802.1X CKNs and KMDs

Basic properties and use

Mick Seaman
mickseaman@gmail.com

CKN

CAK Name - identifies a CAK:[1]

- Allows recipient of an MKPDU to determine which CAK to use to validate the received MKPDU.
- Transmitted in clear, must not be possible to use to CAK
- Value determine by convention, depending on authentication method:
  - Separately derive from MSK material when EAP is used
  - Arbitrarily assigned by administrator when PSK is used

1. The ability to generate a valid MKPDU, protected by a CAK and including a nonce provided by a peer, serves as proof of current possession of the CAK. Current possession of a CAK is proof of prior authentication.

KMD

Key Management Domain - identifies a scope within which CAK/CKN tuple are (likely to be valid) and can be cached:

- May be implicit (if CAKs arise out of authentication over the link to be protected) and will only be used in that context
- Can support roaming of a station between some group of peers that have means (not specified in the standard) of sharing the CAK
- Names a pool of CAKs—scope of CKN, where to look for CKN