EDHOC Evaluation on Constrained Devices

interim-2021-lake-02

Stefan Hristozov, April 22, 2021

Fraunhofer
AISEC

Based on: **The Cost of OSCORE and EDHOC for Constrained Devices** – S. Hristozov, M. Huber, L. Xu, J. Fietz, M. Liess and G. Sigl – 11th ACM Conference on Data and Application Security and Privacy (CODASPY 2021) https://arxiv.org/pdf/2103.13832.pdf.

EDHOC Implementations and Evaluation Details

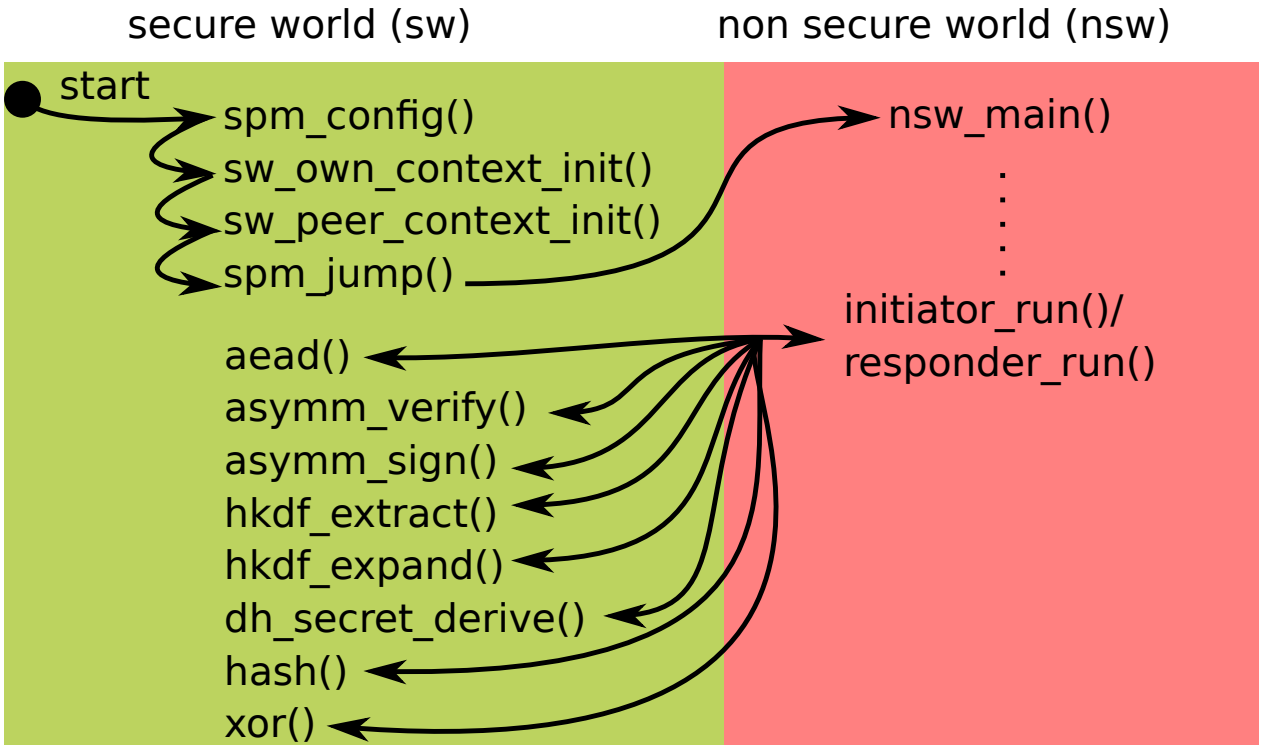
Two implementations in C:

- Regular microcontrollers
- Microcontrollers with a Trusted Execution Environment (TEE)

EDHOC Library for Microcontrollers with TEE

Sensitive assets:

- EDHOC keys
- Algorithms (Signature, DH, AEAD, HKDF)



