Extended Key Update for Transport Layer Security (TLS) 1.3

draft-tschofenig-tls-extended-key-update-02

Hannes Tschofenig , Michael Tüxen , Tirumaleswar Reddy , Steffen Fries , Yaroslav Rosomakho

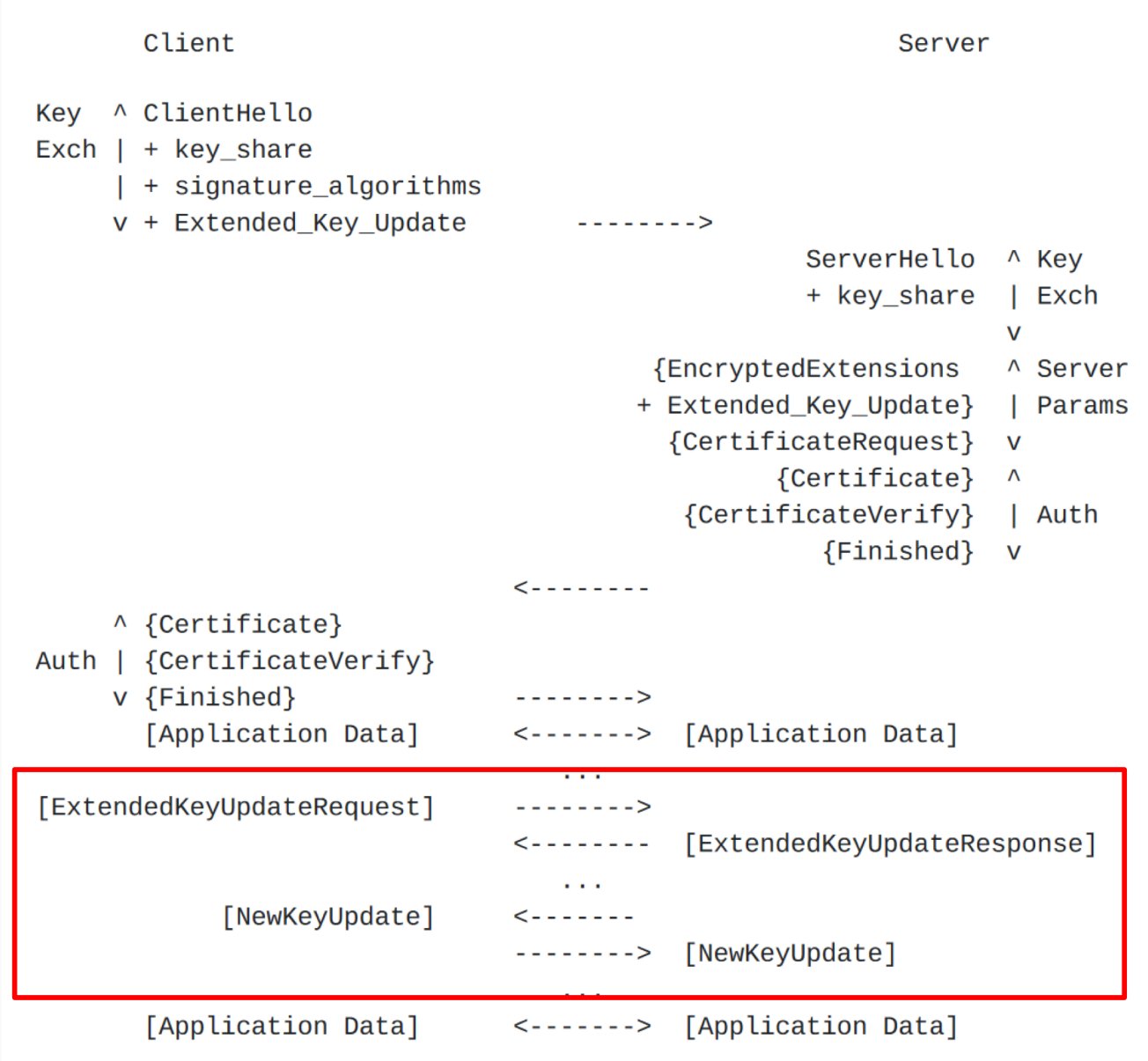
IETF 120 Vancouver
24 July 2024

IETF®

Status

- -02 version with re-design based on feedback from Brisbane meeting
- New design uses:
  - Flags extension to negotiate the feature
  - Message exchange for sharing the key shares
  - Separate exchange to trigger the update of traffic secrets
  - "too_many_extendedkeyupdate_requested" alert

Message Flow



Next Steps

- Call for adoption?

- Additional work ahead of us:
  - Formal analysis
  - Prototyping