PUBLIC RESEARCH CENTRE HENRI TUDOR

Workshop eSanté
WS 1: Architecture & Security

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

CRP Henri Tudor
September 21 2011

Security and Privacy

Overview Platform Proposal

– Introduction, Typical Workflow

– Access Control

– Pseudonymization and 2-step Encryption

– Re-Encryption and 2-step Decryption

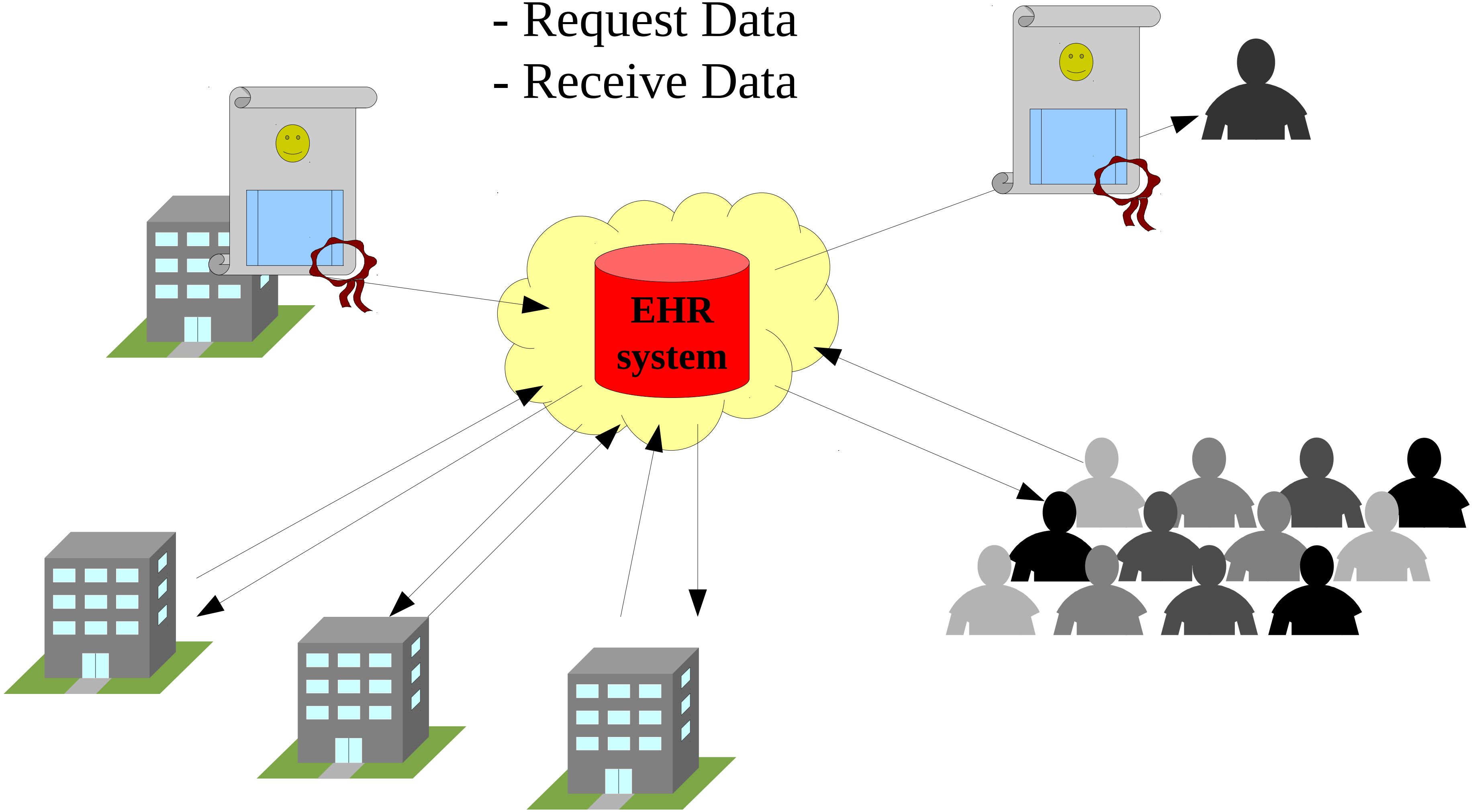
Workshop

– Relevant Topics to be discussed ?

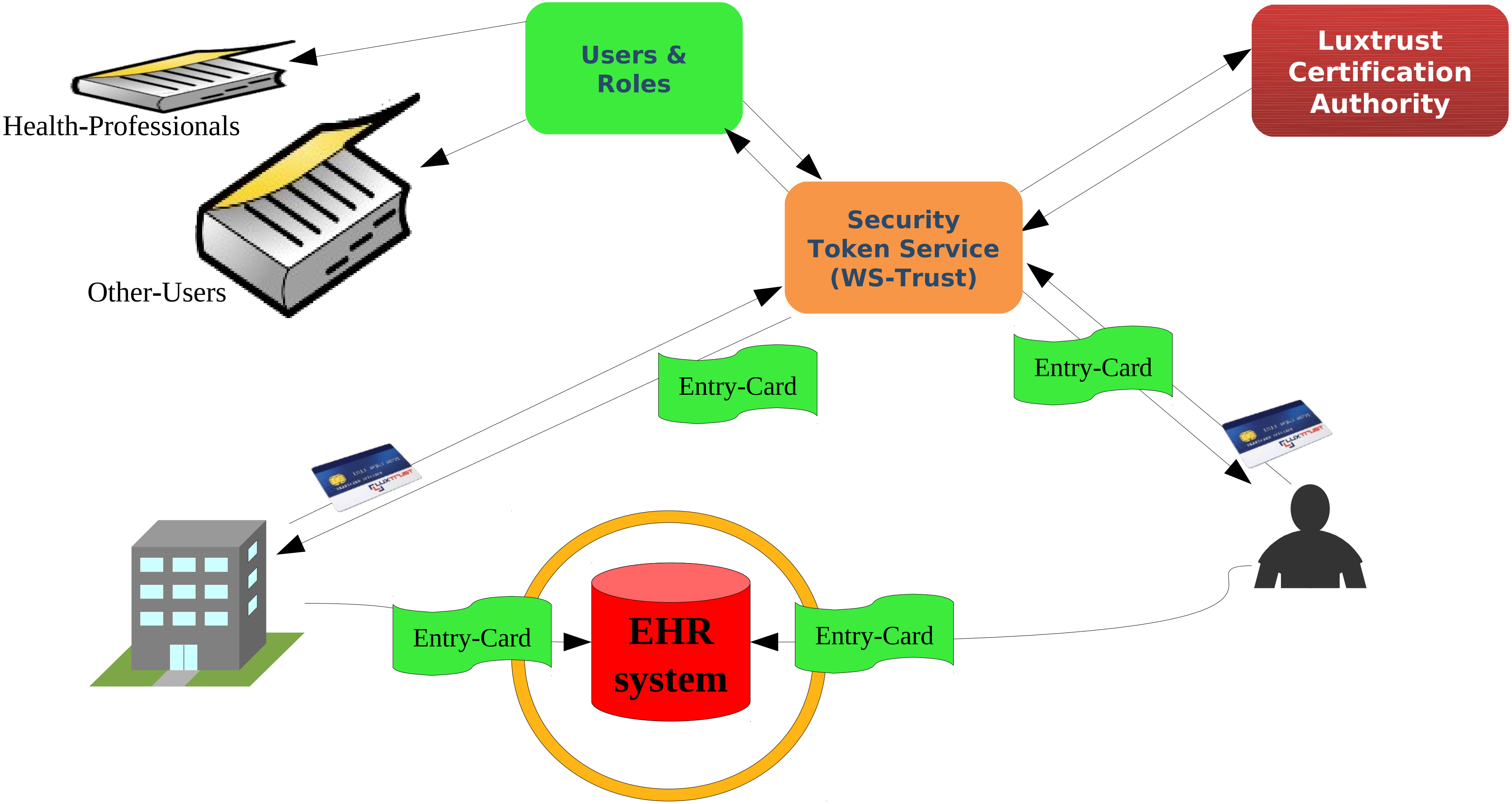
– Your Expectations ?

