

Japan–EU collaboration to establish an interoperability of smart IC card system

Nagaaki OHYAMA

Imaging Science and Engineering Laboratory
Tokyo Institute of Technology

Why do we need smart cards ?

Because we believe

- smart card will be the key device, which enables us to keep safely and efficiently our digital data or information that are indispensable for our social activities.

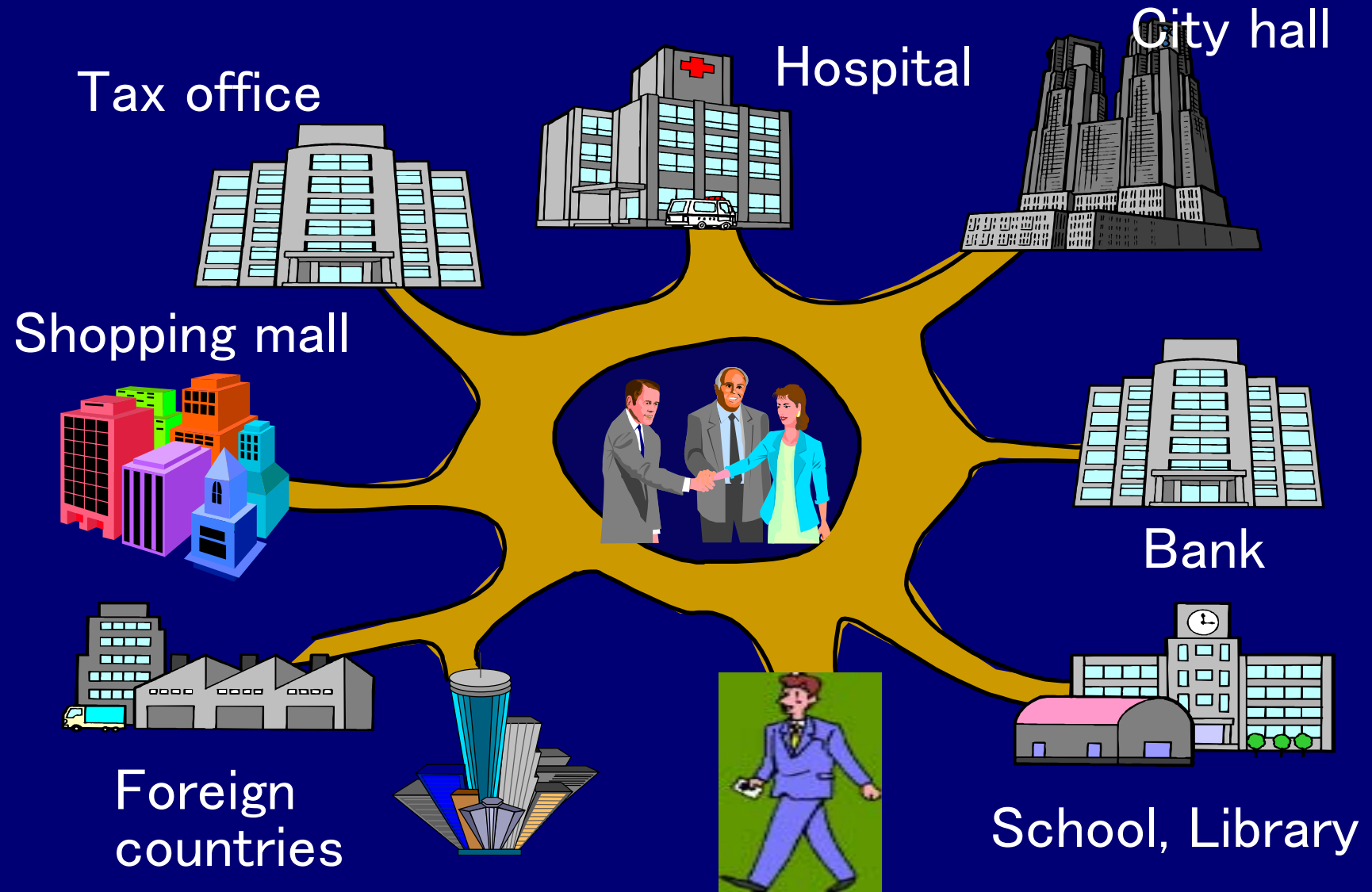
But, we do not think

- smart card at present is infrastructure
- smart card is as convenient as mobile phone
- smart card reaches the mass production level

