

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

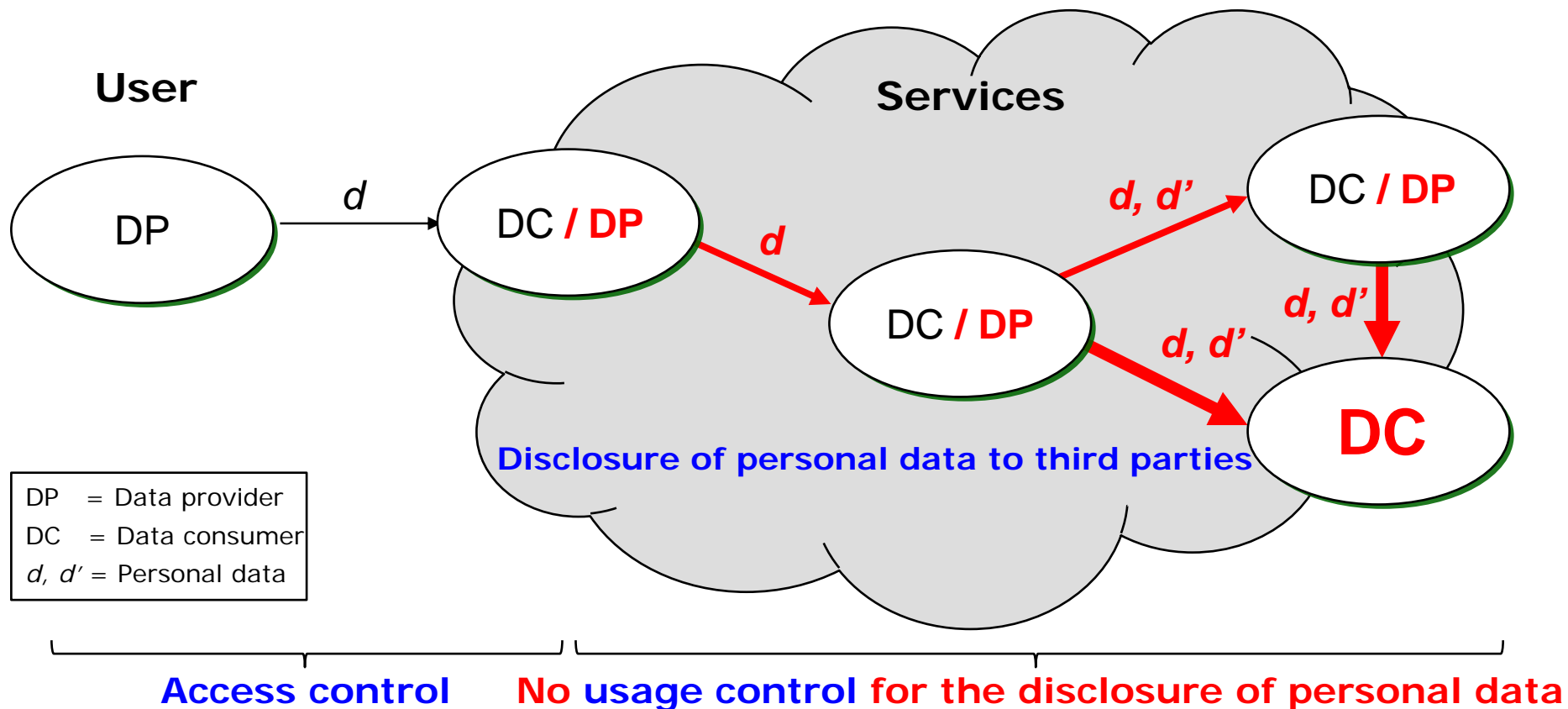
University of Freiburg, Germany

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)



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*)

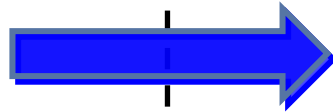
Current scenario



Patient's data is stored in many medical systems.

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

New scenario



Laboratory



Examination



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**.