Introduction: Typical Workflow

- Provide Data
- Request Data
- Receive Data



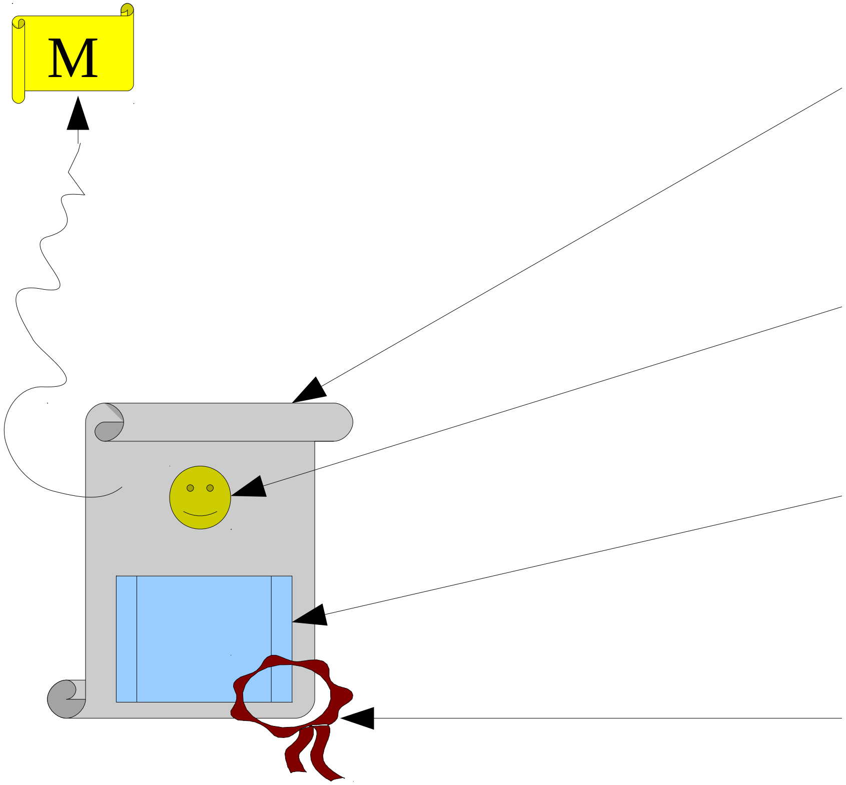
Access Control



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

Schematic Report Representation

General “Medical Report”
+ extraction of Metadata



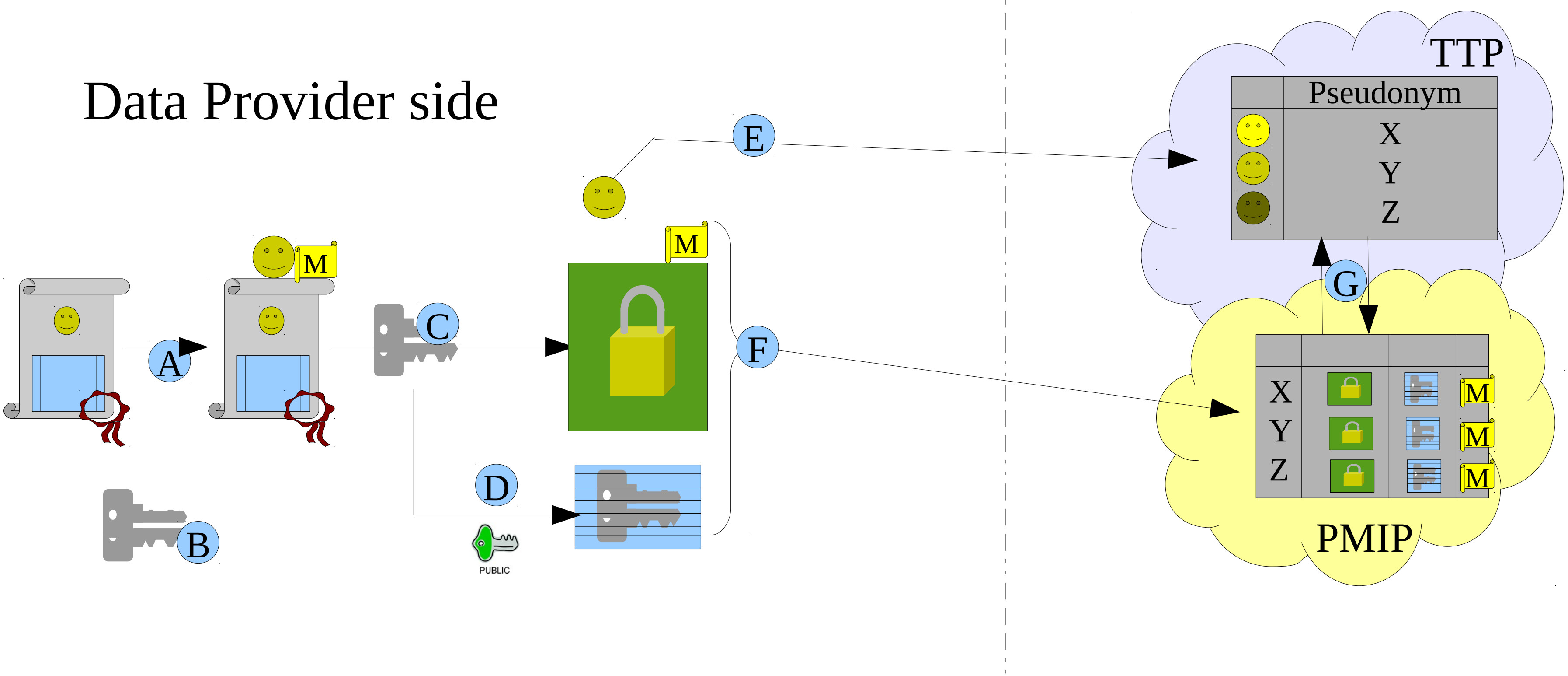
The whole Report

Patient Identity

Results

Signature for
whole Report

Pseudonyms and 2-step Encryption



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

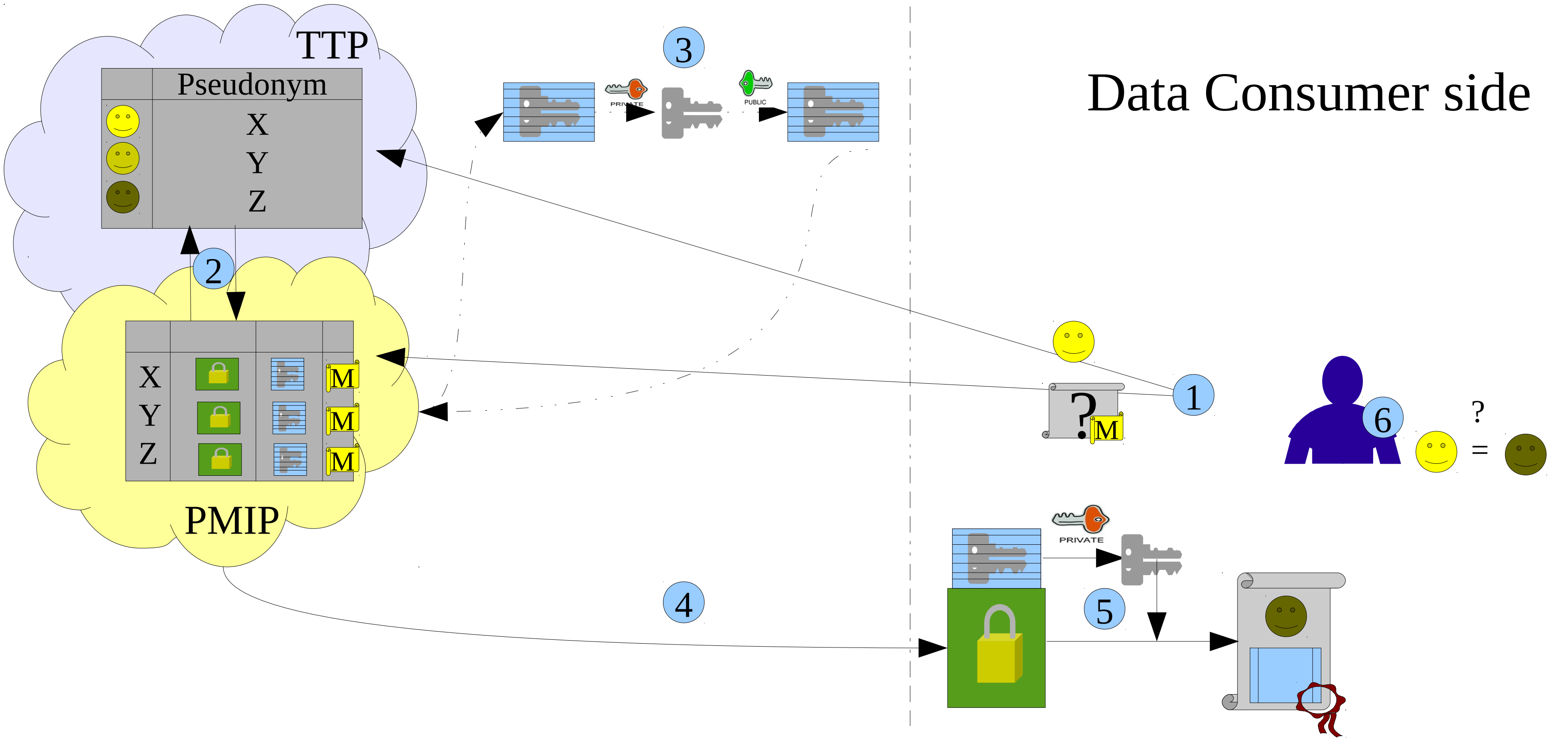
E Provide Identity Data to TTP

F Provide “everything else” to TTP

G Pseudonym Handshake

* TTP = Trusted Third Party, PMIP = Pseudonymized Medical Information Provider, M = Metadata

