ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 9, 2019

G. Selander
Ericsson AB
S. Raza
RISE SICS
M. Furuhed
Nexus
M. Vucinic
University of Montenegro

September 05, 2018

Protecting EST payloads with OSCORE
draft-selander-ace-coap-est-oscore-01

Abstract

This document specifies public key certificate enrollment procedures protected with application-layer security protocols suitable for Internet of Things (IoT) deployments. The protocols leverage payload formats defined in Enrolment over Secure Transport (EST) and existing IoT standards including the Constrained Application Protocol (CoAP), Concise Binary Object Representation (CBOR) and the CBOR Object Signing and Encryption (COSE) format.

Table of Contents

1. Introduction

One of the challenges with deploying a Public Key Infrastructure (PKI) for the Internet of Things (IoT) is certificate enrolment, because existing enrolment protocols are not optimized for constrained environments [RFC7228].

One optimization of certificate enrollment targeting IoT deployments is specified in EST-CoAPs ([I-D.ietf-ace-coap-est]), which defines a version of Enrolment over Secure Transport [RFC7030] for transporting EST payloads over CoAP [RFC7252] and DTLS [RFC6347], instead of secured HTTP.

This document describes a method for protecting EST payloads over CoAP or HTTP with OSCORE [I-D.ietf-core-object-security]. OSCORE specifies an extension to CoAP which protects the application layer message and can be applied independently of how CoAP messages are transported. OSCORE can also be applied to CoAP-mappable HTTP which enables end-to-end security for mixed CoAP and HTTP transfer of application layer data. Hence EST payloads can be protected end-to-

end independent of underlying transport and through proxies translating between between CoAP and HTTP.

OSCORE is designed for constrained environments, building on IoT standards such as CoAP, CBOR [RFC7049] and COSE [RFC8152], and has in particular gained traction in settings where message sizes and the number of exchanged messages needs to be kept at a minimum, see e.g. [I-D.ietf-6tisch-minimal-security], or for securing multicast CoAP messages [I-D.ietf-core-oscore-groupcomm]. Where OSCORE is implemented and used for communication security, the reuse of OSCORE for other purposes, such as enrolment, reduces the implementation footprint.

In order to protect certificate enrolment with OSCORE, the necessary keying material (notably, the OSCORE Master Secret, see [I-D.ietf-core-object-security]) needs to be established between CoAP client and server, e.g. using a key exchange protocol; a trusted third party; or pre-established keys. Different options are allowed and with different properties as is indicated in the next section.

Yet other optimizations to certificate based enrolment are possible further improve the performance of certificate enrolment and certificate based authentication, in particular the use of more compact representations of X.509 certificates.

1.1. EST-CoAPs operational differences

This specification builds on EST-CoAPs [I-D.ietf-ace-coap-est] but transport layer security provided by DTLS is replaced, or complemented, by protection of the application layer data. This specification deviates from EST-CoAPs in the following respects:

- The DTLS record layer is replaced, or complemented, with OSCORE.
- The DTLS handshake is replaced, or complemented, with an alternative key establishment, for example:
  - A key exchange protocol, such as EDHOC [I-D.selander-ace-cose-ecdhe]. The use of a key exchange protocol completes the analogy with EST-CoAPs, and provides perfect forward secrecy (PFS) of the keys used to protect the EST messages. However, PFS is not necessary for the enrolment procedure and adds significant overhead in terms of message size and round trips.
  - Trusted third party (TTP) based provisioning, such as the OSCORE profile of ACE [I-D.ietf-ace-oscore-profile]. This assumes existing security associations between the client and

the TTP, and between the server and the TTP, and reduces the message size and round trips compared to a key exchange protocol.

* Pre-shared keys (PSK). Although one reason for using a PKI is to avoid managing PSK, applying OSCORE directly with PSK specifically during deployment gives a one round-trip enrolment protocol with low message overhead, thereby further reducing the network load and time for commissioning.