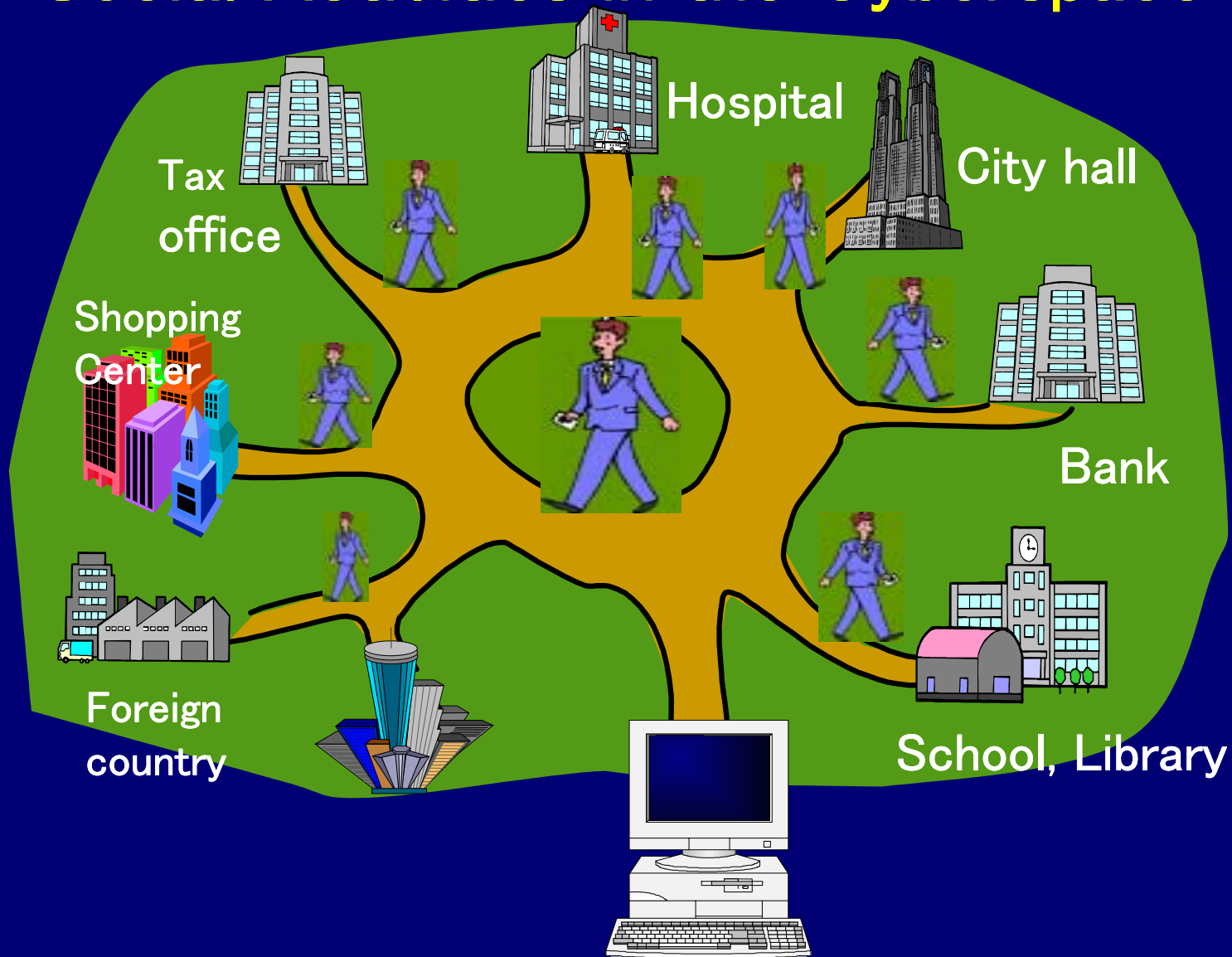
What will happen in the information society ?

- * In the information society, our social activities will be expanded into the cyberspace in addition to the real space.
- * Selection of the spaces should be definitely up to users.

