First Workshop on Contactless Card Interoperability
Mutual European and Japanese Initiative for Interoperability
in Paris on October 24, 2001

Development of Proximity Card

- In compliance with NMDA Implementation Standards -

Masamichi Azuma

Matsushita Electric Industrial Co.,Ltd.

Background of Development Project

“Development of Platform for New Generation Smart Card System”

National Project / Establishment of IT Infrastructure in Industrial and Social Fields
- in the Supplementary Budget of the Fiscal year 1998 -

Directed by *New Media Development Association*

Under the Contract with ‘formerly known as’ *Ministry of International Trade and Industry*

（Currently *Ministry of Economy, Trade and Industry*)

～Requirements for Smart Card System ～

ー*Multi-Application Open System*

>> Ubiquitous

ー*PKI (RSA, ECC)*

>> High Security

ー*Proximity Card*

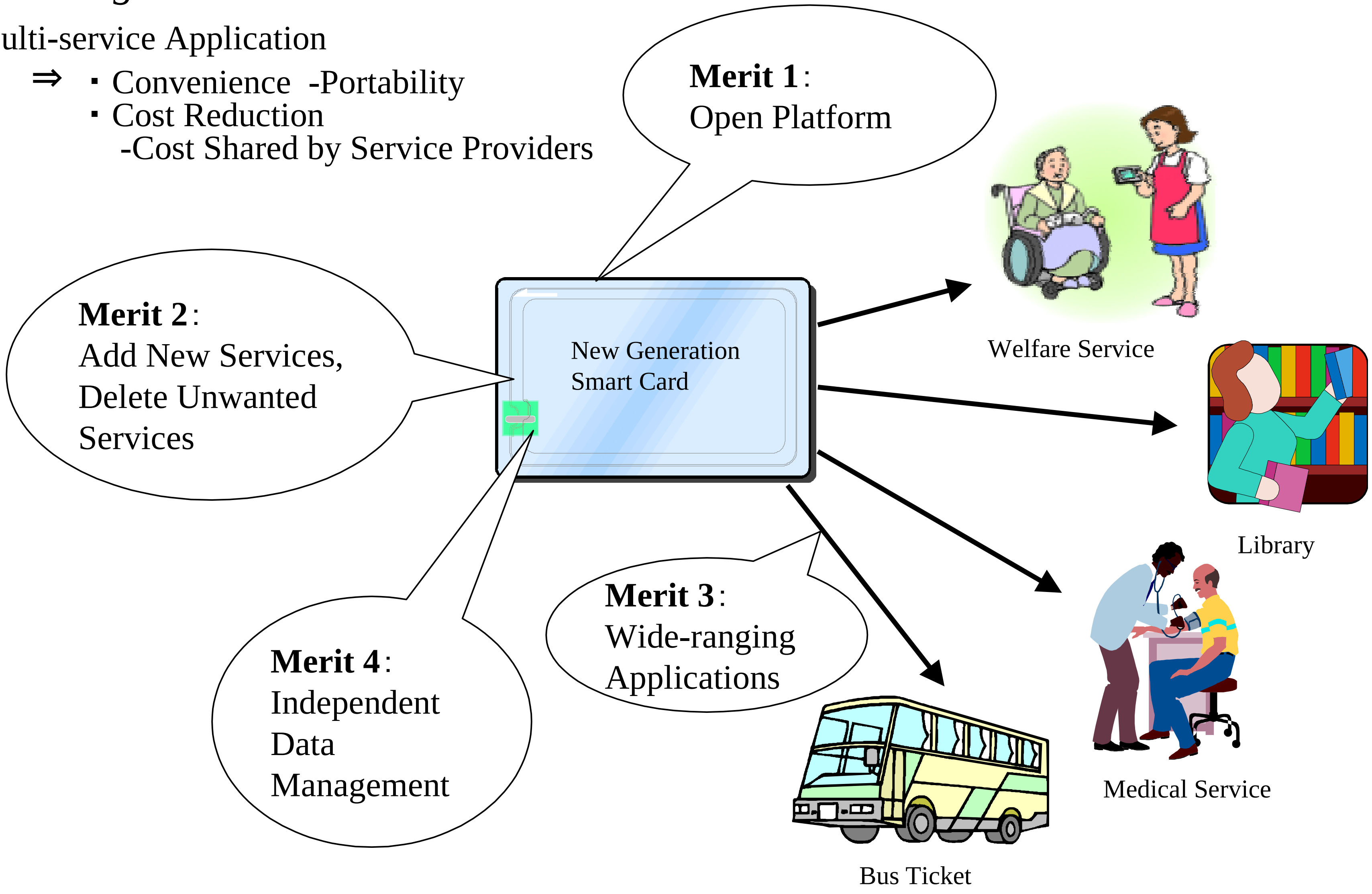
>> Barrier Free, High Speed, Multi Card R/W Operation