Fraunhofer AISEC

Evaluation Details

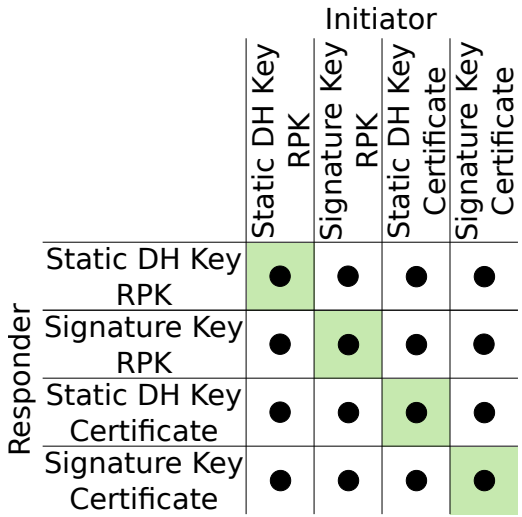
- Cipher suite 0: AES-CCM-64-64-128, HKDF-256, X25519, Ed25519
- Native CBOR certificates[1]
- Crypto implementation: tinycrypt[2] and c25519[3]
- Four different architectures: Cortex-M0@16 MHz, Xtensa@160 MHz Cortex-M4F@64 MHz, Cortex-M33@64 MHz
- TEE test platform: nRF9160 / Cortex M33 with TrustZone-M / 64 MHz

[1] https://datatracker.ietf.org/doc/draft-raza-ace-cbor-certificates/04/

[2] https://github.com/intel/tinycrypt

[3] https://www.dlbeer.co.nz/oss/c25519.html

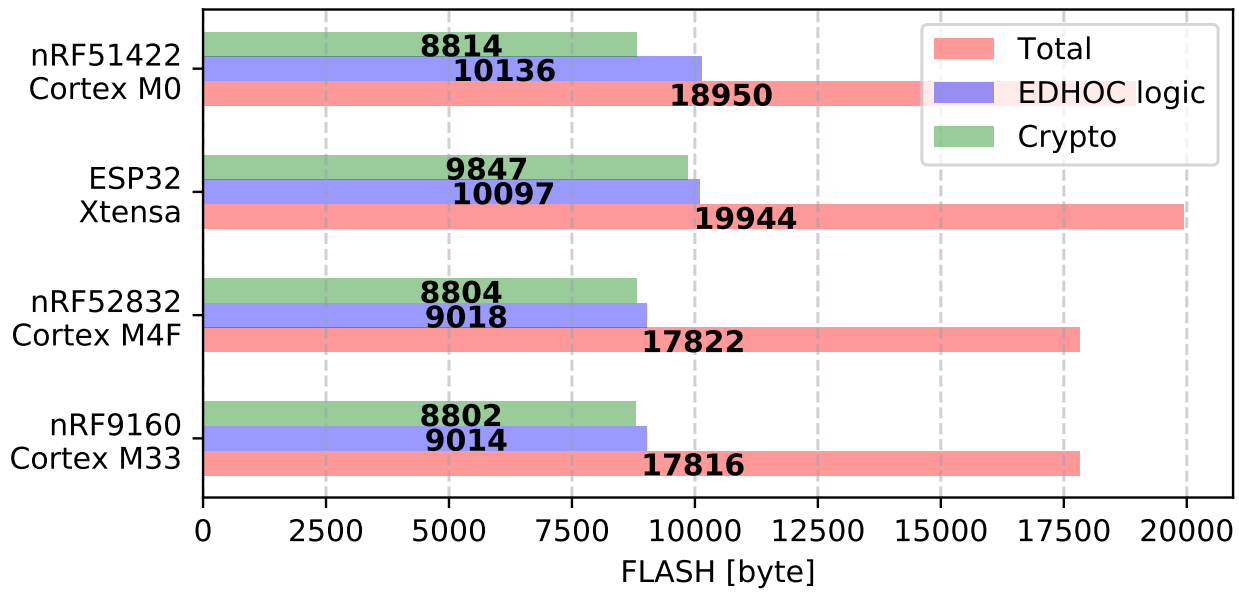
Message Sizes



Authentication mode	Msg 1	Msg 2	Msg 3
Static DH keys / RPK	37	46	20
Signature keys / RPK	37	117	91
Static DH keys / Certificate	37	186	160
Signature keys / Certificate	37	243	217

