Criteria for privacy and integrity protection in Probe Vehicle Systems

Masaaki SATO, PhD
Assistant Professor, KEIO University
Graduate school of Media and Governance

Michiko Izumi, Kanae Matsui, Hiroshi Ito
Keisuke Uehara, and Jun Murai

“Basic principles for personal data protection in probe vehicle information services”（ISO 24100）

- **Basic rules to be observed by service providers who handle personal data in probe vehicle information services.**
  - This rule is aimed at protecting the personal data of probe data senders.
- **The definition of the Basic principles in alignment with the framework of the OECD guideline for personal data protection.**
  - the OECD Council in 1980 concerning guidelines governing the protection of privacy and trans-border flows of personal data
- **We have discussed the personal data protection rule**
  - The element which should standardize a Probe Vehicle System
  - For deploy Probe Vehicle System
  - For more effectual Privacy Protection Scheme

New PWI "Criteria for Privacy and Integrity protection in Probe Vehicle Information Systems"

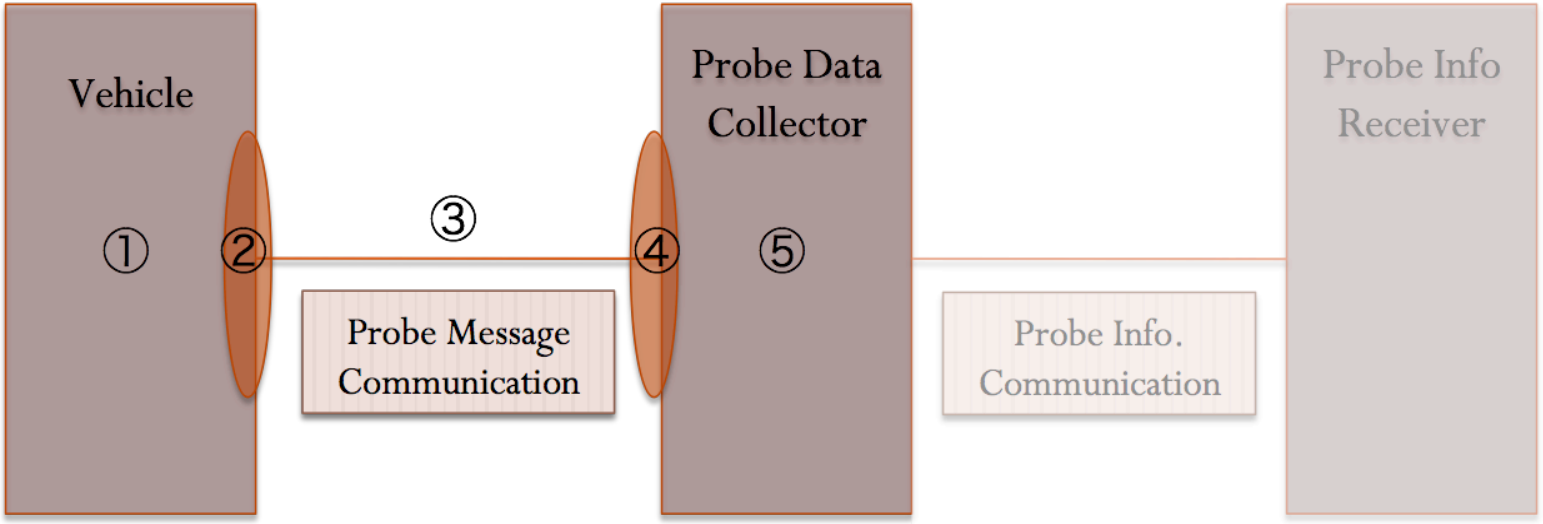
- This international standard is promulgated in order to promote utilization of the probe vehicle information by interconnection and exchange between the probe vehicle systems.
- In particular, the criteria for the characteristics of each probe vehicle system in terms of integrity and anonymity will be established. This will lead to the basis where the sender of the probe data can send information without any anxiety.

- The following deliverables are expected results of this standard
  - The information and the collaborative actions can be exchanged among various information systems.
  - Definition of security requirements as they relate to probe vehicle information systems.
  - Establishment of a common interface in which privacy and integrity are assured in probe vehicle information acquisition.
  - A scheme for protection of probe vehicle information systems in terms of integrity and privacy.

