Advanced Applications for e-ID Cards in Flanders

ADAPID Deliverable D6

E-Health I

B. De Decker, H. Dekeyser, M. Layouni, K. Verslype, and H. Vangheluwe

September 2007

Executive Summary

The protection of personal health information is central to the privacy of citizens. This report describes our work in the area of privacy-preserving electronic healthcare. We present a design for an ehealth system using the Belgian eID card. The system we present focuses on the issuance and handling of medical prescriptions and takes into account the roles of each player in the current Belgian healthcare system.

In addition to being highly compatible with the current health practice in Belgium, our system tries to maximize the protection of the identity and health records of the patients as long as they do not engage in a fraudulent behavior. Furthermore, our system can be optionally parametrized to increase the doctors' privacy (e.g., by hiding their identity, and their prescription habits.) Since, in practice, an e-health transaction is a multiparty procedure, we make sure that each party involved learns only the information it is supposed to have access to. To achieve this we adopt a conservative access control policy, and put in measures to block any data leakage that may result from possible inference channels.

Our design is based on cryptographic primitives such as anonymous credentials, verifiable encryption, and public key certificates. In case of abusive behavior, the system we propose provides a way to provably unveil the identity of the offenders, along with an evidence trail.

Contents

1 Introduction

Healthcare represents one of the main pillars of a strong public service in a society. Over the years, countries around the world have come up with a multitude of ways to improve the quality of their healthcare service. One particular trend however can be noted: there is an increasing number of jurisdictions who choose to use information technologies, and move from the traditional paper-based healthcare system to an electronic one. This should come as a no surprise since electronic healthcare offers a variety of features. In the following we enumerate some of them:

1. easiness and rapidity of access to health data
2. higher cost-efficiency: because it's mostly a paper-less process, less resources are spent on management, and more is allocated to providing services to patients.
3. less medical errors: because data is more easily searchable, and accessible, healthcare professionals have less chance of missing crucial data of the health history of patients, which lessens their chance of making mistakes.
4. versatility: health information can be better exploited, in a more timely fashion (e.g., vital knowledge about a possible disease outbreak can be detected in a timely fashion, thereby allowing the medical authorities to take the required measures to stop its spread)
5. better fraud detection mechanisms: information technology provides more efficient ways to detect fraud (e.g., inaccurate medical cost claims), and questionable or inappropriate prescription behavior on the part of doctors (e.g., doctors receiving kick-backs from pharmaceutical companies to prescribe their products.)
6. increasing easiness of detecting and evaluating global health trends in the population (e.g., obesity, diabetes, HIV rates)
7. shorter refund delays for patients who receive coverage from health insurance organizations.

Despite all the above features, an ehealth system can still become a serious threat to the patients' privacy if no proper measures are taken. In the following we list a number of widely spread practices that need to be avoided if a secure privacy-preserving healthcare system is to be built.

Anatomy of naïve ehealth system.

- huge health record databases without proper access control
- electronic health records accessed without the knowledge and consent of the patient

- sensitive information about the patient's history (e.g., consumed medicine, visited doctors, illnesses) finding their way to the public domain
- information about a law-abiding doctor's prescription behavior can be regarded as sensitive.

A naïve ehealth system such as the one above may result into a series of negative repercussions.

Consequences of a naïve ehealth system:

- Unlawful disclosure of personal health information
- Discrimination and profiling practices based on a person's health condition
- In presence of an ehealth system that does not preserve privacy, patients mistrust the system, and will be reluctant to use it. As a result, patients will consult less, and the average health of the population will decrease.

CONTRIBUTION. In this report, we design an electronic health system using the Belgian e-ID card. The system we propose provides solutions to the problems addressed above. In addition to being highly compatible with the current health practice in Belgium, our system protects the identity and health records of the patients as long as they do not engage in a fraudulent behavior. Furthermore, our system can be optionally parametrized to protect the privacy of the doctors (e.g., by hiding their identity, and their prescription habits.) Since, in practice, an e-health transaction is a multiparty procedure, we make sure that each party involved learns only the information it is supposed to have access to. To achieve this we adopt a conservative access control policy, and put in measures to block any data leakage that may result from possible inference channels.

Our design is based on cryptographic primitives such as anonymous credentials, verifiable encryption, and public key certificates. In case of abusive behavior, the system we propose provides a way to provably unveil the identity of the offenders, along with an evidence trail.

In the system we propose, the eID card is used to store the digital credentials of patients and doctors. Future versions of the eID card with higher computational power can be used to perform more elaborate cryptographic operations and identity proofs.

ORGANIZATION. The remainder of this report is organized as follows. First we start with a list of related work in Section 2. In Section 3, we give a real world description of the parties involved in the current Belgian eHealth system, and their respective roles. Section 4 discusses the set of requirements a viable ehealth system needs to achieve. Section 5 introduces the main cryptographic building blocks used in our system. Section 6 presents a naïve approach one

needs to avoid when designing an ehealth system. In Section 7 we describe our solution for a viable ehealth system, and show how it achieves the previously defined requirements. In Section 8 we highlight our progress in implementing a prototype of the protocol proposed in Section 7. Section 9 provides an overview of the legal aspects surrounding our ehealth application. Finally in Section 10, we conclude and discuss ways to add more functionalities to our system.

2 Related Work

Most work available in the literature focuses mainly on migrating health services from the paper-based setting to the electronic setting. A great deal of work has been allocated for instance to features such as semantic web and interoperability between various health organizations [19, 20, 22, 37]. Other issues have been addressed as well, such as reliability, accessibility, availability, storage integrity, and fault-tolerance [27, 35, 36]. The issue of privacy has been considered but in a very modest way. For instance, [40] proposes a role-based access control system to and applies to a healthcare context. While interesting in itself, the work in [40] cannot be considered privacy-preserving as it is based on traditional public-key, and attribute, certificates which have no means to hide the identity of their holders.

This is in contrast to our work where the goal to let the patient (and the Doctor if required) be in control of disclosing any information about his identity, and health condition. There are few works, e.g., [9, 3], in the literature however with similar goals to ours. Although the work in [9, 3] is related to ours, it does not address the the specific context of electronic healthcare. Unlike other contexts such as ecommerce, an ehealth transaction involves, in addition to the patient and doctor, a multitude of parties (e.g., pharmacist, insurer, public safety organizations etc). The presence of all these parties in the system makes it a lot harder to design protocols satisfying privacy requirements.

Another area of research dealing with privacy in electronic health is that of privacy preserving data-mining [39, 11, 26, 2] and data anonymization [34, 33]. The latter results can be used as complementary measures in our context, as they deal primarily with the management of data after it has been collected. In our work we first focus on the release of data by the patient, and provide ways to control that disclosure.

3 Real World Description

This section describes the different relevant roles in the Belgian social security system and the most common real world scenario; i.e. the issuing and processing of a prescription. This section describes the real-life scenario which is not ideal w.r.t. privacy. Current practice is for the major part historically grown.

3.1 Roles

The different roles are the patient, the doctor, the pharmacist, the MPA, the HII, the IFEB and the RIZIV.

3.1.1 Patient.

The patient pays the standard fee for a doctor's consultation to the doctor. However, the better part can be recovered by submitting the reimbursement statements he received from the doctor to his HII (Health Insurance Institute, see below). The prescription is evidently given to the pharmacist. Also, the SIS card (see below) is shown to the pharmacist, such that the pharmacist is convinced that the patient is member of a HII and such that the pharmacist knows the social security status (widow, orphan, person on welfare, ...) of the patient. This social status will determine the amount of money the patient has to pay for the prescribed medicines.

3.1.2 Doctor.

The doctor issues prescriptions and reimbursement statements to patients. The doctor has a personal health record archive and has some doctor's accreditation, which is often visible on the wall of the doctor's practice.

3.1.3 Pharmacist.

The pharmacist provides medicines to the patient (or a delegate) after having received the prescription and money (dependent on the social security status of the patient) and after having read and verified the info in the SIS card. The prescriptions are sent to the pharmacist's MPA.

3.1.4 MPA.

MPA (Medical Prescription Administration, 'tariferingsdienst' in Dutch) receives prescriptions from the pharmacists subscribed to that MPA, sorts these by HII (see below), generates invoices that are sent to the HII. After having received the payments from the HII, the MPA pays back the pharmacists. The MPA also provides two types of statistics to the IFEB (see below): 1) drug consumption per patient category (i.e. social security status) and per drug category and 2) the prescription behavior of the doctors. Multiple MPAs exist in Belgium (Kovag, APB, ...); in 2004, there where 32 registered MPAs.

3.1.5 HII.

Each Belgian citizen is obliged to have a medical insurance by one of the 60 HIIs (Health Insurance Institutes, 'ziekenfondsen' in Dutch) in Belgium. The HII is responsible for paying back the bigger part of the amount the patient payed the doctor for a consultation. The patient only pays a minor part of the

prescribed medicines. The HII is responsible for paying back the pharmacist (via the MPA). Therefore, it receives invoices from the MPA. The HII can request the MPA for prescription samples.

The HII keeps for each member track of the amount of money the member already spent on healthcare. If this amount exceeds a legally determined maximum, the HII has to intervene. A Belgian citizen registered to a HII will thus not have to pay more than this maximum amount by him/herself.

In general, the HIIs are historically grown within some political ideology, as a consequence of the Belgian Pillarisation. Still, most current HIIs have ties with some ideology/pillar (christian democracy, social-democracy, liberals and Flemish nationalists). A small minority of the HIIs claims to be politically neutral.

3.1.6 IFEB

IFEB ('Instituut voor farmaco-epidemiologie van België' in Dutch) gathers statistical data from the MPA, merges and interprets them. The IFEB also checks whether substitution drugs such as methadone are prescribed by multiple doctor's to the same person, even if that person is not subscribed to a HII (e.g. non-Belgians).

3.1.7 RIZIV.

The RIZIV ('Rijksinstituut voor Ziekte- en Invaliditeitsverzekering' in Dutch) pays the patient and pharmacist via the patient's HII. It is also able to do checks on samples of prescription which it can request from the MPAs. The RIZIV has direct access to the IFEB database.

3.2 Objects

The different roles all need a kind of accreditation; the patient has a SIS card (see below) and an identity card, the doctor has a doctor's accreditation, the pharmacist has a pharmacist's accreditation, but also the HIIs, MPAs, IFEB and RIZIV will need accreditations in some way.

The *SIS* ('Sociaal InformatieSysteem' in Dutch) *card* is a smart card issued by the HIIs to their members and serves to authenticate citizens for social security issues. It thus serves as a social security credential. It contains the owner's name, date of birth, gender, and social security number, social security status, health insurance institute (HII), HII member number and information about the owner's health insurance. The SIS card is shown to the pharmacist, in hospitals, etc. It also contains an issuance and expiry date. It is the intention of the Belgian government to include the functionality of the SIS card in future eID cards.

Other objects are the prescriptions, reimbursement statements and invoices. The *prescription*, contains at least the patient's id, the prescribing doctor's id, the prescribed medicines, prescription date. The *reimbursement statement*

contains at least the ids of the patient and the consulted doctor, the consultation date and one or more codes associated with the type of given medical treatments. The *invoices* sent by the MPA to the HII contain at least the ids of the MPA and the patient, the amount of money paid by the patient to the pharmacist and the date.

3.3 Real World scenario

In this section, two common real world scenarios are discussed: prescription handling and health record access. The focus is on the former scenario.

3.3.1 Prescription Handling.

Three tables are shown to illustrate the real-life scenario of how prescriptions are issued, used and further processed.

Table 1 shows the interactions of the patient with the doctor and pharmacist. First, the patient visits a doctor (e.g. his/her general practitioner). The doctor proves to the patient that he is an accredited doctor by showing his doctor's accreditation (1). In real life, this accreditation is often done in a more implicit, passive way, e.g. by hanging the doctor's diploma on the wall. The patient will usually identify himself to the doctor as well (2). In practice, this is not done if the doctor already knows the patient. The doctor then accesses the health records and examines the patient. Thereafter, the doctor can add a health record. We refer to the next section for the health record handling. Then, the doctor issues a reimbursement statement and if necessary a prescription (3).

