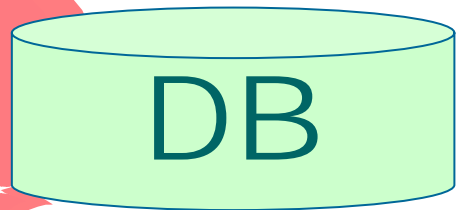# Aspects of Privacy for RFID Systems

Sozo INOUE

System LSI Research Center,
Grad. Sch. Information Science & Electrical Engineering,
Kyushu Univ., Japan

SLRC

An RFID System is...

- **Unique nouns** to every person, and any objects in the world by IC cards & RFID tags
- Automatic correspondence between name (virtual) and entity (real) Automatic updates of the states, locations

DB

Network

RFID tags (with ID**s**)

Readers

Wireless Communication
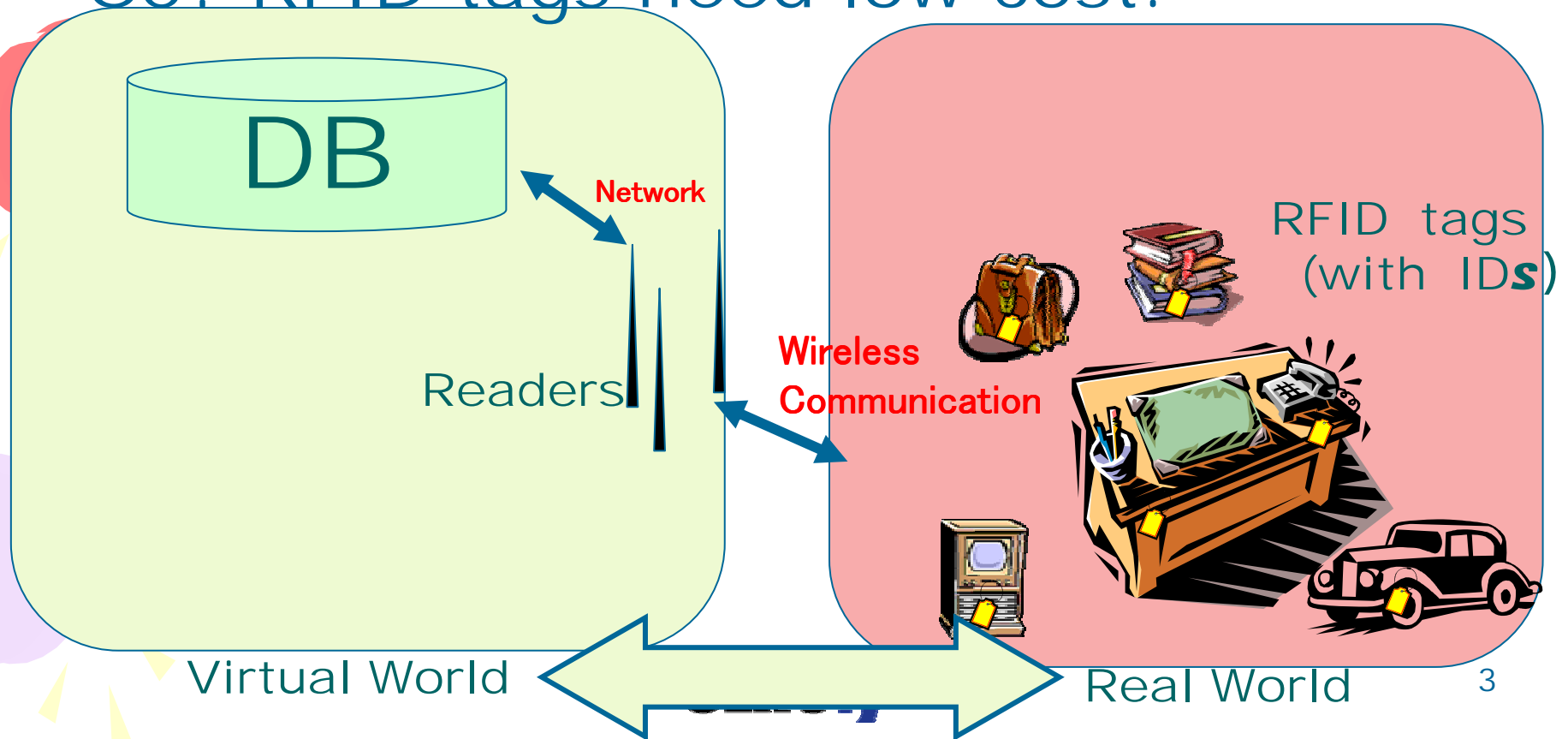
Virtual World

Real World

2

What is special privacy in RFID systems?

