Digital Patient Assistants

—Privacy vs. Cost in Compulsory Health Insurance—

Gerrit Bleumer
AT&T Labs-Research, USA *

Matthias Schunter
Universität des Saarlandes, Germany †

November 1, 1998

Abstract

Many countries have a compulsory health insurance system in place. Compulsory health insurers charge income related fees as opposed to private health insurers who charge risk related fees. Compulsory health insurance is based on solidarity among policy holders and can give them more privacy than any private health insurer can. As an example, we consider the German health insurance system, and we discuss how the charging and clearing of medical services can be implemented so as to support both the legitimate privacy interests of patients and physicians and the health insurer's interest to control the overall cost. We present a cryptographic solution that is based on digital patient assistants, i.e., personal palmtop computers, organizers or PDAs. Patients are thus able to manage their own health insurance certificates, referrals and prescriptions. Although still too expensive for large scale introduction, digital patient assistants have a number of significant advantages over any chip-card or paper based system: (i) significantly more efficient and reliable data communication between the various health care providers involved in treatment; (ii) real patient privacy through direct and offline communication between digital patient assistants and physicians' practices; (iii) a huge potential to develop telemedicine in a privacy oriented way. Finally we present one possible implementation in more detail. We also show how compulsory health insurers can use our solution to control their overall costs.

1 Introduction

In most western democracies the increasing diversification of healthcare providers and competition between them provides pressure for lean administration, charging and clearing. As more and more computers become networked, we can expect the integration of almost all healthcare related processes between physicians, hospitals, online medical

*Shannon Laboratories, 180 Park Avenue, Florham Park, NJ 07932-0971, ph: +1 973 360 8347, fax: +1 973 360 8970, e-mail: `bleumer@acm.org`

†Fachbereich Informatik (Geb. 45), Im Stadtwald 45, D 66123 Saarbrücken, ph: +1 49 681 302-5608, fax: +1 49 681 302-4631 e-mail: `schunter@acm.org`

databases, pharmacies, health insurers, and so on. However, the legitimate privacy interests of patients and physicians are likely to be ignored if today's paper-based procedures are naively simulated by networked computer systems. We show electronic solutions for charging and clearing expenses which allow insurers to enforce an annual limit on total expenditure while maintaining the privacy of patients and physicians.

Former and current paper-based procedures have relied heavily on identifiable patient data in order to ensure data integrity and accuracy. Although in many countries data protection laws apply to such information, the most effective protection against privacy breaches still is the cost of collecting, transferring, storing and analysing large volumes of paper files. Patients usually accept that they will have little if any privacy against healthcare professionals directly involved in their treatment, but wish to protect their privacy against outsiders like healthcare insurers, attorneys, employers and landlords.

The transition from a paper-based healthcare environment to one based on networked computers is unlikely to respect the distinction between medical and non-medical parties. Firstly, the interaction of clinical and non-clinical participants in the treatment process will be rationalised by computers in just the same way as the interaction between the clinical participants. Secondly, both integration processes are driven by the same medium: the Internet. Finally, some non-medical parties have legitimate and illegitimate interests in identifiable patient data. So the easier it is to access, transfer, store and analyse large amounts of data, the more we must protect identifiable patient data; and if these protection measures are to be effective, they will have to be built into the technical infrastructure.

On the one hand, the new technologies support new potential abuses of medical data for surveillance, control and marketing purposes [26, 34], while on the other hand they also facilitate a new level of privacy, by enabling systems to be built which avoid the storage of large amounts of identifiable patient data in central repositories. One particular solution which we will explore here is to equip patients with digital patient assistants. We envisage these devices to be mobile user devices like palm pilots, personal digital assistants or other mobile user devices [30]. Digital patient assistants can help to develop telemedicine in a way that respects the privacy of patients and physicians alike. They can also help patients to avoid prescription errors [35, 36] and to better manage chronic diseases like diabetes [20] or cancer.

Healthcare providers are about to invest millions in new communication and computing infrastructures [37, 22]. The market for chip-cards for both patients and physicians is expected to grow rapidly within the next few years. However, such investments will only be worthwhile if the fielded technologies can support legal requirements such as data protection, and if they are found acceptable by all participants from patients through clinical professionals to health insurers. The G7 and some national initiatives [11] have stimulated such technologies, the topic has been suggested for further research to the Commission of the European Communities [3, 4] and specific solutions for the US market are under development [24, 25].