Social Activities in the real world



Social Activities in the Cyberspace



What should we do for the information society ?

- Everything that we need for social activities should be electronic so that their functions can be digitally performed.
 - Concrete object
 - Money ⇒ Electronic Money
 - Signature ⇒ Electronic signature etc.
 - Intangible asset
 - Right ; Election, medical care, etc.
 - Duty ; Tax, education, etc.
- Entry points into the cyberspace had better be everywhere.
 - Computer, Kiosk, Public phone, home electronics etc.
 - **Multipurpose smart IC cards ⇒ Cyber space passport**

} **citizenship**

Hospital

Health insurance number patient ID etc.
name address sex birthday etc.

City hall

Resident ID etc.
name address sex birthday etc.

Tax office

Tax payer ID etc.
name address sex birthday etc.

Information necessary
to receive services
and
to show licenses

Common Information
(name, address, sex, birthday)

Public sector : Services are subject to the constitution, regulation etc.

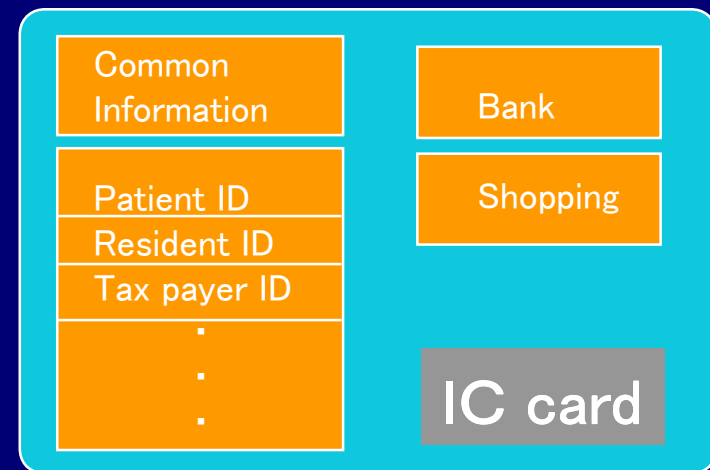
Bank

account number account type etc.
name address sex birthday etc.

Shopping

credit card number customer ID
name address sex birthday etc.

