DAAD Deutscher Akademischer Austausch Dienst
German Academic Exchange Service

National Institute of Informatics NII

Privacy in Business Processes

- Identifying Non-Authorized Disclosure of Personal Data to Third Parties -

Austria-Japan Workshop 2010

October 18, 2010

Dr. Sven Wohlgemuth
Prof. Dr. Isao Echizen
Prof. Dr. Noboru Sonehara
National Institute of Informatics, Japan

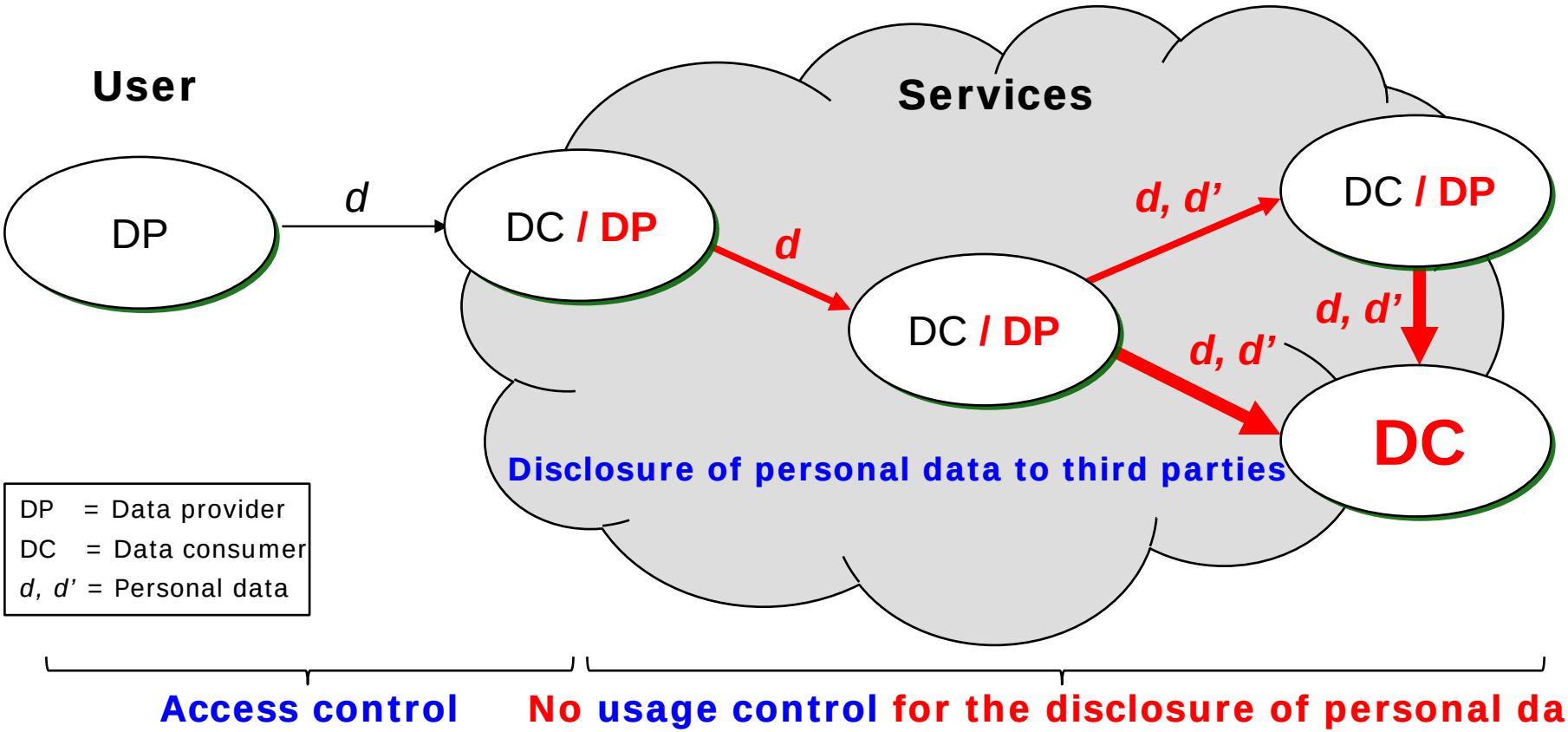
Prof. Dr. Günter Müller
University of Freiburg, Germany

Privacy and Disclosure of Personal Data to Third Parties

Privacy legislation:

„Privacy is the claim of individuals, groups and institutions **to determine for themselves**, when, how and to what extent information about them is communicated to others.“

(Westin, 1967 ➔ regulations of Germany/EU, Japan and HIPAA)



Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N. and Müller, G., 2009

Agenda

1. **Shift to a new Scenario**
2. **User becomes a Target**
3. **Usage Control by Data Provenance**
4. **DETECTIVE: Data Provenance with Digital Watermarking**
5. ***Safety* of Data and *Liveness* of Services**

1. Shift to a new Scenario

(e.g. Electronic Health Records, Gematik in Germany)

Current scenario

Patient's data is stored in many medical systems.

Each medical system is in charge of patient's data.

New scenario

Examination

Laboratory

Dentist

Patient

Hospital

Pharmacy

All data about the patient stored in one location: A central EHR

Patient is in charge of this data.

