



**e-ID Activities in Japan
- Update on IC Card Systems
in Public Sector
including e-Passports**

October 19, 2004

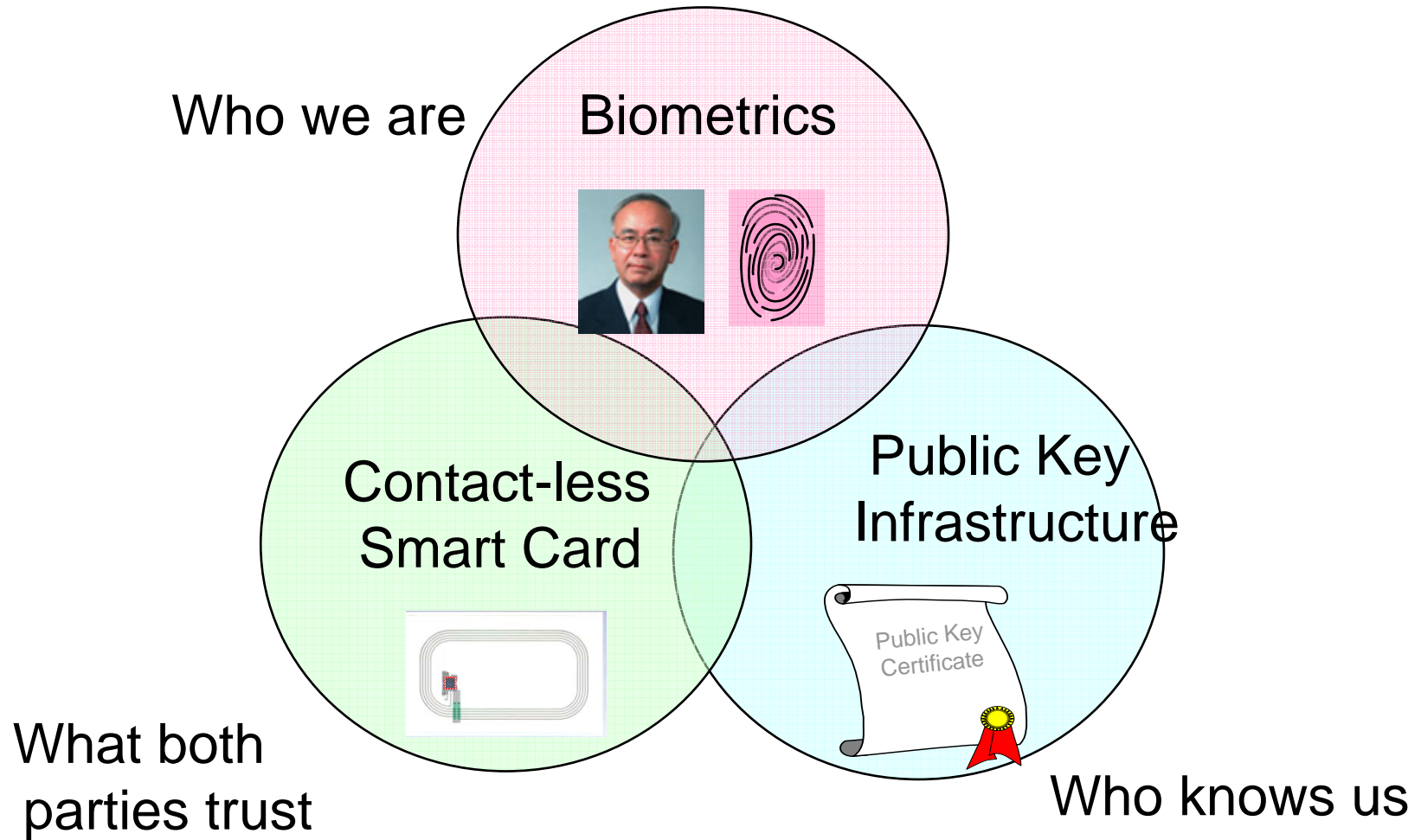
Akio Kokubu

New Media Development Association (NMDA)