- Virtual world: Merely the same as the conventional information systems.

- <u>So? RFID tags need low cost.</u>

DB

Network

Readers

Wireless
Communication

RFID tags
(with ID**s**)

Virtual World

Real World

RFID tags on nameplates at a conference
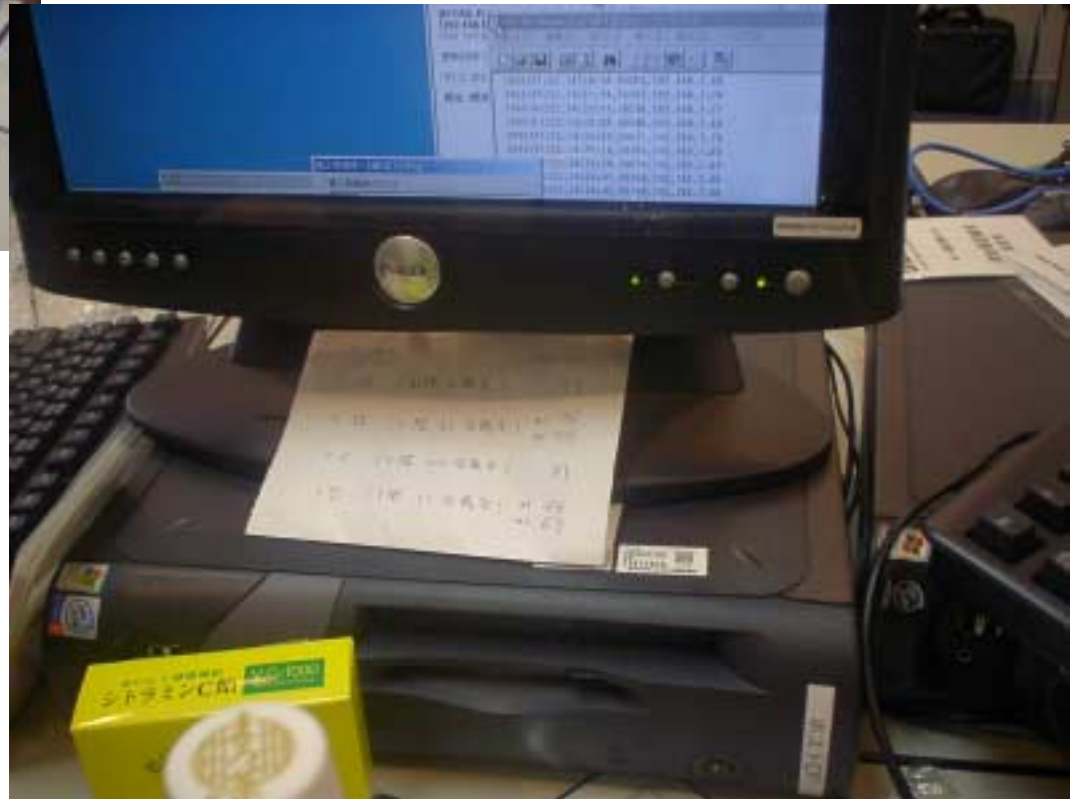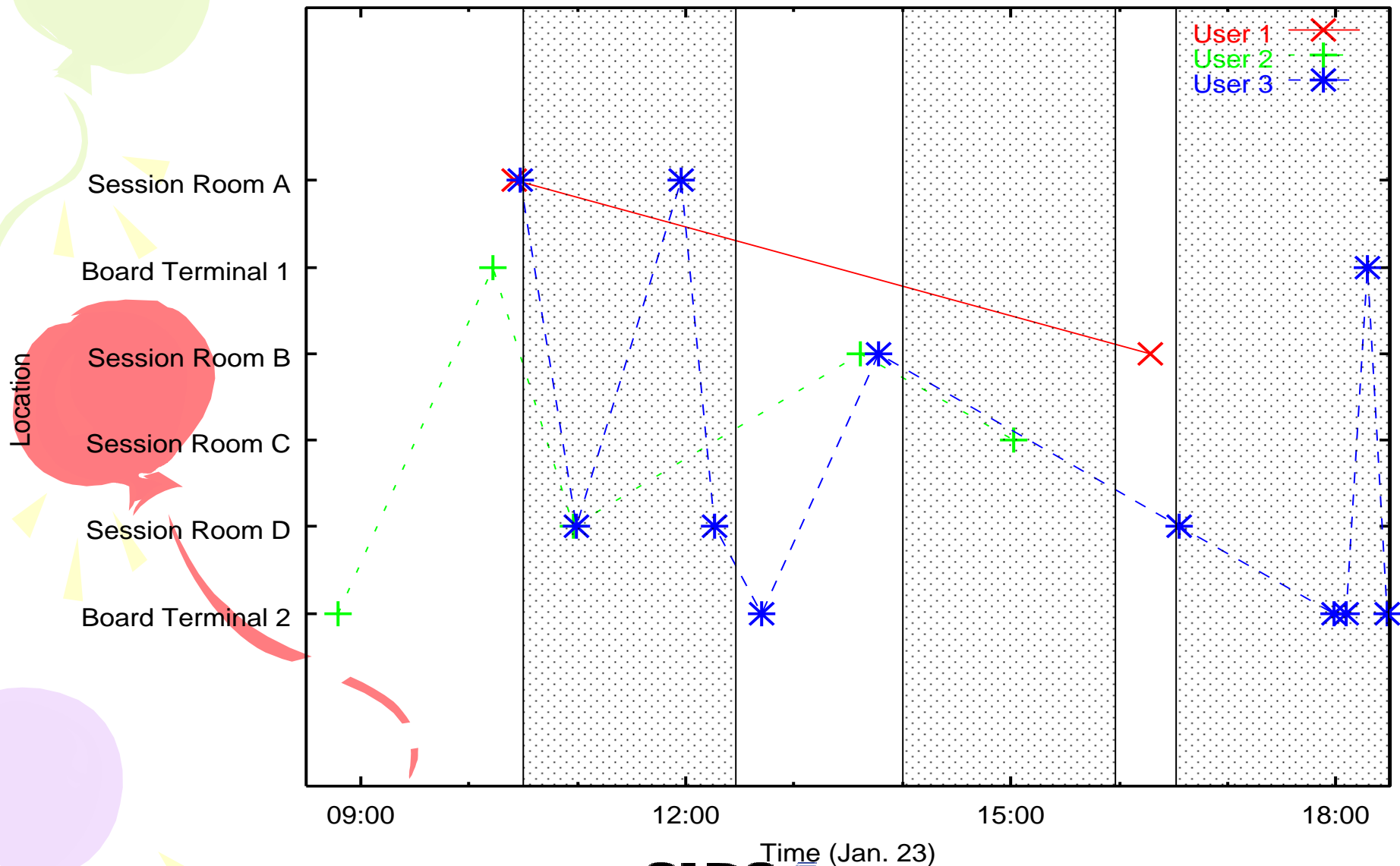
Session Entrance

