EAP Multiple Pre-Shared Keys (EAP-MPSK) Method

draft-yan-emu-eap-multiple-psk-00

IETF 119, Mar. 2024

Lei YAN
ray.yanlei@huawei.com

Problem

- The existing PSK-based EAP methods assumed that only one PSK had been configured on a pair of EAP peer and server.
  > EAP-GPSK [RFC5433]
  > EAP-PSK [RFC4764]
  > EAP-SAKE [RFC4763]
  > EAP-PAX [RFC4746]
- Using a single PSK does not provide perfect forward secrecy [RFC5433]
- Compromise of the PSK leads to
  > compromise of recorded past sessions
  > impersonating the peer and server
  > compromise future sessions

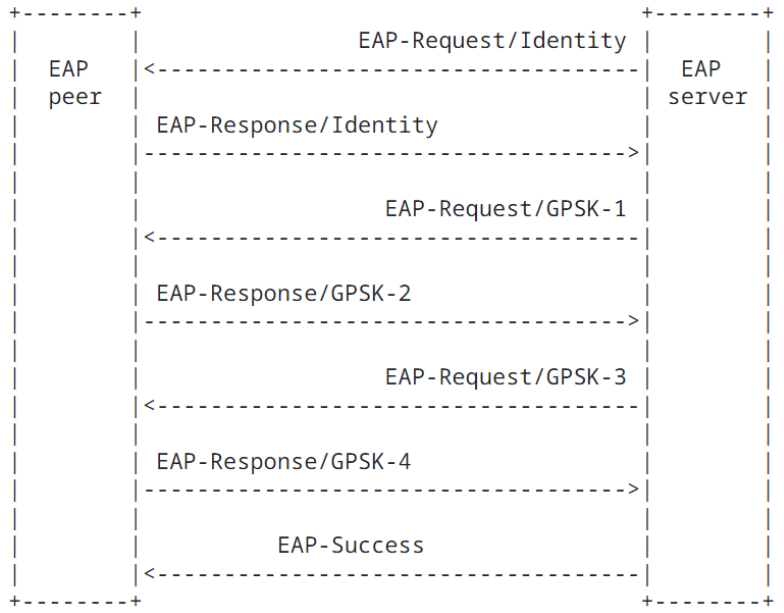


Figure 1: EAP-GPSK: Successful Exchange

The full EAP-GPSK protocol is as follows:

GPSK-1:

ID_Server, RAND_Server, CSuite_List

GPSK-2:

SEC_SK(ID_Peer, ID_Server, RAND_Peer, RAND_Server, CSuite_List, CSuite_Sel, [ENC_PK(PD_Payload_Block)])

GPSK-3:

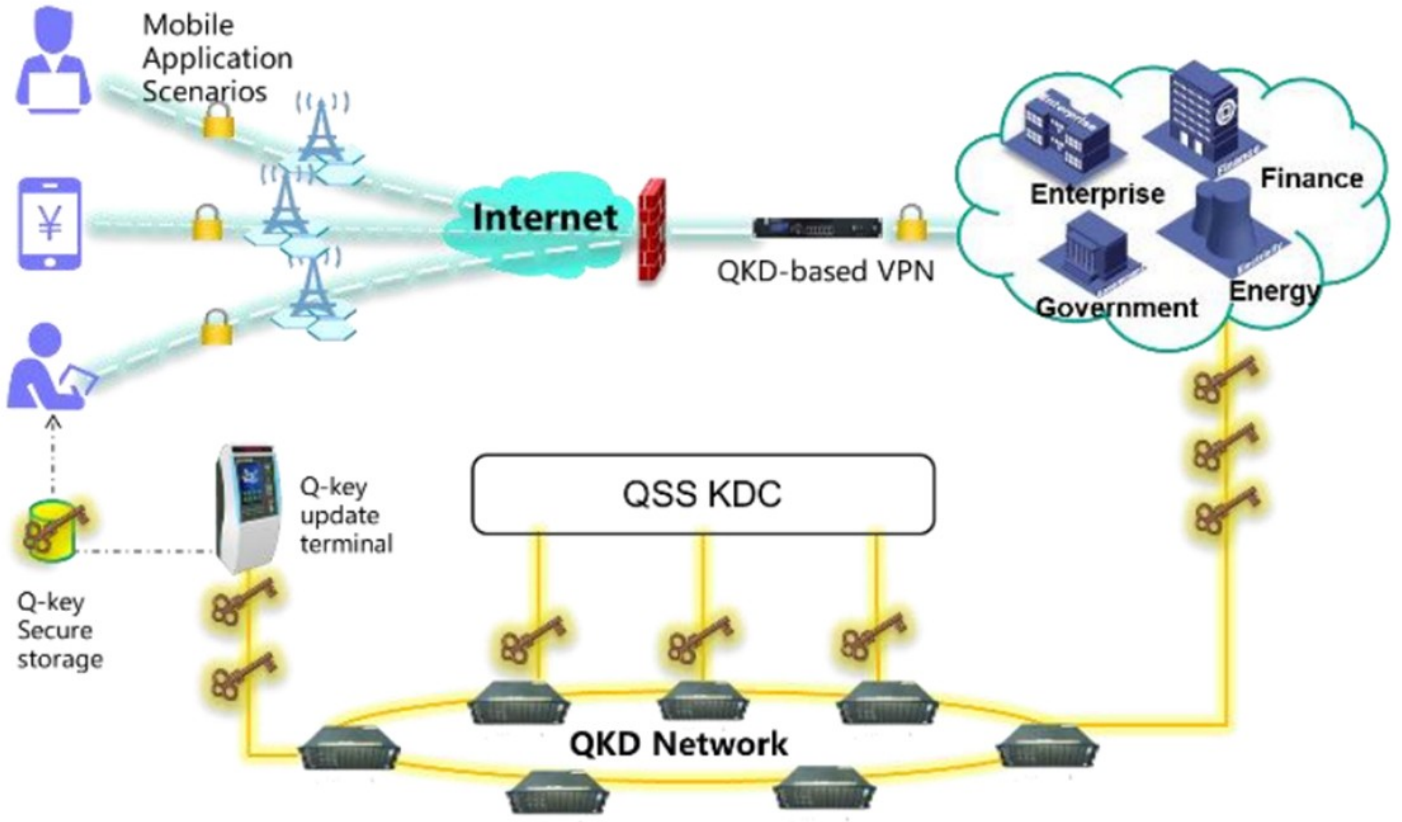
SEC_SK(RAND_Peer, RAND_Server, ID_Server, CSuite_Sel, [ENC_PK(PD_Payload_Block)])

GPSK-4:

SEC_SK([ENC_PK(PD_Payload_Block)])

Using multiple PSKs is one solution

- Traditional manual configuration of PSKs
  > lacks automation
  > less efficient
- Quantum keys generated by a quantum network[1]
  > automatically obtained through a network
  > offline implanted for mobile devices
  > easy to get plenty of PSKs
- Using each PSK only once
  > perfect forward secrecy
  > compromising a used PSK cannot
    - impersonate the peer and server
    - influence future sessions



[1] ITU-T FG QIT4N D2.2 Quantum information technology for networks use cases: Quantum key distribution network

Existing works related to multiple PSKs

- Existing works supporting the negotiation among multiple PSKs
  > TLS [RFC 8446]
  > IPSec [RFC 8784, draft-smyslov-ipsecme-ikev2-qr-alt-09]
- Existing methods of storing and transferring PSKs
  > RFC 6030
  > RFC 6031

Key Management Issue: PSK identity collisions

- Different PSK configuration manners:
  > traditional manual configuration
  > obtained through quantum key generators
- Lack of a unified plan for PSK IDs
  > in different configuration methods
  > even among different quantum key generators
- Two PSK identities may clash
- Multiple PSKs should be managed by category
  > classified by the key producer

Future work

- We plan to modify the EAP-GPSK to support the negotiation of a PSK among multiple PSKs.
- The details of the negotiation needs to be discussed.
- It can be negotiated by
  > a key list, such as TLS [RFC 8446]
  > a key ID, such as IPSec [RFC 8784]

Thank you!

Questions?

Anyone interested to collaborate on the draft ?