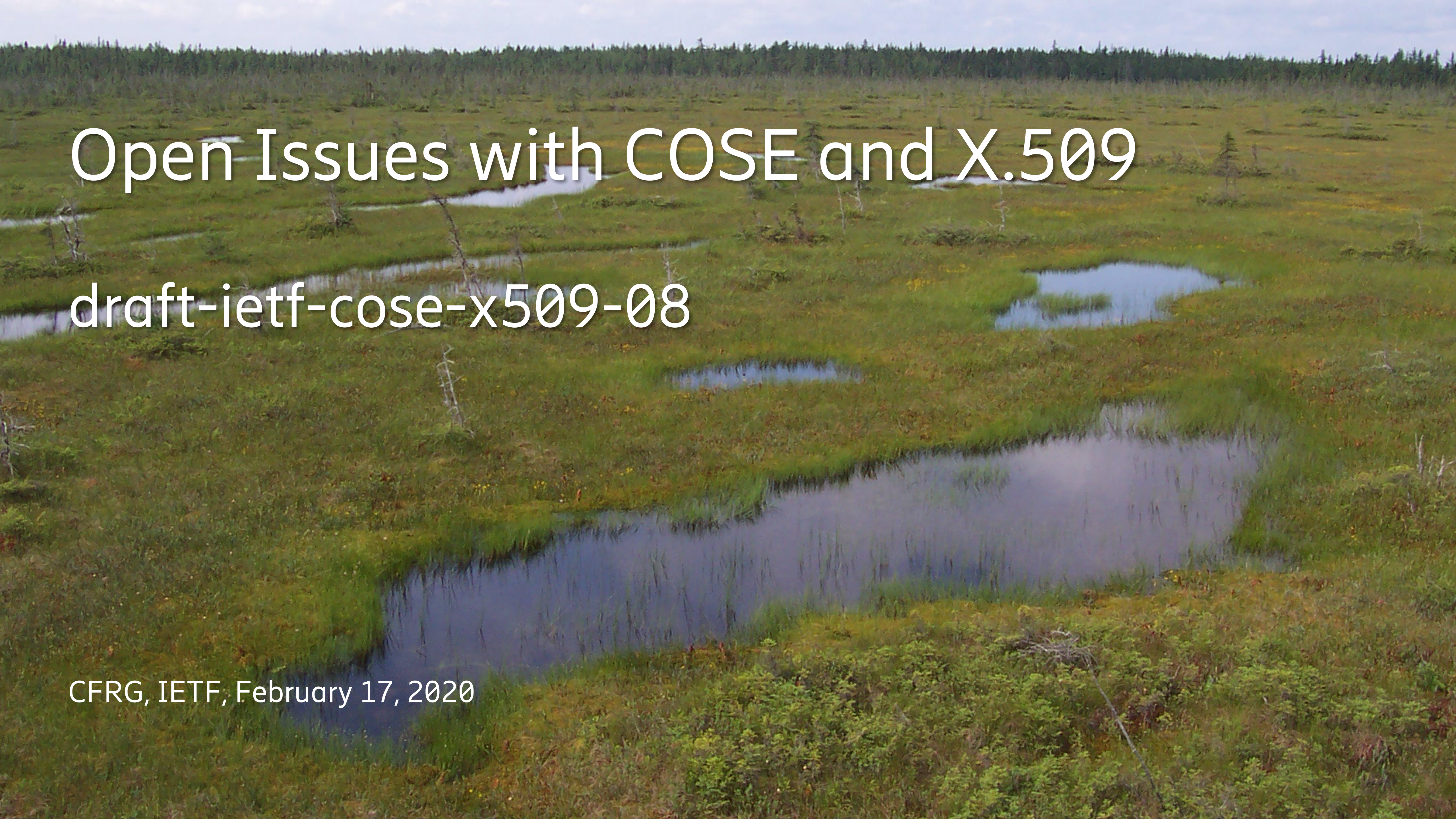


Open Issues with COSE and X.509

draft-ietf-cose-x509-08

CFRG, IETF, February 17, 2020

Open Issues with COSE and X.509

draft-ietf-cose-x509-08

Major discussion points:

1. Many people have expressed that they don't understand the trust assumptions mentioned for x5u.

> “As this header parameter implies a trust relationship between the party generating the x5u parameter and the party hosting the referred-to resource, this header parameter MUST be in the protected attribute bucket.”

Is x5u meant to distribute trust anchors in some way?

I

Open Issues with COSE and X.509
draft-ietf-cose-x509-08

Major discussion points:

2. It was suggested that parts of the end-entity certificate need to be integrity protected. This would make the current specification of x5bag and x5chain insecure.

“As the contents of this header parameter are untrusted input, the header parameter can be in either the protected or unprotected header bucket.”

Several comments that information needs to be protected. One reason for protection mentioned in [SIGMA] is that an attacker can ”borrow” a public key and register it with a different identity. CA has in the past not always required proof-of-possession of the private key.

