

Workshop eSanté

WS3: Unique Identification of Patients

Dr Stefan Benzschawel
CRP Henri Tudor – SANTEC
stefan.benzschawel@tudor.lu

CRP Henri Tudor
September 21 2011

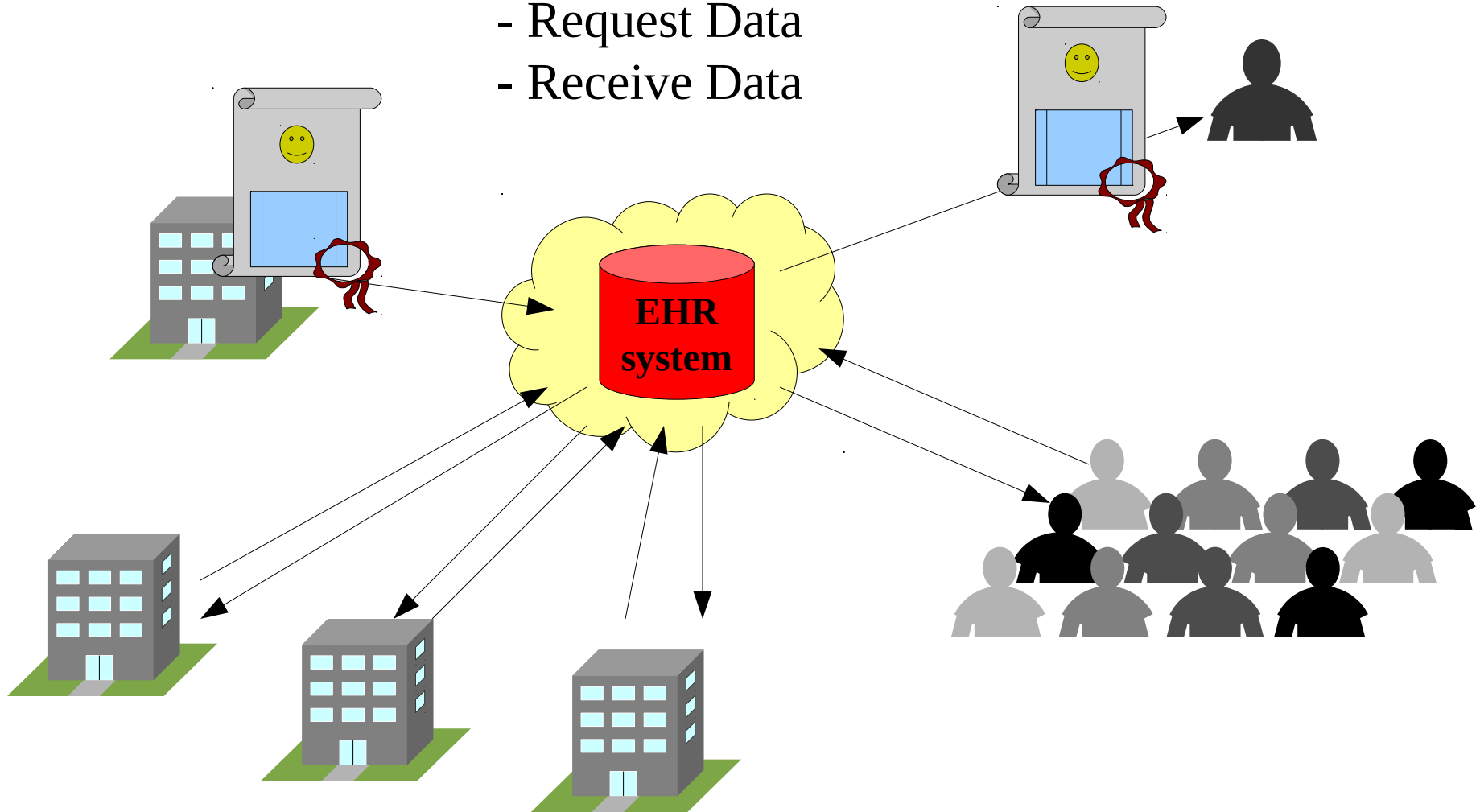
Overview Platform Proposal

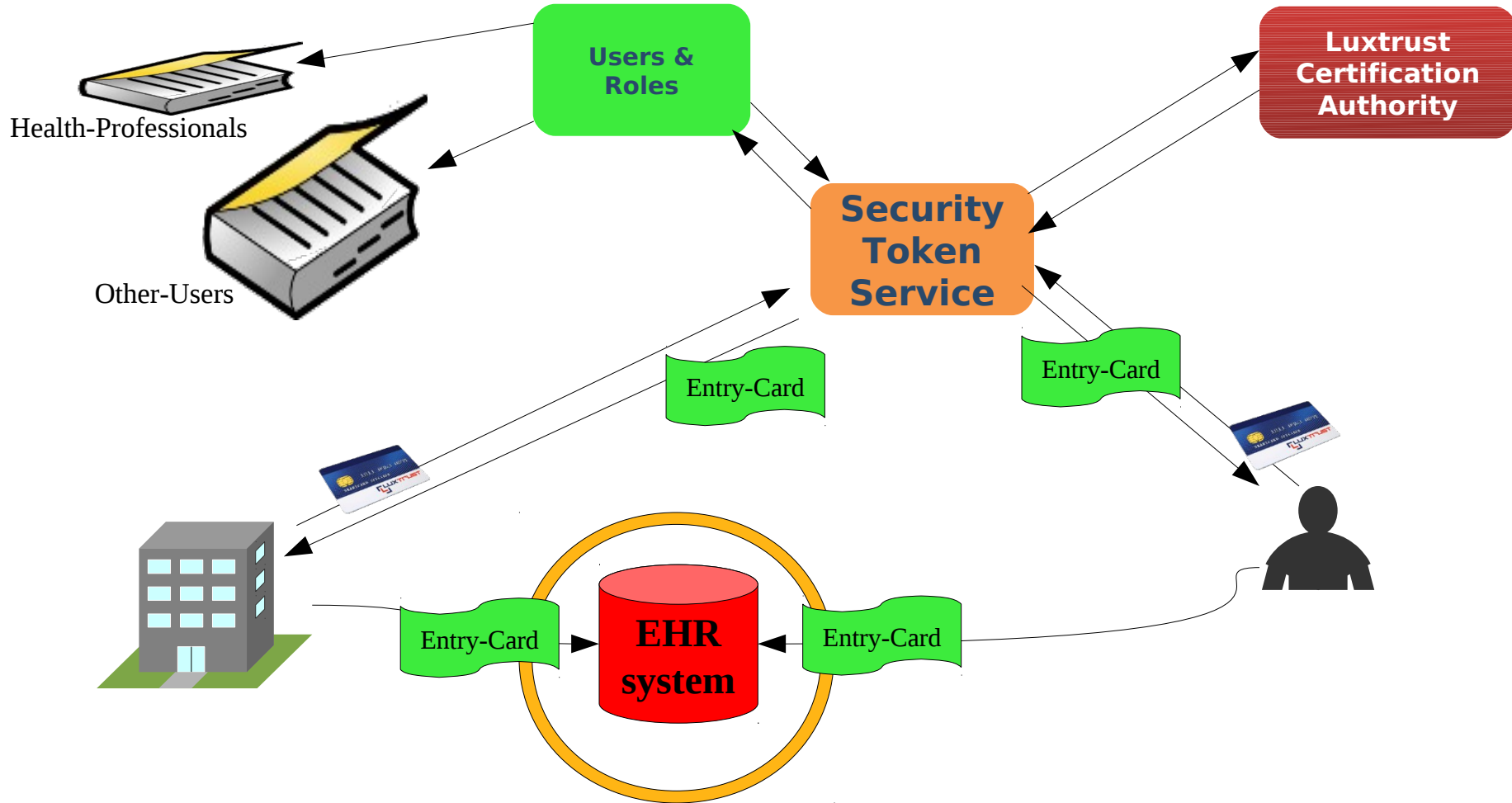
- Introduction, Typical Workflow
- Access Control
- Pseudonymization and 2-step Encryption
- Re-Encryption and 2-step Decryption