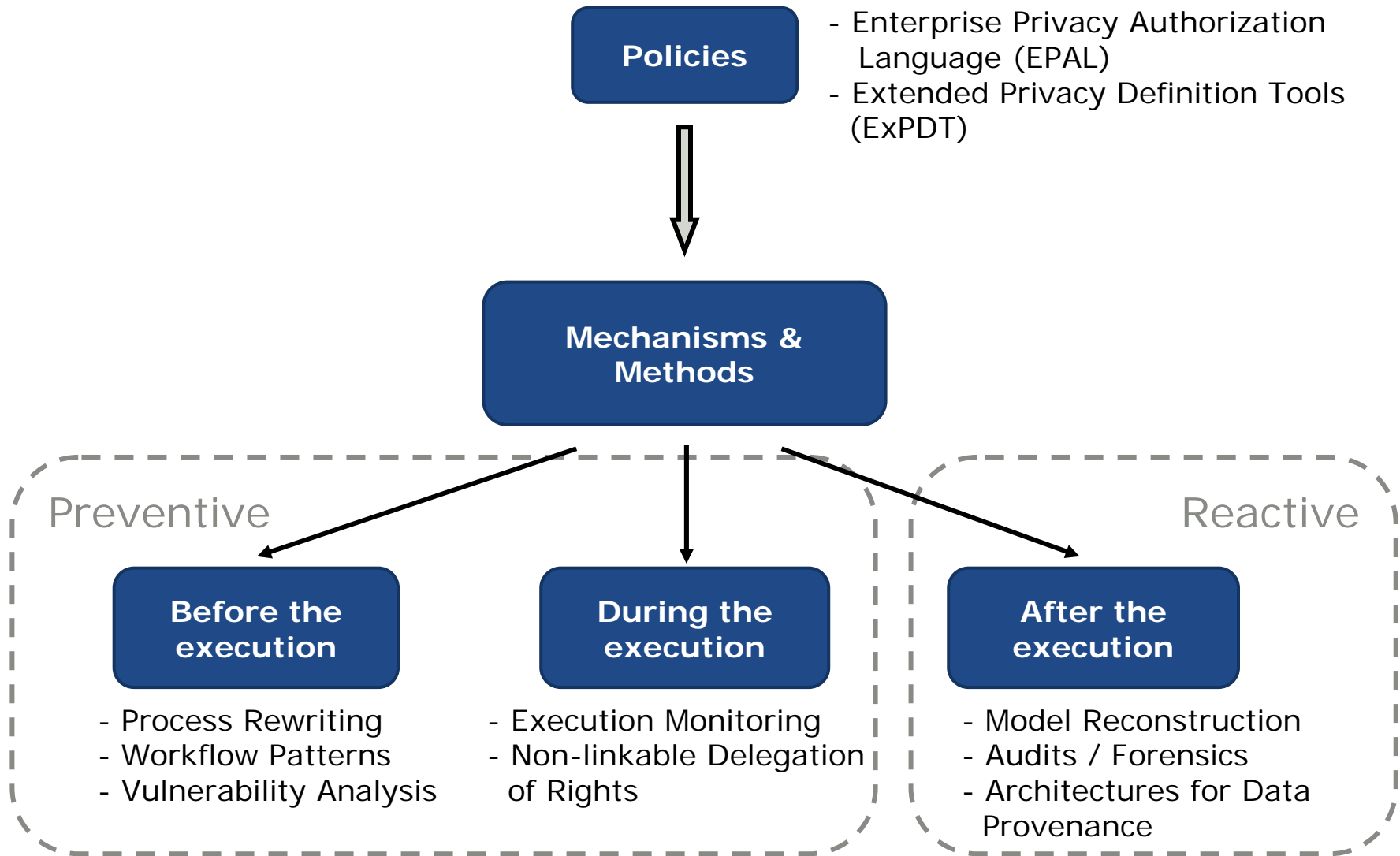
➤ Privacy Problem

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)