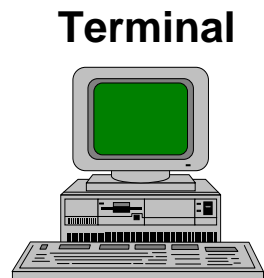
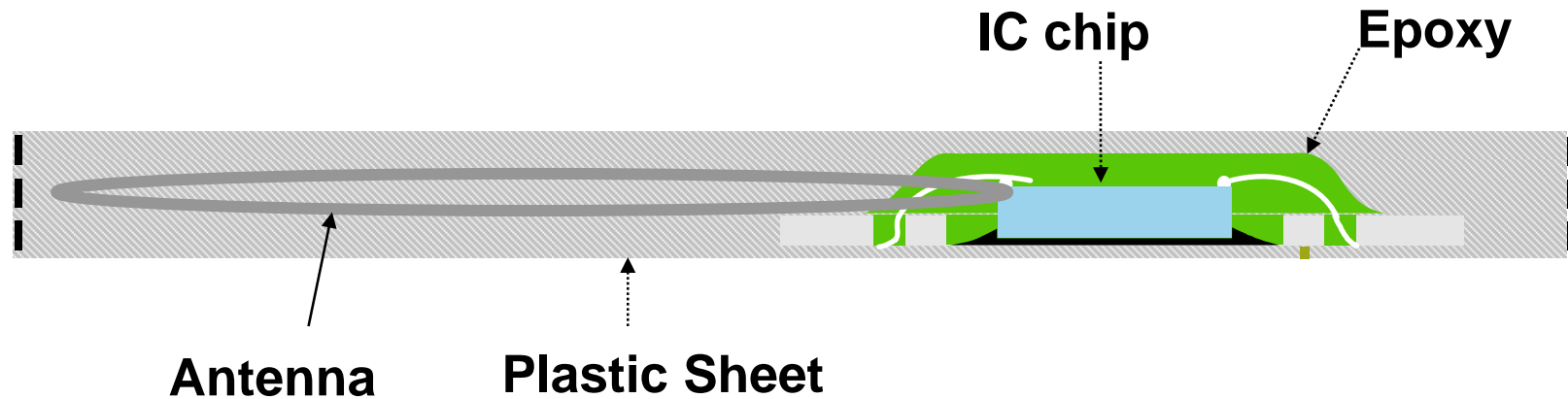
Who is the NMDA?

- Non-profit and independent organization for the public interests.
 - Financial support from Japanese Ministry of Economy, Trade and Industry is two third of total revenue.
- R & D platform for industry to establish the standard of information society technologies
 - Development and deployment of advanced smart card systems including e-Passport initiative as an information infrastructure
 - Technological development of e-Government systems

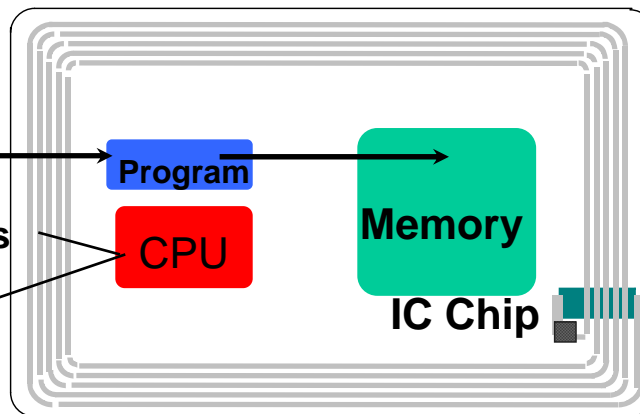
Three technologies of e-IDs



Contactless Smart Card (Contactless IC Card)



