Lightweight AKE for OSCORE: Requirements

IETF 105, LAKE BoF, July 22, 2019
Göran Selander et al.

Background

- LAKE is about specifying a lightweight authenticated key exchange protocol for OSCORE (RFC 8613)

- The requirements for the lightweight AKE are based on conditions for deploying OSCORE in constrained environments

- This is not a new subject in the IETF
  - On the agenda for ACE WG F2F meetings at IETF 96-99, 101-103
  - Extensively discussed in SecDispatch 2019, dedicated virtual interim March 5

- Most content in this presentation comes from draft-selander-lake-reqs-01 summarising the discussion in Secdispatch

Outline of this slide set

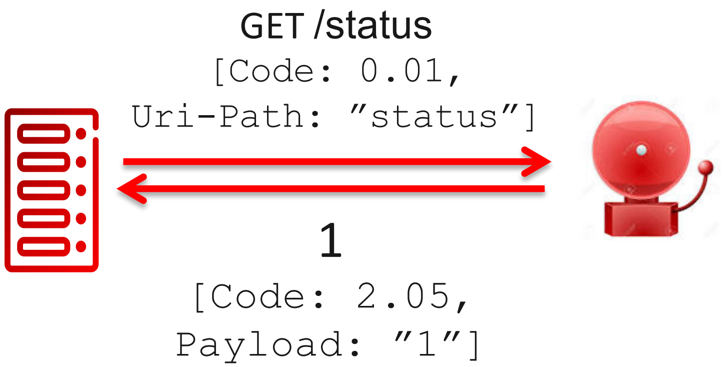
- Background (this slide)
- OSCORE background
- Requirements
  - Input and transport requriments
  - Authentication credentials
  - Crypto agility
  - Lightweight
  - Benchmarks
- Summary

OSCORE background

OSCORE (RFC 8613)

- Communication security protocol for CoAP/REST
- Supports CoAP proxies and change of transport protocol
  - Selective protection of CoAP header fields & options
- Designed for peer-to-peer and group communication
- Defined in terms of CoAP, CBOR and COSE
- Lightweight:
  - Low message overhead
  - Uses/reuses primitives for constrained environments

OSCORE is symmetric key based
→ A matching AKE is needed for forward secrecy and public-key based authentication

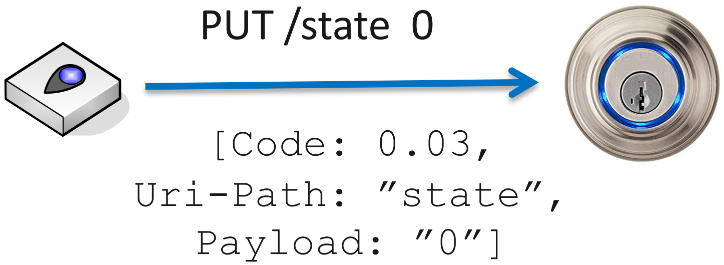


GET /status

```
[Code: 0.01,
Uri-Path: ”status”]
```

1

```
[Code: 2.05,
Payload: ”1”]
```



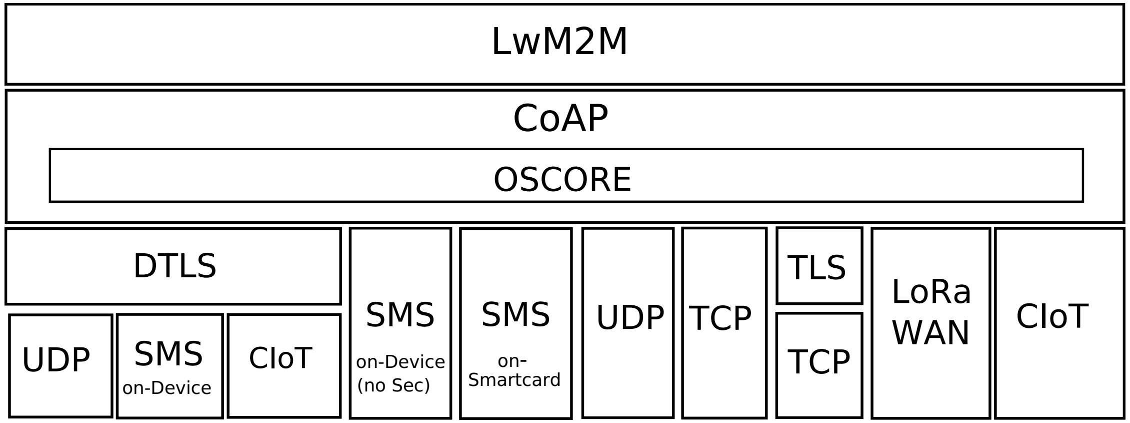
PUT /state 0

```
[Code: 0.03,
Uri-Path: ”state”,
Payload: ”0”]
```