Board Personalization

Poster

Banquet

Indeed, at the backstage,

Can trace personal behavior!!!

Unlinkability

- The property that the system is not able to identify multiple accesses from a user as the same person.
    - Independent of whether the system knows who the person is (anonymity).

- [S. Steinbrecher and S. Köpsell,"Modelling Unlinkability", Workshop on Privacy Enhancing Technologies 2003.]

Suppose: Ad.: Super RFID chips which protect complete privacy!

New!
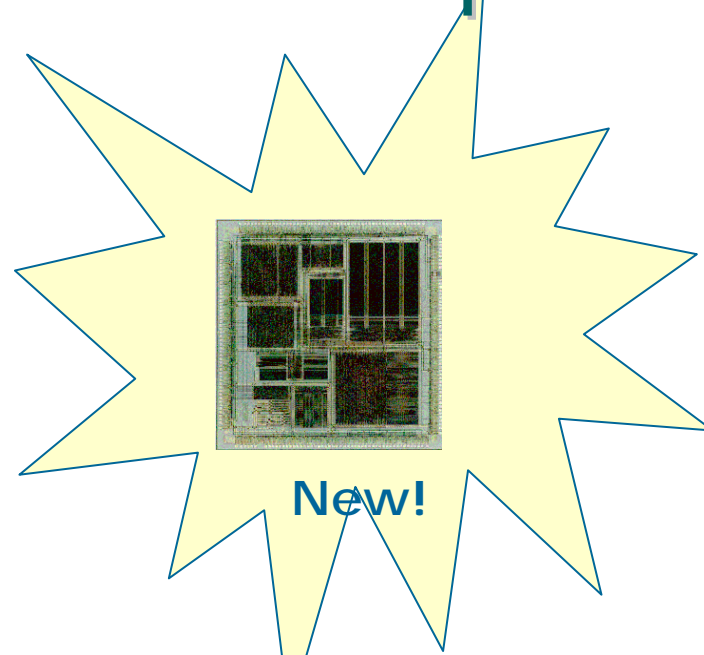
.........Really?
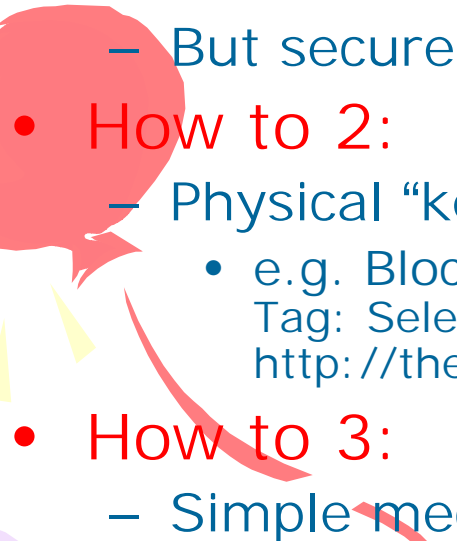
How can we believe?

→the **Visibility** of Privacy Protection!

How? Visibility?

- Fully-automatic approach is not appropriate.
- How to 1:
  - Users can have something to do in a way they can trust,
  - But secure by default
- How to 2:
  - Physical "key" device to control the privacy.
    - e.g. Blocker tags: [A. Juels, R. Rivest, M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", http://theory.lcs.mit.edu/~rivest/, (2003)]
- How to 3:
  - Simple mechanism which is easy to understand.

Proposal of RFID marks

- [H. Takagi, "ユビキタス社会を支えるICタグの現状と課題", *IC Card World 2004*]
  - Red: ID and personal information
  - Yellow: ID
  - Blue: No fixed ID
  + Plus:
  - Communication range,
  - Security level,

Our research

Technique for controlling **unlinkability**
while ensuring **visibility** to users.

- 3 approaches:

1. User oriented ID definition

    [S. Inoue, et al., ``Privacy in the Digitally Named World with RFID Tags'',
    Workshop on Socially-informed Design of Privacy-enhancing Solutions
    in Ubiquitous Computing, 2002]

2. Physical distribution of IDs

    [S. Inoue, et al, ``RFID Privacy by User-controllable Uniqueness'', RFID
    Privacy Workshop, 2003]

3. Trusted third party

Related work

- [S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, ``Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems'', Int'l Conf. Security in Pervasive Computing, 2003]

- [M. Ohkubo, K. Suzuki, S Kinoshita, "Cryptographic Approach to a Privacy Friendly Tag", RFID Privacy Workshop, *2003*]

- [A. Juels, R. Rivest, M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", http://theory.lcs.mit.edu/~rivest/, (2003)]

1ˢᵗ Approach

Combination of ROM and rewritable memory on an RFID tag

- globally unique ID on the ROM

- localized ID on the rewritable memory (EEPROM, FRAM)

