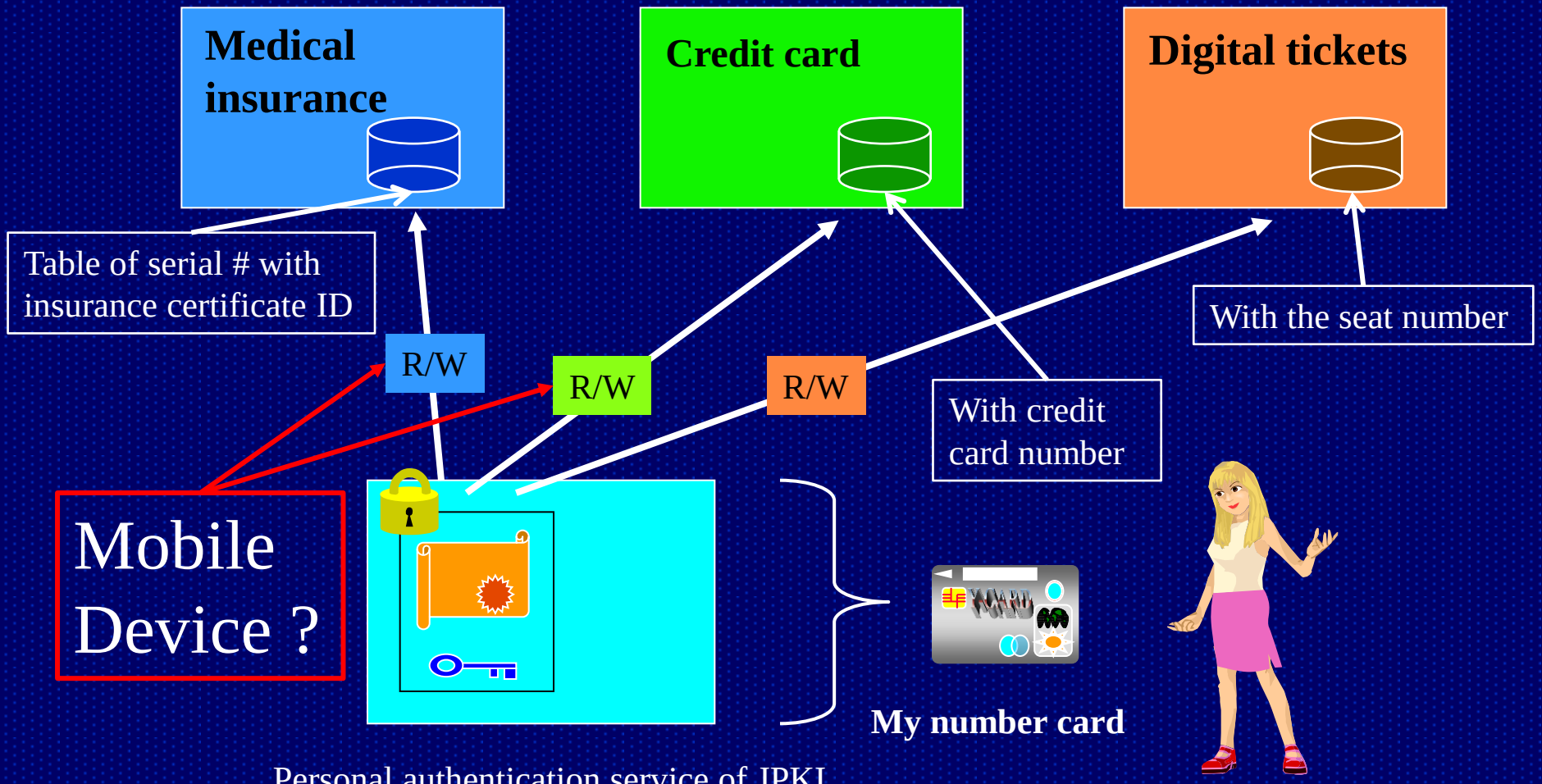
Pragmatic approach to PHR in Japan

ASIST（Advanced research center for Social Information Science and Technology）
Institute of Innovative Research
Tokyo Institute of Technology

Prof. Nagaaki OHYAMA

Multi-application using my number card



Sample of e-ID card under practical use

Front side

Back side

New e-ID card

- We call the new e-ID card “my number card”
- My number card is based on the my number act
- My number card has begun to issue since Jan., 2016
- During last eight months more than 11M cards are requested by residents including foreigners
- Budget for 30M card within this fiscal year
- My number card supports both digital signature（non-repudiation）and personal authentication（log in）
- Personal authentication supports PIN-less scheme like sign-less

