

A nighttime photograph of the Vienna State Opera House, a grand neoclassical building with a green-tiled roof and ornate facade. The building is illuminated with warm lights. In the foreground, a yellow and green double-decker bus is parked on a wet street, reflecting the lights. The sky is dark blue with some clouds. The text "COSE interim meeting" is overlaid in a large, black, sans-serif font.

COSE interim meeting

2022-01-26 @ 16:00 UTC

NOTE WELL



This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (<https://www.ietf.org/contact/ombudsteam/>) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- [BCP 9](#) (Internet Standards Process)
- [BCP 25](#) (Working Group processes)
- [BCP 25](#) (Anti-Harassment Procedures)
- [BCP 54](#) (Code of Conduct)
- [BCP 78](#) (Copyright)
- [BCP 79](#) (Patents, Participation)
- <https://www.ietf.org/privacy-policy/> (Privacy Policy)

Living the IETF Code of Conduct

Reminder of key points of the Code of Conduct [RFC 7154]:

1. IETF participants extend respect and courtesy to their colleagues at all times.
2. IETF participants have impersonal discussions.
3. IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments.
4. Individuals are prepared to contribute to the ongoing work of the group



Agenda

1. Administrivia (Chairs) - 5 min
2. Document Status (Chairs) - 10 min
3. x509 (Chairs) - 10 min
4. draft-ietf-cbor-encoded-cert - 5 min
5. HPKE for COSE - 20 min
6. AOB - 10 min



Administrivia

- Note well
- Minutes - <https://notes.ietf.org/notes-ietf-interim-2022-cose-01-cose>
 - Note taker(s):
- Jabber - chairs
 - Jabber Scribe:
- Meeting and attendees (in the minutes) are recorded
- Agenda bartering



Document status

- Draft-ietf-cose-hash-algs - in RFC-Editor wait reply
 - [Issue #42](#) seems blocking
- Draft-ietf-cose-rfc8152bis-algs (RFC 9053 to be) - AUTH48, almost all questions/discussions are completed
- Draft-ietf-cose-rfc8152bis-struct (RFC 9052 to be) - AUTH48, waits confirmation of latest version and publication
- Draft-ietf-cose-countersign - with Ben
- Draft-ietf-cose-x509 - past IESG evaluation, some open discussion on next slide

x509 open issues



Filters Labels 11 Milestones 0 New issue

✕ Clear current search query, filters, and sorts

<input type="checkbox"/>	5 Open ✓ 4 Closed	Author ▾	Label ▾	Projects ▾	Milestones ▾	Assignee ▾	Sort ▾
<input type="checkbox"/>	ISO 18013-5 replying on x509 fixed? x509 #39 opened on Oct 10, 2021 by ivajloip						
<input type="checkbox"/>	media-type parameter, CoRE Content-Formats, fixed? x509 #37 opened on Jun 23, 2021 by emanjon						1
<input type="checkbox"/>	Allow OSCORE [RFC8613] for x5u CoAP URIs fixed? x509 #33 opened on Jan 21, 2021 by emanjon						
<input type="checkbox"/>	What is the trust relationship for the x5u parameter? x509 #31 opened on Dec 18, 2020 by laurencelundblade						3
<input type="checkbox"/>	Header protection and consistency with JWS fixed? x509 #30 opened on Dec 18, 2020 by laurencelundblade						8

💡 **ProTip!** Add [no:assignee](#) to see everything that's not assigned.

x509 - issue #31



- Trust relationship for the x5u parameter
 - John: Uses cases?
 - Ivaylo: Constrained device sends smaller payload?

x509 to close



- Header protection and consistency with JWS [#30](#)
- Allow OSCORE [RFC8613] for x5u CoAP URIs [#33](#)
- media-types [#37](#)

draft-ietf-cbor-encoded-cert



HPKE for COSE





AOB?



Goodbye and have a nice day!