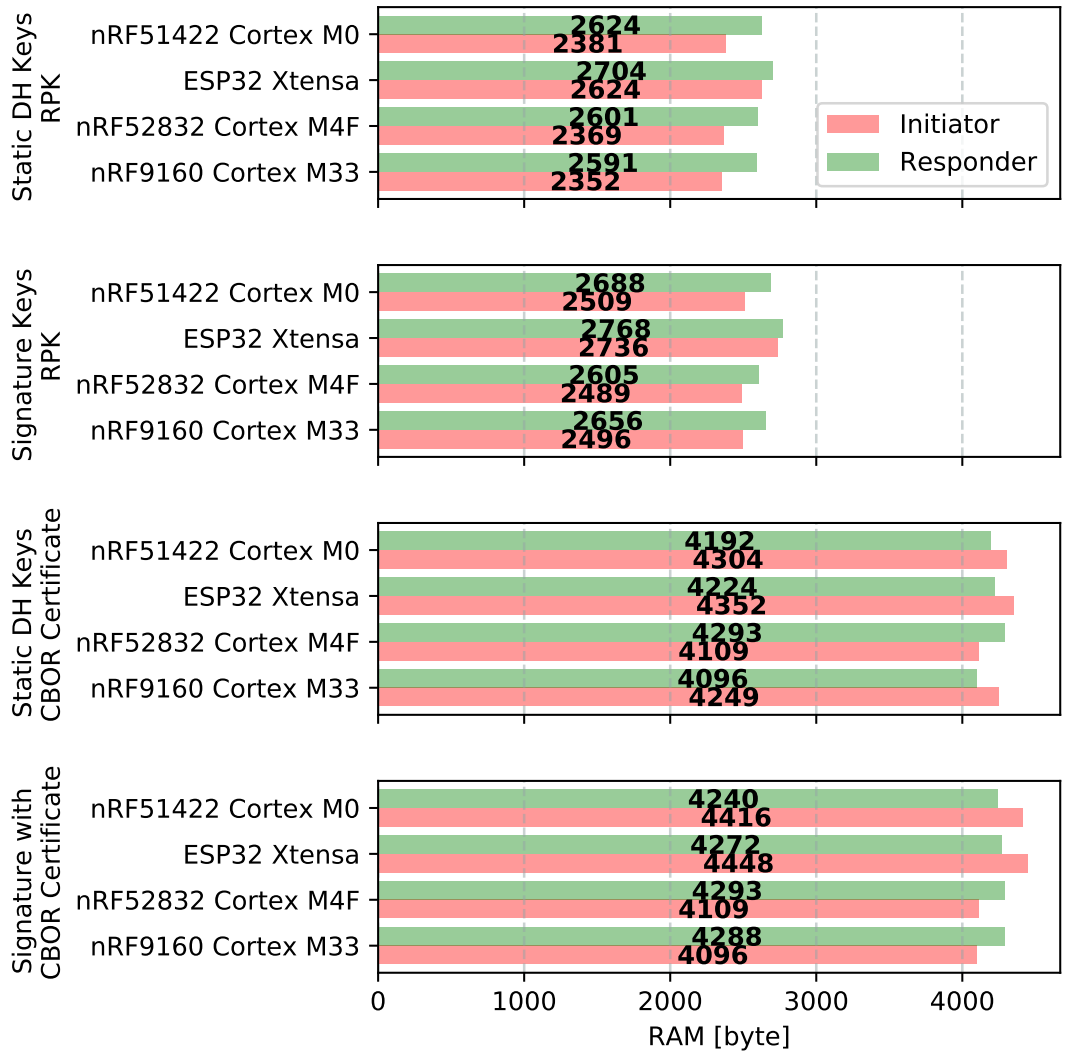
Fraunhofer AISEC

EDHOC without TEE – FLASH



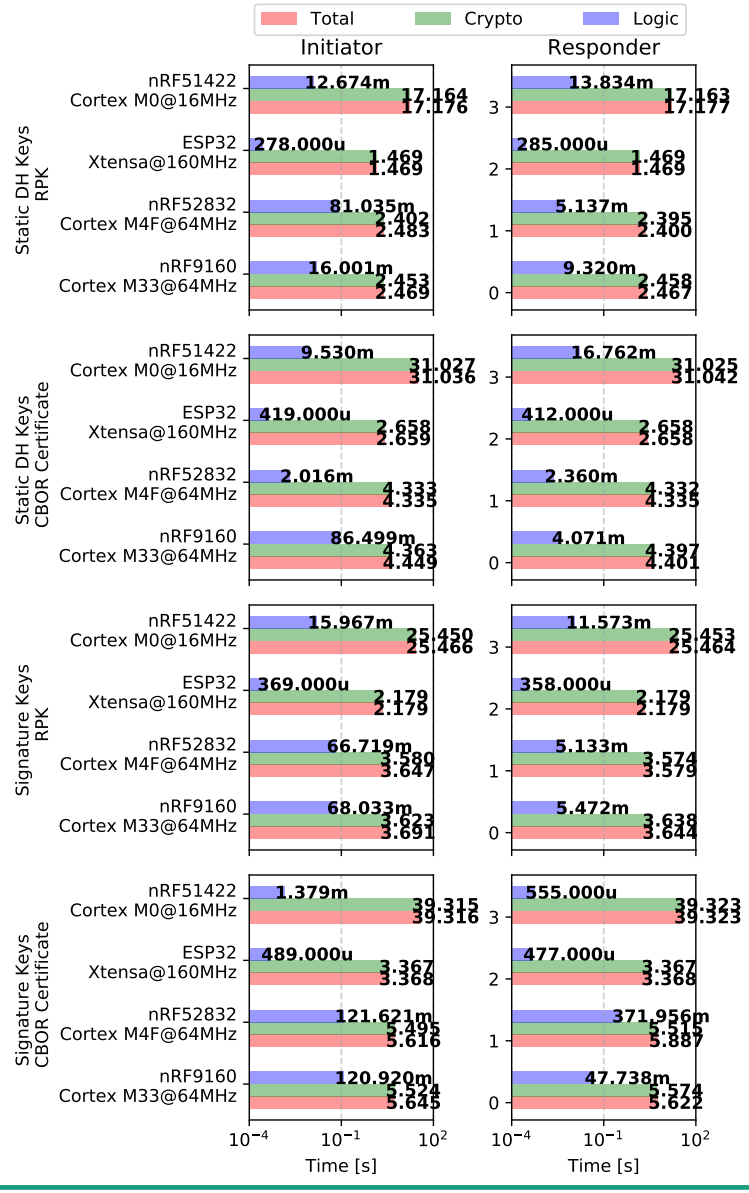
Fraunhofer AISEC

EDHOC without TEE – RAM



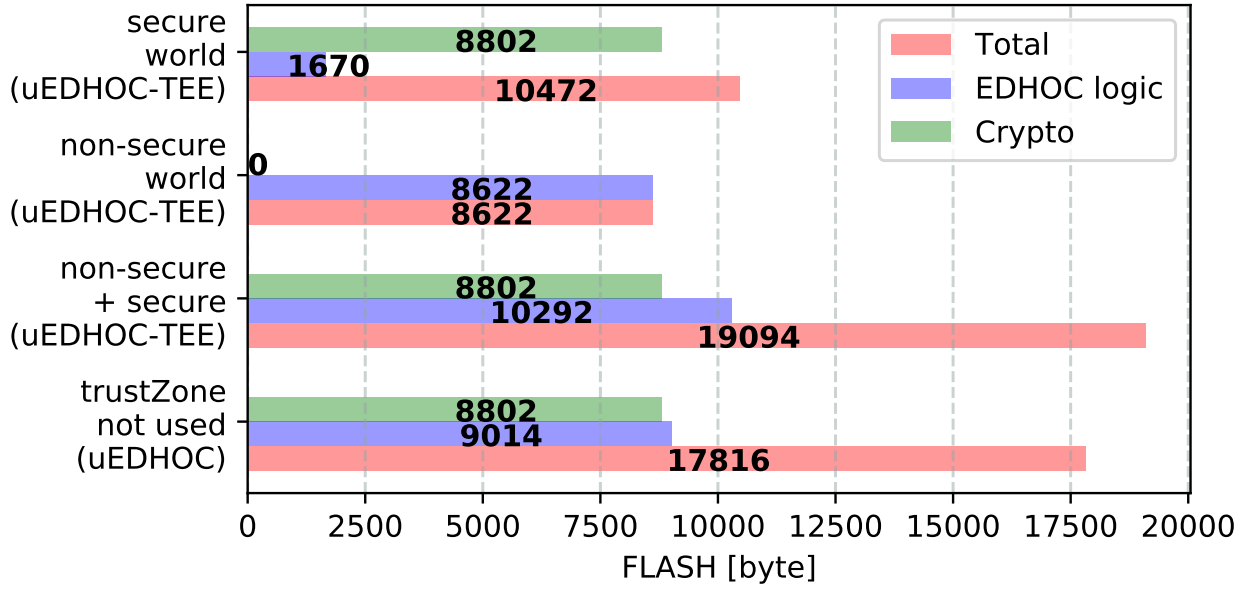
Fraunhofer AISEC

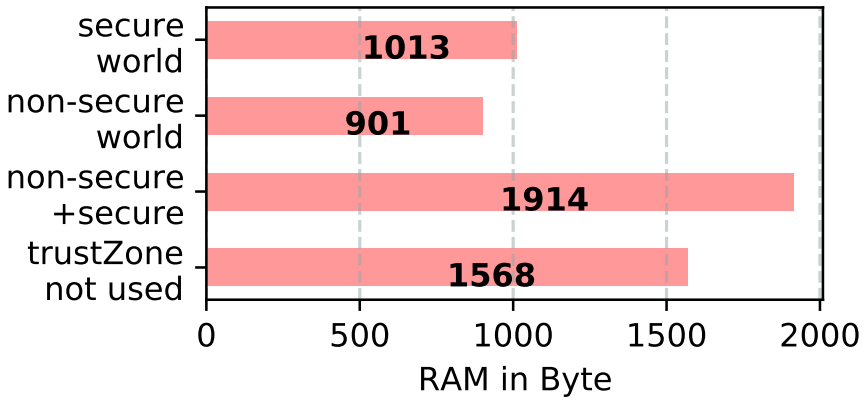
EDHOC without TEE – Computing Time

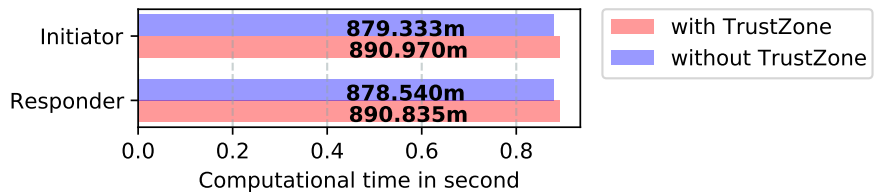


Fraunhofer AISEC

EDHOC with TEE – FLASH and RAM and Computing Time







Fraunhofer AISEC

Open Source Implementation

- EDHOC (and OSCORE) implementations available as open source[4]
- Dual permissive license MIT or Apache 2
- Integration in Zephyr OS (work in progress)
- Contribution highly appreciated

[4] https://github.com/Fraunhofer-AISEC/uoscore-uedhoc

Contact Information

Stefan Hristozov

Hardware Security Department

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Lichtenbergstr. 11
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de

Phone: +49 89 3229986-157
Fax: +49 89 3229986-222
E-Mail: stefan.hristozov@aisec.fraunhofer.de

Fraunhofer AISEC