IC card policy of Japan

Katsuya Makiuchi
Director, IT project office
METI
Political Positioning of IC card

- Personal Identification in Cyber World
- Network Certification
  - JPKI (Japanese Public Key Infrastructure) (2004/1~)
  - Corporate Certification (2000/4~)
  - GPKI (Government Public Key Infrastructure) (2001/4~)
  - LGPKI (Local Government Public Key Infrastructure)
- Security and Safety
Technology of IC card

• Contact-less
  - ISO/IEC 14443 Type B Interface

• Chip
  - 32bit CPU, 32KB~1MB Memory, Coprocessor for PKI

• NICSS (the Next generation Ic Card System Study group)
  - NICSS Framework for multi-application IC card

• NMDA (New Media Development Association)
  - Proximity Communication Interface Implementation Specifications
  - Test for Interoperability of Contact-less IC Cards

• JICSAP (Japan IC Card System APplication Council)
  - JICSAP IC Card Specifications
Project overview

Research project on Cities Equipped with IT
IT City project
Basic Residential Registers Network System
e-passport

Fields

<table>
<thead>
<tr>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ø</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Experiment

- Public and Private sector
- Multi application
- Contact-less IC card
- PKI
- Multi application
- Contact-less IC card
- PKI
- Wide area service
- Interoperability

Practical Use

- Multi application
- Contact-less IC card
- PKI
- Wide area service
- Interoperability
- Biometrics
- Global use

Functions

- Secure IC chip project
- Digital Rights Management
- Remote maintenance of Medical instruments
- Music Distribution on Network
- Receipt Network
Establishment of Global Standard

- ISO/IEC (JTC1/SC17)
  International standards of IC card
  - Physical characteristics
  - Command
  - RF power and signal interface
  - Transmission protocol
  - Test method
  etc.

- GCF (Global Collaboration Forum)
  NICSS (Japan), eESC(EU), NIST(USA)
  - Agree on a general smart card based global framework for interoperable e-authentication.
  - Define a minimum common core specification for implementations of this approach

- Japan/China/South Korea (Asia IC Card Forum)
  - Establishment of Asian standard
  - Discussion on e-payment system in using IC card among Asian countries
  - Prevention of doubled investment on related infrastructures in Asia
IC Card in e-Japan Strategy

- Resident Registration card (from Aug. 2003)
  - Multi-application IC card for receiving e-Government services (Local-government services, JPKI services, etc.)

- National Government Employee IDs (from 2005FY)
  - In order to enhance security further, decisions will be made during 2004 concerning the adoption of common standards and measures for shared use of systems concerning the introduction of IC cards for national government employee IDs. Implementation will follow in stages.

- IC Passports (from 2005FY)
  - As one aspect of anti-terrorism and security measures utilizing IT at airports and seaports, ICs in passports that comply with international standards will be used and immigration controls using such passports will be reinforced. Testing will be conducted in fiscal 2004 toward actual use in fiscal 2005. From the perspective in enhancing security throughout Asia, the Government will consider support for the introduction of IC passports in response to requests from other Asian countries.

- Driver’s license (from Apr. 2004)
  - High security IC card Driver’s license
• Dual Stack Trusted Architecture by PKI
  – 1\textsuperscript{st} stack PKI: Management for status of IC Chip layer
  – 2\textsuperscript{nd} stack PKI: Management for status of Service layer
    • e-Ticket, Digital Signature, etc.

• CLIC (Contact-Less IC card deployment center)
  - Issuing contact-less IC cards (include the Resident registration cards)
  - Evaluation compatibility between IC cards and R/Ws
  - Technical consultations
e-Passports

• ICAO Standard
  The standard of e-Passport will be publish by ICAO (International Civil Aviation Organization) at May 2004.
  - Biometrics, PKI, Contact-less IC, LDS (Logical data structure), etc.

• Three Japanese Proposals
  1. Implementing standard for Contact-less ICs in e-Passport
  2. Test tool for e-Passport interoperability
  3. Test Demonstration