- EST payloads protected by OSCORE can be proxied between constrained networks supporting CoAP/CoAPs and non-constrained networks supporting HTTP/HTTPs with a CoAP-HTTP proxy protection without any security processing in the proxy.

1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses terminology from [I-D.ietf-ace-coap-est] which in turn is based on [RFC7030] and, in turn, on [RFC5272].

2. Protocol Design and Layering

EST-oscore uses CoAP [RFC7252] and Block-Wise [RFC7959] to transfer EST messages in the same way as [I-D.ietf-ace-coap-est]. Figure 1 below shows the layered EST-oscore architecture.

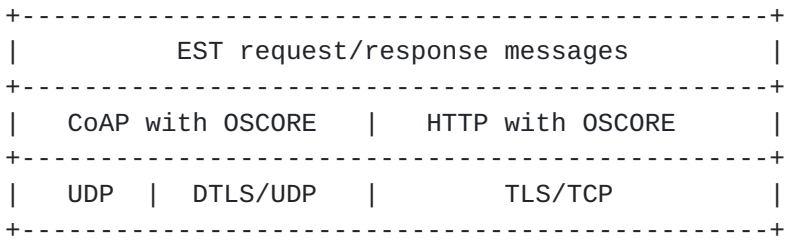

Figure 1: EST protected with OSCORE.

EST-oscore follows closely the EST-coaps and EST design. The message types for simple enroll, reenroll, CA certificate retrieval, CSR Attributes request messages and server-side key generation messages apply. Section references in this paragraph refer to EST-coaps ([I-D.ietf-ace-coap-est]): The payload format, content format,

message bindings and CoAP response codes specified in Section 4.1 - 4.3 apply. The procedure for handling delayed responses described in section 4.4 may also be used with OSCORE. For server-side key generation, the procedure described in Section 4.5 may be used with DecryptKeyIdentifier established out of band or derived from the OSCORE Master Secret. Message fragmentation based on CoAP Block options specified in Section 4.6 is also applicable with OSCORE.

3. Discovery and URI

The discovery of EST resources defined in Section 5 of [I-D.ietf-ace-coap-est], as well as the new Resource Type defined in Section 9.1 of [I-D.ietf-ace-coap-est] apply to EST-oscore. Support for OSCORE is indicated by the "osc" attribute defined in Section 9 of [I-D.ietf-core-object-security], for example:

```
     REQ: GET /.well-known/core?rt=ace.est

     RES: 2.05 Content
   </est>; rt="ace.est";osc
```

The abbreviated EST-coaps URI paths defined in Section 5 of [I-D.ietf-ace-coap-est] also apply.

4. OSCORE-Based Security

EST-oscore depends on the application layer security provided by OSCORE for protecting CoAP and CoAP-mappable HTTP independent of transport. The establishment of keys for OSCORE defines many of the properties of the protocol.

If a key exchange protocols is used, fragmentation of the protocol messages needs to be handled. EDHOC [I-D.selander-ace-cose-ecdhe] may be carried in CoAP in which case Block fragmentation can be used.

(Editor's note: Compare and complete with the analogous Section 6 in EST-coaps)

5. Proxying

As is noted Section 7 of [I-D.ietf-ace-coap-est], in real-world deployments, the EST server will not always reside within the CoAP boundary. The EST-server can exist outside the constrained network in a non-constrained network that does not support CoAP but HTTP, thus requiring an intermediary CoAP-to-HTTP proxy.

Since OSCORE is applicable to CoAP-mappable HTTP the EST payloads can be protected end-to-end between EST client and EST server independent of transport protocol or potential transport layer security which may need to be terminated in the proxy, see Figure Figure 2. The signed certification request SHOULD be bound to the OSCORE security context using a derived secret analogously to the use of tls-unique as described in Section 3.5 of [RFC7030]. The mappings between CoAP and HTTP referred to in Section 6 of [I-D.ietf-ace-coap-est] applies and the additional mappings resulting from the use of OSCORE are specified in Section 11 of [I-D.ietf-core-object-security].

