

Technical and Functional Components behind the eSanté Platform

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

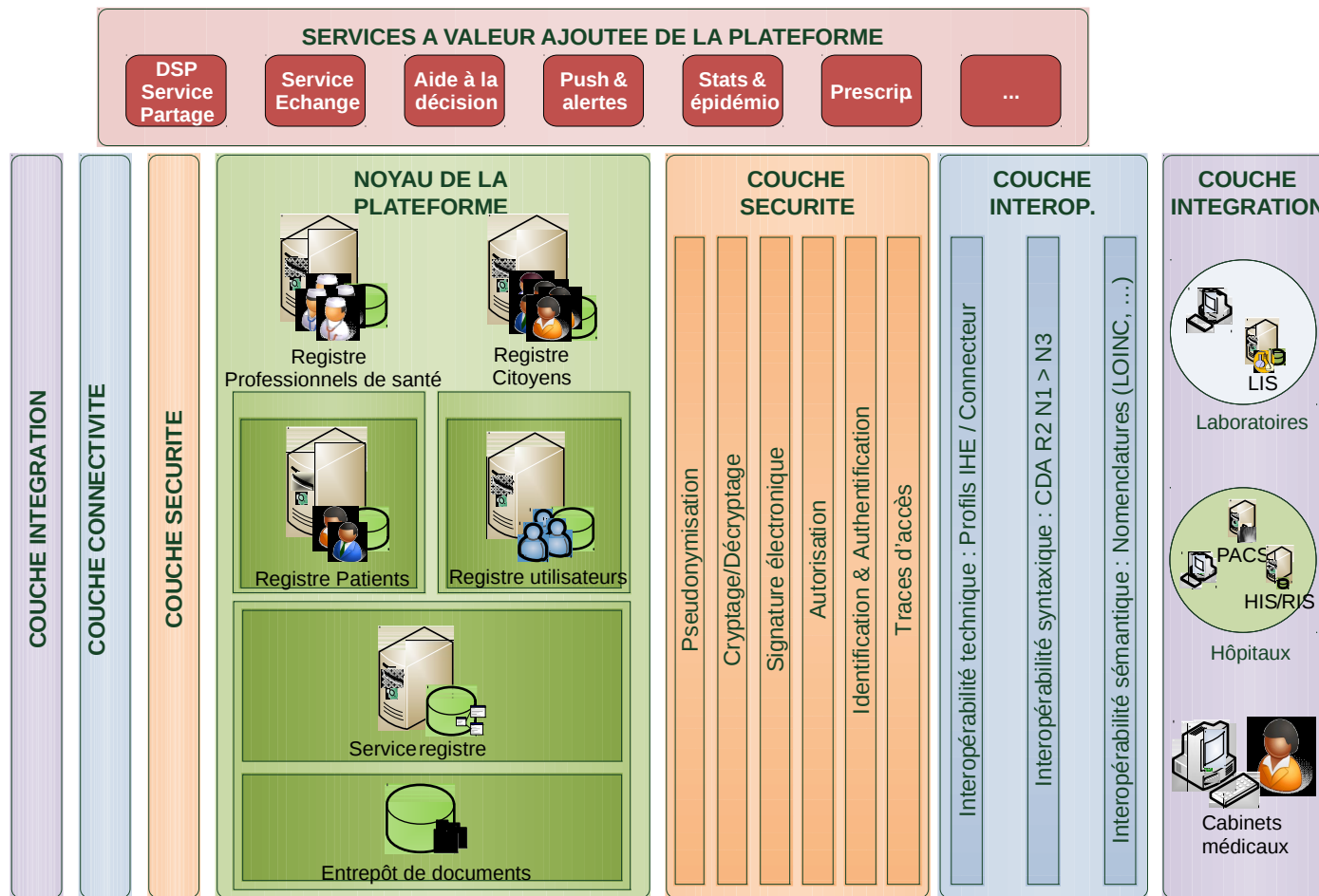
Toward a national eHealth Platform

Amphithéâtre Waasserhaus
Domaine Thermal de Mondorf
June 29 2011

CRP Henri Tudor / CR SANTEC

Is working as contractual partner for the Health Ministry

- Some Current Topics are
 - eSanté
 - GECAMed (Medical Office Data Software)
 - Bio4D (Integrated BioBank of Luxembourg)
- eSanté Projects
 - Analysis & Feasibility Study for eHealth (EFES)
 - National Electronic Radiology Record (CARA)
 - Electronic Exchange of Laboratory Results (LABO)



Part 1

- Exchanging Medical Information
- Sharing Medical Information

Part 2

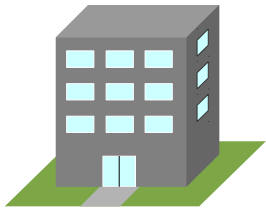
- How to guarantee Data Privacy ?
- How to ensure Data Privacy and Statistics ?

Part 3

- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- Logging and Alerts

information provider

information receiver



1 Hospital

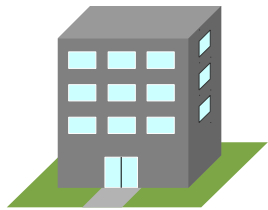
Medical Report



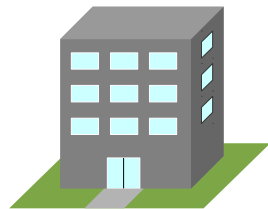
1 Doctor

information provider

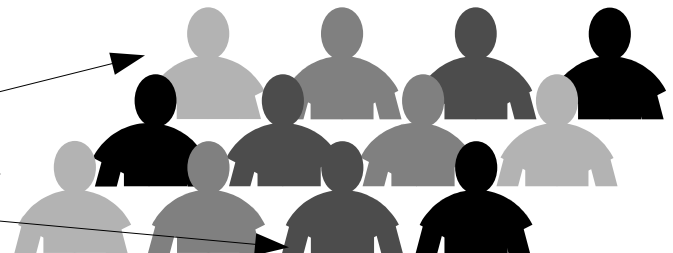
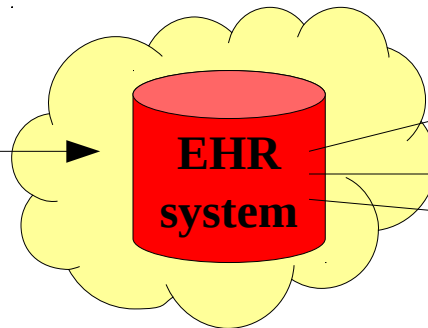
information receiver



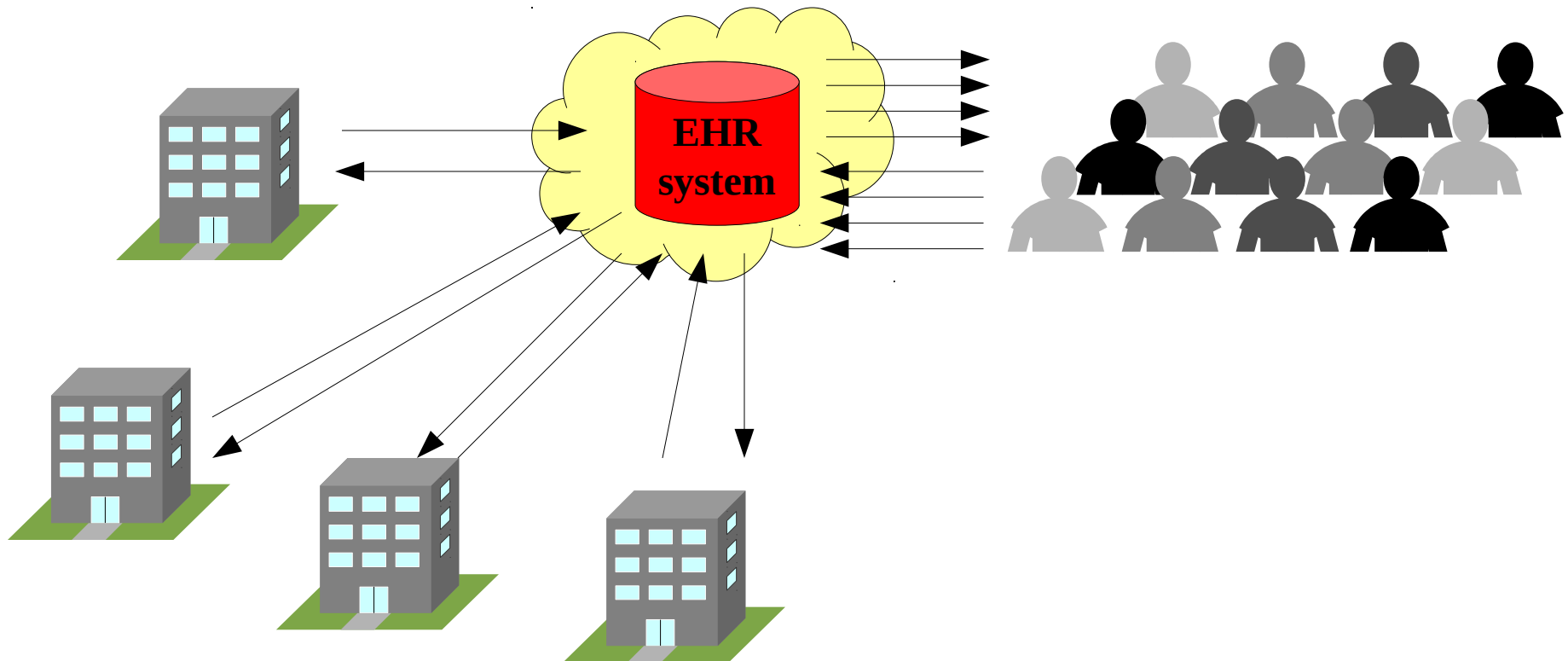
Medical Report

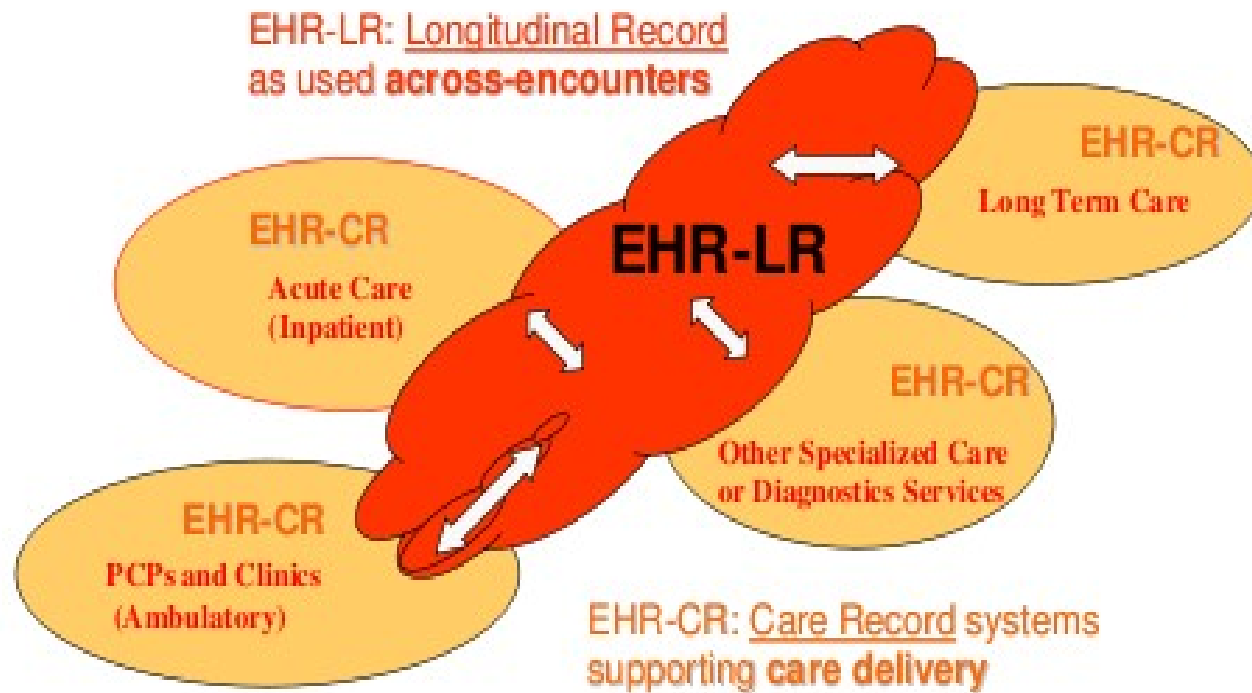


Hospital



information provider = information receiver = eHealth participant





Picture source: IHE International. IHE Profiles. URL: <http://www.ihe.net/profiles/>

Part 1

- Exchanging Medical Information
- Sharing Medical Information

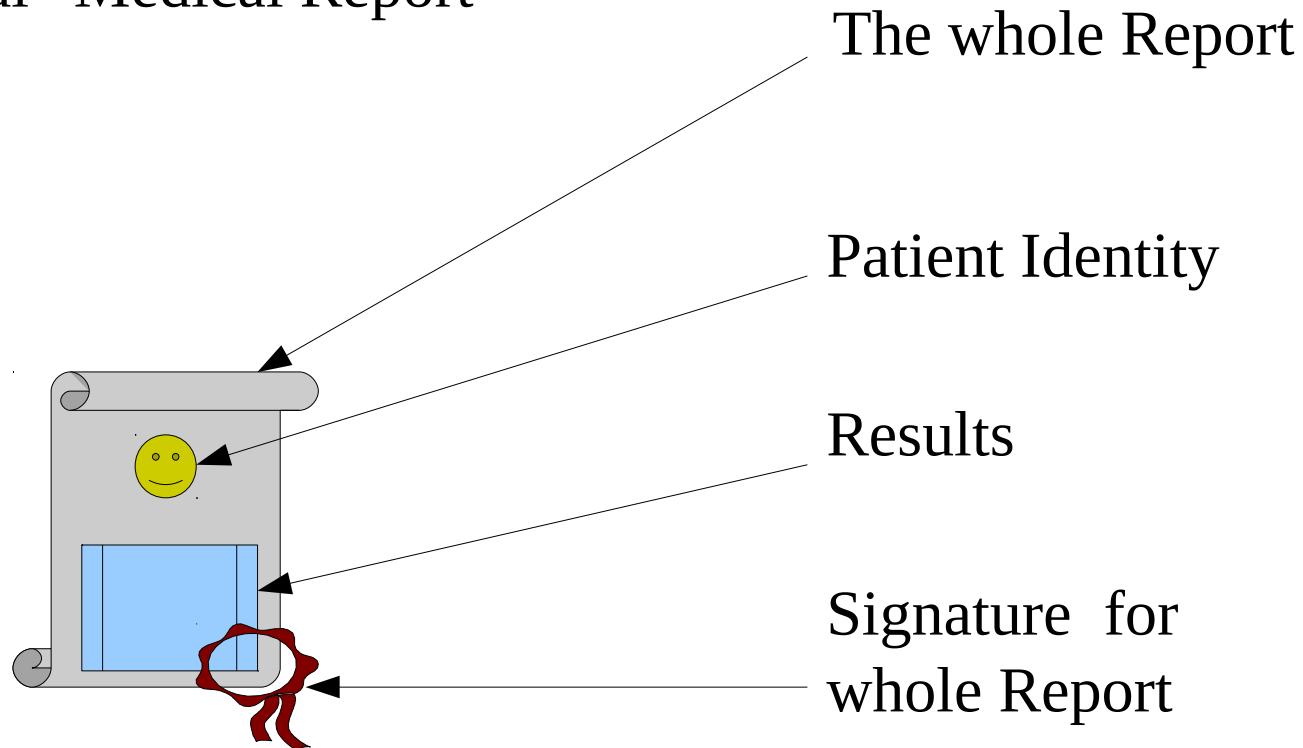
Part 2

- How to guarantee Data Privacy ?
- How to ensure Data Privacy and Statistics ?

Part 3

- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- Logging and Alerts

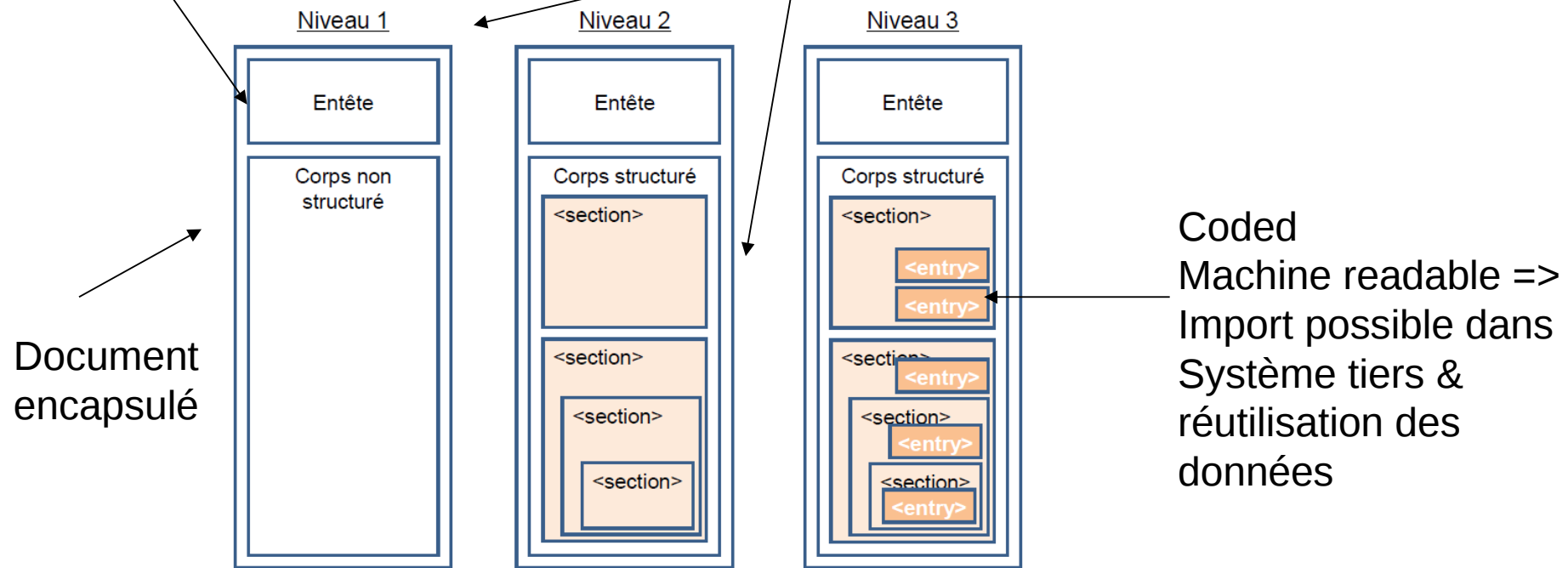
General “Medical Report”



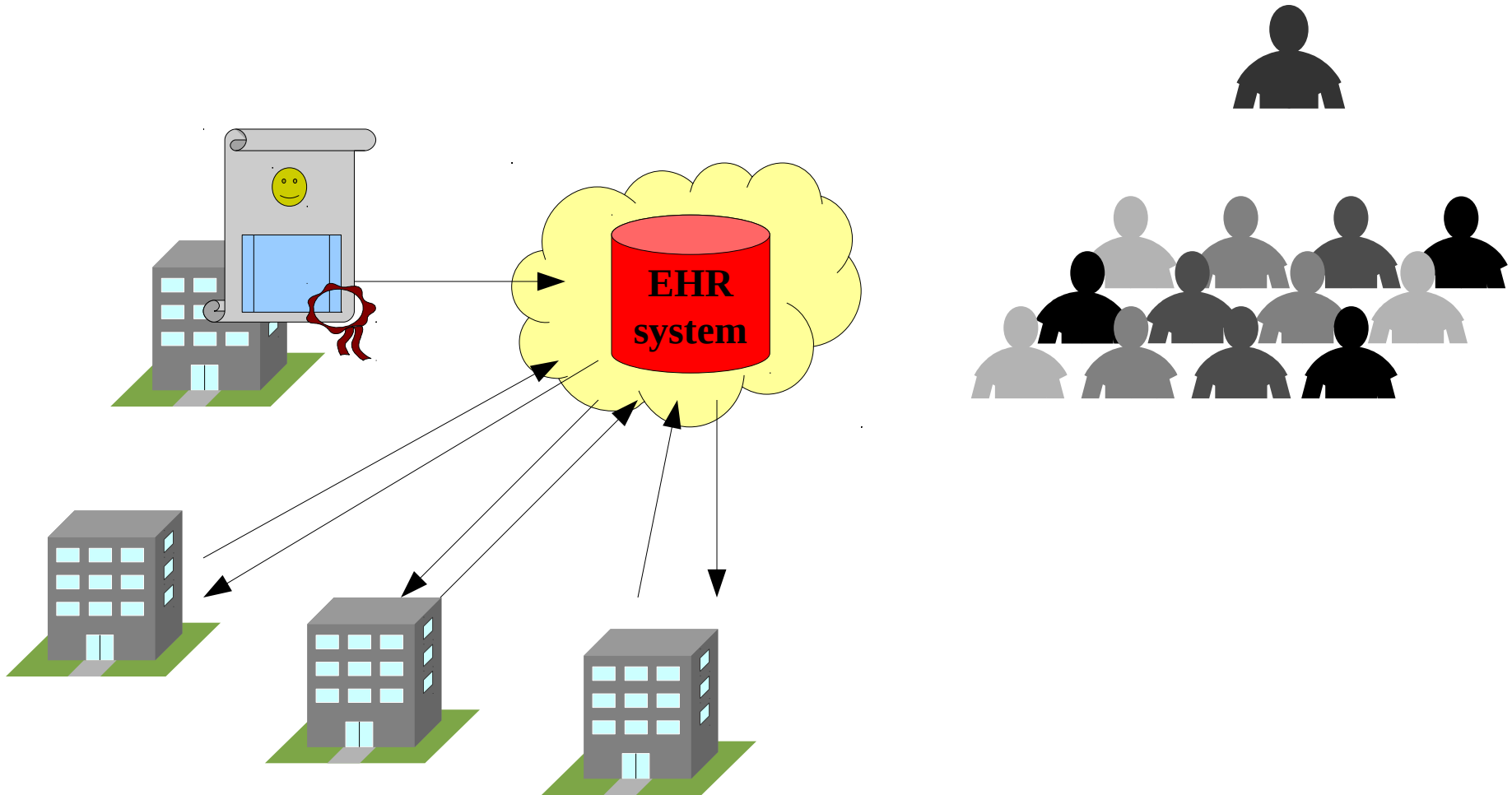
Technically represented as
Clinical Document Architecture (CDA)

Contexte comme méta-
données dans l'entête
(patient, laboratoire,
auteur, date,....)