Applied Scene of New Generation Smart Cards

Advantages

Multi-service Application

⇒ ▪ Convenience -Portability
▪ Cost Reduction
-Cost Shared by Service Providers



Merit 1: Open Platform

Merit 2: Add New Services, Delete Unwanted Services

Merit 3: Wide-ranging Applications

Merit 4: Independent Data Management

New Generation Smart Card

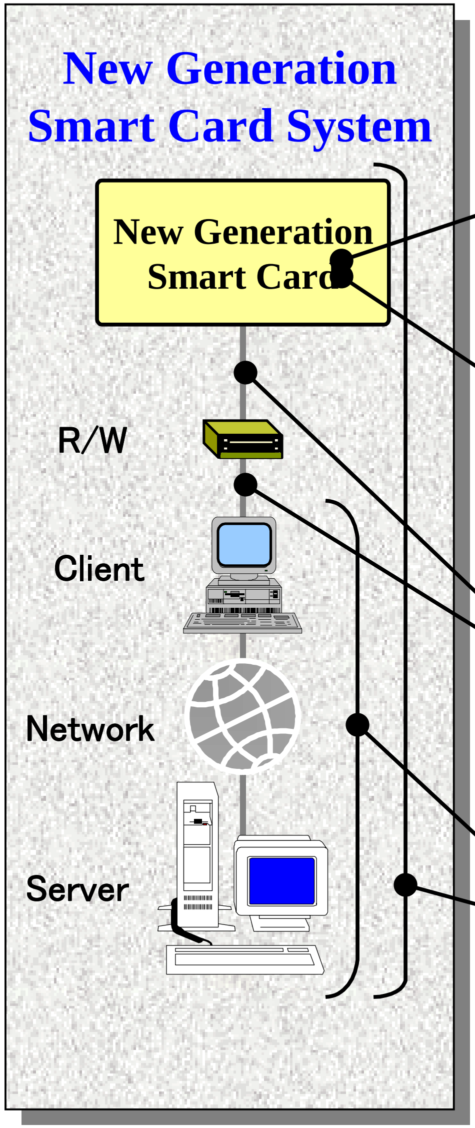
Welfare Service

Library

Medical Service

Bus Ticket

Key Issues for Interoperability



Interoperability

① Interindustry Command Specification

- On Demand Command Support for ISO、JICSAP、EMV
- Based on ISO Specification

② Allows Expanded Function for Card Platform

- Secure Download Scheme 、 Standardization of Application Management
- Open Platform（Java Card、MULTOS、Native Card）
- High Security Multi-Application

③ Interoperability of Proximity Cards

- ISO/ICE 14443 Type B
- Implementation rules for IC Card & R/W

④ System Architecture with Application Interoperability

- System Model for Multi-Application
- Development of IC Card Operation (issuing cards, providing services)

Interindustry Command Library

◆**Interindustry Command Library**

－Integrate Major Standardized Command Libraries
(i.e. JICSAP, EMV, “Zenginkyo” Library)

