InkBridge Networks

EAP-TLS

IETF 127

Copyright © 2026 InkBridge Networks

REVIEW

- RFC 9190 (EAP-TLS) and RFC 9742 (other TLS-based EAP methods) define EAP for TLS 1.3
- The main issue is session tickets.
  - TLS 1.2 they are in the TLS header
  - TLS 1.3 they are sent after the TLS header

Copyright © 2026 InkBridge Networks

THE PROBLEM

- Most implementations assume that TLS 1.3 session tickets come *immediately* after the TLS header
  - But this is not a requirement of TLS 1.3!
- Stateless session tickets are also allowed for TLS 1.3
  - But if they’re sent after inner username/password, supplicants fail!
- This is a poorly tested code path

Copyright © 2026 InkBridge Networks

THE PROBLEM (2)

- Heikki's post to the EMU list 16 November 2026
  - supplicants assume a correlation between EAP fragment and TLS data
  - i.e. the EAP state machine can be driven from reception of EAP fragments, and not from TLS state!
- This (and previous) problems are seen in multiple supplicants

Copyright © 2026 InkBridge Networks

THE PROBLEM (3)

- PQC certs are large
  - 80+ round trips with 1K fragments
  - Leading to 10s+ authentication time
- Question: How can we send large packets across a RADIUS proxy fabric?

  Answer: You can’t

Copyright © 2026 InkBridge Networks

SOLUTION(S)

- Reiterate that EAP state machine MUST allow for all possible TLS behavior
  - MUST NOT assume a correlation between TLS messages and EAP fragments
  - MUST NOT change EAP state based on EAP fragmentation
  - MUST support TLS 1.3 session tickets after inner tunnel authentication succeeds

Copyright © 2026 InkBridge Networks

SOLUTION - STATE MACHINE

- Reiterate that EAP state machine MUST allow for all possible TLS behavior
  - MUST NOT assume a correlation between TLS messages and EAP fragments
  - MUST NOT change EAP state based on EAP fragmentation
  - MUST support TLS 1.3 session tickets after inner tunnel authentication succeeds

Copyright © 2026 InkBridge Networks

SOLUTION - PAC

- Partial solution, and leverages the previous fixes
- Separate TLS resumption from inner-tunnel auth
  - Allow resumption *and* inner-tunnel auth
- Addresses much of the issues with PQC

Copyright © 2026 InkBridge Networks