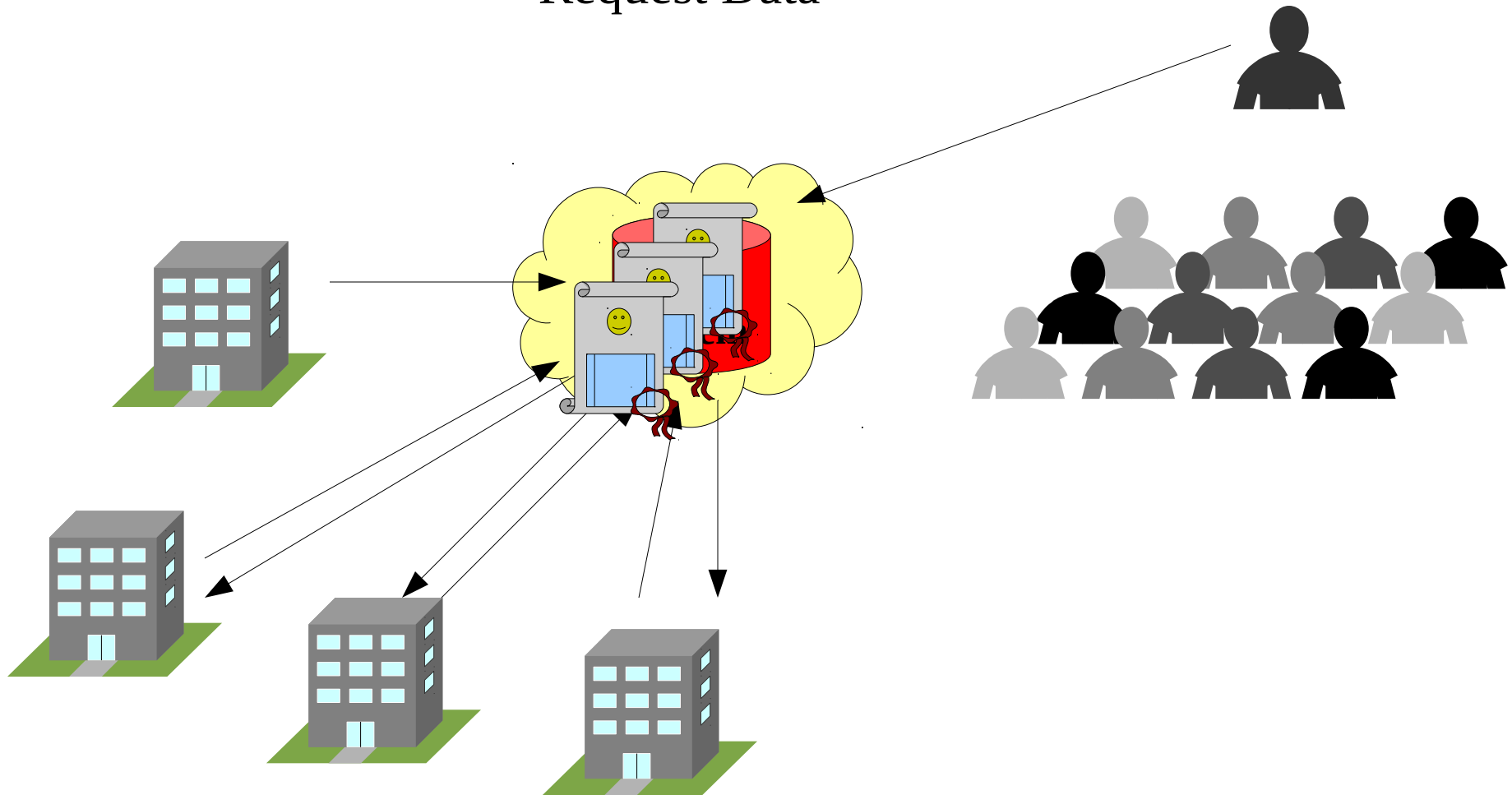
Human readable=> affichage utilisateur



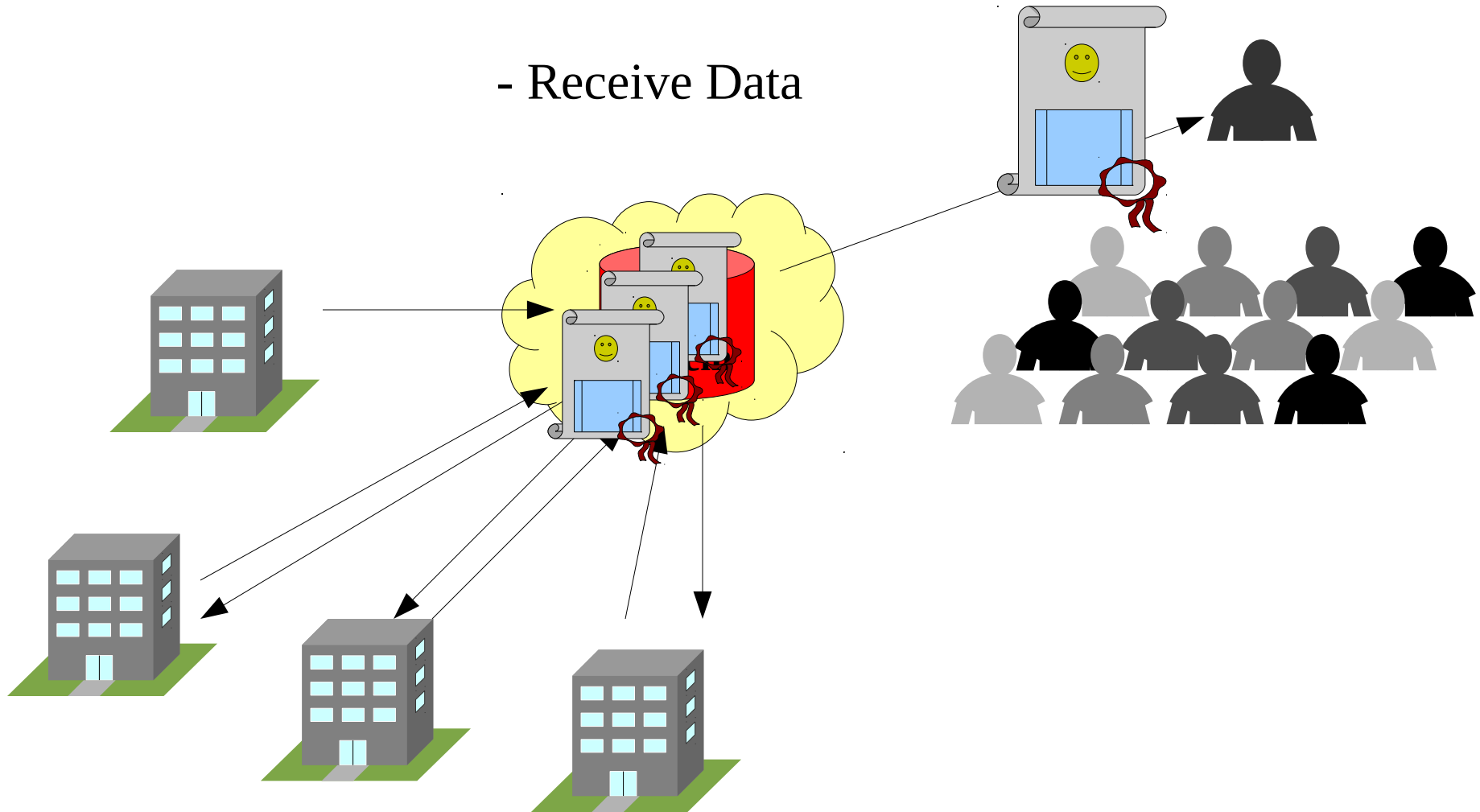
- Provide Data



- Request Data

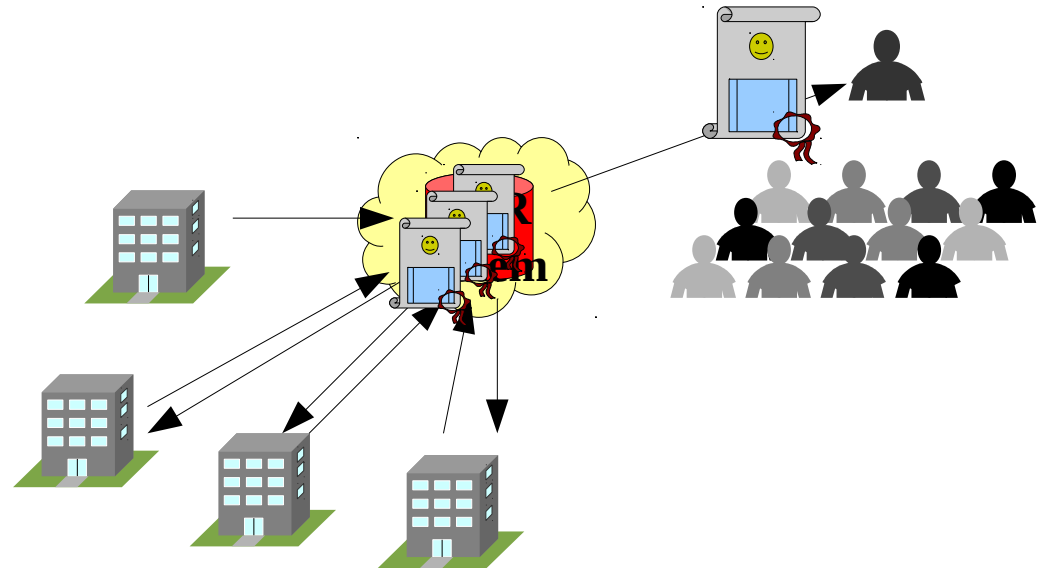


- Receive Data

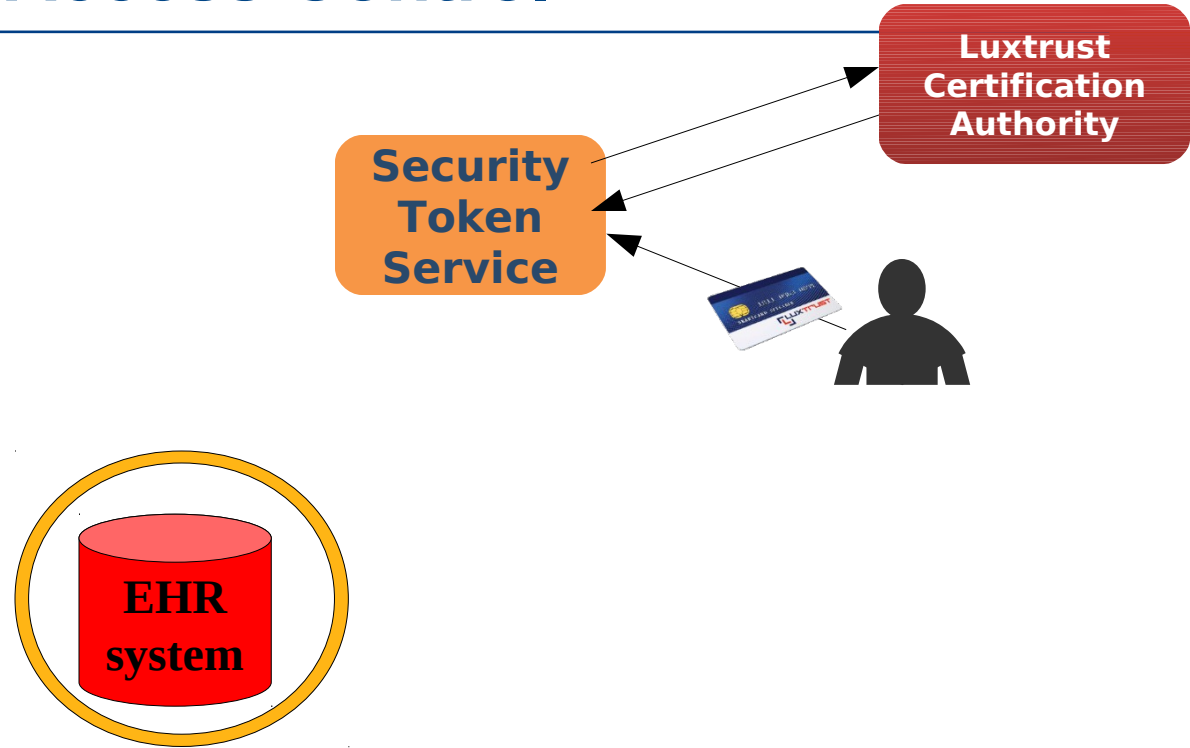


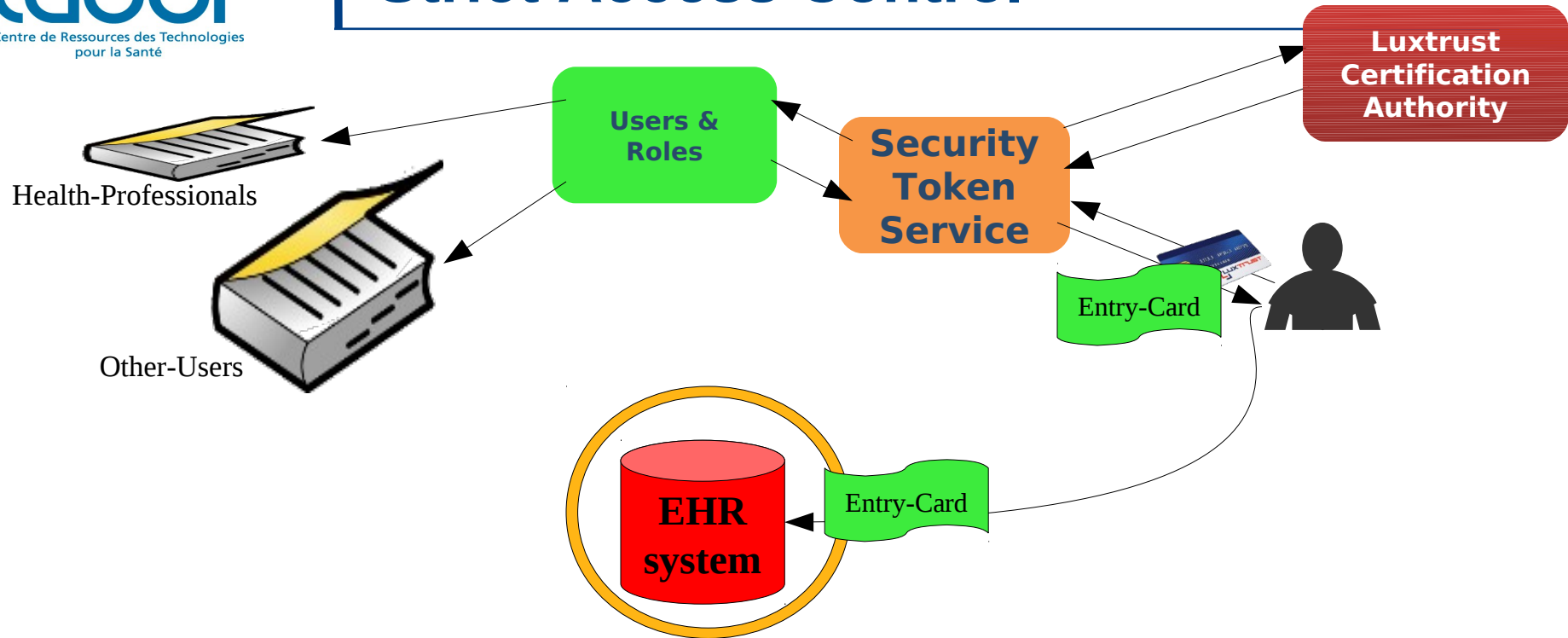
- Life and Accident Insurance Companies
- Building and Loan Association
- Employer, current and future
- ...

- Strict Access Control
- Encryption of Medical Information



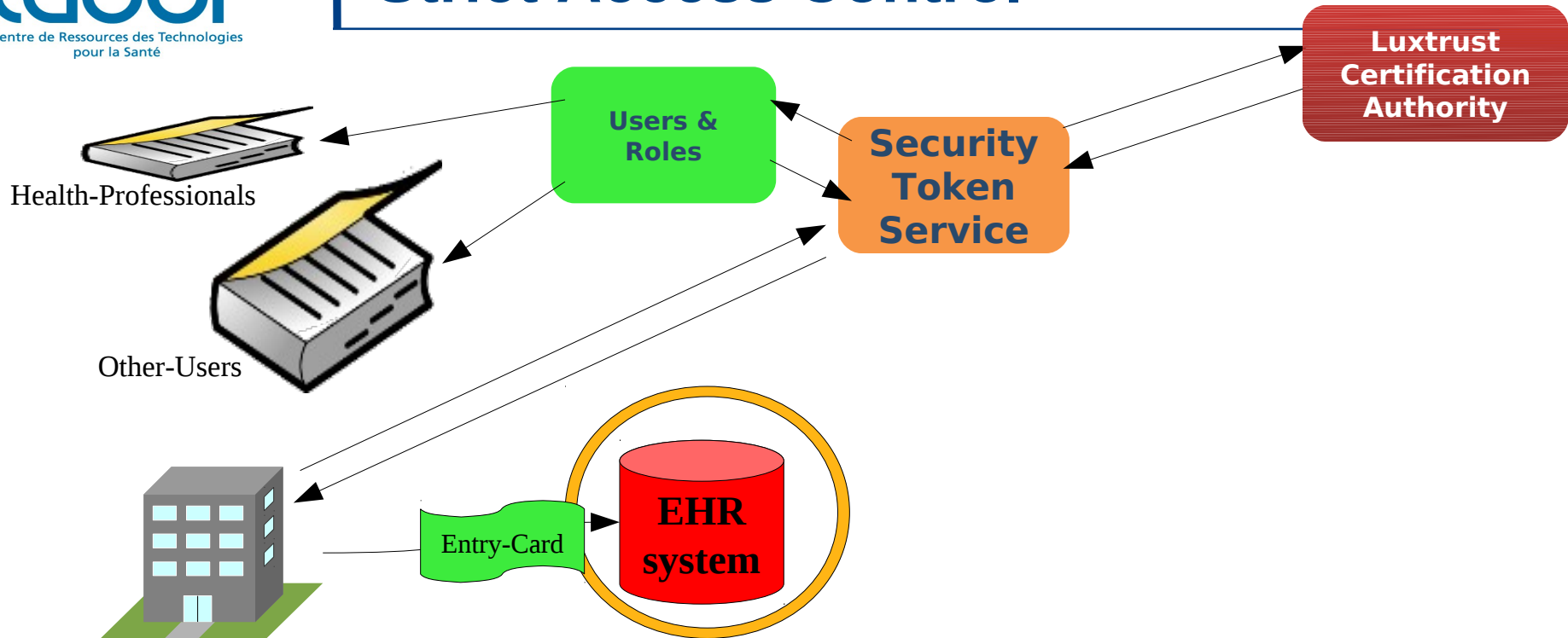
Strict Access Control





Access only with Temporary Entry Card

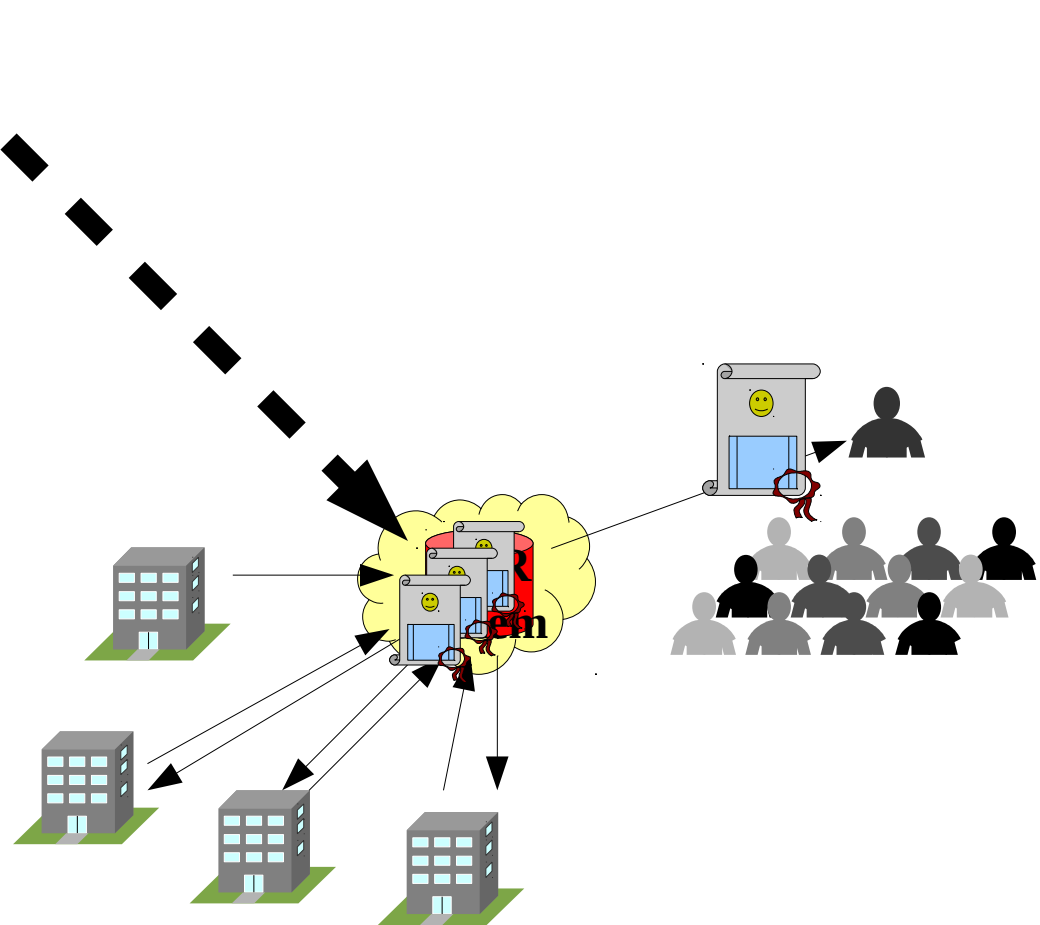
Strict Access Control



**Same processing for Data Provider
(institutional or private credentials)**

Strict Access Control

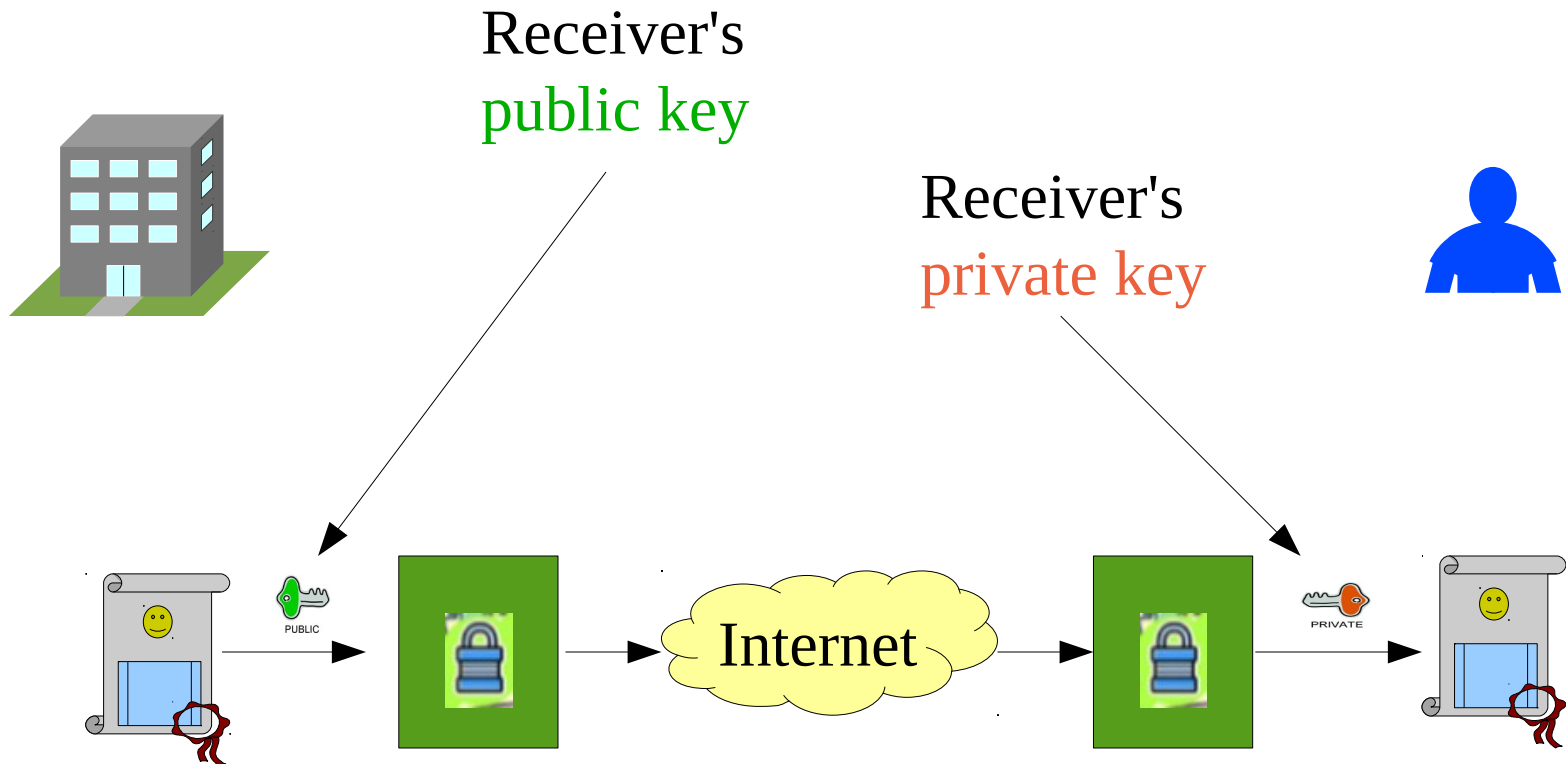
Encryption of Medical Information



Secure 1 → 1 exchange

1 Provider

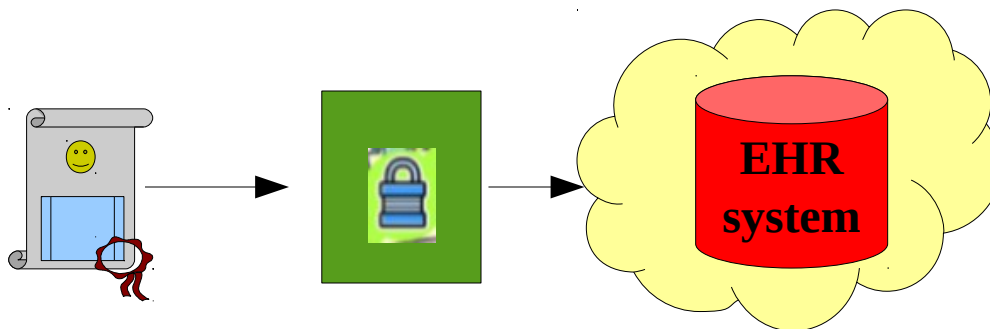
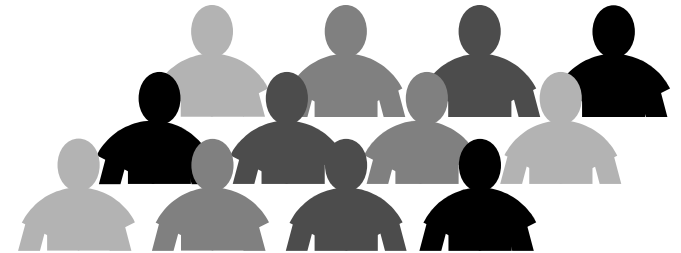
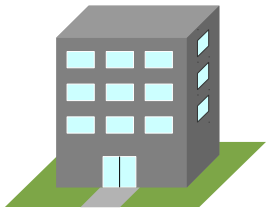
1 Receiver