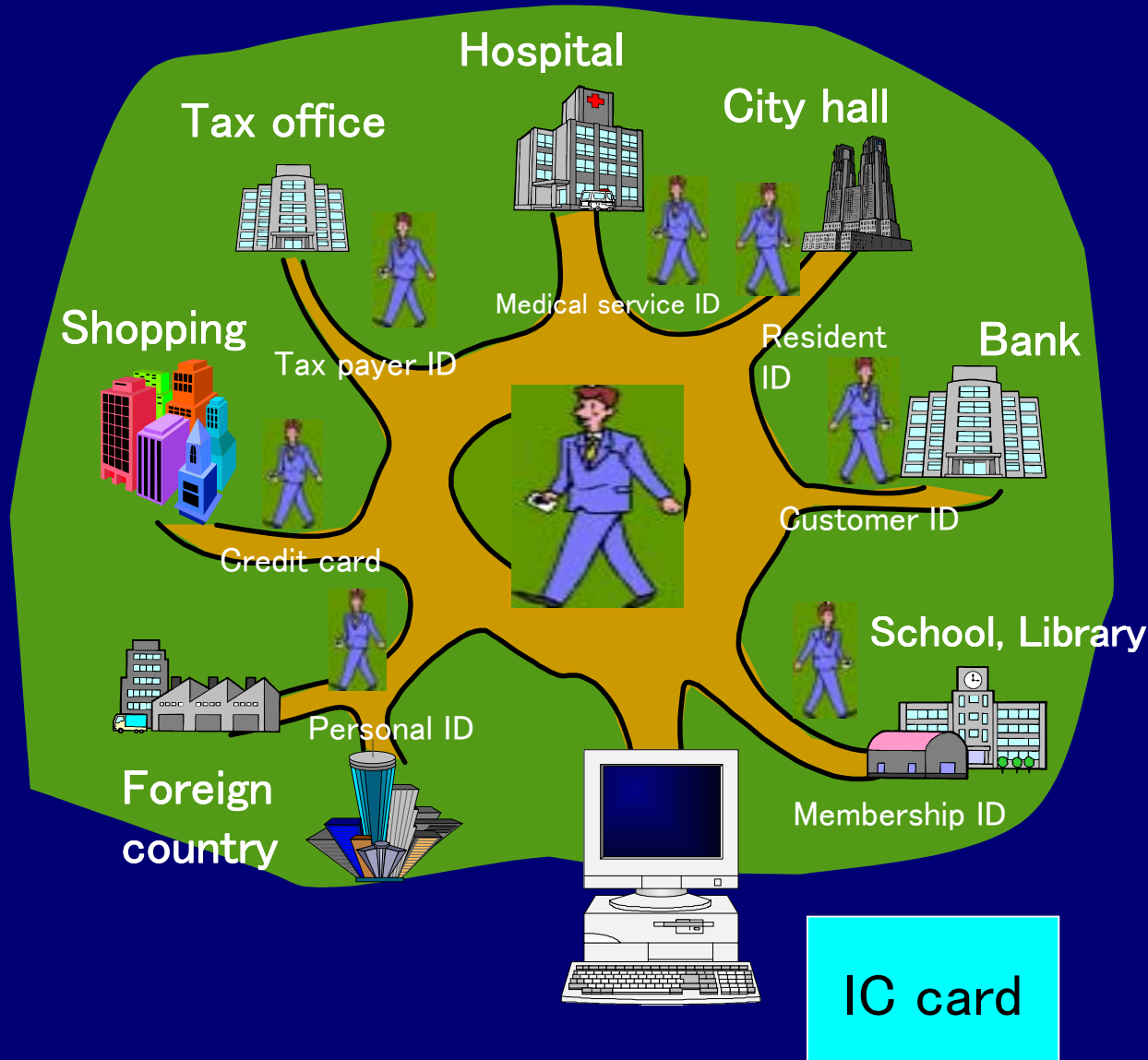
Cyberspace passport



If possible

Private sector : Services are provided on the contract basis.

Social Activities in the Cyberspace



In the public sector

Hospital
City Hall
Tax office
etc.



Passport
for public services

In the private sector

Bank
Shopping Mall
etc.

Concept of Cyber-Passport

- * Cyber-passport is an electronic identification to be used to check the cardholder's citizenship.
- * Cyber-passport is originally issued by the government on request when people want to receive electronic government services in the cyberspace.
 - ⇒ Resident registration law has been revised
- * Cyber-passport may also record services that the holder receives and licenses that the holder has.
 - ⇒ Multiple application should be supported
- * Cyber-passport could also support electronic signature or inkan.
 - ⇒ PKI should be supported

Note: the number of cards and the selection of the services are totally up to the user's choice