Mykey kun

PIN-less scheme（1）

- In case of emergency, for example, when the card holder is unconscious, PIN-less scheme enables the ambulance crew to make an access to the emergency data of the card holder
- PIN-less scheme is supported by my number card as a default function
- PIN-less scheme uses the mutual authentication process; prior to the internal authentication（the server checks the card）, external authentication（the card checks the server）is carried out in place of PIN
- This mutual authentication uses PKI and the field（device or organization）code
- The field code changes the response to the server to distinguish the correct response from others; other field or device, or verified PIN

PIN-less scheme（2）

- When we use PIN-less scheme, both the server and the card digitally and automatically sign the transaction data used for mutual authentication
- Together with time stamp, the signed transaction produced through the PIN-less scheme could be an evidence to tell which hospital provides the healthcare service, whose card is used and when ⇒ audit trails
- Keeping copies of these records tells us the location of our healthcare records in chronological order

  Note: all records are kept by the hospital by regulation for 5 years at least
- For the records after 5 yeas we need to study most effective way to keep and manage such as a summary including key images and lab data

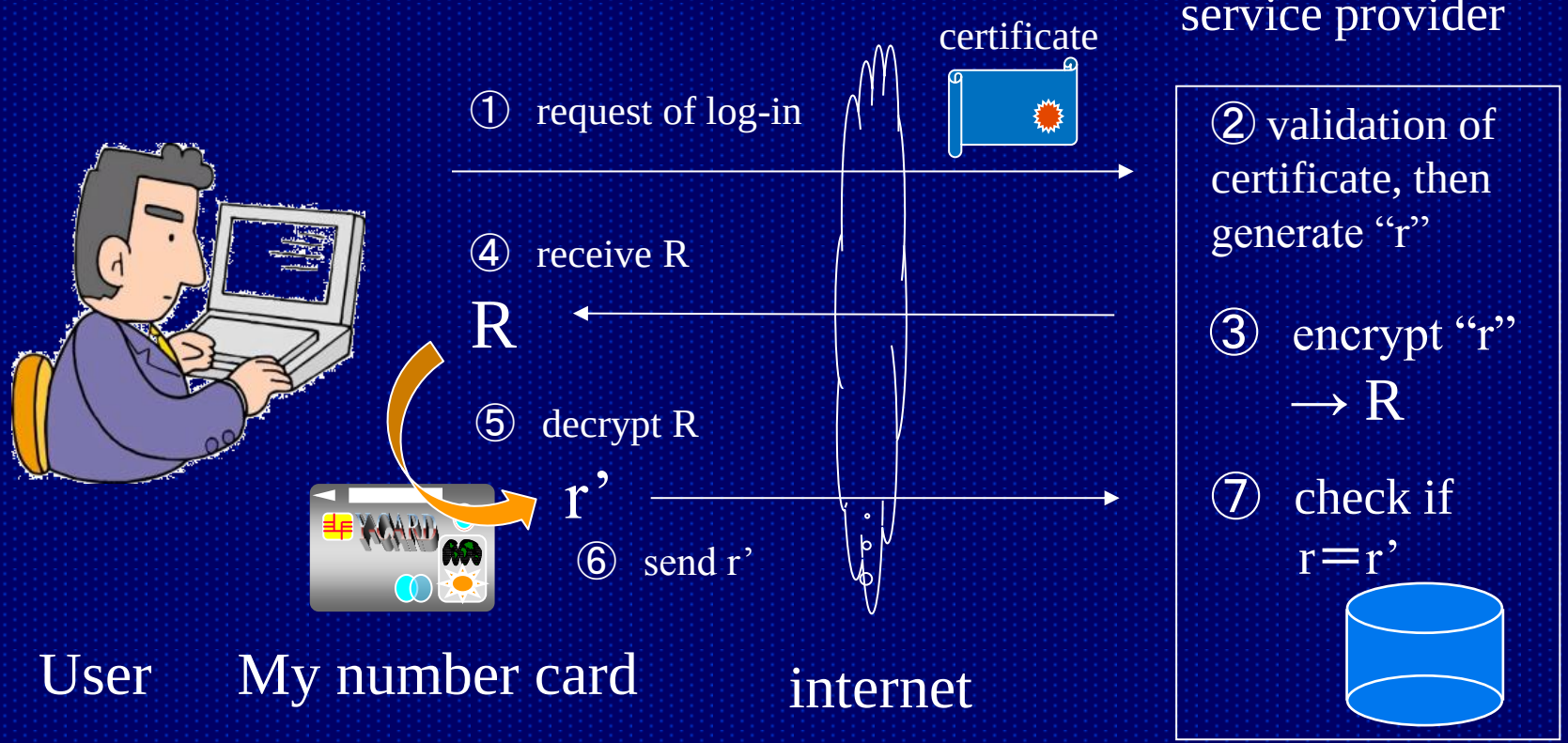
New infrastructure in healthcare field

- PIN-less scheme will be practically used to check the validity of the medical insurance from April, 2018 ⇒ we can collect the signed transaction（link data）to tell when and where we received healthcare services
- HPKI card is also used for digital signature with healthcare license such as medical doctor, pharmacist and dentist
- Dedicated network for healthcare information exchange ⇒ for competitive market and security, IX is planned to be constructed connecting local networks currently under use in healthcare field; supposed to be available from April, 2018