2. User becomes a Target

(e.g. Patient)

Patient "inherits" responsibility and risk.

Dishonest parties may modify or disclose personal data to 3rd parties without authorization.

- **Privacy Problem**

How can the patient control the disclosure of medical data to 3rd parties?

Different data protection legislations
(e.g. EC 95/46/EC, Japan, HIPAA)



Dentist Laboratory

Examination

Patient

Drug maker

Hospital

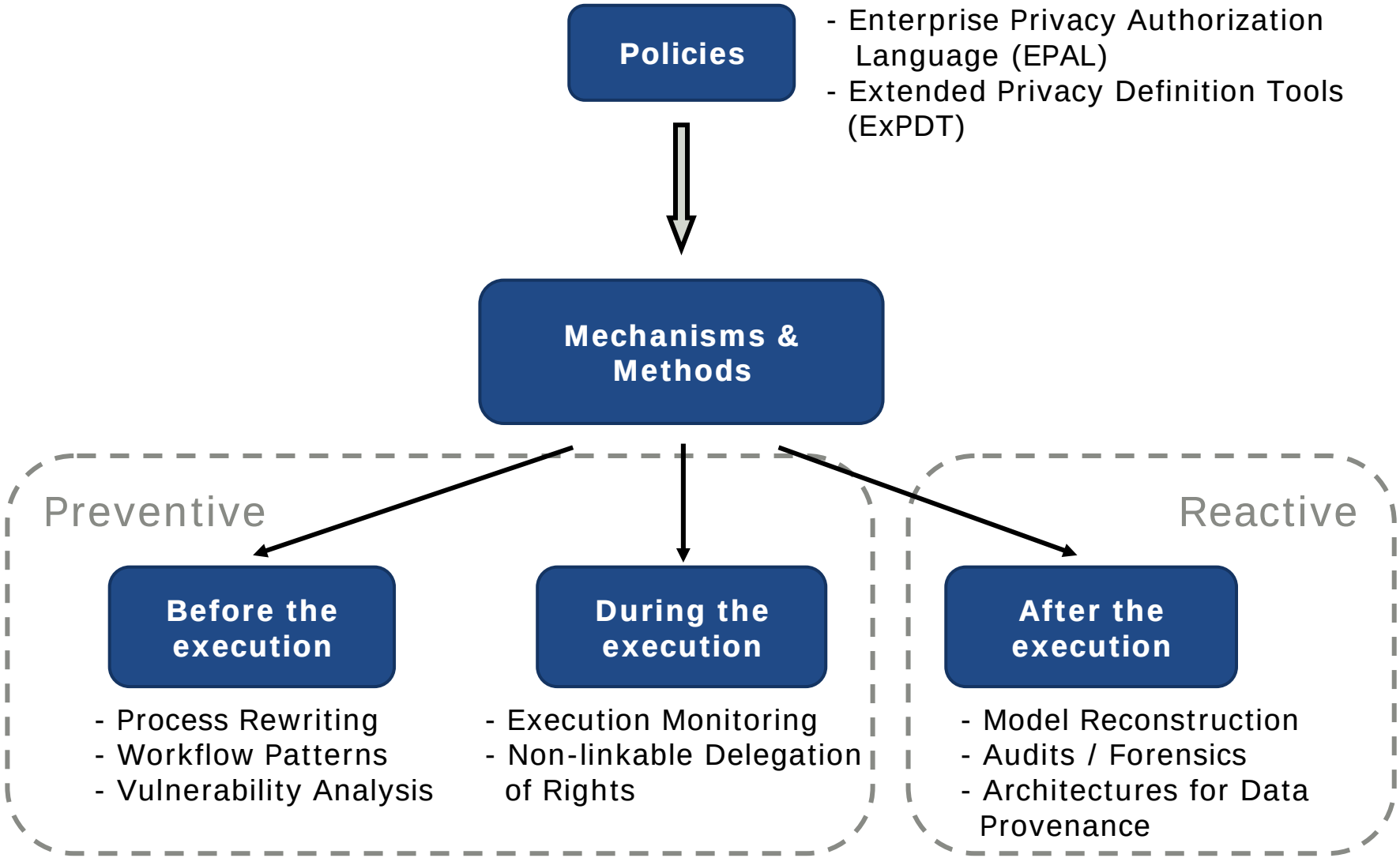
Advertiser

Pharmacy

Employer

