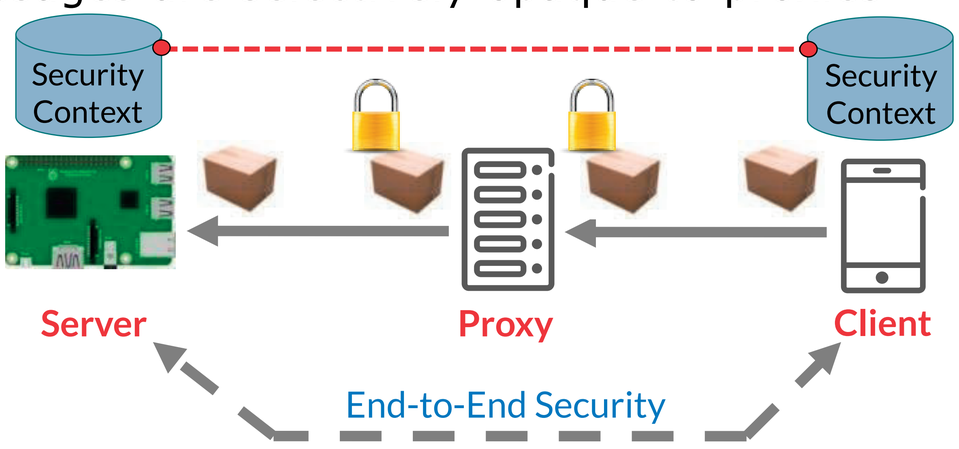
TinyTor: Enabling Onion Routing for the IoT

OSCORE Protocol

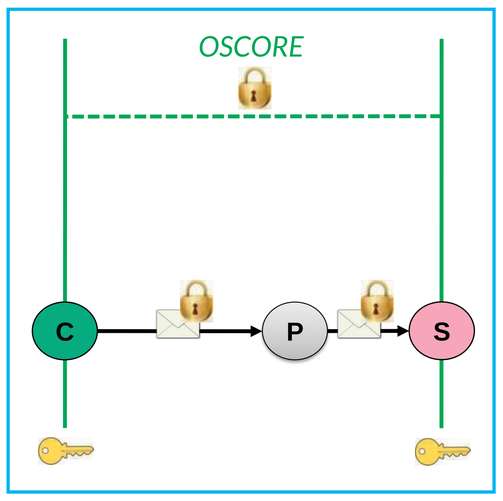
Constrained Application Protocol (CoAP)
- Web-transfer protocol for the IoT
- Lightweight, typically running over UDP
- Support for intermediary proxies

OSCORE Protocol
- End-to-end communication security for CoAP
- Between data originator and data consumer
- Works wherever CoAP works
- Supports message relaying through proxies
- Messages are selectively opaque to proxies

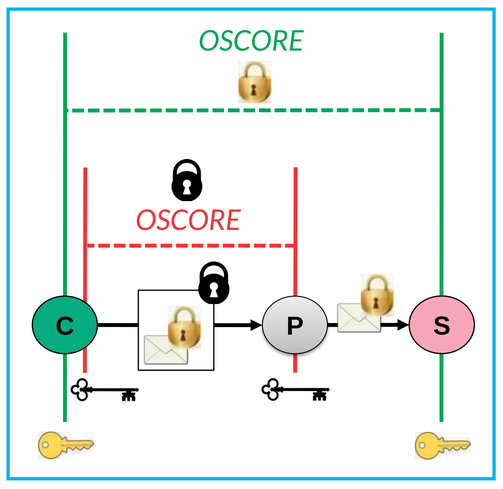


OSCORE-Capable Proxies and Nested OSCORE

- Original OSCORE can't be used <u>at</u> proxies, but only end-to-end between client and server
- In many use cases, the proxy would benefit from using OSCORE to identify message senders



- New: use OSCORE <u>at</u> proxies (e.g., between client and proxy)
- New: multiple OSCORE-protection of the same CoAP message (e.g., between client and server, and between client and proxy)