Workshop

- **Relevant Topics to be discussed ?**
- **Your Expectations ?**

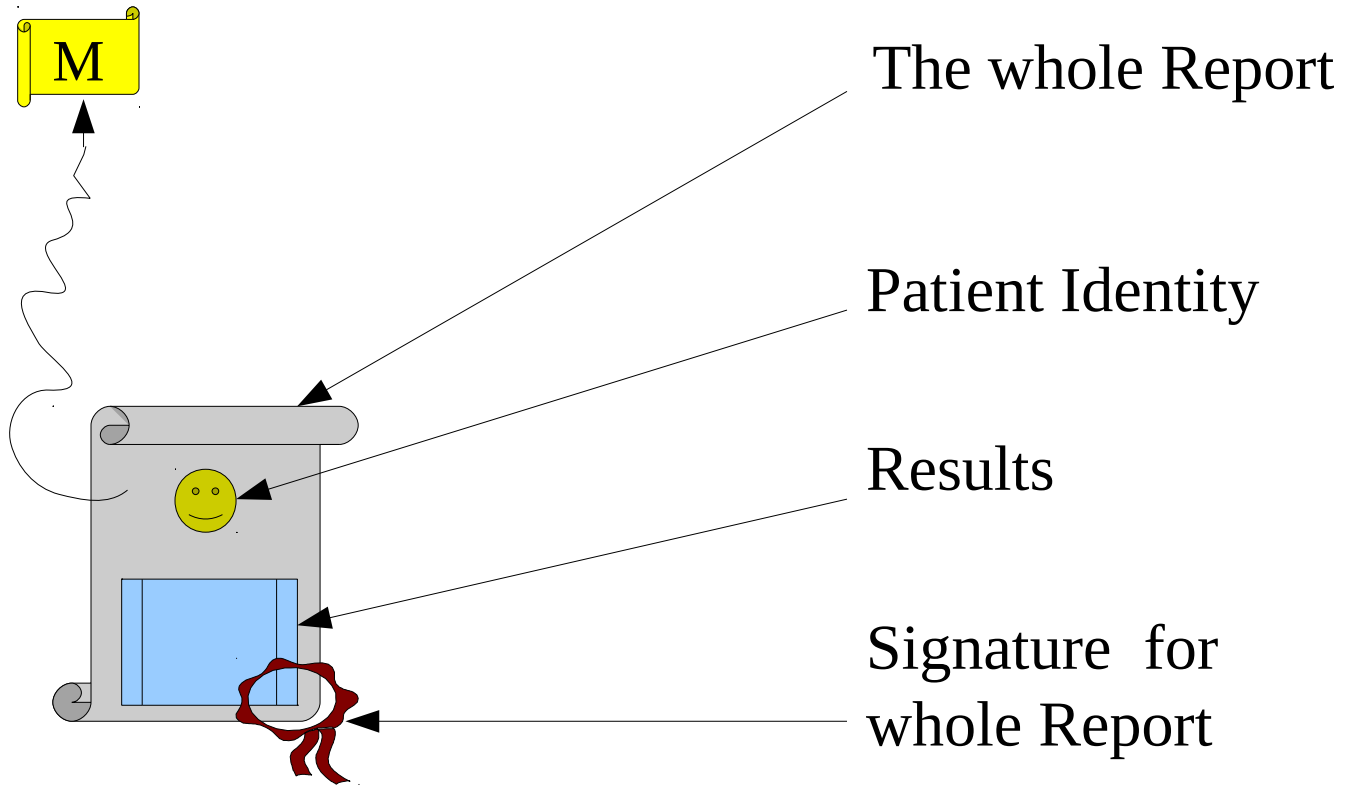
- Provide Data
- Request Data
- Receive Data