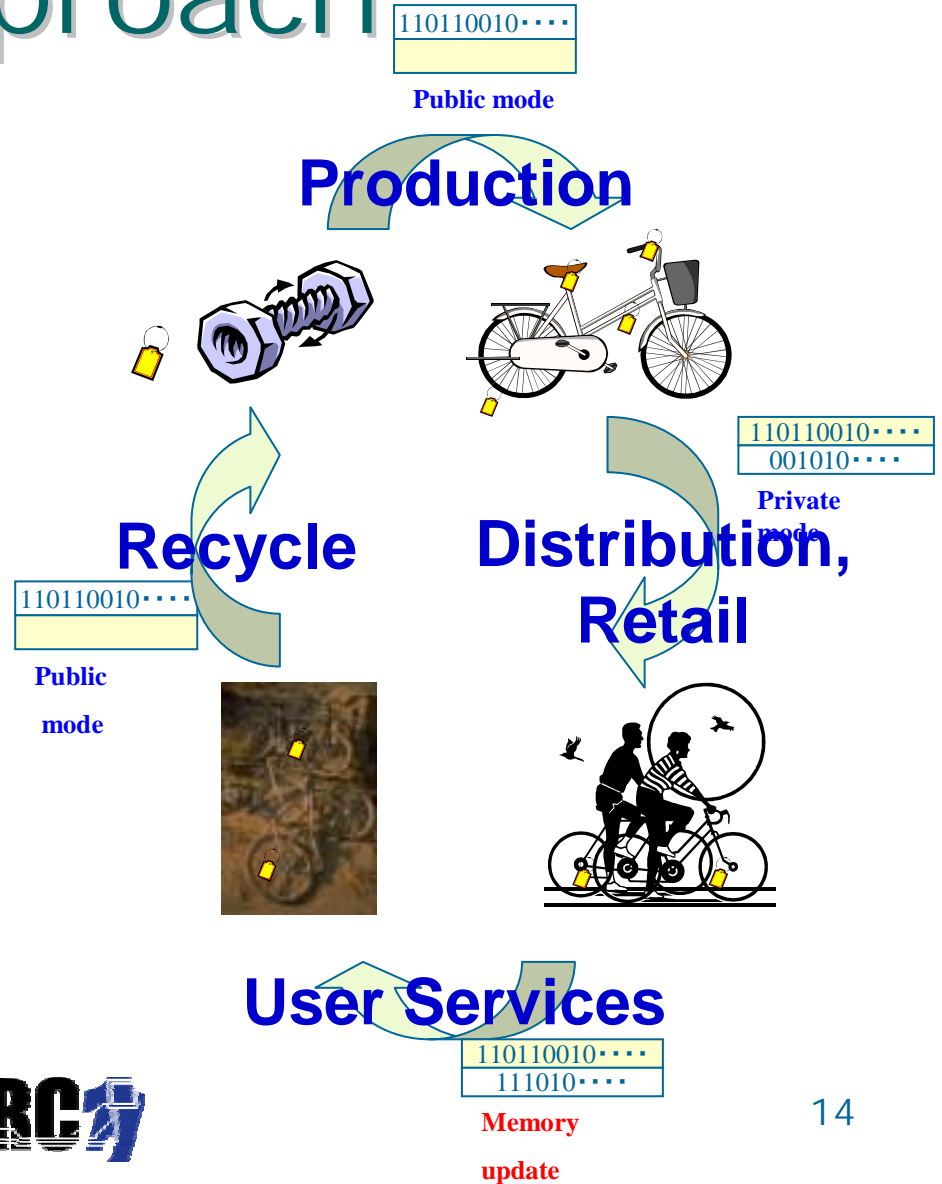- Users cannot access the ROM when a private ID is set.

ROM
Rewritable

110110010····

Public-ID mode:

ROM
Rewritable

110110010····
001010····

Private-ID mode:

13
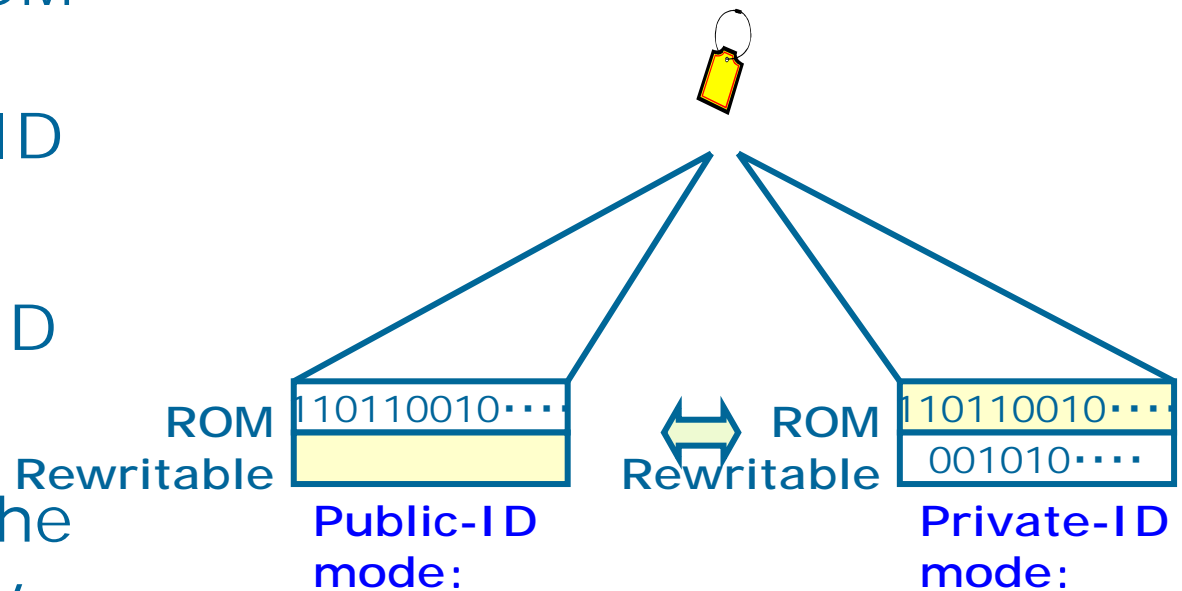
1ˢᵗ Approach

- Public-ID mode:
  - Any users can identify the product.
- Private-ID mode:
  - The owner **decides** the private ID value.

