NN November 2025

IETF 124 Session title

This session is being recorded

I E T F®

Note taker

HedgeDoc

Volunteers?

Note Well

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies. For a linked version of this text, please visit **www.ietf.org/note-well** or use the QR code below.

IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times (see **RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy**). If you have any concerns about behavior, please contact the *Ombudsteam* who have a duty of confidentiality and extensive powers to act, as set out in **RFC 7776: IETF Anti-Harassment Procedures**.

If you are aware that any IETF contribution (as defined in **RFC 5378: Rights Contributors Provide to the IETF Trust**) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see **RFC 8179: Intellectual Property Rights in IETF Technology**).

For detailed process information consult **RFC 2026: Internet Standards Process** and *RFC 2418:* **IETF Working Group Guidelines and Procedures** and updates to those.

The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the **IETF Privacy Statement**.

For advice, please talk to Working Group chairs or Area Directors.

This session is being recorded

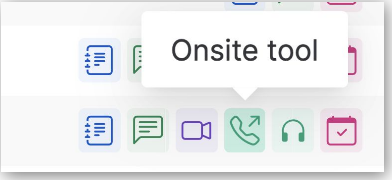
IETF 124 Meeting Tips

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to join the queue, show hands
- *Keep audio and video off if not using the onsite version.*

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session.
- Use of a headset is strongly recommended.



All participants

- State your name each time you begin speaking in the queue

Resources for IETF 124 Montreal

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/meeting/preparation/
- If you need technical assistance, see the Reporting Issues page:
  https://www.ietf.org/meeting/issues/

Agenda

- Welcome and Administrivia - Chairs - 10
- Status of Adopted Documents - Henk Birkholtz - 15
- Receipt Profiles - Amaury Chamayou - 15
- SCITT & OCP Case Study - Nobuo Aoki - 15
- Applying SCITT to FDA Labels - Dick Brooks - 15
- Slack/AOB - All - 20

Any agenda bashing?

I E T F®

Status of Adopted Documents

WG Drafts

An Architecture for Trustworthy and Transparent Digital Supply Chains

SCITT Reference APIs

Related Drafts

COSE Merkle Tree Proofs

COSE Hash Envelope

Status of Adopted Documents

WG Drafts

An Architecture for Trustworthy and Transparent Digital Supply Chains

SCITT Reference APIs

Related Drafts

SUBMITTED TO IESG FOR PUBLICATION 🎉

COSE Merkle Tree Proofs

COSE Hash Envelope

IETF

Architecture - V22

ALSO SUBMITTED TO IESG FOR PUBLICATION 🎉

```
9.4.2.  Key Compromise

   It is important for Issuers and Transparency Services to clearly
   communicate when keys are compromised, so that Signed Statements can
   be rejected by Transparency Services or Receipts can be ignored by
   Relying Parties.  Transparency Services whose receipt signing keys
   have been compromised can roll back their Statement Sequence to a
   point before compromise, establish new credentials, and use them to
   issue fresh Receipts going forward.  Issuers are encouraged to follow
   existing best practices if their credentials are compromised.
   Revocation strategies for compromised keys are out of scope for this
   document.

9.4.3.  Bootstrapping

   Bootstrapping mechanisms that solely rely on Statement registration
   to set and update registration policy can be audited without
   additional implementation-specific knowledge, and are therefore
   preferable.  Mechanisms that rely on pre-configured values and do not
   allow updates are unsuitable for use in long-lived service
   deployments, in which the ability to patch a potentially faulty
   policy is essential.

9.5.  Implications of Media-Type Usage

   The Statement (scitt-statement+cose) and Receipt (scitt-receipt+cose)
   media types describe the expected content of COSE envelope headers.
   The payload media type ('content type') is included in the COSE
   envelope header.  [STD96] describes the security implications of
   reliance on this header parameter.

   Both media types describe COSE_Sign1 messages, which include a
   signature, and therefore provide integrity protection.

9.6.  Cryptographic Agility

   Because the SCITT Architecture leverages [STD96] for Statements and
   Receipts, it benefits from the format's cryptographic agility.
```

GitHub PRs

67 PRs
>5 Substantial reviews

Side-by-side diff

IETF 123: v14
IETF 124: v22

SCRAPI - v05

In Working Group Last Call 📣

Transparency Service Keys

This endpoint is used to discover the public keys that can be used by relying parties to verify Receipts issued by the Transparency Service.

The Transparency Service responds with a COSE Key Set, as defined in {{Section 7 of RFC9052}}.

Request:

```
GET /.well-known/scitt-keys HTTP/1.1
Host: transparency.example
Accept: application/cbor
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/cbor

Body (in CBOR diagnostic notation)

[
  {
    -1:1,
    -2:h'65eda5a12577c2bae829437fe338701a10aaa375e1bb5b5de108de439c08551d',
    -3:h'1e52ed75701163f7f9e40ddf9f341b3dc9ba860af7e0ca7ca7e9eecd0084d19c',
    1:2,
    2:'kid1'
  },
  {
    -1:1,
    -2:h'bac5b11cad8f99f9c72b05cf4b9e26d244dc189f745228255a219a86d6a09eff',
    -3:h'20138bf82dc1b6d562be0fa54ab7804a3a64b6d72ccfed6b6fb6ed28bbfc117e',
    1:2,
    2:'kid2'
  }
]
```

GitHub PRs

2 PRs
1 substantial add

Current Version

IETF 123: v05
IETF 124: v05

Questions?

We're in the home straight with the current documents and scope. What's missing?

This time we skipped over what the adopted documents are actually for. Is anyone unclear?