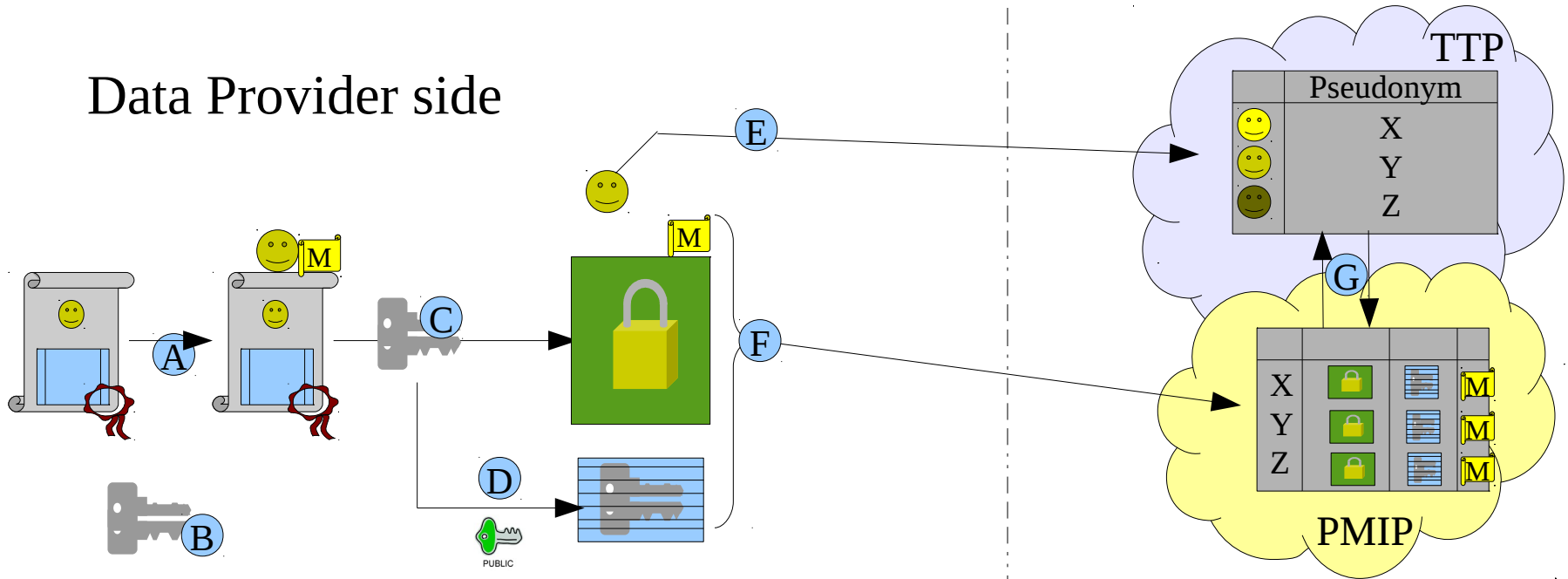


1. Pre-registered PERSON / INSTITUTION
2. Pre-registered PLATFORM USER with ROLE

General “Medical Report” + extraction of Metadata



Data Provider side

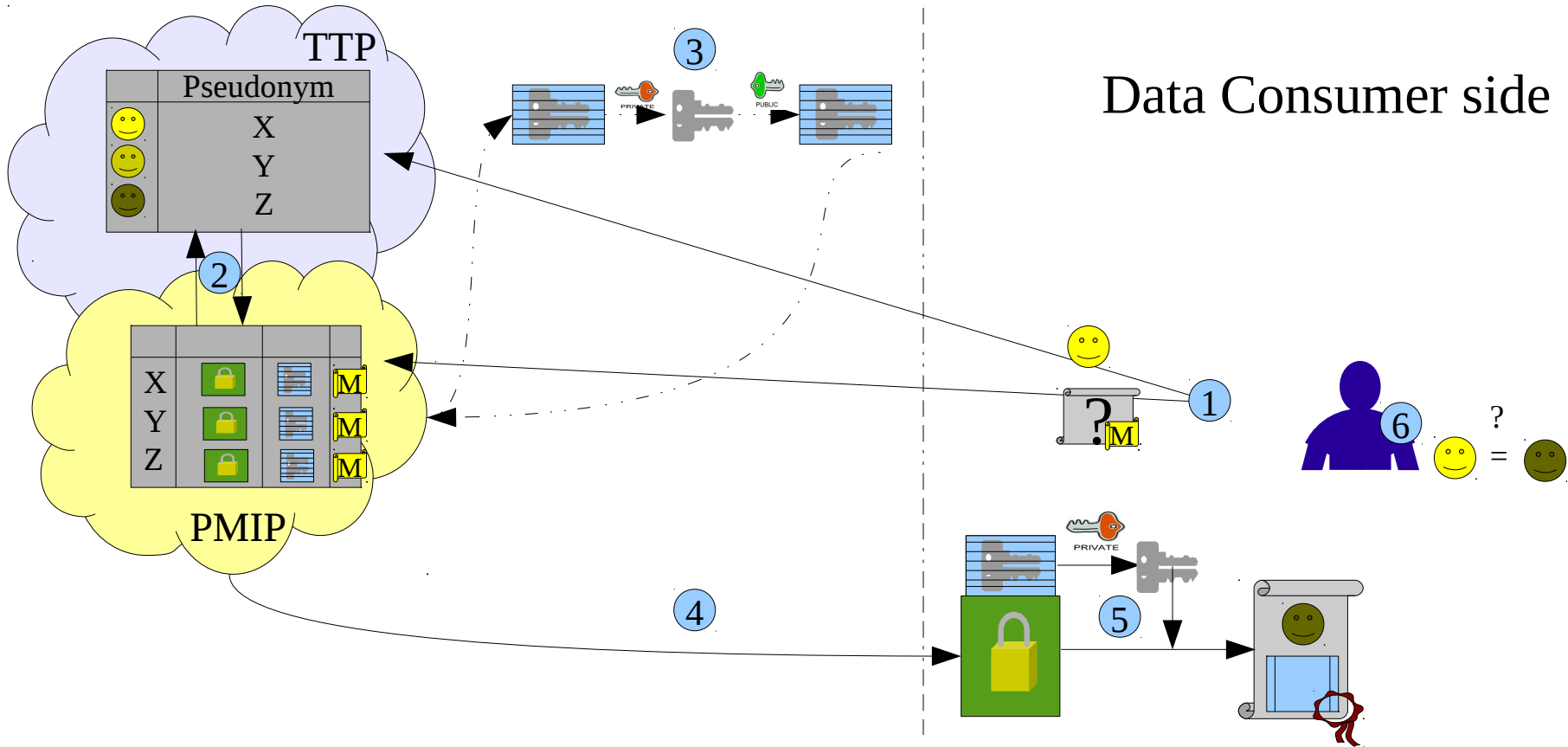



- A** Extract Identity Data and Metadata
- B** Generate a Symmetric Key (for each document)

- C** Encrypt Report with Symmetric Key
- D** Encrypt Symmetric Key with TTP's Public Key