When the patient visits the pharmacist, he is convinced of the pharmacist's accreditation (4). this happens mostly implicitly; e.g. by seeing the pharmacist logo. The prescription is shown by the patient to the pharmacist, together with his SIS card (5). The latter is required to convince the pharmacist that the patient is subscribed to a HII (and that the pharmacist will thus get refunded) and of the patient's social security status. After having checked the stock whether the prescribed drugs are immediately available, the pharmacist receives the prescription and a limited amount of money from the patient, and in return the patient receives the drugs (6). The amount of money that the patient has to pay depends on his social security status.

As shown in table 2, after mutual authentication (1), the pharmacist sends in batch all the prescriptions he received to his MPA in order to get refunded. The MPA checks whether the prescriptions are correct (3) and sends an invoice to the different HIIs (5), again preceded by mutual authentication (4). These invoices are per patient, such that the HII can update the patient's account (7). The HII pays the invoice to the MPA (6) and the MPA in turn pays the pharmacists (8). The HII keeps track of how much each patient already had to pay. If this amount is too high, the patient will be issued a tax refund statement, enabling him to get the money back in the form of a tax reduction.

One of the tasks of the MPA is generating anonymized/pseudonymized statistics and sending these to the IFEB as shown in table 3. This data is

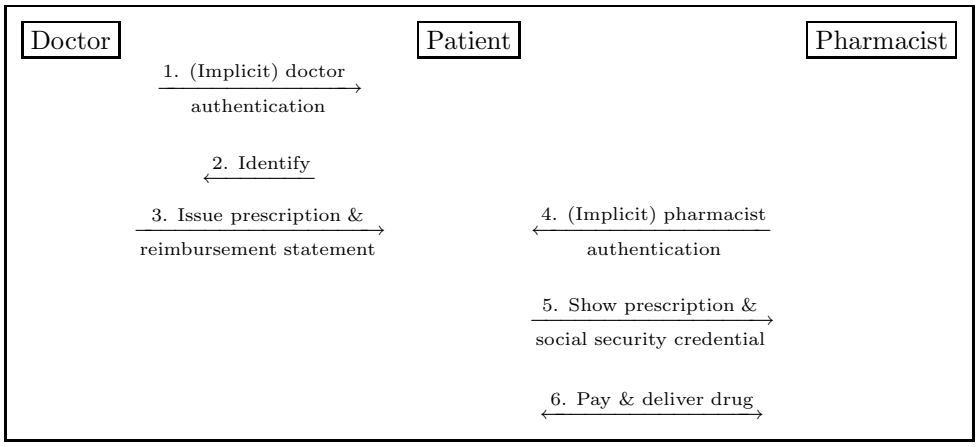

Table 1: Patient interactions with doctor and pharmacist

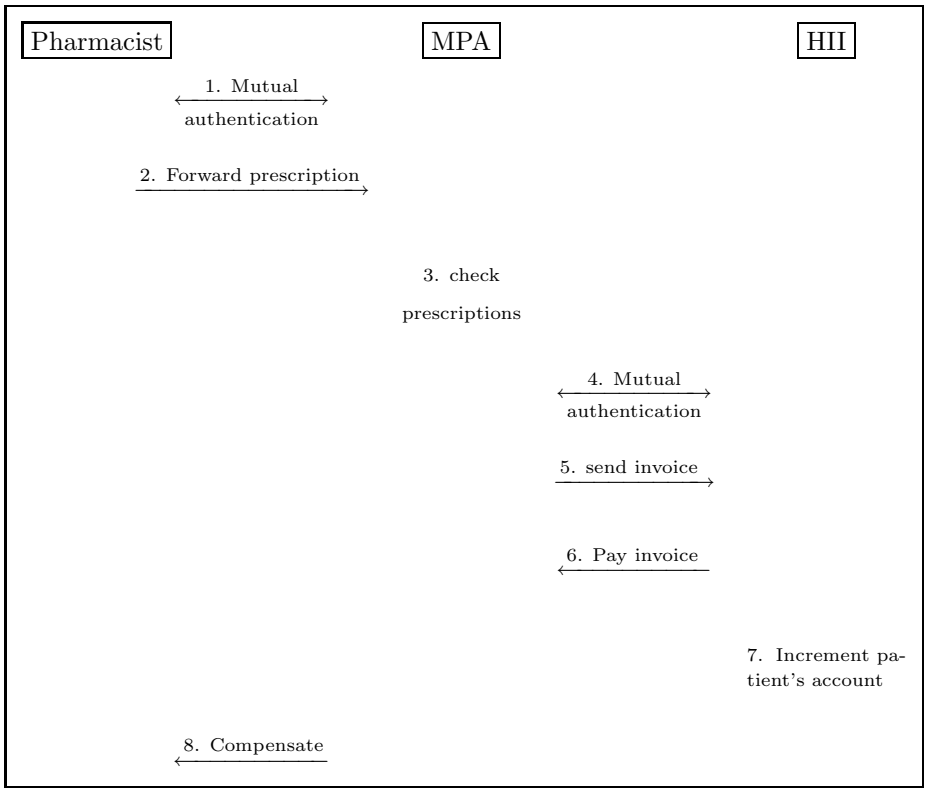

Table 2: Pharmacist 'backend' prescription handling.

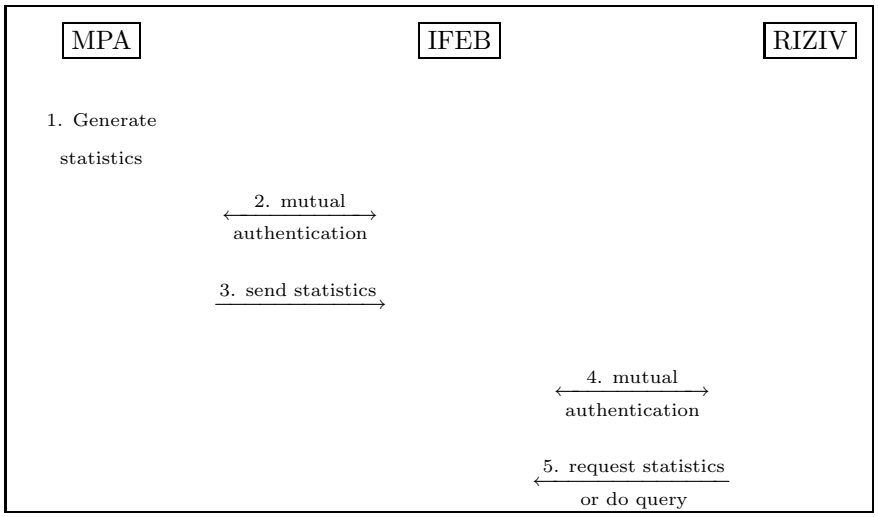

Table 3: Statistics generation and queries for statistics

merged by the IFEB and can be directly accessed by the RIZIV. First, the statistical data are generated by the MPA (1). These are sent to the IFEB (3) after mutual authentication (2). The RIZIV has direct access to the statistics centralized and merged by the IFEB and can thus query it (5), again after mutual authentication (4).

The patient is not always able to get the medicines from the pharmacist himself. This can be easily solved by giving the prescription and the SIS card (social security credential) to e.g. a relative as no pin code is required to use the SIS card.

3.4 Access to Health Records

In current health practice, each doctor keeps his own file with health records of his patients. This has serious drawbacks as none of the doctors the patient visited has a complete overview of the patient's health records. Therefore, another approach where each doctor uploads the patient's health record in an integrity protected, encrypted and anonymized way is proposed, such that the central EHR (Electronic Health Record) server cannot exctract or change any information. The doctor can only access the patient's EHRs after being granted authorization by the patient. Evidently, in case of an emergency, the emergency doctor is given the possibility to immediately access the EHRs of that patient. A system with similar functionalities is given in [15].

4 Requirements

We sum up the functional, privacy, security and other requirements derived from the prescription handling and health record handling description. We refer to Deliverable 2: Requirements where an informal overview of the e-health requirements is given. Also a list of possible disputes that must be prevented or at least solvable is given.

4.1 Functional Requirements

We refer to the description of the scenarios in the previous section for the functional requirements. The described interaction diagrams still have to be possible. However, some requirements need special consideration.

- **Prescription delegation.** If the patient is too sick, someone else must be able to go to the pharmacist with that prescription. Delegation must be possible in a flexible way, which means that the possible delegates must not be known beforehand, e.g. at the moment the prescription is issued.
- **Ubiquitous prescription issuance.** The doctor must be able to issue prescriptions wherever he is physically located at the moment of prescribing: at his office, in a patient's house, in a hospital, etc. We cannot require that there is an Internet connection everywhere. The use of the GSM (mobile phone) network can be an option, however, still 100% geographical coverage and 100% uptime cannot be guaranteed.
- **Sample check.** Both HII and RIZIV must be able to do checks on prescription samples that can be requested to the MPA.

4.2 Privacy Requirements

In table 4, an overview is given of what parties need to know what information in order to do their job accordingly. The matrix is derived from the real life scenarios in the previous section. If each party does not get more data as indicated in the matrix, the maximum level of privacy is achieved. Entities not mentioned in the table must not know anything of the e-health data.

Table 4: Health-Data Access Control Matrix

Party \ Data	Patient ID	EHR data	Prescription data	Treating Dr. ID	Treating Pharmacist ID	Corresponding MPA ID	Corresponding HII ID
Patient	✓	✓ (Read only)	✓	✓	✓	Not needed	✓
Doctor	✓ (optional: pseudony-mously)	✓ (after patient's authorization)	✓	✓	No	No	No
EHR Server	No	No	No	Proof doctor's accreditation	No	No	No
Pharmacist	Patient's social security status	No	✓	Only in case of anomalies	✓	✓	Valid patient subscription to a HII
Pharmacist's MPA	Patient's social security status	No	✓	Pseudonym	✓	✓	✓
Patient's HII	✓	No	No Only price for patient	No	No	✓	✓
IFEB	Pseudonym	No	No Only statistics	Pseudonym	No, Only region	No	No

Some explanation is given about the less trivial cells in the matrix. The *patient* does not need to know the MPA to which the pharmacist is connected. The *doctor* will in most cases know the identity of the patient. However, in some cases, the patient will choose to remain anonymous. Still, the doctor will need access to the EHRs of that patient, and still the RIZIV must be able to link anonymous visits of the same patient to different doctors and to deanonymize the patient in case abuse is detected. The doctor also does not need to know neither the pharmacist where the medicines will be bought, nor the pharmacist's MPA or patient's HII.

The lesser info the *EHR Server* knows, the better it is. It only needs to be ensured that the party requesting an EHR is indeed an accredited doctor who is authorized to access the patients's EHRs.

The *pharmacist* does not need to know the identity of the doctor who issued the prescription. However, in case the prescription looks very strange (e.g. a potential lethal dose has been prescribed), the pharmacist might want to contact the prescribing doctor. As an alternative, the patient could be asked to verify the prescription with his doctor.

The *MPA* needs the patient's social security status in order to generate the statistics for the IFEB. To generate the statistics, it does not need the patient's id, but at least some patient pseudonym is required therefore. These different patient pseudonyms must be linkable by the IFEB in order to merge the statistics. The RIZIV must be able to deanonymize these in case of abuse.

The *HII* does not need the prescription data, but only some financial data in order to be able to repay the different instances. It is still able to request prescription samples from the MPA.

The *IFEB* does not need the MPA ids of the submitted statistical data, it only needs to be convinced that the data originates from a valid MPA. The region of the pharmacist can also be useful for the statistics. The IFEB keeps per-doctor statistics, however, it does not need to know the identity of that doctor; a unique per-doctor pseudonym that can be deanonymized by the RIZIV if necessary suffices. The same is true for the patient id.