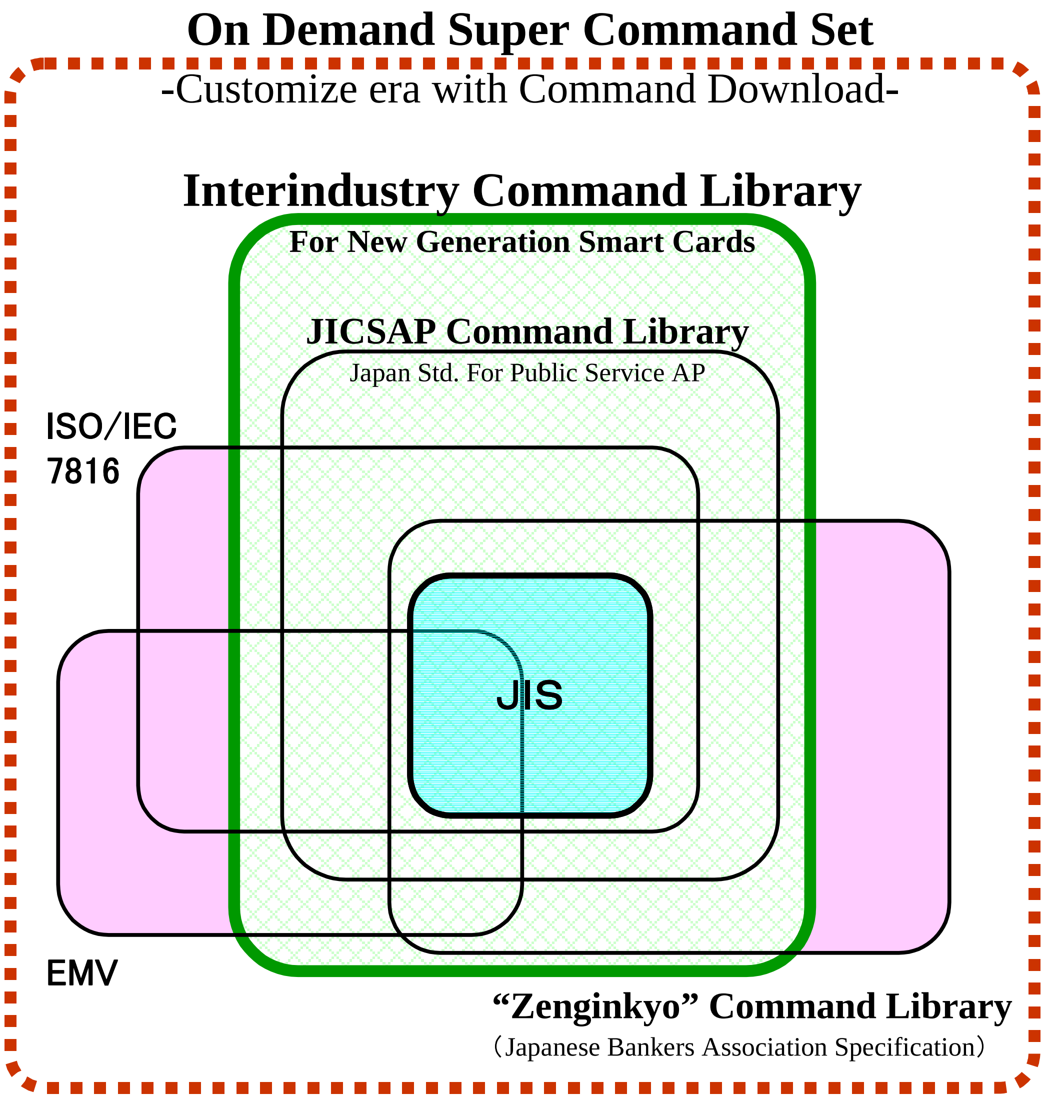
◆**On Demand Extension**
- Download Extended Command