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



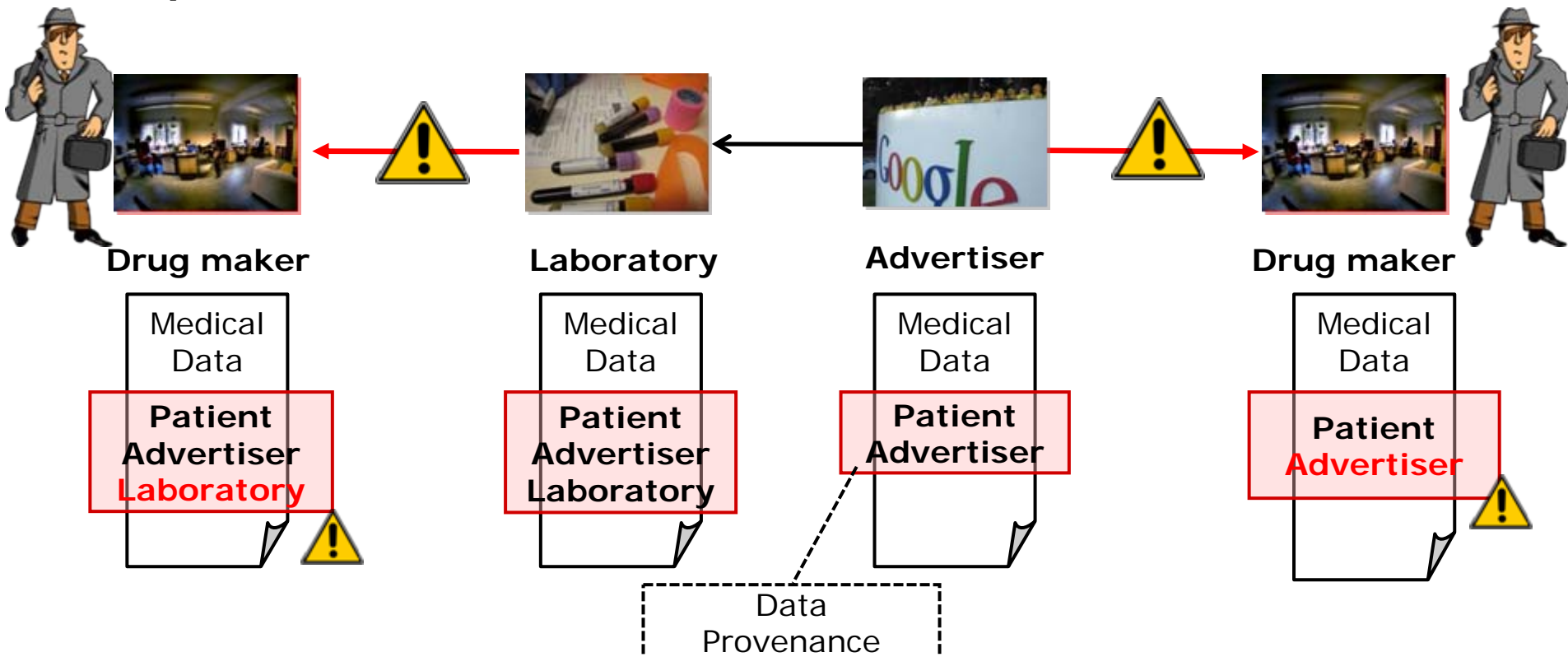
Usage Control by Data Provenance (2/2)

- **Data provenance**

- Information to determine the derivation history

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

Example



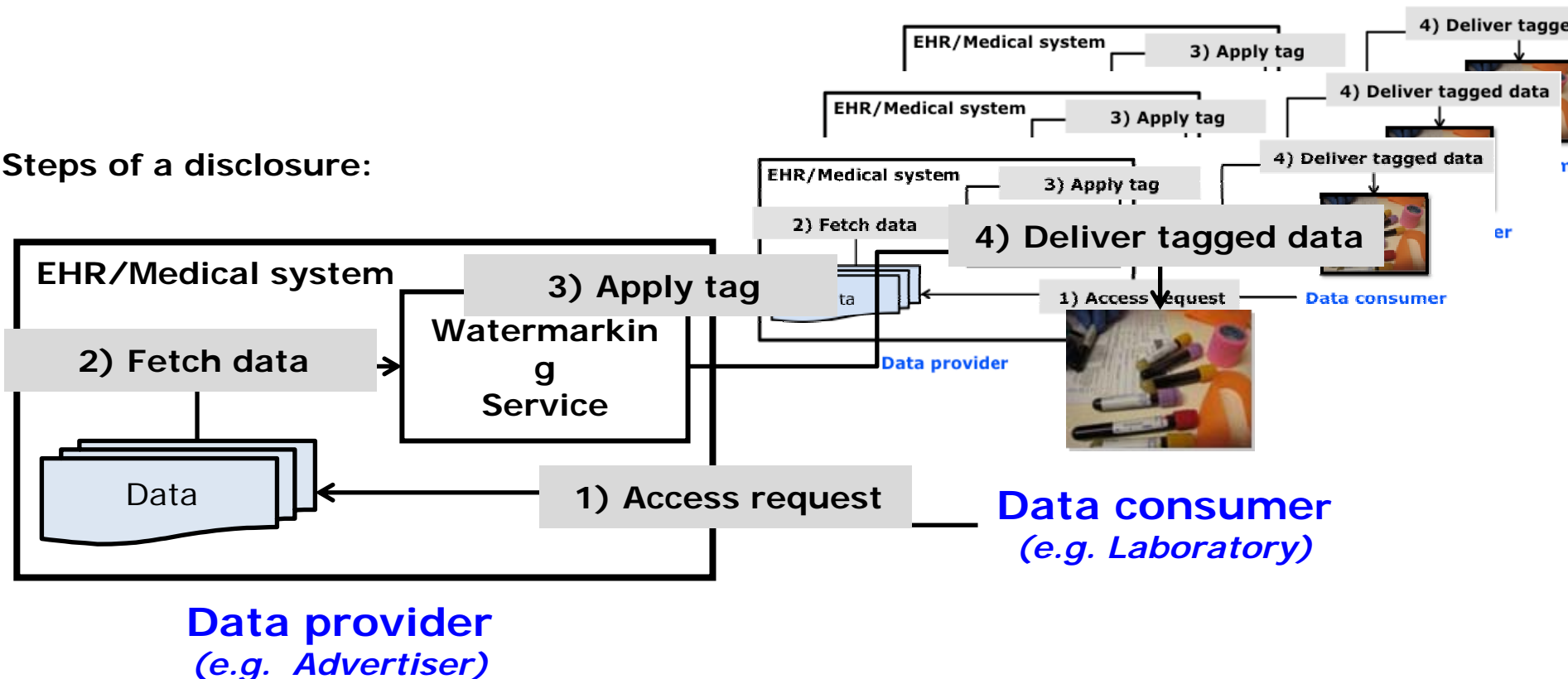
4. DETECTIVE: Data Provenance with Digital Watermarking

