The Next Generation (SP 800-73-4) PIV Card and the Purpose of the Pairing Code in the Wireless Environment

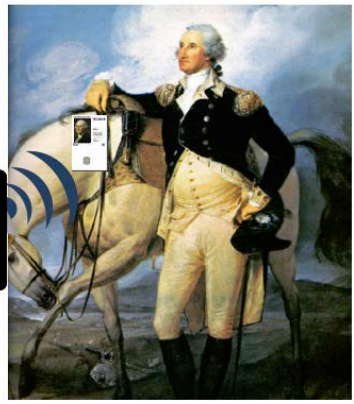
David Cooper
NIST
June 11, 2014

Background

- HSPD-12 includes a mandate to “protect personal privacy.”
- FIPS 201 includes a mandate to “Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of PII.”
- Based on these mandates, current PIV Cards impose strict limitations on the data that can be read over the contactless interface.
  - The only identifiers that may be read over the contactless interface are credential identifiers (Federal Agency Smart Credential Number (FASC-N) and Universally Unique IDentifier (UUID)), which are numbers that are unique to each PIV Card, but that do not identify the cardholder.
- Most data objects may only be read over the contact interface, and access to some of these data objects is PIN protected for additional privacy protection.

FIPS 201-2

- FIPS 201-2 introduces a *virtual contact interface* (VCI), and will allow all data objects to be read over the contactless interface if a VCI has been established.
- Technical specifications for VCI are under development
- The VCI will require the use of encryption, which will protect against passive eavesdropping but not skimming.[1]
- Portable skimmers can read data from cards from up to 25cm away:
  - How to Build a Low-Cost, Extended-Range RFID Skimmer, Ilan Kirschenbaum and Avishai Wool, Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15. Vancouver, B.C., Canada.



[1] **skimming**: Surreptitiously obtaining data from a contactless smart card, using a hidden reader that powers, commands, and reads from the card.

Portable Skimming Device

RFID Hacking – Live Free or RFID Hard
DEF CON 21 – August 3, 2013
http://www.youtube.com/watch?v=6VaG1mwoukQ

Virtual Contact Interface Requirements

- The X.509 certificates on PIV Cards (other than Card Authentication) contain data that has previously been considered to be PII. Examples include cardholder's name, email address, and country of citizenship.
- Currently these certificates may only be read over the contact interface
  - The original specification for PIV Cards, SP 800-73, PIN-protected access to these certificates for privacy reasons.
  - The certificates were subsequently made available for free-read over contact interface when it was discovered that some important applications (e.g., smart card login) would not work if the certificates were PIN protected.
- Revised Draft SP 800-73-4 proposes that establishment of the VCI require submission of a pairing code from the reader to the card.
  - Protects against skimming, since a skimming device wouldn’t know the pairing code.

What is the Pairing Code

- 8-digit value randomly generated by issuer
- May be permanently cached by readers
  - Cardholder provides pairing code to reader (e.g., mobile device) one time and afterwards establishment of VCI can be transparent to the user.
- Can be read from card (over contact interface) and may be printed on the back of the card
  - Cardholders don’t have to memorize the pairing code’s value.
- Does not lock as a result of incorrect guesses
  - No need to establish a mechanism for resetting pairing codes.
  - Length of pairing code makes brute-force attacks infeasible.

Virtual Contact Interface Requirements

- Some commenters have requested that the pairing code be made optional.
  - All cards would protect certificate data from passive eavesdroppers.
  - Cards that require a pairing code would prevent skimmers from reading certificates (with name, email address, etc.) from the card.
  - Cards that don't require a pairing code would allow skimmers to read certificates (with name, email address, etc.) from the card.
- Should SP 800-73-4:
  a) Always require a pairing code to establish a VCI (in order to protect against skimming)?
  b) Allow individual departments and agencies to decide whether the PIV Cards they issue will require a pairing code to establish a VCI?