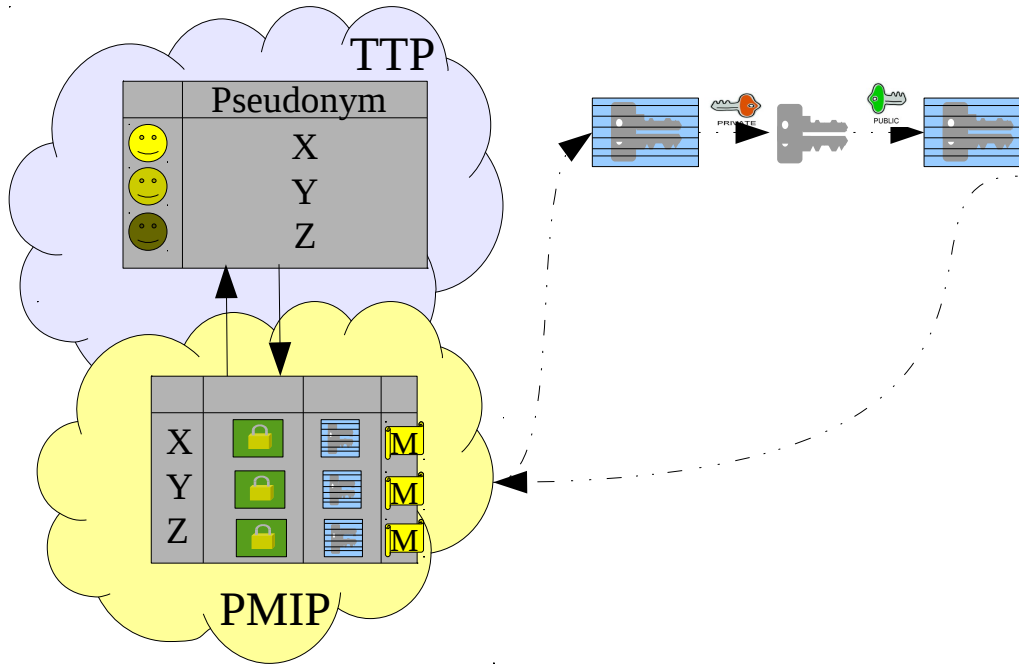
- E** Provide Identity Data to TTP
- F** Provide "everything else" to TTP

- G** Pseudonym Handshake



- 1 Open Query Session
- 2 Pseudonym Handshake
- 3 Re-Encryption of  with public Key of Requester

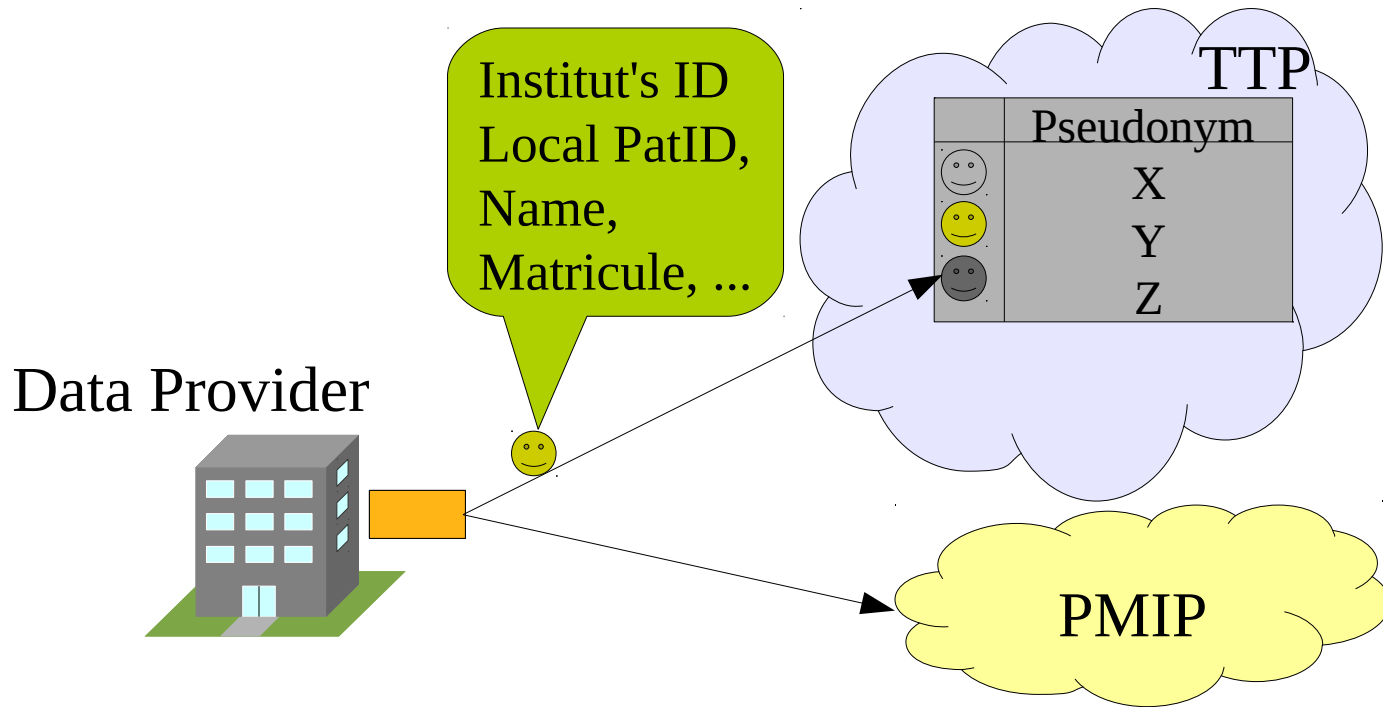
- 4 Deliver Encrypted Report and Key
- 5 Decryption in 2 Steps
- 6 Check Patient's Identity on Report



