

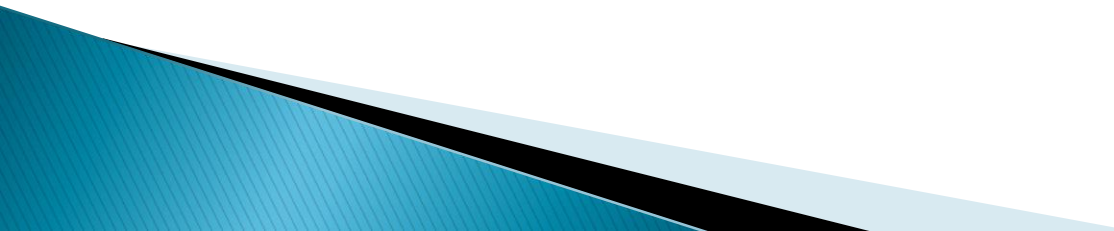
NIST Special Publication Workshop

Interoperability Thoughts & Directions

March 4, 2015



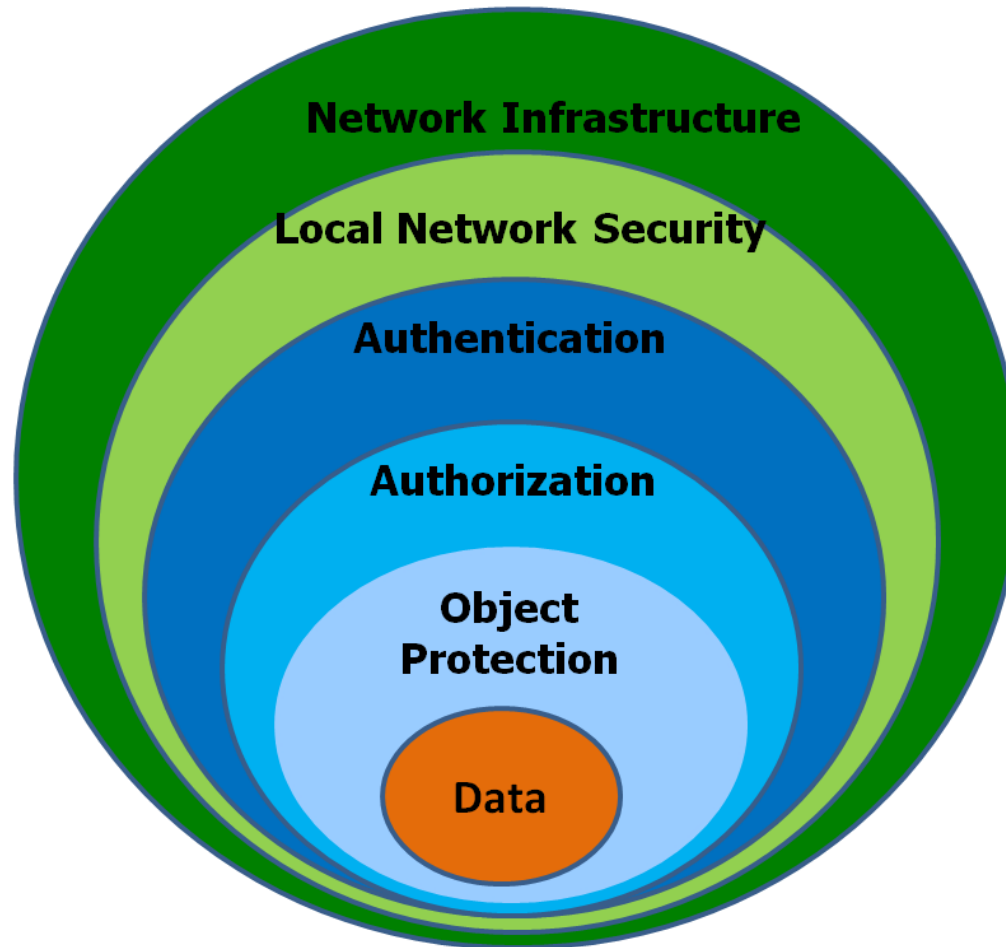
NIST & PIV

- ▶ NIST and Industry have accomplished a great deal in generating FIPS 201 and the multitude of supporting Special Publications, often under incredible time pressures.
 - ▶ We believe that more can be accomplished within the existing specifications and guidelines to improve performance and increase alignment and interoperability with industry and world governments.
- 

