16 October 2024

TLS WG Virtual Interim

This session is being recorded

Internet Engineering Task Force

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)

IETF

Note Really Well

- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

IETF

Agenda

Topic: FATT Process

1. Review intent
2. Discuss Process
   a. Salient Point 1 (Before WG adoption)
   b. Salient Point 2 (Before WG Last Call)
   c. Diagram 1 (FATT Process) & 2 (Overall Process)
3. Discuss
4. Outstanding Issue

NOTE: We scheduled 2 hours; the agenda need not expand to fill the time.

Intent

Preserve existing security properties that have already been proven.

In other words, maintain the pact the TLS WG made with security researchers during development of TLS 1.3.

Question

Does anybody think that maintaining these properties / the pact is a bad thing?

Salient Point 1: Before WG Adoption

The WG the chairs will send the document for triage by the FATT to get an opinion on what sort of security analysis is appropriate for the document to ensure that:

1. the security properties of TLS are maintained
2. any newly defined security properties are verified

The review **does not** gate WG adoption. The opinion will be provided to the WG so that appropriate action can be taken to provide the appropriate security analysis indicated by the FATT.

FATT assigns a Liaison to interact with WG.

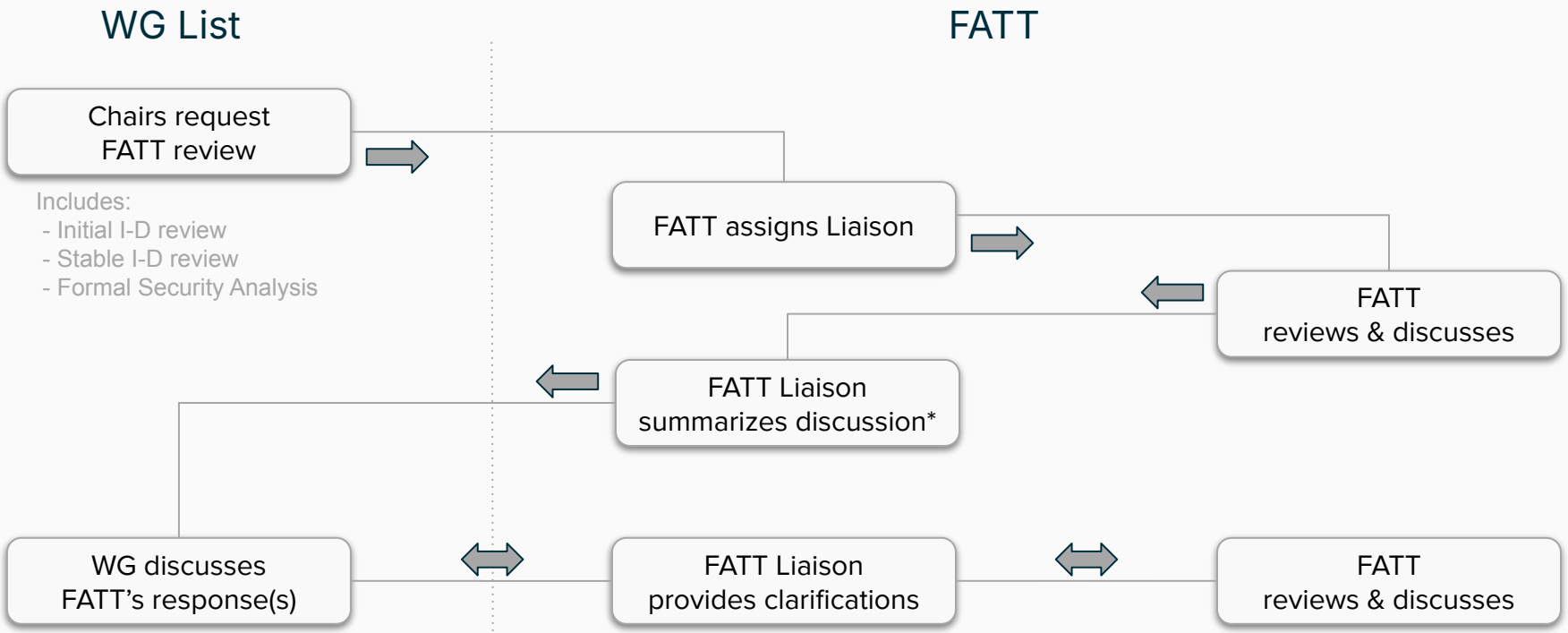
