

draft-ietf-tls-pake

TLS 1.3 PAKE authentication

Laura Bauman, Apple

David Benjamin, Google

Samir Menon, Apple

Chris Wood, Apple

Issues Closed at IETF 124

draft-ietf-tls-pake-01

-00 —> -01

- Issue #35: Add CPace (Resolved) ✓
- Issue #23: SPAKE2+ Context String? (Resolved) ✓
- Issue #4: State properties required for PAKES used (Resolved) ✓
- Issue #21: Server choice between PSK/PAKE/Certs (Resolved) ✓
- Issue #26: Make future PAKE integration constraints more clear (Resolved) ✓
 - Sub-Issue #38: Generic vs protocol specific extension (Resolved) ✓
 - Sub-Issue: Multi-Round PAKE Integration (Resolved) ✓

Open Issues

- Issue #6: Clarify client + server identity negotiation
 - No clear use cases for changing.
- Issue #39: Uses cases / motivation for using PAKE instead of other authentication methods
 - Additional text on motivation could be useful
- Issue #41: Add OQUAKE?

Formal Analysis

- **Goal:** Prove that explicit key confirmation messages are sufficiently replaced by TLS Finished messages
- **Approach:** extend the TLS 1.3 model in ProVerif (used for analyzing ECH)
- **Status:** Needs polish before being added to GitHub

Next Steps

- Add ProVerif model to GitHub
- Content-wise we seem mostly converged