Financial Services Security Layers

Security Functions

Intrusion Det. Biometric Compliance Tokens Devices Framework
Firewalls Antivirus Guards
Intrusion Det. Biometric Tokens PIN
Encryption LDAP
Dynamic Encryption



X9.84 X9.112 X9.125 (D)
X9.79, X9.42, X9.44, X9.63, ISO 11568, ISO 21188
X9.8 X9.112 (D) X9.122 (D) ISO 9564
TR-31, TR-39, X9.24, X9.42, X9.44, X9.62, X9.63, X9.69, X9.80, X9.82, X9.92, X9.95, X9.97, X9.98, X9.102, X9.79(D), X9.123(D), X9.124(D)
X9.73, X9.31, X9.62 ISO 16609
X9.119, X9.8, X9.117

**Standards, Standards
Everywhere**

Mapping Security Across
Banking Services:

- Payments Security Trans
- Contracts
- Trusts
- Mobile
- Cloud

The Business of Security:

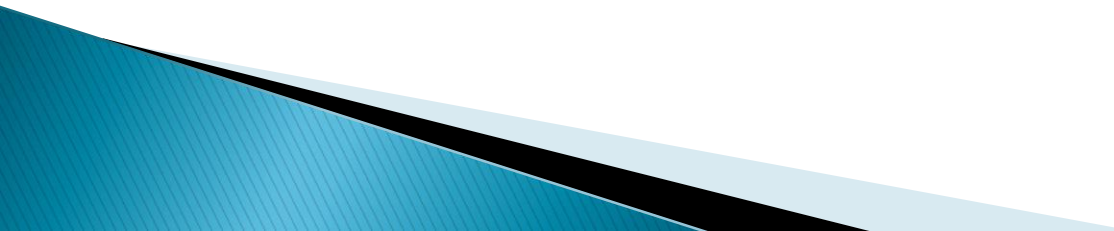
- Regulatory and Legal
- Audit and Contractual
- Risk and Remediation
- Privacy and Laws
- Liability and Obligations
- Contracts

FIPS 201 Contactless

SP 800-96

2.3.5 Type A and B Communication Signal Interfaces

The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.



Initial Development & Differences

Technical Aspect	ISO14443A	ISO14443B	ISO15693	General Comments (For more specific feedback, pls request further info)
Origins	~1990	~1995	~2001	Type B was derived at a much later date than Type A, so has a number of advantages.
Data Rate	106 Kbs	106 up to 847 Kbs	1.65/26.4 kbs	Type B is adaptable to application speed requirements. 14443-3 supports negotiation of higher data-rates with Type B.
Anti-Collision	Medium Binary-search-tree with inefficiencies	Excellent Slotted-ALOHA with dynamic slot adaptation by reader	Excellent Slotted deterministic concept	Type B Slotted ALOHA is the more efficient and sophisticated anti-collision mechanism compared to binary tree search.
Multi-Applications	Yes - Medium	Yes - Fast	Yes - Slow	No clock recovery required with Type B for multi-applications.
Modulation Depth	100% (NO data processing DURING off pulses)	10% (Data processing DURING off pulses)	100% and 10%	100% modulation may offer greater noise immunity for long read-range applications >0.5-1m , but no difference for small read-range applications <.1m.
Air-Interface Complexity	Low (only 100%)	Low (only 10%)	Medium (10% and 100%)	Limited differences in air-interface complexity when using fixed depths of modulation.