Only **the owner** can identify, and can relate the private ID and the public ID.

Avoids Linkability by visibly changing the private ID.

Low cost than implementing crypto.
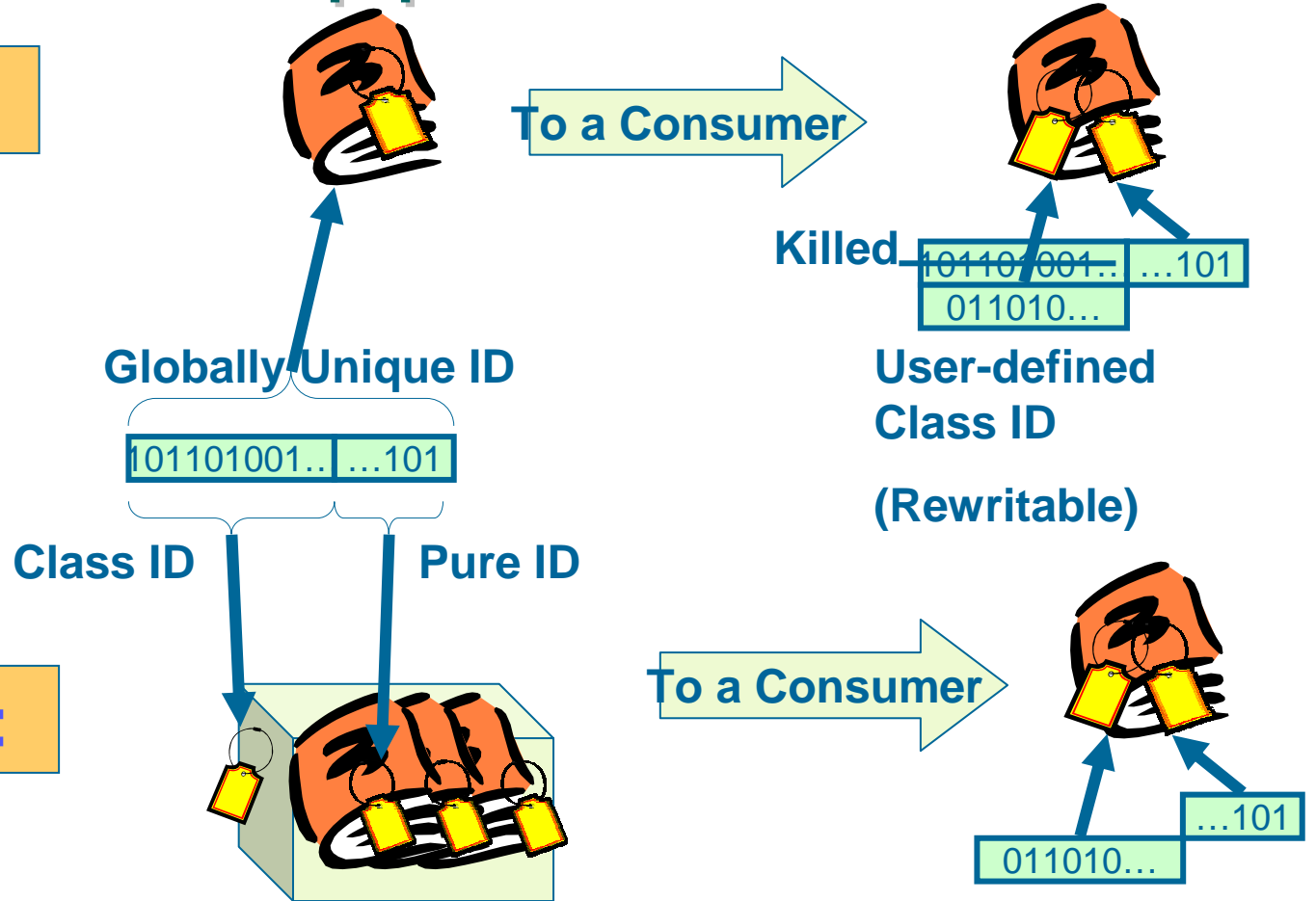
Production
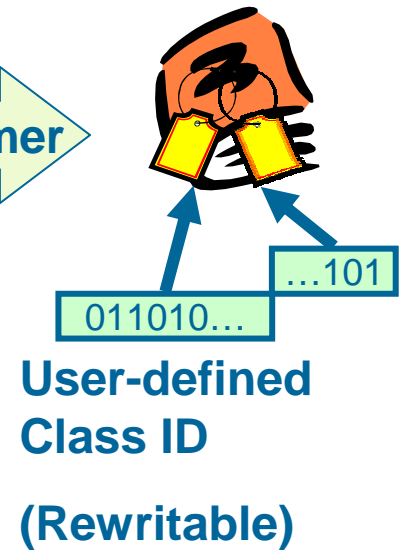
110110010····