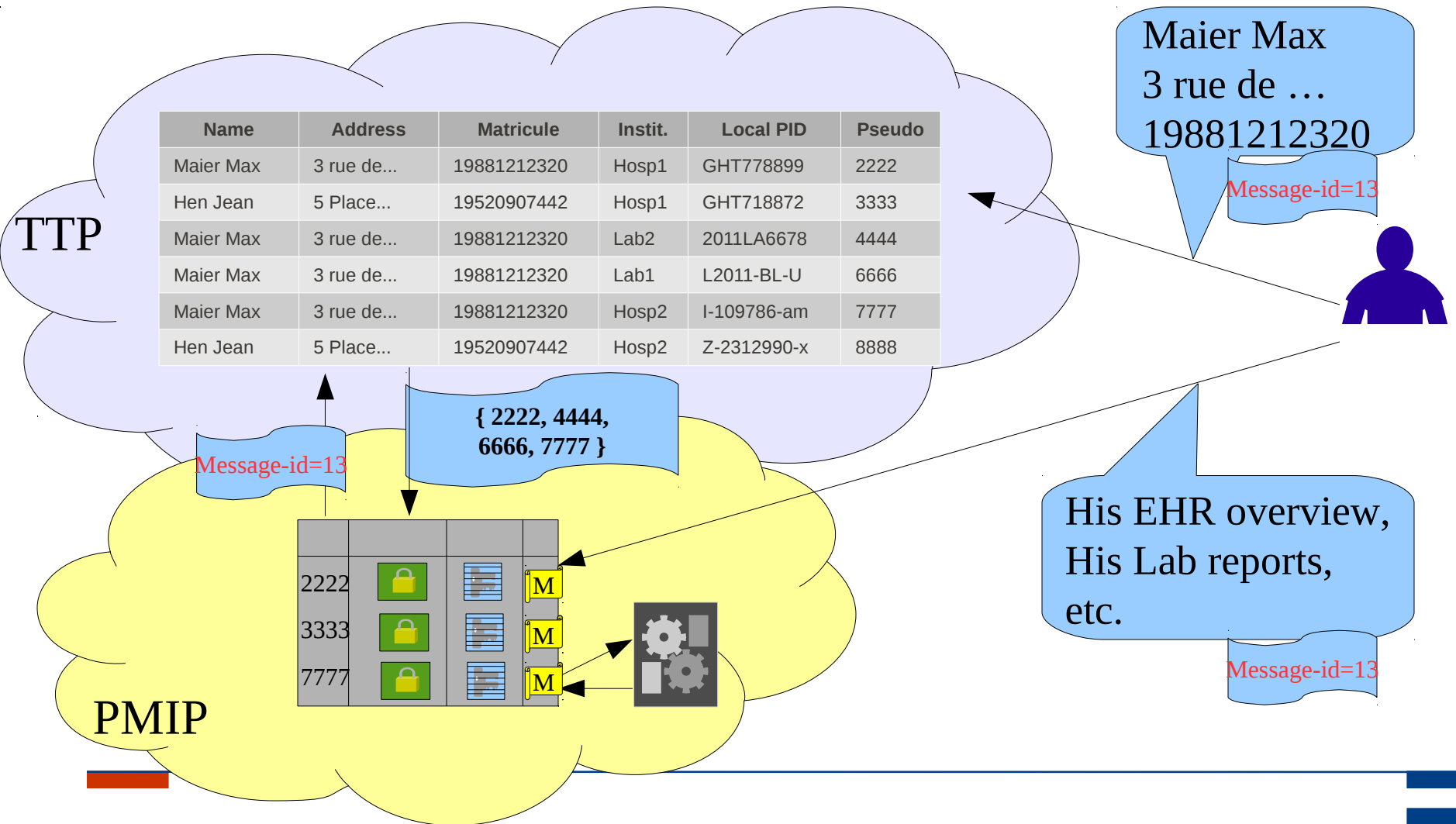
Metadata is protected by **Pseudonymization**
Medical Reports are protected by full **Encryption**
Non-Disclosure against single Admin/Intruder
Non-Disclosure even during **Re-Encryption** !

Workshop

- Relevant Topics to be discussed ?**
 - Your Expectations ?**
-
- Which ID Data are used / useful?
 - National Person Registry Involvement?
 - Patient as User of the eHealth Platform !



Information Retrieval



Results of Workshop-Discussion:

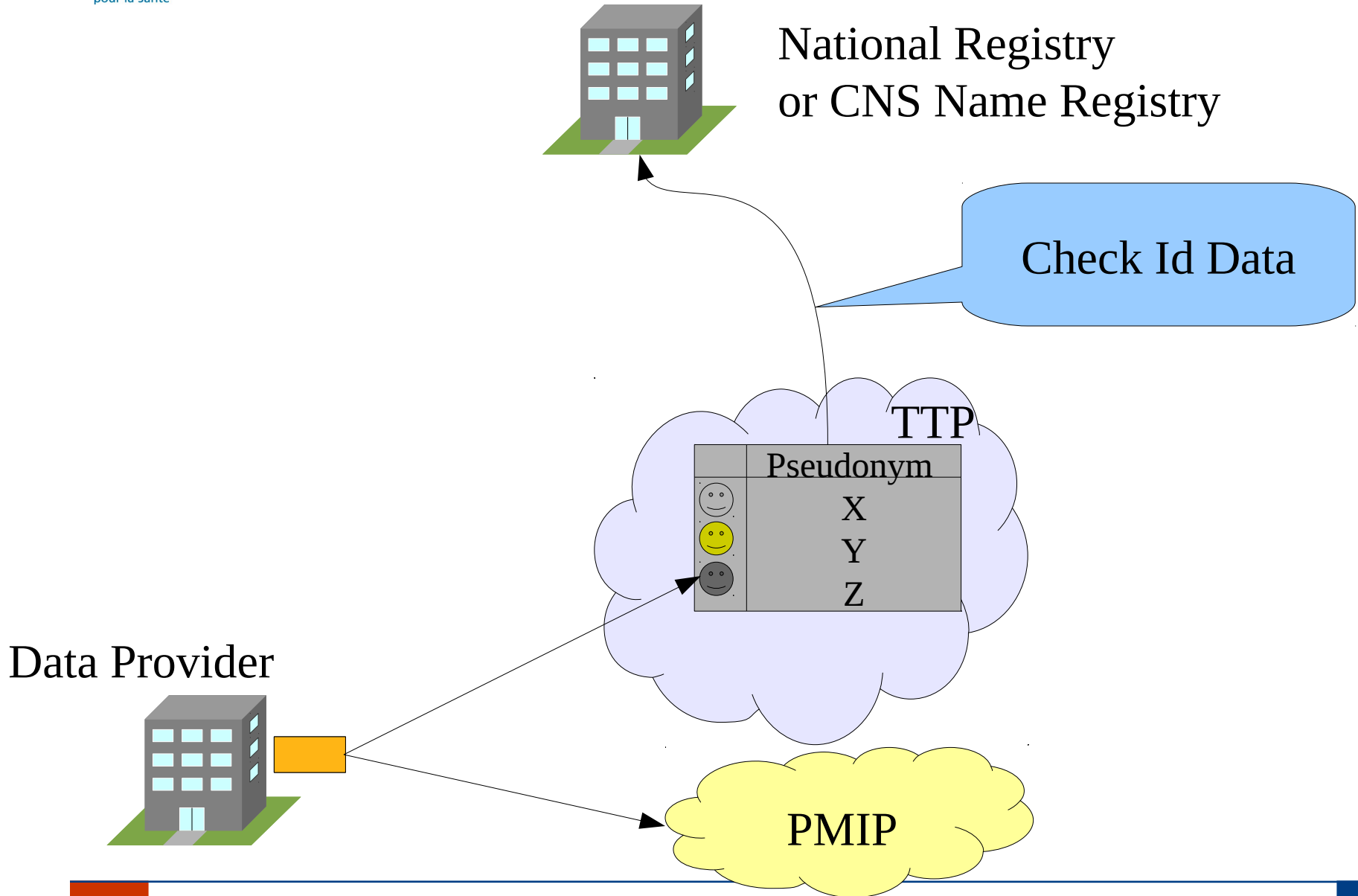
Which data is relevant to identify a patient?