Re-Encryption and 2-step Decryption



1 Open Query Session

2 Pseudonym Handshake

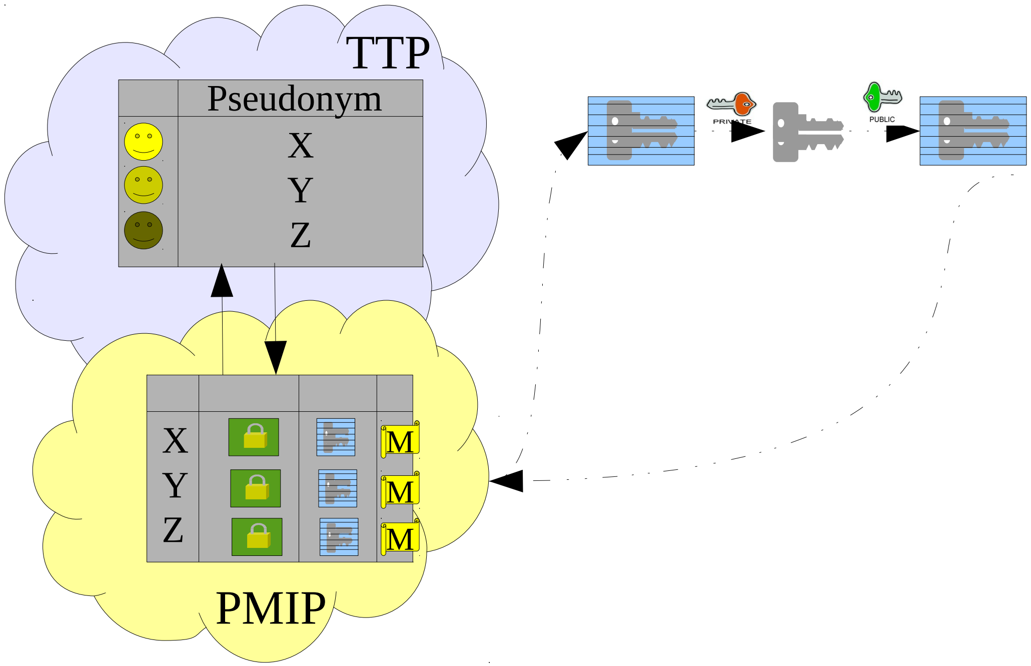
3 Re-Encryption of 🔑 with public Key of Requester

4 Deliver Encrypted Report and Key

5 Decryption in 2 Steps

6 Check Patient's Identity on Report

Benefits of this Combination



Metadata is protected by **Pseudonymization**

Medical Reports are protected by full **Encryption**

Non-Disclosure against single Admin/Intruder

Non-Disclosure even during **Re-Encryption** !

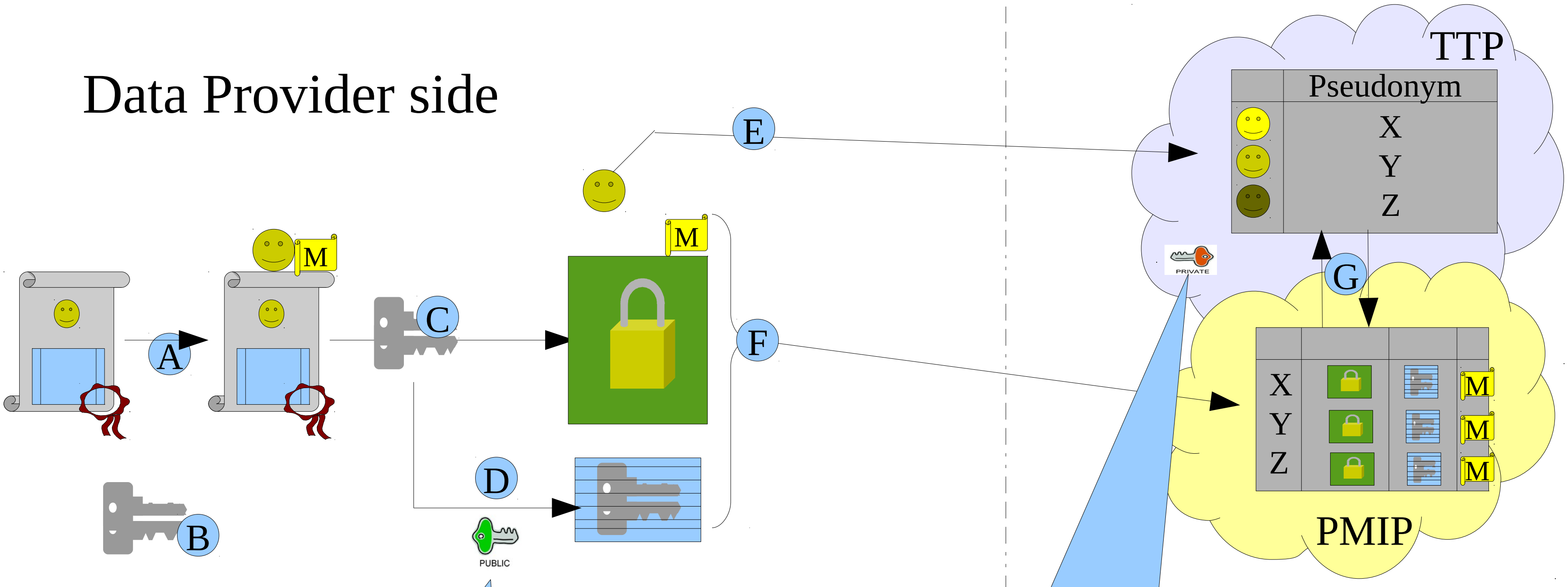
Architecture & Security

Workshop
– Relevant Topics to be discussed ?
– Your Expectations ?

→ TTP's Public Keys … or …
→ Signature PKI mimics costly Encryption PKI
→ Central and De-central Repositories
→ Alerts and Access Logs
→ Scheduled Pseudonym Exchange
→ Multiple Pseudonymization
→ Reduced Security Features for 1st Realization (?)
→ Extension for Statistical Usage