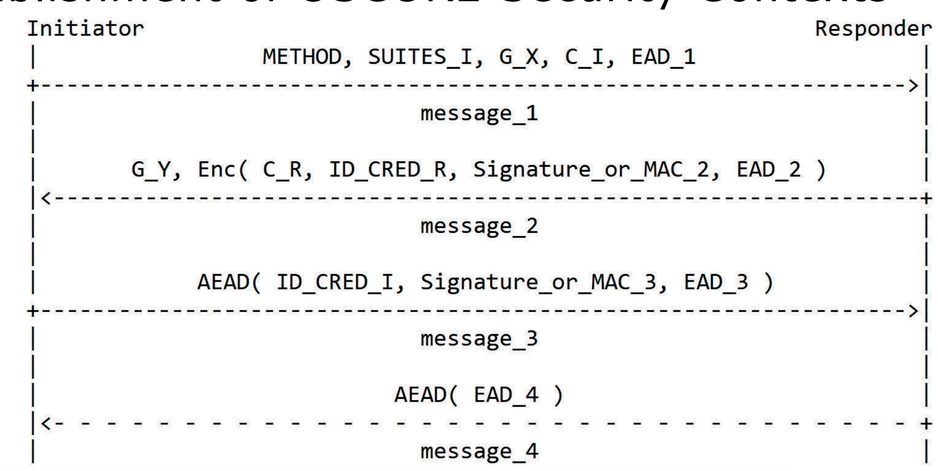


EDHOC Key Exchange Protocol

EDHOC: Ephemeral Diffie-Hellman Over COSE
- Based on SIGMA-I MAC-Then-Sign
- Lightweight, with mutual peer authentication
- Core protocol is a 3 message exchange

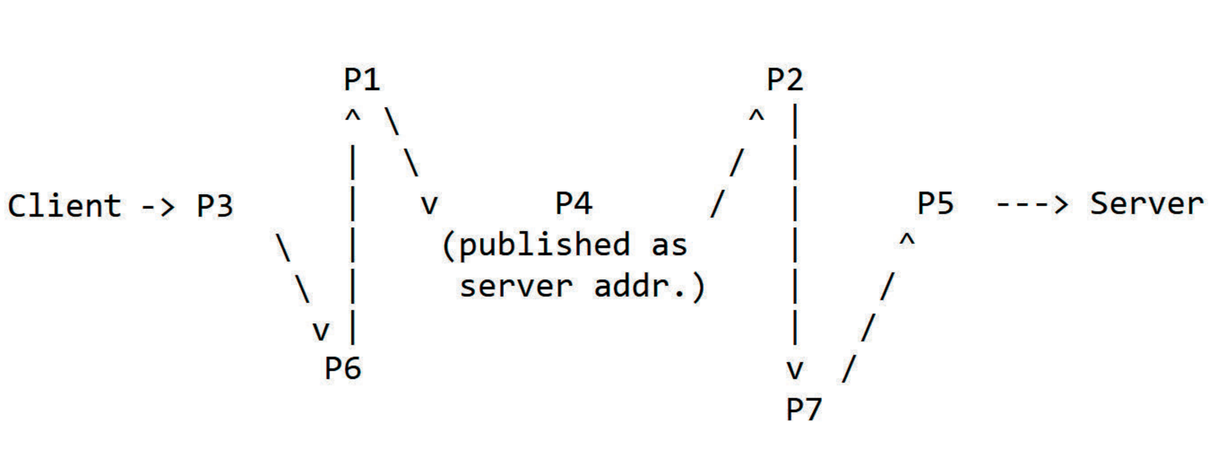
Authentication based on MACs or signatures
- Credentials exchanged by value or reference

Establishment of a secret key
- Based on Diffie-Hellman (forward secrecy)
- Establishment of OSCORE Security Contexts



TinyTor Functionality

- Roots-of-trust distribute signed shards of the list of proxies; shards can also be retrieved via proxies
- Shards contains information about proxies including credentials, location, and optionally a public IP
- The server/client chooses a set of 3 proxies to build their individual chains
- The server/client uses EDHOC to establish authenticated OSCORE Security Contexts with the proxies (via the current proxies in the chain)
- The client targets the proxy at the end of the server's chain and protects its request with multiple layers of OSCORE
- TLS can be used between the proxies to harden the system against traffic analysis



VINNOVA
European Commission

This work has been partially funded by: the Sweden's Innovation Agency VINNOVA through the Celtic-Next project CYPRESS; and the H2020 project SIFIS-Home (Grant agreement 952652).
Solutions presented in this slide are undergoing standardization in the IETF.

IETF

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

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

RI. SE