Security and Interoperability in Contactless Smart Card Systems

Presentation to the NIST Workshop on Storage and Processor Card-based Technologies 9 July 2003

Ray Freeman – Director of Card Technology - Assa Abloy ITG

Current Trends

- Customers are demanding “interoperability” in contactless smart card systems.

- What does “interoperability mean?

Current Trends

What is interoperability?

A common expectation of an interoperable contactless card system is that cards and readers purchased from different and competing suppliers will work interchangeably.

Current Trends

What is interoperability?

A card from supplier A should work with readers from supplier B, C, and D. A reader from supplier A will read cards from supplier B, C, and D.

Current Trends

- Less clear is whether “interoperability” means that there should be a choice in IC technologies and/ or suppliers.

- If reliance on a single IC technology (or chip operating system) is acceptable then “interoperable” systems are available (typically through a licensing scheme).

Current Trend

- An interoperable contactless card system that will work with different IC suppliers is technically possible.
- There are readers on the market that read multiple chip technologies.
- Use of these readers in “interoperable” (multi-vendor) systems is not common probably due to the cost of these readers.

Current Trends

- Interoperability of card ICs from different manufacturers that have a microprocessor can be achieved through the use of common operating system.

- Microprocessor based ICs are available that conform to all parts of 14443 are or are becoming available.

Current Trends

- Contactless memory card ICs that do not contain a microprocessor are what is common in the market today.

- Systems that will use competing contactless card memory IC technology must be made “interoperable” by a reader manufacturer.

Limitations

- Conformance to all parts of ISO/IEC 14443 does not assure “interoperability”.
- ISO/IEC 14443 has no provisions for implementing security.
- ISO/IEC 14443 has no provisions for access to the application areas of the IC.

Limitations

Differences in how security is implemented is a major reason that contactless cards and readers that conform to ISO 14443 are are not necessarily “interoperable”.

Limitations

- Card Readers that are able to read and write to card ICs from more than one manufacturer currently must use multiple proprietary security modules or ASICs from the manufacturer of the IC.
- Certain features of these modules or ASICs are usually redundant (though not interoperable). This can add to the cost.

Limitations

- Security implementations on most contactless memory ICs are based on encryption algorithms that are neither published, nor disclosed to customers.

- The customer has no way to judge the strength or weaknesses of security based on these secret algorithms.

Limitations

- Interoperability that is achieved with card readers that can read memory ICs from different competing companies currently rely on these unknown (secret) algorithms.
- This use of secret algorithms is a risk that is difficult to quantify by it's nature (it's a secret).

Forecast

Secure and interoperable contactless smart card systems in the future will be based on:

1. Cards with microprocessor ICs,

2. Card and reader based on all four parts of ISO/IEC 14443,

Forecast

Secure and interoperable contactless smart card systems in the future will be based on:

3. Strong, published, encryption algorithms embedded in the IC operating system and the card reader,
   (DES, 3DES, AES, RSA……..)

Forecast

Secure and interoperable contactless smart card systems in the future will be based on:

4. Simple, secure, tamper-proof readers, and

5. Key management procedures and components built on “best practices”.

Forecast

- Contactless memory IC cards could “gain traction” if an “open” security standard were to emerge for this class of card.

- Don’t expect anything in the way of a security standard from the ISO/ IEC JTC1/ SC17 working groups.

Thank You

- Comments?
- Questions?