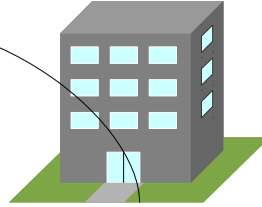
Currently used ID data in Hospital, Labo, HomeCare, etc.:

Additional ID data to mention are:

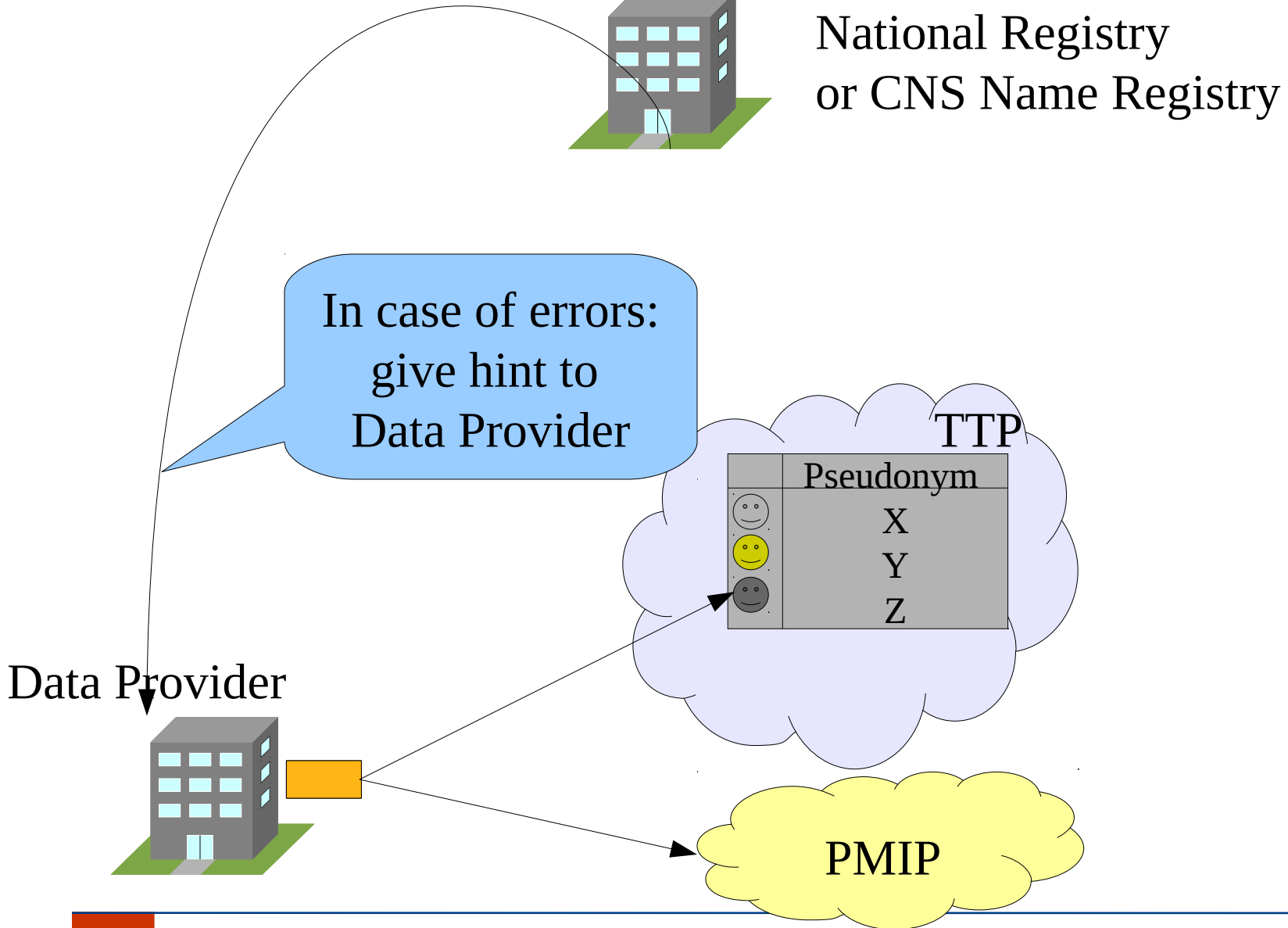
Other ideas, remarks:

National Registry Involvement





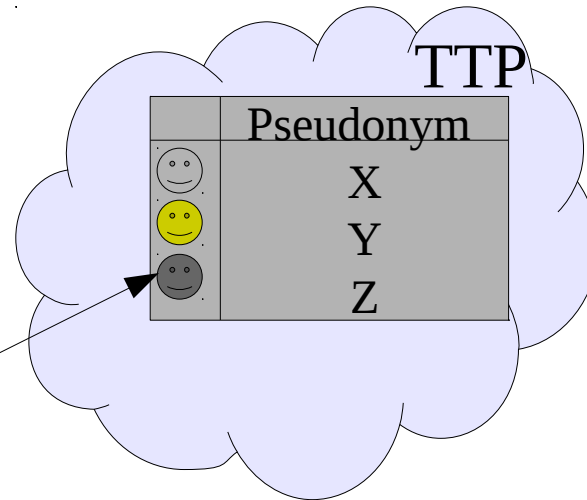
National Registry
or CNS Name Registry



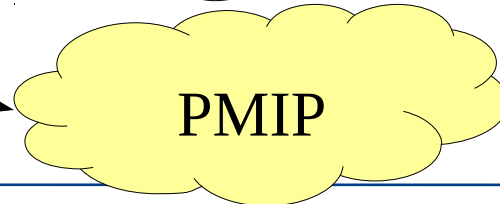
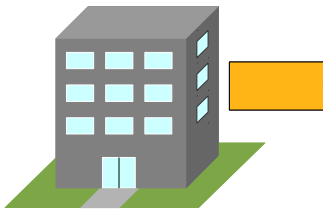


