

# A Privacy-Preserving eHealth Protocol compliant with the Belgian Healthcare System

Bart De Decker<sup>†</sup>, Mohamed Layouni<sup>‡</sup>, Hans Vangheluwe<sup>‡</sup>,  
Kristof Verslype<sup>†</sup>

<sup>†</sup>Department of Computer Science, KULeuven, Belgium

<sup>‡</sup>School of Computer Science, McGill University, Canada

Fifth European PKI Workshop  
16-17 June 2008  
NTNU

- 1 Introduction
- 2 Overview of the Belgian Healthcare System
- 3 Security and Privacy Requirements
- 4 Building Blocks
- 5 Privacy-Preserving Protocol for eHealth
- 6 Discussion

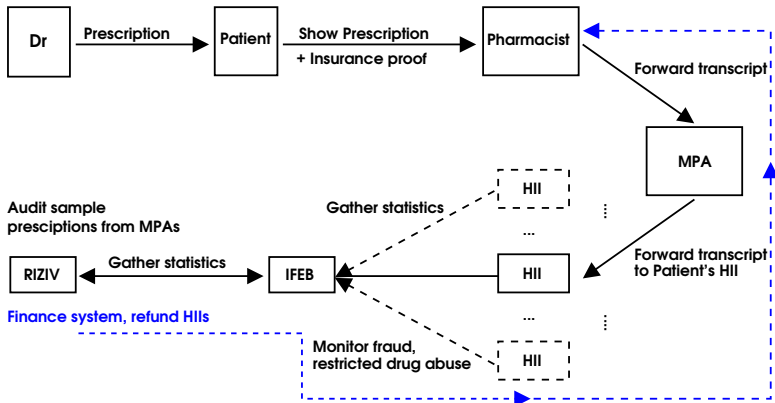
## Why privacy in eServices is useful?

- eServices ⇒ higher convenience, speed, availability  
⇒ improved quality of service
- eServices could be **privacy-invasive** if not built properly  
⇒ users will be reluctant to fully embrace them  
⇒ lack of trust, less growth . . .

Privacy gives users confidence to fully embrace eServices.

We design a [privacy-preserving protocol](#) for prescription-handling, [compliant](#) with the current practice of the Belgian healthcare system.

- ▶ Designing privacy-friendly protocols for real world systems is a challenging task:
  - Real world systems are large, and involve too many parties/roles.
  - Existing infrastructure should not be ignored.



**Figure:** Belgian Healthcare System

- Particularity of Belgian healthcare system: Most HIIs (Health Insurance Institutes) are affiliated with some religious or political body (e.g., The Liberal, Socialist, Christian, Free, Neutral Fund).
- The Patient's politico-religious orientation is a private matter.
- It would be desirable if the Patient could fill his prescription without revealing the name of his HII, and other private information such as health history...
- The Patient proves that he's affiliated with some HII w/o revealing which one.

## Security Requirements:

- Authentication, integrity (prescriptions/transcripts), Revocability (in case of fraud.)
- Single prescription spending.
- Prescription non-transferability.
- Payment fraud detection capabilities . . .

## Privacy Requirements:

- Minimum/Selective disclosure.
- Patient unlinkability except wrt. HII and Dr.
- Patient untraceability except wrt. HII, and RIZIV (if abuse)
- Dr. prescription pattern monitoring prevention (to prevent bribery, kick-backs) . . .

Party\Data	Patient	Presc.	Doctor	Pharm.	MPA	HII
<b>Patient</b>	ID (trivial)	all content	ID	ID	ID	ID
<b>Doctor</b>	nym	PrescID, data (trivial)	ID (trivial)	—	—	—
<b>Pharm.</b>	ss status	data	ID (if anomaly)	ID (trivial)	ID	—
<b>MPA</b>	nym, ss status	PrescID, data	nym	ID	ID (trivial)	ID
<b>HII</b>	ID	PrescID, cost	—	—	ID	ID (trivial)
<b>IFEB</b>	nym, ss status etc.	anon. stat. data	nym	geog. location	—	—

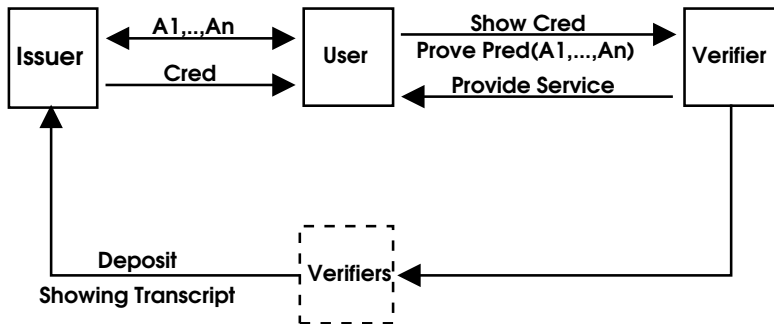
**Table:** Access control matrix

Proposed construction based on :

- Privacy-preserving credentials.
- Traditional public-key certificates, when privacy is not needed (e.g., for public entities.)
- Commitment schemes.
- Verifiable encryption.