To derive an acceptable solution we will state the duties and goals of each participant and then answer the key question:

Who needs what data in order to fulfill their duties and meet their goals?

We will then discuss suitable technical measures for implementing the charging and clearing process in a privacy oriented way. Our analysis indicates that chip-cards are too restricted to really protect the privacy of patients and physicians. Shorter precursors of this paper appeared in [6, 7].

2 Contractual Framework

We will now describe the participants and transaction flows of the German healthcare system [1, 10, 23] with respect to billing and payment for medical services. We will then deduce the security interests of the various participants.

The German healthcare system[1] consists of five supply sectors [1, 12]. *medical outpatient treatment* includes registered physicians and specialists, e.g., dentists, who have their own independent practices. *paramedical outpatient treatment* includes members of professions allied to medicine like physio-therapists and speech therapists. *inpatient treatment* consists of all hospitals for acute cases and special hospitals. *public health services* are provided by state and local public health departments and by the laboratories. The *pharmaceutical supply* is provided by pharmacies.

Health insurers are the clearing houses of the healthcare system. In practice they delegate the clearing tasks to several client-specific organisations (*actual clearing houses*). There are compulsory and private health insurers, each with about half the market in healthcare payments. Roughly speaking, contributions to the former are income related, whereas those to the latter are risk-related. There is a level of income below which compulsory health insurance is mandatory. The privacy interests of patients (and physicians) inherently conflict with the screening interests of private health insurers to such an extent that we suggest our solution for compulsory health insurers only.

Throughout this paper we distinguish four kinds of *healthcare providers* and sketch their business relationships in (Fig. 1).

1. *Registered physicians* are outpatient general physicians or specialists who are registered by compulsory health insurers. They may provide medical treatment, issue prescriptions for medication or paramedical treatment and write letters of referral. They do not claim directly to the health insurers, but to the local associations of registered physicians: Kassenärztliche Vereinigungen (KV). These also serve as clearing houses: Each KV gets a lump sum from the compulsory health insurers and pays the invoices of registered physicians. The registration is done by a joint registration committee of the health insurances and the KVs.

2. *Pharmacies and paramedical providers* serve patients more or less according to prescriptions. The may neither issue prescriptions nor write letters of referral. Their actual clearing houses are the health insurers.

3. *Hospital physicians* are physicians who are registered by compulsory health insurers and who are employed by a hospital. Like registered physicians, they may provide medical treatment, issue prescriptions for medication or paramedical treatment and write letters of referral. They do not claim directly from the health insurers either, but from their hospitals which serve as their first line clearing houses.

[1] A German-English and English-German glossary of the German healthcare system is found in [1].