Legal Access →
Illegal Access →



Features

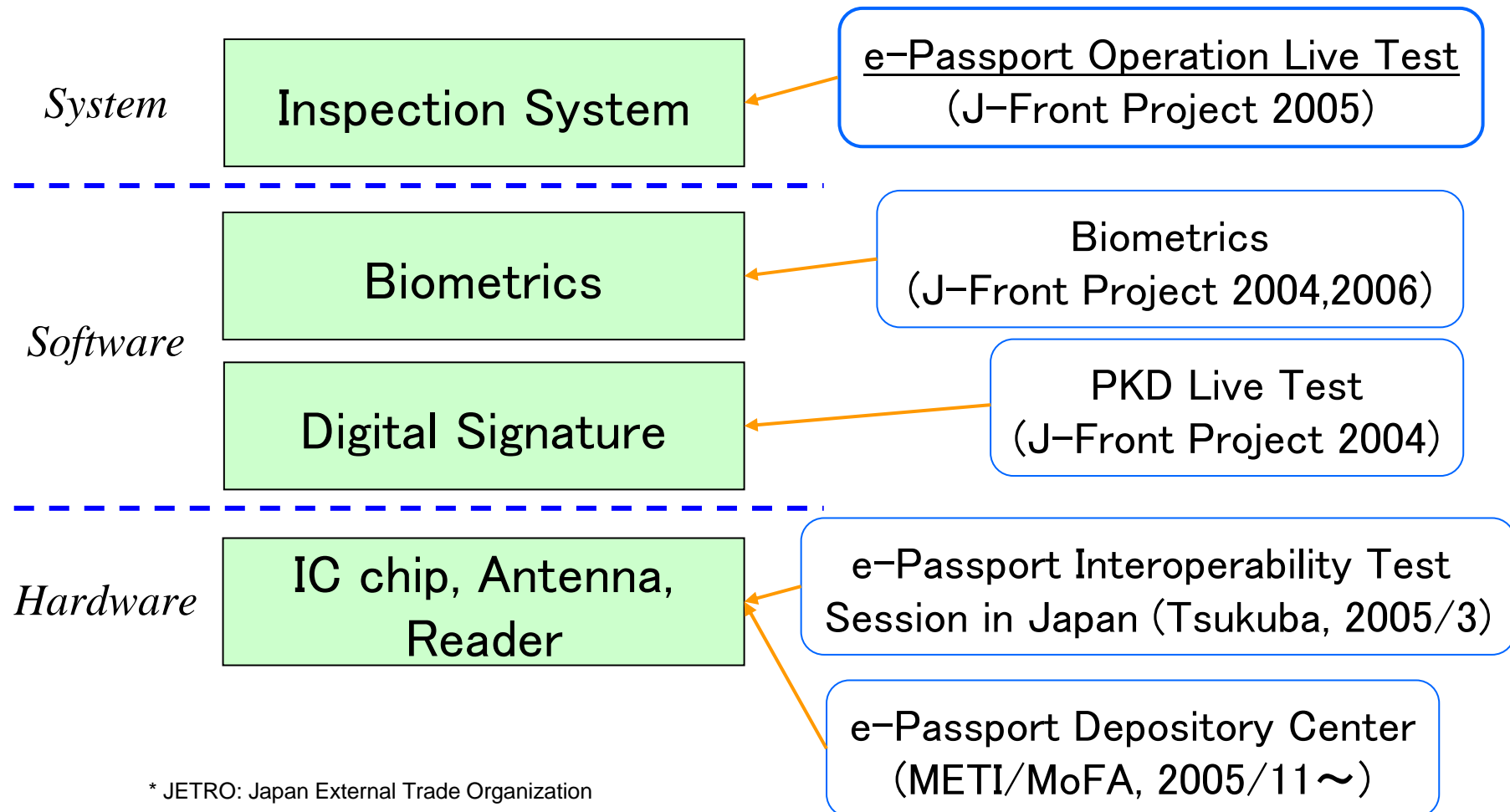
- High security function
Access controlled by CPU
Embedded crypt function
- Large capacity memory

Rejected read
operation of stored
data by CPU

Agenda

- **e-Passport Interoperability & e-Passport Depository**
- **Update on IC card systems in public sector**
 - Basic Resident Registration Cards
 - Driving License Cards
 - Government Employee's Cards