## Two main types of credentials:

- Traditional public key certificates (e.g., X.509) : signature on holder's **serial number**, name/pseudonym, address etc.  
⇒ Offer no privacy.
- Privacy-preserving (anonymous) credentials  
⇒ Technology of choice for handling privacy.



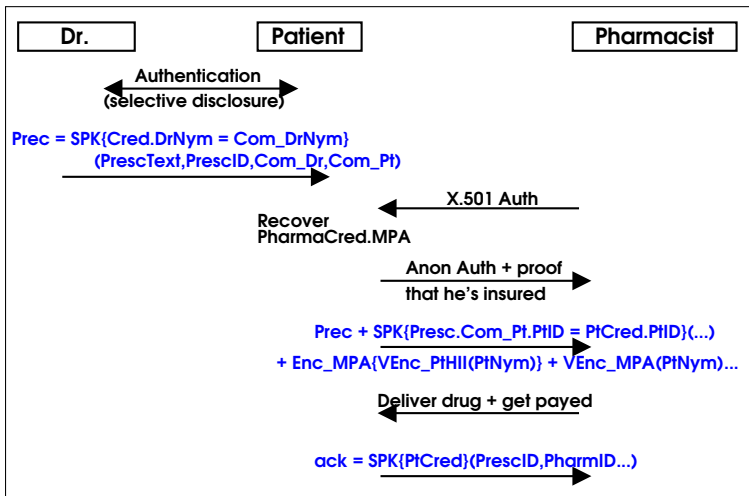
**Figure:** Privacy-preserving Credential Issuing, Showing, and Depositing

## Properties of privacy-preserving credentials

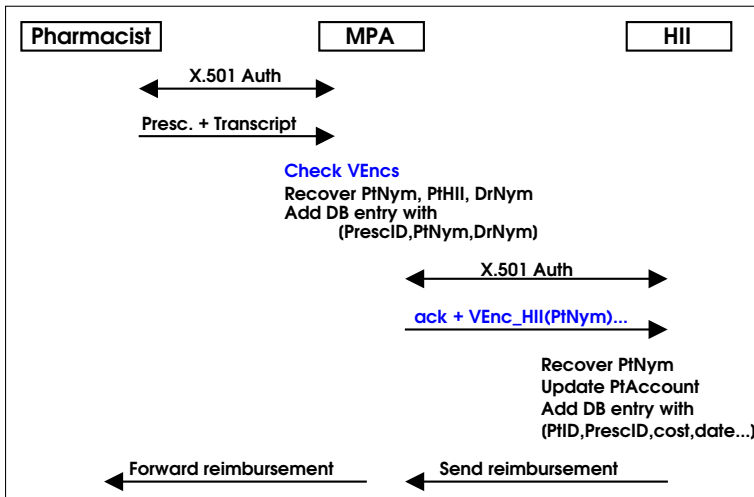
- Unforgeability (issuing)
- Selective disclosure (in the sense of Zero Knowledge)
- Soundness (no false claims)
- No framing (showing transcript unforgeability)
- Untraceability (showings wrt. issuing)
- Unlinkability (between showings)
- *Limited-show* unlinkability, untraceability . . .

## Existing implementations (in alphabetic order!)

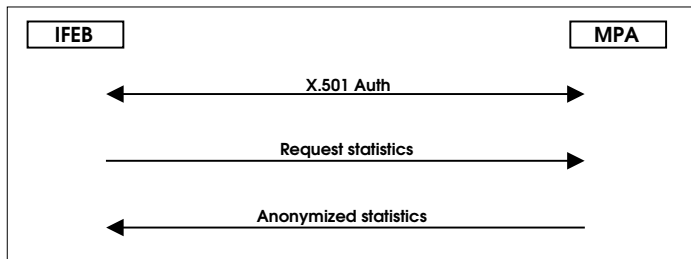
- IBM's IDEMIX (Camenisch and Lysyanskaya)
- Credentica's U-Prove (Brands)



**Figure:** Privacy-Preserving Protocol for Belgian Healthcare (1)



**Figure:** Privacy-Preserving Protocol for Belgian Healthcare (2)



**Figure:** Privacy-Preserving Protocol for Belgian Healthcare (3)

- The MPA knows the Patient and Dr. only by their pseudonyms (PtNym and DrNym)
- The pseudonyms make it possible to generate statistics but not to identify individuals, when population is large.

## Lessons learned . . .

- Designing real world systems is not easy (b/c size and pre-existing infrastructure)
- Analysing them is equally complicated . . .
- Experience gained while designing one (healthcare) system can be greatly beneficial to new ones.

Possible extensions to our system:

- *k*-show creds. can be used with [refillable prescriptions](#),
- Protocols for access control to remotely stored personal data can be used for delegated/authorized access to EHRs. *For example:*

Mohamed Layouni, *Accredited Symmetrically Private Information Retrieval*, IWSEC'07

**Thank you!**