A special privacy requirement is that ideally neither the pharmacist, nor the MPA should be able to detect whether a prescription is delegated or not. However, if abuse is detected, it must be possible to know whether the patient or delegate was involved in the abuse.

4.3 Security Requirements

- **Entity authentication.** All parties need to be able to authenticate themselves. This means that they either have to be able to identify themselves or have to show properties about themselves (e.g. 'I am an accredited doctor'). This will depend on the privacy requirements.

- **Item integrity.** Prescriptions, EHRs, invoices and their derivatives have to be integrity protected to prevent tampering (e.g. by patient or EHR

server). All parties involved in the processing of an item must be able to check the integrity.

- **Confidentiality.** An overview of what entity may be given access to what data is given in table 4 in the 'EHR' data and 'prescription data' column. The invoices sent by the MPAs to the HIIs may only be accessed by the HIIs.
- **Token revocability.** It must be possible to revoke tokens such as prescriptions, invoices, and credentials, for instance, when the corresponding secret key has been exposed.

4.4 Other Requirements

- **Adaptability.** Legislation will change and entities involved in the interactions described in the previous section will be given new tasks by the government; tasks will change or will be granted to other entities. New entities can be introduced or can disappear, etc. Therefore, it is important to make the anonymity preserving protocols easily adaptable.
- **Efficiency.** The protocol must be executable in a acceptable timespan: e.g. showing a prescription to a pharmacist must not last several minutes.

4.5 Dispute handling

Because not all abuse can be prevented, at least it must be detectable and provable.

- **Single prescription issuance (D1).** The patient must not be able to go to multiple doctors to get multiple prescriptions for the same disease. This must absolutely be detected. The prescription thus must contain the user's identity in some way such that this practice is detectable by the RIZIV.
- **Single prescription spending (D2).** A prescription must only be usable once. A patient must not be able to use the same prescription multiple times (e.g. by going to different pharmacists).
- **Prescription - Social Security Status Linking (D3).** Both the pharmacist and MPA must be able to verify whether the shown social security status and the prescription are linked to the same person.
- **Fraudulent doctor behaviour (D4).** The doctor can in principle deliberately issue prescriptions to people who do not need the prescribed medicines. Similarly, the doctor can issue fraudulent medical certificates
- **Prescription theft (D5).** It must not be possible to steal a prescription. This means that someone else who could get hold of the prescription must not be able to use it.

- **Correct processing of prescription (D6).** If a pharmacist doesn't get refunded by the MPA, it must be able to proof that it received insufficient money. It can be the MPA, HII or RIZIV who made a fault. The MPA could for instance sent wrong or incomplete invoices to the HII. These faults must be detectable and provable.
- **Correct statistics (D7).** The IFEB must be ensured that it receives correct statistics.
- **Pharmacist misbehaviour (D8).** The pharmacist must not be able to use a cost statement twice or to get compensated for all the prescribed medicines on one prescription, while only a part of the medicines have effectively been delivered.

5 Building blocks

Classical building blocks are digital signatures [32, 29, 10], symmetric [30, 13] and asymmetric [32, 17] encryptions, cryptographic hash functions [23] and X.509 certificates [24, 25, 21]. Also, some less commonly known techniques will be used in this deliverable: commitments, anonymous credentials and verifiable encryption.

5.1 Commitments.

A commitment [31, 14] can be seen as the digital analogue of a "non-transparent sealed envelope" [18]. It enables a committer to hide a set of attributes (non-transparency property), while at the same time preventing her from changing these values after commitment (sealed property). The primitive

$$E : \mathit{Comm}, \mathit{OpenInfo} = \mathit{Comm}(\{\texttt{attrName} := \mathit{attrValue}, \ldots\})$$

enables an entity E to create a commitment *Comm* to a set of attributes. Additionally, she retrieves a secret key *OpenInfo* containing, among others, the attributes encoded into *Comm*. This key can be used to prove properties concerning the attributes.

$$E_1 \rightarrow E_2 : \mathit{CommProps}(\mathit{Comm}, P(\texttt{attr1}, \ldots))$$

The public input to this protocol is both a commitment *Comm* and a boolean predicate P concerning *Comm*'s attributes. If E_2 accepts, she is convinced that E_1 knows the *OpenInfo* belonging to *Comm*, and that *Comm*'s attributes satisfy predicate P. She does not find out any other information about *Comm* and its attributes.

The *CommProps* protocol is an interactive protocol. Nevertheless, we adopt the one-headed arrow $E_1 \rightarrow E_2$ in our notation. This is to avoid any ambiguity that may result from our traditional (double-headed) arrow notation. Intuitively, the one-headed arrow makes clear that it is E_1 who proves commitment properties to E_2, and not the other way around.

5.2 Credentials

Anonymous credentials allow for anonymous yet accountable transactions between users and organizations. In this section, a simplified version of the Idemix anonymous credential system [4, 5] is presented and extended with a new protocol for credential updating. The protocols are used as basic building blocks in our system. They typically run over an anonymous communication channel.

RegNym Protocols. An individual can establish multiple non-transferable pseudonyms (i.e. nyms) with the same organization. Two registration protocols are discussed:

- $U \leftrightarrow O : (Nym_{UO}, Sig_{UO}) = RegSignedNym(Cert_{UA})$. During the signed nym registration protocol, the user signs the established Nym_{UO} with his signature key, which is certified through an external certificate (which links the user's public key with his identity). Hence, the organization holds a provable link between the nym and the identity certified by the certificate.
- $U \leftrightarrow O : Nym_{UO} = RegNym()$. The (ordinary) Nym Registration protocol is used to register a regular nym between a user U and an organization O.

ProofNymPossession Protocol. $U \leftrightarrow O : ProofNymPossession(Nym_{UO})$. A user U can prove to an organization O to be the owner of a nym Nym_{UO}.

Issue Protocol. $U \leftrightarrow I : Cred_{UI} = IssueCred(Nym_{UI}, sl, \{attr1 = G(.), ...\}, ...)$. An issuer I can issue a credential $Cred_{UI}$ to a nym Nym_{UI}. The retrieved credential is known only to the user and cannot be shared. During the issue protocol, the showlimit sl of the credential is set to be either a constant k or unlimited. Also, a number of attributes is embedded into the credential. $Cred_{UI}$ contains a secret key for showing it to a verifier.

Each attribute is constructed as a separate function $G(.)$ of public values and attributes encoded into previously shown credentials or commitments. As an example, $\texttt{attr}_1$ may be constructed as $\texttt{attr}_1 := Cred_x.\texttt{a}_1 + 5$, where $Cred_x.\texttt{a}_1$ refers to attribute $\texttt{a}_1$ of a previously shown credential $Cred_x$. I cannot find out any information concerning the credential's final attributes, apart from the fact that they are constructed correctly based on $G(.)$.

Show Protocol. $U \leftrightarrow V : Transcript_{UV} = ShowCred(Cred_{UI}, [Nym_{UV}], [DeanCond], [AttrProperties], [Msg])$. A user U proves to a verifier V that he is in possession of a valid credential $Cred_{UI}$. This action results in a transcript for the verifier. During the protocol, several options may be enabled. The user may show his credential with respect to a pseudonym Nym_{UV} , by which he is known to V . This provably links the transcript and the nym. In addition, the resulting transcript may be deanonymizable: upon fulfillment of a condition $DeanCond$, a trusted deanonymizer is allowed to recover the nym on which the

credential was issued. Moreover, the user may disclose some information about the attributes encoded into the credential. He may reveal either an attribute or a property of the attribute, and may decide to sign a message Msg with his credential; creating a provable link between the transcript and the message. Note that different transcripts for the same credential cannot be linked (unless the value of a unique attribute is proved), nor can they be linked to the credentials issue protocol.

U can reveal a boolean predicate P concerning public values, attributes occurring in *Cred* and attributes occurring in previously shown credentials or commitments. For example, P may be the predicate $(\mathtt{attr}_1 > C_x.\mathtt{a}_1 \wedge \mathtt{attr}_1 < C_x.\mathtt{a}_2)$, where $C_x.\mathtt{a}_1$ and $C_x.\mathtt{a}_2$ refer to attributes $\mathtt{a}_1$ and $\mathtt{a}_2$ encoded into a previously shown commitment C_x. V cannot learn any new information from the execution of the protocol, apart from the fact that U has a valid credential which is issued by I and of which the attributes satisfy P.

An eavesdropper listening in on the execution of either a *CredGet* or a *CredShow* protocol, cannot find out any other information than what can be deduced by the organization involved in the protocol. Hence, as long as the interaction is performed over an anonymous communication channel and as long as no confidential information is communicated between the parties, no confidentiality protection is needed on the communication lines.

Local Deanonymization Protocol.
$D : (Nym_{UI}, DeAnProof) = DeanonLocal(Transcript_{UV})$. If a credential show is deanonymizable, the pseudonym NymUI on which the credential was issued can be revealed by a trusted deano- nymizer D. DeAnProof proofs the link between the transcript and the nym. D is only allowed to perform the deanonymization when DeanCond is met.

Delegation of credentials has been examined in [16]. Three methods where described: 'transferable credentials', 'signed warrants' and 'new credentials' A transferable credential is a credential that can be used by a predetermined set of users, who have to be involved in a preparatory phase?. Thus, the complexity raises with the number of delegates.

In principle, it should be possible to combine transferable credentials with DRM (Digital Rights Management).

5.3 Verifiable encryptions.

Verifiable encryptions [1, 6, 8] have all the characteristics of regular encryptions. Additionally, they enable their creator U to demonstrate properties of the encrypted plaintext

Verifiable encryption is denoted as $P \rightarrow V : c \leftarrow Venc(x; props, PK)$ where plaintext x is private input given by P and *props* and PK is known by both P and V. This protocol results in a ciphertext c of plaintext x using key PK. If

V accepts, it knows c and it is convinced that x, i.e. the decryption of c, has properties *props*. As an example, P can prove to E that the encrypted plaintext is encoded as an attribute in a credential or commitment.

A verifiable encryption is an interactive protocol between a prover P and verifier V, but can be adapted such that it is non-interactive: V generates a proof that is, potentially at a later moment, sent to and verified by P. This can be denoted as $P : c \leftarrow genNIVenc(x, props, PK)$. Verification of such a non-interactive verifiable encryption is denoted as $V : true/false \leftarrow verifyNIVenc(c, props, PK)$.

Non-interactive verifiable encryptions can be verified by multiple parties at every moment, while interactive verifiable encryptions can only be verified by one party (the verifier) at the moment the verifiable encryption protocol is run.

6 Naive Solution Using Well Established Building Blocks.

In this section, an overview is given of how the real life prescription processing scenario in section 3 can be digitalized using classical, well established cryptographic building blocks such as digital signatures, secure hash functions, certificates, etc. This protocol is an almost literal translation of the real life scenario described in section 2. The advantage is that it is easy to implement and very feasible. The disadvantage is that the level of privacy for each of the entities is zero or at least very low.

6.1 Protocol

First of all, each entity is issued a classical X.509 certificate by some trusted certification authority (CA) in order to *authenticate* him/her/itself. For example, the doctor is issued a doctor's accreditation license by the RIZIV, the patient is issued a social security credential by his/her HII id, containing the patient's name, social security status (sss) and HII, the MPA can prove its accreditation using a MPA certificate, issued by the RIZIV as well.

The simplest approach for a digital *prescription* is a tuple signed by the doctor. Such a prescription could look like

$$prescription \leftarrow (id_{doctor}, id_{patient}, id_{prescription}, data_{prescription})sig_{doctor}.$$

The prescription thus contains the ids of the doctor and the patient. A globally unique prescription id is included as well. This uniqueness can be provided by generating the prescription ids as

$$id_{prescription} \leftarrow H(id_{doctor}, i),$$

where i is only used once by the doctor in a predetermined time interval. As an

alternative, a trusted server could issue prescription ids. The prescription tuple is finally signed by the issuing doctor. The prescription can as well be a X.509 certificate issued by the doctor, where a corresponding keypair is generated by the patient.