Signature PKI vs. Crypto PKI

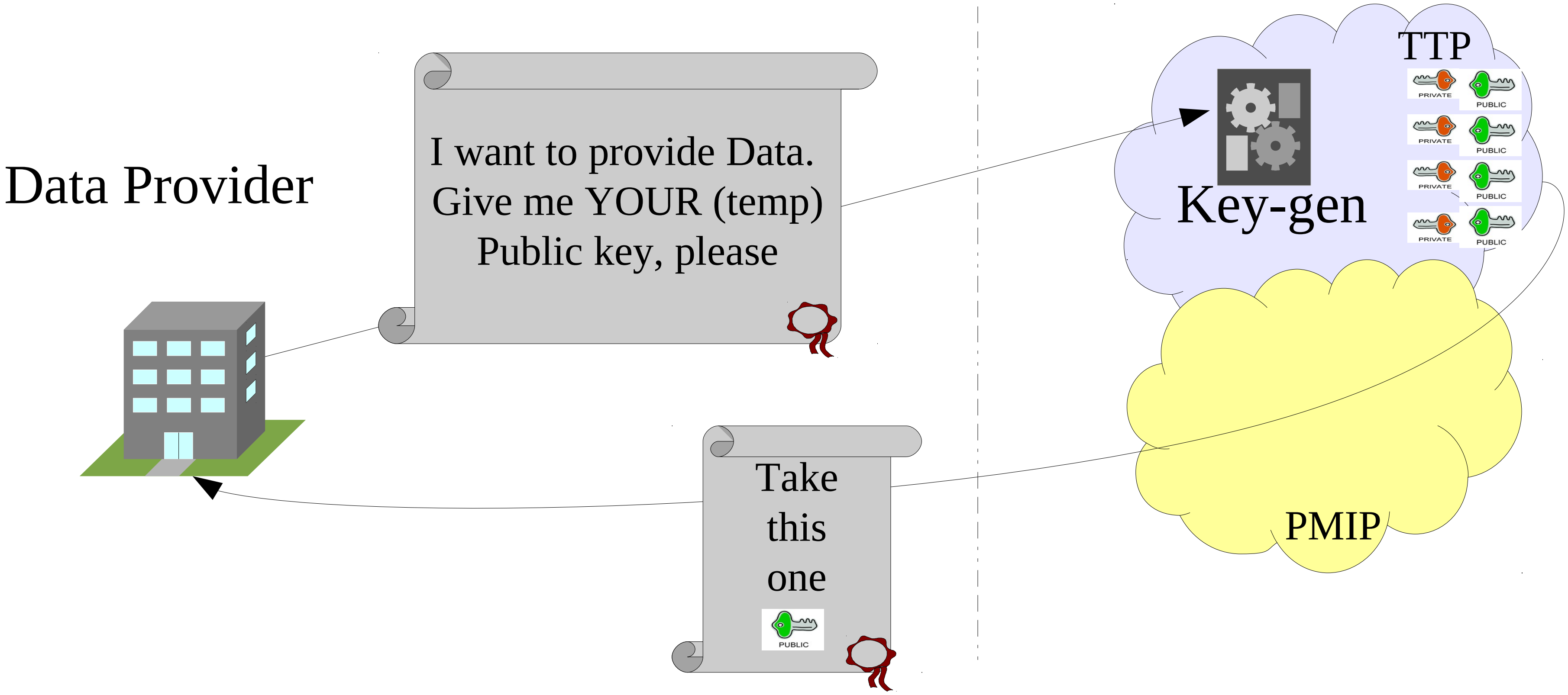
Data Provider side



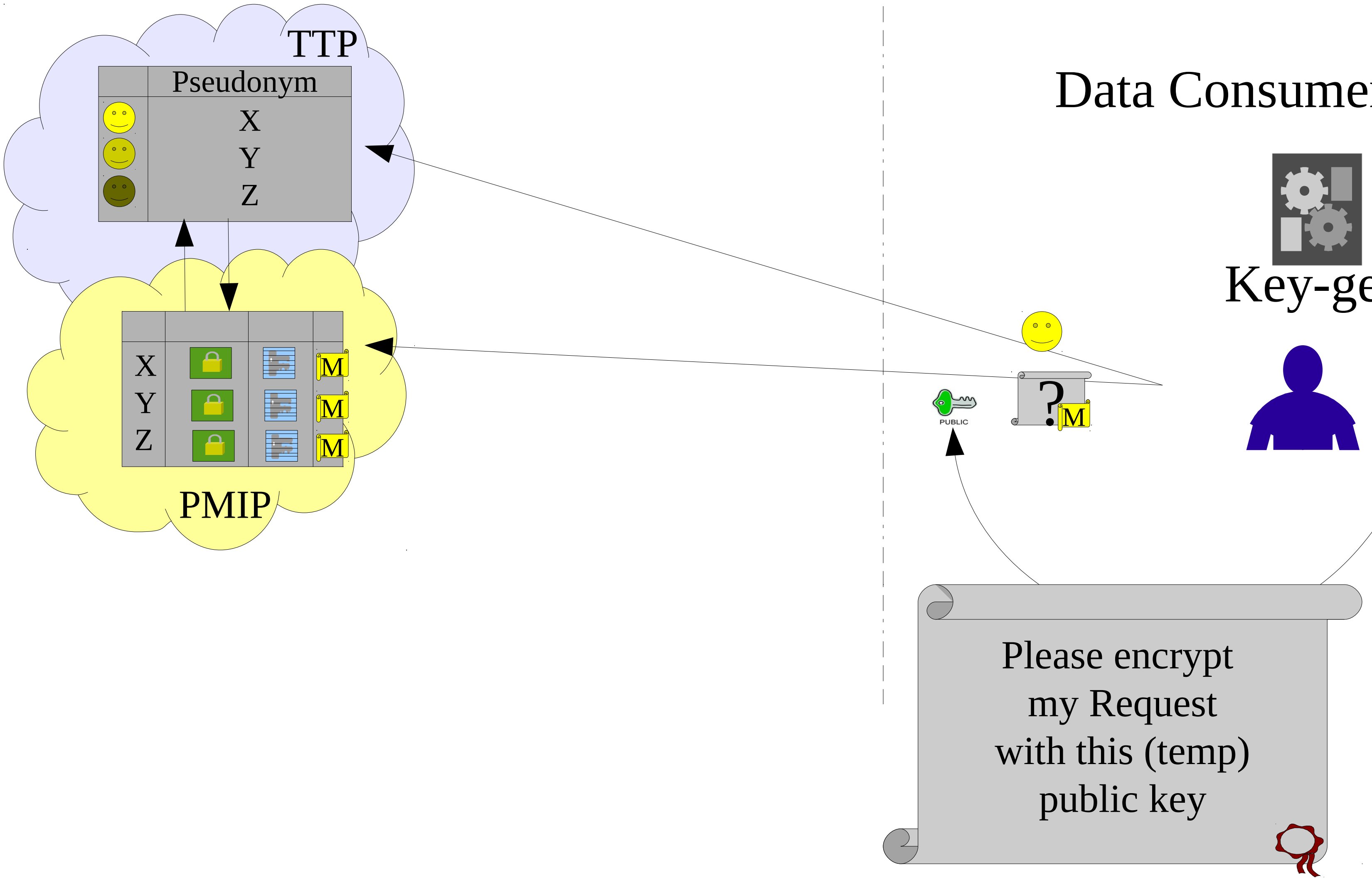
About this public key...

… and its corresponding private key at TTP

Signature PKI vs. Crypto PKI (provide)



Signature PKI vs. Crypto PKI (request)



Please encrypt
my Request
with this (temp)
public key

Signature PKI vs. Crypto PKI

Learned:
When using POP mechanisms
… a signature PKI can simulate a (temp) crypto PKI

The benefit:
– Signature PKI is already provided by Luxtrust and others
– Crypto PKI is more cost intensive because of Backups

Remark:
– Backups of signatures' private keys are forbidden
(non-repudiation of electronic signatures)

Signature PKI vs. Crypto PKI

Results of Workshop-Discussion:

Proposed (temp) encryption keys acceptable?

____

Resulting “Multi-TTP-Key” solution sufficient for security?

____

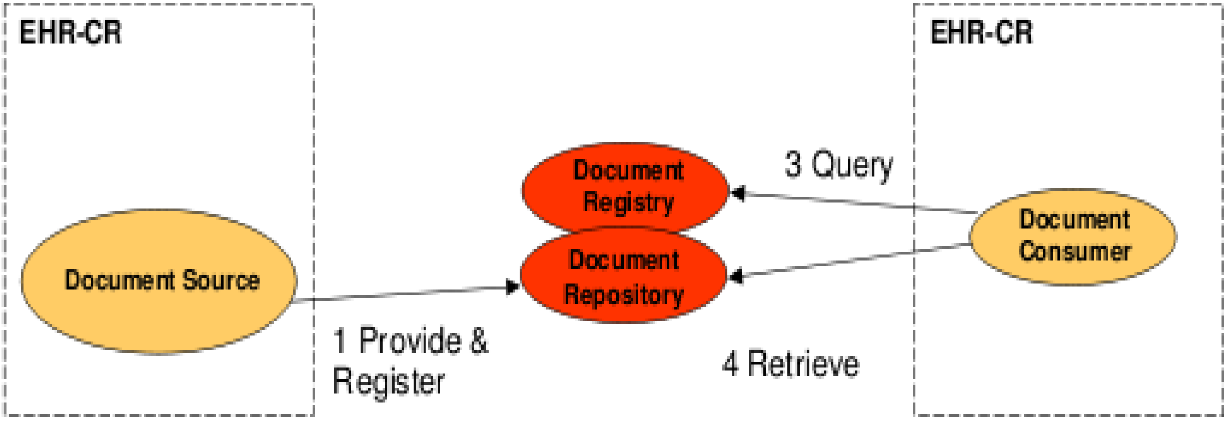
Other ideas, other remarks?