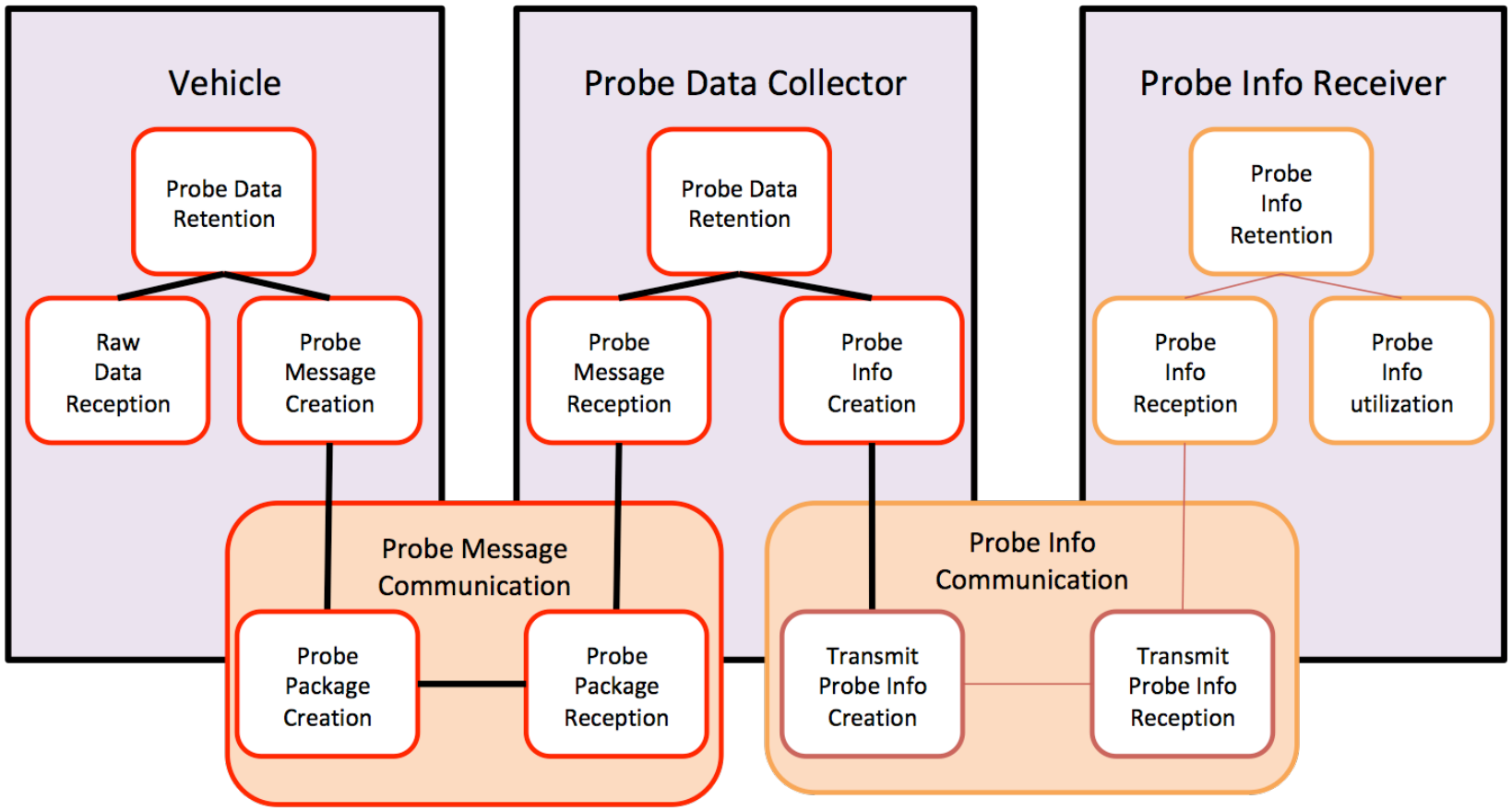
Architecture

- RA is based on 22837 and 24100
  - using RA of 24100(it has consistency 22837)

- Conceptual model
  - RA explains a logical structure of PVS
  - It is necessary for Privacy Criteria to support a existing PVS.
  - Define Context model for discuss about Privacy Criteria



Context model



Context model

- **Raw Data Reception**

  Raw Data Reception obtains sensor data based on sensors which vehicles equipped.

- **Probe Data Retention**

  Probe Data Retention creates and retains a probe data by the sensor data obtained from *Raw Data Reception*.

- **Probe Message Creation**

  Probe Message Creation creates a Probe message from more than one probe data which *Probe Data Reception* retained.

Context model

- **Probe Message Communication**
  Probe Message Communication is a communication platform for the probe message which transmits by using the probe package.

- **Probe Package Reception**
  Probe Package Reception receives the probe package transmitted via Probe Message Communication.

- **Probe Message Reception**
  Probe Message Reception receives the transmitted probe message from the vehicles through Probe Message Communication.

- **Probe Data Retention**
  Probe Data Retention stores the received probe message systematically and prepares the probe data in the form for using.

- **Probe Information Creation**
  Probe Information Creation creates probe information which was suitable for use from the probe data stored in *Probe Data Retention*.

- **Probe Information Communication**
  Probe Information Communication is a communication platform for the probe information which transmits by using a format suitable for Probe Information Receiver's purpose.

Plan for the criteria

- Our plan
  - Privacy Protection in Probe Vehicle Information System
    - Not “the whole security” on the probe vehicle information system
    - Criteria for the scheme of privacy and personal data protection.
    - “Evaluate” is not on equal terms with “Compete”
      - We cannot say that one is better than the other, since the purpose, the scale and the situations… the use cases using a probe vehicle information system may be different.
- Based on the other international common criteria
  - ISO/IEC 15408 “Common Criteria for Information Technology Security Evaluation”
- From the discussion of ISO/TC204/SWG16.3 meeting…
  - We need evaluate some “data integrity”
    - There are some techniques to hide the personal data to defect the accuracy of time and space data intentionally
    - Trade-off: data accuracy, data freshness...