The patient needs to proof that it is the owner of the prescription. Therefore, a prescription is always shown to a pharmacist in combination with the user's social security credential *ssc*, which contains at least the patient's id and social security status.

The pharmacist needs a *cost statement* in order to get repaid. Therefore, the patient signs a cost statement after the pharmacist checked the stock and sent the price to the patient. The signed cost statement looks like

$$proof_{service} \leftarrow (id_{prescription}, price, sss, date) sig_{ssc}$$

where the *price* is the amount of money paid by the patient, *sss* is the social security status of the patient and date is the date of the visit by the patient to the pharmacist.

The prescriptions, cost statements and certifictes are sent to the corresponding MPA, who generates the statistics and does some checks. The MPA generates invoices which are sent to the patient's HII:

$$invoice \leftarrow (''invoice'', id_{MPA}, id_{patient}, price_{pharmacist}, price_{patient}, (id_{prescription}, date_{prescription})[], date) sig_{MPA},$$

where $price_{patient}$ and $price_{pharmacist}$ are the amount of money the patient had to pay and the part the pharmacist had to advance respectively. This signed tuple is sent to the HII, who can update the patient's account and pay the MPA using classical electronic ways of payment. The $(id_{prescription}, date_{prescription})[]$ is a list of prescription ids, together with the date of usage of the prescription, of that specific patient the MPA received from the pharmacists. The invoice data is signed by the MPA.

To *delegate a prescription*, the patient just signs

$(\text{“}delegation'', id_{prescription}, id_{patient}, id_{delegate})$ tuple using his social security certificate. The delegate

shows this and authenticates to the pharmacist (e.g. using his eID card or his own social security certificate. The delegate can sign the cost statement.

To obtain access to the EHR ciphers on the EHR server, the patient gives the doctor authorization

$$auth_{EHRaccess} \leftarrow (id_{patient}, id_{doctor}, rights_{usage}) sig_{patient},$$

where $rights_{usage}$ contains restrictions on the access by the doctor. e.g. the doctor authorized to access the EHR till the end of the year. One or more keys must be given to the doctor as well in order to decrypt the EHRs. The

doctor proves to the EHR server being an accredited doctor with id id_{doctor} and proves as well that he is authorized to access the patient's EHRs by showing the signed authorization tuple. The EHRs are decrypted using the key K, provided by the patient to the doctor, such that the EHR server cannot get hold of the decrypted ehealth records.

Revocation of the different token types is possible by using unique identifiers that might be added to the tokens. These unique identifiers can be added to an online blacklist.

6.2 Evaluation

No thorough evaluation will be given. We focus on the privacy requirements and on the possible disputes.

Privacy. It should be clear that privacy is the weakest point. The EHR server knows which EHRs are from which patient, knows when which doctor accessed what records, knows what doctor added which records. The EHR server can potentially thus extract a lot of information. for example, if often an EHR by a highly specialized doctor is added, the EHR server can know what kind of disease the patient, whom the EHR server can identify, has.

The MPA and pharmacist know all the prescription related data: the patient's id, the doctor's id, the patient's HII (contained in the *ssc*).

Possible disputes. If a patient goes to multiple doctors to get the same medicines prescribed (D1), this will likely not be detected, however, there is always a chance that the RIZIV will detect something by inspecting the statistics, or/and by requesting some prescriptions from MPAs. It will be detected by the MPA if the pharmacists have the same MPA. If a common, centrally managed EHR server is used, the doctor will see that the patient has already consulted another doctor for a specific diseasy or complaint. If a prescription is used twice (D2), this will be detected by the HII, as the prescription has its own unique id, which is as well included in the invoices sent by the MPA to the HII. If the prescriptions ids are also sent by the MPAs to the RIZIV, the RIZIV will be able to detect double spending, which is a better solutions, as the HIIs task is not to catch its members. The pharmacist and MPA can check that the prescription and the ssc belong to the same patient by comparing both patient ids (D3). D4 is harder to detect, but fraudulent prescription behaviour is very risky for the doctor and can be detected by inspecting the statistics. If one can steal a prescription (D5), he/she will also have to steal the *ssc* and the thief will have to be able to sign using that ssc. If the patient does not get repaid (D6), he can still use the proofs signed by the patient, in combination with the prescription and use this when submitting a complaint. If the HII did not pay yet, he will not be able to show a payment proof provided by his bank. De IFEB has to trust that the MPAs deliver the proper statistical data (D8). However, the RIZIV can verify the statistical data by requesting samples of the

prescriptions from the MPAs. In this protocol, it is not possible to consume a part of the prescription. using the same cost statement twice will be detected by the MPA as the cost statement contains the prescription id.

7 Proposed solution

7.1 Settings

Recall that a typical health scenario in our setting, involves a *doctor*, a *patient*, a *pharmacist*, a *Medical Prescription Administration (MPA)*, a *Health Insurance Institute (HII)*, a public safety organization denoted *IFEB*, and a social security organization denoted *RIZIV*. Each of these players 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 practice as a doctor. `DrCred` contains an attribute `Dr_ID` along with other identity attributes.

Patient: has an identifier `Pt_ID`, and a social security status `Pt_sss`. The patient has a credential encoding `Pt_ID`, `Pt_sss`, and a number of additional identity attributes. The patient has also a "health expense account" `Pt_exp_acc` maintained by his *Health Insurance Institute* (HII). The value of `Pt_exp_acc` indicates the amount of money paid sofar by the patient for health expenses. Admissible health expenses charged to the patient beyond a predetermined maximum amount will be covered by the health insurance institute. This is based on the standard, legally determined prices, not the higher price that can be charged to the patient. In general, not any medical cost will be taken into account.
Patient's attributes = `{Pt_ID, Pt_hii, Pt_sss, Pt_exp_acc, ...}`

Pharmacist: has an identifier `Pharm_ID`, a corresponding *Medical Prescription Administration* (MPA), and a credential encoding those attributes and others.

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 of authorized organizations such as IFEB.

HII: has a publicly known identifier `HII_ID`, and a credential certifying its identity. The HII serves a set of patients and maintains their health expense account balances `Pt_exp_acc`, and covers the costs of admissible medical expenses incurred by those patients.

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

RIZIV: has a publicly known identifier `RIZIV_ID`, and a credential certifying its identity. Has various over-sighting activities. It controls organizations such as IFEB.

7.2 Credential material: summary

Based on the anonymity and access control requirements described in the matrix of Table 4, we have made a number choices regarding the type of credentials each participant in the ehealth workflow will need. These choices are summarized in Table 5.

Table 5: Credential type: requirements per participant

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

7.3 Protocol description

In the following we present a detailed description of the protocols we propose to achieve the requirements stated in section 4 and in table 4.

7.3.1 Notations

For a credential $Cred$ with attributes $a_1, \cdots, a_n$, the expression $Cred.a_\ell$ denotes the ℓ^{th} attribute of $Cred$. Given a predicate $\mathcal{P}$ on attributes $a_1, \cdots, a_n$, and a message m, the expression $\text{SPK}\{\mathcal{P}(a_1, \cdots, a_n)\}(m)$ denotes a signed proof of knowledge, on message m, of attributes $a_1, \cdots, a_n$ underlying $Cred$ and satisfying predicate $\mathcal{P}$. Given a receiver Rec, the expression $\text{VENC}_{\text{Rec}}(m, \mathcal{P})$ denotes a verifiable encryption of a message m, satisfying predicate $\mathcal{P}$, under the public key of Rec. A verifiable encryption is typically a ciphertext accompanied by a proof that the ciphertext does indeed decrypt to a message satisfying predicate $\mathcal{P}$. The latter proof is generally made non-interactive using the well-known Fiat-Shamir heuristic. Similarly, the expression $\text{ENC}_{\text{Rec}}(m)$ denotes an encryption of m under the public key of Rec.

7.3.2 Protocol

I. Doctor $\leftrightarrow$ Patient

(a) Dr. anonymously authenticate to Patient using his $DrCred$.

(b) Patient computes $com_{Pt} := comm(Pt\_ID)$,

(c) Patient shows to Doctor his credential $PtCred$, along with com_{Pt}, and proves that $com_{Pt}.Pt\_ID == PtCred.Pt\_ID$

(d) Dr. computes $com_{Dr} := Comm(Dr\_ID)$

(e) Dr. sets $Presc\_text :=$ {plain prescription text}

(f) Dr. computes
Presc := SPK$\{DrCred.Dr_ID == com_{Dr}.Dr_ID\}(Presc_text, com_{Dr}, com_{Pt})$,
and sends it to the patient, along with the opening info of com_{Dr}.

II. Patient $\leftrightarrow$ Pharmacist

(a) Pharm. authenticates to the patient using his X.509 pharmacist certificate.

(b) Pt. authenticates to Pharmacist using his anonymous credential, and provably discloses his social security status

(c) Pt. recovers $PharmCred.MPA\_ID$, the identity of the MPA serving the pharmacist.

(d) Pt. sends to pharmacist :

Presc. + SPK$\{PtCred.Pt_ID == Presc.com_{Pt}.Pt_ID\}(.)$
+
$\text{VENC}_{\text{MPA}}(Pt\_HII)$ + $\text{VENC}_{\text{MPA}}(Dr\_ID)$ + $\text{VENC}_{RIZIV}(Pt\_ID)$
+
$\text{ENC}_{\text{MPA}}\{$
$\text{VENC}_{\text{HII}}(Pt\_ID)$ +
proof that $\text{VENC}_{\text{HII}}(Pt\_ID)$ is consistent with $PtCred.Pt_{HII}$ +
random value $\}$
+
Proof{
$\text{VENC}_{\text{MPA}}(Dr\_ID)$ is consistent with $Presc.com_{Dr}$ $\wedge$
$\text{VENC}_{\text{MPA}}(Pt\_HII)$ consistent with $PtCred$ $\wedge$
$\text{VENC}_{RIZIV}(Pt\_ID)$ is consistent with $PtCred\}$.

NB. The correctness of the proof of consistency of $\text{VENC}_{\text{HII}}(Pt\_ID)$ will be checked by the MPA.

(e) Pharmacist charges patient, gets payed, and delivers drug. The Pharmacist issues an invoice and embeds the prescription's serial number $Presc\_ID$ in it.

III. Pharmacist $\leftrightarrow$ MPA

(a) Pharmacist and MPA mutually authenticate

(b) Pharmacist forwards to MPA prescription + verifiable encryptions

(c) If all is correct continue, if small errors are found, corrections can be added by the MPA, if $\text{VENC}_{HII}(Pt_ID)$ can not be verified, the RIZIV can reveal the identity of the user with the help of $\text{VENC}_{RIZIV}(Pt_ID)$.

(d) Check correctness of $\text{VENC}_{\text{HII}}(Pt\_ID)$, recover Pt_HII, and Dr_ID from verifiable encryptions.

(e) Forward the invoice to the patient's HII, and create a database entry for this prescription.

IV. MPA $\leftrightarrow$ HII

(a) MPA and HII mutually authenticate

(b) HII checks the integrity of the invoice

(c) HII recovers Pt_ID

(d) HII increments patient's account Pt_acc

(e) HII sends amount due (for the received invoice) to the MPA along with the invoice (which contains already prescription serial number.)

(f) HII creates a database entry for the processed prescription, e.g., $\{Pt\_ID, Presc\_ID, Presc\_cost, MPA, date, \cdots\}$

(g) After receiving the refund from the HII, the MPA compensates the pharmacist.

V. IFEB $\leftrightarrow$ MPA

(a) MPA and IFEB mutually authenticate

(b) IFEB requests statistics

(c) MPA provides statistics on prescription data anonymized according to an agreed-upon privacy policy. e.g.,
$\{Pt\_nym, drugs\_name, Dr\_nym, pharmacist\_region\}$

Remarks.