____

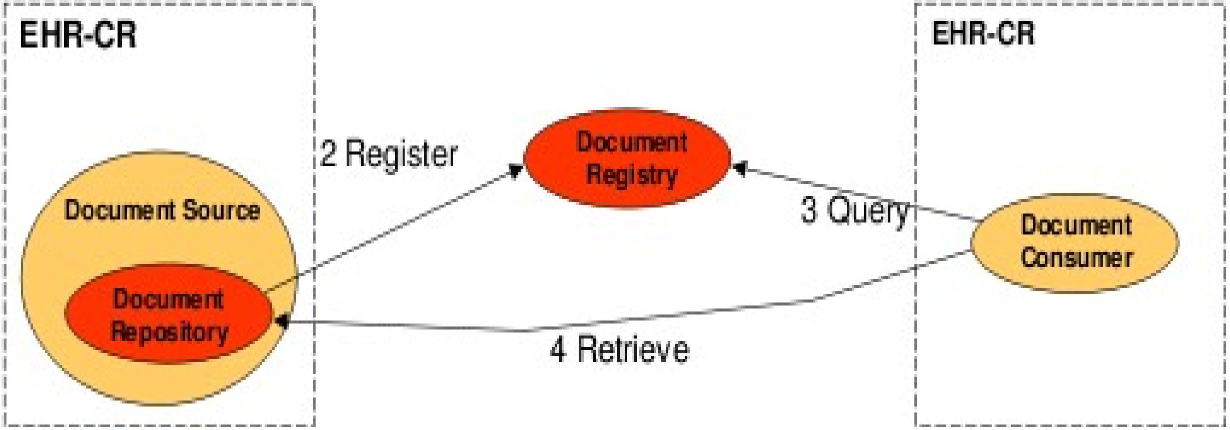
Central and De-central Repositories

IHE XDS

central



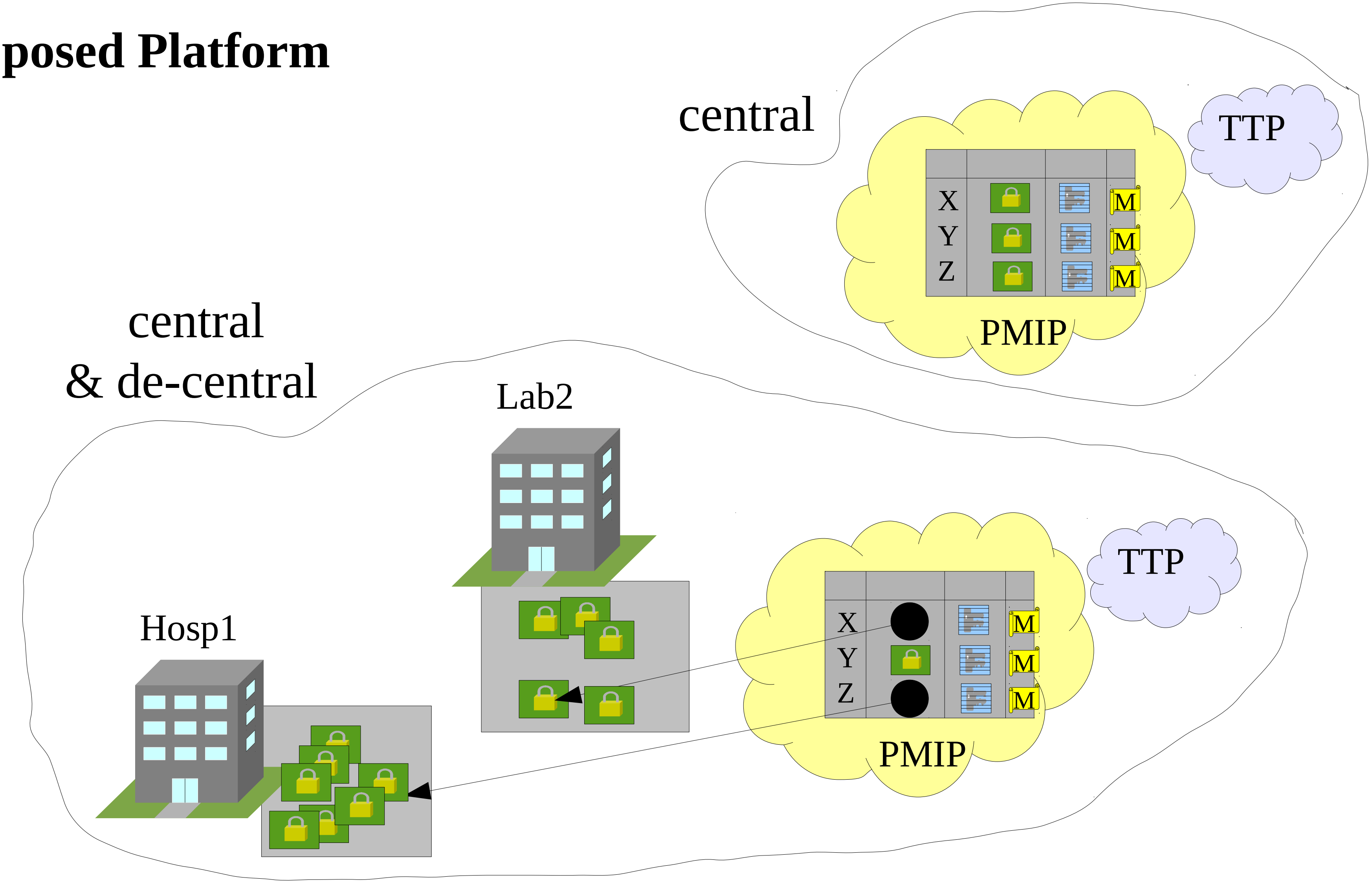
de-central



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

Central and De-central Repositories

Proposed Platform



Central and De-central Repositories

Results of Workshop-Discussion:

Opinion: Will laboratories, hospitals, home care organization, etc. offer "De-Central" Repositories?

____

Should a commercial provider offer "De-Central" Repositories?
→ protection against governmental access (Beschlagnahmeschutz?)

____

Other ideas, other remarks?

____

Alerts and Access Logs

Logging

- Logging of every access, read and write.
- On demand: yearly access report for patient
- Online inspection for logging by patient.

Alerts

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

Alerts and Access Logs

“**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**.”

“In case of **emergency motivated access** to my folder,
a message containing the **accessing emergency unit** (hospital)
Should be send to <patients.brother@his-company.lu>
and per SMS to <+352 66123456>
and …. “

Alerts and Access Logs

Results of Workshop-Discussion:

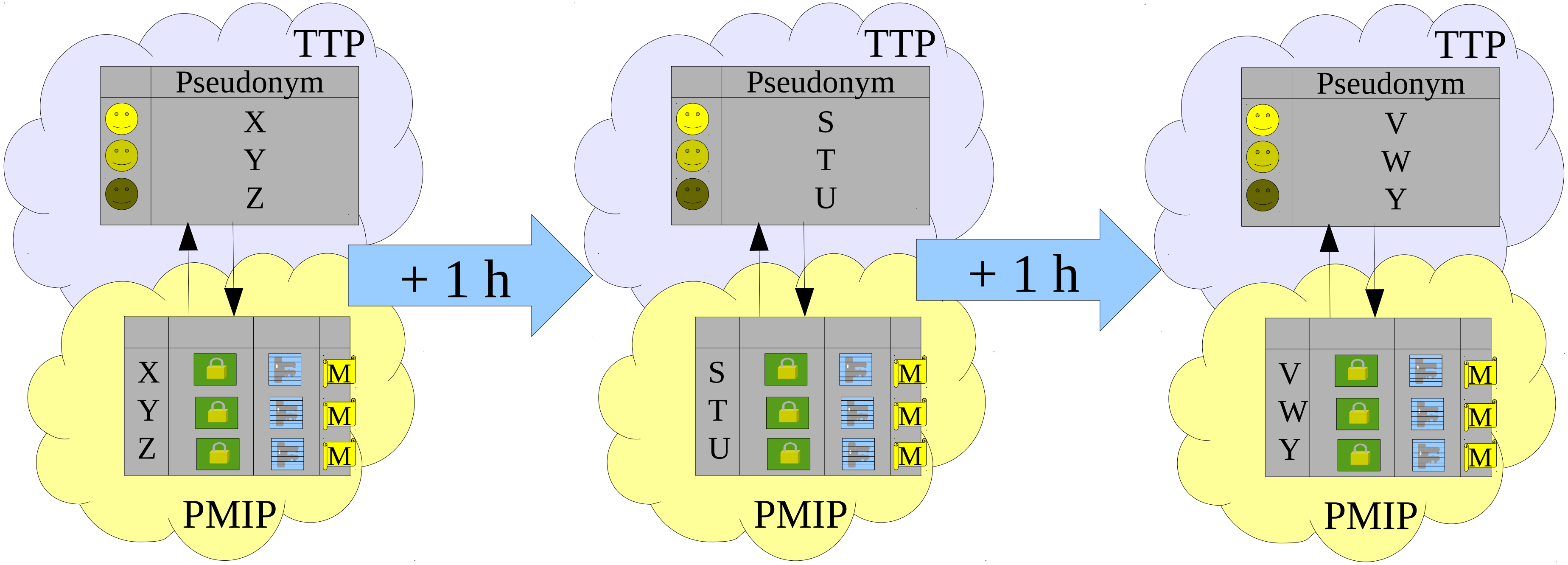
Switch Alert ON with Consent Declaration?