－Adjustable to
Optional Standardized Command Library

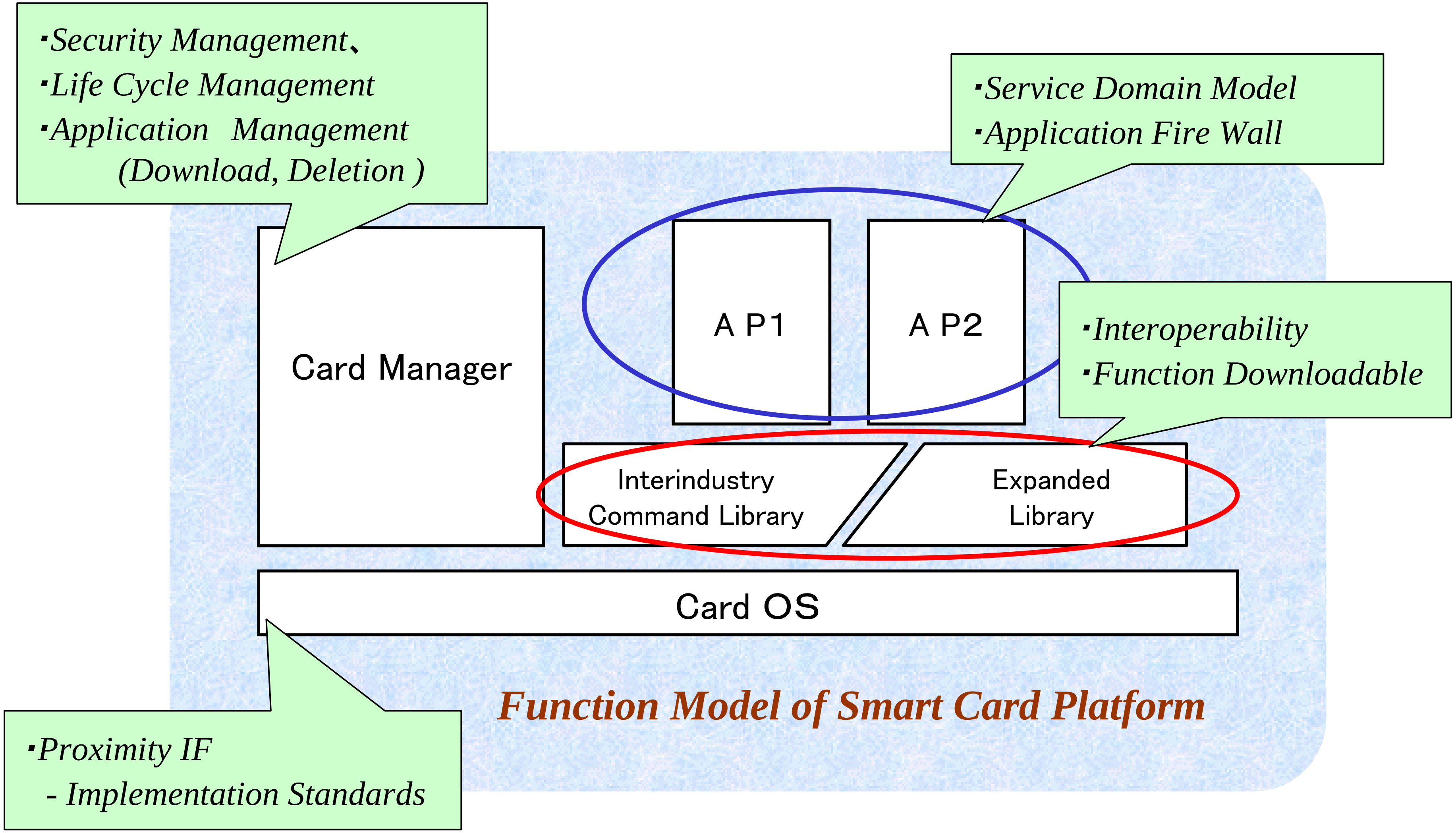
⇩

1. Assured Compatibility with Existing Smart Cards

2. Flexible to Optional Demand


On Demand Super Command Set
-Customize era with Command Download-
Interindustry Command Library
For New Generation Smart Cards
JICSAP Command Library
Japan Std. For Public Service AP
ISO/IEC 7816
JIS
EMV
“Zenginkyo” Command Library
（Japanese Bankers Association Specification）

Smart Card Platform



- *Security Management、*
- *Life Cycle Management*
- *Application Management*
  (Download, Deletion)

