

Automatic IETF Minutes

Eric Rescorla
ekr@rtfm.com



It is characteristic of all committee discussions and decisions that every member has a vivid recollection of them and that every member's recollection of them differs violently from every other member's recollection. Consequently, we accept the convention that the official decisions are those and only those which have been officially recorded in the minutes by the officials.

—Sir Humphrey Appleby, ["Yes, Prime Minister": S2E1](#).

All working group sessions (including those held outside of the IETF meetings) shall be reported by making minutes available. These minutes should include the agenda for the session, an account of the discussion including any decisions made, and a list of attendees. The Working Group Chair is responsible for insuring that session minutes are written and distributed, though the actual task may be performed by someone designated by the Working Group Chair. The minutes shall be submitted in printable ASCII text for publication in the IETF Proceedings, and for posting in the IETF Directories and are to be sent to: minutes@ietf.org

—RFC 2418, S 3.1



But taking
minutes sucks

Automatically Generating Minutes from Meetecho Transcript

[Markdown Version](#) | [Recording 1](#) | [Recording 2](#)

Session Date/Time: 22 Jul 2025 15:00

tls

Summary

This TLS working group meeting covered several key topics, including status updates on working group documents, adoption calls for new drafts, and discussions around post-quantum cryptography (PQC). A significant portion of the meeting focused on the transition to PQC, including dual certificates, hybrid key exchange, and ML-KEM only key agreement. The meeting also addressed extended key update, jumbo records and a potential applicability statement.

Key Discussion Points

- **Working Group Document Status:** Several documents are nearing completion, including 8447 BIS, ECH drafts, and TLS 1.3 updates. Concerns regarding expired drafts and the need for author availability were raised.
- **Adoption Calls:** Discussion on adoption calls for SLHDSA, composite MLDSA, dual certs, and MTLS flags. The working group will proceed with adoption calls with an awareness of address harvesting and the need for a hybrid approach.
- **PQ Algorithm Considerations:** The need to decide whether PQ algorithms will be informational or standards track documents was highlighted, as well as the development of applicability statements and security considerations.
- **Stephen's Catch Draft:** A working group last call was considered, but delayed to incorporate community comments.
- **Extended Key Update:** Discussion of forward secrecy vs post compromise security and simplification of conflict resolution and

With Markdown Suitable for Cutting-and-Pasting

****Session Date/Time:**** 22 Jul 2025 15:00

tls

Summary

This TLS working group meeting covered several key topics, including status updates on working group documents, adoption calls for new drafts, and discussions around post-quantum cryptography (PQC). A significant portion of the meeting focused on the transition to PQC, including dual certificates, hybrid key exchange, and ML-KEM only key agreement. The meeting also addressed extended key update, jumbo records and a potential applicability statement.

