**TLS PAKE**

Sometimes you only have a (low-entropy) password

With TLS <1.3, could use SRP ciphersuites [RFC5054]

... but SRP doesn’t map well to 1.3

... and there’s been some more work on PAKEs since SRP

... for example, [draft-irtf-cfrg-spake2]

Proposal: Add an extension to enable TLS 1.3 to use SPAKE2 for key exchange and mutual authentication

https://github.com/bifurcation/tls-pake/blob/master/draft-barnes-tls-pake.md
TLS 1.3 + SPAKE2?

Key Exchange

ClientHello
+ spake2*
| + key_share*
| + signature_algorithms*
| + psk_key_exchange_modes*
\v + pre_shared_key* -------->
ServerHello
^ Key
+ spake2*
| Exch
+ key_share*
+ pre_shared_key*
\v {EncryptedExtensions} ^ Server
{CertificateRequest*} v Params
{Certificate*} ^
{CertificateVerify*} | Auth
\v {Finished} <--------

Application Data*

Key Confirmation

^ {Certificate*}
Auth | {CertificateVerify*}
\v {Finished} -------->

^ {Certificate*}
\v {Finished}