Requirements for PAKE schemes

draft-irtf-cfrg-pake-reqs

Why PAKEs?

Possibilities:

- Print (easy to enter) passwords on small devices
- Passwords for initial authentication
- Derive / recover long-term keys
- Use passwords in lieu with certificates

The Target - Why an RFC?

- Add structure to the PAKE discussion
  - Prevent discussing the same points each time a PAKE is suggested
- Agreeing on common requirements
- Guideline for (drafts on) PAKE schemes
- Increase comparability

What’s in it?

- Taxonomy
- Applications
- Security
- Implementation issues

→ Resulting in a list of requirements

Requirements - Design

- A PAKE scheme MUST clearly state its features regarding balanced/augmented versions.
- A PAKE scheme SHOULD come with a security proof and clearly state its assumptions and models.
- The authors of a scheme MAY discuss variations of their scheme that allows the use in special application scenarios.
- The authors MUST declare the status of their scheme with respect to patents.

Requirements - Implementations

- It SHOULD be possible to implement the PAKE scheme in constant time.
- The authors MAY show how to protect an implementation of their PAKE scheme in hostile environments.
- In case the PAKE scheme is intended to be used with ECC, the authors SHOULD discuss their requirements for a potential mapping or define a mapping to be used with the scheme.
- A PAKE scheme MAY discuss its design choice with regard to performance, i.e., its optimization goals.

Status

- First draft submitted
- Should serve as starting point

Comments / feedback / suggestions are very welcome!