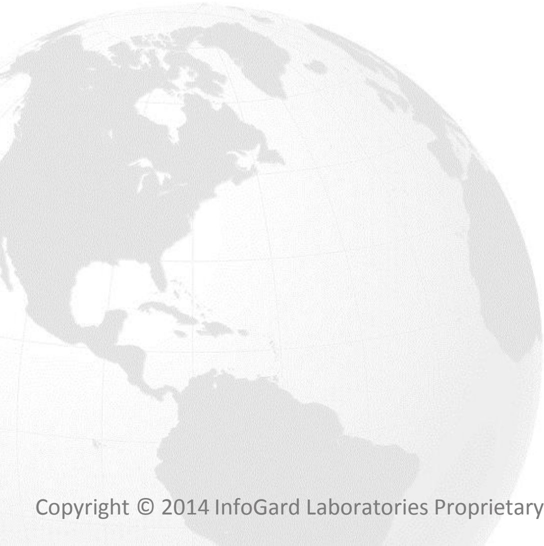
# PIV Performance:

## What about Power Transfer and other factors?

**Steve Weymann**
SWeymann@infogard.com



# Power Transfer Relationship to Card Performance

- In contactless mode, **the 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 cards sold for PIV in the federal space implement asymmetric crypto using crypto accelerators
- **Crypto acceleration for RSA and ECC is power hungry**
- **Insufficient power transfer from reader to card is likely to limit comms rate options and slow critical crypto**
- Also, readers and cards must be tuned to work well together

# Are Readers Providing Enough Power?

- **FIPS 201 specifies maximum operational distance (10 cm)** but not minimum distance, or **any power transfer or tuning characteristics**
- **EMV specifications require operation up to 4 cm from the landing plane**
  - EMV is not PIV … but the technology is the same, and the user experience and acceptance issues are similar
- InfoGard experience in past GSA 201 testing was that operation up to 1 cm was more typical
- **Operational distance should not be a security factor if the system/protocol is well designed**

# Possible Experiment

- Test power transfer for several common readers using ISO 10373-6 / EMV methods (establish a baseline)
  - Possible method: EMV C'less Level 1 PCD Analogue Test Plan (Sect. 7.8.1.1)
- Assure test equipment and sample cards are tuned within tolerance.
- Script the reader transaction for use on a virtual reader.
- Using production PIV cards, vary power produced by the virtual reader. Does power variation affect transaction time?
  - Specialized equipment for contactless low-level testing must be used.
- Another helpful data point: determine power transfer conditions for operation at some lower bound … say 4 cm

# Possible Remedies and Other Considerations

- Deployment should assure readers and cards are well tuned
  - Is that the case for PIV card/physical reader deployment?

http://www.smartcardalliance.org/resources/pdf/PIV_Card_Reader_Guide_102212.pdf

- If experimental results warrant, assure minimum operating distance and/or power transfer
  - **Consider the EMV approach as a model**
  - Operating distance is a function of card and reader
  - Use existing test methods based on ISO 10373-6
- Other performance considerations
  - Reader efficiency in the transaction is likely #1 factor
  - **Next generation chips should be faster when available**
  - **POST improvement may be on the order of several hundred ms**
  - **Move from RSA to ECC has 2x impact (POST + transaction)**