Secure 1 → N exchange

1 provider

N receivers

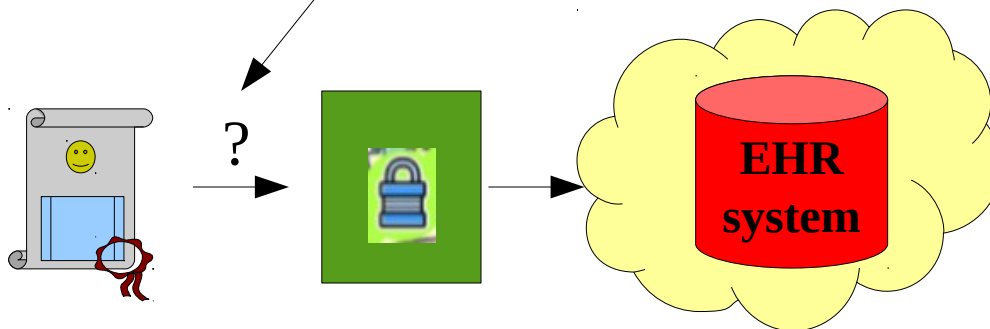
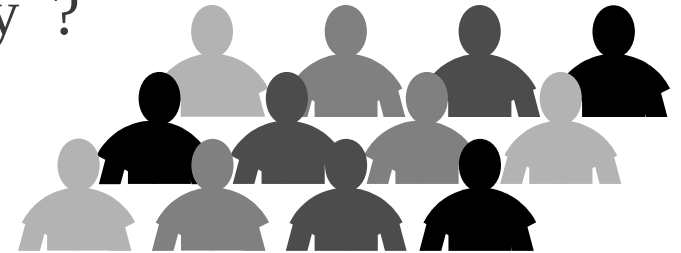
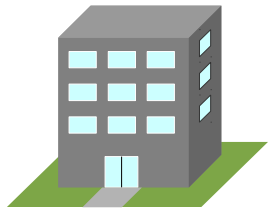


Question 1: which public key

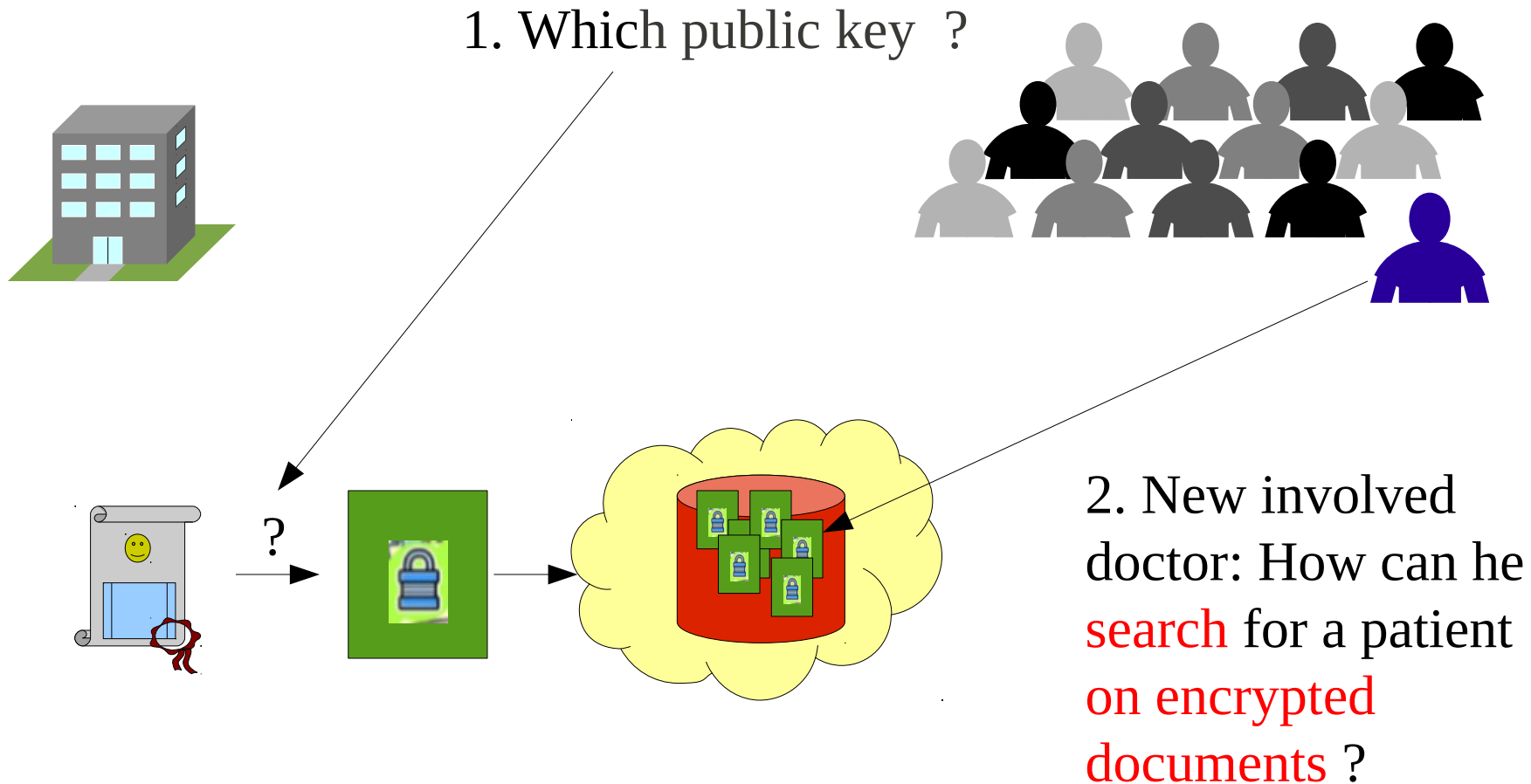
N receivers

1 provider

1. Which public key ?

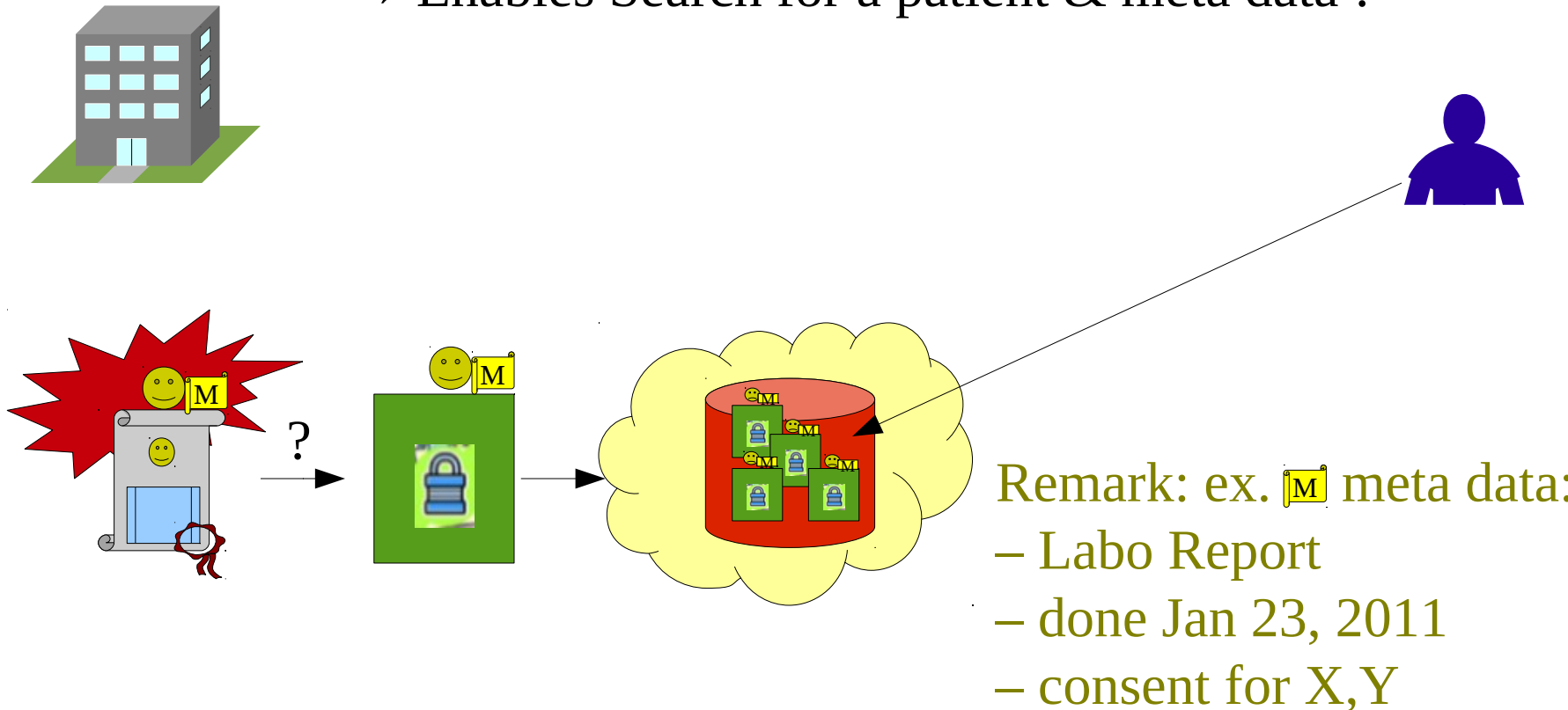


Question 2: new receiver involved

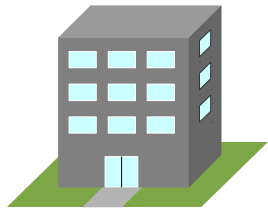


Solution for Patient Search

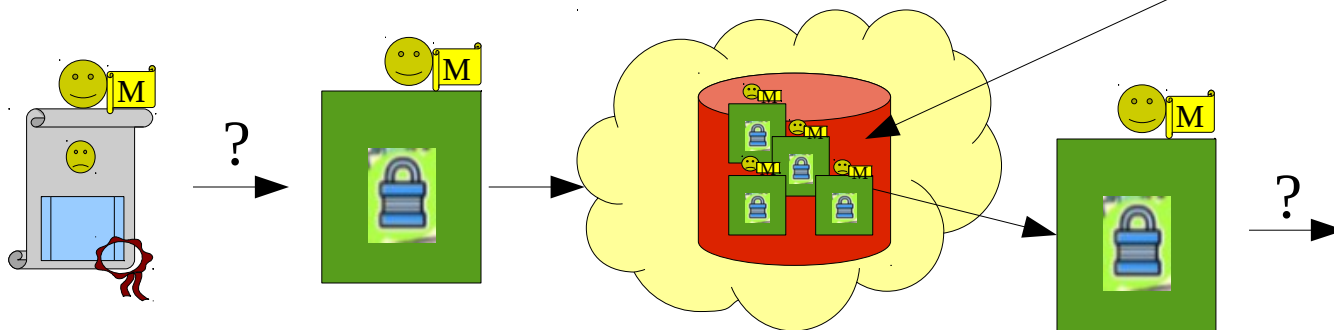
- a) Extract **Identity data & Meta data** ☺ M
- b) Attach Meta data without encryption:
→ Enables Search for a patient & meta data !



Open: Encryption / Decryption



... but ... Encryption ?
Decryption ?

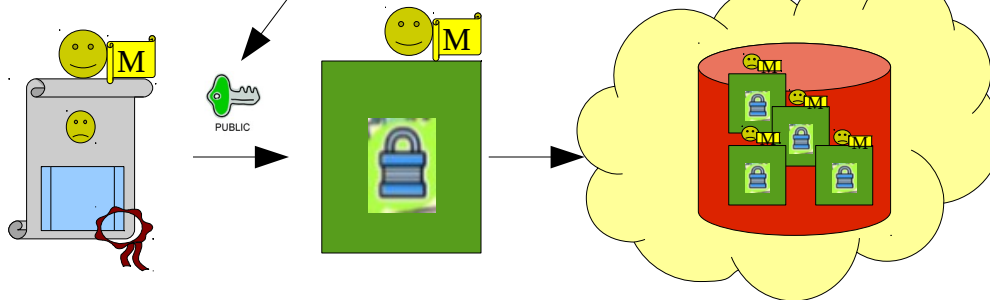
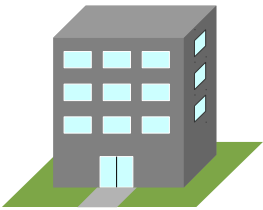


Encryption

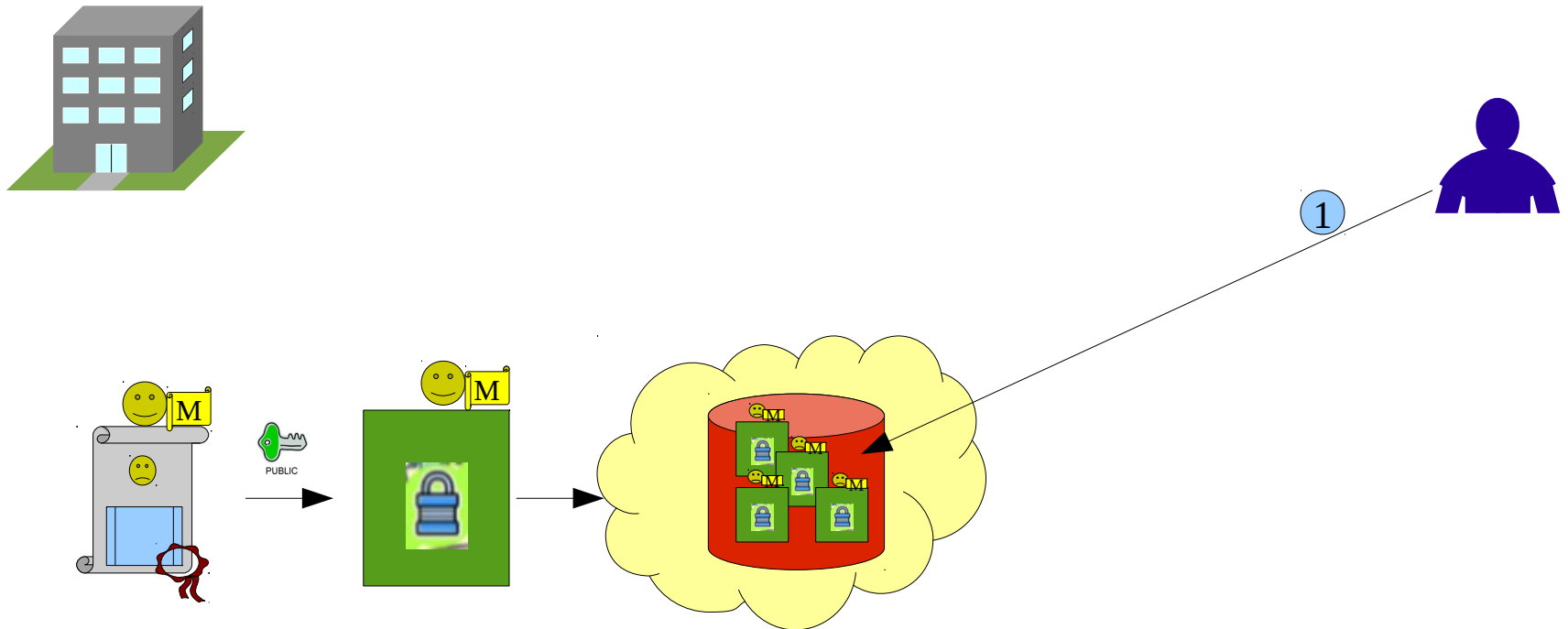
Solution: Encryption with server key

Use the
Server's
public key

... & re-encrypt later for a
requesting receiver



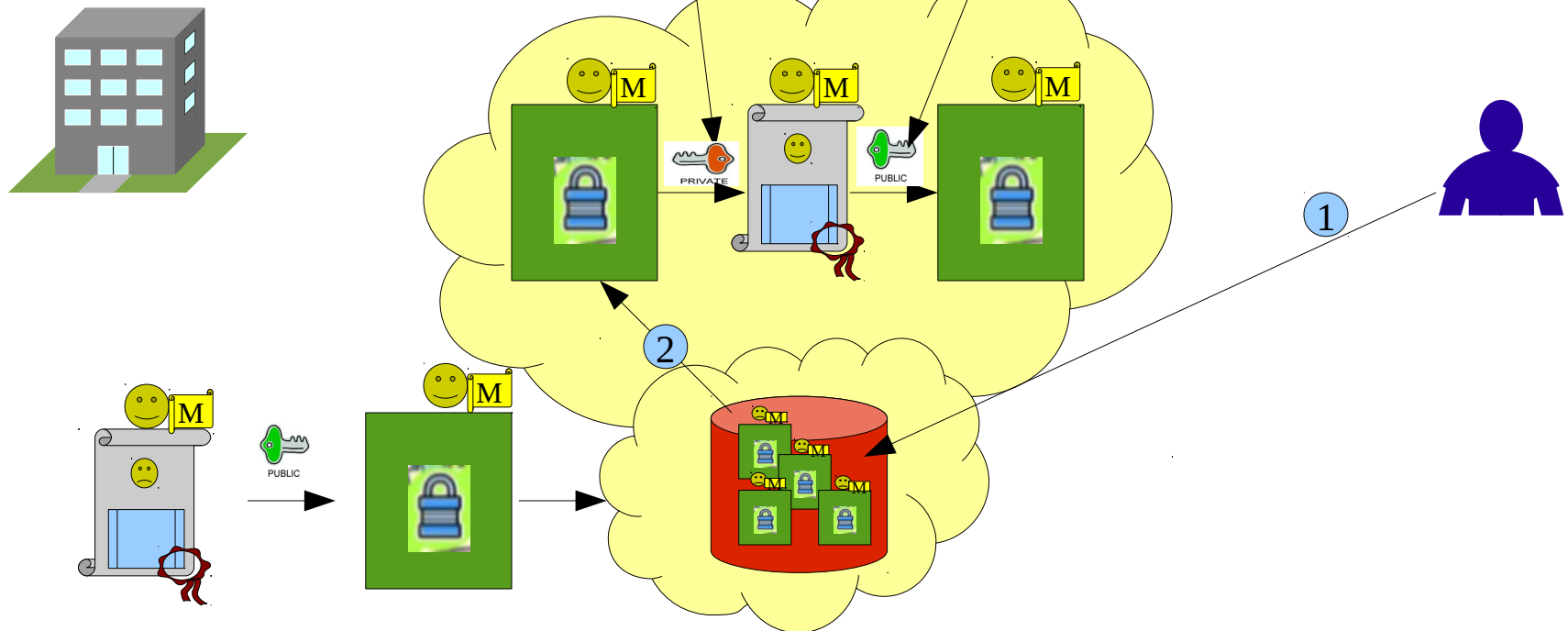
① Search for Patient



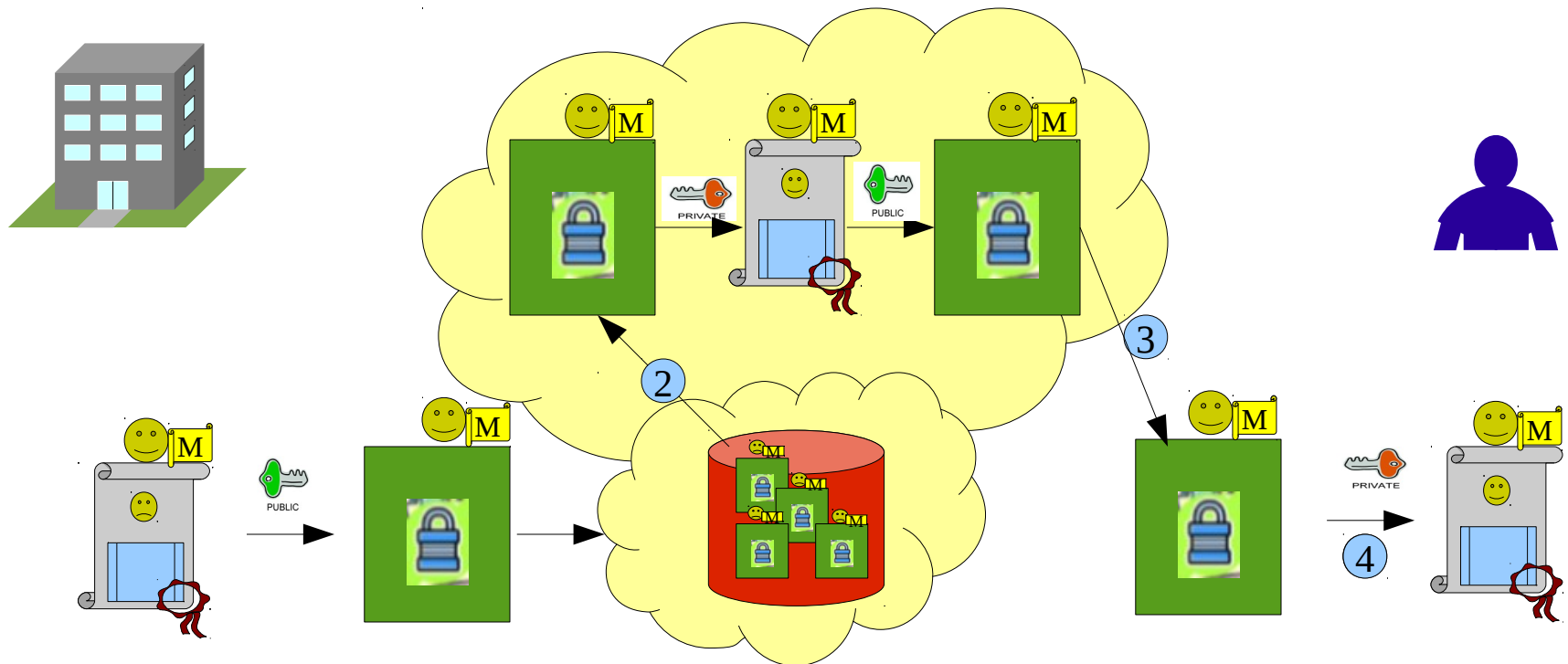
- 1 Search for Patient
- 2 Re-Encryption for Receiver

