TLS PAKE

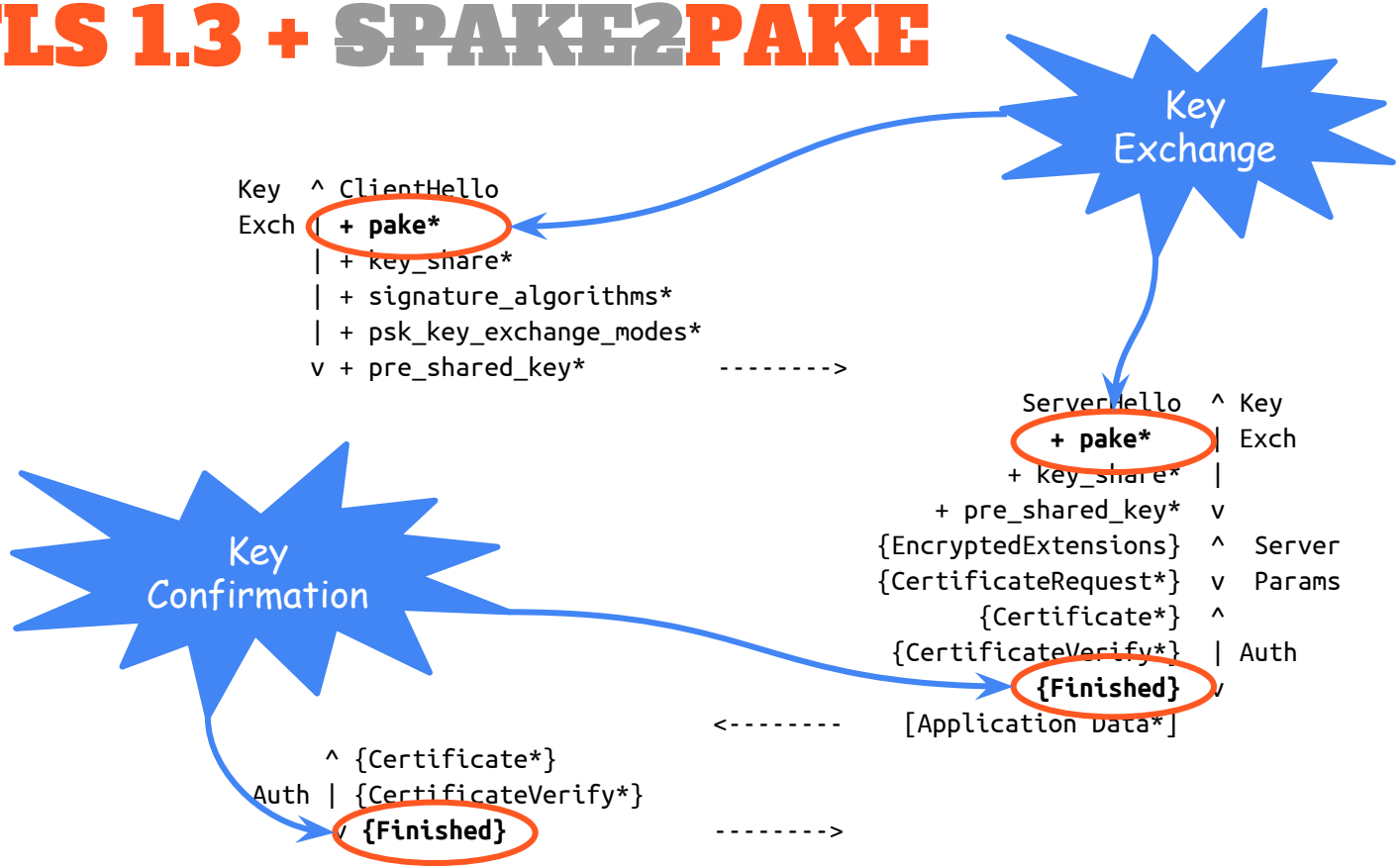
Sometimes you only have a (low-entropy) password

With TLS <1.3, could use SRP ciphersuites [RFC5054]
… but SRP suites don't translate directly 1.3
… and there's been some more work on PAKEs since SRP
… for example, draft-irtf-cfrg-spake2, draft-krawczyk-cfrg-opaque

Proposal: Add an extension to enable TLS 1.3 to enable use of PAKEs for key exchange and mutual authentication

https://datatracker.ietf.org/doc/draft-barnes-tls-pake/

TLS 1.3 + ~~SPAKE2~~PAKE



Since last time...

Interest in other PAKEs: Dragonfly, OPAQUE, ...

Changed to be a general framework for any PAKE with the right shape

- ClientHello/ServerHello extension + Key schedule integration
- Per-PAKE definition of messages carried in CH/SH

Open questions:

- Identity protection?
- Need to negotiate PAKEs?