Haas, S., Wohlgemuth, S., Echizen. I, Sonehara, N. and Müller, G., 2009

3. Usage Control by Data Provenance (1/2)



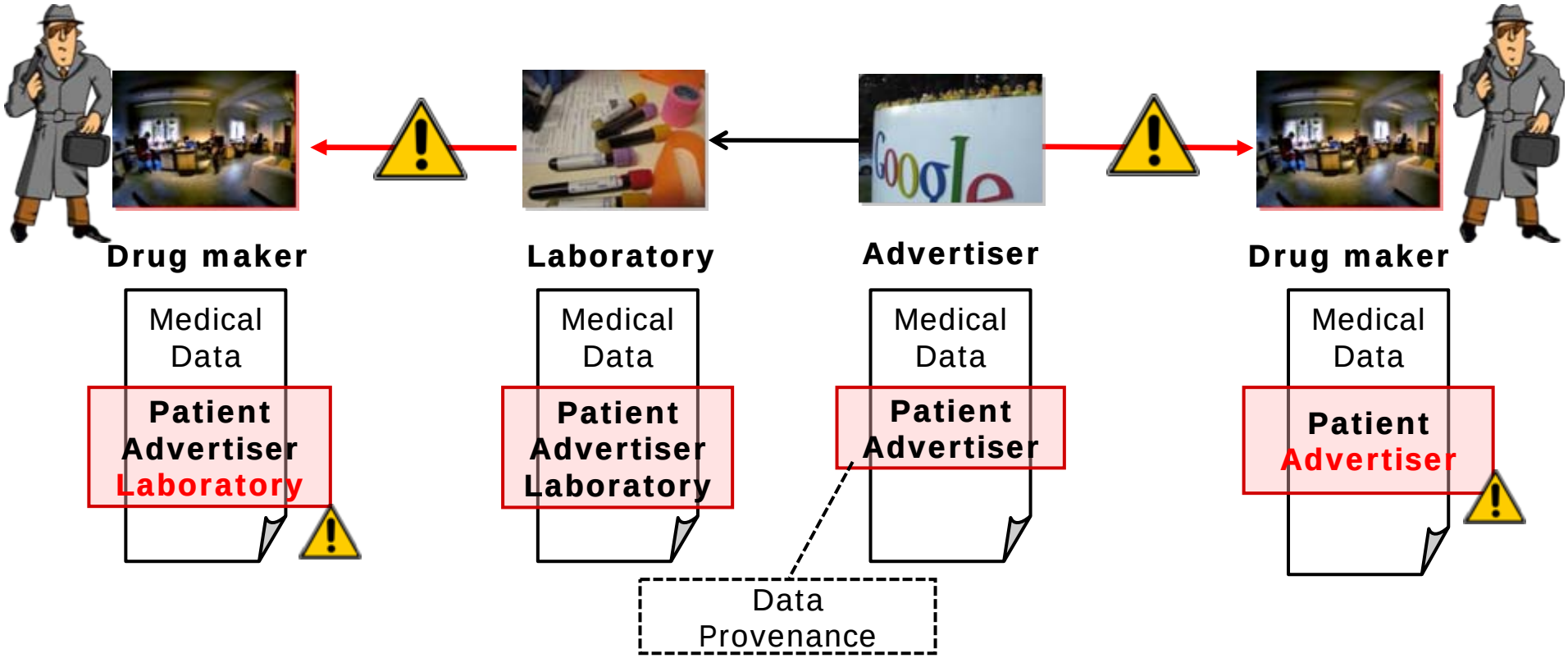
Müller, G., Accorsi, R., Höhn, S. and Sackmann, S., 2010

Usage Control by Data Provenance (2/2)

- **Data provenance**
  - Information to determine the derivation history

- **In an audit, data provenance can be used to restore the information flow.**

Example



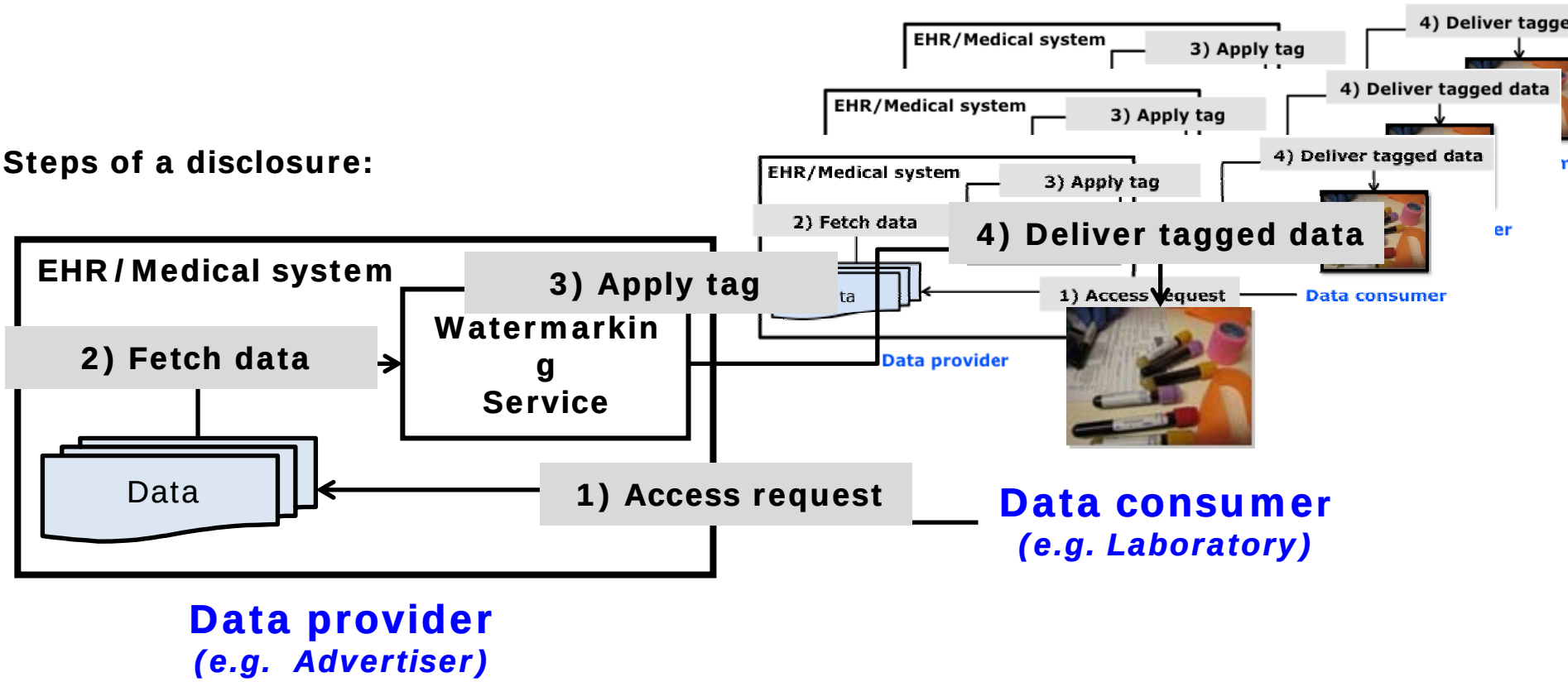
4. DETECTIVE: Data Provenance with Digital Watermarking

