Extended Key Update

draft-tschofenig-tls-extended-key-update-01

Hannes Tschofenig, Michael Tüxen, Tirumaleswar Reddy, Steffen Fries
History

• TLS 1.3 redesigned many of the features of earlier TLS versions.
• Features were also removed, such as renegotiation.
• Some features were only partially added back.

• Post-Handshake Authentication Example:
  • RFC 8446 adds post-handshake authentication to allow the server to request authentication of the client.
  • RFC 9261 “Exported Authenticators” adds mutual post-handshake authentication.

• Key-Update Example
  • RFC 8446 adds a key and IV update as a post-handshake message.
Motivation: Long-Lived Connections

• Use cases:
  1. Securing telco signaling traffic
     • Based on design team in TSVWG (IETF#118 meeting presentation)
     • TLS replaces IPsec
     • Requirements
  2. Industrial IoT
     • Example: Power System Automation

• Requires
  • mutual re-authentication (offered by RFC 9261), and
  • key update with forward secrecy.
Design Rational of -01 draft

• Details changed quite significantly from -00 to -01 due to feedback on the list
  • Thanks to Martin Thomson, Ilari Liusvaara, Benjamin Kaduk, Scott Fluhrer, Dennis Jackson, David Benjamin, and Thom Wiggers

1. Follows Key Update design from RFC 8446
   • New message to trigger the update

2. To offer forward secrecy we use HPKE as a KEM
   • One-shot message; a non-interactive KEM
   • Supports DH-KEM and hybrid scheme

3. Follows the design of RFC 9261 “Exported Authenticators”.
   • Application layer protocol exchanges HPKE payload and public keys
Questions to the group

• Is this use case, key update with forward secrecy, relevant?

• Do you have opinions on the solution design?
  • Use of application layer to exchange payloads in the style of Exported Authenticators

• Adopt document as a starting point for future work?