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

Bart De Decker[1], Mohamed Layouni[2], Hans Vangheluwe[2], and Kristof Verslype[1]

[1] Department of Computer Science, K.U.Leuven, Celestijnenlaan 200A, B-3001 Leuven, Belgium
[2] School of Computer Science, McGill University, Montreal, Quebec, Canada

**Abstract.** Real world healthcare systems are generally large and overly complex systems. Designing privacy-friendly protocols for such systems is a challenging task. In this paper we present a privacy-preserving protocol for the Belgian healthcare system. The proposed protocol protects the patients' privacy throughout the prescription handling process, while complying with most aspects of the current Belgian healthcare practise. The presented protocol relies on standard privacy-preserving credential systems, and verifiable public key cryptography, which makes it readily fit for implementation.

**Keywords:** anonymous credentials, electronic healthcare, privacy.

## 1 Introduction

Healthcare represents one of the main pillars reflecting the quality of public service in our society. Over the years, countries around the world have experimented with a multitude of technical choices and policies to improve the quality of their health service. One technical choice that seems to be turning into a trend is the migration from traditional paper-based healthcare to electronic healthcare. The latter has a number of advantages. Among them we note the greater convenience and speed to access health data, which translates into shorter treatment delays, less medical errors, better statistics, higher cost-efficiency, better fraud detection mechanisms, and shorter refund delays for patients covered by health insurance plans.

Despite all the above benefits, patients around the world have shown a certain reluctance and skepticism towards new electronic healthcare systems. The reason for this skepticism is mainly attributed to the lack of assurances about the way patient data is handled, and the implications that may result from it on patients' privacy.

To help reduce this lack of trust one should design ehealth protocols with both security and privacy in mind. Due to the sensitive nature of health data, such protocols should be based on well established cryptographic primitives, and should provide defences against possible user inadvertencies such as ID card losses.

Designing protocols however without consideration for the current procedures, practices, and existing infrastructures, represents a great obstacle to the adoption

S.F. Mjølsnes, S. Mauw, and S.K. Katsikas (Eds.): EuroPKI 2008, LNCS 5057, pp. 118–133, 2008.

of these protocols regardless of their ingenuity. This is due in part to the high costs required to change the existing infrastructure before the new system can be used. In some cases the proposed protocols require the elimination of entire parties. Sometimes these parties represent on the ground a government agency or a ministry, and removing them is simply unrealistic.

In this work, we design a protocol that protects the privacy of patients throughout the prescription handling process, while complying with most aspects of the current Belgian healthcare practice [1]. The Belgian healthcare system is a large and complex system with many players who do not necessarily share the same interests. The ehealth protocol we propose protects (1) the privacy of patients by eliminating any information leak that may harm the interests of the patient, (2) the privacy of doctors, their prescription habits, and their interactions with patients, and (3) the interests of the government by avoiding any provable evidence of a doctor's prescription behaviour, which could be sold to pharmaceutical companies for example. Moreover, our protocol has mechanisms to handle disputes and retrace fraudsters, all without changing the structure of the current Belgian healthcare practice.

Furthermore, healthcare systems with a structure similar to that of the Belgian system, can benefit from the protocol proposed in this paper modulo a few minor adaptations.

**Paper Organization.** First we start with related work in section 2. Then in section 3 we introduce the Belgian healthcare system. In section 4 we describe the security and privacy requirements achieved by our protocol. In sections 5 and 6 we describe the building blocks as well as the protocol we propose to achieve the previous requirements. In section 7, we evaluate the the proposed protocol. We conclude in section 8, and discuss a few ideas to extend our work.

## 2 Related Work

A significant amount of work related to ehealth can be found in the literature. One of the major focus points so far has been on the issue of migrating services from the paper-based setting to the electronic one. A great deal of work for instance has been dedicated to features such as semantic web and interoperability between various healthcare organizations [12,13,14,19]. Other issues have been addressed as well, such as reliability, accessibility, availability, storage integrity, and fault-tolerance [16,18].

Privacy in healthcare has also been addressed. Ateniese et al. [1] propose an ehealth protocol compatible with the healthcare system in the US. The proposed protocol provides *pseudonymous* privacy to the patients, and protects the identity as well as the prescription patterns of doctors. The patient's privacy relies on a tamper-resistant smartcard solution based on conventional public key certificates. The doctors' privacy however is based on a group signature scheme, allowing them to issue prescriptions to patients on behalf of an accredited group

[1] There are auxiliary procedures in the Belgian healthcare system that are not covered in this paper. The proposed protocol can be slightly modified to include them.

of doctors. The doctors' anonymity can be revoked by an escrow party, and all the prescriptions issued by a given doctor are linkable to each other by the insurance company. Prescription linkability is an added feature in [1], and is intended to allow insurance companies to gather statistics. The protocol we propose uses privacy-preserving credentials equipped with a selective disclosure feature, and provides stronger privacy guarantees for the patient and doctors. Moreover our protocol is more efficient than that of [1] owing to the higher performance of credential systems in comparison with group signatures.