____

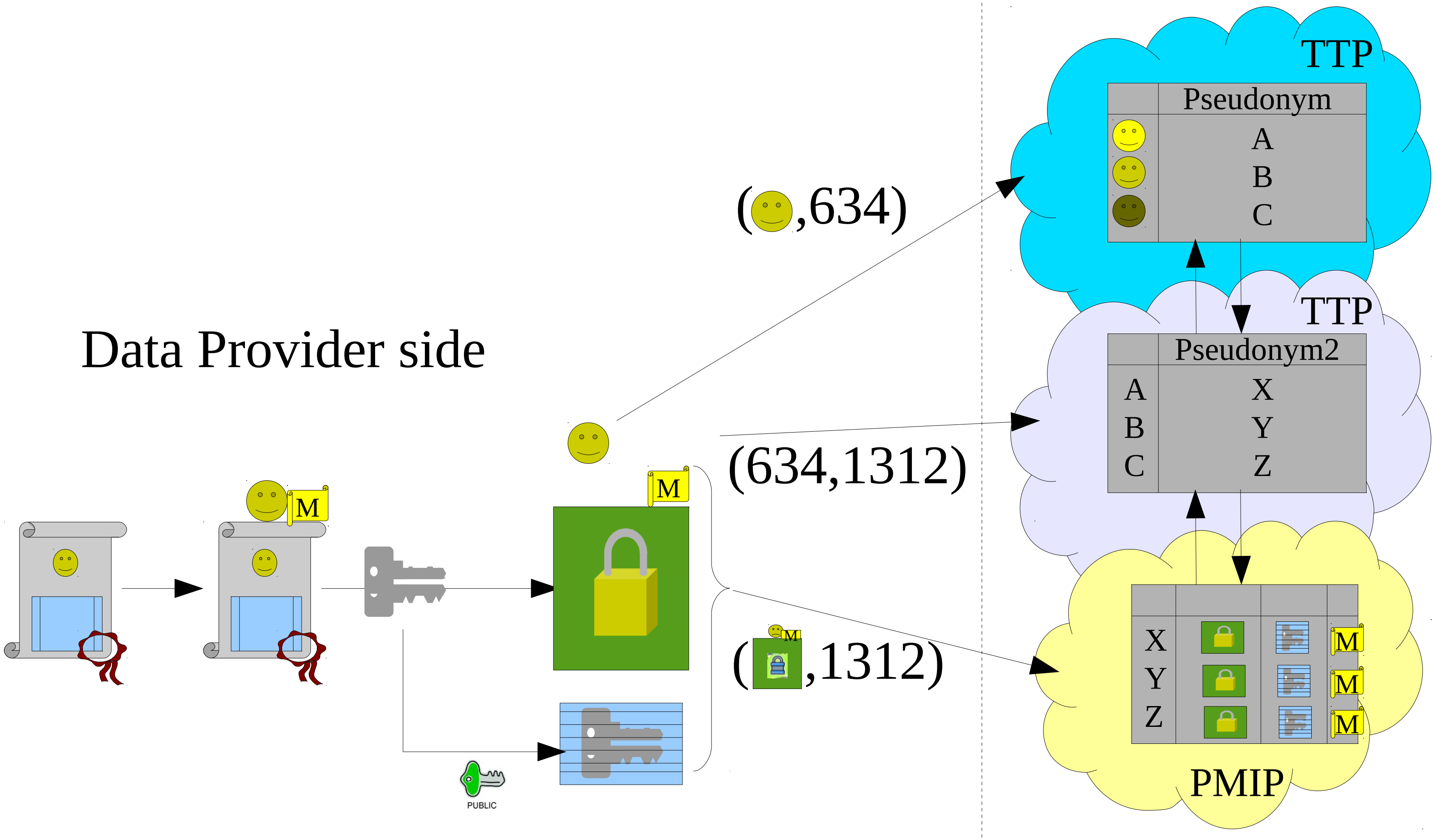
Other ideas, other remarks?

____

Scheduled Pseudonym Exchange



Multiple Pseudonymization



Data Provider side

(☺,634)

(634,1312)

(🔒,1312)

TTP

	Pseudonym
☺	A
☺	B
☺	C

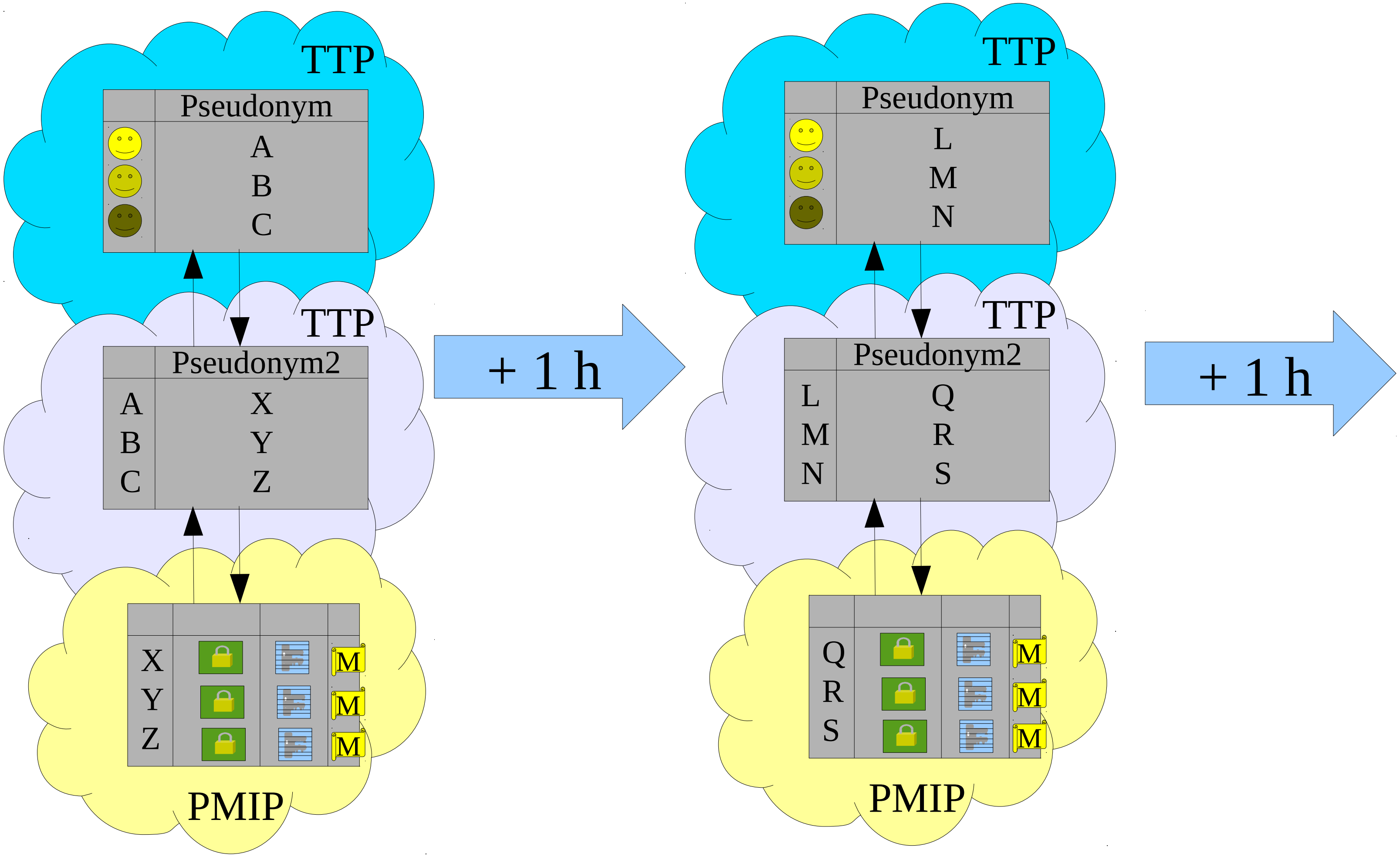
TTP

	Pseudonym2
A	X
B	Y
C	Z

X	🔒	▨	M
Y	🔒	▨	M
Z	🔒	▨	M

PMIP

Combination of Both (SPE, MP)