Server's **private key**

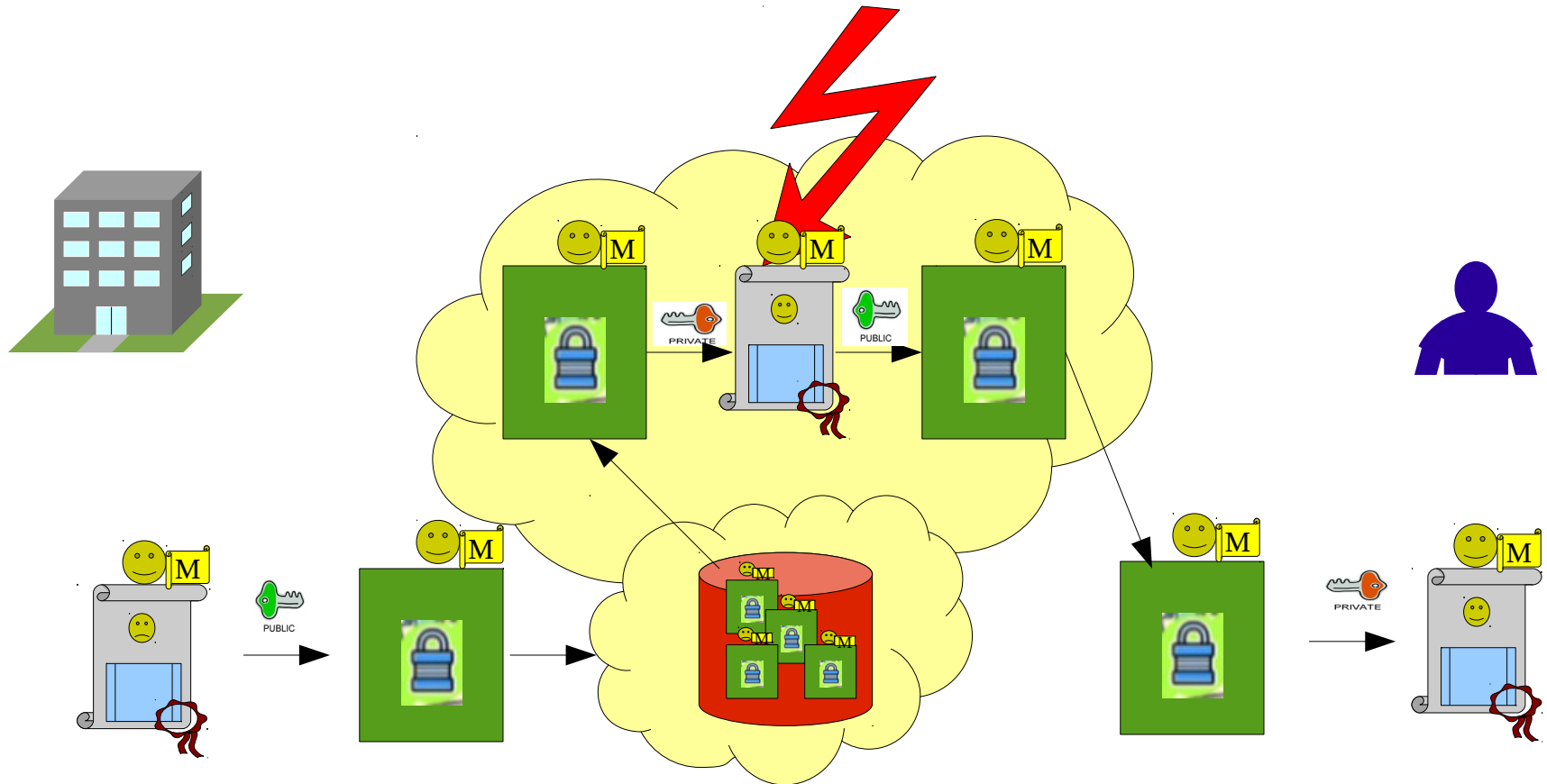
Receiver's **public key**



- 1 Search for Patient
- 2 Re-Encryption for Receiver
- 3 Deliver
- 4 Decrypt on Receivers side

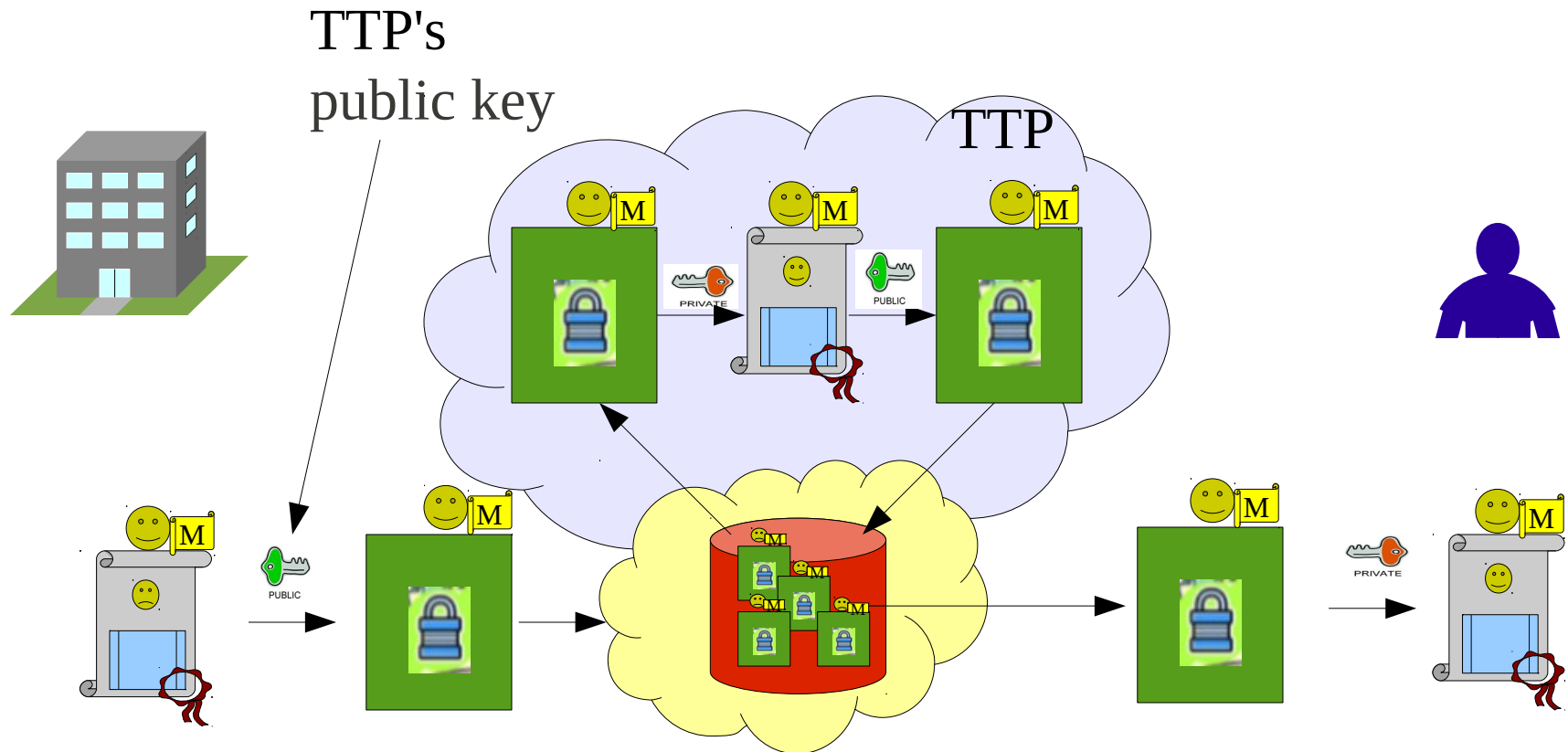


SECURITY PROBLEM !



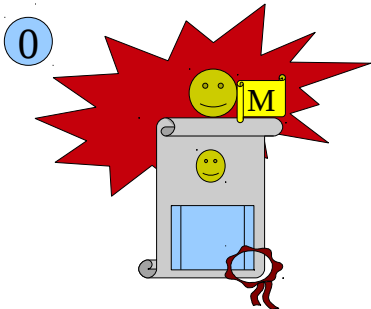
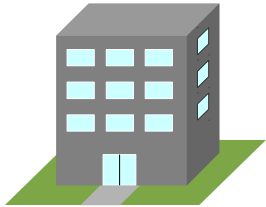
.... report is disclosed during re-encryption on server

Trusted Third Party (TTP) for Re-Encryption ?



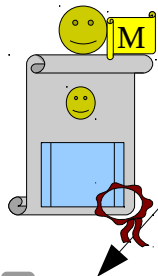
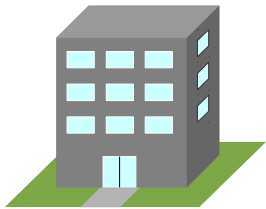
.... only shifts the intruder/admin problem to the TTP

0 Extract Identity Data and Metadata



Solution for Secure Data Sharing

- ① Extract Identity Data and Metadata
- ② Generate a symmetric key (for each document)

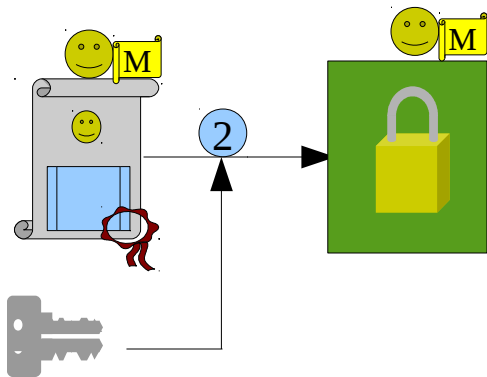
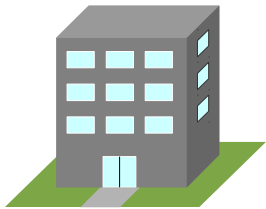


①



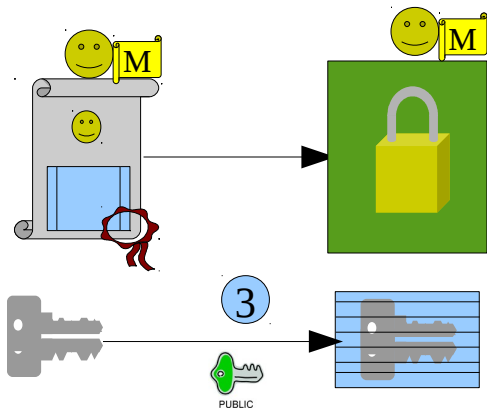
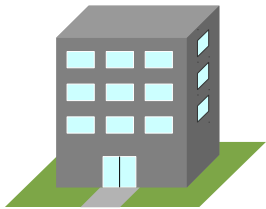
Solution for Secure Data Sharing

- ① Extract Identity Data and Metadata
- ② Generate a symmetric key (for each document)
- ③ Encrypt Report with symmetric key



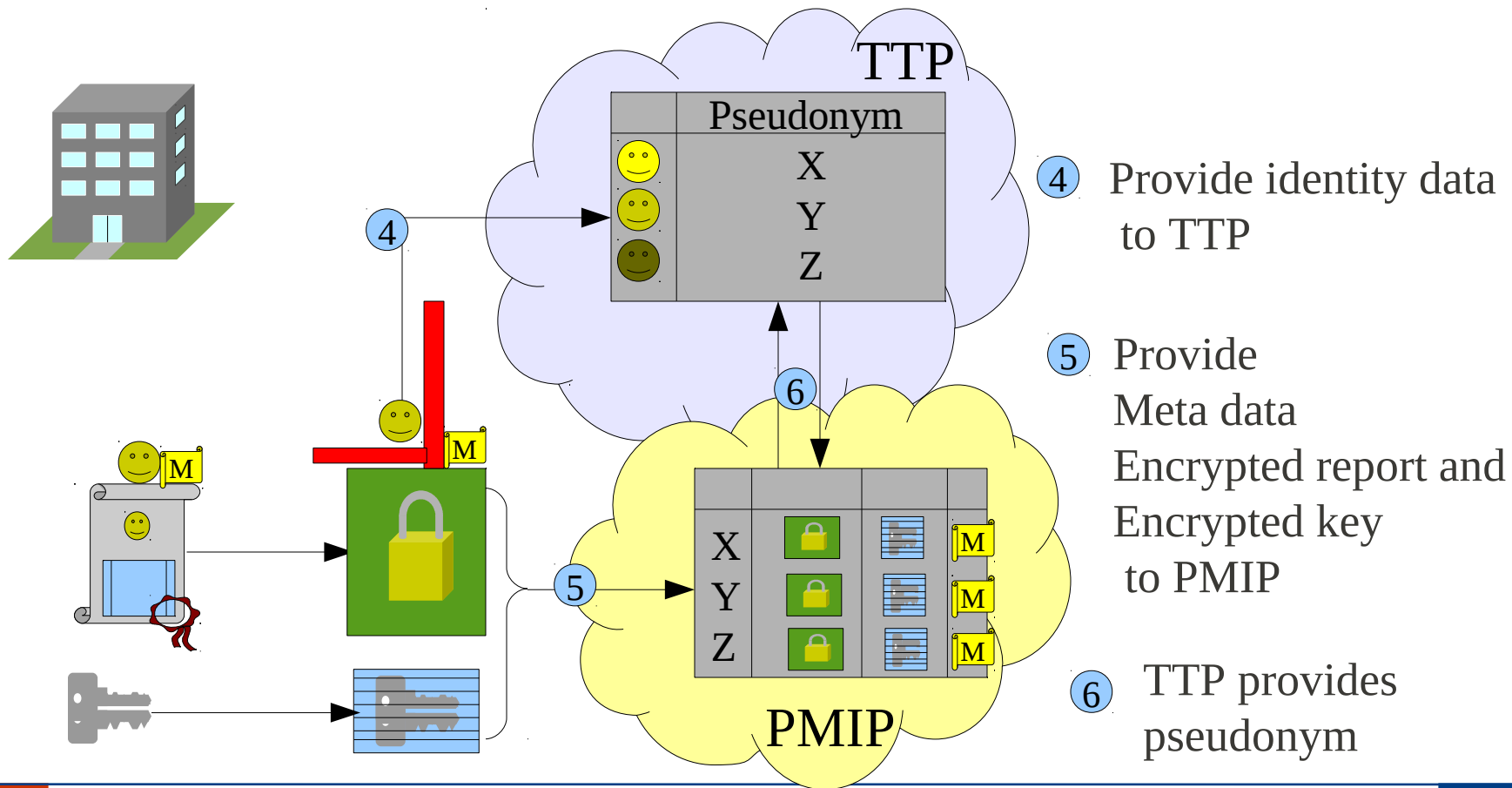
Solution for Secure Data Sharing

- ① Extract Identity Data and Metadata
- ② Generate a symmetric key (for each document)
- ③ Encrypt Report with symmetric key
- ④ Encrypt symmetric key with TTP's public key

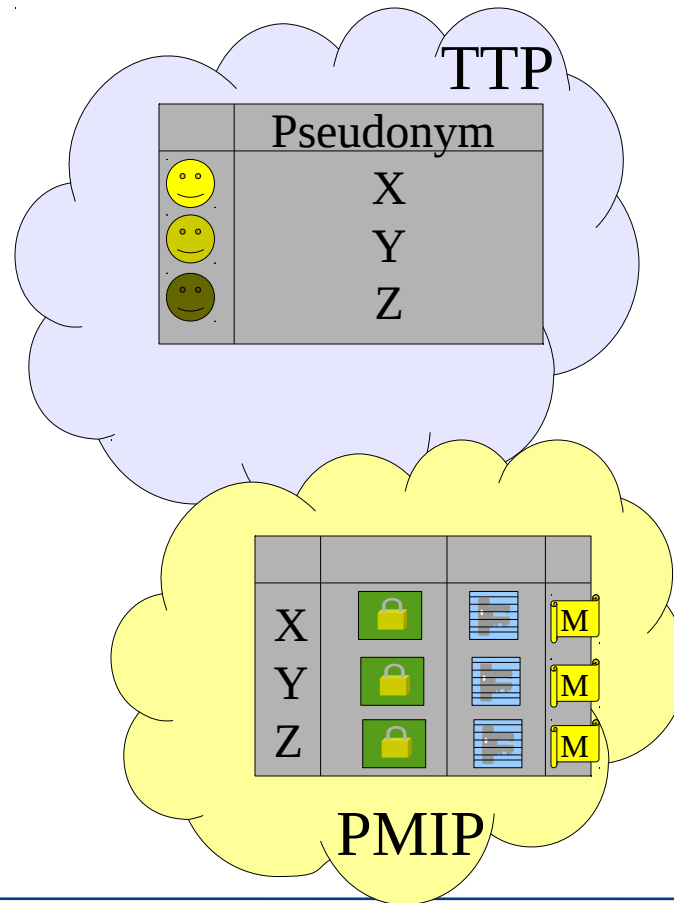


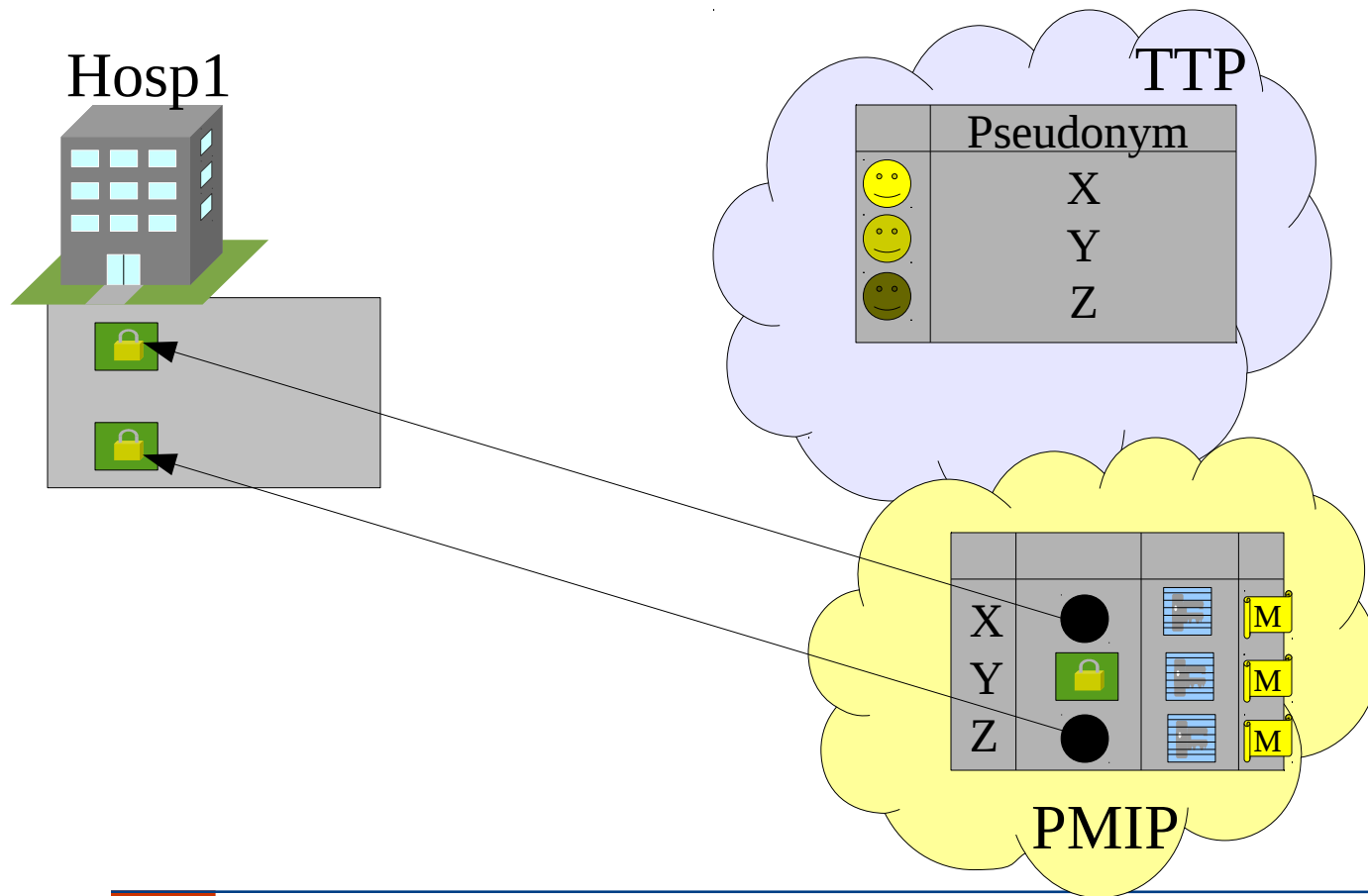
Solution for Secure Data Sharing

- 0 Extract Identity Data and Metadata
- 1 Generate a symmetric key (for each document)
- 2 Encrypt Report with symmetric key
- 3 Encrypt symmetric key with TTP's public key



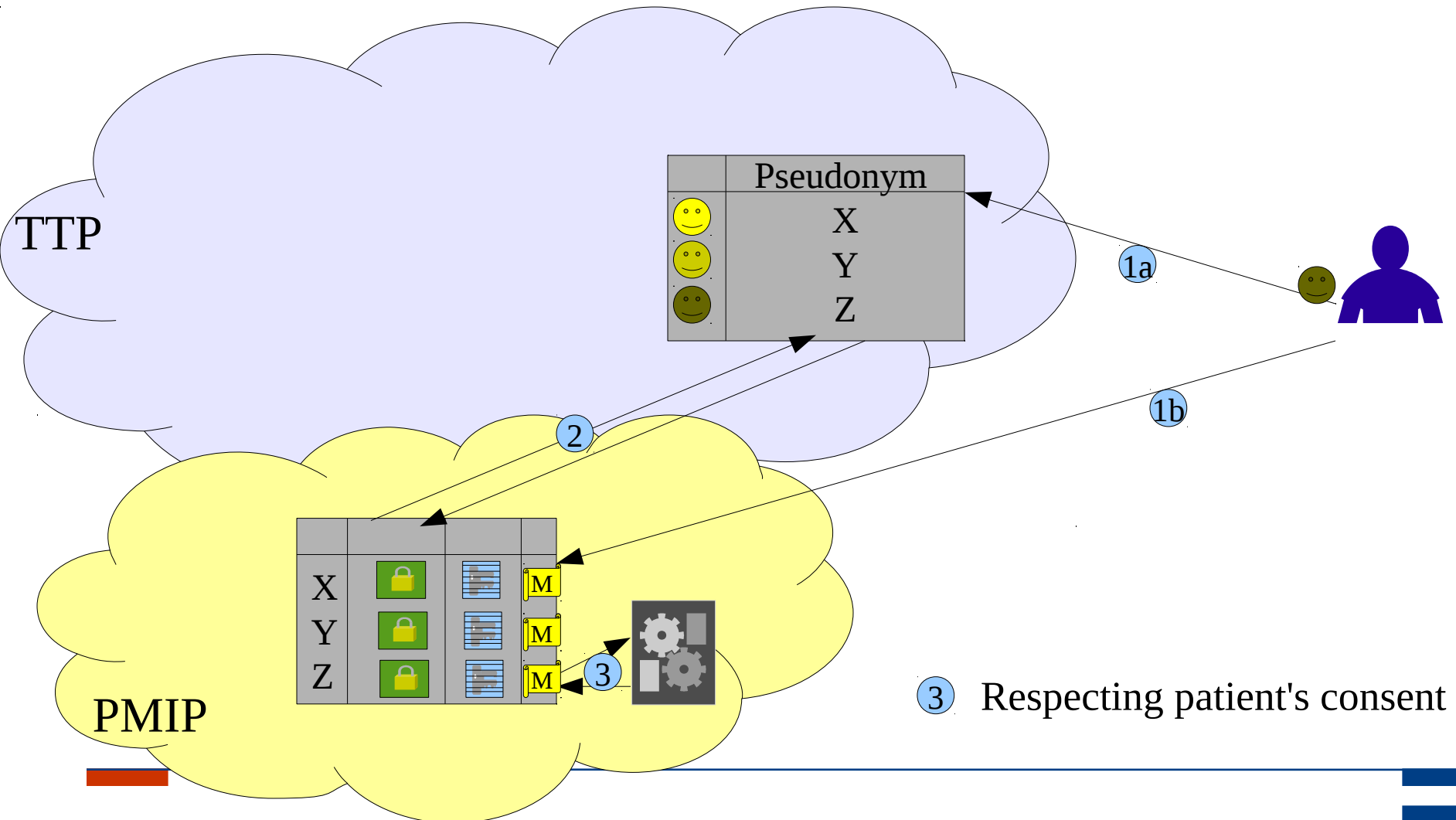
- TTP holds private key to decrypt symmetric keys.
- Symmetric key is needed to decrypt the report.
- Patient search on TTP is possible.
- **Admin or intruder problem solved for data storage!**