e-Passport Interoperability in Hardware, Software & System



Status on e-Passport in the world

Oct-06

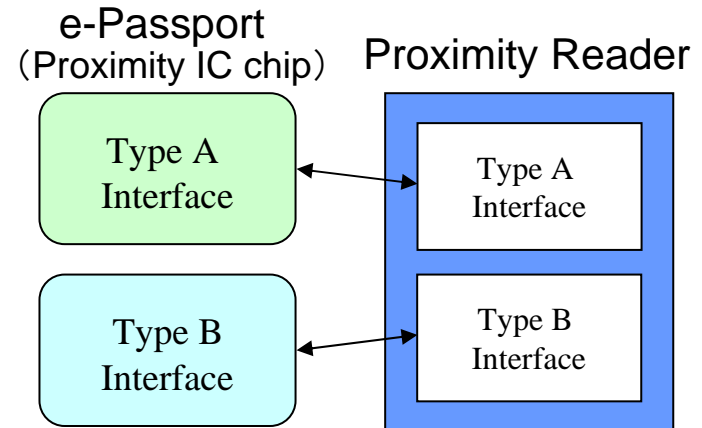
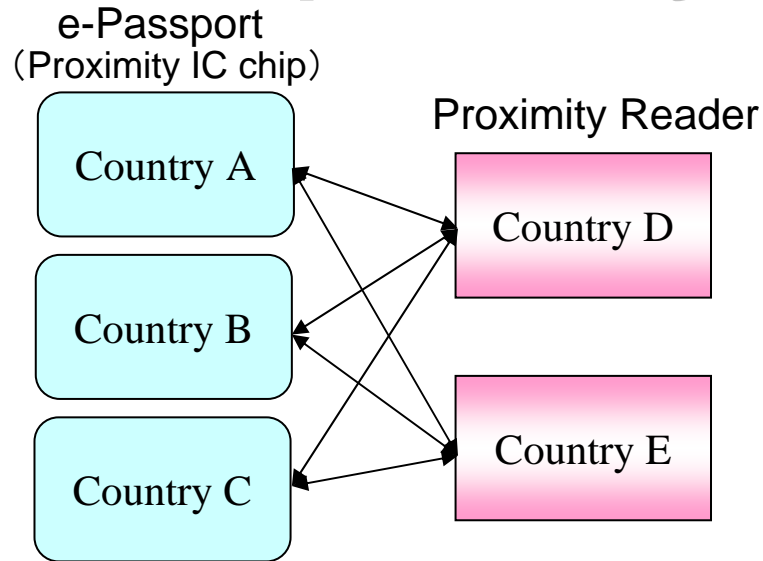
Country	Interface Type	Issuance	Notes
Belgium		2004/11 start	350,000 (9/2005)
Thailand	Type A	2005/5 (Diplomatic) & 2005/6 (Citizen)	820,000 5/2006
Australia	Type B	2005/10 start	700,000 (5/2006)
Sweden		2005/10 start	01/10/2005
Norway		2005/10 start	03/10/2005
Denmark		2005/10 start	
New Zealand	Type A	2005/11 start	180,000 (5/2006)
Germany	Type A	2005/11 start	550,000 (2/2006)
UK	Type A	2006/3 start	02/03/2006
Japan	Type B	2006/3 start	20/03/2006
Italy	Type A & B	2006/3 (Diplomatic)	08/2006 for Citizen
France	Type A	2006/4 start	
Iceland		2006/5 start	
Austria	Type A	2006/6 start	
USA		2006/8 start	
Singapore	Type A	2006/8 start	
Luxemburg	Type A	2006/8 start	
Portugal	Type A	2006/8 start	
Finland		2006/8 start	21/08/2006
Netherlands		2006/8 plan	
Poland		2007/8 planned	
Switzerland		2006/9 strat	04/09/2006
Czech		2006/9 planned	
Slovenia	Type A	2006/9 planned	
Russia		2006 planned	
Canada		2007/1 planned	
South Korea		2007 expected	
China		2007 expected	
Hong Kong		2007 expected	
Taiwan	Type A	2007 expected	
Indonesia		2007 expected	

Source: ICAO-NTWG country reports and UKPS reports

Japanese e-Passports

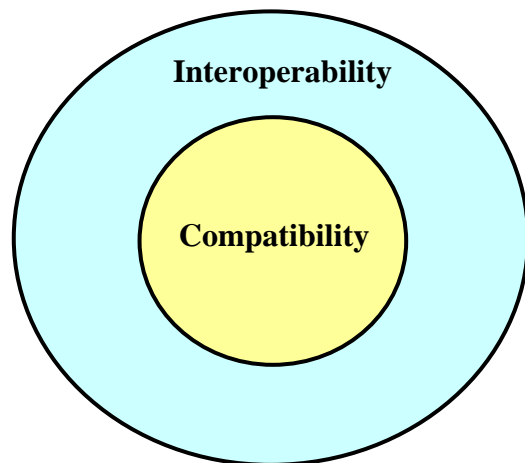
- **Ministry of Foreign Affairs (MOFA) started to issue e-Passport to Japanese citizen from March 20, 2006.**
- **National Printing Bureau, the manufacturer of Japanese passports procured 2,560 thousands sheets of IC chip with antenna from Toshiba and Sharp for fiscal 2005.**
- **For fiscal 2006, an open bid is underway. Bidders were requested attachments of test data measured by MNDA.**
- **Major specifications:**
 - Contact-less interface (ISO/IEC14443 Type B) for reading
 - The sheet of IC chip with antenna is located in center of booklet.
 - BAC (Basic Access Control) with MRZ (Machine Readable Zone) is adopted.
 - Facial biometrics data is stored (Fingerprint data is not stored).

