Smart Cards in Government: Symposium on Secure Identification Initiatives

Joe Pilozzi
Business Development Manager
(508)851-2228
Joe.Pilozzi@philips.Com
Contactless Smart Cards & Physical Access
Overview

- Benefits of contactless cards
- Standards
- Security considerations
- Technology availability/ status
Introduction to Contactless Smart Cards

- Large volume of public transport cards and infrastructure have driven down the cost for all other applications
Benefits (1) Convenience of Using the Card/token

- Can be used to gain access without removing it from wallet/sleeve
- IC can be completely encased in plastic
  - Can be embedded in keyfob/watch.....
  - Last longer; less likely to be damaged

- Faster to pass token quickly by reader
Benefits (2) Reliability of Readers Improved

- No contacts to wear out
- No card slot to unclog
- Cold & weather not a problem
- Resulting in low maintenance
Benefits (3)
Speed of Communications Increased

- Current contact cards communicate at 9.6kbit/sec acc. to ISO7816

- ISO14443 is 106kbit/sec
  - up to 848 kbit/sec is possible today

- Biometrics images transferred 10 to 100 times faster
# Contactless Standards Summary

<table>
<thead>
<tr>
<th></th>
<th>ISO14443A</th>
<th>ISO14443B</th>
<th>ISO15693</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Cards</td>
<td>250M</td>
<td>4M</td>
<td>15M</td>
</tr>
<tr>
<td># of Readers</td>
<td>1M</td>
<td>10K</td>
<td>50K</td>
</tr>
<tr>
<td>Read Range</td>
<td>10cm</td>
<td>10cm</td>
<td>1M</td>
</tr>
<tr>
<td>KBytes EEPROM</td>
<td>16 (64*)</td>
<td>8 (32*)</td>
<td>1.25</td>
</tr>
<tr>
<td>Anti-Collision</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>PKC Enabled</td>
<td>yes</td>
<td>maybe</td>
<td>no</td>
</tr>
<tr>
<td>Secure Micro</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Speed, Kb/Sec</td>
<td>106*</td>
<td>106*</td>
<td>50</td>
</tr>
</tbody>
</table>
Other Non-standardized Offerings

• 125Khz/134Khz
  – Used primarily for logistics and physical access
  – Communications rates slower @ 20Kb/s
Security Considerations??

- Is a card that can be read/written through radio waves any less secure than one with which contact must be physically made?

- Depends upon:
  - Type of IC
  - Type of conditional access system used
  - Degree of security required
Security Considerations (1)
Hardwired ICs

• Typical features include:
  – Unique serial number
  – Password protection
  – Random number generation
  – 3 pass authentication
  – Proprietary stream cipher, DES or 3DES used for encryption
  – Access keys for memory blocks
Security Considerations (2)
Micro Controller Based Ics

• Dual interface possible:
  – Contact mode used to initialize/load ID......
  – Contactless mode used for application

• Active countermeasures under core control are available including sensors
• Public Key/Private Key Cryptography, DES, 3DES, AES, ECC… built in
Technology Availability/status (1)
ISO14443 Proximity Smart Card IC

• Low end devices ranging from
  – Few bytes of memory for sub $0.20 paper tokens to
  – 4K bytes of memory for ID and multi-appl. Contactless smart cards

• Higher end devices now available offering
  – Microcontroller core
  – Private and/or Public key accelerators
  – Memory firewalling
  – VISA HW Security Level 3 approved
Technology Availability/status (2)
ISO15693 Vicinity Card IC

• Low end devices ranging from
  – 32 bit read only number to
  – 1K bit read/write

• Higher End Devices
  – up to 1.25K bytes of memory for ID and multi-appl. contactless cards
  – Proprietary security features
Technology Availability/status (3)
Reader ICs

• Integrated ics supporting:
  – ISO14443
  – ISO 15693
  – ISO14443, plus ISO15693
Technology Availability/status (4) Biometrics

- Physical access systems using fingerprints or photo ID almost universally implemented contactlessly
  - Speed of image transfer faster
  - Low cost ICs with sufficient security available now
Conclusion

• Contactless solutions fit very well with physical access (and other) smart card applications
  – Technology is stable, reliable, secure and available
  – Best fit for all environments when quick, convenient card/reader communications are required