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

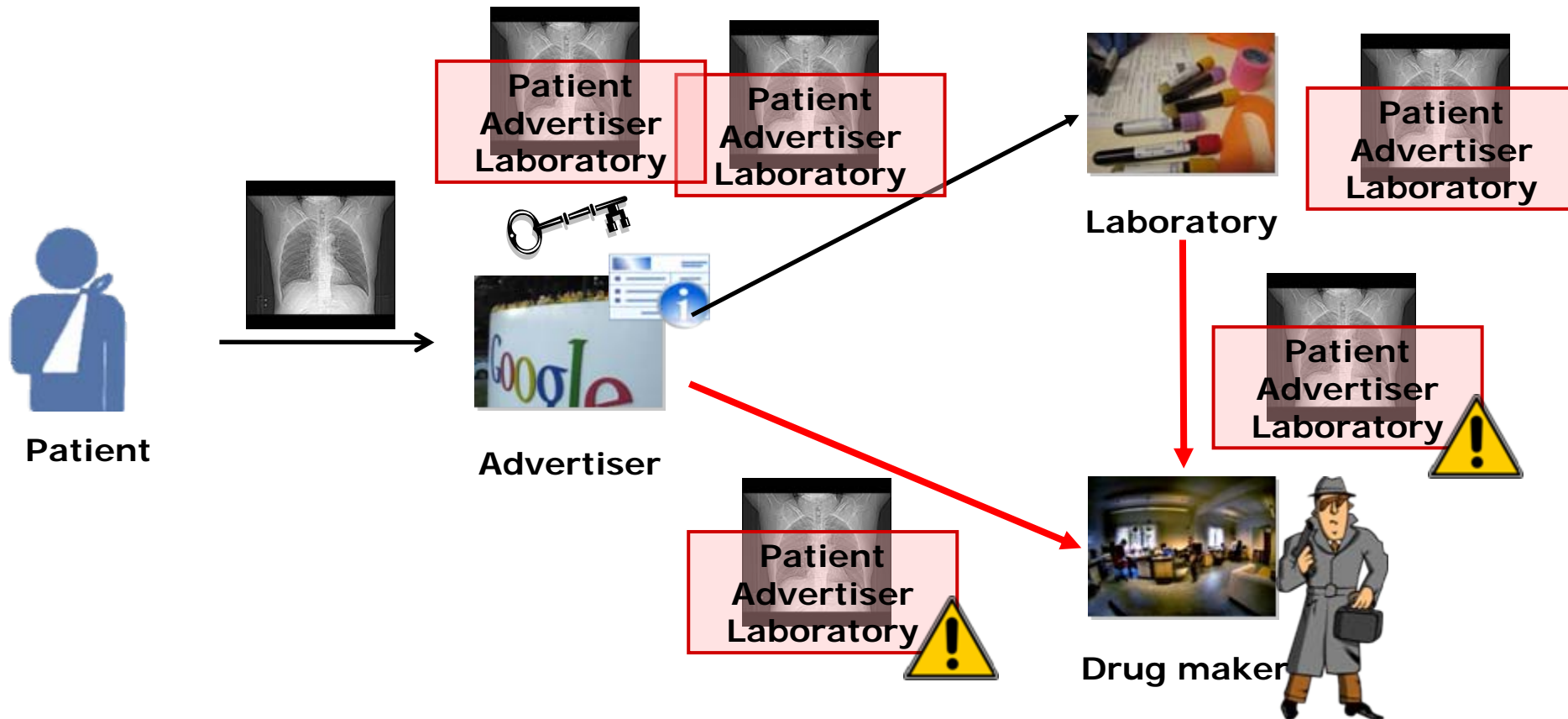
The EHR/Medical system must enforce that