Importance of Maintaining Interoperability and Compatibility



Two type of e-passport to be supported.

Interoperability between countries and manufacturers



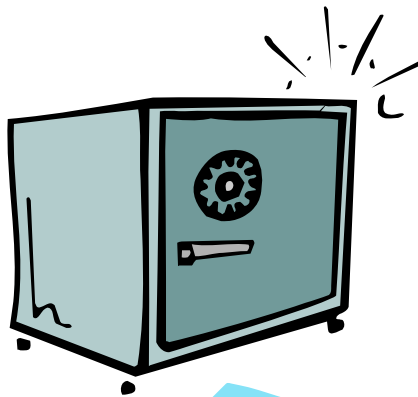
Interoperability: A concept that encompasses compatibility. It means that an e-Passport can communicate with any reader and any passport control system in any country and that passport services are available for anyone who want.

It is required to realize the interoperability and the conformity to ICAO specifications.

Compatibility: It means that e-Passports and readers can communicate each other basically and bi-directionally in view of radio characteristics, protocols and commands.

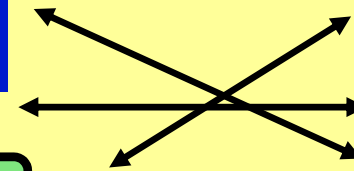
It is required to realize the conformity with ISO standards and the compatibility with the implementation specifications.

e-Passport Depository Operation

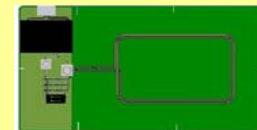


Sample e-Passports from various countries kept at the Depository

Carry-in Tests



Depository Tests



Merits of Using e-Passport Depository

Overall Objectives:

- To carry out evaluation tests safely in the environment where the security policies are established and to promote the interoperability between countries and manufacturers.
- To serve the nations and the institutions concerned as a permanent center for testing the interoperability. Application for testing is acceptable any time via Web site.