Summary

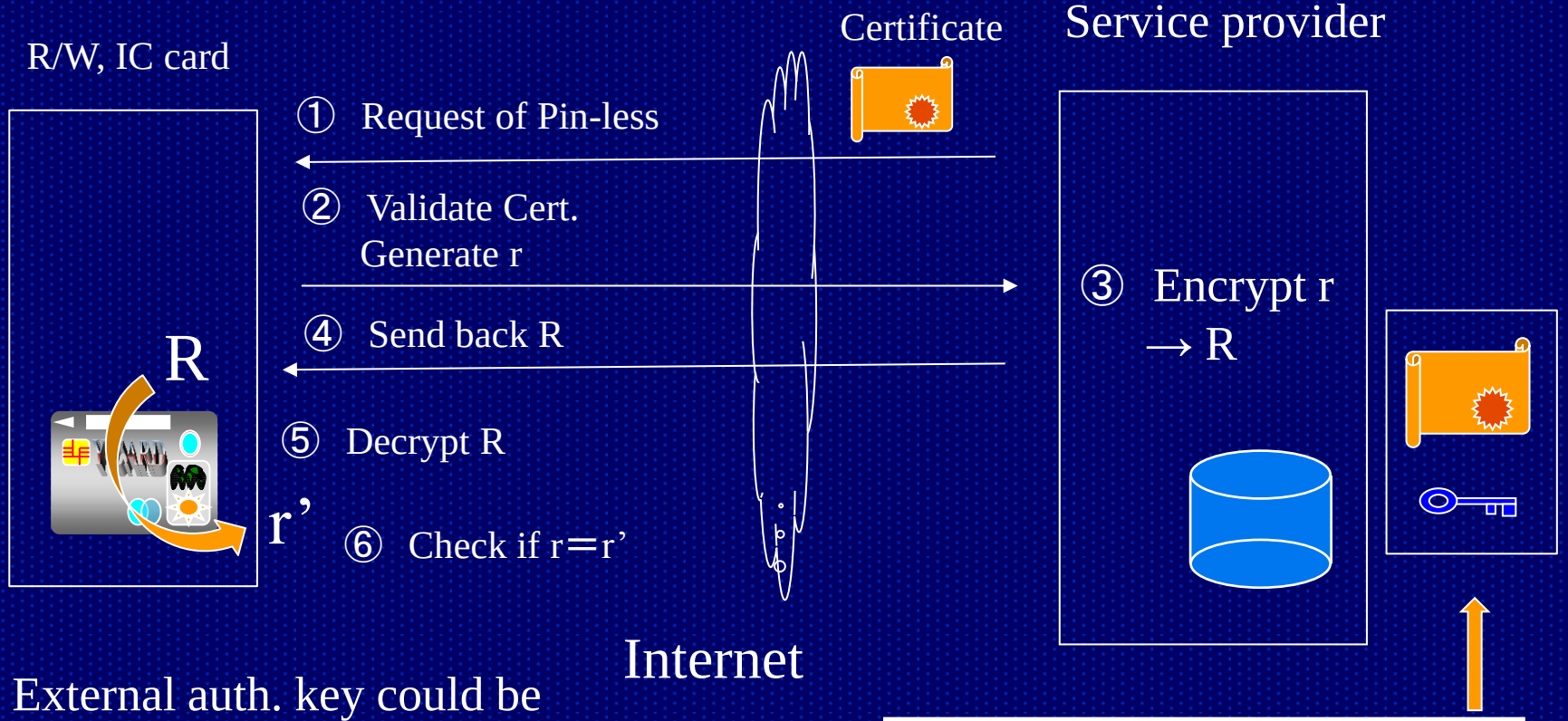
- My number card, HPKI card and IX inside the healthcare field will be widely available and practically used from April, 2018
- Together with the time stamp, PIN-less scheme produces an evidence to tell when and where we receive healthcare services
- Copies of the singed transaction could form PHR
- PHR will be launched on the voluntary basis
- My number card could be also used as a credit card for payment
- My number card entitles you to receive healthcare services whenever and wherever necessary in Japan, because of e-ID

Personal authentication service



- This certificate uses pseudonym
- PIN is required

External Auth. in place of PIN



- External auth. key could be kept by Intelligent R/W
  → Mobile device☐

- PKI for Pin-less scheme provided by J-LIS
- Certificate includes service ID