- 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

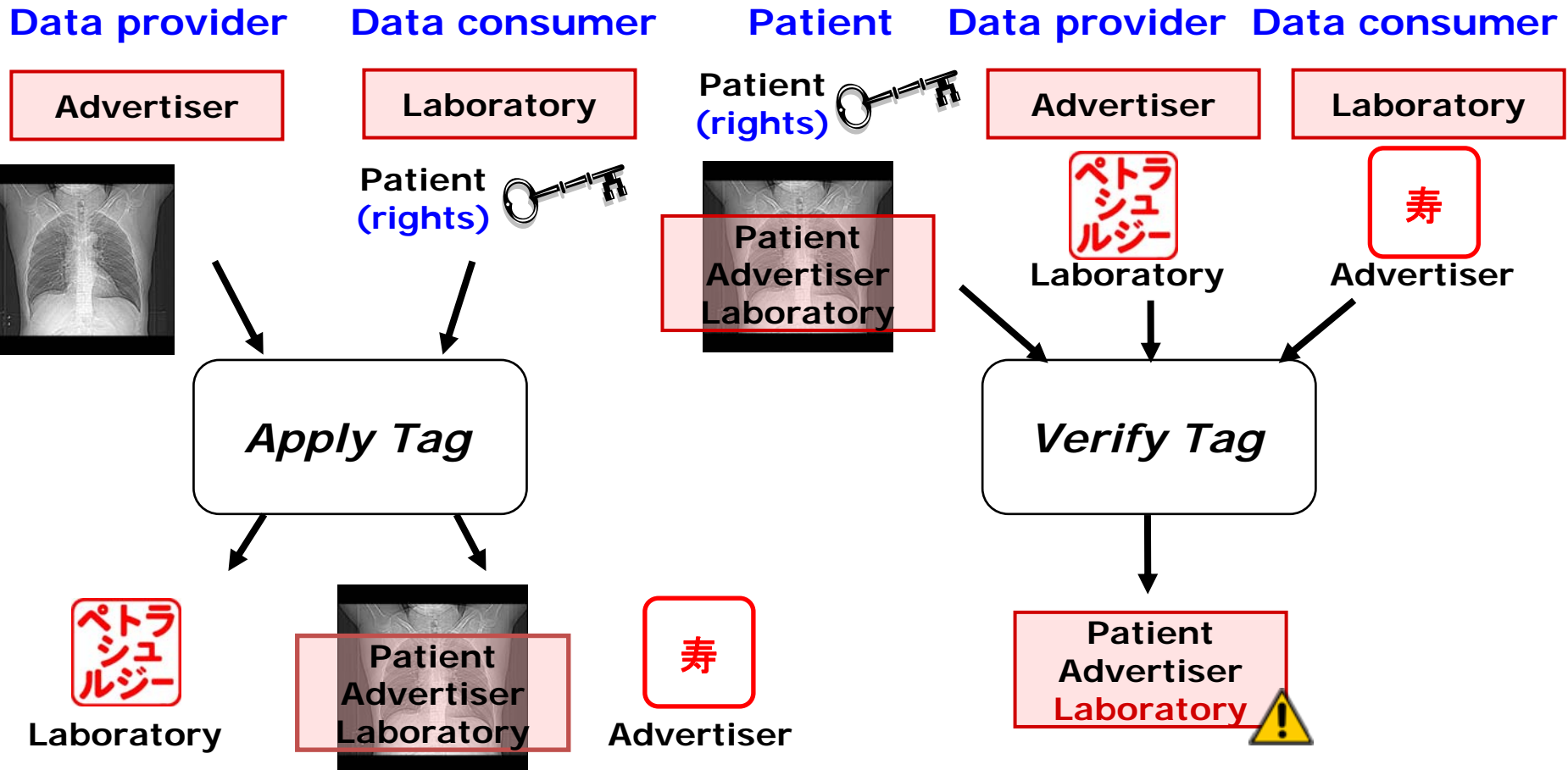
→ No identification of last data provider