Yang et al. [21] propose a smartcard-enabled electronic prescription system compatible with the healthcare system in the US, similar to that of [1]. They also present a signature delegation feature that allows a patient to authorize a delegate (e.g., family member) to pick up prescribed medicines, and sign a reception pad on the patient's behalf, without the patient giving his signing key to the delegate. Unlike Ateniese et al.'s construction, the scheme in [21] advocates for storing all patient health data on the smartcard in order to facilitate patient mobility, and spare doctors the burden of querying remote medical databases through an unreliable network. The smartcard in [21] is also used to store patient signing keys and certificates, as well as to compute signatures. While the smartcard paradigm is interesting in many ways, the protocol as described in [21] makes the security and privacy the patients completely dependant on the tamper-resistance of the card. Moreover, the construction in [21] is such that the identity of the pharmacist is fixed by the doctor at the time of issuing the prescription. This is clearly too restrictive from the patient's point of view, since no alternative is given if the patient cannot obtain all prescribed medicine at the designated pharmacist, or if he decides to fill his prescription at a pharmacist of his choice. Moreover, allowing doctors to designate a particular pharmacist at prescription issuing time, may result in kickback schemes between doctors and pharmacists.

In [20], Yang et al. present a password-based authentication scheme for healthcare delivery systems. The rationale behind their scheme is to allow patients to authenticate to healthcare providers using long-term short passwords, as opposed to public-key certificates which assume the existence of a public key infrastructure. It is a well known fact [4,11] however that password-based authentication systems are vulnerable to dictionary attacks. To protect against dictionary attacks, the authors in [20] propose a special network architecture with a front-end *service server* known to users, and a back-end *control server* hidden from users. To authenticate to the system, the user interacts with the service server, who in turn cooperates with the control server in order to validate the authentication request. The system in [20] is purely for authentication purposes; it provides no privacy for the patient, and does not consider issues such as controlling access to health data.

In [9], a system for privacy-preserving electronic health records is presented, which allows a patient to control who has access to her health records. Furthermore, both patient and doctor will remain anonymous towards any central authority. Since this system is also based on anonymous credentials, our system could easily be augmented with these privacy-preserving health records.

## 3 Brief Overview on the Belgian Healthcare System

A typical workflow in the Belgian healthcare system involves a *doctor*, a *patient*, a *pharmacist*, a *Medical Prescription Administration (MPA)*, a *Health Insurance Institute (HII)*, a public safety organization denoted *IFEB*[2], and a social security organization denoted *RIZIV*[3]. Every patient is member of one of the existing HIIs. Every pharmacist is attached to one of the existing MPAs. The latter is called the pharmacist's local MPA. An MPA processes all the prescriptions filled by its client pharmacists, and plays the role of an intermediary between pharmacists and the patients' HIIs. Similar to a router, it sorts received prescriptions by HII, and then forwards them in batch to the right HIIs.

A basic healthcare scenario can be described as follows. The patient visits a doctor and receives a prescription. The patient then takes his prescription to a pharmacist. The pharmacist checks the validity of the prescription, and charges the patient only a portion[4] of the cost. The remaining cost of the prescription will be paid for by the patient's Health Insurance Institute (HII). The pharmacist delivers the prescribed medicine to the patient, and forwards a copy of the prescription as well as an invoice to his local MPA. The MPA in turn processes the received data and forwards it to the patient's HII. The patient's HII checks the validity of the data, updates the patient's records (e.g., total medical expenses so far this year) and sends a reimbursement back to the MPA, who in turn relays it to the pharmacist.

Concurrently with executions such as the one above, the IFEB gathers statistical data from MPAs and interprets it. The IFEB also watches for fraud instances involving restricted drugs such as methadone. The RIZIV also plays a major role in the Belgian healthcare system. It finances the healthcare system by compensating the HIIs. In addition, the RIZIV oversees the overall healthcare system by retrieving and auditing sample prescriptions from the MPAs. The RIZIV is assumed to have direct access to the IFEB database.

*System Model.* Each player in the system above possesses a number of identity attributes. We describe the most important ones in the following.

Doctor: has a credential *DrCred* asserting that he is allowed to practise as a doctor. The Doctor has a unique identifier *DrID*, and a pseudonym *DrNym*. The correspondence between *DrID* and *DrNym* is known only to a trusted oversight authority such as the "College of Physicians". The Doctor's credential *DrCred* contains *DrID* and *DrNym* in addition to other identity attributes.