Watermarking is a method to bind provenance information as a tag to data.

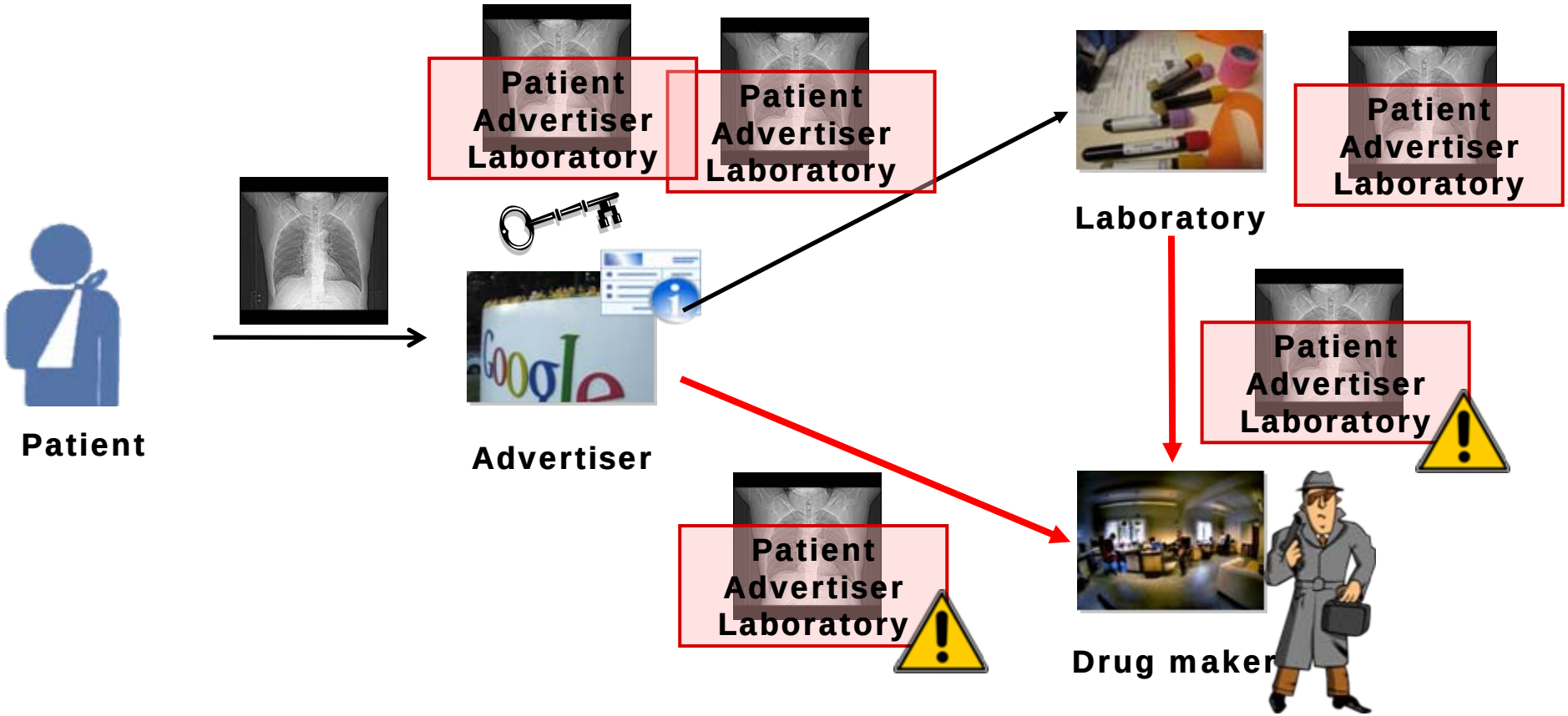
The EHR / Medical system must enforce that

- disclosed data is tagged with updated provenance information
- provenance information is authentic.