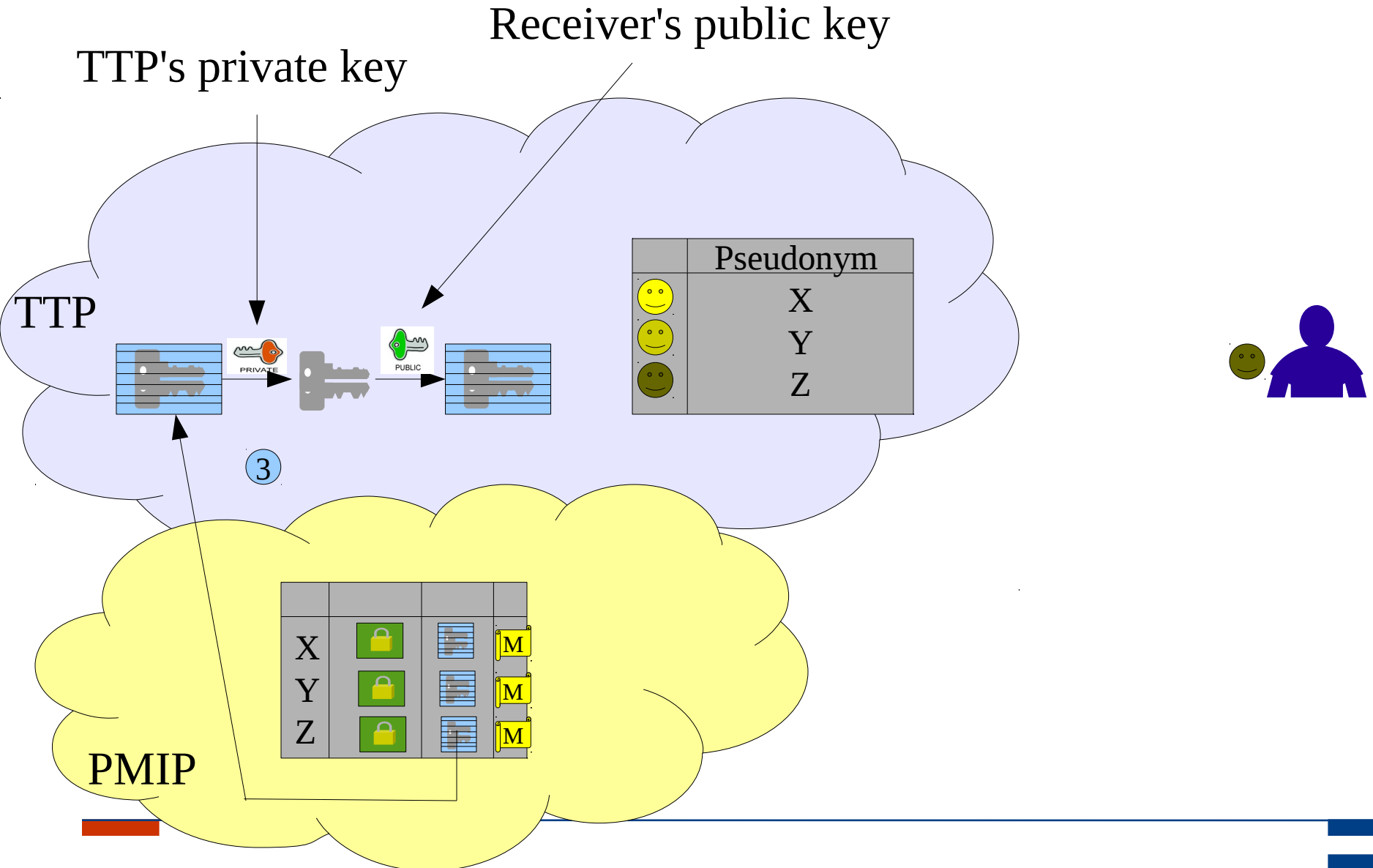


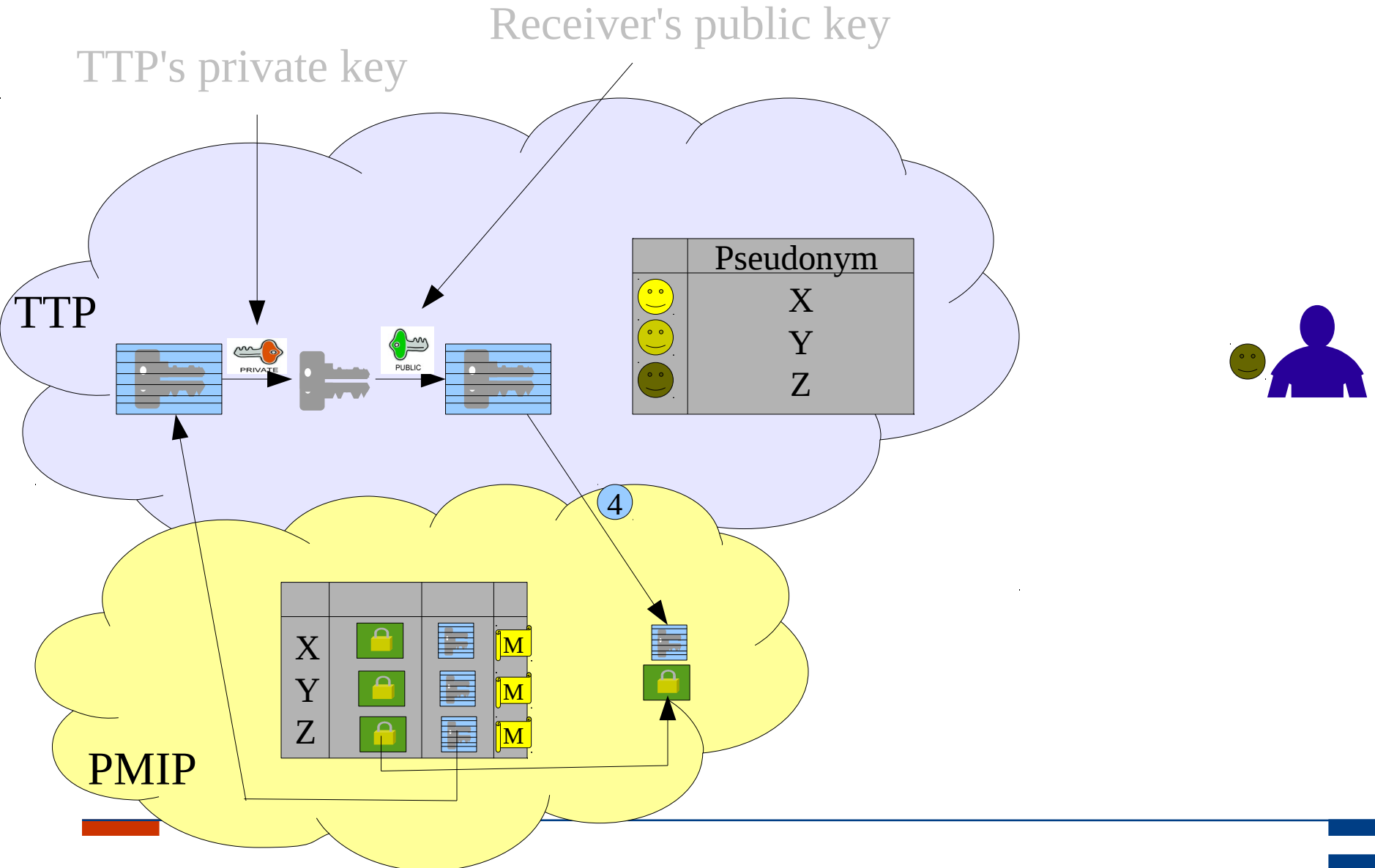


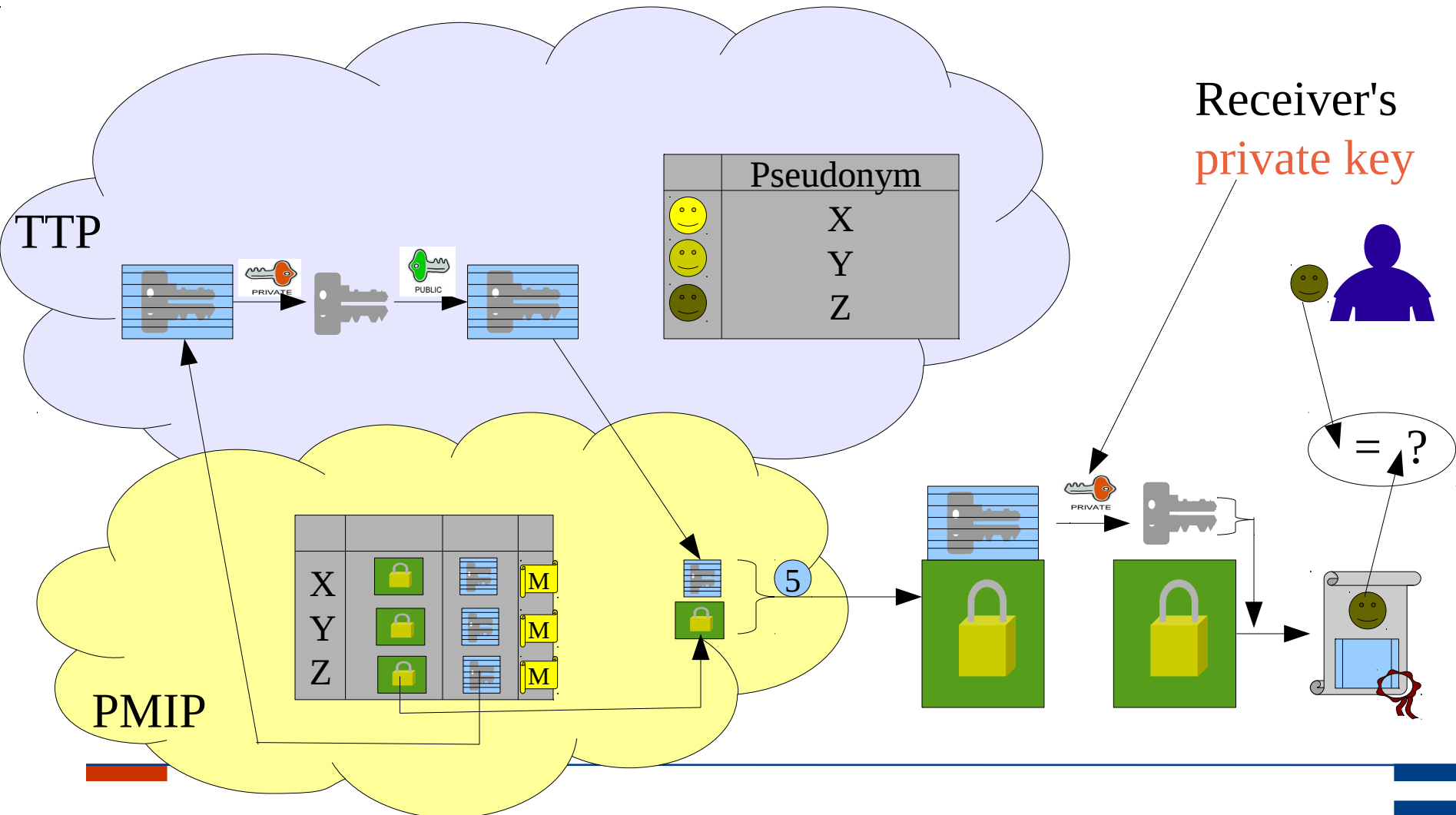
Information Retrieval

- 1a Open a query session for a patient
- 1b Searching available Labo Results
- 2 PMIP Pseudonym retrieval

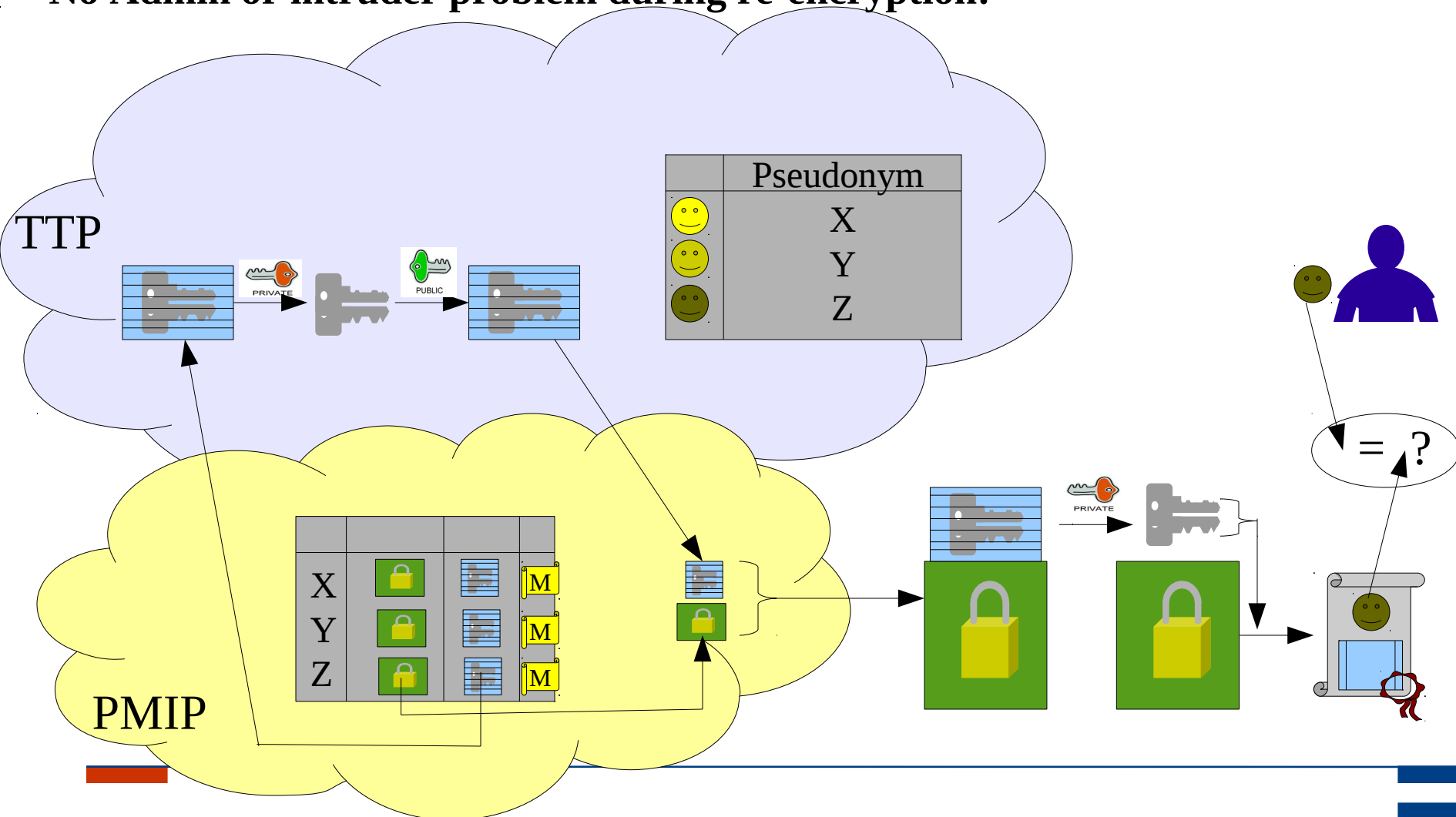








- TTP re-encrypt (discloses) the report keys, but it never has access to the reports.
- PMIP manages encrypted report keys and encrypted reports, but it never has the keys.
- **No Admin or intruder problem during re-encryption!**



Part 1

- Exchanging Medical Information
- Sharing Medical Information

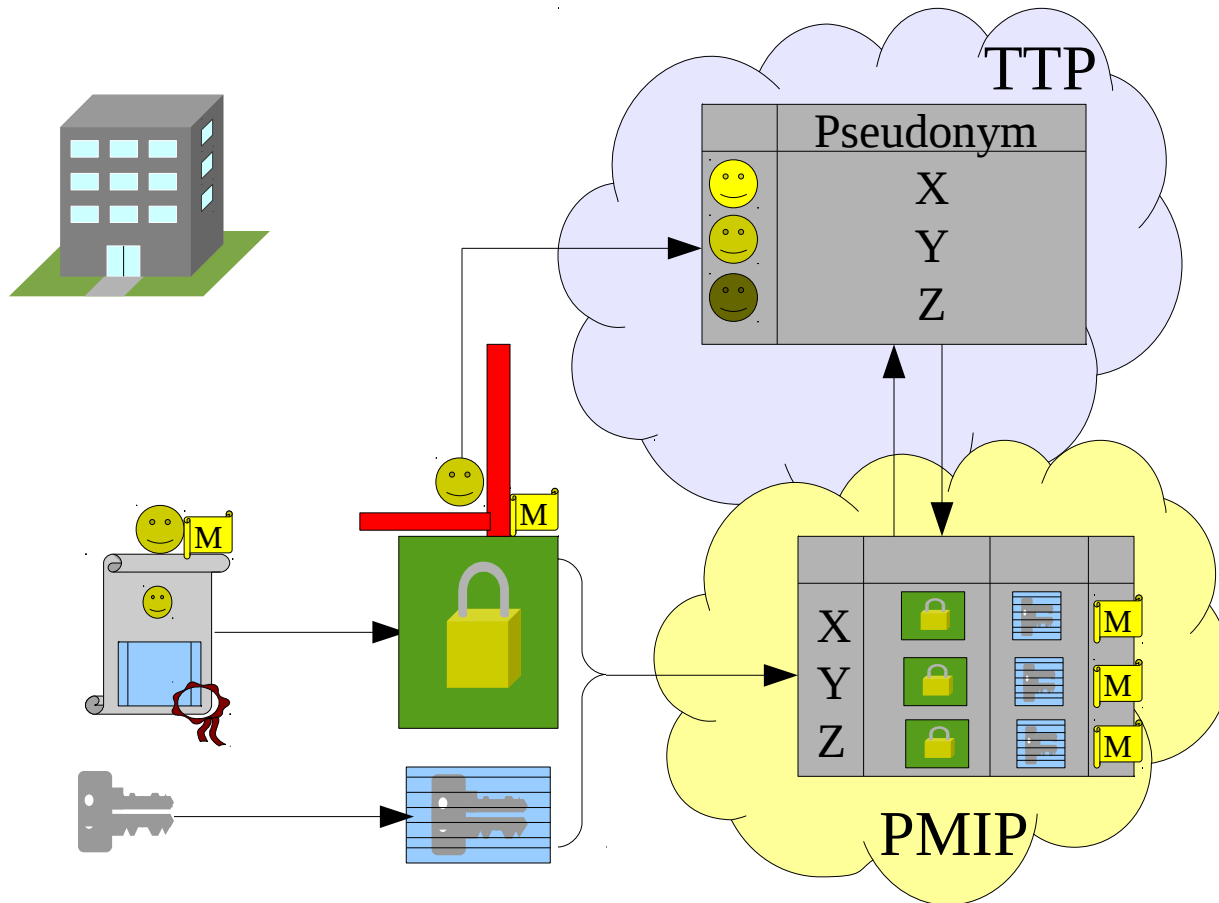
Part 2

- How to guarantee Data Privacy ?
- How to ensure Data Privacy and Statistics ?

Part 3

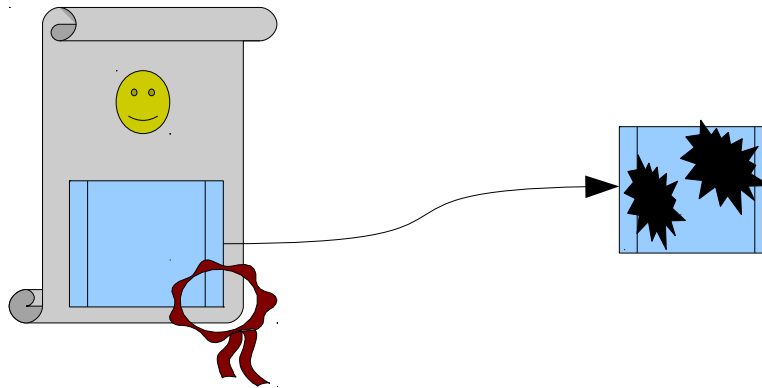
- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- Logging and Alerts

Statistic evaluations possible on
non-encrypted Meta data



Further statistical evaluations are possible:

- *Stripped fragments of the CDA documents*
- *Fragments without any person identifying data*
- *Same Pseudonymization Technique*
- *Approval necessary (Law, Ethic commission, etc.)*