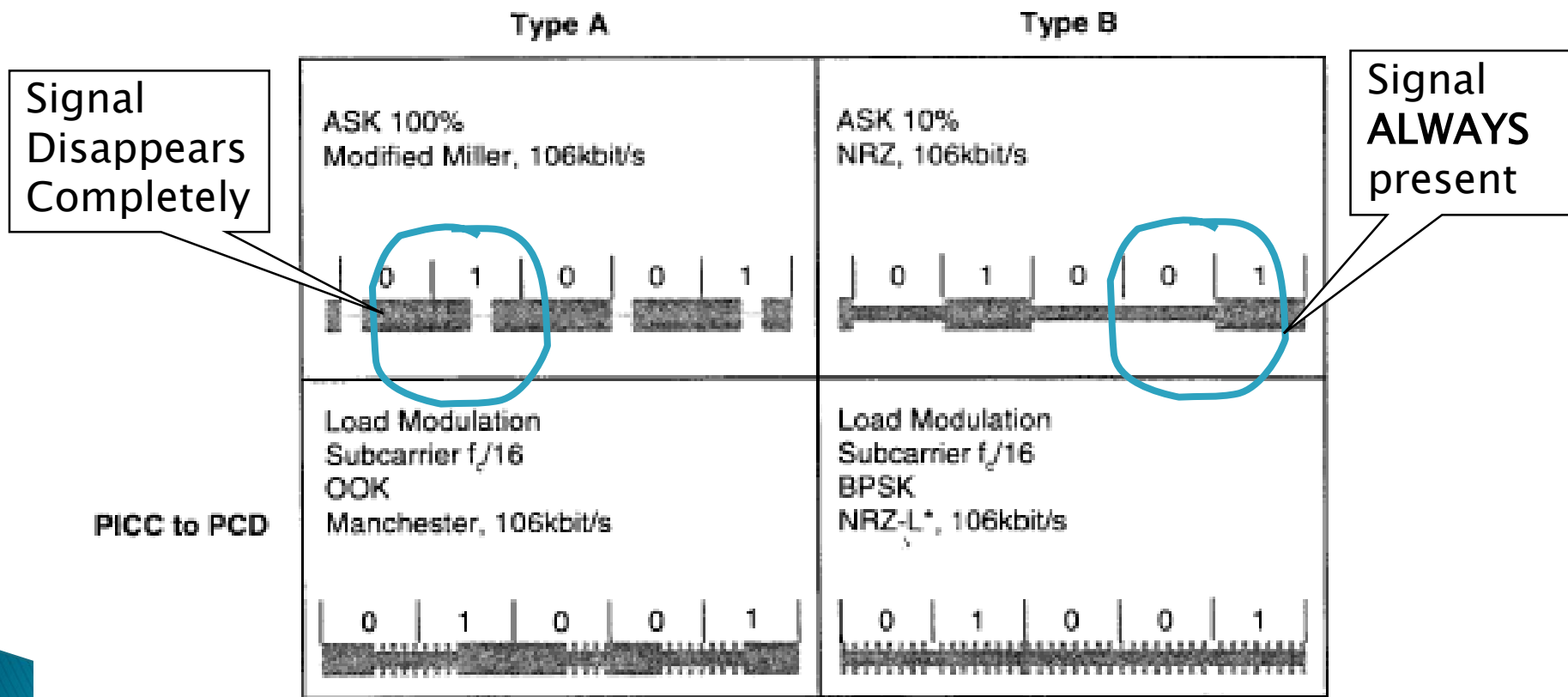
Power Related Issues

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

Operational Differences

- Different Structures
- Different Responses

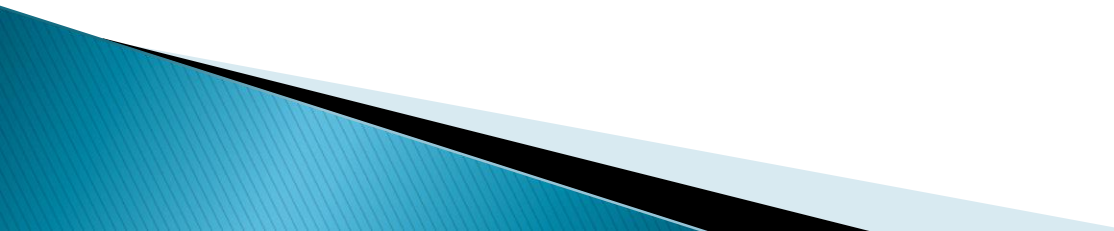


* Inversion of data is also possible

How this might Impact Operation

- ▶ Type A signaling utilizes 100% amplitude modulation of the RF field for communication from the reader to the card with Modified Miller encoded data . Communications from card to reader utilizes OOK modulation of an 847.5 kHz subcarrier with Manchester encoded data. In Type A signaling, the RF field is turned off for short periods of time when the reader is transmitting. The integrated circuit must store enough energy on internal capacitors to continue functioning while the RF field is momentarily off during field modulation.
- ▶ Temporary stopping power can result in:
 - Loss of sync forcing restarts
 - Card entering low power mode:
 - May power down the crypto coprocessor
 - Reduced communications speed
- ▶ Higher Speed means faster validation at entrances...
- ▶ Higher Speed only reliable with B
- ▶ EMV has solved the issue of utilization of both
- ▶ Type B was designed by a group of manufacturers and users for smartcard applications requiring greater security, larger data transfers, more complex functions such as biometric match and cryptographic validations.

Variations in Deployment

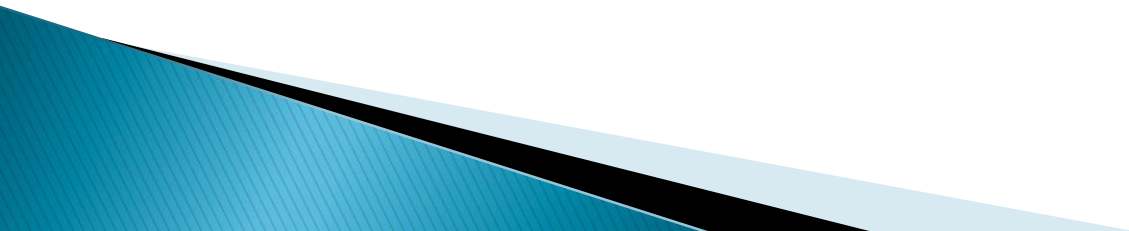
