Physical Access Control with New Authentication Mechanisms

Ketan Mehta, NIST

Slides by David Cooper

March 3, 2015

Changes Since SP 800-116

- CHUID authentication mechanism has been deprecated in FIPS 201-2, and is expected to be removed in next revision.
- Asymmetric Card Authentication key (CAK) has been made mandatory
- Secure messaging (SM) and on-card biometric comparison (OCC) are new, optional card capabilities.

Authentication for Physical Access

Assurance Level	Authentication Mechanism
LITTLE or NO confidence	VIS, CHUID
SOME confidence	PKI-CAK, SYM-CAK, SM-AUTH
HIGH confidence	BIO
VERY HIGH confidence	Two factor: BIO-A, PKI-AUTH, OCC-AUTH, SM-AUTH + PIN Three factor: PKI-CAK + BIO, SYM-CAK + BIO, SM-AUTH + BIO

- Green – based on mandatory card features
- Underlined – based on new, optional card features

PKI-CAK

- PKI authentication using Card Authentication key
- Works over contactless interface
- Only authentication mechanism that
  - Uses only mandatory features of card
  - Provides fast one-factor authentication
  - Provides at least SOME authentication assurance

SM-AUTH

- Authentication via secure
  - Key confirmation step of key-establishment protocol authenticates card
- Works over contactless interface
- Provides SOME authentication assurance
- Requires support for new, optional card feature
- Building block for stronger authentication mechanisms (e.g., OCC-AUTH)

PKI-CAK vs. SM-AUTH

- Each involves a single asymmetric cryptographic operation
  - RSA or ECDSA signature for PKI-CAK
  - ECC CDH for SM-AUTH
- PKI-CAK includes revocation checking, SM-AUTH does not
- For pre-registered cards, performance of SM-AUTH and optimized PKI-CAK should be about the same.

OCC-AUTH

- On-card biometric comparison over secure messaging (SM-AUTH + OCC)
- SM-AUTH provides “something you have”
- OCC provides “something you are”
  - OCC without SM provides card activation, but no authentication
- SM-AUTH + PIN also provides two-factor authentication

SM-AUTH + BIO

- Off-card biometric comparison over secure messaging
- Comparable to CAK + BIO in SP 800-116
- Authenticates card, PIN, and biometric
- Comparable to OCC-AUTH + (SM-AUTH + PIN)