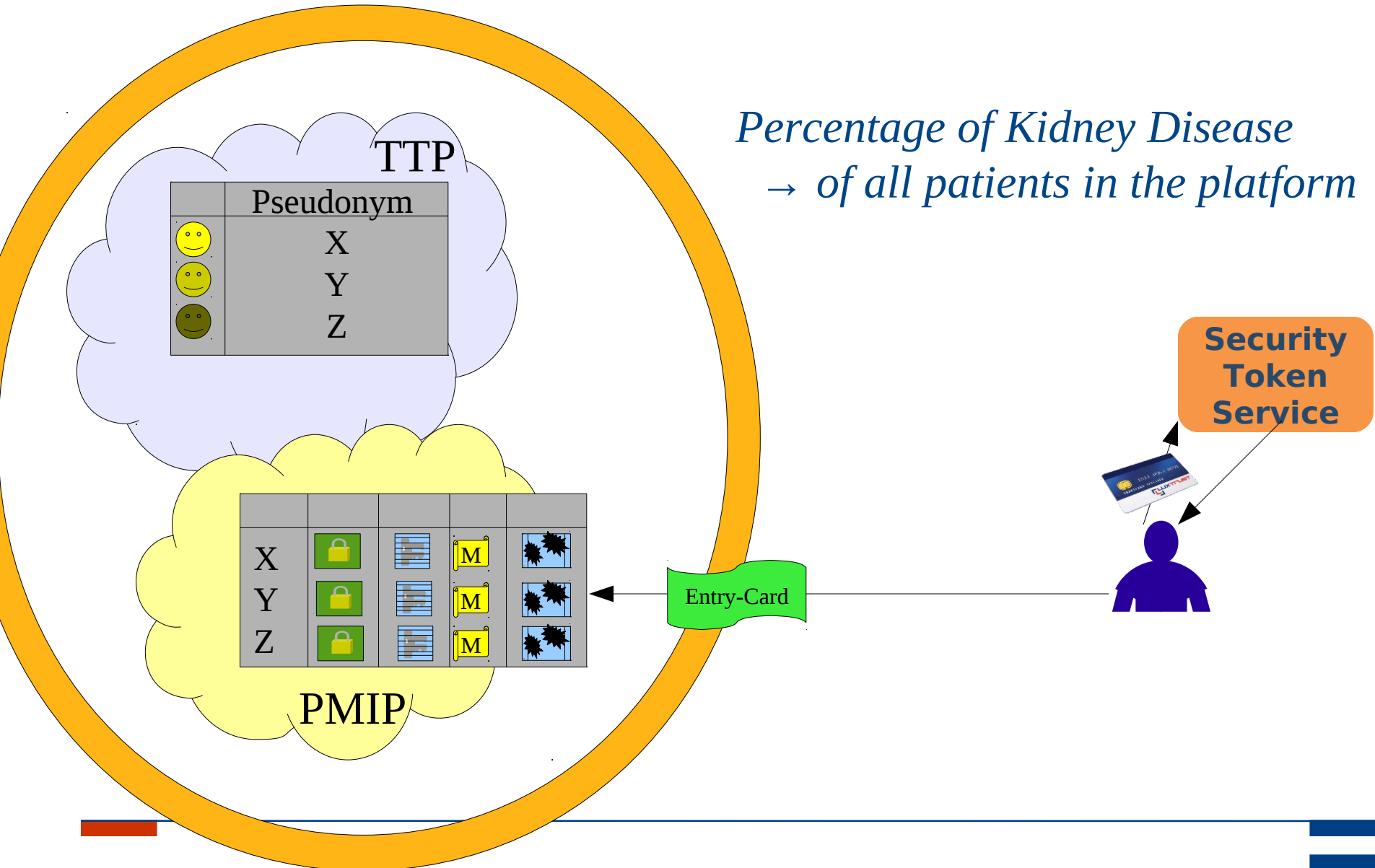


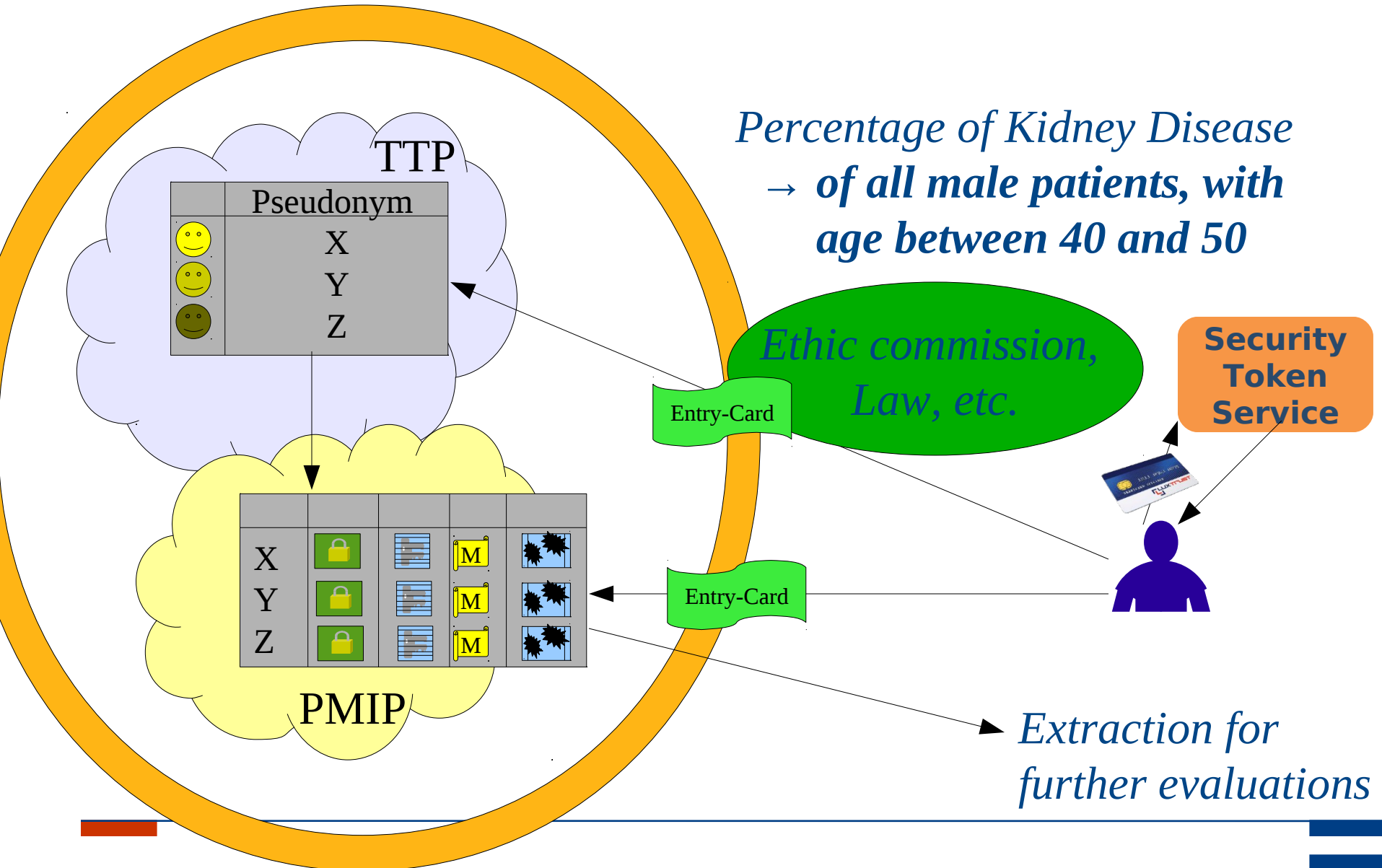


Example Diabetes:

- *Heart Disease and Stroke*
- *Hypertension*
- *Blindness and Eye Problems*
- *Kidney Disease*
- *Nervous System Disease*
- *Amputations*
- *Dental Disease*
- *Complications of Pregnancy*
- *Other Complications*

Reference: <http://diabetes.niddk.nih.gov/dm/pubs/statistics/>





Part 1

- Exchanging Medical Information
- Sharing Medical Information

Part 2

- How to guarantee Data Privacy ?
- How to ensure Data Privacy and Statistics ?

Part 3

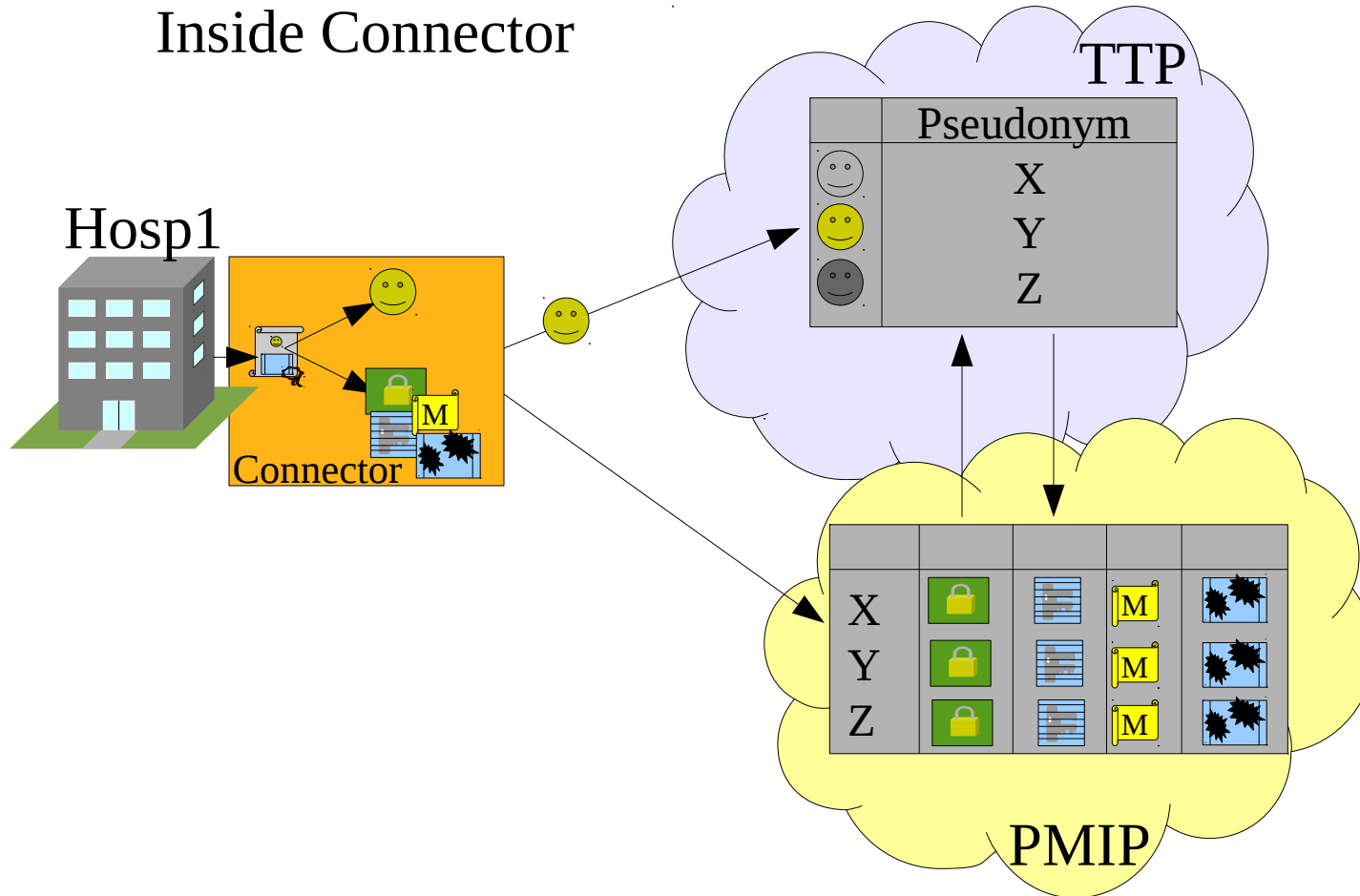
- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- Logging and Alerts

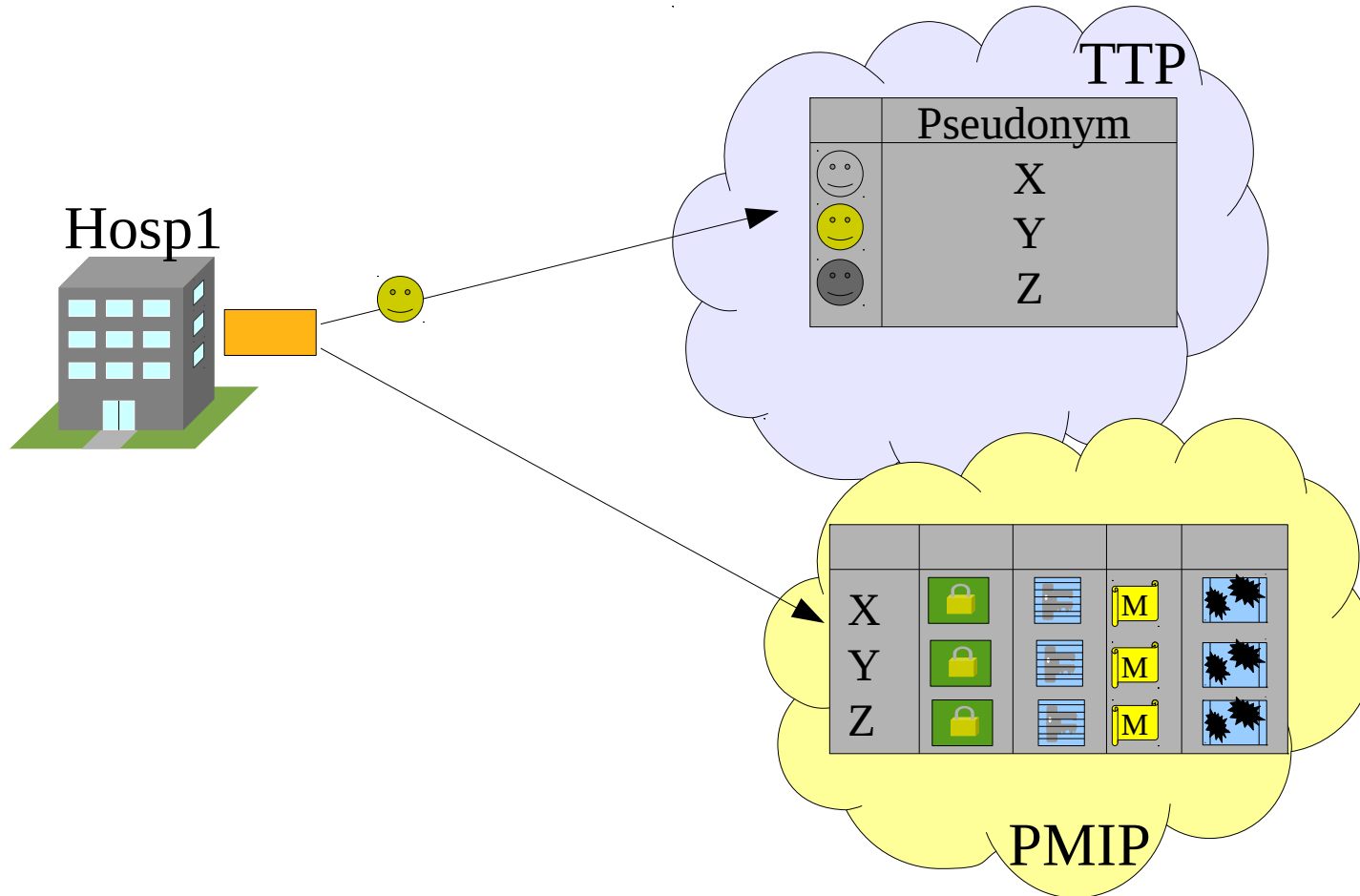
These are Topics for Workshops:

Part 3

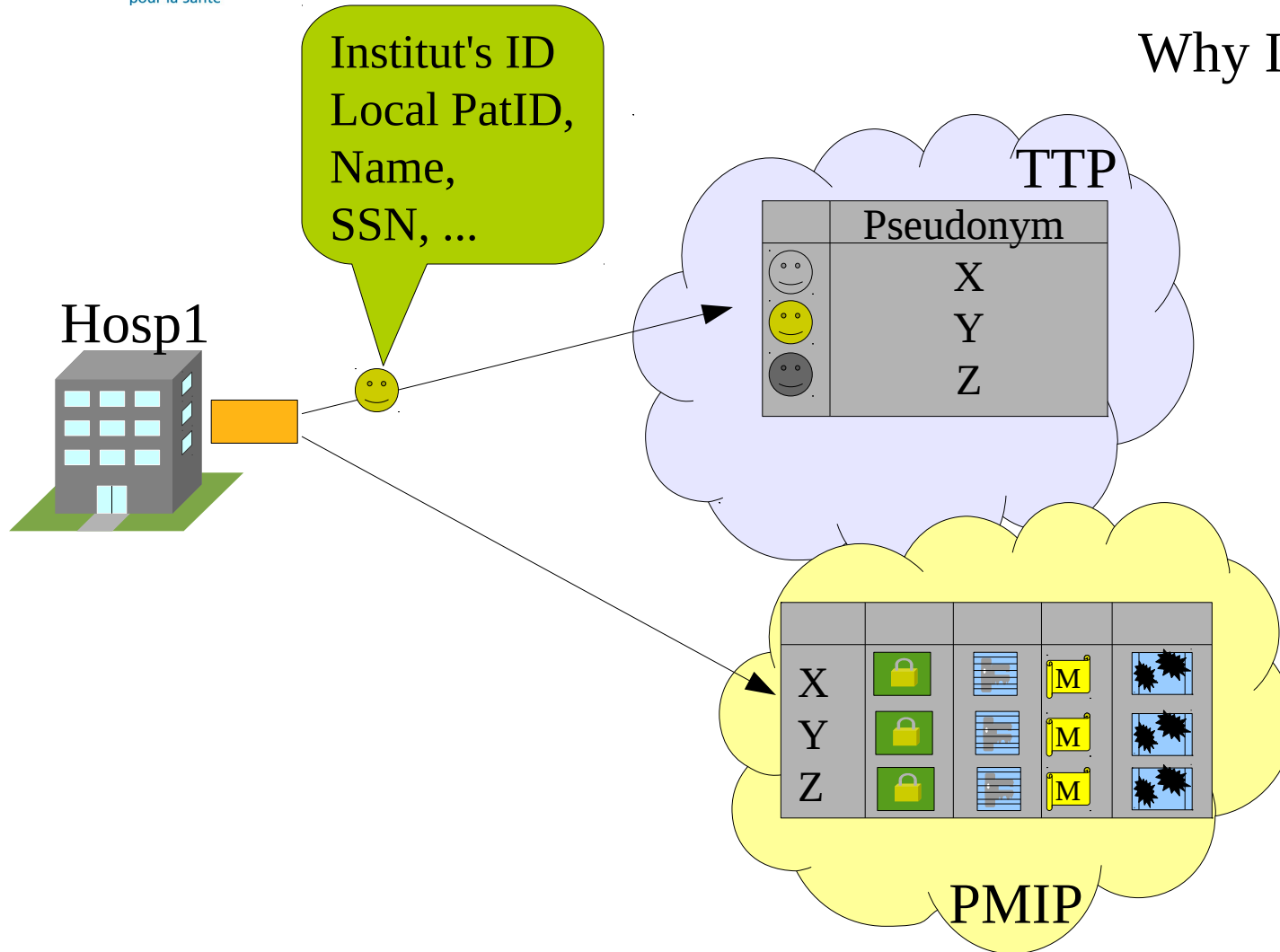
- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- Logging and Alerts

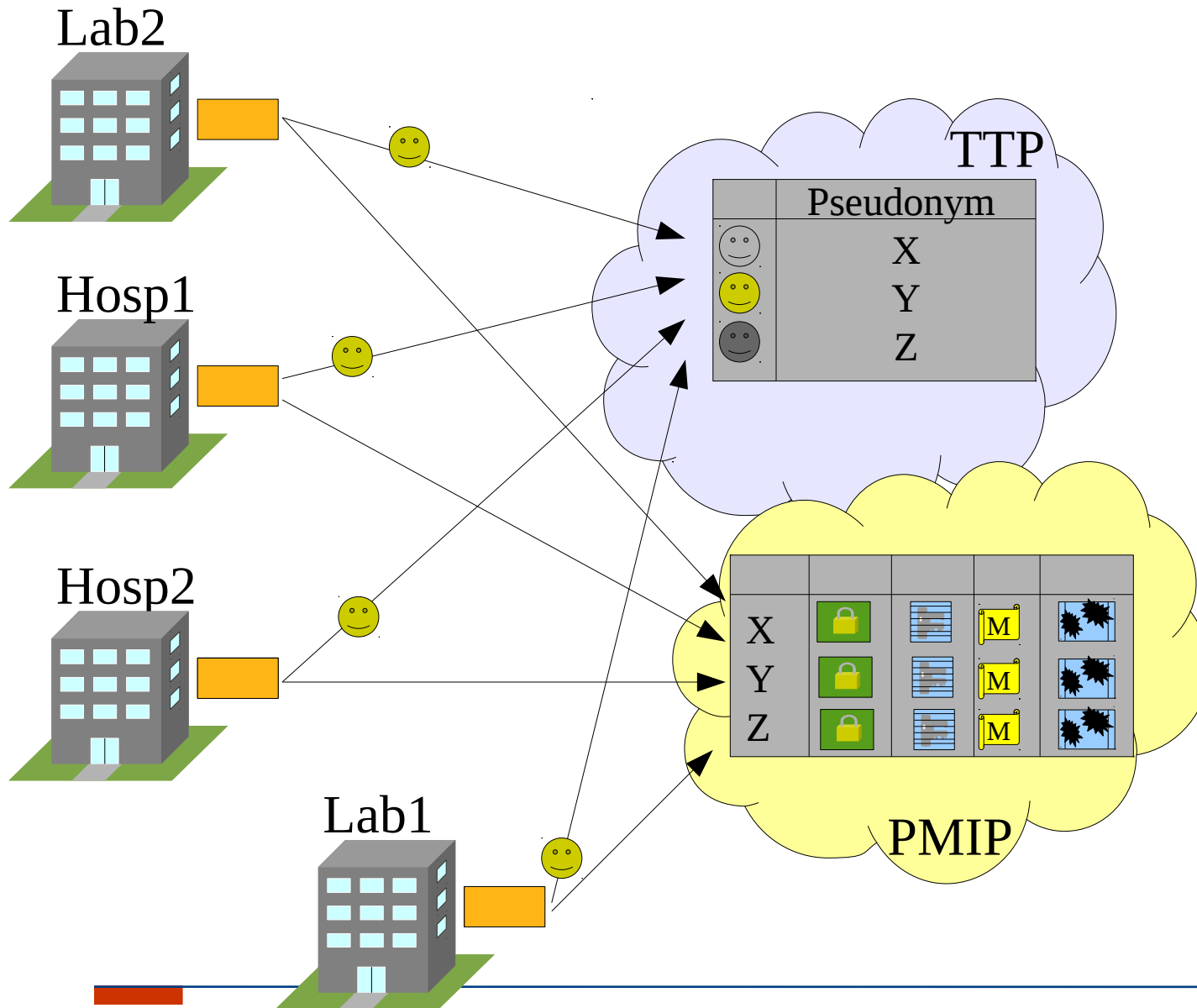
Inside Connector





Why Institut's PID?