Steps of a disclosure:



Digital Watermarking and Disclosure of Personal Data



Both service providers have same digital watermark

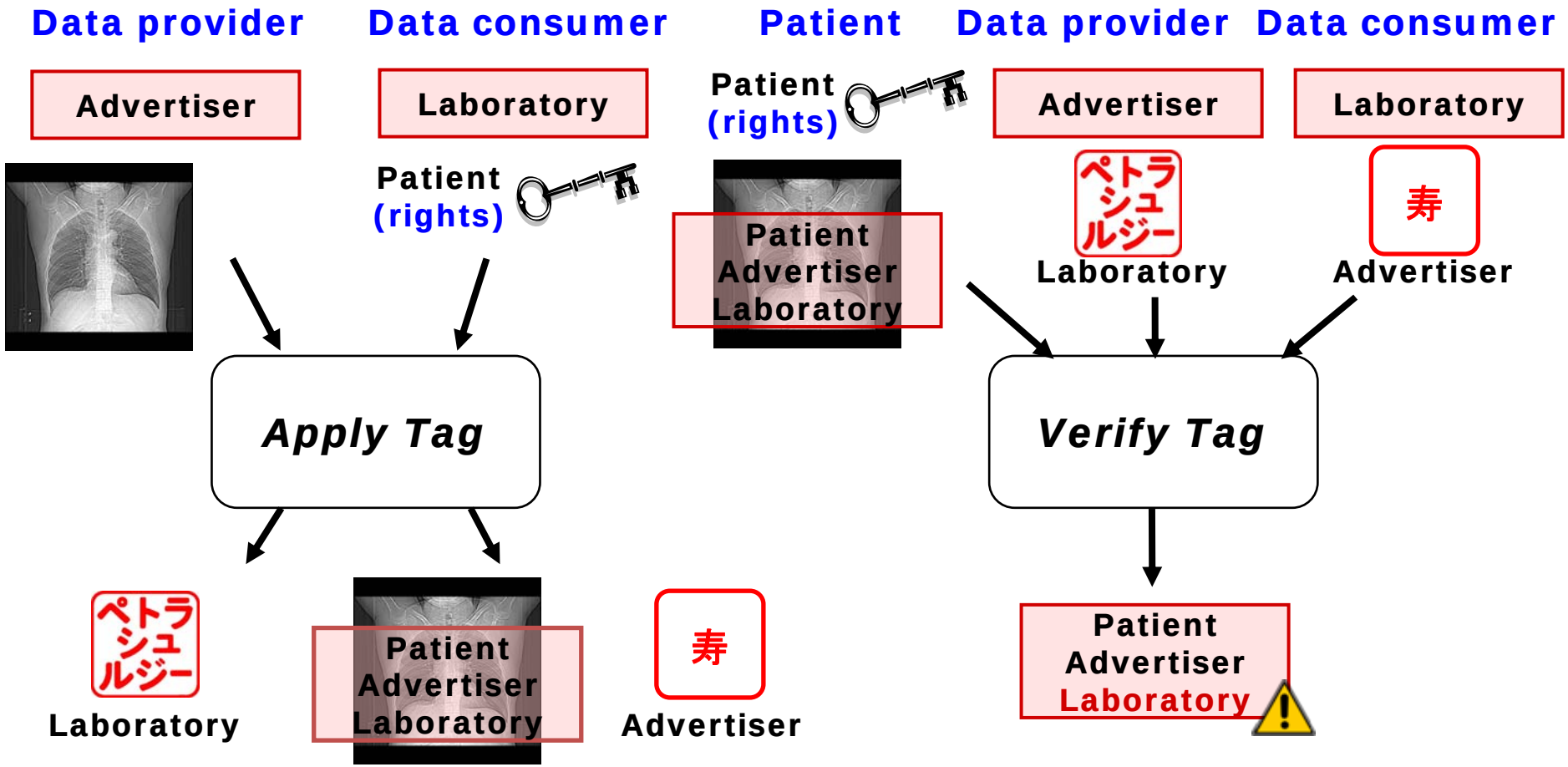
➔ **No identification of last data provider**

