Profiling EDHOC for CoAP and OSCORE
Combining EDHOC and OSCORE
draft-ietf-core-oscore-edhoc-02

Francesca Palombini, Ericsson
Marco Tiloca, RISE
Rikard Höglund, RISE
Stefan Hristozov, Fraunhofer AISEC
Göran Selander, Ericsson

CoRE WG interim meeting, October 27th, 2021
Recap

› **EDHOC**: lightweight authenticated key exchange developed in the LAKE WG
  – Main use case: keying OSCORE for establishing a Security Context
  – Normal workflow: two round-trips, before starting to use OSCORE

› **Original contribution of this draft**
  – Optimized combination of EDHOC (run over CoAP) with OSCORE
  – EDHOC message_3 combined with the first OSCORE-protected request
    › A single EDHOC + OSCORE request, transporting both
  – Achieved minimum number of round trips to run EDHOC and use OSCORE
Update since IETF 111

› **Agreed at IETF 111 to broaden the document scope**
  – Define CoRE-specific optimizations/features that are too specific for LAKE
  – New scope: profile the use of EDHOC for CoAP and OSCORE

› **What is covered now**
  – EDHOC + OSCORE request
  – Efficient conversion from OSCORE identifiers to EDHOC identifiers
  – Extension and consistency of EDHOC applicability statement
  – Web linking

› **Broader scope reflected in new title/abstract/introduction/TOC**
**EDHOC + OSCORE request**

› Now aligned to EDHOC v-12
  – “true” not part of EDHOC message_1
  – C_R not part of EDHOC message_3
  – Consistent (non-)use of Content-Format
  – Updated client and server processing
  – …

› “EDHOC” CoAP Option number 21
  – Requested for early IANA allocation in the CoAP Option Numbers registry
  – Not confirmed yet
OSCORE ID ➔ EDHOC ID

› Conversion method from OSCORE Sender/Recipient IDs to EDHOC IDs
   – Was an appendix; now revised and part of the document body

› Two "equivalent" EDHOC IDs exist for each OSCORE ID (CBOR int or bstr)
   – This method deterministically picks either the int or the bstr EDHOC identifier
     › Required for the EDHOC+OSCORE request, as including an OSCORE Sender ID
     › Performance advantage: the selected EDHOC identifier is the smallest of the two

› MUST use if:
   – The server supports the EDHOC + OSCORE request;
   AND/OR
   – Explicitly indicated to use, e.g., in the applicability statement

If used ➔ Additional EDHOC message processing to ensure that the peers comply
EDHOC applicability statement

› It defines how client and server can use EDHOC
  – Here extended with more information elements and consistency rules

› If the server supports the EDHOC + OSCORE request …
  – SHOULD indicate the support
  – SHOULD indicate the new ID conversion method (and no other method is admitted)
  – MUST NOT indicate that EDHOC message_4 shall be sent

› Otherwise …
  – MAY indicate the ID conversion method to use by both peers
  – If none is indicated, each peer independently uses any preferred method
Web linking

- The EDHOC draft defines the resource type rt="core.edhoc"
  - It can be used to discover EDHOC resources at the server

- This draft defines target attributes for a link with rt=core.edhoc
  - Different target attributes for different information elements of the applicability statement
  - Authentication methods, ciphersuites, support for EDHOC + OSCORE request, …

- Discovery of applicability statements
  - From the server or from a Resource Directory
  - Spare negotiation or Error Messages when running EDHOC
  - Besides rt="core.edhoc" , any attribute that MUST/SHOULD be in the link?

REQ: GET /.well-known/core

RES: 2.05 Content

  </sensors/temp>;osc,
  </sensors/light>;if="sensor",
  </.well-known/edhoc>;rt="core.edhoc";csuite=0;csuite=2;
  method=0;cred_t="c509";cred_t="ccs";idcred_t="4";comb_reg
Open points

› Need an IANA registry for EDHOC → OSCORE ID conversion methods?
  – First entry would be the method defined in this document
  – Never specified in EDHOC/OSCORE messages
  – Specified in applicability statement and link-format documents
  – Opinions?

› Error handling at the server (assuming the EDHOC option is understood)
  – A request has EDHOC option but no OSCORE option
  – Proposal: return 4.00 (Bad Request) – Ok with this?

  – After OSCORE decryption, the request has the EDHOC and OSCORE options
  – Proposal: admit it, as possible with nested OSCORE – Ok with this?
Summary and next step

› Profile of EDHOC for CoAP and OSCORE
  – EDHOC + OSCORE request, optimizations, CoRE-specific features, …

› We have running code (again) built for Eclipse Californium (Java)
  – EDHOC + OSCORE request, aligned to EDHOC v -12
  – https://github.com/rikard-sics/californium/tree/edhoc

› Next steps
  – Use of “URI compression" option from Christian once it is available
    › https://datatracker.ietf.org/meeting/interim-2021-core-05/materials/slides-interim-2021-core-05-sessa-core-option-for-well-known-resources-00.pdf
  – Additional error handling
  – More on web-linking
  – Considerations on triggering block-wise; security considerations

› Comments are reviews are welcome!
Thank you!

Comments/questions?

https://github.com/core-wg/oscore-edhoc/
EDHOC + OSCORE request