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?