OSCORE development and applications

- IETF WGs applying OSCORE
  - CoRE, ACE, 6TiSCH, LPWAN, …
- Other IoT fora
  - OMA SpecWorks
  - Open Connectivity Foundation
  - Fairhair Alliance

- OSCORE development/testing activities
  - IETF interop tests, incl. multicast
  - Eclipse: Californium/Leshan
  - 6TiSCH Minimal Security for OpenWSN
  - F-Interop
  - Wireshark
  - LwM2M over NB-IoT/CIoT
  - SCHC over LoRaWAN
  - On top of Zephyr, for Nitrogen
  - RIOT OS
  - libCoAP
  - …



LwM2M

CoAP

OSCORE

DTLS

UDP

SMS on-Device

CIoT

SMS on-Device (no Sec)

SMS on-Smartcard

UDP

TCP

TLS

TCP

LoRa WAN

CIoT

Figure: 4.-1 The Protocol Stack of the LwM2M Enabler

Figure from
OMA SpecWorks
LwM2M Transport Bindings
Version: 1.1

Requirements

OSCORE input and transport requirements

O1. At the end of the AKE the two parties shall agree on

- OSCORE Master Secret with PFS and good amount of randomness
- OSCORE Sender IDs of peer endpoint, arbitrarily short
- COSE algorithms to use with OSCORE

O2. The AKE shall support the same transport as OSCORE

Authentication credentials

A1. The AKE shall support authentication using

- pre-shared keys
- raw public keys
- public key certificates

A2. Mixed public key credentials ← *Discussed on the LAKE mailing list: Not in draft-selander-lake-reqs-01*

Crypto agility

C1. The AKE shall support negotiation of crypto algorithms

— used with OSCORE (COSE AEAD algorithm and HKDF, including HMAC)

— used in the AKE (AEAD algorithm, signature algorithm, DH algorithm, …)

Lightweight

L1. The AKE shall be 'lightweight' in terms of resource consumption as measured by

— bytes on the wire
— wall-clock time to complete
— power consumption
— amount of new code required on end systems which already have an OSCORE stack

General:

— Bytes on the wire impact time to complete and power consumption, see Benchmarks
— Time to complete implies **L2. as few round trips as possible** (1 RTT / 3 messages)
— Power consumption depends in particular on radio technology, see Benchmarks
— An indication of new code required is the degree of reuse of OSCORE building blocks (CoAP, CBOR, COSE encryption and signature constructs, algorithms, etc.)

Specific: See Benchmarks (NB-IoT, LoRaWAN, 6TiSCH) using message sizes specified in draft-ietf-lwig-security-protocol-comparison-03

Benchmark 1: NB-IoT energy consumption

Cellular licensed spectrum radio with low data rates supporting

- extreme coverage conditions
- device battery life of 10 years or more
- low device complexity and cost
- high system capacity of thousands of connected devices per square kilometer

Licensed spectrum allows high device transmit power, which in combination with low data rates causes **high per-byte energy consumption** for uplink transmissions

Benchmark: Energy consumption estimate based on model used in 3GPP (see interim slides)

Conclusion: Higher message overhead results in higher energy consumption

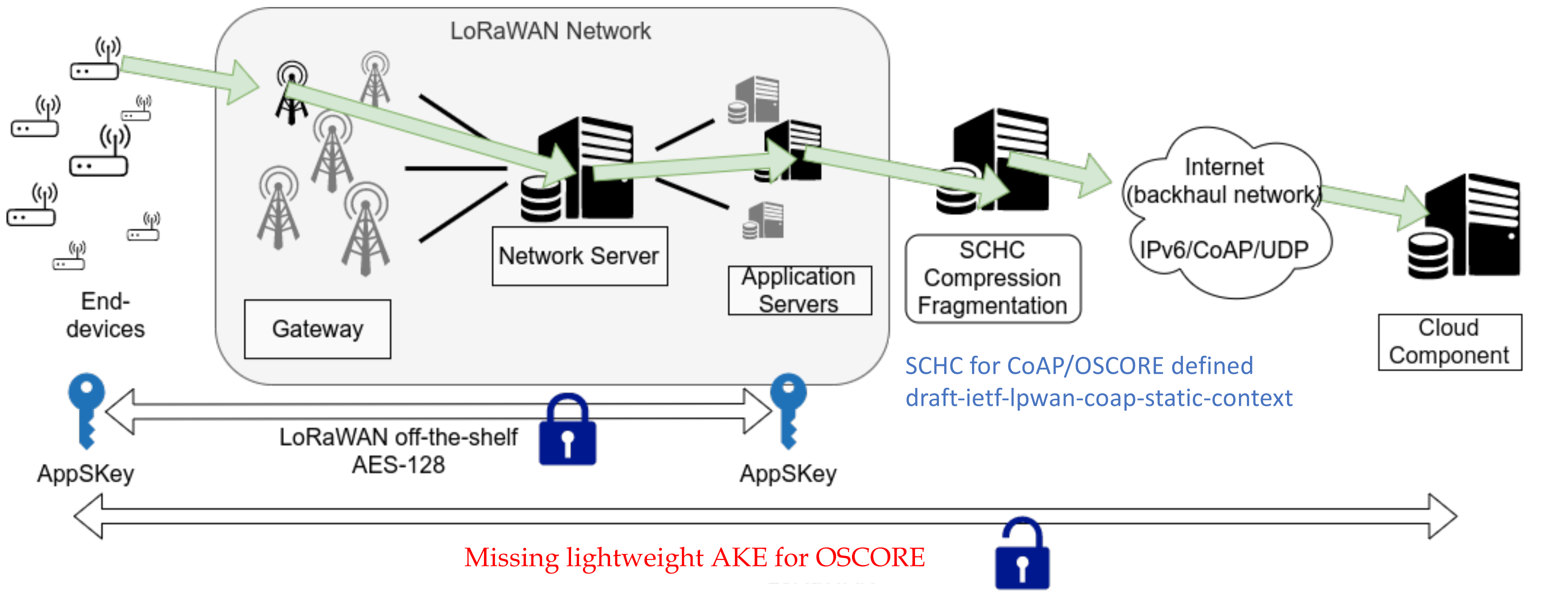
B1. The AKE shall have as few bytes as reasonably achievable

