EST for C509 Certificates

draft-liao-ace-est-c509-02

IETF 126 ACE WG

Lijun Liao · NIO

Background

The **COSE WG** is working on CBOR encoded X.509 (C509) certificates and CSRs

- Efficiency: reduce bandwidth / storage, accelerate TLS handshakes, and lower parsing / serialization overload
- Reduced complexity: Avoiding ASN.1/DER reduces code size, complexity and attack surface
- Complementing parts for a C509 based PKI in progress: CRL, OCSP, etc.

Missing component: EST for C509

- In systems with diverse device classes, using a common certificate format (**C509**) simplifies integration and provisioning

The **ACE WG** has worked on efficient and low-complexity enrolment

- EST-CoAPs
  - **RFC 9148**
  - does not support C509
- EST-OSCORE
  - **draft-ietf-ace-coap-est-oscore**
  - supports C509

This draft: EST for C509 via COAP and HTTP

- CoAP
  - Updates RFC 9148 to support C509
- HTTP (for devices without CoAP capability)
  - Updates RFC 7030 to support C509

*C509 specification

(Data Retrieval) Operations

HTTP OP	CoAP OP	Description	Request	Response
caps	-	Capability discovery	(none)	**Plaintext list of supported operations**
cacerts	crts	Single CA certificate or CA certificate set/chain retrieval		**C509Certificate* or COSE_C509*, depends on the 'Accept' option in Request**
crli	**crli**	**CRL metadata retrieval**	**(none)**	**C509CRLInfo (liao-cose-c509-revocation)**
crl	**crl**	**CRL retrieval**	**(none)**	**C509CRL (liao-cose-c509-revocation)**
csrattrs	att	CSR template retrieval	(none)	**C509CertificationRequestTemplate***

*C509 specification

(Certificate Enrollment) Operations

HTTP OP	CoAP OP	Description	Request	Response
kemc	**kemc**	**Challenge for KEM-only keypairs**	**C509PublicKey (this I-D)**	**C509KemChall (this I-D)**
simple enroll	sen	Certificate enrollment	**C509Certification Request***	**C509Certificate***
simpler eenroll	sren	Certificate re-enrollment	**C509Certification Request***	**C509Certificate***
serverk eygen	skc	Certificate enrollment with keypair generated by the server	**C509Certification Request***	**C509_PEM***

WG Adoption?

- This I-D fills a gap for enrolment of lightweight certs.

	CoAP/DTLS	CoAP/OSCORE	HTTPS
X.509 Certificates	RFC 9148 (ACE WG)	draft-ietf-ace-coap-est-oscore (ACE WG)	RFC 7030
C509 Certificates	**This I-D**		**This I-D**