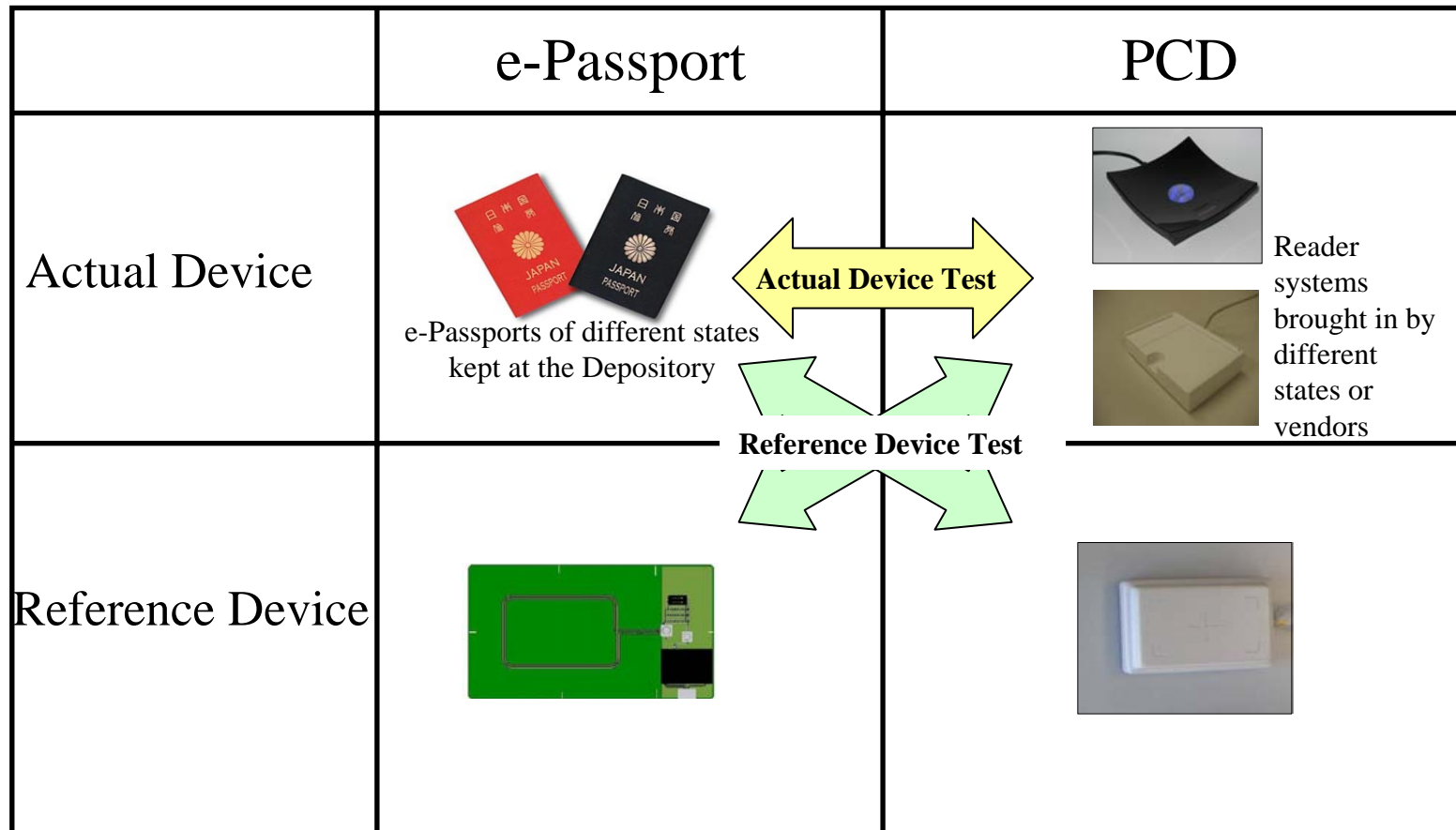
For Institutions that deposit e-Passports:

- By depositing e-Passport samples at the Depository, the institutions can obtain results of interoperability tests with ICAO-reference PCDs. The interoperability tests are also carried out with the PCDs of major companies of various countries and its results are reported to the institutions.
- Also, the interoperability tests are carried out at the Depository each time a company developing PCDs brings in its new PCD products. The test results are also reported to the institutions.

For Companies that carry in PCDs:

- By carrying in PCDs to the Depository, the interoperability testing can be performed efficiently with e-Passports of various countries across the world that are kept at the Depository.
- By testing the interoperability with ICAO-reference e-Passports, the data can be obtained and utilized when companies are developing new versions of PCD products.

e-Passport Depository Testing Combinations



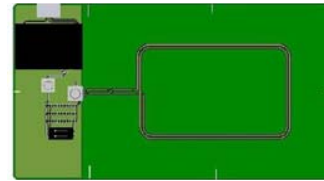
PCD: Proximity Coupling Device

e-Passport Depository Test - System Components

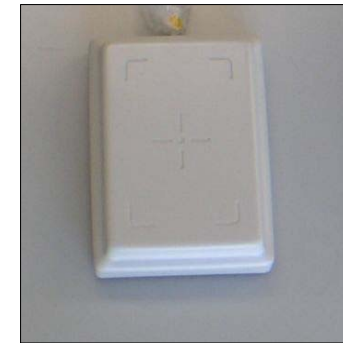
ICAO Reference Software



ICAO Reference e-MRP and Reader



Type B, 424kbps, BAC



Type A/ B: NMDA TM-PR-400



MRZ Reader



Type A: Philips Pegoda



Type A/ B:SCM R/W

e-Passport Depository Testing System Specifications

The testing system shall comply with the following:

- ICAO TR LDS ver1.7
- ICAO TR PKI ver1.1
- ICAO Supplement Doc.9303

And shall implement the following:

- DG2-JPEG/DG2-JPEG2000
- Basic Access Control presence/absence handling
- MRZ Reading
- Active Authentication, RSA (PSS, v1.5), ECDSA,
- DSA handling
- GepA1 – A4, GepB1 – B4 handling etc.

The sample e-Passport shall:

Comply with the ICAO specification and shall have all required information specified by the standards of each state.