- In step I-(f) the Doctor computes the prescription as a signed proof of knowledge on the tuple $(Presc\_text, com_{Dr}, com_{Pt})$. The predicate being asserted in the proof is that com_{Dr} contains the same attribute Dr_ID embedded in $PtCred$. This results in the following properties:
  - Because the prescription is a signed proof, any one can check its validity non-interactively.
  - The prescription is tied both to the identity of the Dr. and that of the Patient. We assume here that the Dr. would not accept to sign com_{Pt} if the underlying Pt_ID was not consistent with $PtCred$ (the consistency proof was performed by the Patient in step I-(c).)
  - The Dr. discloses the decommitment information of com_{Dr} to the patient, to allow him to verifiably encrypt Dr_ID under the public key of the pharmacist's MPA (later in step II-(d).) Note that the Doctor cannot do this since the identity of the pharmacist where the patient will buy his drugs is usually not known at the time of the prescription issuing. Moreover, this gives more flexibility to the patient, since it leaves the patient free to buy his medicines at any pharmacy he wants. There is also a gain in privacy to the patient since he does not have to disclose where he buys his drugs, to the Doctor.

- In step II-(d), the pharmacist is not supposed to learn the identity of the patient's HII, and yet we want to be sure that the patient has correctly encrypted his identity under the HII's public key. If the patient gives the proof, that $\text{VENC}_{\text{HII}}(Pt\_ID)$ is consistent with $PtCred$, directly to the pharmacist, the latter will need to know the public key of the HII (and thus the identity of the HII) in order to check the verifiable encryption. That's why the proof is encrypted under the MPA's public key. When the MPA (who is allowed to know the identity of the patient's HII) receives the transcript above, he decrypts the ciphertext:

  $$\text{ENC}_{\text{MPA}}\{\text{proof that } \text{VENC}_{\text{HII}}(Pt\_ID) \text{ is consistent with } PtCred\}$$

  and verifies that the recovered proof is consistent with $\text{VENC}_{\text{HII}}(Pt\_ID)$ and the public key of HII.

- In step V-(c), the statistics data returned by the MPA, may contain real Patient/Doctor pseudonyms. It is clear that this may reveal linkabilities between different transactions performed by the same party (patient or doctor). To avoid this linkability, the IFEB can sanitize the data received from the MPAs by removing the real pseudonyms, and replacing them with random ones if needed. Obviously, this option allows more freedom to the IFEB who can then generate a larger variety of meaningful statistics, but at the cost of putting some trust in the IFEB.

7.4 Evaluation

Security. Our solution achieves entity authentication, and integrity owing to the unforgeability of the underlying signed proofs of knowledge and the X.509 signatures. Confidentiality also follows from the security of the underlying encryption schemes. As for token revocability, it is easily achieved using the revocation mechanisms of the credential system being used.

Privacy. The protocol we propose enforces the access control policies of Table 4, thereby satisfying the privacy requirements of Section 4.2. It is worth noting however that the IFEB needs to be trusted not to divulge information about the patients' health records without proper anonymization. Alternatively, the MPAs could remove themselves any identifying patient information from the records prior to sending them to the IFEB. In this case, the range of statistical information that can be extracted is relatively diminished. A compromise between the two options can be reached depending the type of statistical needed.

Fraud detection and Dispute handling.

- Single prescription issuance (D1): As indicated in step I-(f), the patient's ID is tied to the prescription, and can serve as a means to detect abusive multiple doctor consultation.

- Single prescription spending (D2): Prescription are forwarded to the patient's insurer HII, who will be able to detect double spending.
- Prescription - Social Security Status Linking (D3): follows straightforwardly from the soundness of signed proofs of knowledge.
- False Prescription issuance (D4): Additional law-enforcement resources (possibly non-technological) are needed to handle false prescription issuing, e.g., witnesses, whistle blowing.
- Prescription theft (D5): This follows straightforwardly from the security of the credential system we use.
- Correct processing of prescription (D6): Information available in the transcript is sufficient prove mistakes that may occur in the processing of prescriptions.
- Correct statistics (D7): The MPA can be required to keep an archive of all transaction transcripts. These transcripts can be later audited to determine if the generated statistics are correct. This method is vulnerable however to omission attacks where the MPA would erase complete database entries. Depending on the database architecture, omissions can be guarded against by tying the different database records through (multidirectional) sequencing scheme. Further investigation on this topic is needed.

8 Prototype implementation

To demonstrate and test the quality of the design presented in Section 7, we use the Idemix system [7] to build our prototype. It is worth noting however that the Idemix SDK currently available is very limited, and does not provide any documentation. At the time of writing this report, our work on the prototype implementation is still ongoing. A complementary report describing our prototype implementation will be released shortly.

9 Legal Aspects

9.1 Legal framework applicable to electronic prescriptions

9.1.1 What is a 'prescription'?

The law does not at present define what a 'prescription' is in general. A prescription is a document which gives a patient permission to obtain something relevant to his health, e.g. medication. The patient is free whether or not to actually use the prescription and to choose a health care provider.[1]

[1] Freedom of choice of a health care provider is enshrined in art. 6 Patients' Rights Act.

Specific types of prescriptions can be distinguished, and for some of these some requirements regarding contents or form are in place. Prescriptions for medications are to be distinguished from prescriptions for treatments of a diagnostic, preventative or curative nature or for medical aids (e.g. glasses, prosthetics). Only the first category is considered in the Adapid electronic prescription application, therefor only this category will be discussed here. Regarding prescriptions for treatments and medical aids, one can only note that no general rules are in place, though prescriptions for specific types of treatment are subject to various legal obligations.[2]

9.1.2 Content requirements

Prescriptions for medication must contain the following information[3]:

- Full name and address of the prescribing health care professional;
- RIZIV identification number of the health care professional, in digits and – where applicable – in bar code;
- name of the medicine;
- full name of the patient;
- dose per day and – where applicable – the fact that the patient is an infant or child;
- date of the prescription;
- date from which the medication may be issued, where applicable;
- mode of administration;
- strength of the medication;
- indication of the amount of medication;
- indication that the medication is a magisterial preparation;

[2]For instance prescriptions submitted to the Special Solidarity Fund ('Bijzonder solidariteitsfonds') are regulated by art. 25 septies Coordinated Law of 14 July 1994 regarding obligatory health care insurance and benefits (*M.B.* 27 August 1994), hereafter Obligatory Health Care Insurance Act. Regarding prescriptions for radiological diagnosis, see art. 69ter of the same law.

[3]Art. 21 Royal Decree nr. 78 of 10 November 1967 regarding the exercise of health care professions (*M.B.* 14 November 1967), hereafter Health Care Royal Decree, and Royal Decree of 10 August 2005 regarding the modalities of prescriptions for human use (*M.B.* 20 september 2005).

9.1.3 Requirements of form

Prescriptions for medication must be signed and dated by the health care provider in order to be valid.[4] The signature may be a handwritten or an electronic signature, in accordance with the provisions of the Certification Service Providers Act.

The Health Care Royal Decree grants the government the authority to impose an obligation to use qualified electronic signatures by Royal Decree. So far, the government has not made use of this faculty. The e-Signatures Directive allows member states to impose additional requirements – such as the use of qualified electronic signatures – in the public sector, insofar as these requirements are objective, transparent, proportionate and non-discriminatory. Also, the requirements must relate to the specific characteristics of the application concerned and may not constitute an obstacle to cross-border services for citizens.[5] In passing this provision into law, the legislator simply assumes that the activity of health care providers is part of the public sector.[6] This assumption is open to serious debate. Even though health care is heavily funded by the government, many health care professionals are self-employed, independant consultants and would not consider themselves to be part of the public sector. The requirement to use qualified electronic signatures is justified in the preparatory works by referring to the need to identify the prescriber unambiguously combined with the fact that only qualified signatures are assimilated with handwritten ones by force of law.[7] This justification is questionable, as the definition of the advanced electronic signature already stipulates that it must be capable of identifying the signatory.[8] The qualified electronic signature does not imply that a rigorous method for checking the true identity of certificate holders is adhered to, even though the CSP issuing qualified certificates must "verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued".[9] In light of these issues, imposing the use of qualified electronic signatures for electronic prescriptions may run foul of EU legislation and ultimately result in a conviction from the European Court of Justice.

To date, a large subcategory of prescriptions for medicine must still be issued in paper form. The Obligatory Health Care Insurance Act stipulates that prescriptions issued to non-hospitalized patients must comply with a model form[10] and have the health care provider's RIZIV identification number printed on it in bar code. Despite technical possibilities to mimick the layout of the model form, and perhaps even to combine the use of an image of the prescribers handwritten signature in the document with an electronic signature on the file, from a legal

[4] Art. 21 Health Care Royal Decree.

[5] Art. 3 §7 e-Signatures Directive.

[6] Doc. Parl. Chambre 51 nr. 473/1, p. 82 ff.

[7] Doc. Parl. Chambre 51 nr. 473/1, p. 82 ff.

[8] Art. 2 §2 e-Signatures Directive.

[9] Annex II d) e-Signatures Directive.

[10] Royal Decree of 8 June 1994 regarding the model form for prescription of pharmaceutical products to non-hospitalized beneficiaries (*M.B.* 14 Juni 1996).

point of view the prevailing interpretation is that currently the use of paper is required.

There is no similar model imposed for prescriptions issued to patients in a hospital setting. A number of hospitals have implemented internal electronic prescription systems.[11]

9.1.4 Electronic prescriptions as an information society service?

Does the issuance of electronic prescriptions by the health care provider make him an information service provider in accordance with the definition of the e-Commerce Directive?[12]

An 'information society service' comprises any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. 'By electronic means' is to say that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means. 'At the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.[13]
'At a distance' means that the service is provided without the parties being simultaneously present. Prescriptions are generally issued during a consult of a patient with his health care provider, after some form of physical examination. Therefor, the health care provider does not become an information society service provider by issuing electronic prescriptions. Insofar as the patient still has to physically go to the pharmacy to use his electronic prescription, no information society service can be discerned here either. The pharmacist can be expected to forward the prescriptions he receives to the MPA electronically. Thus the pharmacist and the MPA can be said to interact 'at a distance'. 'Normally provided for remuneration' means that only economic activities are covered, as opposed to research trials or hobby projects.[14] As a rule, government activities are not considered economic activities, thus health care services operated and funded by the government would fall outside the scope of this definition. There

[11] One example is the Virga Jesse Hospital located in Hasselt (Belgium), which started the rollout of its electronic prescription system in 2001. [41].

[12] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J.* L 178, p. 1-16. This directive was transposed into Belgian law by the Law of 11 March 2003 on certain legal aspects of information society services, *Moniteur Belge* 17 March 2003, hereafter e-Commerce Act.

[13] Art. 1 para. 2 Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, as modified by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998, referred to by art. 2, b) e-Commerce Directive. Implemented in Belgium in art. 2 1°e-Commerce Act.

[14] Recital 18 e-Commerce Directive.

are however exceptions to this rule, notably when a state activity is not funded by public funds, but is mainly funded by the fee paid by the users or a third party. In such situations, no distinction is to be made between private and public entities.[15] Whether a particular health care service constitutes an economic activity must be regarded on a case-by-case basis. In the electronic prescription scenario described within ADAPID, the MPAs are the most likely candidate for being an information society service provider.

Being an ISSP brings with it a number of advantages, in particular the freedom of establishment and provision of services as well as the 'country of origin' principle.

Freedom of establishment and provision of services means that EU member states may not subject the establishment of an ISSP to prior authorisation or any equivalent measure.[16] Thus, any organisation is – in theory – free to start and operate a MPA in any EU member state without needing to request permission or accreditation beforehand. Voluntary accreditation schemes are permitted.[17] Belgian law however does impose a requirement of prior authorisation upon MPAs.[18] Since this authorisation scheme does not specifically and exclusively target information society services, it is allowed by the e-Commerce Directive.[19]

The 'country of origin' principle means that ISSPs are submitted to the rules of the EU member state in which they are established. They do not have to take into account the rules of all the European countries in which they provide their services. Once they respect the rules of the country in which they are established, their services have to be considered in line with the rules of all the member states in which they operate. In every member state, providers originating in other member states should have the same chances for providing their services as the providers established in the member state, particularly in the fields covered by the e-Commerce Directive.[20] Especially supervision or accreditation schemes should never lead to legal or practical restrictions for the provision of information society services by providers established in other member states.

