PACS
Reader Infrastructure Enhancements

SP 800-96
PIV Card to Reader Interoperability Guidelines

Steve Rogers
President
IQ Devices

FIPS 201-2 Associated Special Publication's Workshop
March 3, 2015

Presented by:

IQ Devices

PIV Cards & Readers

- The PIV card is a microprocessor smart card with a 13.56Mhz radio.
- PIV limited PACS read range only a reader related issue = **FALSE**
- Read range is a combination of both cards and readers = **TRUE**
- External factors also play a role = **TRUE**
- Key four parties involved in this combination that can make the transaction a success or failure.
  - Reader manufacturers (party A)
  - Card manufacturers (party B)
  - System installers (party C)
  - System end-users (part D)

Presented by:

IQ Devices

Power Transfer / Card Performance
from POST meeting Nov2014

- Contactless card is powered by the reader's magnetic field.
- Cards manage power by adjustments to clock rates and subsystems, affecting comms and crypto accelerators.
- All PIV cards in FedGov use asymmetric crypto w/ accelerators.
- Crypto acceleration for RSA and ECC is power hungry.
- Insufficient power transfer from reader to card likely:
  - ✓ Limit communications rate options
  - ✓ Slows critical crypto.
- Readers and cards must be tuned to work well together.

Presented by:

IQ Devices

ISO 14443
Reader Principals

- **Reader output power** -The relation between output power and reading distance is non-linear:
  - ✓ Double the read distance requires ~ 8X increase in the readers' output power.
    - ø maximum allowed limits
    - ø physically achievable limits

- **Reader receiving sensitivity** - card may receive enough power to operate at certain distance… however not enough card data signal left for reader to detect

- **The larger the reader output power** - the more difficult it is to detect the small data return signal of the card, due to the large reader generated RF field.

Presented by:

IQ Devices

ISO 14443
Card Principals

- **Card power requirements** - NO requirement for the energy efficiency of the card. Power hungry cards require more power to operate.
- **Card antenna design** - determines card resonance frequency:
  - ✓ influences power efficiency of the card
  - ✓ influences transmission / modulation efficiency of the card.
  - ✓ Strict ISO limits for readers to operate within…
  - ✓ No limits for cards; witnessed card tuning varying from 14 MHz - 24 MHz
- **Card noise** - Some cards so power hungry that power consumption of the card's CPU results in modulating the RF field = invalid data or valid data getting corrupted
- **Communication speed** - Higher communication speeds result in smaller reading distances. Demonstrated lowest speed 106 kbps achieves best distance.

Presented by:

IQ Devices

ISO 14443 Combined Reader & Card Principles

- **Coupling factor between card and reader** – determines efficiency between the card and the reader:
  - ✓ varies from reader manufacturer to card manufacturer
  - ✓ varies between the same card and different readers
  - ✓ varies between the same reader and different cards

- **Conducting surfaces or metal in surroundings** – absorb /reduce /short-circuit the amount of transmitted RF power.

- **External RF noise sources** – at the same or close to the same frequency as the reader will deafen the reader for card data:
  - ✓ creating a mix product of the two signals that will be detected as false data
  - ✓ the other source is so loud that the card signal can't be detected.

Presented by:

IQ Devices

ISO 14443
Antenna & Use Considerations

- Antenna size has a direct relation on card/reader coupling:
  - ✓ too small is bad
  - ✓ too large isn't good either
  - ✓ minimum = reader antenna same size as transponder antenna
- Parallel geometry provides best card/reader coupling and best results
- Present card quickly with proper orientation and hold - - - -
- Do Not place card against reader, always provide spacing using finger:

i Tuned loop ≅ same resonance frequencies repel like ++ magnets
  - ✓ too close = resonance ƒ peak shifts (one ↑, the other ↓)
    - Poorer power transfer
    - Less sensitive data receiver

Presented by:

IQ Devices

Reader Installation Don’ts

- Conducting surfaces de-tunes the reader antenna circuit:
  - ✓ less power transfer
  - ✓ less data receiving sensitivity.
- 13.56 MHz reader antenna spaced as far as possible from conducting surface, a plastic spacer will reduce the influence of the conducting surface . Avoid steel beams, copper clad…
- Don't make access holes larger than you need and never the same diameter as the reader antenna (e.g. avoid mud rings).
- Do Not Install readers near 13.56MHz radiating sources, examples:
  - ✓ Other 13.56MHz Readers
  - ✓ Baby Wandering Systems
  - ✓ Anti-Shoplifting System

Presented by:

IQ Devices

Reader Installation Do's

- Single cable from one point to point, avoid splices, ≡ hi-power, etc.
- Maintain good connections (solder or proper crimp).
- Keep twisted pairs twisted to the end - no spider web connections.
- Use only manufacturer specified power supplies, never under-power.
- If smaller gauge conductors necessary, compensate with higher voltage to avoid loss due to cable resistance. Ohm's Law does apply!
- Use Power Test Card with reader, tune for optimum coupling yields:
  - ✓ best data exchange / reading distance
  - ✓ transmission speed ↑

Presented by:

IQ Devices

Reducing PACS Transaction Time
"The Need For Speed"

Major Factors where high time yields can be obtained:

- Reduction of POST time
- Optimal CHUID layout for FASC-N retrieval (read + parse CHUID to find FASC-N data)
- Optimal Challenge data size (512 nonce = 16 bytes + padding)
- Improve Cryptographic performance (ECC vs RSA)
- Proper Tuning of Cards with Readers
- Proper Installation and Implementation

Presented by:

IQ Devices

Recommendations to Minimize Performance Issues

- **Test card with reader and tune** for optimum coupling yields:
  - ✓ best data exchange / reading distance
  - ✓ transmission speed ↑
- Train and use **proper installation** techniques.
- **End-user training**, at issuance, on proper use and expectations of card and reader
- **Require interoperability testing** like ICAO performed for ePassport , requiring both reader and card manufacturers to conduct tests together (e.g. ISO 10373-6).

Presented by:

IQ Devices

Additional Information

FIPS 201 PIV II Card Use with Physical Access Control Systems: Recommendations to Optimize Transaction Time and User Experience

Smart Card Alliance

Access Council White Paper

May 2007

www.smartcardalliance.org

Presented by:

IQ Devices

THANK YOU

Steve Rogers

INID BV
Managing Director

IQ Devices
President

steverogers@iqdevices.com

www.iqdevices.com

+1-831-238-1580

Number 32,
Carmel Valley, CA 93924

Presented by:

IQ Devices