Patient: has an identifier *PtID*, and a social security status *PtSSS*. In addition, the patient has a "health expense account" *PtAcc* maintained by his HII. The latter is denoted *PtHII*. The value of *PtAcc* indicates the amount the patient has spent sofar in the current year on

[2] "Instituut voor farmaco-epidemiologie van België" in Dutch.
[3] "Rijksinstituut voor Ziekte- en Invaliditeitsverzekering" in Dutch.
[4] The size of this portion is determined by the patient's social security status.

health expenses. Admissible health expenses charged to the patient beyond a predetermined maximum amount will be covered by the HII. Finally, the patient has a pseudonym *PtNym*. The correspondence between *PtID*and *PtNym* is known only to the patient's HII. In summary, the patient's credential contains the attributes {*PtID, PtNym, PtHII, PtSSS, PtAcc, ...*}

Pharmacist: has an identifier *PharmID*, and a corresponding MPA denoted *PharmID_MPA*. The pharmacist's credential contains a number of attributes including *PharmID* and *PharmID_MPA*.

MPA: has a publicly known identifier *MPA_ID*, and a credential certifying its identity. The MPA serves a set of pharmacists, and generates statistics on prescription data on request from authorized organizations such as IFEB.

HII: has a publicly known identifier *HII_ID*, and a credential certifying its identity. The HII maintains the health expense accounts *PtAcc* of affiliated patients, and covers their admissible medical expenses.

IFEB: has a publicly known identifier *IFEB_ID*, and a credential certifying its identity. It gathers statistics, and conducts studies on public safety.

RIZIV: has a publicly known identifier *RIZIV_ID*, and a credential certifying its identity. it performs various oversight activities, and controls organizations such as IFEB.

## 4 Requirements

In this section, we discuss the main security and privacy properties we want to achieve in the proposed ehealth protocol. The functional requirements can be easily derived from the workflow described the previous section.

### 4.1 Security Requirements

**General Security Requirements**

- **Entity authentication (S1).** All parties should be able to properly authenticate each other. No party should be able to succeed in claiming a false identity, or false information about his identity.
- **Item integrity (S2).** Transcripts generated during the prescription lifecycle cannot be tampered with, without being detected with an overwhelming probability.
- **Revocability (S3).** It should be possible to revoke the credentials as well as the anonymity/pseudonimity of abusing parties.

**Security Requirements Specific to the Belgian Healthcare System**

- **Multiple prescription issuance detection capability (D1).** Oversight authorities such as the RIZIV should be able to detect malicious patients

who visit multiple doctors for the same illness in order to get multiple prescriptions of a particular drug.
- **Single prescription spending (D2).** A patient must not be able to fill the same prescription multiple times.
- **Prescription non-transferability (D3).** It should not be possible for a party to fill a prescription, if he is not the patient to whom the prescription was originally issued.
- **Inappropriate prescribing patterns detection capability (D4).** It should be possible to detect doctors who systematically prescribe expensive drugs (instead of generic, and hence, cheaper ones), or doctors who prescribe significantly more drugs of a certain type (e.g. antibiotics) despite known counter-indications etc. In such cases, the doctors involved might be served a warning, or an investigation might be initiated.
- **Correct pharmacist reimbursement (D5).** A pharmacist who is not correctly refunded by the MPA, should be able to prove it in order to be compensated.
- **Payment fraud detection capability (D6).** The pharmacist should be refunded only if he has indeed delivered the medicine to the patient. It should be possible to detect pharmacists who claim expenses for non delivered medicine.
- **Correct statistics (D7).** The IFEB must be ensured that the received statistics are correct.

### 4.2 Privacy Requirements

- **Minimum disclosure (P1).** During a medical consultation, the patient and doctor should be able to selectively (and provably) reveal to each other any property or predicate about their respective identities. In addition, parties involved in the prescription processing workflow should not be able to learn any information about the patient and doctor except what the latter willfully disclose to them. Data exchanged during the ehealth protocol execution should satisfy the access control requirements defined in table 1.
- **Patient unlinkability (P2).** Prescriptions issued to the same patient should not be linkable to each other, except by the patient's HII, or by the doctor (if the patient accepts to reveal such information to the doctor.) On the other hand, two patient prescriptions that cross the same MPA should be linkable to each other, but not to the patient's identity.
- **Patient untraceability (P3).** No party involved in the prescription workflow, except the HII and RIZIV, should be able to determine the identity of the patient. The RIZIV identifies patients only in case of abuse.
- **Absence of provable doctors' prescription behaviour (P4).** To prevent elicit kickbacks and bribery between doctors and pharmaceutical companies, pharmacists should not be able to provide evidence to pharmaceutical companies about doctors' prescription behaviour.

**Table 1.** Access control matrix

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

## 5 Building Blocks: Brief Overview

### 5.1 Commitments

A commitment scheme [17,10] allows a committer to hide a set of attributes inside a token, also called commitment. Later the committer can open the commitment by revealing the underlying attributes. The former phase is called the commitment phase, while the latter is called the opening phase. The commitment scheme is such that the committer cannot open the commitment to a set of attributes that is different from the one embedded in the commitment phase.