The 'country of origin' principle does not completely liberate ISSPs from complying with the different rules of the various member states. This privilege only applies to regulations falling within the so-called 'coordinated field' of the e-Commerce Directive. The coordinated field comprises all requirements laid down in member states' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.[21]

[15] Compare [12], p. 10 ff.

[16] Art. 4 §1 e-Commerce Directive. Implemented in Belgium in art. 4 e-Commerce Act.

[17] Recital 28 e-Commerce Directive.

[18] Art. 165 Obligatory Health Care Insurance Actas executed by Royal Decree of 15 June 2001 regarding criteria for recognition of medical prescription administrations (*M.B.* 27 July 2001).

[19] Art. 4 §2 e-Commerce Directive.

[20] Art. 3 e-Commerce Directive. Implemented in Belgium in art. 5 e-Commerce Act.

[21] Art. 2, h) e-Commerce Directive, implemented by art. 5 e-Commerce Act.

Under specific circumstances and subject to stringent conditions, a member state may overturn the 'country of origin' principle and take measures against an ISSP established in another member state.[22]

Since MPAs that are not authorised by the Belgian government may not operate in Belgium, the 'country of origin' principle is of little relevance to this case.

Note that ISSPs established outside the EU cannot invoke this principle, and can therefor be subjected to the legislation of each EU member state. The same holds for a services operated by the government, insofar as it is not considered to be an ISSP.

ISSPs are also subject to a number of obligations, notably with respect to the rights of the recipient of the service (both consumers and professional users).[23]

9.1.5 The electronic prescription application as a certification service?

The freedom of establishment and 'country of origin' principles are also part of the legal framework on electronic signatures and certification service providers.[24] Interestingly, no distinction is made between private and public entities in this framework, therefor it is worth considering whether the proposed electronic prescription application could fall within its scope of application.

A certification service provider is defined very broadly as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures".[25] In turn, electronic signature are defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication".[26] The preamble gives a number of examples of related services: registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures.[27] The examples denote services intended to support the deployment of electronic signatures in practice.

A fundamental question is wether the electronic prescription application makes use of electronic signatures within the meaning used in the law. With-

[22] Art. 3 §4-6 e-Commerce Directive, implemented by art. 2 Wet betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij als bedoeld in artikel 77 van de Grondwet.

[23] [38, 28]

[24] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *O.J.* L. 13, p. 12-20, hereafter e-Signatures Directive. This directive was transposed into Belgian law by the Law of 9 July 2001 on a legal framework for electronic signatures and certification service providers, *Moniteur Belge* 29 September 2001, hereafter Certification Service Providers Act

[25] Art. 2 §11 e-Signatures Directive, implemented in art. 2 10° Certification Service Providers Act.

[26] Art. 2 §1 e-Signatures Directive, implemented in art. 2 1° Certification Service Providers Act.

[27] Recital 9 e-Signatures Directive.

out going into the discussion whether the term 'authentication' is used here in the same sense as it is understood by computer scientists, suffice it to say that traditionally two functional requirements are ascribed to signatures: identification of the signatory and subscription to the message. A third functional requirement, namely guaranteeing integrity of the message, is somewhat more controversial. Though the electronic prescription application developed within Adapid explicitly aims to ensure that the doctor 'signing' a prescription is not identifiable by default, under the right conditions he is identifiable. Likewise, the fact that the doctor issues the prescription signifies his subscription to its contents. In this view, the electronic prescription application can be considered to at least make use of electronic signatures within the sense of the law. Even then, there is reason to doubt whether such an application would constitute a certification service provider in the legal sense. The service provided by the electronic prescription application is not intended to support the deployment of electronic signatures, thus it is not a service 'related to electronic signatures'. Rather it constitutes a service making use of electronic signatures. The definition of certification service provider does not include services that merely make use of electronic signatures, neither in the e-Signatures Directive nor in the Certification Service Providers Act. The recitals to the e-Signatures Directive, however, do suggest to include such services.[28] More clarity regarding the exact scope of the notion 'certification service provider' can only be expected through jurisprudence of the EU Court of Justice.

9.1.6 The electronic prescription application as a service

In December 2006, a new directive was adopted providing a general framework for services in the internal market.[29] The Directive has entered into force on 28 December 2006, making the text binding upon the member states. The deadline for transposition into national law is 28 December 2009.[30]

The notion 'service' is defined very broadly as "any self-employed economic activity, normally provided for remuneration".[31] A 'provider' is a natural or legal person with sufficient ties to a Member State, who offers or provides a service.[32] Clearly, very few professional activities based in the EU will escape from the broad definition of a 'service provider'.

The directive does not apply to healthcare services whether or not they are provided via healthcare facilities, and regardless of the ways in which they are organised and financed at national level or whether they are public or private.[33] The exclusion of healthcare from the scope of the directive covers healthcare and pharmaceutical services provided by health professionals to patients to assess,

[28] Recital 9 e-Signatures Directive.

[29] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, *O.J.* L 376, p. 36-68, hereafter Services Directive.

[30] Art. 44 §1 Services Directive.

[31] Art. 4 1) Services Directive. See also [12], p. 10 ff.

[32] Art. 4 2) Services Directive. See also [12], p. 16 ff.

[33] Art. 2 §2 f) Services Directive.

maintain or restore their state of health insofar as those activities are reserved to a regulated health profession in the member state in which the services are provided.[34] Thus, the issuance of medical prescriptions is excluded. This exclusion does not extend to the activities of the MPA, since these offer a service to pharmacists and not directly to patients.

The Services Directive reiterates the freedom of establishment and provision of services principle already contained in the e-Signatures Directive and e-Commerce Directive. Notably, the Services Directive subjects authorisation schemes to stringent conditions pertaining to non-discrimination, justifiable cause and proportionality.[35] Authorisation schemes may be maintained only if they are non-discriminatory, justified by an overriding reason relating to the public interest and proportionate. The Belgian government will have to assess whether the authorisation scheme applicable to MPA's is permissible under the Services Directive.

Unlike the e-Signatures Directive and e-Commerce Directive, the Services Directive does not introduce the 'country of origin' principle. Since the Services Directive does not harmonize the regulations in place in the member states or provide mininum requirements, introducing such a principle could have negative consequences for the quality of services available in the internal market.[36] In stead, the directive restricts which requirements member states may impose on the access to or the exercise of a service activity.[37]

Member states must subject service providers to a number of obligations intended to guarantee the quality of service, notably with respect to the rights of the recipient of the service (both consumers and professional users).[38]

9.1.7 Data protection

In the scenario of the electronic prescription application there are a number of parties who play the role of data controller or data processor: the doctor, the pharmacist and the MPA. The only difference between being a data controller or a data processor is that the latter works under supervision and responsability of someone else – who is then the real data controller – whereas the former works under his own responsability. Over all, the obligations of the Data Protection Act must be complied with in the same way.[39]
The patient is exempt for the Data Protection Act insofar as he only processes data for personal purposes.[40]

[34] Recital 22 Services Directive. See also [12], p. 13 ff.

[35] Art. 9 Services Directive. See also [12], p. 31 ff.

[36] This might encourage service providers to establish themselves in the member state with the lowest quality requirements to provide their services in the entire EU from there.

[37] With regard to requirements for establishment, see art. 15-16 Services Directive. With regard to requirements for cross-border services, see art. 16-18. See also [12], p. 38 ff.

[38] Art. 22-27 Services Directive. See also [12], p. 63 ff.

[39] Law of 8 december 1992 on the protection of privacy with regard to the processing of personal data, *M.B.* 18 March 1993.

[40] Art. 3 §2 Data Protection Act.

The only means to escape the grasp of the data protection act is to reasonably show that none of the data held in storage qualifies as personal data as defined by the Data Protection Act. Considering the astounding breadth of the notion 'personal data' as it is interpreted in Belgium at present, this is nearly impossible. Even in case all the data were encrypted with keys not in the data controller's possession, this would not be sufficient. As long as there is another party who could – with reasonable means – identify the data subjects, e.g. by decrypting or deanonymizing data, the data is considered personal data with regard to anyone who has it in his possession.

The doctor will generally know who his patient is and includes a patient id in the prescription. Thus the prescriptions are personal data. In the rare case where the patient does not reveal his identity or cannot reveal his identity, a pseudonym might be used. The pseudonym too refers uniquely to the patient, which in turn makes it personal data.

The pharmacist receives prescriptions which contain personal data in encrypted form, in particular the doctor's id and the patient's id. Although the pharmacist cannot decrypt this information by default, there are other parties who could decrypt the information with reasonable means. The HII is capable of decrypting the patient's id. The MPA is capable of decrypting the doctor's id and the patient's social security status. Thus, the prescription is personal data, even with regard to a pharmacist who cannot himself derive the identity of the patient or doctor involved from it. Abstraction is made here from the fact that the patient or his delegate may identify himself by paying with a debet or credit card.

As explained above, once a prescription is recognized as personal data in the hands of one party, it is personal data with respect to anyone who handles it. Thus the MPA processes personal data about both the doctor and the patient, even though it needs help from the HII to actually obtain the patient's identity.

Data controllers may only process personal data if they comply with the provisions of the Data Protection Act. Three important principles lay at the basis of the Data Protection Act: legality or transparency, finality and proportionality. In each case, the provisions of the Act elaborate the practical effects of these principles. Furthermore, the data subject is granted a number of rights which are aimed to give him the power of control over how his data is processed.

The legality or transparency principle signifies that anyone must reasonably be able to know what information is being processed about him or her, why this is being done and who is doing it. The data controller must provide clear information so that all those concerned are reasonably aware of which privacy expectations they may harbor. Transparency must be guaranteed at all times during processing. Since the doctor is the first in a chain of data processors, it would be most efficient if he informs the patient about which data is collected, how it is processed and for which reasons, as well as how long it will be stored and who it will be forwarded to. This information does not need to be provided at each consult, it suffices if it is given with the first electronic prescription issued to the patient. If the way in which data is processed changes, the patient should be informed about this. If doctors, pharmacies and MPA's cannot come

to an agreement about who will inform the patient, they must each provide the necessary information independantly.

Legality also means that the data processing is justifiable based on the grounds recognized by the Data Protection Act. Since prescriptions are imposed by law, this is sufficient justification for processing the data they contain. Prescriptions are medical data[41], the processing of which is subject to more stringent conditions than other data. As a rule, processing medical data is prohibited, unless one of the exceptions listed in the law applies. One such exception is that the processing is necessary for to provide care or treatment to the data subject or a relative, or for the management of medical services in the interests of the data subject.[42] Also, medical information may be processed in all cases in which this is required by a law, decree, ordinance, a royal decree or a ministerial order for reasons of grave public interest.[43] The data must be processed under the supervision of a health care professional who is subject to an obligation of secrecy.[44] Moreover, medical information must, in principle, be obtained from the data subject himself. Requesting medical information from third parties is only allowed when this is the only justifiable option.[45] This last condition is relevant for the MPA, and for the pharmacist in those cases where a delegate collects the medicine for someone else.

The principle of finality signifies that personal data may only be processed for a very specific, explicitly defined and justifiable purpose. Using the data for a different purpose is only permitted if this new purpose is compatible with the original one. The compatibility must be evaluated taking into account all relevant factors, specifically the reasonable expectations of the data subject, and the applicable laws and regulations[46]. Further processing of the data for historical, statistical or academic purposes are not considered incompatible under the conditions established by Royal Decree.[47] Collecting information because it may come in handy some day is out of the question.

