802.1X MKA PSKs [1] — out-of-band key distribution

Follow up to "Integrating Quantum Key Distribution with IEEE 802.1X"
https://www.ieee802.org/1/files/public/docs2022/new-talwar-qkd-1x-integration-1022-v00.pdf,
"802.1X CKNs and KMDs"
https://www.ieee802.org/1/files/public/docs2022/x-seaman-ckns-kmds-1022-v0.pdf,
and 802.1 Security TG discussion 2022-11-01.

Mick Seaman
mickseaman@gmail.com

[1] MKA: MACsec Key Agreement. PSKs: Pre-shared Keys, sometimes referred to as PPKs (Pre-placed Keys). 802.1X uses 'PSK' to refer to any CAK supplied 'out-of-band' , i.e. not a result of PAE (Port Access Entity) mutual authentication protocol with an intended peer. Proof of current possession of the symmetric CAK (Connectivity Association Key) [demonstrated by protecting an MKPDU with an ICV (Integrity Check Value) calculated using AES-CMAC and a key (ICK) derived from the CAK] provides proof of prior authentication to peers possessing the same CAK.

Agenda

- Context—Why this presentation
- CAK/PSK distribution
- CAK/PSK standardization options
- Out-of-band SAK distribution?

Context

- Interest in additional ways of providing a CAK/PSK
  - Not just ‘mechanical’ entry to a device by network administrator or delegate (console keyboard, USB stick etc). [1]
  - One, but not the only possible, case is use of QKD (Quantum Key Distribution), over separate fiber from subsequent MKA and MACsec protected communication).
  - ETSI group has specified an API for key retrieval from a QKD Server.
- Possible interest in out-of-band SAK [2] distribution
  - MKA Key Server (currently) distributes each SAK using AES Key Wrap in MKPDUs. Distribution tied to the MKA Live Peer List. [3]
- Question: what (if anything) needs to be standardized, and by whom?

[1] While this is a common mental model for PSKs, a PSK is simply a CAK that is provided by means outside of the scope of 802.1X. Such a

[2] SAK: Secure Association Key. One, or a succession of, SAK(s) is used (by MACsec with a standardized GCM or alternate CipherSuite) to protect the data. Distribution frequency significantly reduced for XPN (Extended Packet Number) CiperSuites. Not clear if there is an out-of-band distribution requirement: some discussion in the 2022-11-01 Security TG meeting (rapid key refresh, distribution of a number of keys in advance of their subsequent use) more relevant to SAKs rather than CAKs.

[3] 802.1X takes considerable care to avoid SAK/nonce reuse by GCM. This may be challenging for out-of-band distribution.

CAK/PSK distribution

- MKPDU recipient identifies CAK using CKN, can use with KMD [1] (if present).
- CKN assigned by convention, depending on authentication method:
  - — Separately derived from MSK material when EAP is used
  - — Administratively assigned (arbitrary) for a mechanically entered PSK
- Distribution considerations:
  - — Possession implies mutually authentication of parties. Third-party distribution requires transitive trust.
  - — CKN assignment/generation and KMD use conventions may need to be specified for each use method.
  - — Reuse (nonce requirement) not an issue. Lifetime/revocation required.

[1] CKN: CAK Name (up to 32 octets), used by the MKPDU recipient to select the CAK used to validate the MKPDU. Transmitted in clear, it must not be possible to determine the CAK algorithmically from the CKN. KMD: Key Management Domain advertizes scope of the CKN and (in a prior Announcement) scope of the acceptable {CAK, CKN} tuples. The KMD can thus advertize a network identity, a set of network access points with common access to stored CAKs, the MKPDU transmitter's identity (so that the recipient can retrieve the CAK from the appropriate store), or part of the recipient's CAK store (that the transmitter believes was associated with the CAK when first assigned).

CAK/PSK standardization options

Alternatives:

1. *802.1 Lite*. No new information elements/code points are needed, other standards organization can already specify use in their field of application. [1] Liaison desirable.
2. *802.1 Clarification*. Add 802.1X Informative Annex, describing the 'Lite' approach. Use examples possible (with liaison). New elements/code points only if strictly necessary. [2]
3. *802.1X QKD Support*. Full normative specification in the ETSI QKD key exchange/server use case, and potentially others. [3]

[1] Where needed for multi-vendor interoperability, not needed for direct configuration of CAKs in each of the communicating systems.

[2] Hopefully a quick simple project. Need contribution before PAR to confirm scope.

[3] Potentially difficult, if in the end rewarding. Need significant interest/active participation for each use case. Responsibility for validating complete solution (restriction of each key to mutually authenticated parties even if common resources for distribution) and security benefits/characteristics (potential non-reliance on assymetric crypto, but how is mutual auth/reauth with potential revocation and resumption supported). Liaison and potential copyright issues, even in initial stages, if elements of solution split across standards organizations. Initial liaison from ETSI could help (for all alternatives). Final ballot pool will be tough and inquisitive (as it should be).

Out-of-band SAK distribution? [1]

- Must avoid accidental SAK PN reuse. [2]
- SAKs must be tied to current authentication. [3]
- SAKs currently tied to CAK, MI, and Live Peer List. [4]

Suggestions: [5]

— Cannot rely on non-integrated key storage one-time retrieval.

— Could add MKA parameter SKN (SAK Key Name) comprising Key Server MI and Live Peer List with (possibly) a free format name for out-of-band key storage retrieval. [6]

[1] No substantive proposal to date (a.f.a.i.k) but as noted above (Slide 3) some discussion seemed more relevant to SAK distribution. Currently SAKs only distributed by MKPDU using AES Key Wrap.

[2] While nonce reuse resistant Cipher Suites are available there is a performance impact, and cipher over cipher can be less work, as well as protecting against other implementation errors. Reuse prevention more challenging where a physically separate key store is being used.

[3] ‘Code book’ distribution in advance of authentication/reauthentication either not possible or requires access constraint enforcement.

[4] The CAK changes on reauthentication, the SAKs KI (Key Identifer) comprises the Key Server’s MI (Member Identifier, 96 bits) and a KN (Key Number) allocated sequentially by the Key Server [which is one of the participants in the secure (protected by MACsec) CA (Connectivity Association)]. A participant’s MI changes whenever that participant loses memory of prior SAK use, an SAK is only used if the participant appears in the Live Peer List, and a Key Server does not distribute any given SAK in MKPDUs with different Live Peer Lists.

[5] Only if there is serious interest in and benefit to out-of-band SAK distribution:

[6] QKD cannot support Group CAs directly.