DETECTIVE: Digital Watermarking Scheme

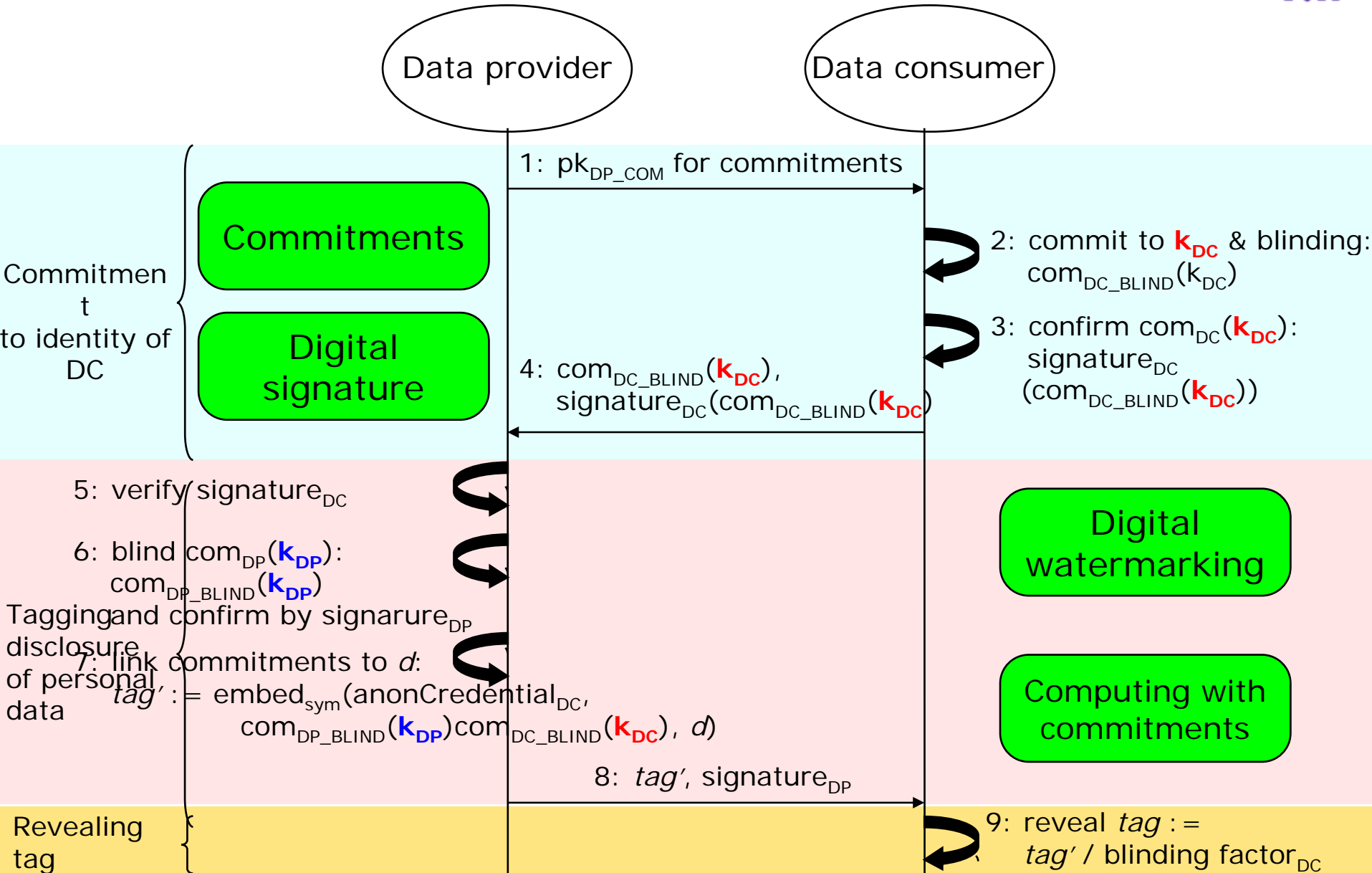
Data provenance information

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

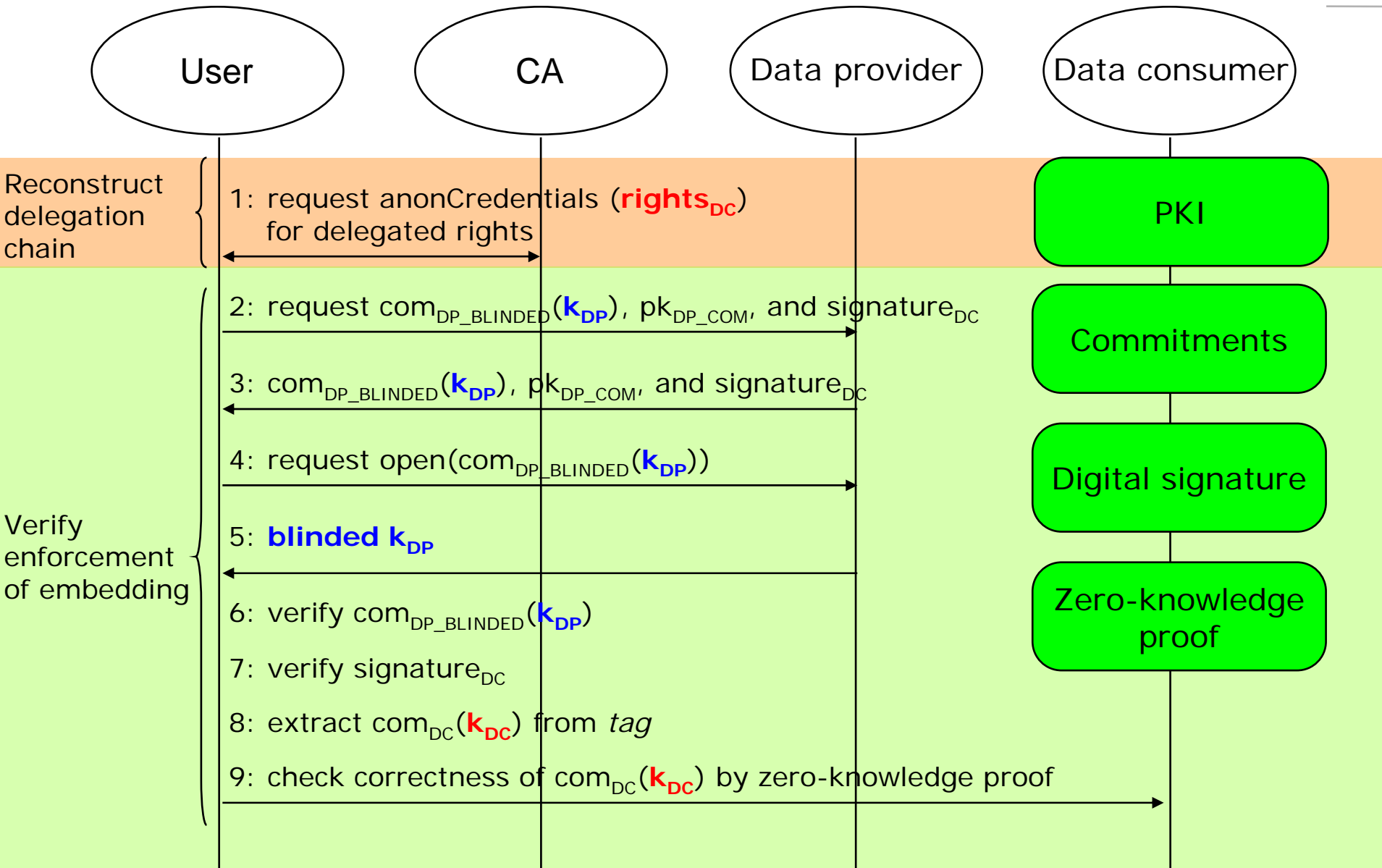
Detection by the patient via **delegated rights (privacy policy)** to personal data.



DETECTIVE: Protocol Tag



DETECTIVE: Protocol Verify



DETECTIVE: Proof-of-Concept Implementation

Case study: Telemedicine – Consulting a clinic abroad


EHR Provider

File View Actions Help

Electronic Health Record

Patient Name: Doe, John Date of Birth: 1960/12/12
Sato, Hanako 1944/08/03

Patient Information

 Patient Id: 1359 Address: Misty Meadow Lane
Date of Birth: 12/12/1950 Postal Code: 35205
Gender: ☒ Male ☐ Female Country: Houston
Age: 60 Blood Group: A+

Health Information

Disease: Chronic Coughing Pain: Severe

Medical information (past or present)

☒ Asthma ☒ High Blood Pressure ☐ Cancer ☐ Hemophilia
☐ Heart Disease ☒ Diabetes ☐ Malaria ☐ Convulsions

Immunizations

☐ Tetanus ☒ Polio ☐ Mumps ☐ Rubella ☐ Measels ☐ Pertussis ☐ Diptheria

X-ray image

☒ Lung ☐ Hand ☐ Leg

Current Medications

☒ Antidepressant ☐ Aspirin ☐ Chemotherapy

Test Result




Red blood cells	14	Normal
White blood cells	4,600	Normal
Urinalysis	1.010	Normal
X-ray	Lung	Attention

Next

Adding Data Provenance Information

File Actions Help

Tag

 →  → 

Begin Finish
0 100%

EHR (Foreign Data Center)

Consumer

com_DC_Blinded_k_DC: 10:09:10:49:20:50:13:00
Signature_DC: 00:10:32:01:89:20:90:17:80

Blinded Digital Watermark: 10:09:10:49:20:50:13:00
Signature_DP: 00:10:32:01:89:20:90:17:80