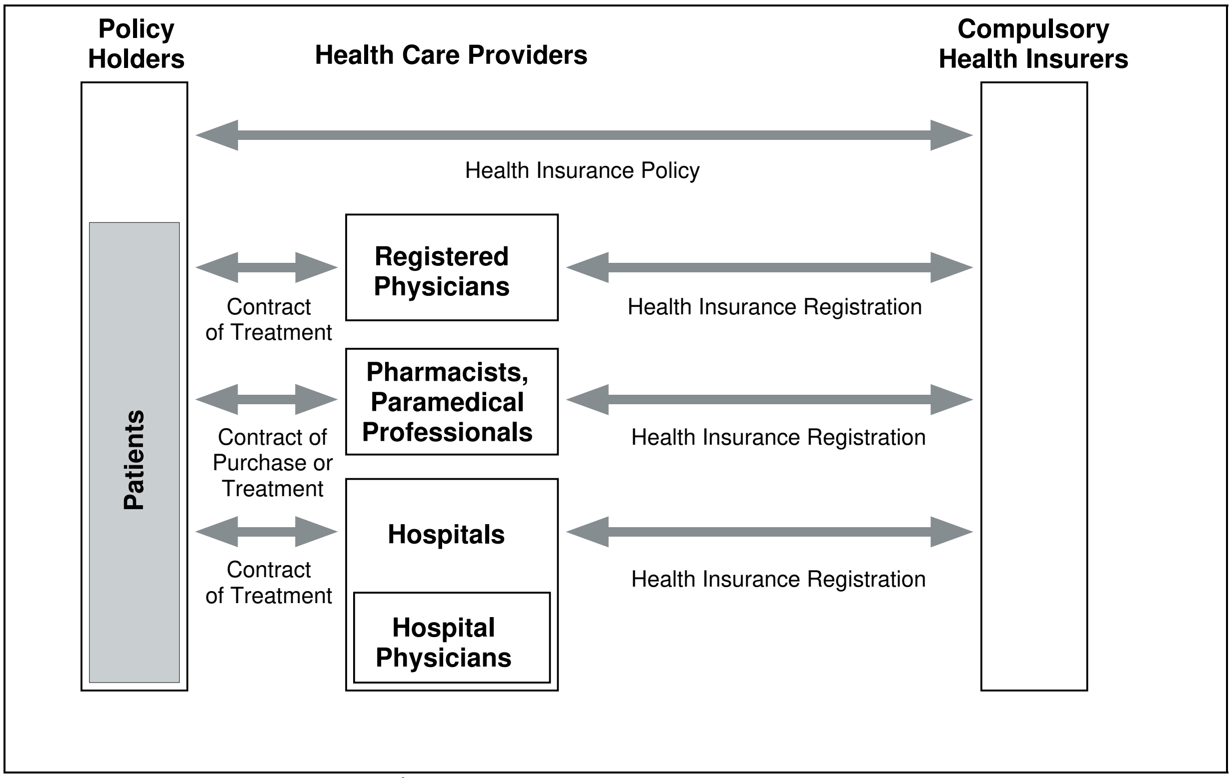

Figure 1: Contractual Framework

4. *Specialists* are all those outpatient and hospital physicians who provide medical treatment according to letters of referral.

3 Paper-based Charging and Clearing

We will now describe in more detail how the costs of medical treatment and supplies are claimed in the German system. Interactions between two participants consist of "real" actions and of "paper" actions. For example, a physician treats a patient, sends an invoice for the treatment and is finally reimbursed. We regard the first and last of these actions as "real" and the second as a paper action. Our focus is on electronic transactions substituting the paper actions, particularly those containing identifying patient data (Fig. 2).

Consider a typical treatment process: A patient requests treatment from her GP by presenting a valid health insurance card ("Krankenversichertenkarte"), which contains the data necessary for charging medical treatment. The GP may provide some treatment on his own and in addition:

1. prescribe some medication, and

2. refer the patient to a specialist or hospital.

During the process of healthcare, these steps can be iterated with various medical professionals taking responsibility for the patient and delegating it further. In each of the three cases, the GP produces a medical record that contains accounting data and