- *Service Domain Model*
- *Application Fire Wall*

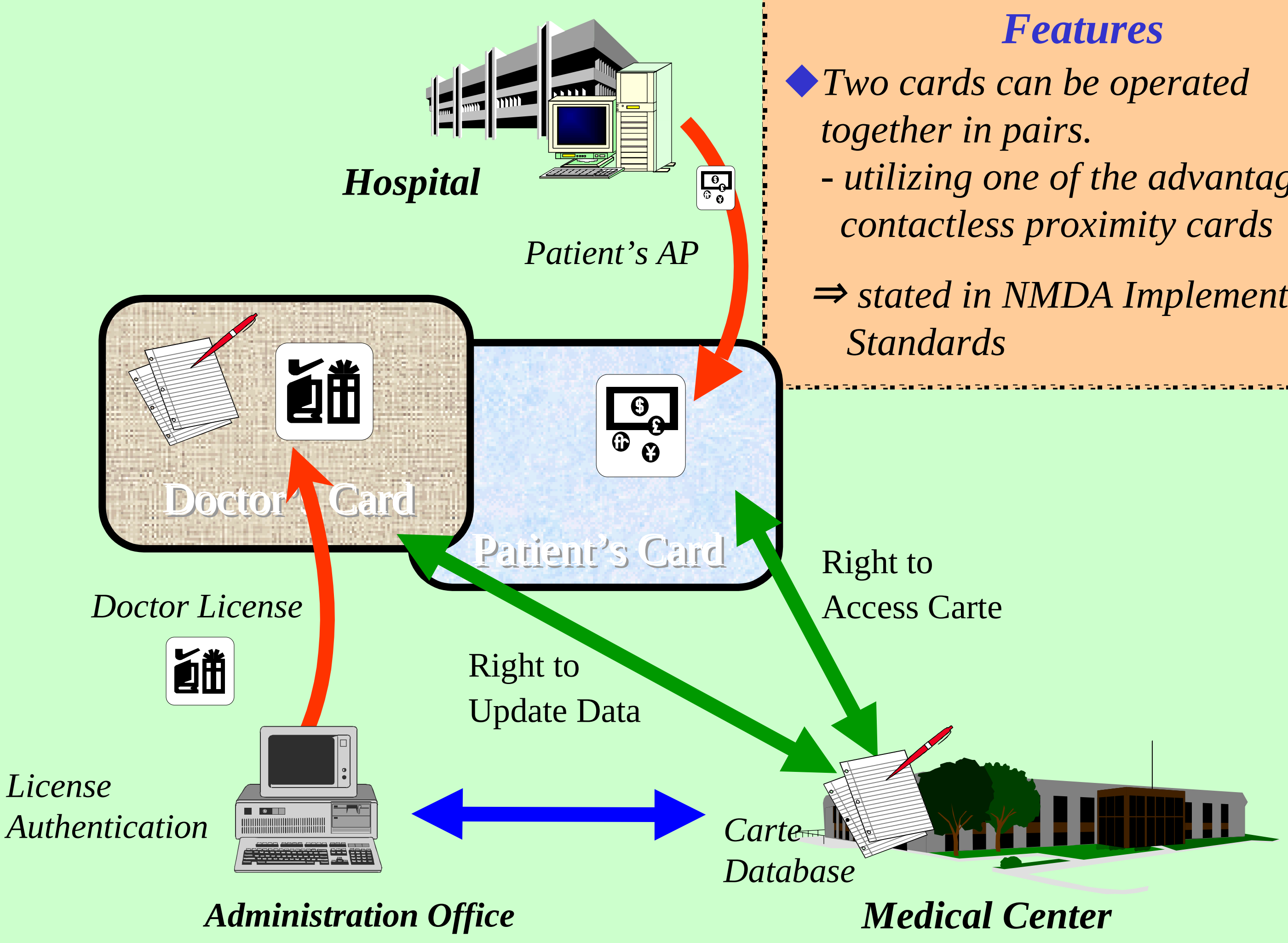
- *Interoperability*
- *Function Downloadable*