- Putting everything in protected would be problematic for Michael's use case with middleboxes removing intermediary certs.

- Putting the cert in external_aad like EDHOC would change the COSE processing...

Open Issues with COSE and X.509

draft-ietf-cose-x509-08

Minor discussion points:

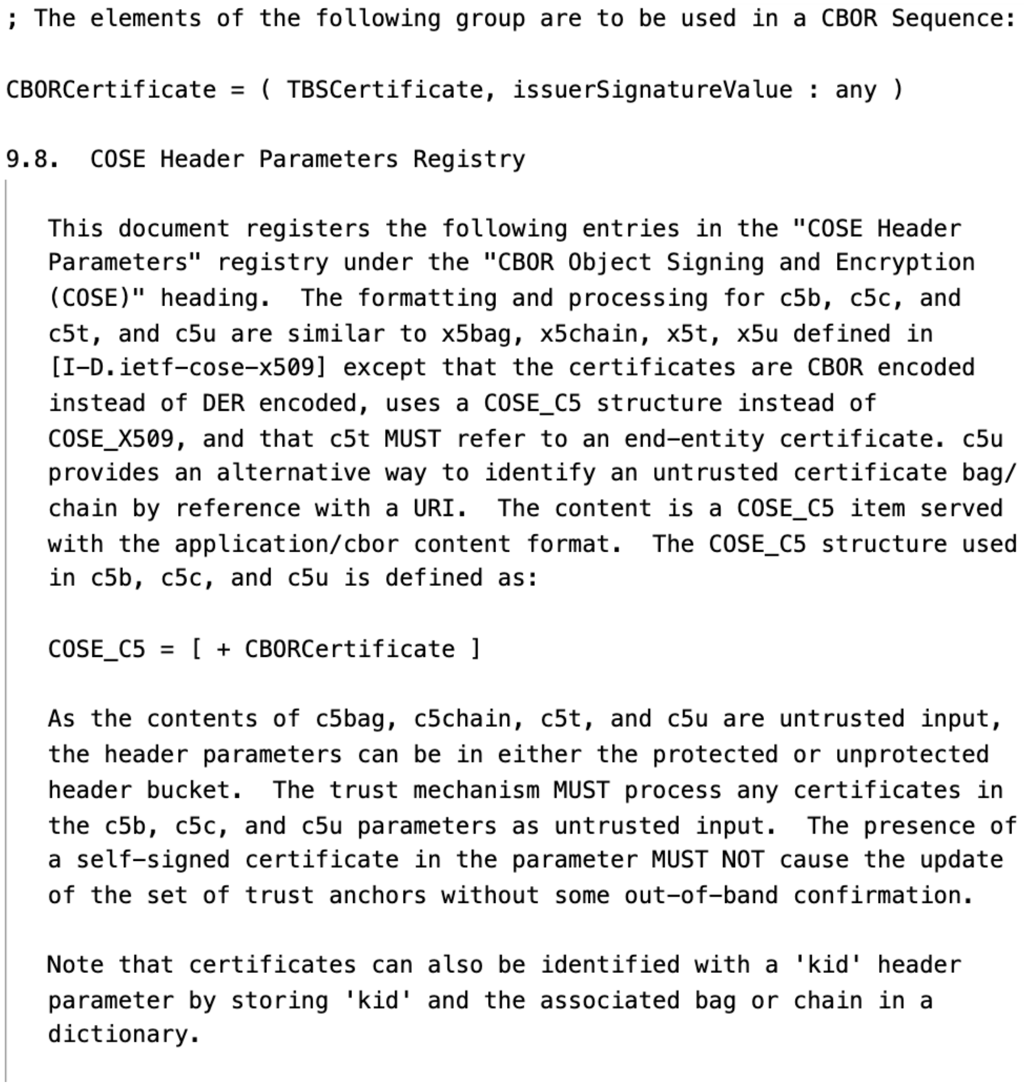
3. - Protection requirements for x5u is https or coaps

- OSCORE and other protection mechanisms are not allowed.
- Unclear why protection is even needed, maybe linked to point 1?

4. – Mandatory to use PKCS7 instead of COSE_X509

Related issues with CBOR encoded X.509 Certificates

draft-mattsson-cose-cbor-cert-compress



```
; The elements of the following group are to be used in a CBOR Sequence:

CBORCertificate = ( TBSCertificate, issuerSignatureValue : any )
```

