NIST Special Publication 800-96 PIV Card to Reader Interoperability Guidelines

Hildegard Ferraiolo
PIV Program Lead
National Institute of Standards and Technology
March 3, 2015
FIPS 201-2 Associated Special Publication's Workshop

Purpose of SP 800-96

- Recommendations for PIV card readers in the area of:
  - **performance,** communications and
  - enhanced interoperability between any card and any reader.

Revising SP 800-96 to Improve PACS Transaction Time

Transaction Time:

- SP 800-96 specifies transmission speeds of fc/128 (~106 kbits), fc/64 (~212 kbits/s) and fc/32 (~424 kbits/s)

Rev Option: Shall Rev 1 of SP 800-96 drop fc/128 (~106 kbits) to improve speed?

Revising SP 800-96 to Improve PACS Transaction Time

Extended Length APDU:

- PIV Card currently limited to 256 byte blocks of data
- Extended Length APDU can read 65 536 byte data blocks

Consideration:

- No speed improvement for PKI (CAK) authentication if FASC-N is read and X.509 is cached.
- Substantial reader upgrade to discover and process extended length cards

Revision of SP 800-96 to Improve PACS Transaction Time

- Other considerations:
  - Add reference to EMV to improve speed
  - Add requirement for a strong RF field
  - Require powerful (fast) processors for both card and PACS components

Revising of SP 800-96 to Improve PACS Transaction Time

More considerations:

- Require a 1.5 second limit for transaction (from presentation of card to green light to opening the door

- **Question to Panel: Is 1.5 seconds possible and what would have to change?**

- **Note: Recent measures of 3.5 to 4 second reflect current reader setup, logic, technologies, its infrastructure and current cards. Is 1.5 seconds possible with next generation of cards and optimization to reader and PACS component?**

Thank you!

Questions?

Hildegard Ferraiolo
PIV Project Lead
NIST ITL Computer Security Division
hildegard.ferraiolo@nist.gov