Watermarking Text: 10:09:10:49:20:50:13:00

Phase A Complete
Phase B Complete
Phase C Complete

Domestic Medical Clinic

Provider

com_DC (k_dc): 00:99:00:88:77:66:55:88
com_DC (b): 14:02:10:89:20:90:11:80

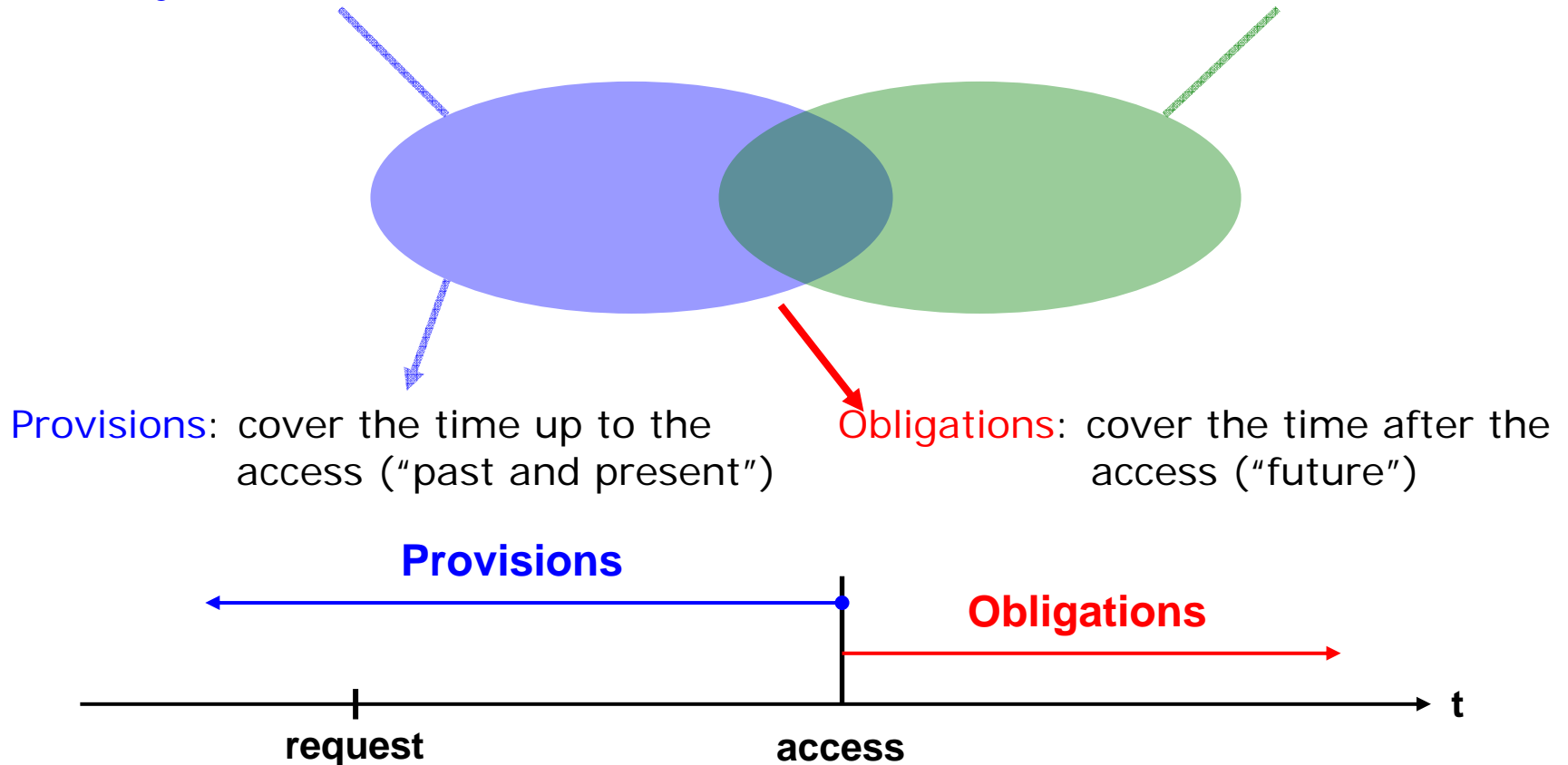
com_DP (k_DP): 00:10:32:01:89:20:90:17:80
com_DP (K_DP): 10:09:10:49:20:50:13:00
Watermarking Key: 10:09:10:49:20:50:13:00

Next Exit

5. Safety of Data and *Liveness* of Services

Safety: Authorized execution

Liveness: Reachable states



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