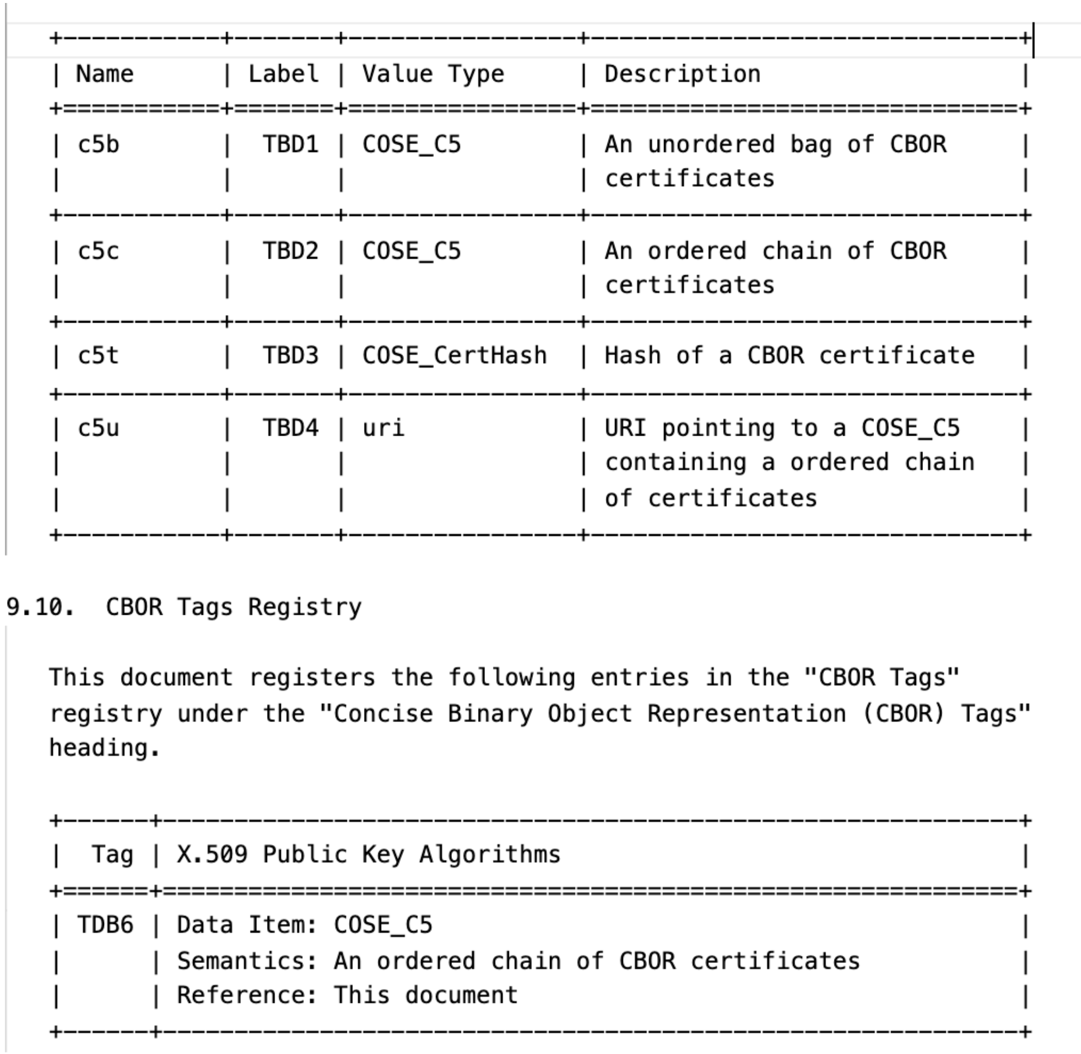
9.8. COSE Header Parameters Registry

This document registers the following entries in the "COSE Header Parameters" registry under the "CBOR Object Signing and Encryption (COSE)" heading. The formatting and processing for c5b, c5c, and c5t, and c5u are similar to x5bag, x5chain, x5t, x5u defined in [I-D.ietf-cose-x509] except that the certificates are CBOR encoded instead of DER encoded, uses a COSE_C5 structure instead of COSE_X509, and that c5t MUST refer to an end-entity certificate. c5u provides an alternative way to identify an untrusted certificate bag/chain by reference with a URI. The content is a COSE_C5 item served with the application/cbor content format. The COSE_C5 structure used in c5b, c5c, and c5u is defined as:

```
COSE_C5 = [ + CBORCertificate ]
```

As the contents of c5bag, c5chain, c5t, and c5u are untrusted input, the header parameters can be in either the protected or unprotected header bucket. The trust mechanism MUST process any certificates in the c5b, c5c, and c5u parameters as untrusted input. The presence of a self-signed certificate in the parameter MUST NOT cause the update of the set of trust anchors without some out-of-band confirmation.

Note that certificates can also be identified with a 'kid' header parameter by storing 'kid' and the associated bag or chain in a dictionary.



Name	Label	Value Type	Description
c5b	TBD1	COSE_C5	An unordered bag of CBOR certificates
c5c	TBD2	COSE_C5	An ordered chain of CBOR certificates
c5t	TBD3	COSE_CertHash	Hash of a CBOR certificate
c5u	TBD4	uri	URI pointing to a COSE_C5 containing a ordered chain of certificates

9.10. CBOR Tags Registry

This document registers the following entries in the "CBOR Tags" registry under the "Concise Binary Object Representation (CBOR) Tags" heading.

Tag	X.509 Public Key Algorithms
TDB6	Data Item: COSE_C5 Semantics: An ordered chain of CBOR certificates Reference: This document