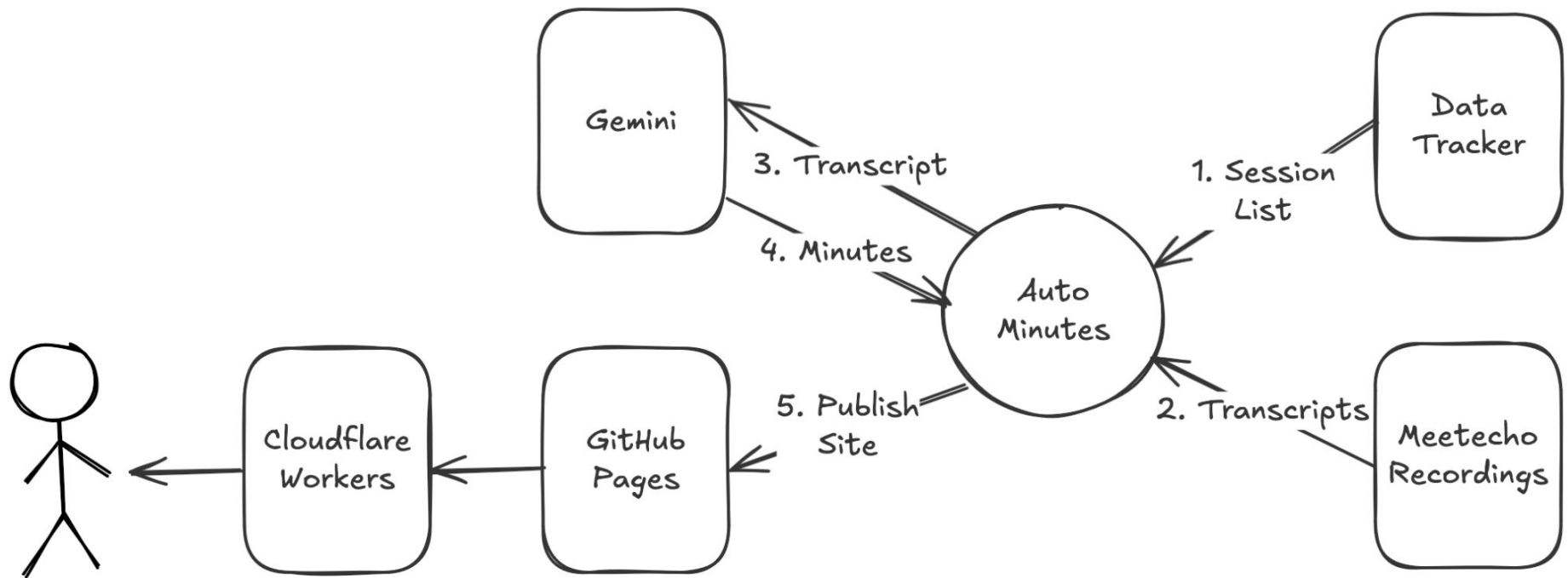
Key Discussion Points

- * ****Working Group Document Status:**** Several documents are nearing completion, including 8447 BIS, ECH drafts, and TLS 1.3 updates. Concerns regarding expired drafts and the need for author availability were raised.
- * ****Adoption Calls:**** Discussion on adoption calls for SLHDSA, composite MLDSA, dual certs, and MTLS flags. The working group will proceed with adoption calls with an awareness of address harvesting and the need for a hybrid approach.
- * ****PQ Algorithm Considerations:**** The need to decide whether PQ algorithms will be informational or standards track documents was highlighted, as well as the development of applicability statements and security considerations.
- * ****Stephen's Catch Draft:**** A working group last call was considered, but delayed to incorporate community comments.
- * ****Extended Key Update:**** Discussion of forward secrecy vs post compromise security and simplification of conflict resolution and rejection of key updates.
- * ****Jumbo Records:**** Presentation on large record sizes for TLS and DTLS, including implementing variable length length field and new record type format.
- * ****ML-KEM Only Key Agreement:**** Updates on the draft, including removing unnecessary text and addressing concerns about failures.
- * ****PAKE Authentication:**** Presentation on TLS 1.3 PAKE authentication, with concerns on how to integrate with three-move PAKE integration.
- * ****Dual Certificates:**** Extensive discussion on the transition to PQC and the pros and cons of dual certificates versus composite certificates. The working group members have conflicting ideas and a consensus needs to be met.

Decisions and Action Items

- * ****Extended Key Update:**** Work with FAT on proper text and address DTLS section to retransmissions.
- * ****Jumbo Records:**** Review, and implement variable length length field in a PR, then discuss on the list.
- * ****PAKE Authentication:**** Schedule an adoption call with the understanding that the content will be open to change after adoption.
- * ****Dual Certificates:**** Revisit on the mailing list.

Workflow



More info



Site: <https://ietfminutes.org>

Live-ish minutes for IETF 124 (hopefully) at:
<https://ietfminutes.org/minutes/ietf24>

Source:
<https://github.com/ekr/auto-minutes/>

ekr@rtfm.com