*Notation.* For a commitment *comm* with attributes $(x_1, \cdots, x_p)$, the expression $comm.x_j$ denotes the $j^{\text{th}}$ attribute embedded in *comm*. To further conceal the values of the attributes underlying a commitment, one of the embedded attributes can be chosen at random and used as a blinding factor. A commitment can be opened by revealing the attributes in it. The latter is called opening information, and denoted *openInfo*.

### 5.2 Digital Credentials

A digital credential issued to user $U$ is typically a set of assertions made by an certification authority about the identity attributes of $U$. To be viable, a credential system should satisfy a number of security properties such as unforgeability, and integrity. These properties are further discussed below. The X.509 public key certificate standard [15] is a well known example of digital credentials.

*Privacy-preserving* digital credentials (e.g., [5,6,7]) represent a more elaborate type of credentials, also referred to as *anonymous* credentials. In addition to the

usual security properties necessary for traditional digital credentials, privacy-preserving credential systems possess a number of properties intended specifically to protect the identity of honest credential holders. Among these we note *selective disclosure*, *token untraceability*, *tokens unlinkability*, *multi-show unlinkability*, *limited-show untraceability*, and *signed audit trails* [5,6,7]. Privacy-preserving credentials are used as a major building block in this paper.

We distinguish three types of participants in a privacy-preserving credential system:

(1) An *issuer*, generally a recognized certification authority, who issues credentials to users in an *issuing protocol*.
(2) A *user*, to whom credentials are issued. The user, also referred to as the credential holder, shows his credentials, in a *showing protocol*, to third parties in exchange for goods and services. The user can selectively reveal any information about any subset of the attributes underlying his credential. The credential showing can be turned into a non-interactive signed proof. The resulting transcript can be used then as a *signed audit trail*. One desirable feature of this type of credentials is *token untraceability*. This feature ensures that no party, including the issuer can link a showing transcript to the identity of the credential holder. When different credentials owned by the same user are unlinkable to each other, we say that the credential system satisfies *token unlinkability*. When multiple showings of the same credential are not linkable to each other we say that we have *multi-show unlinkability*. The *limited-show untraceability* property is achieved when the identity of the credential remains hidden as long as the credential is not shown more than a predefined maximum number of times.
(3) A *verifier* to whom the user shows his credential. The verifier may later *deposit* the showing transcript at the credential issuer, for instance to redeem e-coins in the context of ecash. The latter protocol is called a *depositing protocol*.

*Notation.* For a credential *Cred* with attributes $(a_1, \cdots, a_n)$, the expression $Cred.a_\ell$ denotes the $\ell^{\text{th}}$ attribute of *Cred*. For example if we assume that the Doctor has an anonymous credential denoted *DrCred*, then *DrCred.ID* and *DrCred.exp* denote the identifier and expiry date of *DrCred* respectively.

Let $A$ be a party holding an anonymous credential *Cred* and commitment *comm* encoding attributes $(a_1, \cdots, a_n)$ and $(x_1, \cdots, x_p)$ respectively. Party $A$ can selectively disclose any information about the attributes underlying *Cred* and *comm*. Given (1) a predicate $\mathcal{P}$ on attributes $(a_1, \cdots, a_n)$ and $(x_1, \cdots, x_p)$, and (2) a message $m$, the expression $\text{SPK}\{\mathcal{P}(a_1, \cdots, a_n, x_1, \cdots, x_p)\}(m)$ denotes a signed proof of knowledge on message $m$, of attributes $a_1, \cdots, a_n$, $x_1, \cdots, x_p$ underlying *Cred* and *comm* respectively, and satisfying predicate $\mathcal{P}$. The expression $\text{SPK}\{comm.DrID == DrCred.ID \wedge DrCred.exp \geq \text{today}\}(m)$ for example, denotes a signed proof of knowledge on message $m$, where the prover convinces a verifier that (1) he knows all the attributes underlying *comm* and *DrCred*, (2) that the *ID* embedded in *DrCred* is the same as the one embedded in *comm*, and (3) that credential *DrCred* has not expired yet.

### 5.3 Verifiable Encryption

A verifiable encryption scheme (e.g., [8]) for a relation $R$ is a protocol that allows a prover to convince a verifier that a ciphertext is an encryption of a value $w$ under a given public key such that $w$ satisfies $R$, and no other information about $w$ is disclosed. In a verifiable encryption scheme, the ciphertext is checked with respect to a public key associated with a known "decryptor".

*Notation.* The expressions $VEnc_A(\cdot)$ and $Enc_B(\cdot)$ denote the verifiable encryption under party $A$'s public key, and the conventional public-key encryption under party $B$'s public key respectively.