Salient Point 2: Before WGLC

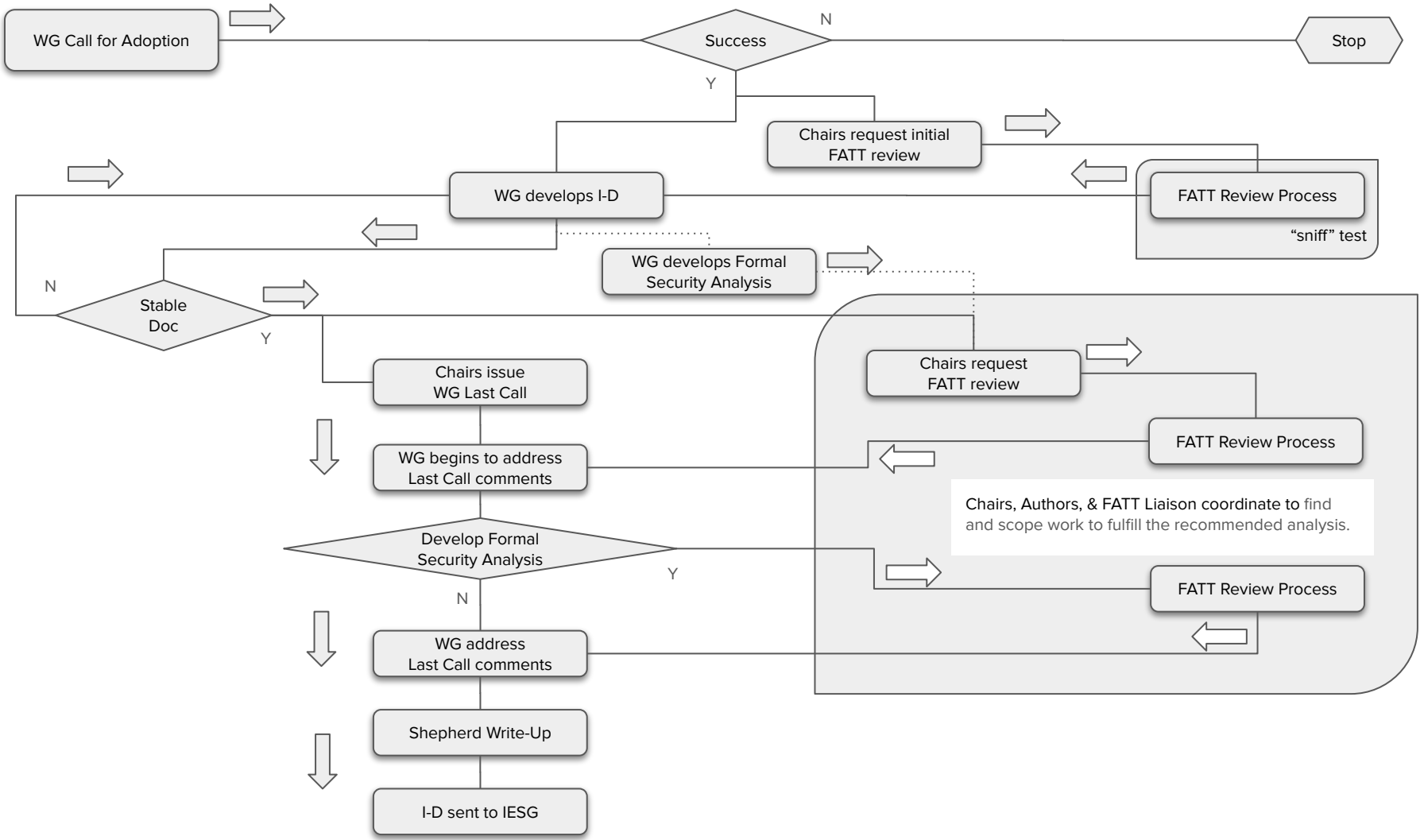
When the protocol is stable the document will again be reviewed by the FATT along with available security analysis to determine if additional security analysis is required due to changes in the protocol or due to insufficient analysis based on the initial review.

The opinion will be provided to the working group for evaluation during the WGLC. If the FATT indicates more security analysis is appropriate the working group will need consensus to move the document forward without completing the recommended analysis.

The type of analysis and status with respect to the FATT recommendation will be noted in the Shepherd Write-Up submitted to the IESG.

FATT Process Diagram




WG Call for Adoption
Success
N
Stop
Y
Chairs request initial FATT review
FATT Review Process
"sniff" test
WG develops I-D
WG develops Formal Security Analysis
N
Stable Doc
Y
Chairs issue WG Last Call
Chairs request FATT review
FATT Review Process
WG begins to address Last Call comments
Chairs, Authors, & FATT Liaison coordinate to find and scope work to fulfill the recommended analysis.
Develop Formal Security Analysis
Y
FATT Review Process
N
WG address Last Call comments
Shepherd Write-Up
I-D sent to IESG

Outstanding Issue

How do we get formal security analysis if one is requested but the authors do not have the expertise to provide one?