Agenda

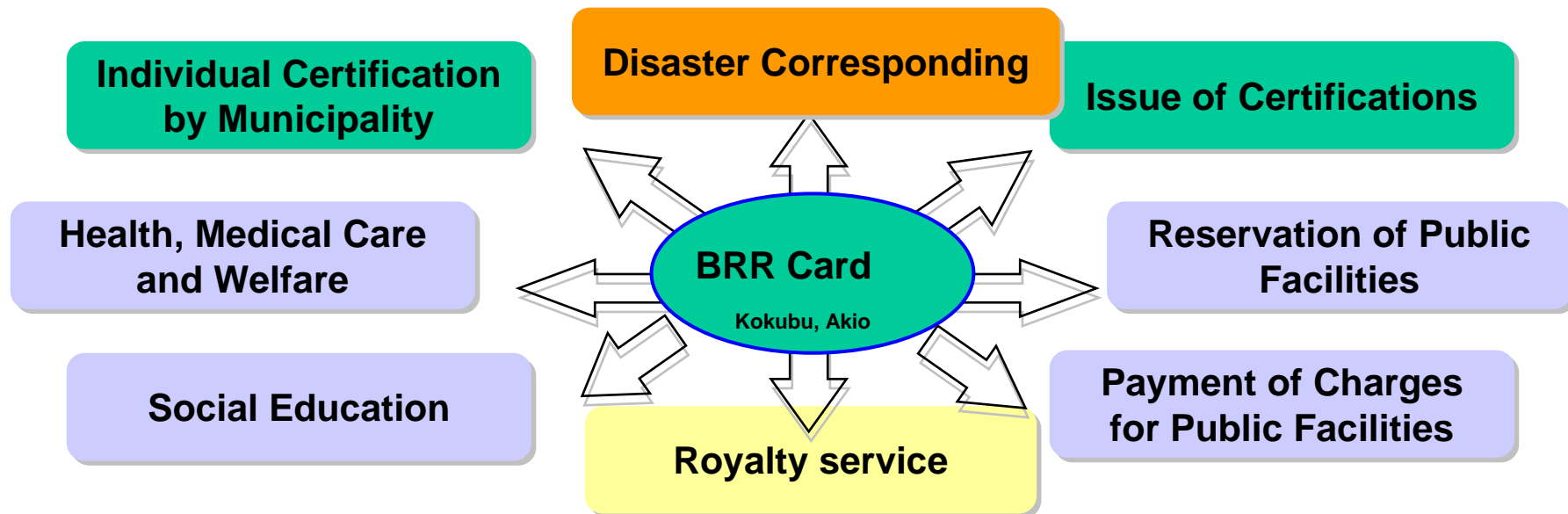
- **e-Passport Interoperability & e-Passport Depository**
- **Update on IC card systems in public sector**
 - Basic Resident Registration Cards
 - Driving License Cards
 - Government Employee's Cards

Update on Basic Resident Registration Card

- What is it?
 - It is a **multiple application card with PKI** and has been issued from municipalities of more than 3000 since August 2003 when residents request to issue.
 - Based on bylaw of municipalities, cards can be used to many public applications such as reservation and payment of charges for public facilities, health, and medical care.
 - Details for such applications will be determined by council of each municipalities.
- Procurement and issuance of cards
 - Dual interface cards were dominant at the first procurement stage though **contactless interface is mandatory** and contact interface is optional.
 - Cards with large capacity (up to 1M bytes) of FLASH memory were preferred because of future addition of applications because they thought they would need more application spaces in the future.
 - The number of cards issued is approaching **one million** though it is a voluntary card and municipalities are reluctant to work with.
- Public personal certification infrastructure
 - It is an application of basic resident registration cards and started in January 2004.
 - It will be used for personal income declaration to the national tax agency, procedure for social insurance.
 - To submit them from home, compact R/Ws for contact-less cards are needed and they are going to be introduced in the market with a relatively cheap prices.

Applications of Basic Resident Registration Cards

- Based on bylaw of municipalities, cards can be used to many public applications such as reservation and payment of charges for public facilities, health, and medical care.
- Details for such applications will be determined by council of each municipalities as bylaw.