NOTE: This is not a strict engineering requirement but a clear indication that message sizes matter

Example
Low coverage
Energy in mJ

PSK ECHDE	EDHOC-12	DTLS 1.3
Flight1	475.7	2021.6
Flight2	11.8	48.6
Flight3	118.9	616.2
Total	**912**	**2992**

Benchmark 2: LoRaWAN duty cycle back-off times


LoRaWAN Network
End-devices
Gateway
Network Server
Application Servers
SCHC Compression Fragmentation
Internet (backhaul network)
IPv6/CoAP/UDP
Cloud Component
AppSKey
LoRaWAN off-the-shelf AES-128
AppSKey
Missing lightweight AKE for OSCORE

SCHC for CoAP/OSCORE defined draft-ietf-lpwan-coap-static-context

DataRate	*N*
0	51
1	51
2	51
3	115
4	222
5	222
6	222
7	222

N = packet size

Example (below)
Duty cycle back-off time in minutes

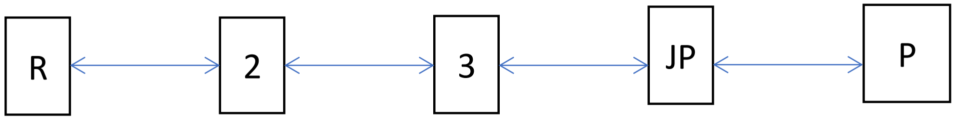
PSK ECHDE	EDHOC-12	DTLS 1.3
Flight1	4.3	13.8
Flight2	0	13.8
Flight3	0	4.6
Total	**4.3**	**32.3**

Unlicensed radio frequency bands

- Maximum payload size is limited for each LoRaWAN DataRate configuration
- **back-off time** period after transmission called **duty cycle**, typically 1% in Europe

Benchmark: Back-off time with packet size 51 bytes
Conclusion: High penalty in completion time for exceeding the packet size
B2. The AKE messages shall fit into as few packets as possible

Benchmark 3: Number of 6tisch message frames



- 6tisch network, 4 hops deep, in a network formation setting
- Calculation of available CoAP payload in a production network
- Based on OpenWSN dump as of March 2019

The time to join increases with number of frames required for the AKE protocol, and this is significant during network formation when many devices join at the same time

Benchmark: Number of frames needed for the AKE messages

- Uplink: (size + 33)/80 rounded up
- Downlink: (size + 23)/74 rounded up

B3. The AKE messages shall fit into as few frames as possible

Example
Number of frames (bytes)
per message

PSK ECHDE	EDHOC-13	DTLS 1.3
Flight1	1 (40)	3 (187)
Flight2	1 (45)	3 (190)
Flight3	1 (11)	2 (57)
Total	**3**	**8**

Note
Error in SecDispatch interim calculation:
The factor is 2.6 instead of 3

Requirements summary

- The AKE shall support PSK, RPK, and certificate based authentication (A1)
- The AKE shall support negotiation of algorithms for OSCORE and AKE, and support the same transport as OSCORE (C1,O2)
- After the AKE protocol run, the peers shall agree on OSCORE Master Secret with PFS and good amount of randomness, OSCORE Sender IDs (potentially short), and COSE algorithms to use (O1)
- The AKE shall reuse CBOR, CoAP and COSE primitives and algorithms for low code complexity of a combined OSCORE and AKE implementation (L1)
- The AKE shall be 3-pass/1 RTT, the messages as small as reasonably achievable and fit into as few LoRaWAN packets and 6TiSCH frames as possible (L2,B1,B2,B3)
- New proposed requirement: mixed public key authentication (A2)