Only information that is really necessary to attain the objectives set may be processed: the data must be sufficient, relevant and may not be excessive.[48] On top of this, the information must be accurate and, if necessary, updated.[49] This does not imply that the original document must be modified, alternatively remarks may be added in an annex. Personal data may not be stored in an identifiable way longer than necessary.[50] The Royal Decree implementing the Data Protection Act contains a special regime for historical, statistical or academic purposes.[51]

[41] Art. 7 §1 Data Protection Act.
[42] Art. 7 §2 j Data Protection Act.
[43] Art. 7 §2 e Data Protection Act.
[44] Art. 7 §4 Data Protection Act.
[45] Art. 7 §5 Data Protection Act.
[46] Art. 4 §1 2°of the Data Protection Act.
[47] Royal Decree of 13 February 2001 implementing the Privacy Act (*M.B.* 13 March 2001).
[48] Art. 4 §1 3°of the Data Protection Act.
[49] Art. 4 §1 4°of the Data Protection Act.
[50] Art. 4 §1 5°of the Data Protection Act.
[51] Royal Decree of 13 February 2001 implementing the Privacy Act (*M.B.* 13 March 2001).

The data controller must take suitable technical and organizational measures to protect personal data against fortuitous or wrongful destruction, accidental loss, modification, unlawful access and any unlawful processing in general. An appropriate level of security must be guaranteed given the state of the art in technology, the costs involved, the nature of the data to be protected and the potential risks[52]. In other words, the data controller must guarantee the confidentiality and integrity of the information.

9.2 The evidence trail produced by the electronic prescription application.

9.2.1 Create connection

At various points in the electronic prescription application, entities need to set up a connection with each other. E.g. a patient or health care professional connects to the EHR server, a pharmacist connects with the MPA, ...

Either party to the connection can log the traffic data related to the connection, e.g. IP-address of the patient.

Such traffic data is personal data if it refers to a natural person, e.g. a patient or a specific employee/representative of an organisation. If the traffic data refers to an organisation as such, it is not personal data. Note that one-man corporations are a special case.

In case anonymous communication channels are used, the traffic data logged by either party may lose it's status of personal data. This depends on whether or not the traffic data can be deanonymized, either by the connecting parties or by a third party. Note that this is true in Belgium, where a very broad concept of 'personal data' is used, whereas in other EU countries a more restrictive view has been adopted.

Generally, the parties setting up a connection will authenticate themselves towards each other. In some cases authentication will entail proving one's identity, in others only certain attributes will be proven. Authentication happens in two steps:

1. Party A authenticates him/herself towards a local device (e.g. handheld device). The local device issues credential or gives access to existing credentials on the device.

2. Party A shows a credential to Party B.

The parties involved in the credential show protocol can save transcripts of the protocol's execution as evidence. In order for this transcript to have any evidentiary value, reliable information is necessary about the time when the protocol was executed, who the involved parties were and what the context of the credential show was. Context information can be added in the anonymous

[52] Art. 16 §4 Data Protection Act.

credential show and signed anonymously, which ensures that only some properties of the signer are revealed, but not his real identity. Likewise, it should be possible to adapt classical authentication protocols using X.509 certificates to include this contextual info.

If the credential can in no way be deanonymized, it is not personal data. A deanonymizable credential is legally considered to be personal data, regardless whether the person who has it in his possession can execute deanonymization himself or not. As indicated above, perfectly anonymous credentials have little to no value as evidence in case of a dispute, since they cannot be traced back to their owner.

9.2.2 Visit doctor and obtain prescription

During the consult, the doctor may issue a prescription to the patient in the form of a (deanonymizable) credential.

The doctor should not be able to repudiate issuing the prescription. This is trivially true because the patient has a prescription which could only have been issued by a (deanonimizable) doctor.

The patient should not be able to repudiate receiving the prescription. A prescription is an anonymous credential, meaning that the issuance protocol results in a transcript for the doctor. This transcript can serve as receipt as well. The doctor should thus store this evidence for a while (locally or remotely).

As explained above, the prescription is personal data about both the patient and the doctor.

9.2.3 Visit pharmacist and use prescription

Showing a prescription amounts to showing an anonymous credential. A transcript of the credential show is kept by the patient and by the pharmacist. Thus, neither the patient nor the pharmacist can repudiate that a prescription was shown.

As explained above, the prescription is personal data about both the patient and the doctor.

9.3 Legal framework for electronic health records

To date, every health care provider keeps a record on his/her patients and already use electronic systems. Each of these systems is generally completely independent and is not co-ordinated in any way. Through the development of standards and recommendations, the government is trying to lay the foundation for an electronic health network that will allow records relating to a given patient to be linked to one another. The protection of the privacy of all those concerned is the greatest challenge here.

The legal framework for electronic health records is a highly complex matter, amongst other factors due to concurrent regulatory initiatives on the federal and regional levels. Since the focus of the ADAPID demonstrator lies with electronic

prescriptions rather then shared electronic health records, only those national regulations specifically targeted at electronic health records will be analysed.

9.3.1 Federal initiatives and regulation regarding electronic health records

Federal regulation

The backdrop for any platform for electronic health records is of course the Data Protection Act and the Patients' Rights Act.[53] Health data is an especially sensitive category of data, the processing of which is strictly regulated. As a rule, processing such data is prohibited, unless a valid legal ground for doing so is present.[54] Keeping track of whether a specific act of data processing is legitimate is a particularly thorny issue.

The Patients' Rights Act obliges health care providers to keep health records on all patients which are to be conscientiously maintained and securely stored.[55] This obligation is elaborated upon in several other legal texts:

1. The Royal Decree of 3 May 1999 on the minimal requirements applicable to the medical record, as referred to in art. 15 of the Hospital Act coordinated on 7 August 1987 (*M.B.* 30 July 1999), stipulates that a medical record must be created for each patient treated. These records must be archived for at least thirty years in the hospital.

2. The Royal Decree of 3 May 1999 on the General Medical Record (*M.B.* 17 July 1999) requires every patient to have a medical record managed by a general practitioner. The General Medical Record was introduced to serve as the basis for a shared (electronic) health record.

3. Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical record for each patient. Art. 46 of the Code of Medical Ethics provides that medical records must be preserved for thirty years after the last contact with the patient. The Medical Code of Ethics is drafted by the National Council of the Belgian Medical Association.[56]

4. According to art. 146 quinquies §1 of the General Health and Safety Regulation (A.R.A.B./R.G.P.T., *M.B.* 11 February 1946), each industrial doctor must create a medical record for each patient that he/she examines.

The term "medical record" is not defined as such by law, though the Royal Decree on the General Medical Record describes it as a functional and selective collection of relevant data of a medical, social and administrative nature. The

[53] Law of 22 August 2002 regarding the rights of patients, (*M.B.* 26 September 2002), hereafter Patients' Rights Act.

[54] Art. 7 Data Protection Act.

[55] Art. 9 §1 Patients' Rights Act.

[56] The text is available at `http://www.ordomedic.be/`

texts cited above impose certain obligations to create a medical record and describe what it must contain as a minimum. The medical record has three functions: it is an important tool for the doctor, it serves as evidence in disputes about medical liability and, in the long term, it is a source of information for academic research.

The Data Protection Act grants data subjects a right of access to their data, thus patients have a right to access the health records about them kept by their health care providers. The Patients' Rights Act provides for an exception to the right of access in those cases where giving such access would manifestly result in serious compromise of the patient's health (therapeutic exception). The health care provider must consult with a colleague before invoking this exception.[57] Likewise, personal notes of the health care provider are exempt from the right of access.[58] Both exceptions preclude a system whereby the patient has automatic full access to his health records.

The Patients' Rights Act also grants a limited right of access to certain relatives of the patient. This right can only be exercised after the death of the patient and is subject to a number of conditions. The request must be sufficiently motivated and must be denied in case the patient protested against such access during his lifetime. Relatives cannot claim direct access, but may designate a health care professional to obtain access for them. In this case, personal notes are not exempt from access.[59]

Federal initiatives towards an Electronic Health Network

As part of the modernization of health care, the government has taken various steps toward an electronic health network and a shared patient record accessible to all health practitioners treating the patient. The general medical record was introduced as the first step in this evolution. All the information relating to the patient's state of health is centralized in this record. The general practitioner chosen by the patient manages the general medical record. The intention of this system is to improve the quality of health care greatly by centralizing medical data so that it can be processed more efficiently, with the general practitioner as pivotal figure. This allows all those involved to follow up on the patient's state of health more efficiently. For instance, ordering the same test twice can be avoided. Up to now the patient may decide freely whether or not to allow a general medical record to be created.

The general medical record can only be used efficiently in the health care network when the information is maintained and archived in electronic form. This way everyone involved can have rapid access to the data when necessary. Nevertheless, the law still allows doctors to maintain the record in paper form in stead of electronically.

The "Telematics Standardization Commission For Health Care"[60] (here-

[57] Art. 7 §3 Patients' Rights Act.
[58] Art. 9 §2 Patients' Rights Act.
[59] Art. 9 §4 Patients' Rights Act.
[60] Royal Decree of 3 May 1999 (*Moniteur belge* 30 July 1999).

inafter referred to as "the Telematics Commission") was set up to avoid chaos in the electronic exchange of medical data, to ensure system interoperability and to guarantee the confidential and secure handling of medical data. A telematics cell was also established within the Federal Public Service for Social Affairs, Public Health and the Environment to help achieve these goals.

The Telematics Commission was assigned the task of developing modalities for the electronic exchange of medical data. The role of the commission is advisory only, the competence to issue norms rests with the BIN (Belgian Institute for Normalization), with the CEN (European Committee for Normalization) and the ISO (International Organization for Standardization).

The Telematics Commission developed quality criteria for computer systems used by hospitals and general practitioners. The EMDMI (*Elektronisch Medisch Dossier Médical Informatisé* [Electronic Medical Record]) working group of the Federal Public Service for Social Affairs, Public Health and the Environment developed quality criteria for software applications designed to manage patient records for general practitioners. Software producers can submit their programs to a certification procedure to obtain a quality label. The commission issued several recommendations relating to the preservation of medical records, specifically regarding the content of the record, the preservation period, and the form.[61] Additionnally recommendations were issued to standardize and harmonise the content, the exchange formats and syntax of electronic messages to allow a consistent integration of data in the comprehensive electronic medical record.[62] Finally, guidelines were formulated for the use of the electronic signature so that all persons concerned could be identified unambiguously. In this way, the origin of the information in the record can be verified and access to it restricted.[63]

The federal government has for several years now been working on an ambitious plan for shared electronic health records, which were to be kept in a centralized database by a federal agency. Largely due to great distrust of such a system within the health care sector, little progress has been made. A high level overview of the plans for shared health records – called Health Networks – can be found on the web portal of the Federal Public Service Health, Food Chain Safety and Environment.[64]

With regard to one element of the envisioned Health Networks infrastructure

[61] Telematics Commission, "Langetermijnbewaring van patiëntendossiers in ziekenhuizen" ["Long-Term Storage of Patient Records in Hospitals"], Recommendation 7, available at `http://www.health.fgov.be/telematics`.

[62] Telematics Commission, Recommendation 3 "Messages relating to the Electronic Medical Prescription (General)", Recommendation 4 "Electronic Health Care Messages", Recommendation 5 "Codification System for the Classification of Illnesses" and Recommendation 6 "The Electronic Message 'Medical Prescription Addressed for the Pharmacist' (Part 1)" available at `http://www.health.fgov.be/telematics`.

[63] Telematics Commission, Recommendation 2 "Digital Signatures and Certificates in Health Care" ["Digitale Handtekening en Elektronische Certificaten in de Gezondheidszorg"], available at `http://www.health.fgov.be/telematics`.