- ▶ A Type has long been recognized for transportation and short burst data transfer.
 - ▶ B was designed for and recognized as more appropriate for higher data transfer and better security
 - ▶ Large deployments such as EMV are successfully allowing for both.
 - ▶ INCITS 504 is agnostic to the choice
- 

GAO Report to Congress

PERSONAL ID VERIFICATION

Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards

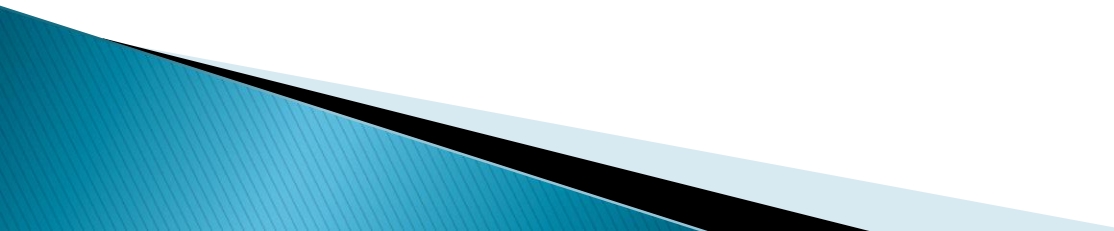
Larger APPS and increased security would benefit from faster interface speeds



Summary

- ▶ Current deployments are exhibiting problems
- ▶ Slow Certificate Processing could be assisted with Increased comms and card speeds
- ▶ Existing Federal Deployments currently exhibit problems and need further testing
- ▶ Path Forward for increased international interoperability should support both types
- ▶ The Bulk of the Market is Supporting Type B
 - More Vendors = Lower Prices
- ▶ Hundreds of Millions of Devices Deployed

An Interoperable Path Forward

- ▶ Encourage support for the existing standard mandating both A and B
 - ▶ While investigating reader improvements, examine all of the options
 - Ensure that readers are truly interoperable and fully configured to support both A & B as defined in the specifications
 - Put a testing program in place to address both technologies and the relationship to the potential power related issues raised by InfoGard
- 

Thank You!



Ron Parsons
ronp@tecsec.com