Let $\mathcal{M}$ be the message space of $VEnc(\cdot)$ the verifiable encryption scheme, and let $\mathcal{P}$ a boolean predicate on $\mathcal{M}$. The expression

$$vc = VEnc_{\text{RecID}}(m)\{\mathcal{P}(m)\}$$

denotes the verifiable encryption of $m$ under the public key of RecID, the intended recipient. Given the public key of RecID, any verifier can be convinced that $vc$ is an encryption under RecID' public key of a non-disclosed message that satisfies predicate $\mathcal{P}$.

## 6 The Proposed Protocol

### 6.1 Setting

Based on the system model and requirements described in Sections 3 and 4, we made a number choices regarding the type of credentials needed by each participant involved in the ehealth protocol. The patients and doctors are widely considered as private entities with high expectations of privacy; we therefore equip them with anonymous credentials. The other parties however are all public entities; it is sufficient to simply identify them with conventional X.509 public key certificates. These choices are summarized in Table 2.

The credentials of the MPAs, HIIs, RIZIV, IFEB, and pharmacists are issued by trusted government-approved certification organizations. The doctors' credentials are issued by a medical certification authority such as the college of physicians. The patients' credentials are issued by a central government-approved certification authority CA. The patient's pseudonym *PtNym* embedded in the patient's credential is not known to CA. The correspondence between *PtNym* and *PtID* is known only to the patient's HII. Issuing anonymous credentials on secret but committed attributes is easily done by standard techniques such as those in [5,6].

**Table 2.** Credential material per participant

| Cred. type \ Party | Patient | Dr. | Pharm. | MPA | HII | IFEB | RIZIV |
|---|---|---|---|---|---|---|---|
| Anon. Cred. | ✓ | ✓ | | | | | |
| X.509 Cert. | | | ✓ | ✓ | ✓ | ✓ | ✓ |

### 6.2 Protocol Description

I. Doctor (Dr.) ↔ Patient (Pt.)

(a) Dr. anonymously authenticates to Patient using his *DrCred*.
(b) Patient computes commitment $com_{Pt} := comm(PtID)$,
(c) Patient anonymously authenticates to Doctor using his credential *PtCred*. Moreover, Patient sends $com_{Pt}$ to Doctor, and proves that $com_{Pt}.PtID == PtCred.PtID$
(d) Dr. computes commitment $com_{Dr} := comm(DrNym)$
(e) Dr. sets $Presc_text := \{$plain prescription text$\}$
(f) Dr. computes the prescription's serial number *PrescID*, e.g., as a hash of *Presc_text*, $com_{Pt}$, and $com_{Dr}$.
(g) Dr. computes
$$\text{Presc} := \text{SPK}\{DrCred.DrNym == com_{Dr}.DrNym\}(Presc\_text, PrescID, com_{Dr}, com_{Pt}),$$
and sends it to the patient, along with the opening information of $com_{Dr}$.

II. Patient ↔ Pharmacist

(a) Pharmacist authenticates to Patient using his X.509 pharmacist certificate *PharmCred*.
(b) Pt. recovers *PharmCred.MPA_ID*, the identity of the MPA serving the pharmacist.
(c) Pt. anonymously authenticates to Pharmacist using *PtCred*, and provably discloses his social security status.
(d) Pt. computes:
   i. $vc_1 = VEnc_{\text{MPA}}(PtHII)\{PtHII = PtCred.PtHII\}$
   ii. $vc_2 = VEnc_{\text{MPA}}(DrNym)\{DrNym = Presc.com_{Dr}.DrNym\}$
   iii. $vc_3 = VEnc_{\text{RIZIV}}(PtNym)\{PtNym = PtCred.PtNym\}$
   iv. $vc'_3 = VEnc_{\text{RIZIV}}(PtHII)\{PtHII = PtCred.PtHII\}$
   v. $vc_4 = VEnc_{\text{MPA}}(PtNym)\{PtNym = PtCred.PtNym\}$
   vi. $vc_5 = VEnc_{\text{PtHII}}(PtNym)\{PtNym = PtCred.PtNym\}$
   vii. $c_5 = Enc_{\text{MPA}}(vc_5)$
(e) Pt. sends to pharmacist:
   i. Presc. and $\text{SPK}\{PtCred.PtID == Presc.com_{Pt}.PtID\}$(nonce)[5]
   ii. $vc_1, vc_2, vc_3, vc'_3, vc_4, c_5$ [6]

[5] The nonce can be chosen jointly by the patient and pharmacist, and may include information such as the date, *PharmID* etc.

[6] The patient Pt. sends $c_5$ to the pharmacist instead of $vc_5$, because Pt. wants to hide the identity of his HII from the pharmacist. In Belgium, health insurance institutes (HIIs) are managed by socio-political groups, and revealing the identity of a patient's HII, may disclose personal information about the patient's political inclination for example. That is why in the protocol above, the patient hides the identity of his HII from the pharmacist. Only the MPA (downstream) needs to know the identity of the patient's HII. The correctness of $vc_5 = Dec_{\text{MPA}}(c_5)$ will be checked by the MPA, prior to forwarding it to the right HII. Additional data that may be useful for statistics, such as PtAge, can be handed to the MPA inside $vc_4$.