Public mode

110110010····
001010····

Private mode

Recycle

110110010····

Public mode

Distribution, Retail

User Services

110110010····
111010····

Memory update

14

2nd Approach

Option 1:

To a Consumer

Killed `101101001..` | `...101`
`011010...`

Globally Unique ID

`101101001..` | `...101`

User-defined Class ID

(Rewritable)

Class ID　　　　**Pure ID**

Option 2:

To a Consumer

`...101`
`011010...`

User-defined Class ID

(Rewritable)

Class ID: the field related the object type.

Pure ID: the field to identify the object in the type.

SLRC

15

2nd Approach

- The **owner can** identify,
- **Other users cannot**, from user-defined Class ID and Pure ID.
- The users **who can see the object** may identify: on-site identification
  - A repairer can know the product type (sometimes from the barcode) and identify from the Pure ID.
- Privacy is protected **by default** (without the owners' labor)
  - Object cannot be identified only by Pure ID.
- Privacy is **visible** by physically-separated RFID tags.
- **No more** special RFID tags.

SLRC

3rd approach: PID

- Originally designed to fit smart cards.
- A scheme for preventing **linkability between multiple services** gathering access logs.

PID: Very long ID sequence for each RFID tag
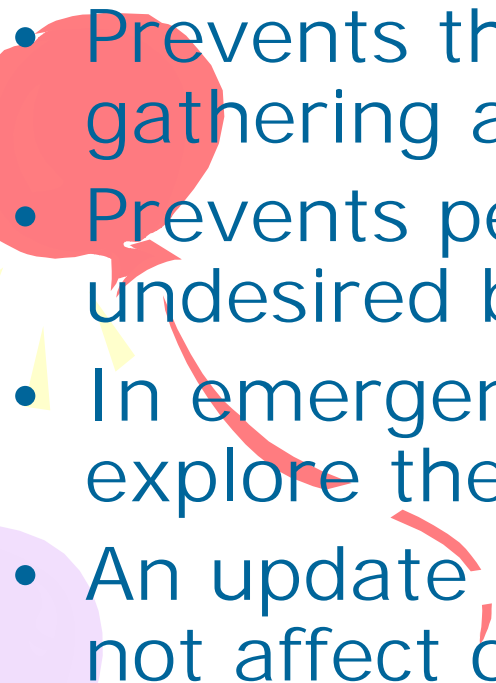
	Service **a**	Service **b**		
RFID tag 1	a1	b1	c1	
RFID tag 2	a2	b2	c2	
RFID tag 3	a3	b3	c3	
RFID tag 4	a4	b4	c4	
RFID tag 5	a5	b5	c5	