	Pseudonym
🙂	A
🙂	B
🙂	C

	Pseudonym2
A	X
B	Y
C	Z

X	🔒	▤	M
Y	🔒	▤	M
Z	🔒	▤	M

	Pseudonym
🙂	L
🙂	M
🙂	N

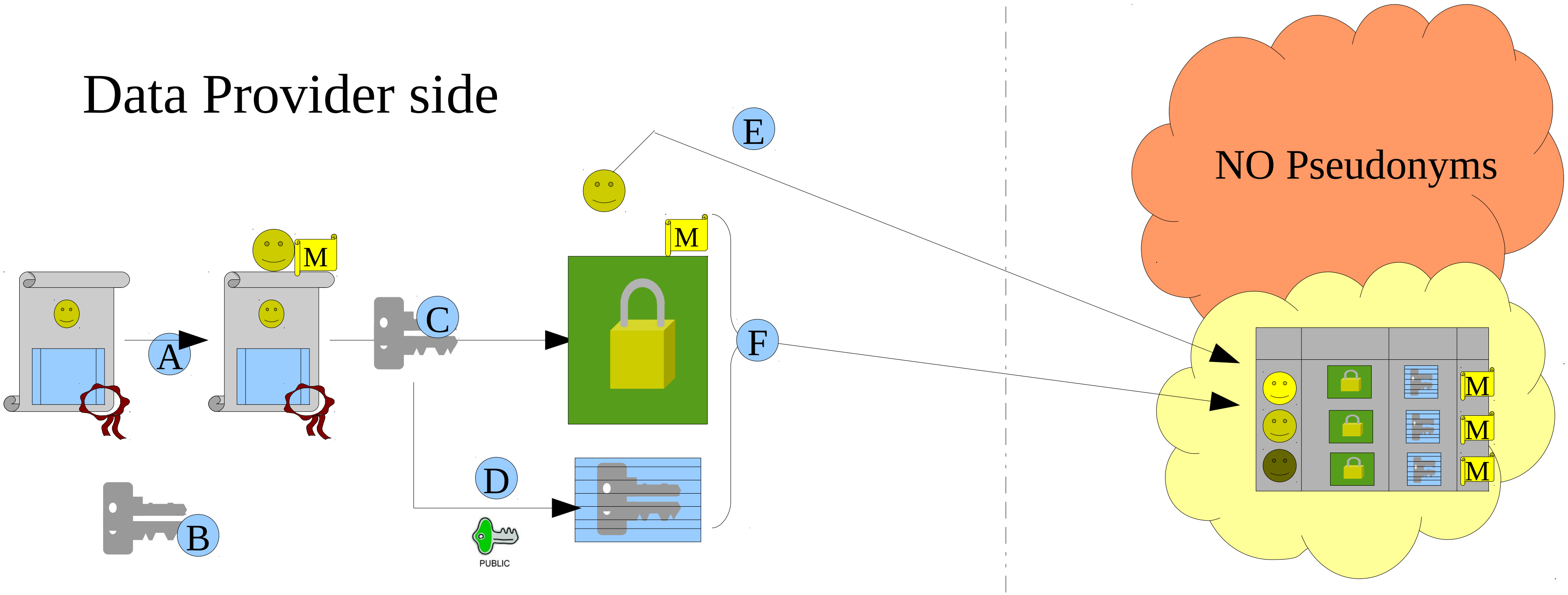
	Pseudonym2
L	Q
M	R
N	S

Q	🔒	▤	M
R	🔒	▤	M
S	🔒	▤	M

… or with different intervals

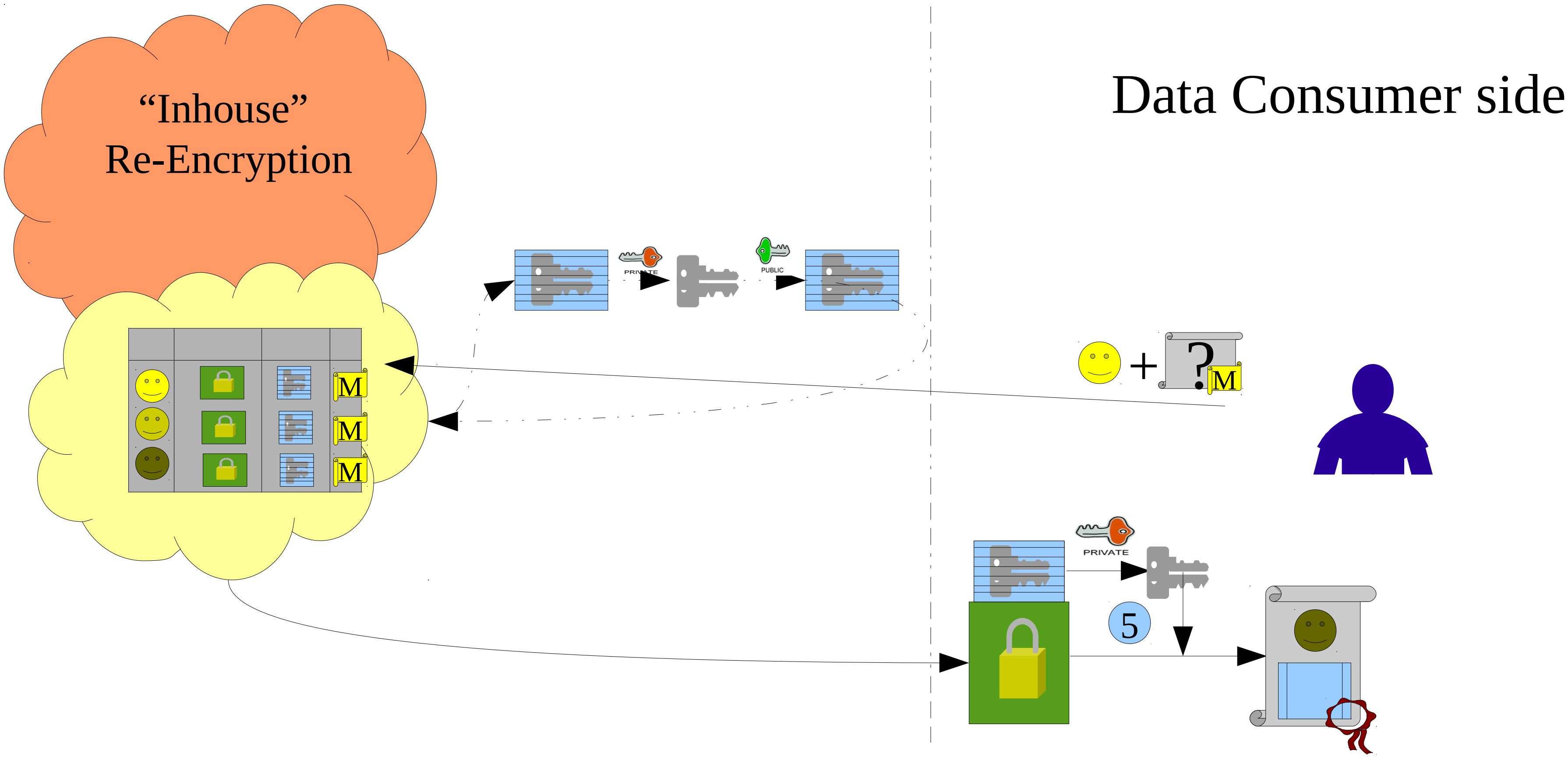
Reduced Security for 1st Realization (?)