Japanese government's actions relating smart IC card systems

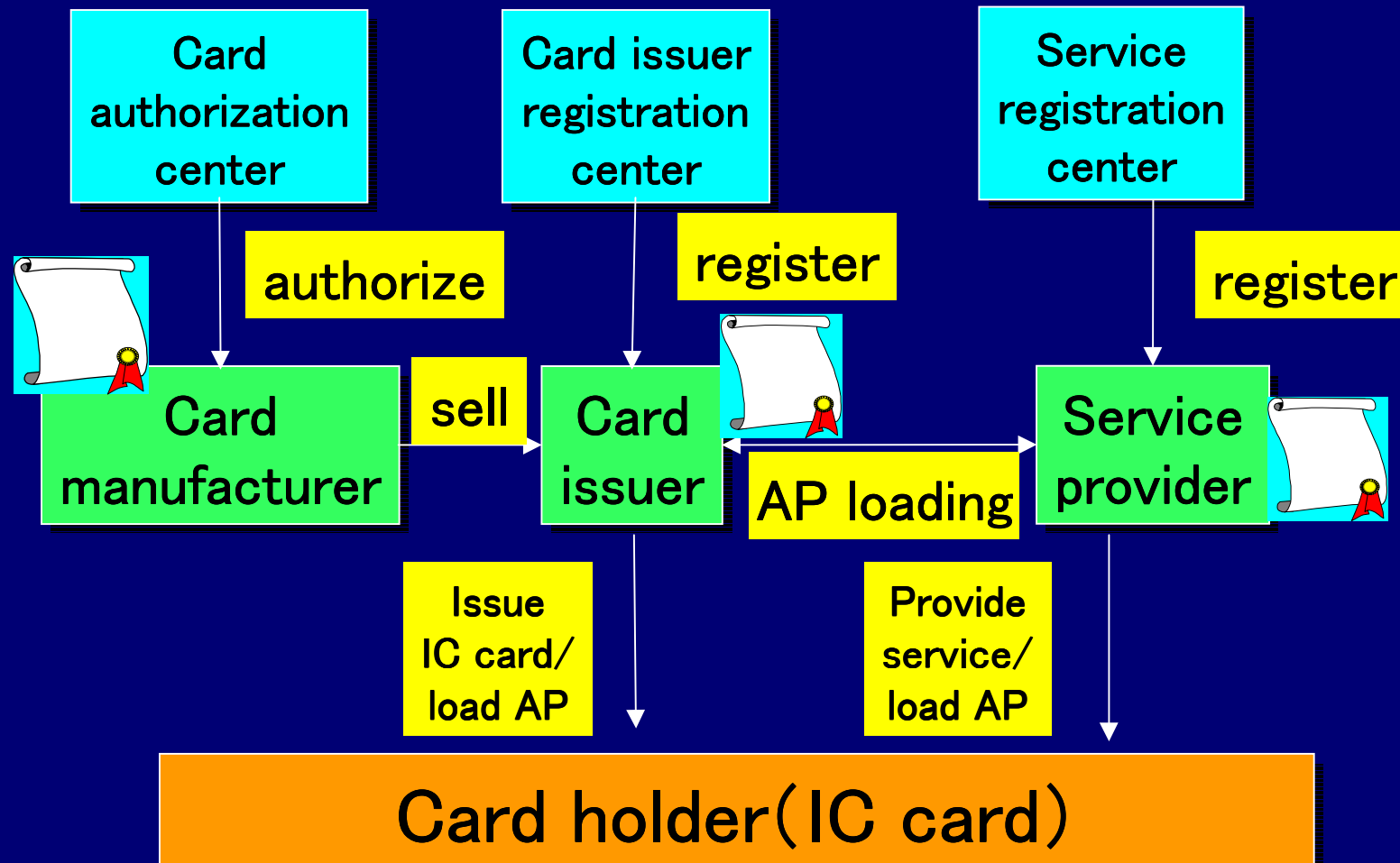
- Electronic signature law from 1st of April, 2001
- Revised resident registration law from Aug., 2002
 - ⇒ Personal Identification for public sector's use
 - ⇒ 10–50 million people are highly expected to have smart IC card from Aug., 2003, if it becomes convenient to the card holder
- Prior to the resident card, 1–3 million cards will be procured by the end of 2001
- Smart IC card is officially defined as an interface between e-government and individual
- **Japan will procure a huge amount of smart card**

Smart card as an infrastructure

Common understandings

- Infrastructure is not a dedicated system
 - ⇒ **Multipurpose** card system
- Infrastructure should be beneficial to everybody ; user, service provider, vender, etc.
 - ⇒ **Convenient**, low cost by **cost share**
- Through the mass production we can reduce the production cost