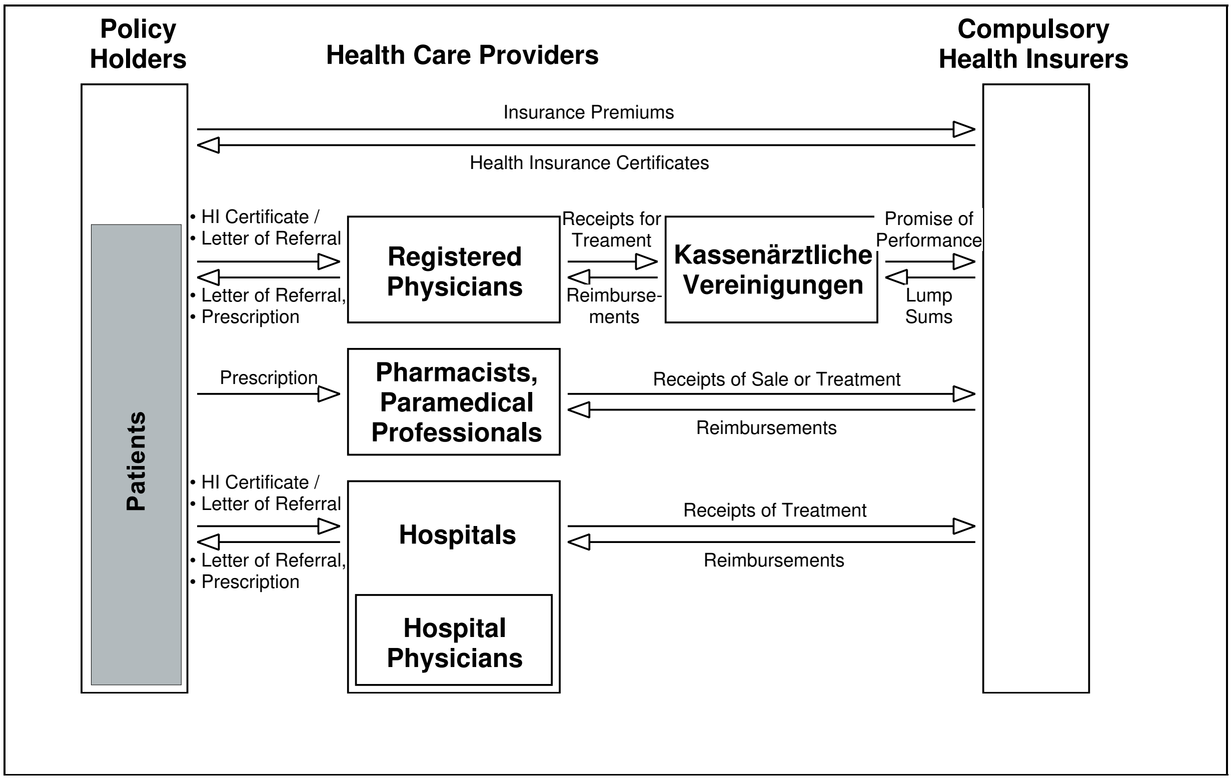

Figure 2: Flow of Information in the German Healthcare System (simplified)

possibly diagnostic, therapeutic or prognostic information about the patient. Usually, the patient passes a relevant excerpt of this record to the next healthcare provider, who then continues the process of treatment. Each healthcare provider copies the relevant part of the patient's record and forwards it to the appropriate clearing house with his invoice.

3.1 Analysis

Since 1992 the compulsory health insurers have equipped their policy holders with personal health insurance cards ("Versichertenkarten"). These are memory chip cards containing the same administrative data that had previously been held on a paper-based health insurance record card ("Krankenschein"). If a patient requests a medical service from a healthcare provider, she has to identify herself by her health insurance card. This is basically a way to enforce the identification of patients – the primary requirement of health insurers. The patients' privacy requirements, however, have simply been ignored.

The paper-based refund system implements a kind of post-paid system. Health insurance cards can be regarded as special kind of credit cards. Showing them allows a patient to get treatment. The patient's health insurer pays lump sums to the various clearing houses which reimburse expenses that are properly supported with receipts.

Alternatively, healthcare providers could also claim directly to the patients, as most private insurers do (such as private health or car insurers). In this case, policy holders get to know the detailed cost of their treatment and could, if suitably motivated, help to control costs by asking their healthcare providers for less expensive services and checking all invoices carefully. They might also occasionally decide not to use their health insurer but to pay some items themselves.

Usually, receipts for everyday's commercial transactions do not contain much personal information about the payer; but receipts in healthcare are different. In paper-based systems the invoices of the healthcare providers and thus the receipts received by the clearing houses contain a tremendous amount of highly personal and sensitive information about both patients and physicians. For example, every participant involved gets to know each patient's prescription, and with private insurers, all documents referring to a patient are linked from the treating physician through to the insurer. The mere existence of such information tempts people to use it for secondary purposes.

3.2 Participants and Their Specific Security Requirements

We now ask which participants really need to have which information in order to fulfill their tasks. We will analyse the services to be provided by each participant and then consider additional constraints posed by the specific confidentiality and privacy needs of the various participants.

3.2.1 Availability and Integrity Requirements

PHYSICIAN: Each patient shall receive no more treatment and medication than is prescribed. In particular, each prescribed treatment shall be provided at most the specified number of times. (This is all the more important if drugs are dispensed by robots [31].)

POLICY HOLDER: If she presents a valid enrollment authorisation in a suitable health plan and a letter of referral or prescription to a healthcare provider of her choice, then the provider shall indeed offer the requested service or perform the treatment prescribed.

PHARMACIES AND PARAMEDICAL PROVIDERS: Any of their expenses should be reimbursed by the health insurers if the healthcare provider is registered and if the claims are properly supported by proof of treatment.