- *Proximity IF*
  - Implementation Standards

Function Model of Smart Card Platform

Dual Card Operation Scene

License Authentication in Medical Practice

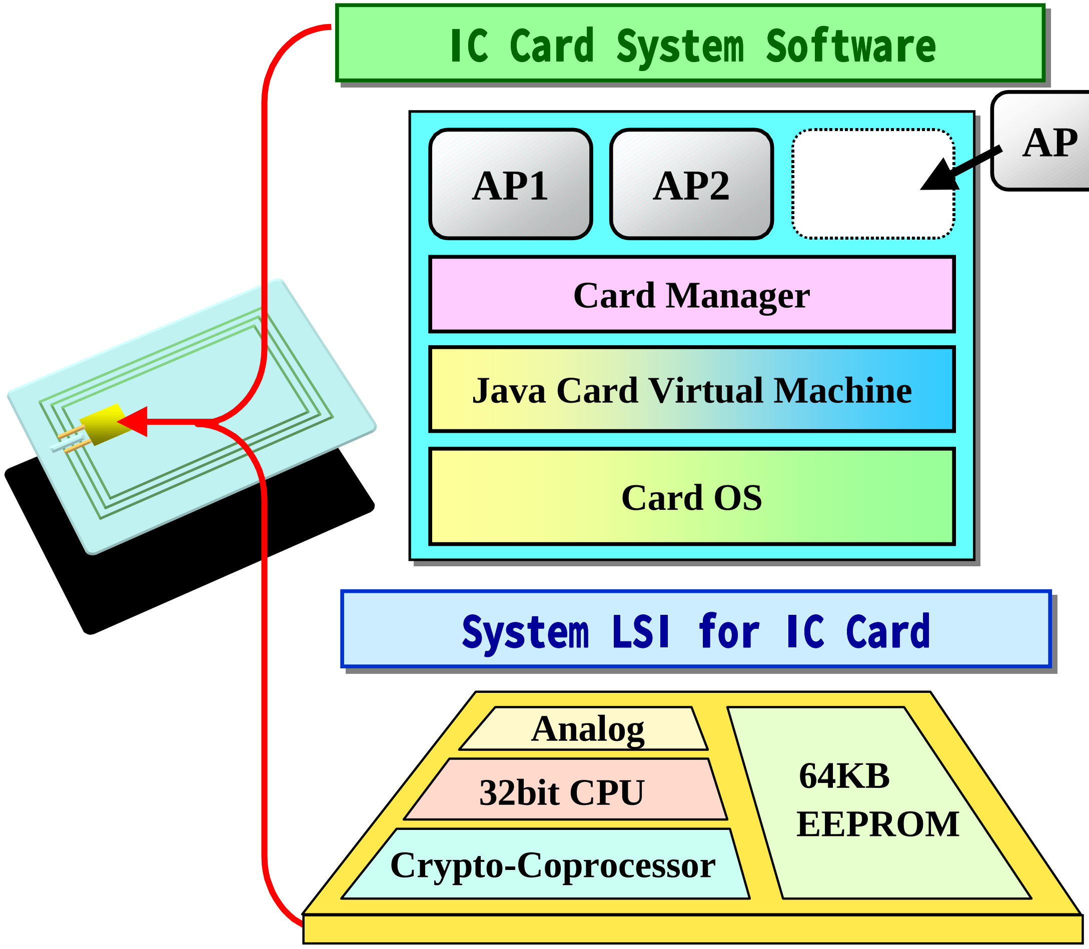


Features

- *Two cards can be operated together in pairs.*
  - *utilizing one of the advantages of contactless proximity cards*