(f) Pharmacist checks if Presc., SPK, and $vc_1, vc_2, vc_3, vc'_3, vc_4$ are correct. If all is correct then continue, else abort. If Presc. contains an anomaly (e.g. unusual or possibly lethal dosage), the pharmacists asks Pt. to name the doctor. The pharmacist will contact the doctor to correct the problem.
(g) Pharmacist charges patient, gets payed, and delivers drug.
(h) Pharmacist issues an invoice to Patient with the prescription's serial number *PrescID* embedded in it.
(i) Patient computes:
reception_ack := SPK$\{PtCred\}$(*PrescID*, *PharmID*, $vc_1, vc_2, vc_3, vc'_3, vc_4, c_5$),
and sends it to Pharmacist. This proves that the patient has indeed received the medicine from the pharmacist.
(j) Pharmacist checks if reception_ack is correct. If correct continue, else abort.

III. Pharmacist ↔ MPA (*PharmCred.MPA_ID*)
(a) Pharmacist and MPA mutually authenticate
(b) Pharmacist forwards to MPA Presc., $vc_1, vc_2, vc_3, vc'_3, vc_4, c_5$, and reception_ack.
(c) If all is correct, the MPA continues. Else if $Dec_{\mathrm{MPA}}(c_5)$ is incorrect, then forward $vc_3, vc'_3$, and rest of transcript to RIZIV and request patient deanonymization.[7]
(d) MPA computes:
i. $PtNym = Dec_{\mathrm{MPA}}(vc_4)$,
ii. $PtHII = Dec_{\mathrm{MPA}}(vc_1)$,
iii. $DrNym = Dec_{\mathrm{MPA}}(vc_2)$,
iv. $vc_5 = Dec_{\mathrm{MPA}}(c_5)$
(e) MPA adds a DB entry indexed by *PrescID*, *PtNym*, *DrNym*, and stores any information relevant to the prescription.

IV. MPA ↔ HII (*PtHII*)
(a) MPA and HII mutually authenticate
(b) MPA forwards reception_ack and $vc_5$ to the patient's HII
(c) HII checks the integrity of reception_ack and $vc_5$
(d) If correct, HII recovers $PtNym = Dec_{\mathrm{HII}}(vc_5)$, else abort and forward transcript to RIZIV for patient deanonymization.
(e) HII recovers *PtID* corresponding to *PtNym*
(f) HII updates patient *PtID*'s account *PtAcc* with proper amount
(g) HII sends reimbursement amount due to the MPA, along with the corresponding invoice containing *PrescID*.
(h) HII creates a database entry for the processed invoice with information such as *PtID*, *PrescID*, prescription cost, date etc.
(i) After receiving the refund from the HII, the MPA compensates the pharmacist.

[7] The RIZIV first recovers *PtNym* and *PtHII*) from $vc_3$ and $vc'_3$), then files a complaint with the judicial authorities who can subpoena the HII to provide the real identity of the fraudulent patient.

V. IFEB ↔ MPA
   (a) MPA and IFEB mutually authenticate
   (b) IFEB requests statistics
   (c) MPA provides statistics on prescription data anonymized according to the privacy laws in place.

   The data available to the MPA is identified only by Doctor and Patient pseudonyms. This data is sufficient to generate meaningful statistics, including measurements requiring the aggregation of prescription data per patient or per doctor. The data available to the MPA, and the subsequently released statistics do not compromise the real identities of patients or doctors.

   Alternatively, the IFEB can obtain statistics from the HIIs. This can be done without weakening the privacy of the patient or inducing additional disclosures, since the HIIs already know the prescription data of their affiliated patients. The IFEB first queries the different HIIs for a specific statistical measurement, and then aggregates the separate *anonymized* results to derive the global measurement for the whole population. Data from the HIIs can also be used to double-check the accuracy of statistics collected from the MPAs.

Remarks

- In step I-(g) the Doctor computes the prescription as a signed proof of knowledge on the tuple ($Presc\_text$, $PrescID$, $com_{Dr}$, $com_{Pt}$). The predicate being asserted in the proof is that $com_{Dr}$ contains the same attribute $DrNym$ embedded in $DrCred$. This results in the following observations:
  - Because the prescription is a signed proof, any one can check its validity non-interactively.
  - The prescription is tied via ($com_{Dr}$, $com_{Pt}$) to the identity of both the Doctor and the Patient. Recall that the Doctor issues the prescription only if the value of $PtID$ underlying $com_{Pt}$ is consistent with $PtCred$ (the consistency proof was performed by the Patient in step I-(c).)
  - The Doctor discloses the opening information of $com_{Dr}$ to the patient, to allow him to verifiably encrypt $DrNym$ under the public key of the pharmacist's MPA (in step II-(d-ii).) Note that the Doctor cannot encrypt $DrNym$ in advance since the identity of the pharmacist where the patient will buy his drugs is usually not known at the time of the prescription issuing.