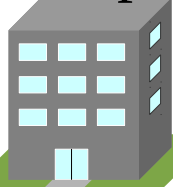




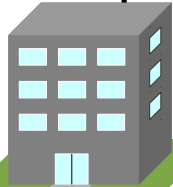
Lab2



Hosp1



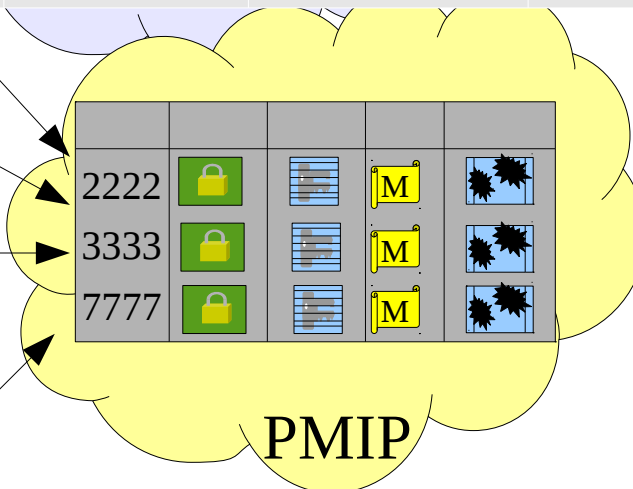
Hosp2



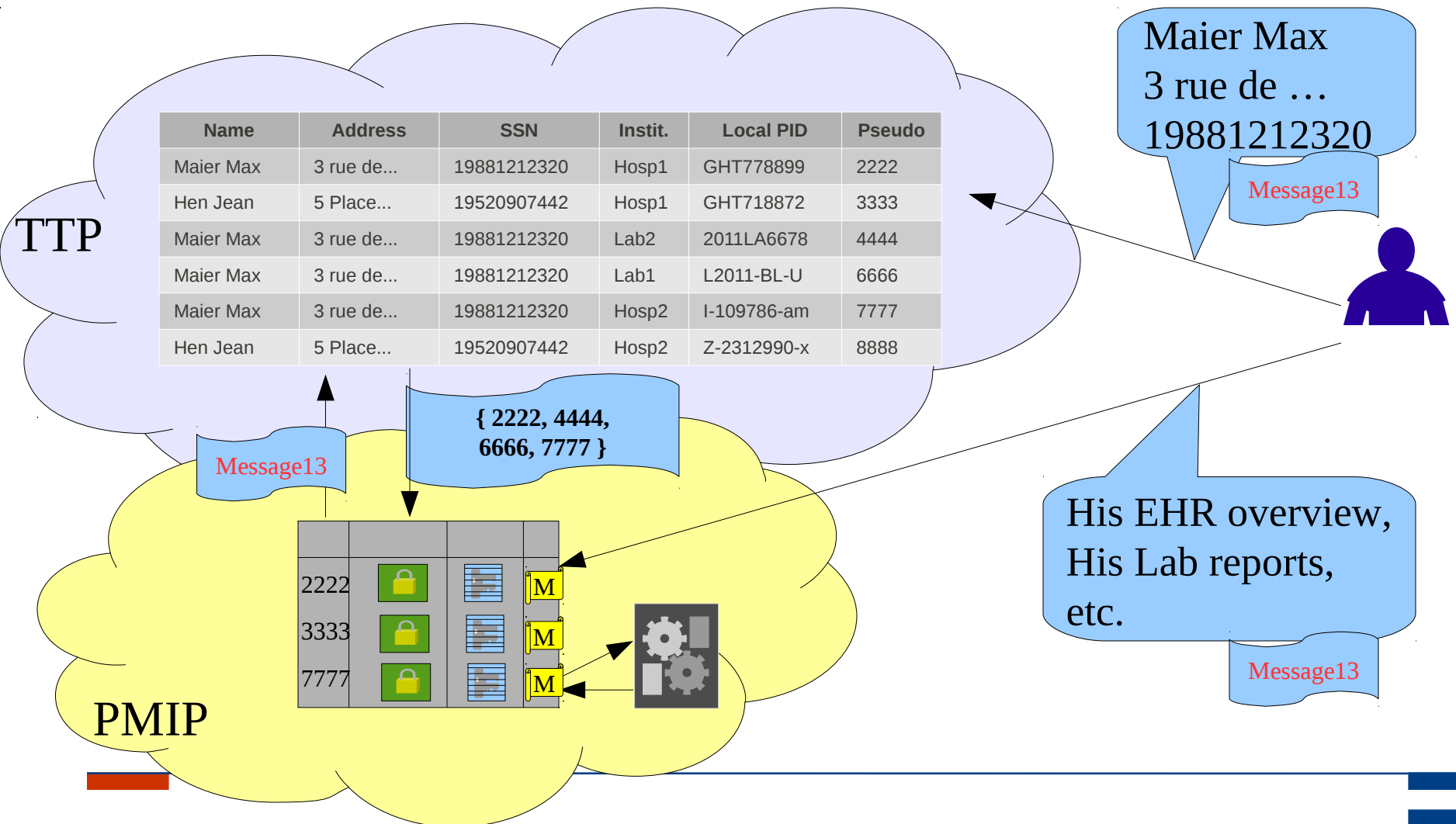
Lab1



Name	Address	SSN	Instit.	Local PID	Pseudo
Maier Max	3 rue de...	19881212320	Hosp1	GHT778899	2222
Hen Jean	5 Place...	19520907442	Hosp1	GHT718872	3333
Maier Max	3 rue de...	19881212320	Lab2	2011LA6678	4444
Maier Max	3 rue de...	19881212320	Lab1	L2011-BL-U	6666
Maier Max	3 rue de...	19881212320	Hosp2	I-109786-am	7777
Hen Jean	5 Place...	19520907442	Hosp2	Z-2312990-x	8888



59



Part 1

- Exchanging Medical Information
- Sharing Medical Information

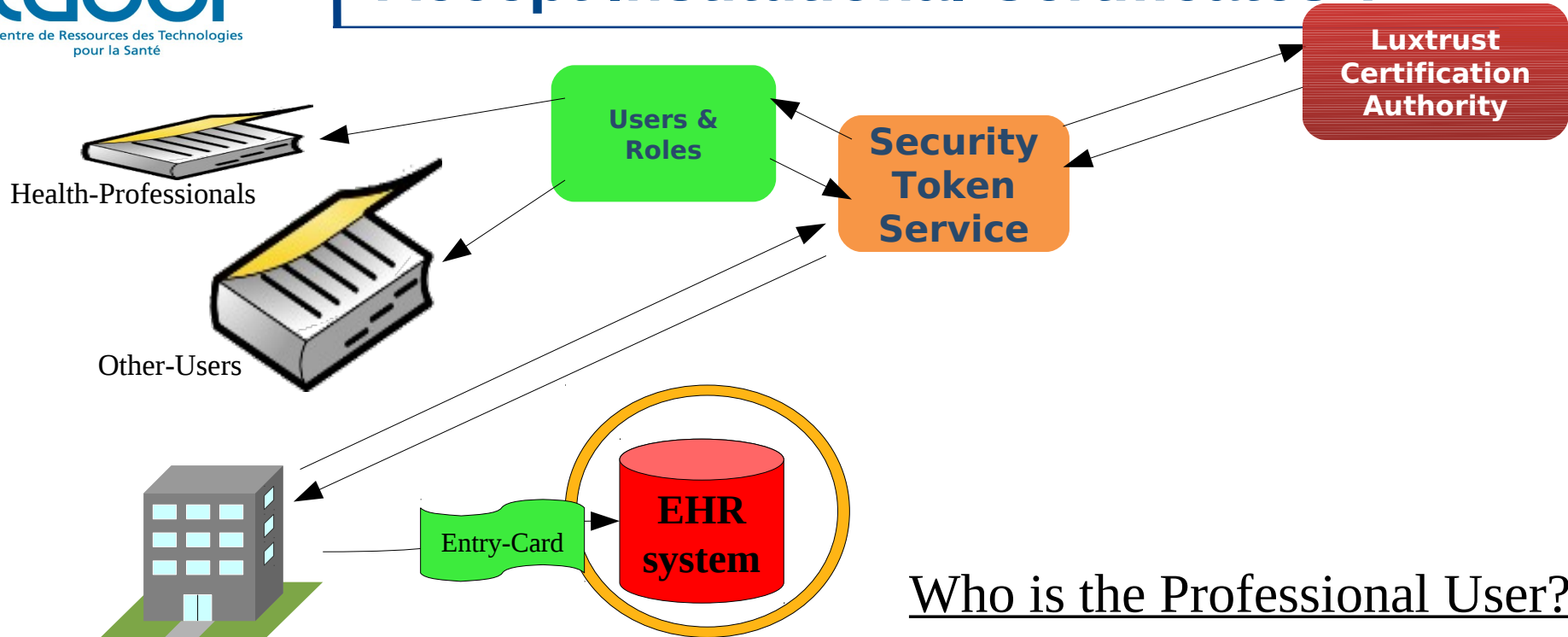
Part 2

- How to guarantee Data Privacy ?
- How to ensure Data Privacy and Statistics ?

Part 3

- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- Logging and Alerts

Accept Institutional Certificates ?



Who is the Professional User?

- Doctor / Biologist as person
- Hospital / Laboratory as institution
- or HIS / LIS grantees for secure Login?

Part 1

- Exchanging Medical Information
- Sharing Medical Information

Part 2

- How to guarantee Data Privacy ?
- How to ensure Data Privacy and Statistics ?

Part 3

- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- Logging and Alerts

Level of Details:

- Participation YES / NO
- Rule Based
- Item Based

Media:

- paper based, doctor set flag in the system and keeps signed paper
- electronic
- electronic with eSignature (?)

- **Opt-Out** for Record Creation
 - * default creation with the option to step out
- **General Rules** for creation and consultation of documents
 - * according to the needs of Health care Professionals
 - * good designed and agreed default values
- **Specific Rules** overwrite the General Rules
 - * definable by the patient
 - * assisted by her/his médecin référent
- **Médecin Référent** with specific access rights
 - * always access to whole record (not hidden documents)
- **Opt-Out** regulation for specific documents

Some Examples:

– **General Rules**

- All stroke units of all Luxembourgian hospitals have read access to everything.
- SAMU has access to the laboratory examinations not older than 2 years.

– **Specific Rules**

- Dr Neighbor is not allowed to access any data.
- Dr Cousin is not allowed to access the psychosomatic case of 2006

– **Opt-Out** regulation for specific documents

- The HIV test (result negative) of 18 Jan 2011 must not be documented.

Part 1

- Exchanging Medical Information
- Sharing Medical Information

Part 2

- How to guarantee Data Privacy ?
- How to ensure Data Privacy and Statistics ?

Part 3

- Cross Institution Patients' Identification
- Acceptance of Institutional Logins
- Patients' Consent Declaration
- **Logging and Alerts**

Logging

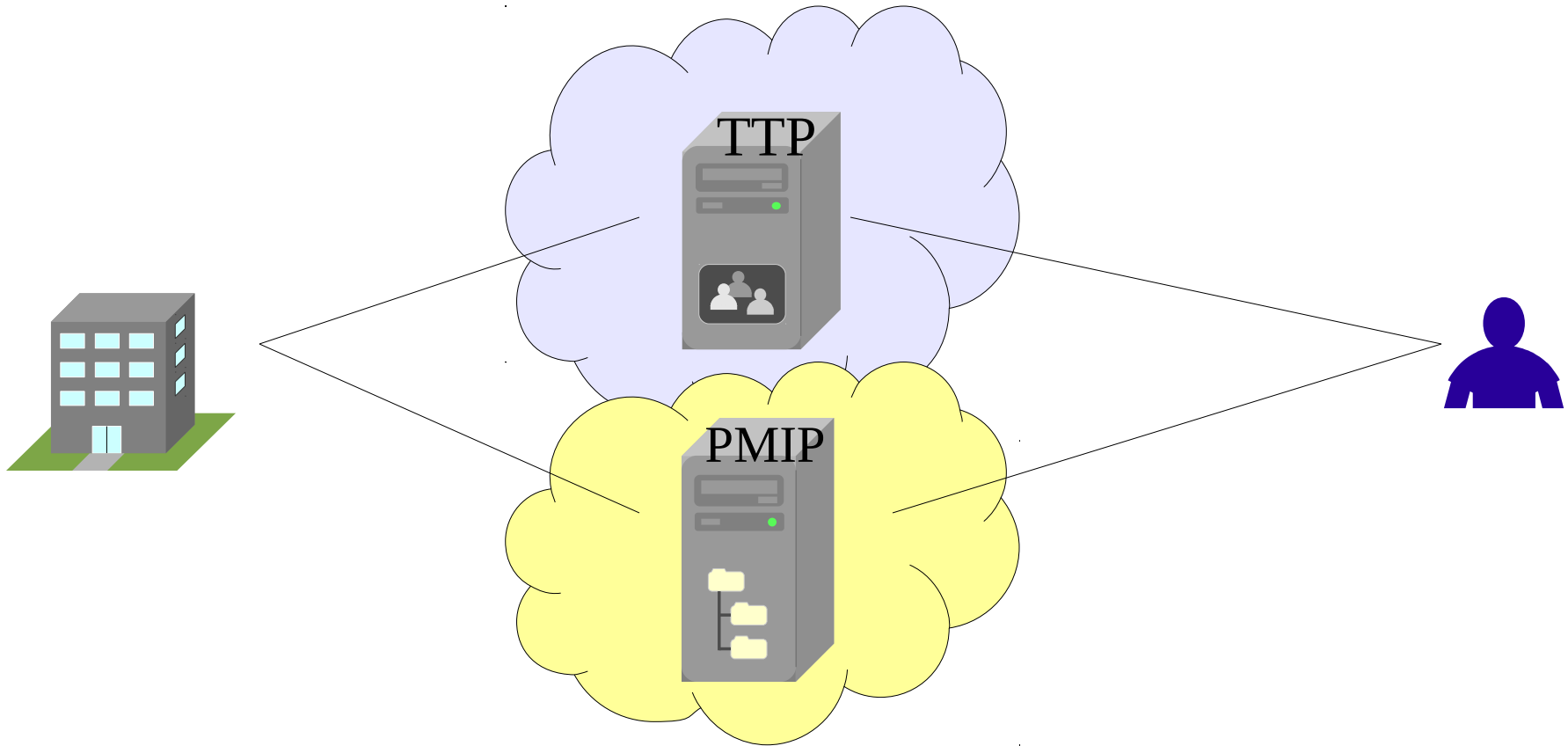
- Logging of every access, read and write.
- Yearly access report for every patient (on demand?)
- Online inspection for logging by patient.

Alerts

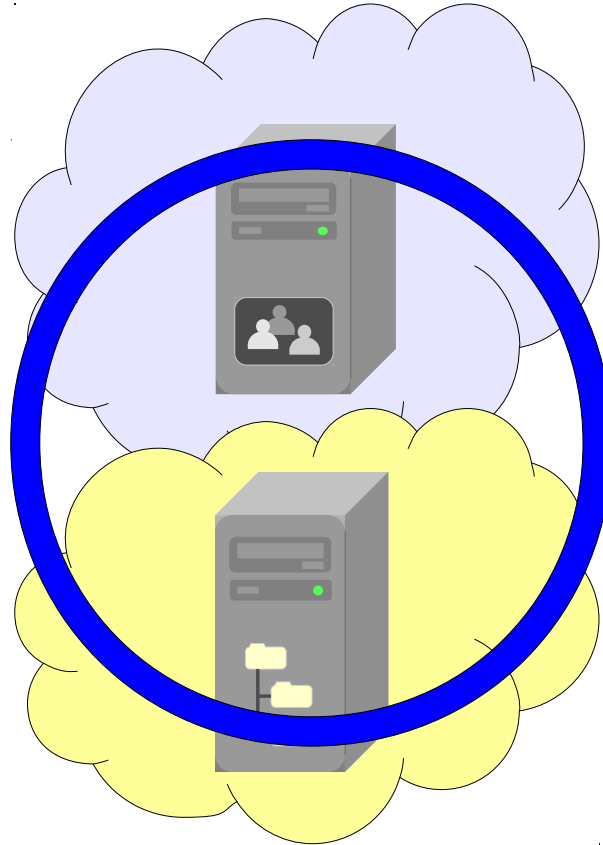
- Emergency access sends out an information to a relative of the patient (SMS, eMail, ...)