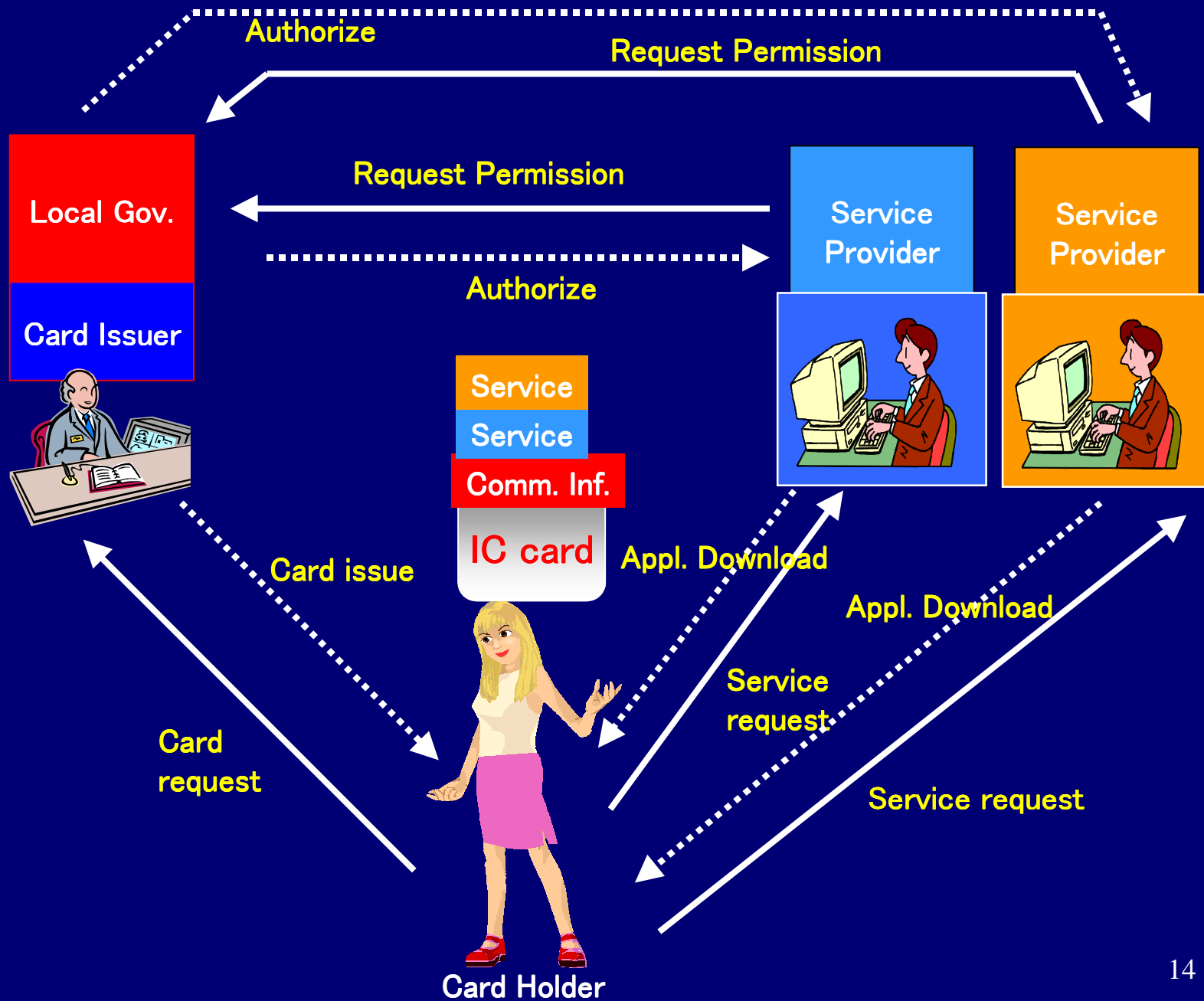
Business model for Multi-application card



Cost share becomes possible

Benefits to the players

- Card Holder
 - Selection of the services → optimized card
 - Most convenient
 - Less number of cards
- Card Issuer
 - Reimbursement of card cost
 - Card holders' satisfaction
- Service Provider
 - Reduction of the initial installation cost
 - High security card at low cost



Requirements to the smart card system

- Multi-purpose
 - Users can select services as they want
 - The number of cards is up to the users
- Asymmetric encryption algorithm
 - Electronic signature
- Contact-less interface
 - Reduction of maintenance cost
 - Combination of different cards; Cf. ownership
ex. Bank card and ID card

Requirements to the smart card system subject to government procurement (proposal)

1. ISO compliant
2. Technical neutral → independent of CPU, OS, language
3. Interoperability
 - Common information ; low level interoperability as data carry use
 - Card and R/W for contact-less interface
4. Multi-purpose
 - Completely independent ; concept of APDU
5. Asymmetric encryption algorithm
 - Objective assessment ; IPA security center
6. High security of card, PP ; ECSEC

Process to the procurement

- List up all possible cards by asking the venders on a voluntary basis
- Organize expert groups to meet the requirements
- Achieve laboratory test to check the interoperability
- Make a list of cards subject to the procurement
- Local government procures IC card among products in the list considering needs, price and performance such as processing speed and memory capacity

We ask a collaboration to European side in the steps 1–

4.