HEALTH INSURERS: Only registered physicians should be able issue prescriptions. Each policy holder should be able to use prescriptions at most once or according to a therapy plan, respectively. Each health insurer should reimburse expenses only once and only if they have been spent for its own policy holders. Health insurers should be able to cap the total reimbursement per year ("Deckelungsprinzip").

Healthcare providers usually need some administrative details of their patients, but much less personal data needs to be communicated between providers. Patients need non-repudiable prescriptions from their physicians. Providers need to verify the prescriptions before giving treatment or medication. They also need to obtain receipts. In paper-based practice, the medical prescription serves for both purposes. But although the insurers need to know the identity of their policy holders, and physicians usually know their patients well, the two do not usually need to be linked. A patient pseudonym is usually quite sufficient for charging. We will see a few exceptions when we discuss particular implementations of the charging and clearing process in Section 4.

3.2.2 Confidentiality and Privacy Requirements

Physician and Patient: Medical treatment requires a relationship based on trust between patient and physician. The *privacy* of their relationship should be protected comprehensively against third parties' interests; diagnoses and therapies should be strictly confidential. This specific rule should override, for example, any obligations to escrow cryptographic keys [27].

Physician Health insurers should not in general be able to monitor physicians' prescription and treatment habits. The cost control interest of health insurers does not justify more detailed control than can be exercised using statistical mechanisms, such as spot-checking a small sample of treatments.

Policy holder: The policy holder's right to ask a healthcare provider of her choice for second opinions implies that different healthcare providers should not monitor policy holders by exchanging views on them. In certain situations, patients might seek a stronger form of privacy, which we will call *untraceability*: even where a patients is referred from one provider to another, they cannot collude to link their views afterwards and find out which records belong to the same patient.

Obviously, the above requirements can be met by legal regulations, but technical means are more effective – especially if they can be enforced by the policy holders themselves. Therefore, we introduce pseudonyms for policy holders as well as for physicians and we propose to employ them consistently in all interactions [28, 29].

3.3 Exceptions

Exceptional cases must be supported because the physician in charge of a patient is ultimately liable for how the patient is treated and may require flexibility. For example, one must be able to deal with emergencies in which the patient is not able to confirm or consent to anything, and cases where a physician decides not to tell the whole story to his patient.

4 Implementation Options

We now discuss the most important implementation options of the charging and clearing process of a healthcare system. We basically consider compulsory health insurers who provide broad coverage of medical expenses. So it is realistic to assume that individuals are enrolled in at most one insurer's health plan. The case of enrollment in multiple insurance plans will be considered below in Section 4.8.

Healthcare insurance is based on a critical separation of duty. Physicians decide about therapies and prescriptions, whereas insurers finance the corresponding treatments and medications. Since the physicians' decisions considerably affect the cost, physicians may need to be authorised by health insurers before they can charge any medical treatment. Similarly, pharmacies and paramedical providers are authorised by insurers. Both types of authorisations are called *registration*.

There are three other types of authorisation, namely a patient's proof of enrollment in a health-insurance plan, a referral to a specialist, and a prescription, which we will describe in detail in Section 5.1. In principle, these authorisations should be non-repudiable and unforgeable, i.e., a principal who has obtained any of them should be able to prove in court that they hold it, but it should be practically impossible to obtain any of these authorisations illegitimately. These common requirements suggest that we implement all authorisations by cryptographic primitives based on digital signatures [21]. (For additional privacy-protecting properties see Section 4.2.) An implication of using digital-signature-based mechanisms is that healthcare providers need not trust the health insurers, because, if need be, the providers can prove all their claims to an arbiter such as a court.

Given that patients are mobile, we assume a system architecture in which each policy holder is equipped with a digital patient assistant, i.e., a mobile user device [30] able to manage authorisations and in particular to produce and verify digital signatures. We further assume that each healthcare provider has equipment to communicate with digital patient assistants. Good candidates for digital patient assistants are palm pilots and palmtop computers. They are more appropriate than smartcards because they include a user interface and power supply and tend to have more computing power and storage capacity.

