Protecting EST Payloads with OSCORE draft-ietf-ace-coap-est-oscore-04

Göran Selander, Ericsson
Shahid Raza, RISE
Martin Furuhed, Nexus
Mališa Vučinić, Inria
Timothy Claeys

ACE @ IETF 119 – 19/3/2024

Status

- Published -04 on 4 March 2024
  - Resolution of remaining issues raised in John Mattsson’s review
  - Misc updates
- Goal of the presentation
  - Present the resolutions of closed issues

Closed Issues

#34: Payload formats should explicitly mention CBOR-encoded objects

Closed

Context

- Table and section summarizing Content-Formats when CBOR encoding is used was missing

Action performed

- Add a new section and a summary table
- TBDs from I-D.ietf-cose-cbor-encoded-cert

URI	Media Type	Type	#IANA
/crts	N/A	req	-
	application/pkix-cert	res	287
	application/pkcs7-mime;smime-type=certs-only	res	281
/sen	application/pkcs10	req	286
	application/pkix-cert	res	287
	application/pkcs7-mime;smime-type=certs-only	res	281
/sren	application/pkcs10	req	286
	application/pkix-cert	res	287
	application/pkcs7-mime;smime-type=certs-only	res	281
/skg	application/pkcs10	req	286
	application/multipart-core	res	62
/skc	application/pkcs10	req	286
	application/multipart-core	res	62
/att	N/A	req	-
	application/csrattrs	res	285

Table 2: EST functions and the associated ASN.1 CoAP Content-Format identifiers

URI	Media Type	Type	#IANA
/crts	N/A	req	-
	application/cose-c509-cert	res	TBD6
/sen	application/cose-c509-pkcs10	req	TBD7
	application/cose-c509-cert	res	TBD6
/sren	application/cose-c509-pkcs10	req	TBD7
	application/cose-c509-cert	res	TBD6
/skg	application/cose-c509-pkcs10	req	TBD7
	application/multipart-core	res	62
/skc	N/A	req	-
	N/A	res	-
/att	N/A	req	-
	application/csrattrs	res	TBD5

Table 4: EST functions and the associated CBOR CoAP Content-Format identifiers

#35: Normative requirements on Content-Format support (ASN.1 / CBOR)

Context

- EST-oscore may transport ASN.1 or CBOR objects
- Content type negotiation happens through CoAP's Accept option
- Specify normative requirements on what is supported
- Discussed at IETF 118 and in GitHub

Action performed

```
+ EST-oscore servers MUST support both the DER-encoded ASN.1 objects and the CBOR-encoded objects.
+ This means supporting formats detailed in {{der}} and {{cbor}}.
+ It is up to the client to support only DER-encoded ASN.1, CBOR encoding, or both.
+ As a reminder, Content-Format negotiation happens through CoAP's Accept option present in the requests.
```

#38: Content-Format support for DER-encoded ASN.1 objects

- Old text had a MAY on Content-Format 287 (application/pkix-cert) on server
- Same as in RFC 9148
- May lead to interoperability issues where client supports only 287 but server only supports 281 (application/pkcs7-mime; smime-type=certs-only)
  - Action performed: Mandate both 281 and 287 on server
- Esko Dijk commented: *“in the ANIMA WG we have discovered that there are some management problems if the client uses type 287 only; it's a very limited method of getting only one CA certificate. So a better solution will be to ensure the client does not use a single request asking for 287, but something more intelligent that enables it to get multiple CA certificates if needed.”*
  - draft-ietf-anima-constrained-voucher-24:
    - When a Registrar receives a "CA certificates request" (/crts) request with a CoAP Accept Option with value 287 ("application/pkix-cert") it MUST return only the single CA certificate that is the envisioned or actual CA authority for the current, authenticated Pledge making the request. An exception to this rule is when the domain has been configured to operate with multiple CA trust anchors only: then the Registrar returns a 4.06 Not Acceptable error to signal to the client that it needs to request another Content Format that supports retrieval of multiple CA certificates.
    - Means that the client SHOULD support 281 which collides with current text "It is up to the client to support only Content-Format 281, 287 or both.”

#43:State sufficient conditions for a signed CSR to be used to enroll a ECDH public key

Context

- Opened by Göran Selander on 9 February 2024
- *“We describe the use of ECDH in the CSR for proving possession of the private key when enrolling a public key to be used with static ECDH based authentication. We should also state that for curves like P-256, P-384, P-521 it is allowed to prove possession by signing the CSR with the same private key… “*
- NIST SP 800-56A and 800-57 allow the use of a static DH key for signing the CSR

Action performed:

- Complemented the Section on Static DH Keys

```
- Because a DH key pair cannot be used for signing operations, the EST client attempting to enroll a DH key must use an alternative proof-of-possession algorithm.
- The EST client prepares the PKCS#10 object and computes a MAC, replacing the signature, over the certification request information by following the steps in {{Section 6 of RFC6955}}.
+ In general, a given key pair should only be used for a single purpose, such as key establishment, digital signature, key transport.
+
+ The EST client attempting to enroll a DH key for a key usage operation other than digital signature SHOULD use an alternative proof-of-possession algorithm:
+ The EST client SHOULD prepare the PKCS#10 object and compute a MAC, replacing the signature, over the certification request information by following the steps in {{Section 6 of RFC6955}}.
```

…

```
+ In some cases, it may be beneficial to exceptionally use the static DH private key associated to the public key used in enrollment for a one-time signing operation of the CSR.
+ While a key pair should only be used for a single purpose (e.g. key establishment or signing), this exceptional use for one-time signing of the CSR is allowed, as discussed in Section 5.6.3.2 of {{SP-800-56A}} and Section 5.2 of
  {{SP-800-57}}.
```

Open Issues

Open Issues

- #36: Consider the use of challengePassword for signature keys without EDHOC
- #29: Adding message flow example
- #19: Clarify scope in the introduction and the abstract

Next Steps

- Resolve remaining open issues
- More reviews?

Thank you!