⇒ stated in NMDA Implementation Standards

Configuration of New Generation Smart Card



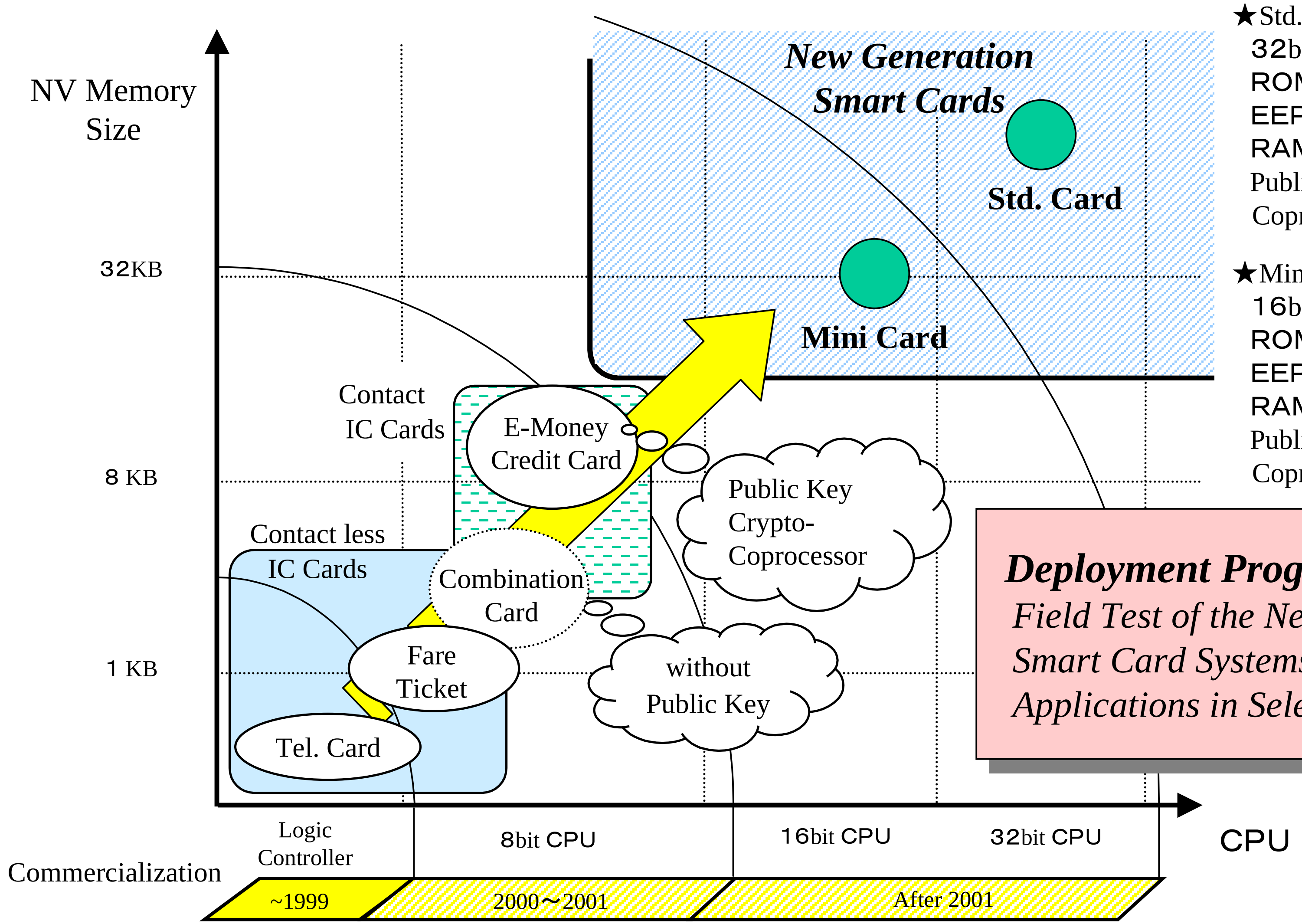
Features of Matsushita Card :

- **Multi Application**
- **Application Downloadable**
- **High Security**
  （eg. mutual authentication,
  digital signature, random number
  generation etc ）
- **Interoperability**
  ⇒ Interindustry Command Library
- **Proximity Interface**
  （ISO/IEC 14443 Type B）
- **Low Power 32bit CPU**
- **Public Key Crypto-Coprocessor**
  （ECC, RSA）

Specification

	New Generation Smart Card	Contact Smart Card	Proximity Card
Interface	**Contact less （ISO/IEC14443 Type B）**	Contact Card （ISO/IEC7816）	Contact less （ISO/IEC14443）
CPU	**32 bit**	8 bit or 16 bit	Logic or 8 bit
RAM	**12KB**	0.5KB～2KB	～0.5KB
ROM	**128KB**	16KB～32KB	～24KB
Nonvolatile Memory	**64KB**	～32KB	～4KB
Cryptography	**RSA、ECC DES、Triple-DES**	RSA、DES Triple-DES	DES Triple-DES
Transmission Protocol	**T=CL （ISO14443）**	T=1 （ISO7816）	Original
Commands	**ISO/IEC7816-4 ISO/IEC 7816-8 ISO/IEC 7816-9 JICSAP … Interindustry Command Library**	ISO/IEC7816-4 JICSAP EMV … Support Ether Single Library	Original
Method to Add Optional Functions & AP	**Downloadable**	Not Supported (e.g. of OP（VISA）, MULTOS)	Not Supported
Notes	**It will be applied to Field Test Under Another National IT Project**	Credit Card Transaction Card in Japan	NTT Phone Cards JR Train Tickets

Roadmap of Proximity Card



★Std. Card
32bit CPU
ROM 128KB
EEPROM 64KB
RAM 12KB
Public Key Crypto-
Coprocessor

★Mini Card
16bit CPU
ROM 50KB
EEPROM 32KB
RAM 4KB
Public Key Crypto-
Coprocessor

Deployment Program :
Field Test of the New Generation
Smart Card Systems for Public
Applications in Selected 21 Areas