Extended Key Update for TLS 1.3

`draft-ietf-tls-extended-key-update-03`

Hannes Tschofenig

Michael Tüxen

Tirumaleswar Reddy

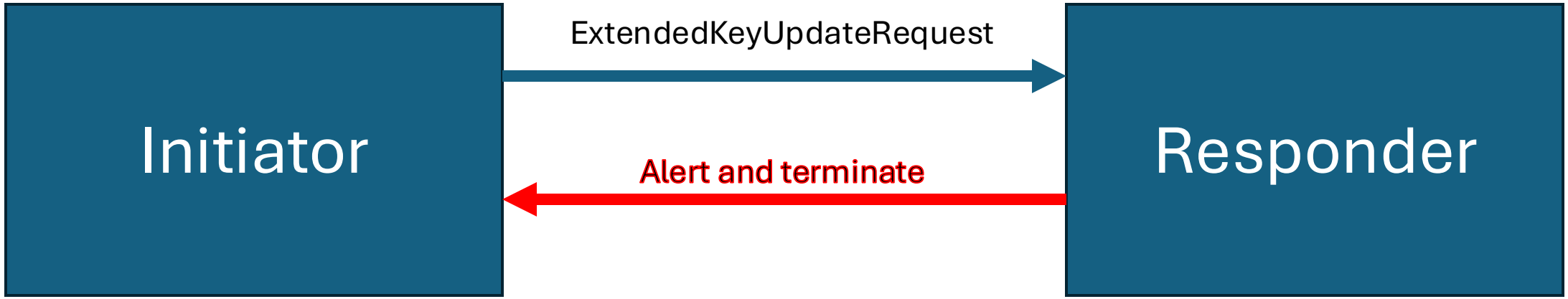
Steffen Fries

Yaroslav Rosomakho*

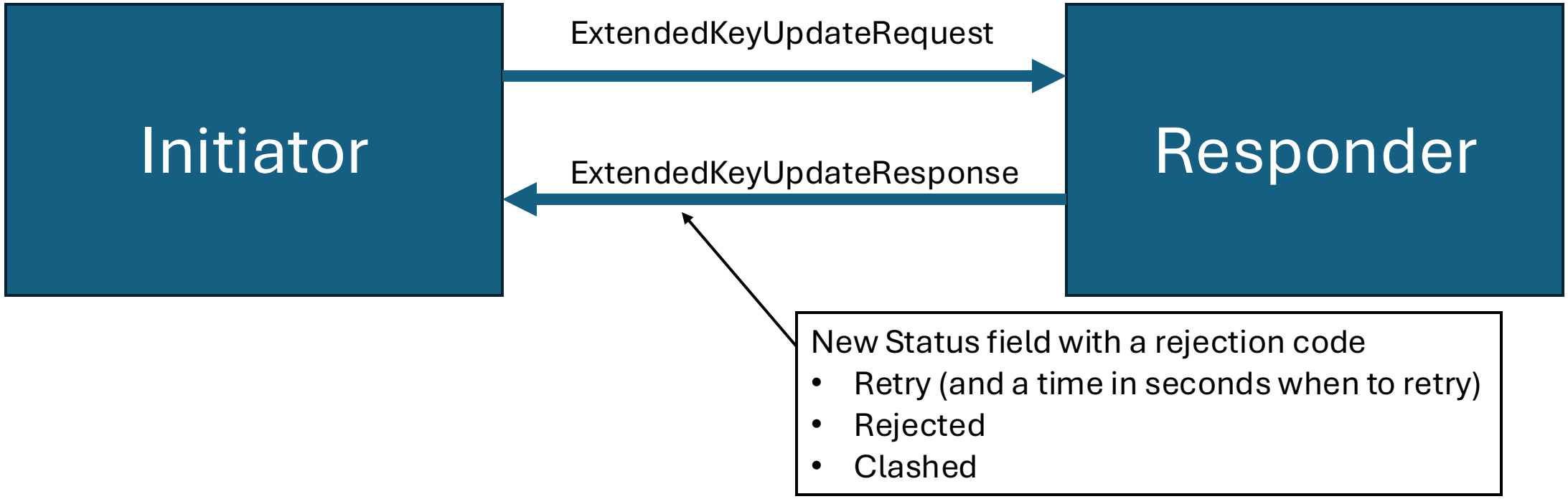
Recap

- Re-introduce ability to perform fresh key exchange in (D)TLS 1.3
- Extended_Key_Update TLS flag to signal capability
- ExtendedKeyUpdateRequest to request re-keying
- ExtendedKeyUpdateResponse to accept
- NewKeyUpdate to confirm that new keys are now used

Rejecting request in the previous draft version…



Rejecting request in the new draft version…



And now initiator gets to decide if it wants to Alert and terminate or to continue.
Or to invoke some application/business logic

SSLKEYLOGFILE update

- CLIENT_TRAFFIC_SECRET_N+1
- SERVER_TRAFFIC_SECRET_N+1

Natural continuation of currently used CLIENT_TRAFFIC_SECRET_0 and SERVER_TRAFFIC_SECRET_0

Exporter considerations

Exporters need to use newly derived key to generate Exported Keying Material

Thank you!

- Is this ready for next steps?