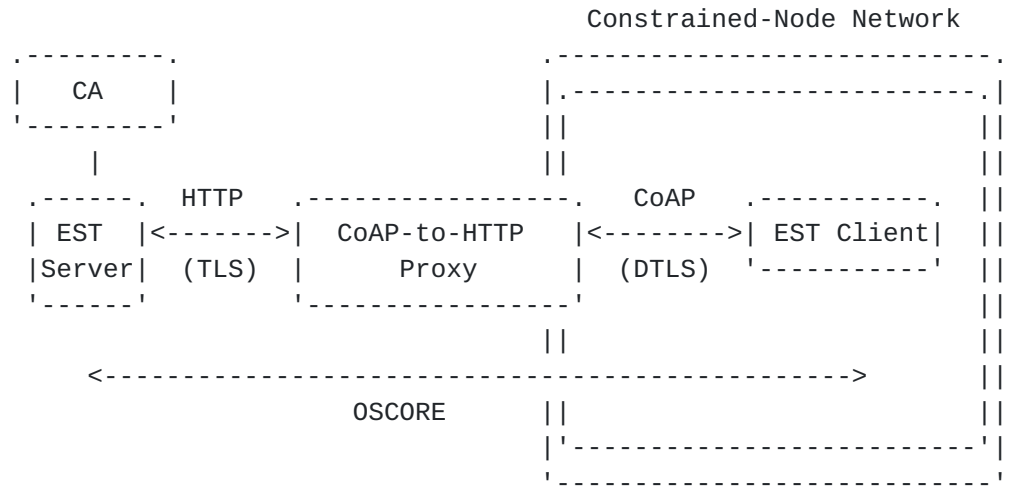

Figure 2: CoAP-to-HTTP proxy at the CoAP boundary.

6. Security Considerations

TBD

7. Privacy Considerations

TBD

8. IANA Considerations

9. Acknowledgments

10. References

10.1. Normative References

[I-D.ietf-ace-coap-est]
Stok, P., Kampanakis, P., Kumar, S., Richardson, M., Furuhed, M., and S. Raza, "EST over secure CoAP (EST-coaps)", draft-ietf-ace-coap-est-05 (work in progress), July 2018.

[I-D.ietf-core-object-security]
Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", draft-ietf-core-object-security-14 (work in progress), July 2018.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7959] Bormann, C. and Z. Shelby, Ed., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)", RFC 7959, DOI 10.17487/RFC7959, August 2016, <https://www.rfc-editor.org/info/rfc7959>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[I-D.ietf-6tisch-minimal-security]
Vucinic, M., Simon, J., Pister, K., and M. Richardson, "Minimal Security Framework for 6TiSCH", draft-ietf-6tisch-minimal-security-06 (work in progress), May 2018.

[I-D.ietf-ace-oscore-profile]
Seitz, L., Palombini, F., Gunnarsson, M., and G. Selander, "OSCORE profile of the Authentication and Authorization for Constrained Environments Framework", draft-ietf-ace-oscore-profile-02 (work in progress), June 2018.

[I-D.ietf-core-oscore-groupcomm]
Tiloca, M., Selander, G., Palombini, F., and J. Park, "Secure group communication for CoAP", draft-ietf-core-oscore-groupcomm-02 (work in progress), June 2018.

[I-D.selander-ace-cose-ecdhe]
Selander, G., Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", draft-selander-ace-cose-ecdhe-09 (work in progress), July 2018.

[RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, DOI 10.17487/RFC5272, June 2008, <https://www.rfc-editor.org/info/rfc5272>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

Appendix A. Examples

TBD

Authors' Addresses

Goeran Selander
Ericsson AB

Email: goran.selander@ericsson.com

Shahid Raza
RISE SICS

Email: shahid.raza@ri.se

Martin Furuhed
Nexus

Email: martin.furuhed@nexusgroup.com

Malisa Vucinic
University of Montenegro

Email: malisav@ac.me