4.1 Enrollment and Prescription Authorisations

The different dynamic types of authorisations are characterised as follows (Fig. 3):

*Patients' enrollment authorisations (*E-authorisation*)* prove that the requested medication, treatment or other service is covered by a health insurance plan. Different health insurance plans may vary in coverage, deductions, fees, and so on; and while individuals are not supposed to give away or sell their enrollments as such, they should have enough power of delegation to ask a friend or relative to go and get a prescribed medication for them. Furthermore, the patients' privacy should be maintained as much as possible even if the health insurer and the physician collude.[2] To provide the strongest protection, we need to provide for patients to use pseudonyms when they enroll at their insurer.

*Patient's referral authorisations (*R-authorisation*)* prove that they have been referred to a hospital or a specialist. In order to be treated, they need to use an enrollment authorisation and a prescription authorisation.

*Patient's prescription authorisations (*P-authorisation*)* prove that a requested medication or service has been prescribed once (or a fixed number of times). In order to get medications or services, policy holders need to use their enrollment authorisation and a prescription authorisation, or send someone else equipped with these authorisations.

Since enrollments, prescriptions and referrals can be issued by different parties, it appears most natural to implement them separately by enrollment authorisations, prescription authorisations and referral authorisations, respectively; the digital patient assistant can bundle them in the necessary combinations for each healthcare encounter. This raises issues of pseudonym management but can also allow patients some freedom to negotiate their purchase with the pharmacy or other provider. For example, they might negotiate

[2]Note that we do not assume that the patient as a person is anonymous but rather that the clearing and billing is anonymous, and that no publicly readable data identifies a patient. We cannot of course stop physicians storing their patients' names in their local files.

with the pharmacist for a drug similar to that prescribed[3] (Fig. 3).