[64] See 'Health Networks' at `http://www.health.fgov.be/telematics`.

some progress can be reported, namely the BeHealth platform. BeHealth will provide services to support electronic exchange of data in the health care sector, without necessarily hosting such data itself. Initially, BeHealth is planned to provide authentication services – including identification and qualification of users – and to manage access authorisations to certain authentic sources. The platform will allow for delegation of authorisations, protect the confidentiality of all processed data, make use of appropriate logging procedures and implement technologies to ensure non-repudiation by users. The system will provide a way to electronically sign documents where necessary.[65]

9.3.2 Flemish initiatives and regulations regarding electronic health records

Concurrent with efforts on the federal level to create a system for shared electronic health records, the Flemish region has adopted its own regulation in order to implement such a system in the Decree Health Information System.[66] The compentency of the Flemish government in the area of health care does not include all health care professionals, therefor the Decree Health Information System is limited in scope. Participation in the two platform is only mandatory for actors which are funded by the Flemish Region. Naturally, there is considerable concern regarding the overlap and interoperability between the federal and regional systems.

The Flemish Health Information System has two dimensions: an operational information system and an epidemiological information system. The former aims to support data exchange between health care providers about individual patients. The latter aims to support data exchange between a wide number of partners in order to improve health care policy.[67]

The Decree Health Information System does not create a fully centralised system for shared electronic health records, rather it expects each health care provider to keep his own records – on paper or electronically – for his patients[68] and imposes a duty to upload an electronic summary into the Flemish Health Information System.[69] The electronic summary should take a uniform and standardised form, the details of which are yet to be determined by the Flemish Government.[70] The electronic summary identifies both the health care provider and the patient by way of a pseudonym only, the specifics of which are also yet to be determined by the Flemish Government.[71] These pseudonyms may

[65] Proposition by the ministers Johan Vande Lanotte, Rudy Demotte and State Secretary Peter Vanvelthoven regarding BeHealth, Memorandum to the council of ministers, `https://portal.health.fgov.be/pls/portal/url/ITEM/0C3B1578D04B41A1E0440003BA383584`.

[66] Decree of 16 June 2006 concerning the Health Information System, (*M.B.* 7 September 2006).

[67] Art. 3-4 Decree Health Information System.

[68] Art. 2 8°and art. 6 ff. Decree Health Information System.

[69] Art. 13 ff. Decree Health Information System.

[70] Art. 13 §2 Decree Health Information System.

[71] Art. 14 Decree Health Information System.

not be divulged in the course of information shared outside the Flemish Health Information System unless the recipient of the information has authorisation use the pseudonym.[72]

Actual sharing of electronic summaries or – where possible – the patient records with other health care providers requires consent of the patient as a rule. In a number of cases, consent is presumed to be given unless the patient protests explicitely against sharing of his data.[73] The implicit consent approach is controversial and was criticized by the Privacy Commission.[74]

To date, no further measures have been adopted by the Flemish Government in execution of the Decree Health Information System.

9.4 Conclusion

To date, a large subcategory of prescriptions for medicine must still be issued in paper form, namely those issued to non-hospitalized patients which must comply with a model form. Prescriptions issued inside hospitals may be in electronic form and some hospitals have implemented electronic prescription applications.

The legal rules most commonly applied to electronic applications – the e-Signatures Directive, the e-Commerce Directive, the Services Directive, and their respective implementing national regulations – do not fit well with the eHealth context. The Services Directive explicitely excludes health care services provided to patients, thus excluding the activities of doctors and pharmacists in relation to patients. Doctors and pharmacists cannot be considered information society service providers, simply because they issue or handle electronic prescriptions. Only the MPAs may fall within the definition of a service provider and an information society service provider under these regulations. Though electronic prescriptions make use of electronic signatures in a way, this would appear insufficient to consider any of the parties involved as a certification service provider. The non-applicability – to a large degree – of these regulations entails that Belgium is by and large allowed to impose its own rules to electronic prescriptions and the parties that handle them.

Data protection regulation has a major impact on any application that involves processing of medical data. The broad interpretation of the notion of personal data in Belgium, poses some challenges for data processors who are deemed to process personal data, without actually being able to identify the persons in question themselves. In the electronic prescription scenario, this can be solved by way of an agreement amongst the data processors involved detailing who will fulfill the Data Protection Act's obligations for all of them.

[72] Art. 21 Decree Health Information System.

[73] Art. 19 Decree Health Information System.

[74] Advice nr. 05/2004 regarding the Flemish Government's proposal for a health information system, available at `http://www.privacycommission.be/`.

10 Conclusion and Future Work

We have presented a new design for a privacy-preserving electronic healthcare system that uses the Belgian eID card. The system we present is highly compatible with the current health practice in Belgium, and tries to maximize the protection of the identity and health records of the patients as long as they do not engage in fraudulent behavior. Furthermore, our system can be optionally parametrized to increase the doctors privacy (e.g., by hiding their identity, and their prescription habits.) Since, in practice, an e-health transaction is a multiparty procedure, we make sure that each party involved learns only the information it is supposed to have access to. To achieve this we adopt a conservative access control policy, and put in measures to block any data leakage that may result from possible inference channels.

In the present deliverable, our main focus has been on the issue of prescription handling, and that of protecting newly created health records. A future line of research would include studying ways to protect previously created and archived records. Further extensions may cover topics such as :

- **Delegation of prescriptions.** The patient will not always be able to go to the pharmacist on own power. Therefore one of his relatives must be able to buy the medicines in place of the patient. However, the patient must still give his/her authorization.
- **Partially used prescriptions.** A doctor can prescribe multiple medicines to the same patient during the same consultation. The pharmacist might not have everything in stock while some medicines are urgent. The patient must be able to get a part of the medicines and to buy the other medicines at some later moment.
- **Adaptability.** The e-health use cases did change in the past and will change in the future. The privacy-friendly implementation described in this deliverable will thus have to change as well. A future research topic could be to develop methods to generate and adapt such protocols in a quick and easy way.
- **Delegation of access rights.** In a hospital, the patient will give the hospital access to his EHRs. These rights must be tied to the main treating doctor, who must be able to delegate subrights to e.g. a nurse.
- **Medical certificates.** Medical certificates can be issued by the doctor to a patient. These contain medical data that is relevant in daily or professional life. E.g. a medical credential could state that the owner is disabled and thus has the right to park his/her car on a disabled-people only parking place. For public safety, some medical certificates must not be hideable on request by an authorized party. E.g. a psychopathic must not be given a weapon license.

References

[1] N. Asokan, Victor Shoup, and Michael Waidner. Optimistic fair exchange of digital signatures (extended abstract). In *EUROCRYPT*, pages 591–606, 1998.

[2] M. J. Atallah and W. Du. Secure multi-party computational geometry. In *WADS2001: Seventh International Workshop on Algorithms and Data Structures*, pages 165–179, Providence, Rhode Island, August 2001.

[3] Endre Bangerter, Jan Camenisch, and Anna Lysyanskaya. A cryptographic framework for the controlled release of certified data. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols Workshop*, volume 3957 of *Lecture Notes in Computer Science*, pages 20–42. Springer, 2004.

[4] S. A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, Cambridge, MA, USA, 2000.

[5] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT*, pages 93–118, 2001.

[6] Jan Camenisch and Ivan Damgård. Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes. In *ASIACRYPT*, pages 331–345, 2000.

[7] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, pages 93–118, London, UK, 2001. Springer-Verlag.

[8] Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. In *CRYPTO*, pages 126–144, 2003.

[9] Jan Camenisch, Dieter Sommer, and Roger Zimmermann. A general certification framework with applications to privacy-enhancing certificate infrastructures. Technical report, IBM Research, Zurich Research Laboratory, 2006.

[10] Chul-Joon Choi, Zeen Kim, and Kwangjo Kim. Schnorr signature scheme with restricted signing capability and its application.

[11] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Zhu. Tools for privacy preserving distributed data mining. *ACM SIGKDD Explorations*, 4(2), 2003.

[12] European Communities. Handbook on implementation of the services directive. Technical report, Office for Official Publications of the European Communities, Luxembourg, 2007.

[13] Joan Daemen and Vincent Rijmen. Rijndael for aes. In *AES Candidate Conference*, pages 343–348, 2000.

[14] Ivan Damgård and Eiichiro Fujisaki. A statistically-hiding integer commitment scheme based on groups with hidden order. In *ASIACRYPT*, pages 125–142, 2002.

[15] Liesje Demuynck and Bart De Decker. Privacy-preserving electronic health records. In *Communications and Multimedia Security*, pages 150–159, 2005.

[16] Liesje Demuynck and Bart De Decker. Credential-based systems for the anonymous delegation of rights. Technical Report CW468, K.U. Leuven, 2006.

[17] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[18] Oded Goldreich. *Foundations of Cryptography*, volume Basic Tools. Cambridge University Press, 2001.

[19] Health level 7 (hl7). http://www.hl7.org/.

[20] Hl7 reference information model. http://www.hl7.org/library/data-model/RIM/modelpage_non.htm.

[21] R. Housley, W. Polk, W. Ford, and D. Solo. Rfc3280: Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile, 2002.

[22] Integrating the healthcare enterprise. http://www.ihe.net/.

[23] International Organization for Standardization. *ISO/IEC 10118-3:2004: Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*. pub-ISO, February 2004.

[24] ITU-T. Recommendation x.509: The directorypublic key and attribute certifcate frameworks. Technical Report Technical report, ITU-T, 1997.

[25] ITU-T. Recommendation x.509: The directorypublic key and attribute certifcate frameworks. Technical Report Technical report, ITU-T, 2000.

[26] Murat Kantarcioǧlu, Jiashun Jin, and Chris Clifton. When do data mining results violate privacy? In *KDD '04: Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 599–604, New York, NY, USA, 2004. ACM Press.

[27] Reto Krummenacher, Elena Paslaru Bontas Simperl, Lyndon J. B. Nixon, Dario Cerizza, and Emanuele Della Valle. Enabling the european patient summary through triplespaces. In *CBMS*, pages 319–324. IEEE Computer Society, 2007.

[28] Etienne Montero, Marie Demoulin, and Christophe Lazaro. La loi du 11 mars 2003 sur les services de la société de l'information. *J.T.*, pages 81–95, 2004.

[29] National Institute of Standards and Technology. Digital signature standard (dss). Technical Report FIPS-186-2, NIST, 2000.

[30] National Institute of Standards and Technology. Data encryption standard. Technical Report FIPS Publication 46-2, NIST, December 1993.

[31] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO*, pages 129–140, 1991.

[32] R. L. Rivest, A. Shamir, and L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. Technical Report MIT/LCS/TM-82, MIT, 1977.

[33] Latanya Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):571–588, 2002.

[34] Latanya Sweeney. k-anonymity: a model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):557–570, 2002.

[35] Svetlena Tavena, Philippe Palanque, Sandra Basnyat, Marco Antonio Winckler, and Effie Law. Analysis of communication breakdowns for ehealth systems design. In *Nordic Conference on eHealth and Telemedicine (NCeHT), Helsinki, Finland,, 31/08/2006-01/09/2006*, page 212, 2006.

[36] Svetlena Tavena, Philippe Palanque, Sandra Basnyat, Marco Antonio Winckler, and Effie Law. Clinical application design: Task modeling with failure in mind. In *World Congress on Internet in Medicine (MedNet), Toronto, Canada, 15/10/06-18/10/06*, 2006.

[37] E. Della Valle, L. Gadda, and V. Perdoni. COCOON: Building knowledge driven and dynamically networked communities within european healthcare systems, April 06 2005.

[38] Patrick Van Eecke and Dumortier Jos, editors. *Elektronische Handel*. Die Keure, Brugge, 2003.

[39] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, and Y. Theodoridis. State-of-the-art in privacy preserving data mining. *ACM SIGMOD Record*, 3(1):50–57, March 2004.

[40] Marc Wilikens, Simone Feriti, Alberto Sanna, and Marcelo Masera. A context-related authorization and access control method based on rbac:. In *SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*, pages 117–124, New York, NY, USA, 2002. ACM Press.

[41] X. Elektronisch medicatievoorschrift raakt stilaan ingeburgerd. *Virghaal Nieuws*, 5, Februari 2003.