PID: Long ID sequence for an RFID tag

Issuer

PID

RFID

PID

Identification

SubPID

Service Provider

RFID

19
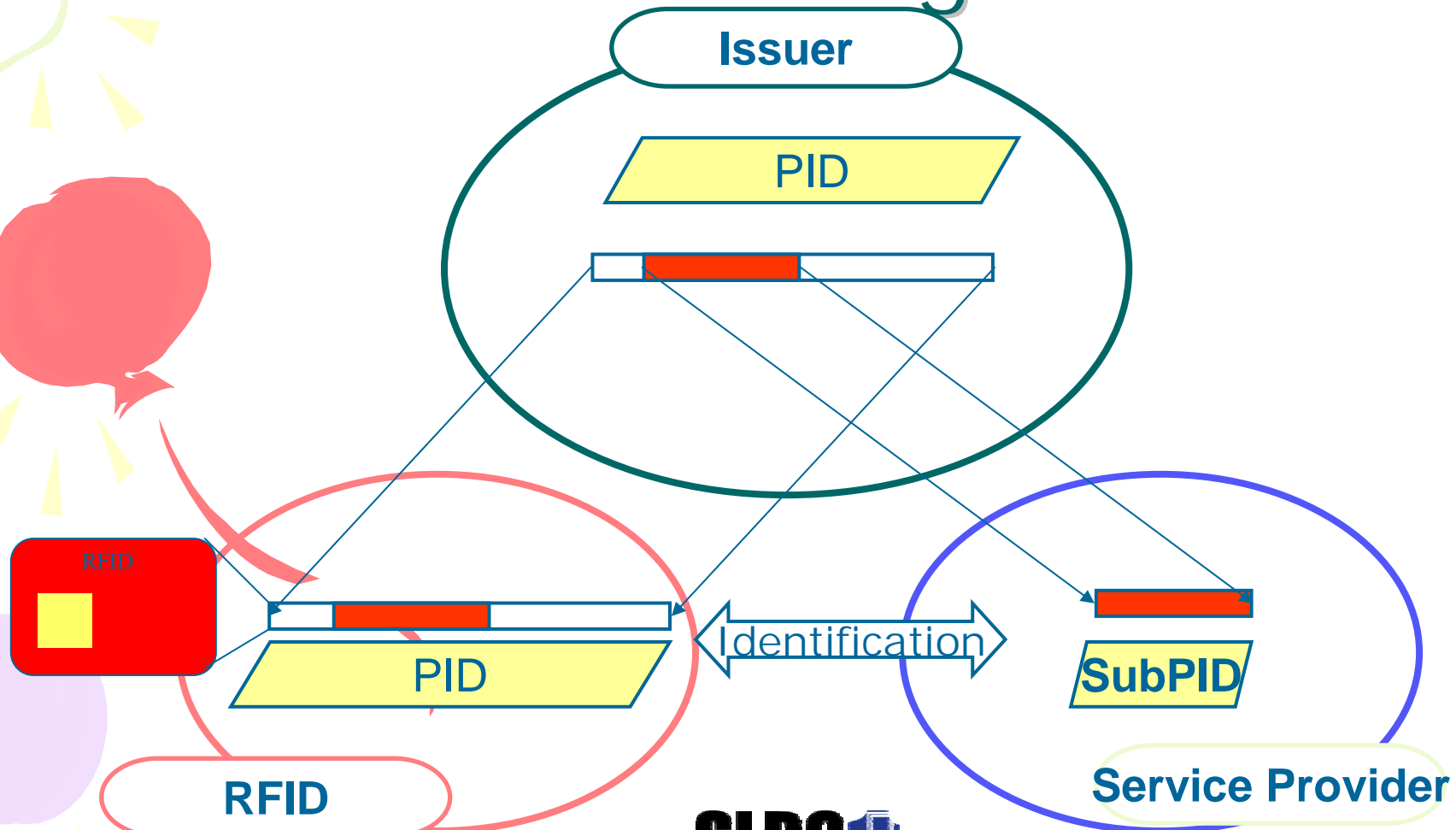
3rd approach

- Intends to use single RFID for multiple services

- Prevents the **linkability between services** gathering access logs.

- Prevents personal information integration undesired by users

- In emergency, the issuer can integrate ore explore the personal information.

- An update of a SubPID for a service does not affect other services.

Experiments in Kyushu Univ.

- Experiments for RFID Systems in middle-sized population:
- **Campus Card** with **PID**
  - IDs for students, staff with multiple usage
  - Keys to buildings, facilities, and parking
  - Access control to campus information
  - E-money
  - E-administration
  - Services to Students
  - NTT, Panasonic etc.
- **RFID Tags** to Equipments
  - Library
  - Equipments management
  - Hazard identification
  - Moving to the new campus

New campus of Kyushu University Open in 2005.

Concluding Summary

1. The **Visibility** of Privacy Protection

2. ID Localization Approach
    1. Combination of ROM and Rewritable memory
    2. Physical-ID Separation
    3. Sub-ID for each service
    -   Not necessarily cryptographic.
    -   Visible to the owner and Low Cost.

3. Future Work:
    -   System level solution for ID conflicts:
        -   Technology for **Semi-AUTO-ID**:
            -   e.g. Location + ID = Unique
    -   2nd approach: how to **associate** a Class RFID and a Pure RFID when there are multiple ones in a range?