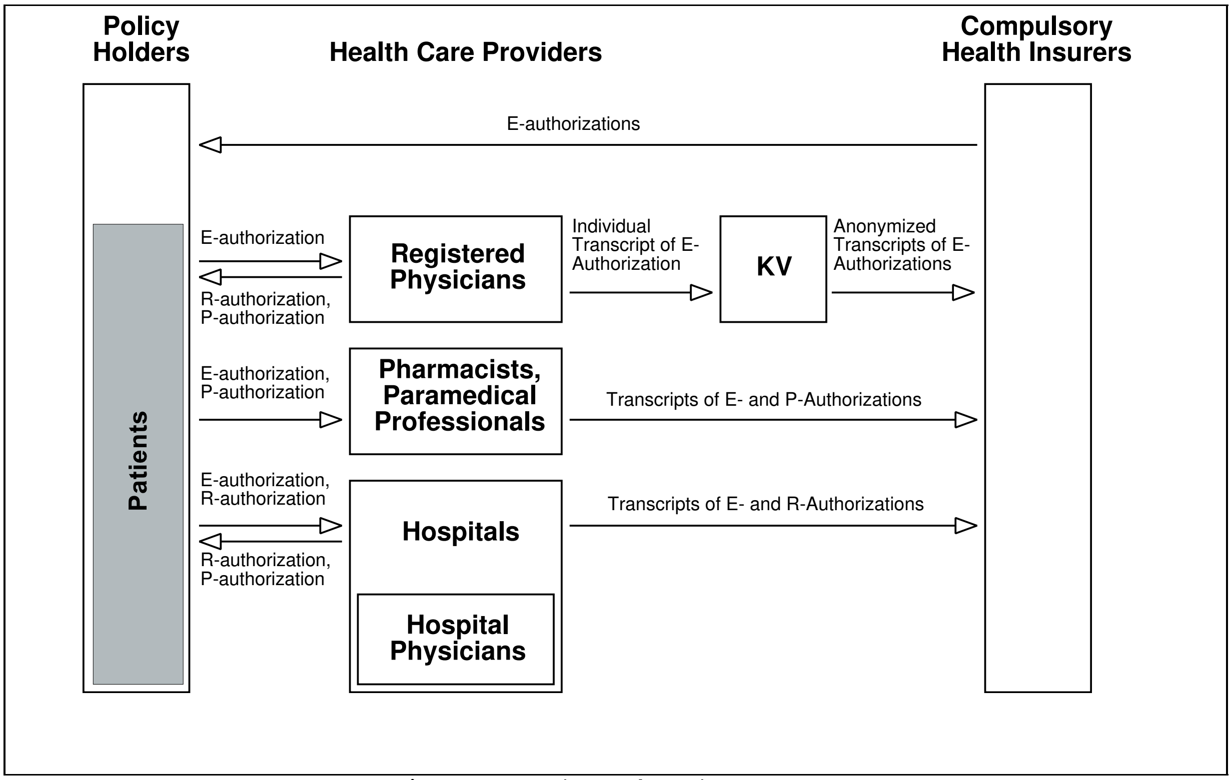

Figure 3: Flow of authorisations

4.2 Anonymity Options

Our goal is to implement all authorisations and the charging of expenses in a way that maintains the privacy of patients and of physicians against the insurer. Individuals act as policy holders to the insurer and as patients to the provider. In neither of these roles do they decide about the cost to be incurred, so they may use different pseudonyms with each health insurer, physician, pharmacy and other provider. These pseudonyms may be unlinkable. In addition, patients who are referred from one physician to another can be untraceable by these physicians. Similarly, patients who receive and fulfill prescriptions can be untraceable by the providers involved. We suggest implementations for additional traceability in Section 4.4.

Physicians are different in that they decide (indirectly) about which patient gets what amount of reimbursement from the health insurer. So we want physicians to remain anonymous as long as they act honestly, but be identifiable after the fact if they fake bills or charge for overly expensive treatment. This affects physicians' registrations, referral-authorisations, prescription-authorisations and charging. An effective way to achieve recoverable anonymity is to form groups of physicians and to enable each member of a group to sign on behalf of the group without revealing their individual identity. However, in case of a dispute later on, the group should be able to re-identify any members by their signatures. In principle, physicians' groups can be managed by the KVs since the

[3] What "similar" means has to be negotiated between purchasers and providers beforehand.

health insurers usually pay lump sums to the KVs, which then redistribute the payments to individual physicians.

In order to provide sufficient anonymity for physicians and patients alike, the physicians' groups should contain a mix of different specialists and general practitioners and not only a few of each. For example, one could group the practitioners of a geographical region, or the physicians of one or more hospitals, etc. The appropriate size of these groups depends on the level of anonymity required, the efficiency of the underlying mechanisms, and additional constraints of the KVs. In the following, we assume a group size of about 100 physicians.

Keeping pharmacies and other providers anonymous is of little use because they do not reveal much more information about patients than what the health insurer learns from prescriptions anyway.

4.3 Cryptographic Building Blocks

Next we sketch the different cryptographic primitives which can be used to realise such a system; they are adapted from mechanisms developed for electronic banking and commerce applications. Some primitives require a tamper resistant module to be implanted into each digital patient assistant. This module is called an *observer* [18] and is encapsulated by the digital patient assistant in such a way that outside communication partners cannot leak any information into the observer (inflow) nor that the observer can leak any information to outside communication partners (outflow).

Pseudonyms: A pseudonym is a digital identity. The strongest privacy is achieved if each pseudonym is used only once. If two participants interact with each other multiple times, they often know each other anyway and therefore can re-use the same pseudonyms. In our application, a policy holder uses one pseudonym with her health insurer, and is free to use one or more pseudonyms for each physician, pharmacy and paramedical provider.

A *digital signature* [21, 33] for some message can be produced by anyone who has previously chosen a private signing key. Once the corresponding verification key is published, everyone can verify the signed message by that verification key (see Section 5.1.1).

A *credential* [14] is a digital signature for a pseudonym. The pseudonym for which a credential is obtained is called the *source pseudonym* and any pseudonym for which the credential is used later is called a *target pseudonym*. The purpose of a credential is to prove an authorisation of the holder, without allowing the issuer and the recipients to link their views of the holder. A credential can be used *offline* if the recipient requires no third party online to accept a credential. Some credential mechanisms require encoding the holder's identity into the source pseudonym and the cryptographic implementation then ensures that the same identity is present in every target pseudonym. We call these *identity based pseudonyms*.

A *personal credential* [5] is a credential that can be used arbitrarily often, but cannot be transferred between individuals. It is based on some biometric verification facility inside the observer of each digital patient assistant. So even giving away one's digital assistant (let alone its loss or theft) does not allow others to use the legitimate owner's credentials. For privacy reasons, we only consider personal credentials that are verifiable offline (see Section 5.1.2). The non-transferability of offline usable personal credentials must rely on the tamper resistance of the observer and its biometric verification facility.