National Registry
or CNS Name Registry

In case of
local correction:
send update to TTP



Data Provider



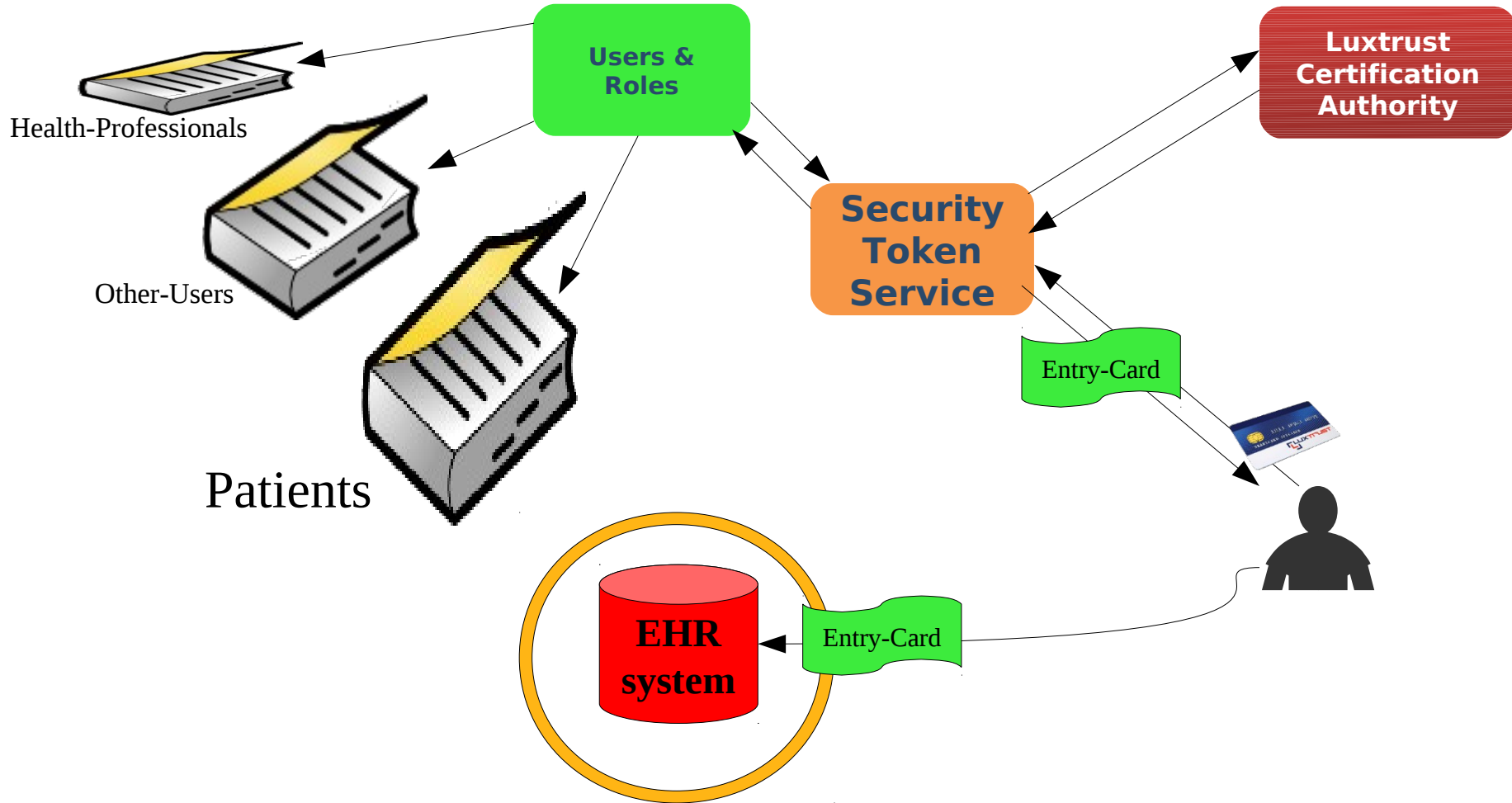
Results of Workshop-Discussion:

National Registry Involvement useful?