Schematic Summary

Separation



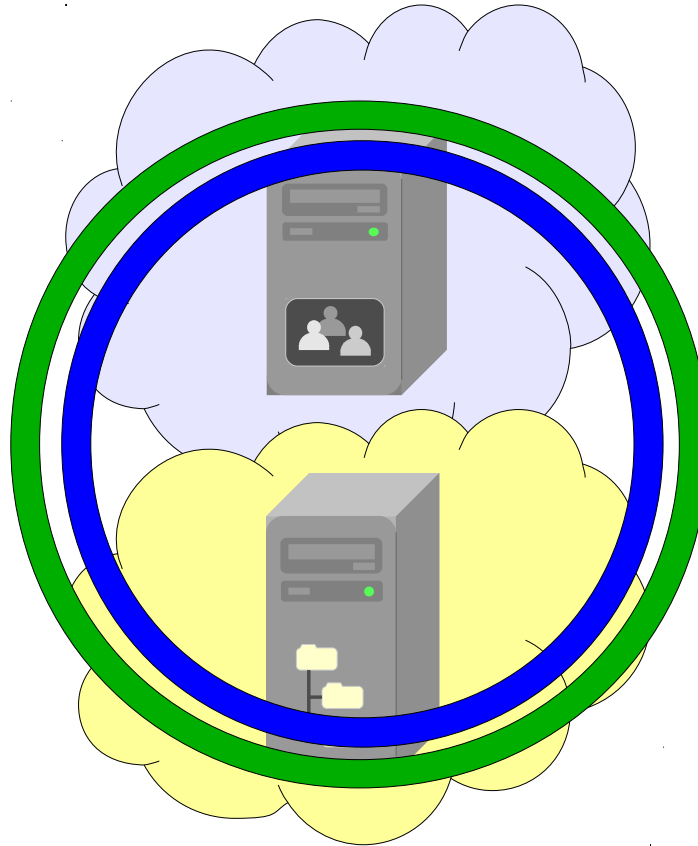
Separation Pseudonymization



Separation

Pseudonymization

Key Re-Encryption

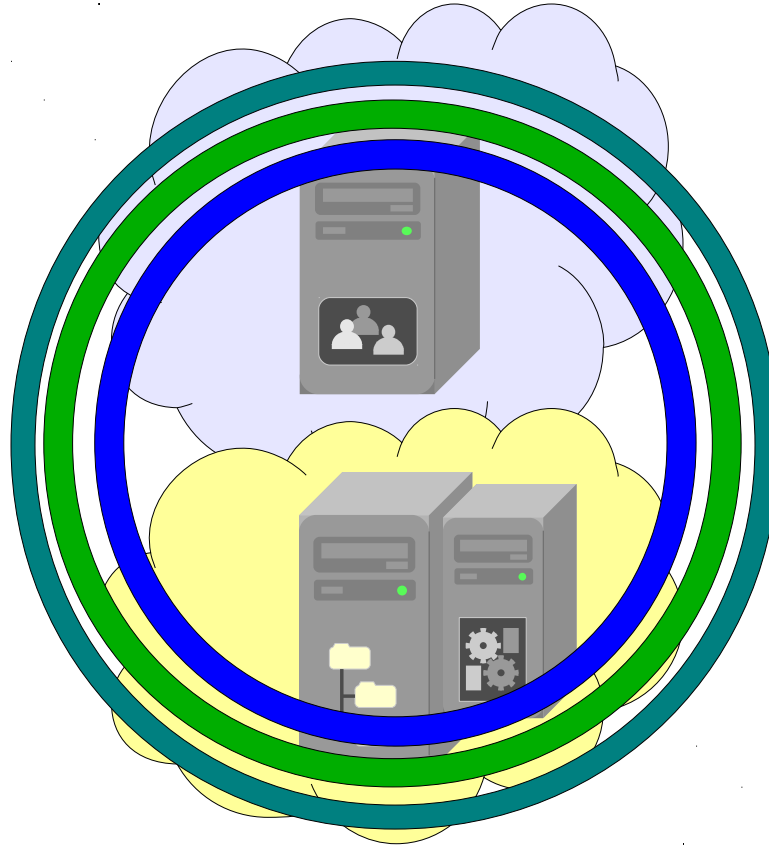


Separation

Pseudonymization

Key Re-Encryption

Consent



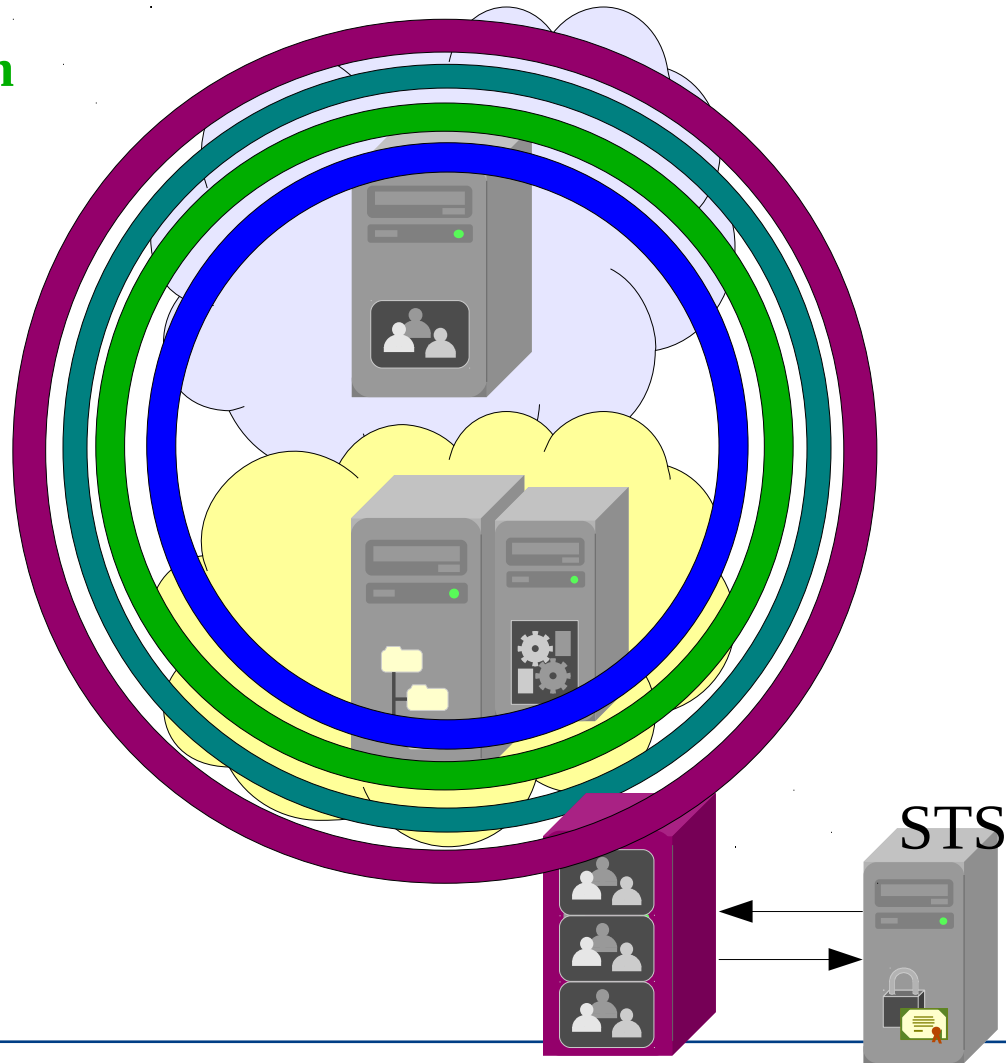
Separation

Pseudonymization

Key Re-Encryption

Consent

Logging&Alerts



Separation

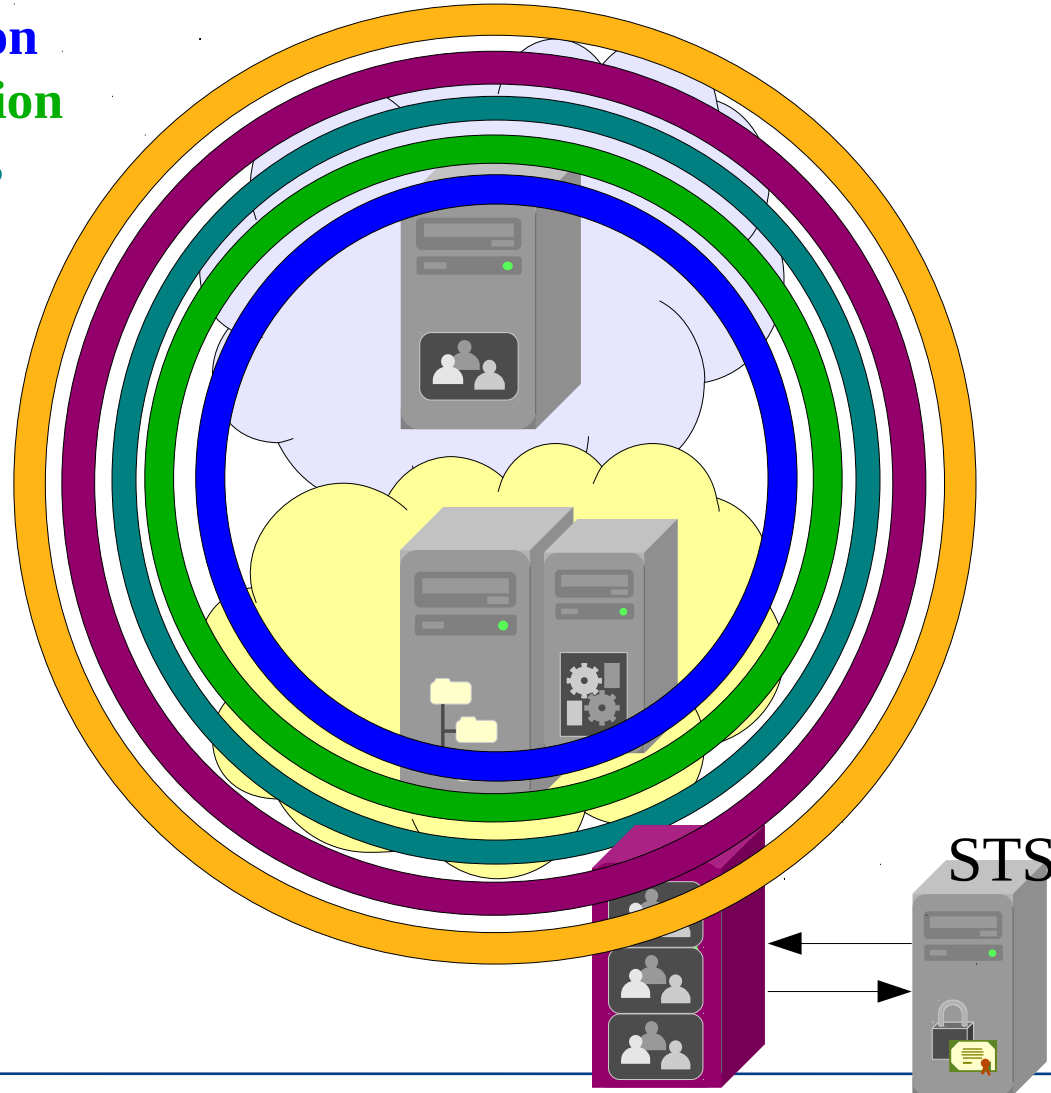
Pseudonymization

Key Re-Encryption

Consent + Alerts

Logging&Alerts

**Security Token
Service**



Separation

Pseudonymization

Key Re-Encryption

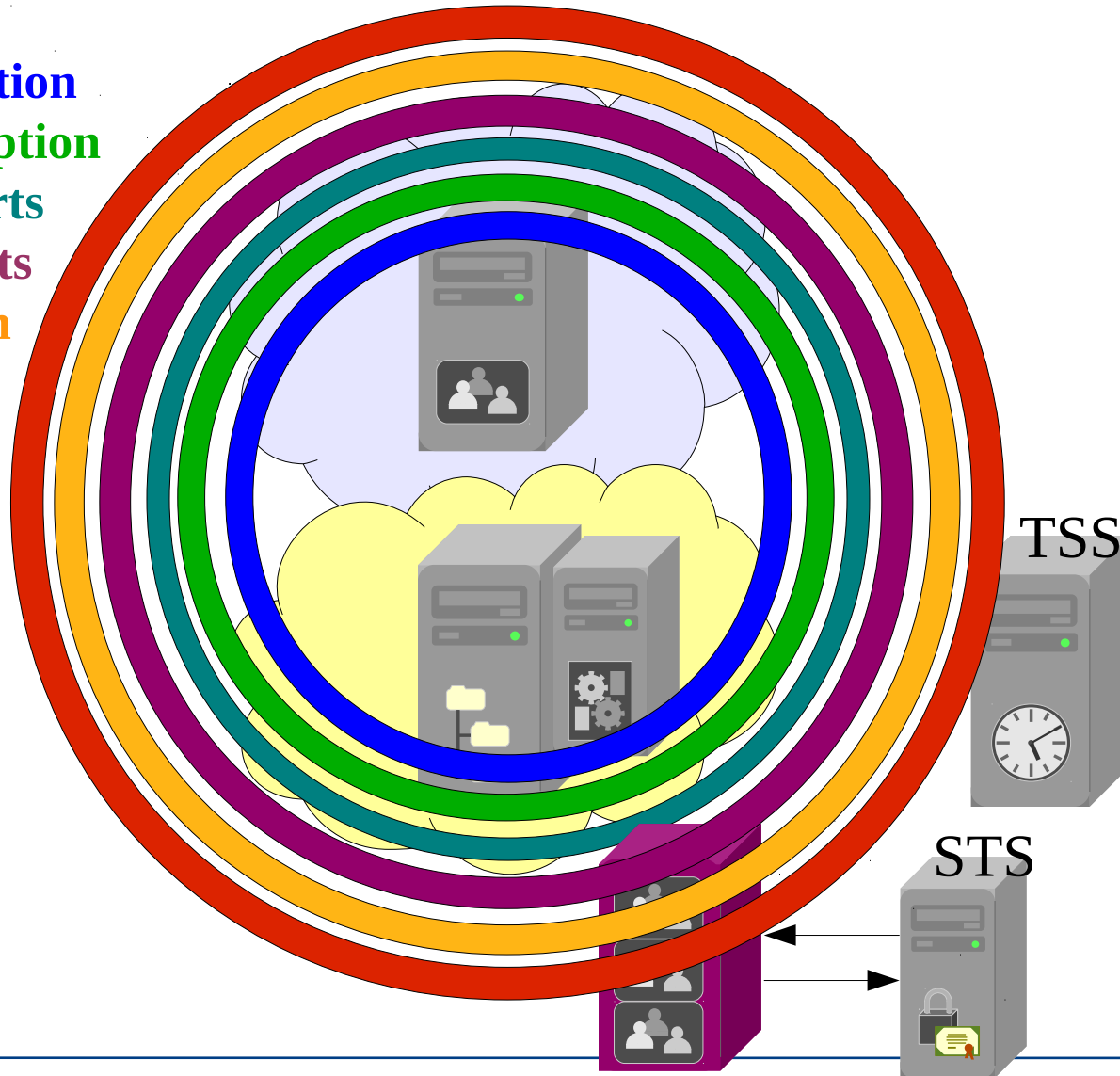
Consent + Alerts

Logging&Alerts

Security Token

Service

Time Stamp



Separation

Pseudonymization

Key Re-Encryption

Consent + Alerts

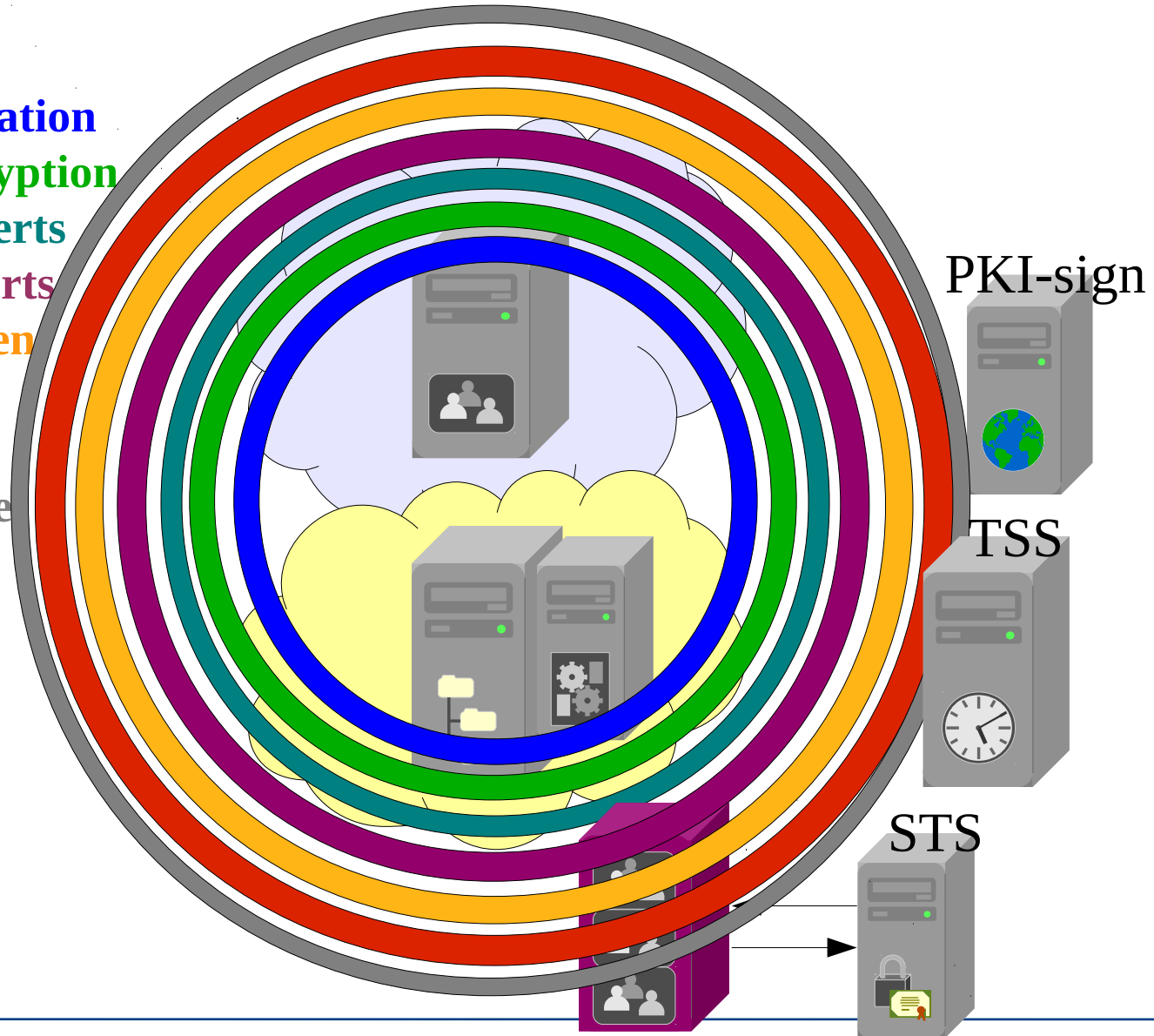
Logging&Alerts

Security Token

Service

Time Stamp

PKI signature



Separation

Pseudonymization

Key Re-Encryption

Consent + Alerts

Logging & Alerts

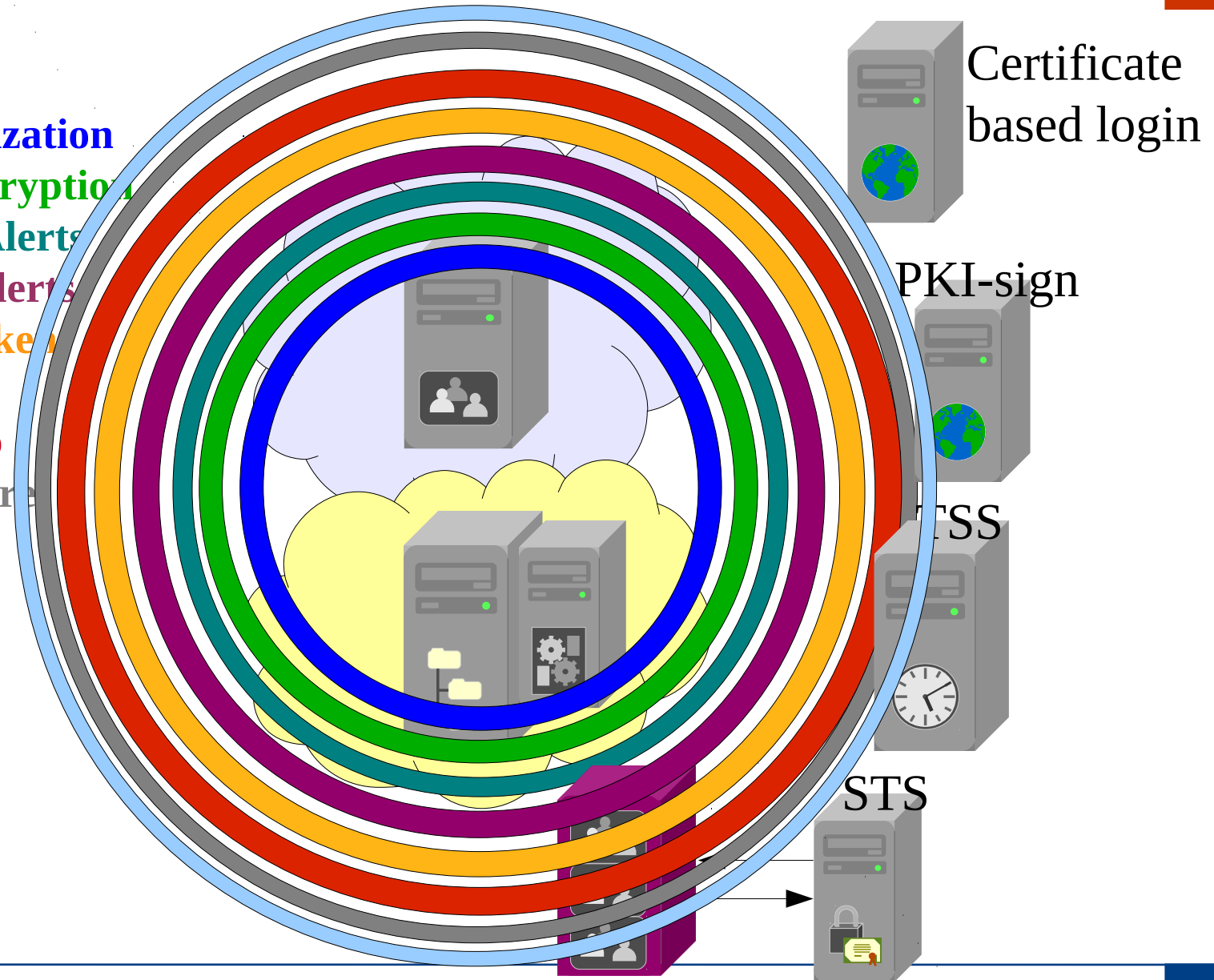
Security Token

Service

Time Stamp

PKI signature

**Certificate
based login**



More Information available at:

http://www.santec.lu/_media/project/esante/efes/ ---> Deliverable 7-8-13 Architecture and Security

Thank you !

**Remarks &
Questions?**

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

CONSENT

RULES: { I do not allow any access to my data. |
I allow access to my data for WHO
[in case of WHEN]
[to WHAT]
[but only of the [TIME-INT | last YEAR years]] . }

WHO: { every_professional |
samu | pharmacy | my_family_GP }
[{and WHO}]}

WHEN: { an_emergency_situation | any_situation }+

WHAT: {DIAGNOSES | TREATMENTS | MEDICATION } { and WHAT }

TIME-INT: {between DATE and DATE} { and TIME-INT }

DIAGNOSES: [all_diagnoses | REFERENCES]

MEDICATION: [all_medication | REFERENCES]

REFERENCES: [(select_information_item_here)]+

YEAR: { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 }

RULES: { I do not allow any access to my data. |
I allow access to my data for WHO
[in case of WHEN]
[to WHAT]
[but only of the [TIME-INT | last YEAR years]] . }

**“I allow access to my data for samu and my_family_GP
in case of an_emergency_situation
to all_diagnoses and all_medication
but only of the last 6 years.”**

TIME-INT: {between DATE and DATE} { and TIME-INT }

DIAGNOSES: [all_diagnoses | REFERENCES]

MEDICATION: [all_medication | REFERENCES]

REFERENCES: [(select_information_item_here)]+

YEAR: { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 }

CONSENT: ITEM [DECLARATIONS .]+ [EXCLUSIONS .]* [EXCEPTIONS .]*

DECLARATIONS: My family GP is <professional_name>

EXCLUSIONS: Hide diag or treatment in CATEGORY of DATE
for {<professional_name> | everybody }.

CATEGORY: {labo | xray | medication | surgery | orthopedics | psychosomatics}

EXCEPTIONS: In no way the following people are allowed
{<professional_name>} [, <professional_name>]+

CONSENT: ITEM [DECLARATIONS .]+ [EXCLUSIONS .]* [EXCEPTIONS .]*

DECLARATIONS: My family GP is <professional_name>

EXCLUSIONS: Hide diag or treatment in CATEGORY of DATE
for {<professional_name> | everybody }.

CATEGORY: {labo | xray | medication | surgery | orthopedics | psychosomatics}

EXCEPTIONS: In no way the following people are allowed
{<professional_name>} [, <professional_name>]+

“ My family GP is Dr Wasp.

Hide diag or treatment in surgery of 1998-01-18 for everybody.

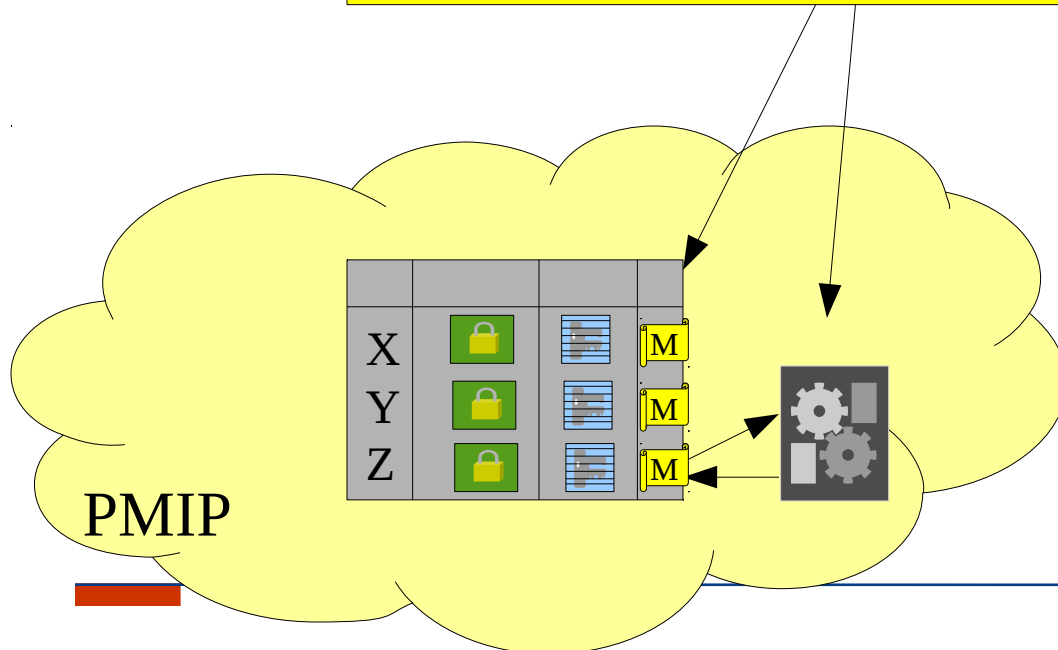
Hide diag or treatment in labo of 2004-02-04 for everybody.

Hide diag or treatment in psychosomatics of 2006--** for Dr Bee.**

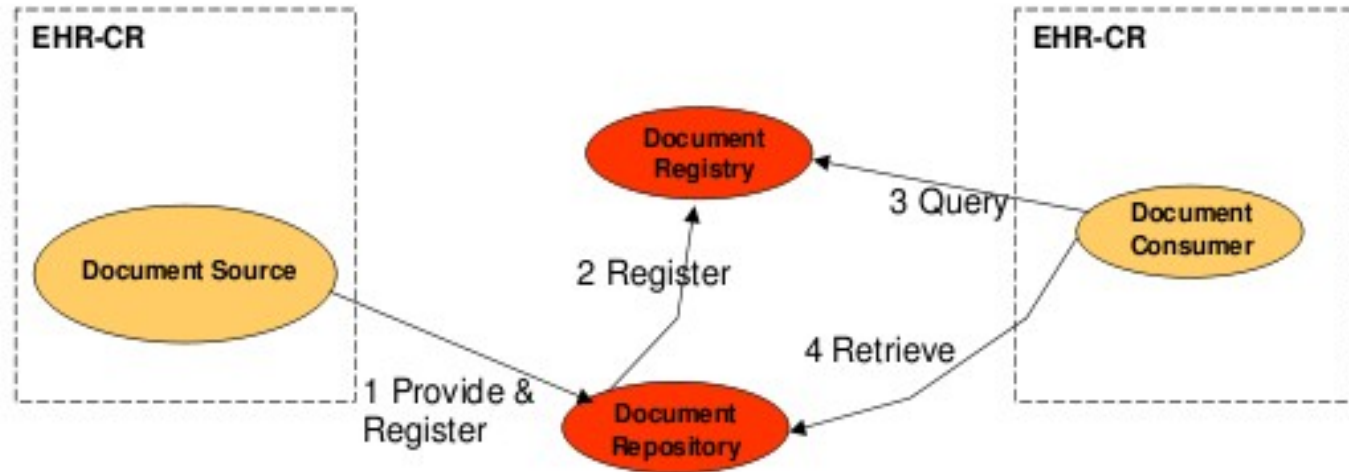
In no way the following people are allowed Dr Neighbor, Dr Who. ”

**“I allow access to my data for samu and my_family_GP
in case of an_emergency_situation
to all_diagnoses and all_medication
but only of the last 6 years.”**

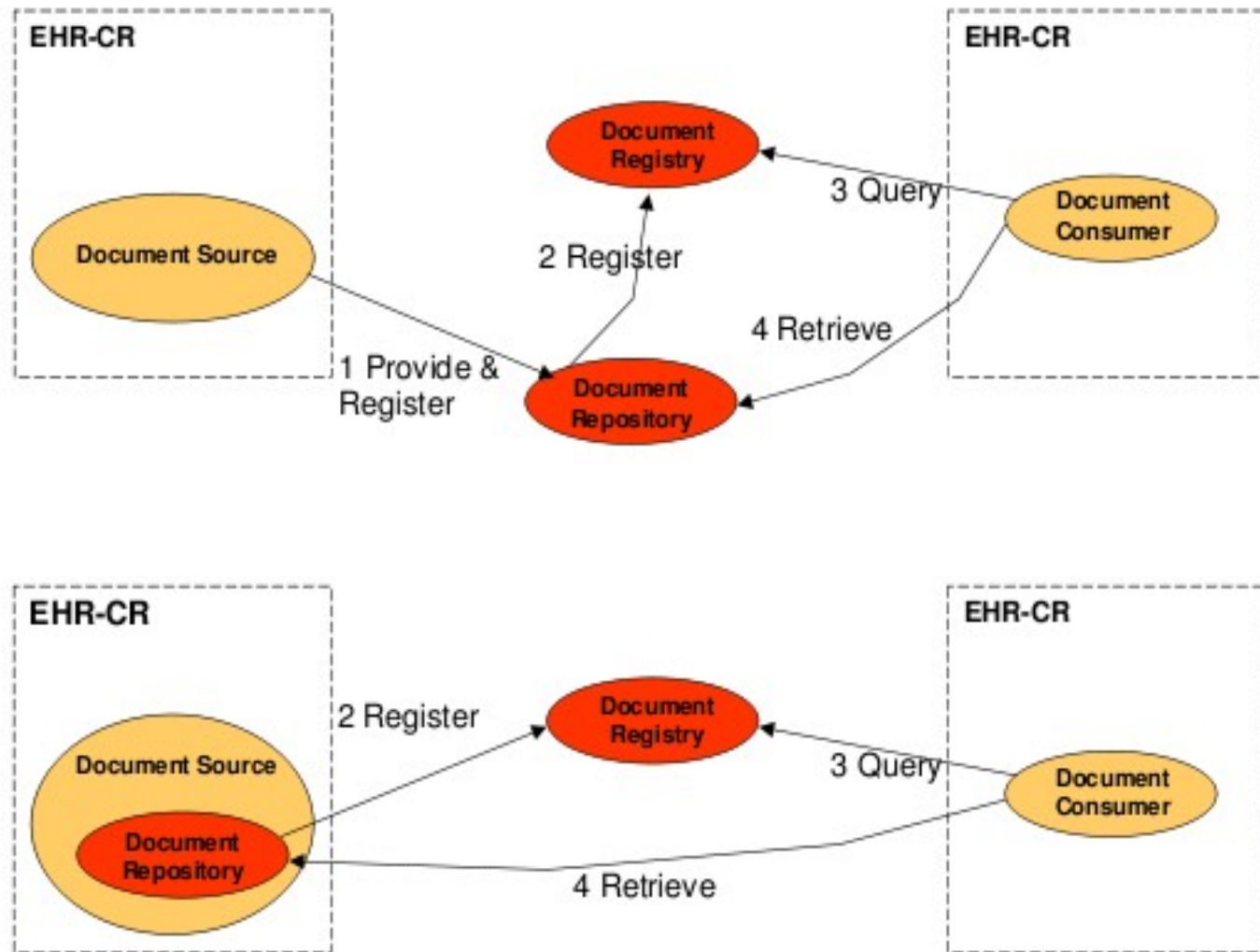
**“ My family GP is Dr Wasp.
Hide diag or treatment in surgery of 1998-01-18.
Hide diag or treatment in labo of 2004-02-04.
Hide diag or treatment in psychosomatics of 2006-**-** for Dr Bee.
In no way the following people are allowed Dr Curious, Dr Who. ”**



IHE XDS DETAILS



Picture source: IHE International. IHE Profiles. URL:<http://www.ihe.net/profiles/>



Picture source: IHE International. IHE Profiles. URL: <http://www.ihe.net/profiles/>

FUTURE WORK

- *Implementation of a Test-Bed (Preparation for Impl. by Vendors)*
- *Data Aging and Archiving, Context preservation*
- *Patients' Access to their Records*
- *Alert Functions and Access Logs*
- *Meta Structuring EHR in Pseudonymized Space*
- *Rule Based and Item-Based IT-Consent*
- *Support for Decision Support Systems*
- *Improvement of Demographic Data Quality*
- *Scheduled Pseudonym Exchange and Multilevel Pseudonym*
- *General further Use-Cases*