DETECTIVE: Digital Watermarking Scheme

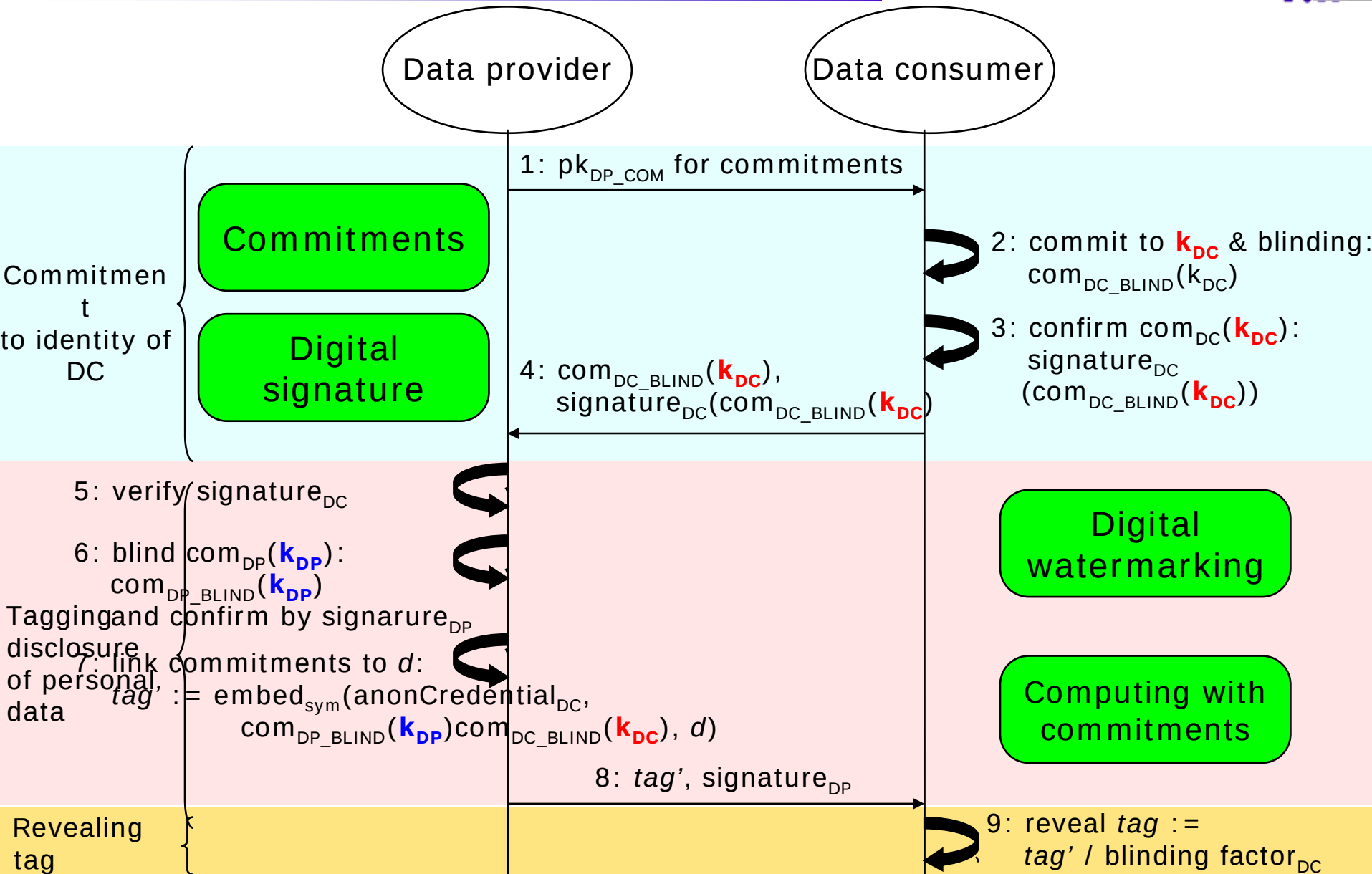
Data provenance information

- Linking identities of data provider and data consumer with access to personal data.

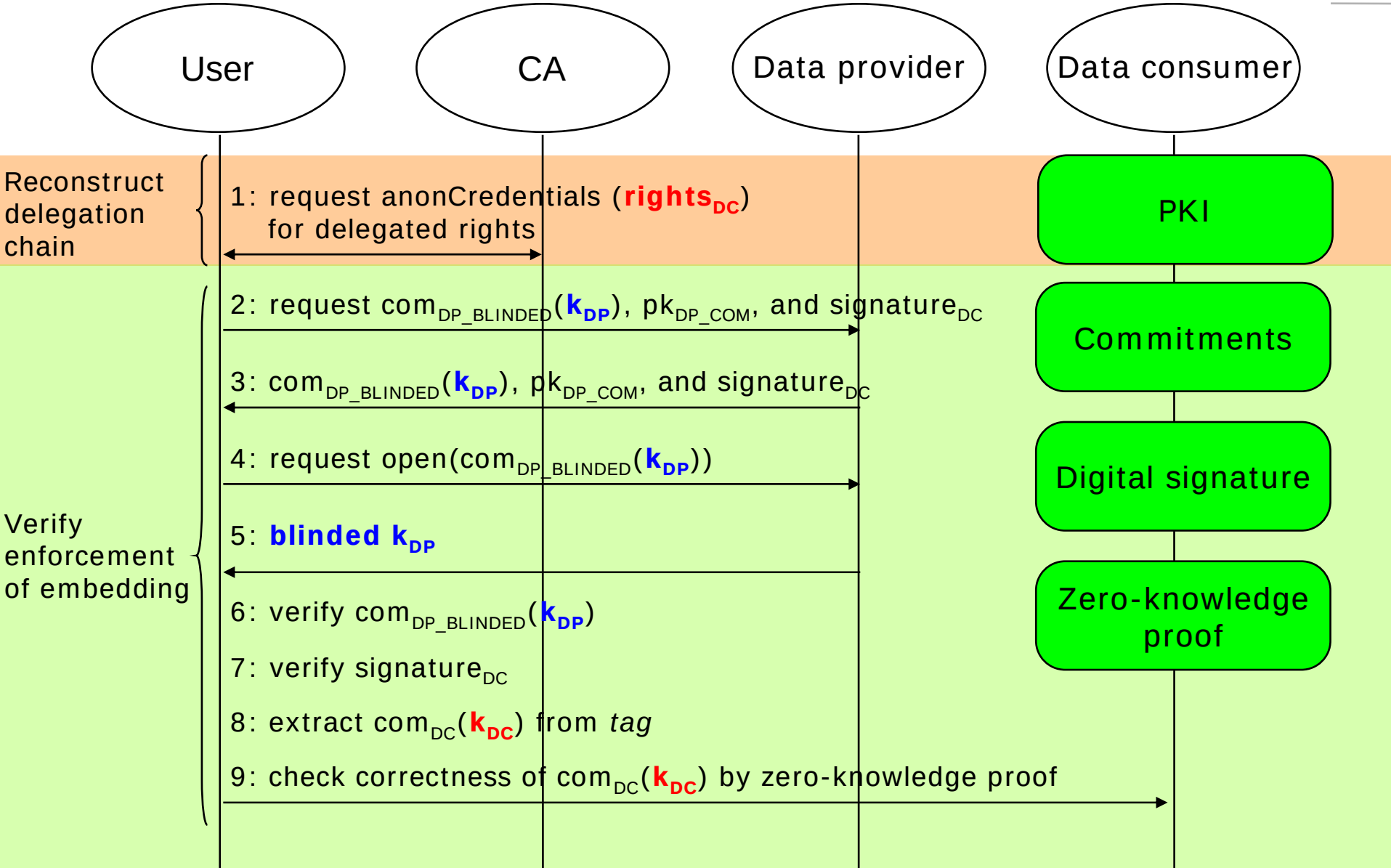
Detection by the patient via delegated rights (privacy policy) to personal data.