## 7 Protocol Evaluation

In the following we provide proof sketches and arguments supporting the security of our protocol. we assume all underlying building blocks secure. A more formal and complete analysis will be given in the full version of the paper.

### 7.1 General Security Requirements

- **Entity authentication (S1).** This property follows immediately from the soundness and unforgeability of the underlying anonymous and public key certificates.
- **Item integrity (S2).** All binding data (e.g., prescription, acknowledgement, verifiable encryptions) exchanged during the protocol of Section 6, are signed either by a conventional public key signature or signed proof of knowledge, and are therefore resistant to any tampering.
- **Revocability (S3).** In case of abuse (which can be detected either by the MPA, the patient's HII, or the RIZIV), the user's identity is unveiled by opening one of the verifiable encryptions $vc_3$, $vc_4$, or $vc_5$. It is then possible to revoke the patient's credentials and prescriptions through blacklisting.

### 7.2 Security Requirements Specific to the Belgian Healthcare System

- **Multiple prescription issuance detection capability (D1).** When filling a prescription, the patient reveals information that will allow the MPA to recover his pseudonym (cf. step II-(d-iv)). Because multiple prescriptions issued to the same patient are linked to each other through the patient's pseudonym, oversight organizations such as the RIZIV or IFEB are able to detect abusive behaviour and stop malicious patients.
- **Single prescription spending (D2).** Follows from the fact that prescriptions are uniquely identified by a *PrescID*, and resistant to tampering.
- **Prescription non-transferability (D3).** This Follows from the soundness of the signed proofs of knowledge in step II-e of the protocol. The patient proves to the pharmacist that the nym in the prescription corresponds to the nym in its *PtCred*.
- **Prescription fraud detection capability (D4).** This can only be detected by the RIZIV by searching for abnormal behaviour in the IFEB database. The IFEB database contains only doctor pseudonyms, which can be linked to doctors' real identities with the help of an authority such as the "college of physicians".
- **Correct pharmacist reimbursement (D5).** For each prescription, the patient generates a *reception_ack*, which is a patient confirmation of provided services by the pharmacist. This proof is verified and stored by the pharmacist, MPA and HII. If something goes wrong, this proof can be used as evidence.
- **Payment fraud detection capability (D6).** The reception acknowledgement *reception_ack* issued by the patient guarantees to the HII that the patient has indeed received the medicine.
- **Correct statistics (D7).** The IFEB needs to rely on the trustworthiness of the MPAs to make sure it receives correct statistics. The latter property cannot be enforced by cryptographic means alone, since a malicious MPA could just ignore half of the transactions it has recorded. For better assurances, oversight organizations (e.g., RIZIV) in practice request random

sample data from health insurance institutes (HIIs) and cross-check them against data returned by the MPAs. A malicious MPA who fails to return consistent data, or returns incomplete data, will be further investigated and may have its licence revoked.

### 7.3 Privacy

- **Minimum disclosure (P1).** Owing to the selective disclosure feature offered by the zero knowledge proofs of knowledge, the security of the commitment and verifiable encryption schemes, the protocol of section 6 satisfies the access control requirements of table 1. This can be easily verified by simple examination of the protocol. Due to space limitation we leave the more formal proof of this property to the full version of the paper.
- **Patient unlinkability (P2).** Prescriptions are tied to the patient's pseudonym *PtNym* which can be recovered only by the MPA processing the prescription and the patient's health insurer (PtHII). All other parties have no access to the patient's identity or pseudonym, and thus cannot link any two prescriptions of the same patient. In the case of a treating doctor, the patient may freely decide to disclose his pseudonym to allow the linkability.
- **Patient untraceability (P3).** An examination of the protocol of section 6 shows that the identity of the patient is accessible only to the patient's HII who knows the correspondence between *PtNym* and *PtID*. In case of apparent abuse, the RIZIV may also have access to the patient's identity by filing a complaint with the judicial authorities who can subpoena the HII to deanonymize the fraudulent patient.
- **Absence of provable doctor's prescription behaviour (P4).** The protocol is designed in such a way that the real identity of a doctor is never associated with the prescriptions' content. The only exception occurs when the pharmacist sees a prescription anomaly (e.g. lethal dosage), in which case he asks the patient to name the doctor. This information however is not a reproducible proof, and thus cannot be used to convince a bribe-giver.

