EAP-SKE: Shared Key Exchange

- Justification: provides mutual authentication and Master Key derivation in only 1 RTT between F-AAA and H-AAA. Ideal for roaming clients. It is **simple**.
- Usage scenario: designed for roaming clients in Wireless and 802.1x LANs, can be used anywhere EAP is supported
- EAP type: not requested yet (20 suggested)
- Mutual authentication
- Fast reconnect: not in the current draft.
- Dictionary attacks: no (as susceptible as HMAC-MD5)
- Key derivation: yes (Master Key), PRF = HMAC-MD5
- Algorithms: HMAC-MD5 based. Can use any existing proven mechanism that uses HMAC-MD5 to derive Master Key from a sufficiently long Shared Key + randoms
- Std. group dependencies: none