DETECTIVE: Protocol *Tag*

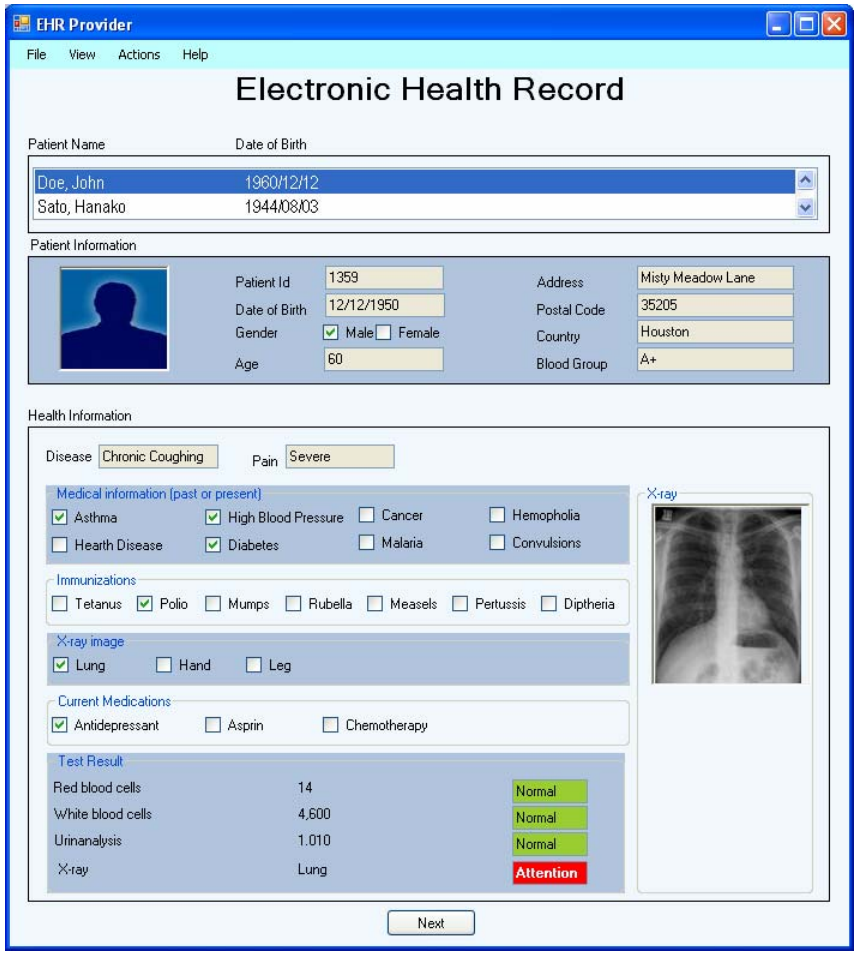


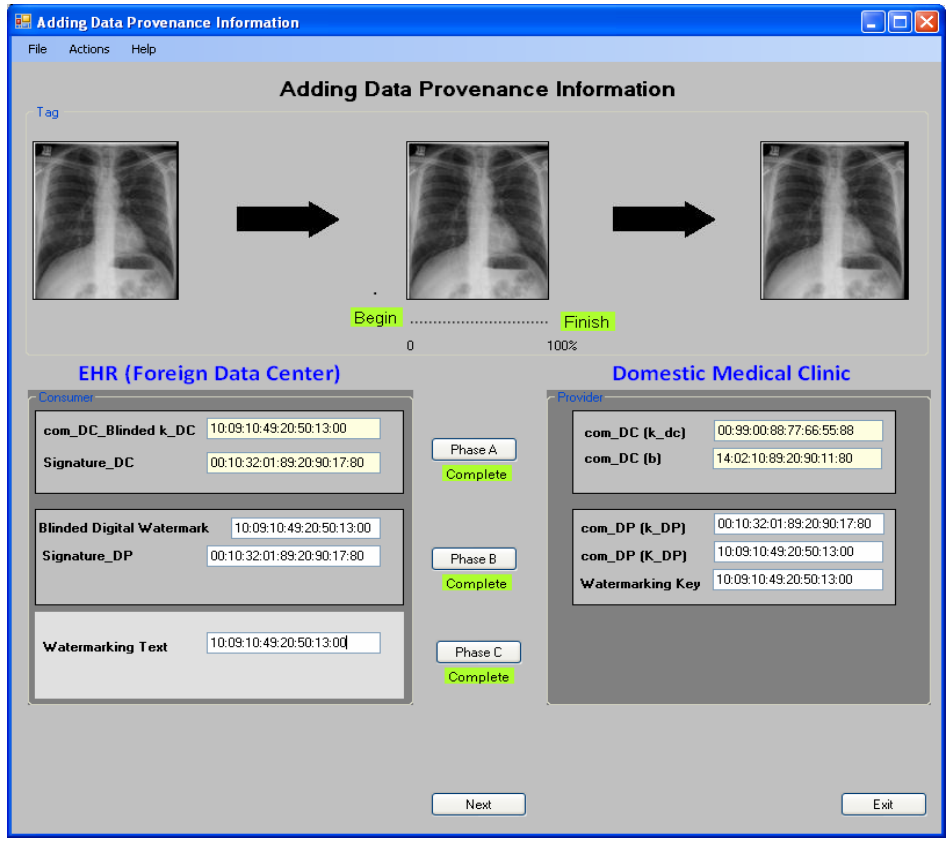
DETECTIVE: Protocol *Verify*



DETECTIVE: Proof-of-Concept Implementation

Case study: Telemedicine – Consulting a clinic abroad

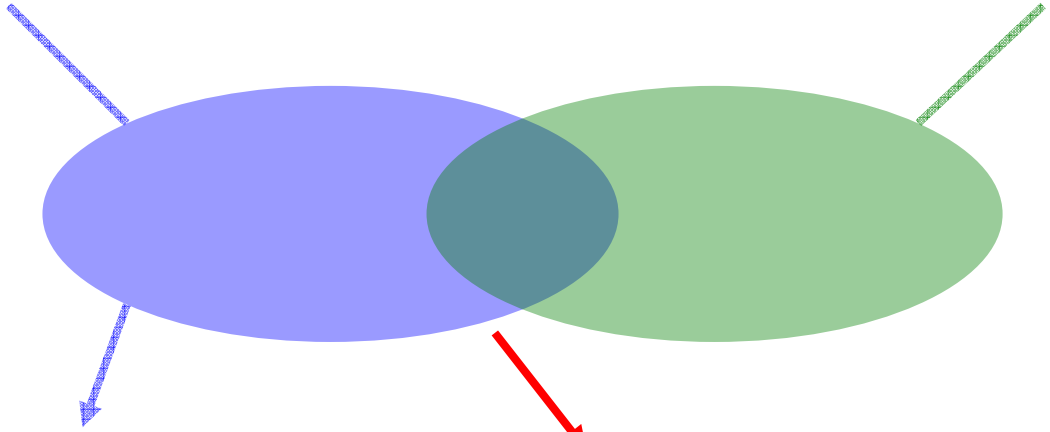




5. *Safety* of Data and *Liveness* of Services