Update on Other IC Card Systems in Public Sector

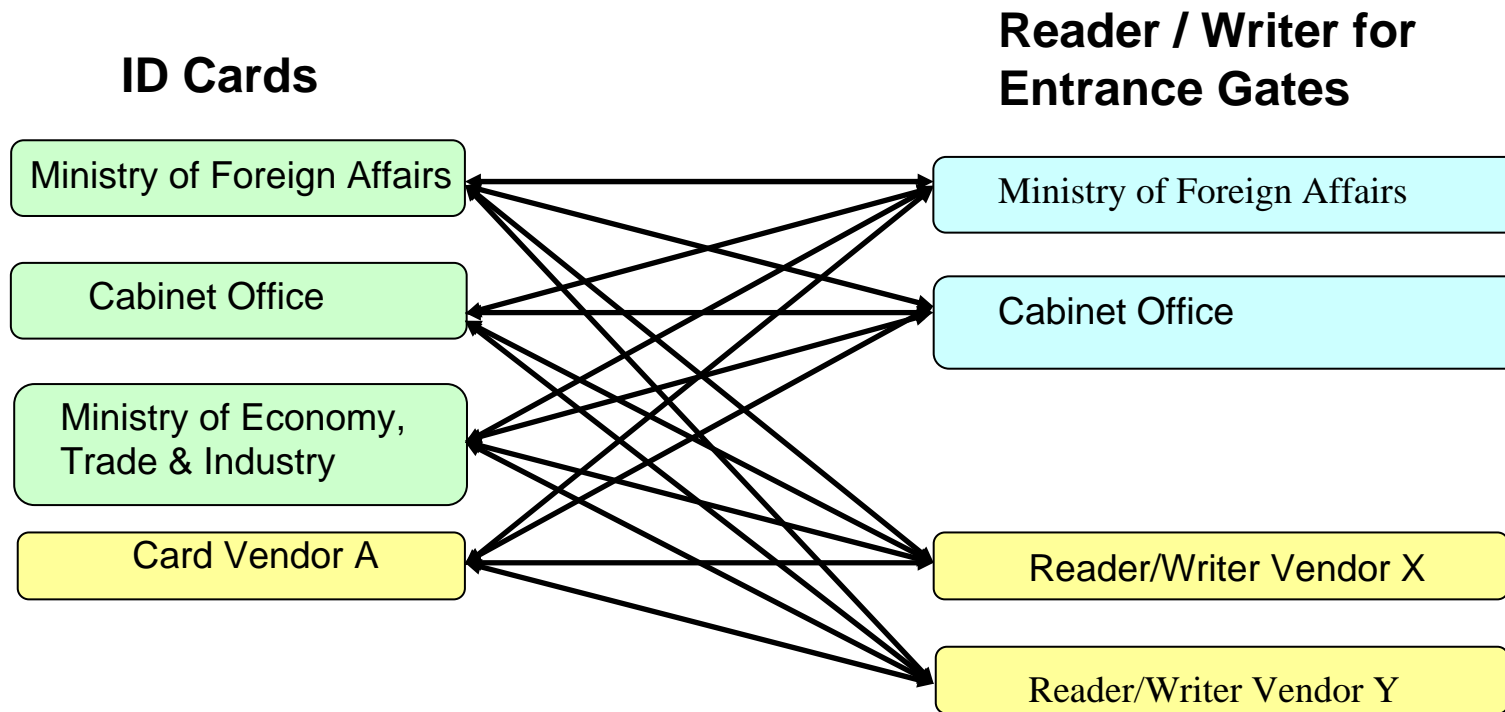
- **Driving license card**

- What is it?
 - It is a driving license card with contactless type B interface.
 - It was expected that local police departments issued them from April 2005. The plan looks postponed because of financial crisis in local governments.
- The issue number expected will be more than 10 millions per year if issuance starts. (The total number of license holders is more than 76 millions in Japan.)
- It will store small capacity face photo data of driver in chip with 8 KB memory.

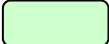
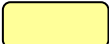
- **Government employee's card**

- Government employees are going to have a smart card with PKI as a certificate for entrance of buildings and access of computer networks.
- The specification was fixed with support of NMDA and then it has been introduced to agencies in a step-by-step manner.
- The number of employees expected to have:
 - Central government: 350 thousands
 - Independent administrative agencies: 200 thousands

Interoperability Test for Government Employee's IC Cards by NMDA



September 2006

-  Installed products at government agencies
-  Bidder's products for government agency's procurements

Thank you.

For further questions, please e-mail to
Kokubu@nmda.or.jp