## 8 Concluding Remarks

The paper presents a privacy-preserving protocol for the Belgian healthcare system. The proposed protocol protects patients' privacy throughout the prescription handling process, while complying with the current Belgian practise. Despite the large number of parties involved, and the complexity of the application, the protocol we present minimizes information disclosure and satisfies the access control requirements of table 1. Furthermore, our protocol is equipped with a set of abuse detection and evidence gathering mechanisms that allow oversight authorities to solve instances of fraud and ensure accountability. In addition to protecting patients' privacy, our protocol provides a mechanism to prevent the intrusive monitoring of doctors' prescription patterns. The ability of third party players to determine the prescription patterns of a given doctor is often considered an undesirable aspect in healthcare, since it can be used by malicious

pharmaceutical companies for example, (1) as a coercive tool against doctors who do not prescribe their products, or (2) as an instrument to facilitate bribery and kick-backs with doctors who do the opposite (cf., [3,2].) In our protocol, doctors are only pseudonymously identified to allow the legitimate gathering of statistical data about medicine consumption and its effect on the population. The real identity of the doctors is unveiled only in case of apparent abuse via a judicial procedure.

The design we propose in this paper is highly modular and can be adapted to other healthcare systems comparable to the Belgian one. For example, if we consider a jurisdiction where the real identity of the doctor (as opposed to his pseudonym) has to be indicated in plaintext in all transcripts generated during the prescription lifecycle, then one can easily adapt our protocol to the new setting by replacing the *DrNym* attribute in the authentication step of phase I, with the *DrID* attribute already embedded in the doctor's credential. The rest of the protocol can be easily modified accordingly.

Further improvements can be made to our protocol. For example one could strengthen access control to health records stored on remote databases by enforcing privacy policies defined by the patients. Another worthy avenue for future work would be to simplify the prescription workflow and reduce interactions (to the extent acceptable by the healthcare procedures and practices in place).

**Acknowledgments.** This research is a contribution to the European PRIME project and is partially funded by the Interuniversity Attraction Poles Programme Belgian State, Belgian Science Policy, the Research Fund K.U.Leuven and the IWT-SBO project (ADAPID) "Advanced Applications for Electronic Identity Cards in Flanders". The second author was previously funded by the Universitary Mission of Tunisia in North America.

## References

1. Ateniese, G., de Medeiros, B.: Anonymous e-prescriptions. In: Jajodia, S., Samarati, P. (eds.) WPES, pp. 19–31. ACM, New York (2002)
2. Biovail faces heart drug kickback inquiry. Pharma Marketletter (September 1, 2003), `http://goliath.ecnext.com/coms2/summary_0199-3378487_ITM`.
3. Grand jury probes biovail over sales practices. The Toronto Star (Feburary 1,2008), `http://www.thestar.com/Business/article/299682`
4. Bellovin, S.M., Merritt, M.: Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. In: ACM Conference on Computer and Communications Security, pp. 244–250 (1993)
5. Brands, S.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. The MIT Press, Cambridge (2000)
6. Camenisch, J., Lysyanskaya, A.: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
7. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)

8. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)
9. Demuynck, L., De Decker, B.: Privacy-preserving electronic health records. In: Dittmann, J., Katzenbeisser, S., Uhl, A. (eds.) CMS 2005. LNCS, vol. 3677, pp. 150–159. Springer, Heidelberg (2005)
10. Damgård, I., Fujisaki, E.: A statistically-hiding integer commitment scheme based on groups with hidden order. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 125–142. Springer, Heidelberg (2002)
11. Gong, L., Lomas, T.M.A., Needham, R.M., Saltzer, J.H.: Protecting poorly chosen secrets from guessing attacks. IEEE Journal on Selected Areas in Communications 11(5), 648–656 (1993)
12. Health level 7 (hl7), `http://www.hl7.org/`
13. Hl7 reference information model, `http://www.hl7.org/library/data-model/RIM/modelpage_non.htm`
14. Integrating the healthcare enterprise, `http://www.ihe.net/`
15. ITU-T. Public-key and attribute certificate frameworks – X.509 Recommendation (2005), `http://www.itu.int/rec/T-REC-X.509/en`
16. Krummenacher, R., Simperl, E.P.B., Nixon, L.J.B., Cerizza, D., Della Valle, E.: Enabling the european patient summary through triplespaces. In: CBMS, pp. 319–324. IEEE Computer Society, Los Alamitos (2007)
17. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992)
18. Tavena, S., Palanque, P., Basnyat, S., Winckler, M.A., Law, E.: Clinical application design: Task modeling with failure in mind. In: World Congress on Internet in Medicine (MedNet), Toronto, Canada (2006)
19. Della Valle, E., Gadda, L., Perdoni, V.: COCOON: Building knowledge driven and dynamically networked communities within european healthcare systems (April 06, 2005)
20. Yang, Y., Deng, R.H., Bao, F.: Fortifying password authentication in integrated healthcare delivery systems. In: ASIACCS 2006: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pp. 255–265. ACM, New York (2006)
21. Yang, Y., Han, X., Bao, F., Deng, R.H.: A smart-card-enabled privacy preserving e-prescription system. IEEE Transactions on Information Technology in Biomedicine 8(1), 47–58 (2004)