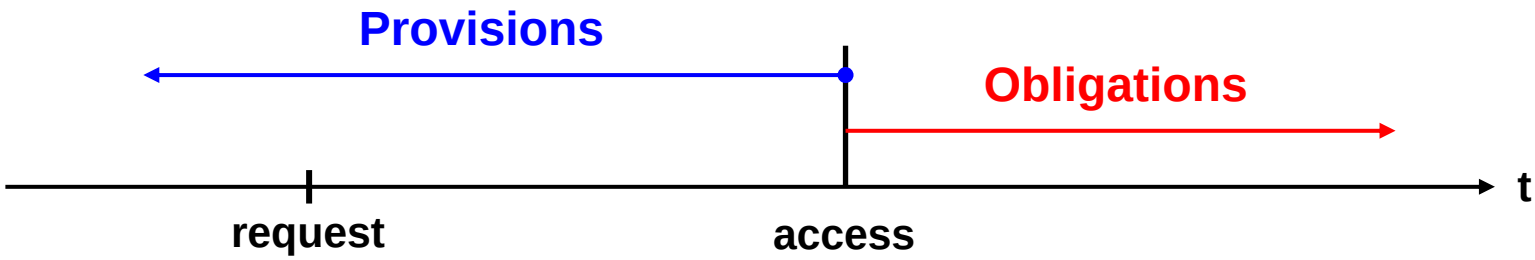
Safety: Authorized execution

Liveness: Reachable states



Provisions: cover the time up to the access ("past and present")

Obligations: cover the time after the access ("future")



Transparency by Policy Enforcement Mechanisms (e.g. DETECTIVE)