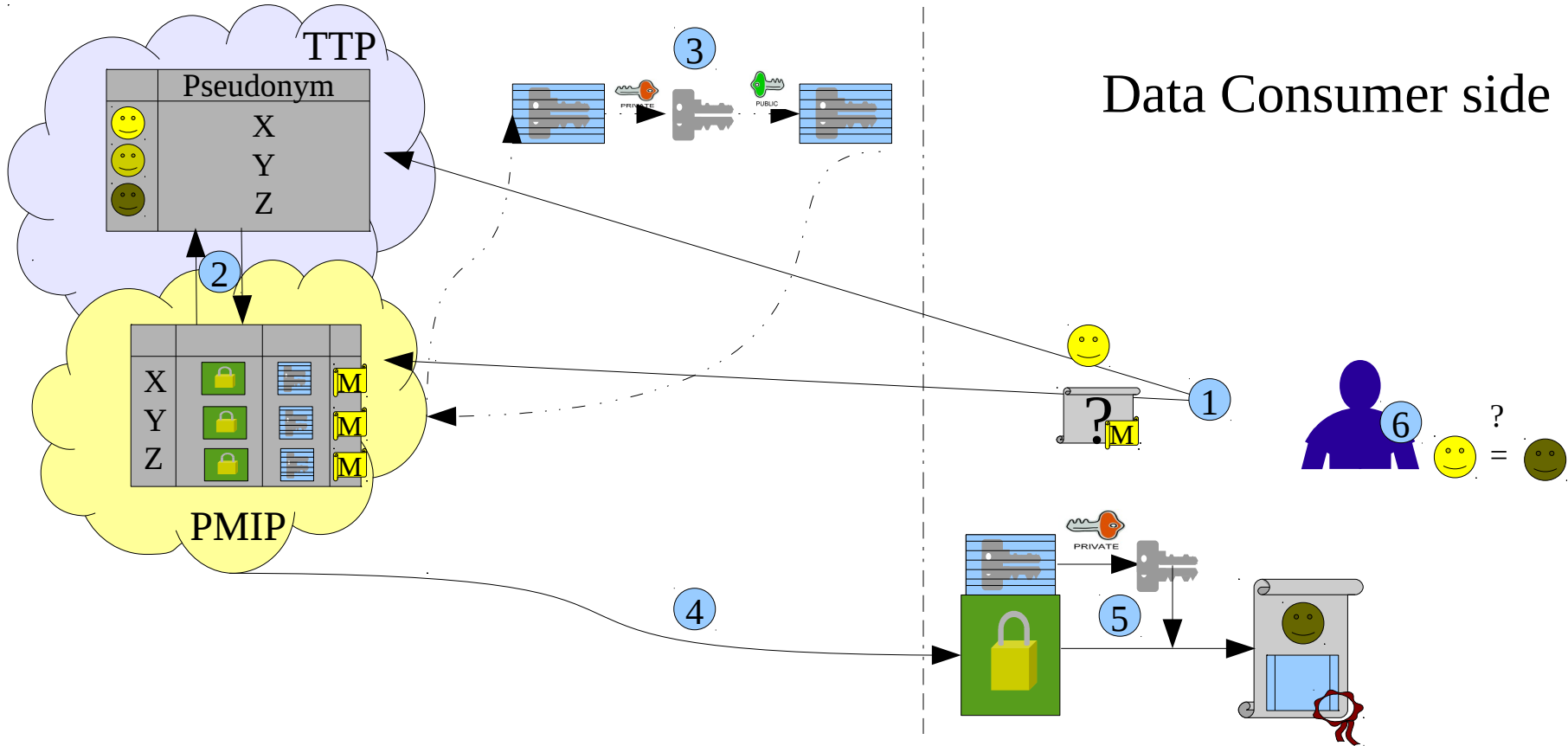
Other Registry Involvements?

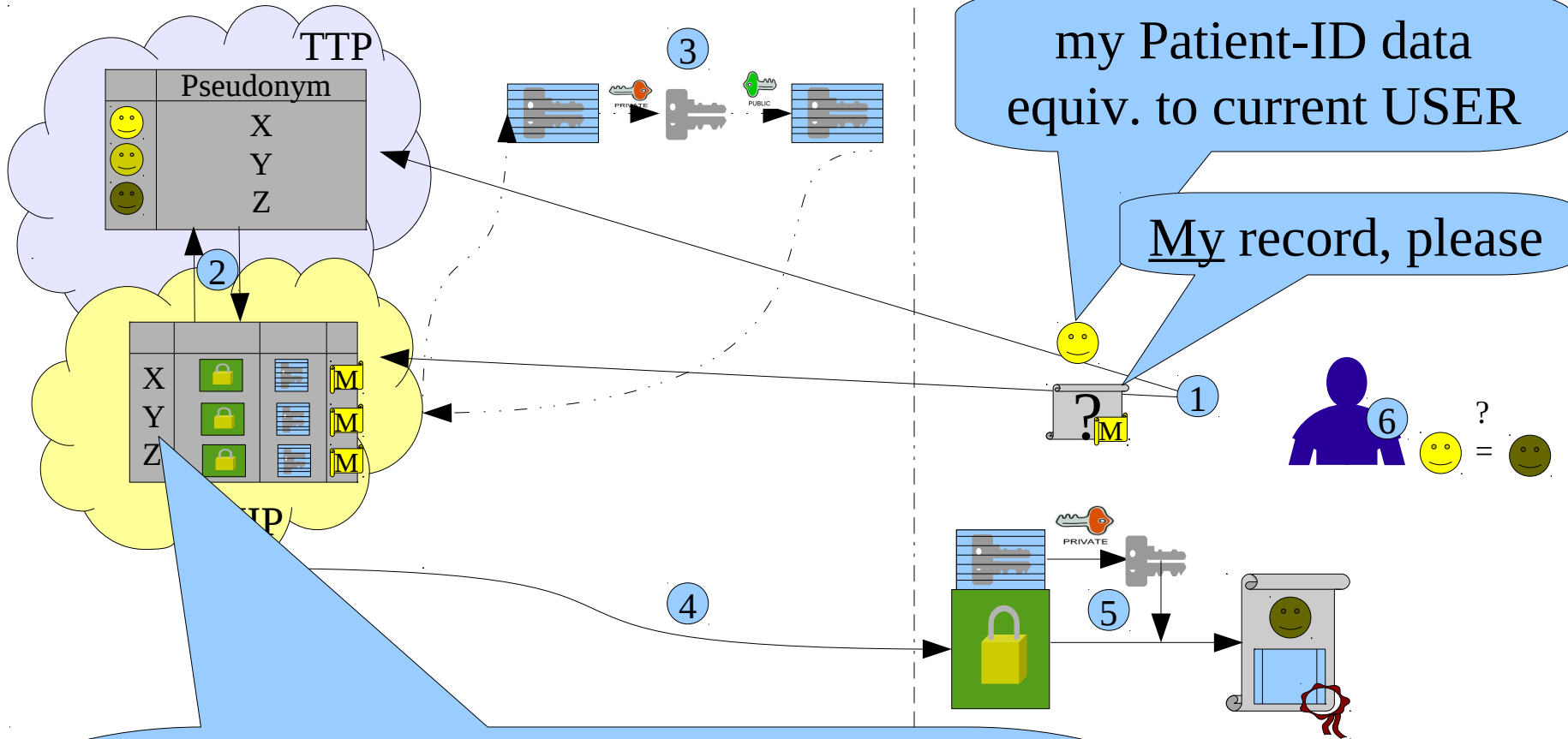
Direct Connections between Data Provider and National Registry?

Other usage, other ideas?



Login: technical re-useable Process for Patient login ?





USER with role PATIENT asks for his own data.
Pseudonym ↔ USER
will disclose
Pseudonym ↔ PATIENT

Results of Workshop-Discussion:

Anonymous login of USER at the eHealth Platform?

→ Login token assigned by the User Management (STS)

Declaration of IT-consent can NOT be (easily) signed !

Same for other documents provided by the patient.

→ USER with provable Login-token is acceptable?

Remarks of the Workshop:

- Other Topics, other remarks?