Data Provider side



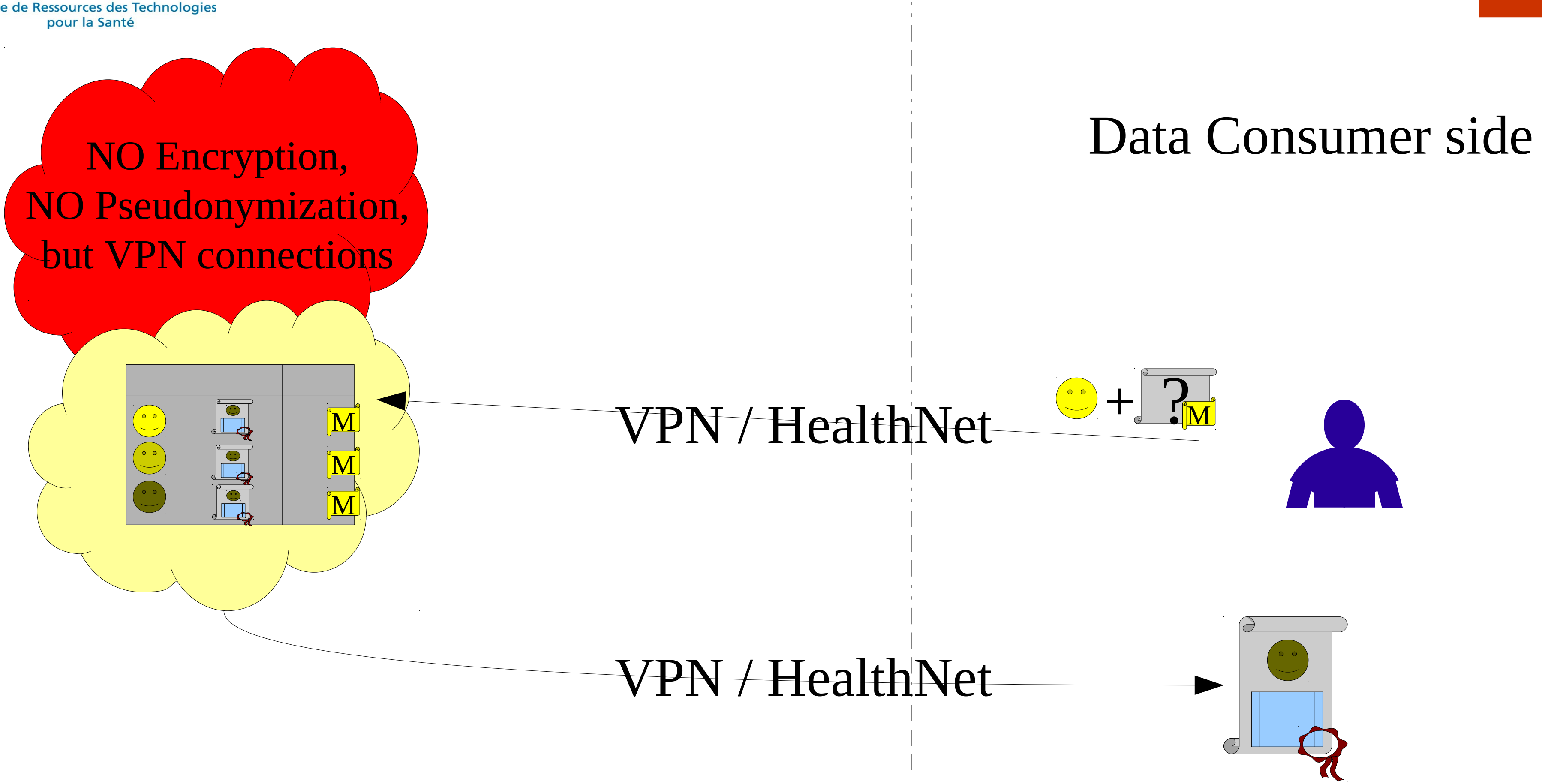
No Pseudonymization

Reduced Security for 1st Realization (?)



– No Pseudonymization, and
– Documents are disclosed during Re-Encryption

Reduced Security for 1st Realization (?)

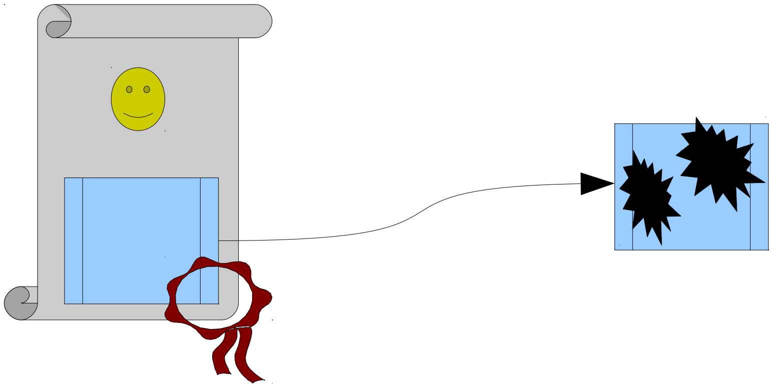


– No Pseudonymization, and

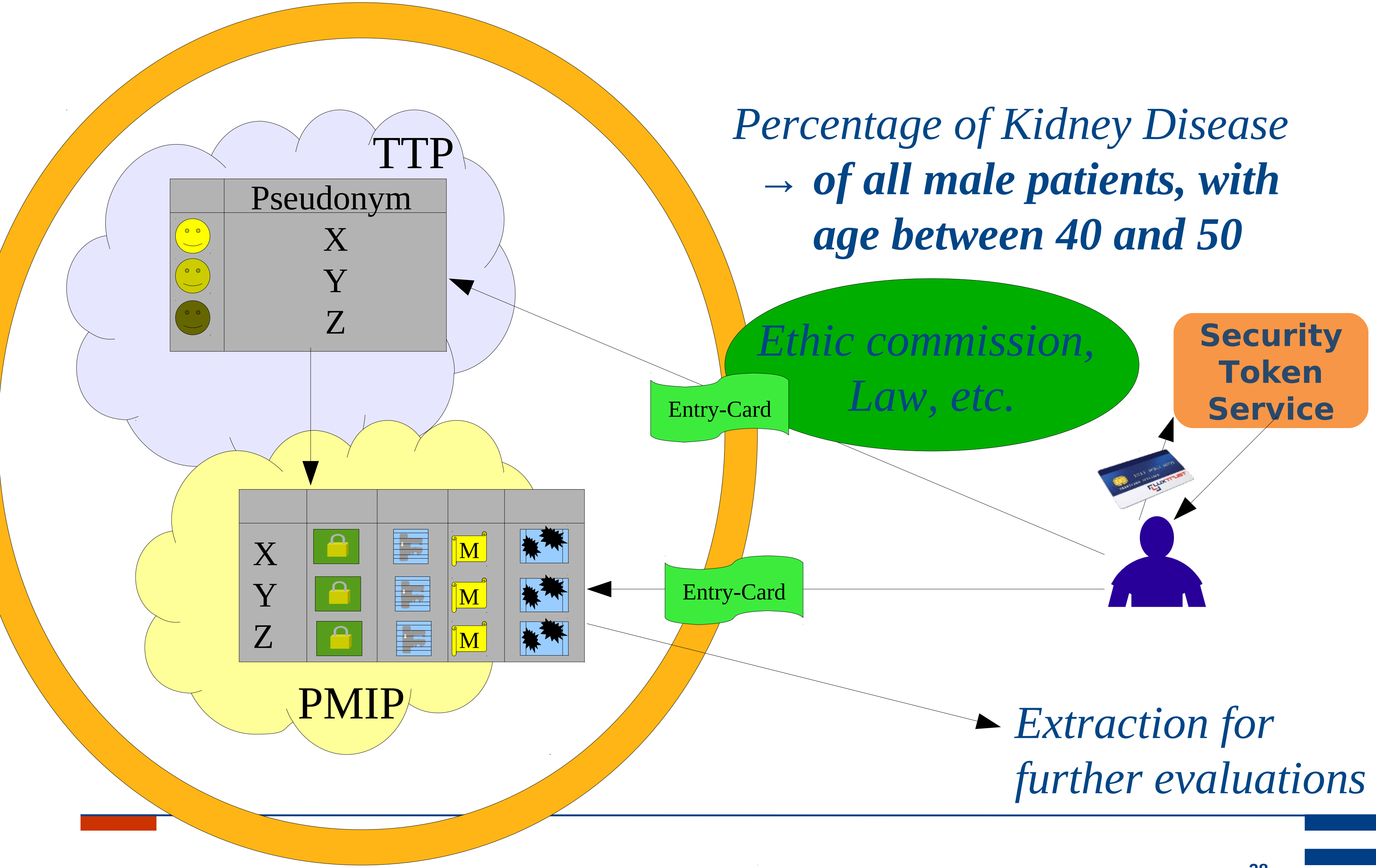
– No (Public-User-Key) Encryption, only VPN line encryption

Extension for Statistical Usage

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



Extension for Statistical Usage



Percentage of Kidney Disease
→ ***of all male patients, with age between 40 and 50***

Extraction for further evaluations

Security Enhancements

Results of Workshop-Discussion:

Opinions about
- Scheduled Pseudonym Exchange (SPE)
- Multi-Pseudonymization (MP)
- Combination of SPE and MP

Security Reductions

Results of Workshop-Discussion:

Opinions about

- NO Pseudonymization
- “Inhouse” Re-Encryption (Disclosure for Admin / Intruder)
- NO Encryption, i.e. only HealthNet / VPN line encryption

Statsitical Usage (secondary usage)

Results of Workshop-Discussion:

Opinions about

– Stripped Fragments for Statistical Usage

____

Thank you for your participation

- Other Topics, other remarks?