Protocols to consider

There are a number of PAKE protocols out there none of them is used widely in the industry and they are very different in scope and mechanics. Studying all of them is not possible within the resources available and it is best to focus on schemes that are most likely to be needed by users.

Wide deployment

Considering PAKE schemes with already wide deployment allows users with existing applications to migrate to PSA. Currently there is only one scheme with non-negligible success in the industry: SRP - Secure Remote Password

Requests

Some PAKE schemes have been requested by the community and need to be supported. These are at the time of writing SPAKE2+ and (EC)J-PAKE.

Standardisation

There are PAKE schemes that are being standardised and will be recommended for use in future protocols. If we want the API be future proof, we need to consider these. Recommended by the CFRG for use in IETF protocols are CPace and OPAQUE. These are recommended for use in TLS and IKE in the future.

Out of scope

PAKE protocols not fitting into any of the above categories won't be studied and considered when designing the API. Some schemes like that are: AMP (IEEE 1363.2, ISO/IEC 11770-4), BSPEKE2 (IEEE 1363.2), PAKZ (IEEE 1363.2), PPK (IEEE 1363.2), SPEKE (IEEE 1363.2), WSPEKE (IEEE 1363.2), SPEKE (IEEE 1363.2), PAK (IEEE 1363.2, X.1035, RFC 5683), EAP-PWD (RFC 5931), EAP-EKE (RFC 6124), IKE-PSK (RFC 6617), PACE for IKEv2 (RFC 6631), AugPAKE for IKEv2 (RFC 6628), PAR (IEEE 1363.2), SESPAKE (RFC 8133), ITU-T (X.1035), SPAKE1, Dragonfly, B-SPEKE, PKEX, EKE, Augmented-EKE, PAK-X, PAKE

(The exception is SPAKE2, because of it is related to SPAKE2+. It also makes the number of balanced and augmented PAKEs in the list equal.)

Applications

Some of these schemes are used in popular protocols. This information further justifies choices already made and might help extending the list at some later point:

- EC-JPAKE: TLS, THREAD v1.1
- SPAKE2+: CHIP
- SRP: TLS

- OPAQUE: TLS, IKE
- CPace: TLS, IKE
- Dragonfly: WPA3 (Before including the Dragonblood attack should be considered as well.)
- SPAKE: Kerberos 5 v1.17
- PACE: IKEv2
- AugPAKE: IKEv2

PAKE List

List of PAKEs to be considered:

Balanced

- ECJPAKE
- SPAKE2
- CPace

Augmented

- SRP
- SPAKE2+
- OPAQUE