A *coin credential* (also called electronic cash [8, 9, 16]) is a credential that can be transferred between individuals, but can be used only once. The issuer of a coin credential ensures that the holder's identity is encoded into the source pseudonym. This identity is not recoverable from the pseudonym unless it is used twice. Double use can be prevented if recipients share an online database of target pseudonyms and accept only coin credentials whose target pseudonyms have not been used before. If two coin credentials are used for the same target pseudonym, then the database has all the information needed to identify the double user. Double use can also be prevented offline by an observer within each digital patient assistant if the observer is required to co-operate in every use of coin credentials. In case it finds a double use, it simply refuses to use this coin credential again. A special case of coin credentials are *check credentials*. At issuing time, a maximum "value" is fixed, and the holder is free to use it later for any amount not exceeding the initial value.

A *group signature* [13, 17, 19] is a digital signature that is verified by a group's verification key. Members of the group can sign in behalf of the group without revealing their individual identity. Groups are administered by certain centers, who manage the admission and suspension of group members. In case of a dispute, the group center can re-identify any of its members by their signatures (see Section 5.1.3).

A *group coin credential* is a coin credential where the digital signature is a group signature. The purpose of a group coin credential is to maintain the holder's and the issuer's privacy (see Section 5.1.4).

4.4 Implementing the Authorisations

Physicians' registrations are usually obtained permanently, i.e., physicians can exercise them as often as they like (limited only perhaps by their age). So the following implementation appears natural: Physicians choose their personal signing keys and have them certified by the health insurer. Finally the KVs admit physicians who provide certified signing keys to certain groups. Furthermore, physicians authorise their invoices for treatment and the prescriptions to their patients by a group signature.

Enrollment authorisations could be implemented by personal credentials. This appears most natural, but makes it difficult for patients to ask a friend or relative to exercise an enrollment for them since personal credentials are non-transferable. Enrollments can also be implemented by coin credentials. When enrolling in a health insurance plan, a policy holder could obtain a batch of coin credentials and could later give away one of them to a friend or relative if the need arises. The easiest way is to configure one's digital assistant to support only the intended purchases and then lend it to a friend or relative. For the same reason however, an implementation by coin credentials probably requires non-digital means to discourage their transfer between individuals. For example, personal devices could have a portrait of their respective owners imprinted. If health insurers want to distinguish different types of enrollment authorisations (e.g., medical treatment, dental treatment, etc.), then for each type the most appropriate implementation can be chosen.

Referral and prescription authorisations need to maintain the issuing physicians' privacy in a way so that the provider can endorse its invoice properly without revealing the identity of the issuing physician. Hence referral and prescription authorisations could be implemented by group signatures or by group coin credentials. Both implementations reveal to the health insurer only the group to which the issuing physician belongs, but not his identity. In case of a dispute, his identity can be reconstructed by help of the group. The groups for issuing referrals and prescriptions can be the same as those for registration because they serve the same purpose, i.e., maintaining the physicians' privacy against insurers.

Group coin credentials differ from group signatures by an additional level of privacy for the policy holders. If referral or prescription authorisations are implemented by group coin credentials, then even if all health care providers collaborate, they could not determine whose referrals or prescriptions are used where. Otherwise, the health care providers could link all their views on the patients. If the health insurer could get hold of data collected at the providers, then it could correlate patients' addresses with the locations of their hospitals, physicians and other providers. In order to protect the patient physician relationship, this additional level of privacy is recommended for referral authorisations. It seems however less important for prescription authorisations, because pharmacies and paramedical providers are not anonymous to health insurers anyway.

4.5 Charging of Medical Treatment

If physicians want to charge for treatment, they first need to see an enrollment authorisation from their patients, so to learn which insurance plan to bill. In the current paper-based system there is little control of what treatment physicians provide and what they later charge for. In particular, the compulsory insured patients do not learn what expenses their physicians claim. This can be implemented as follows: Physicians sign their invoices, endorse them with a proof that the patient is properly enrolled and send them to their KV. The KV keeps the identifiable invoices in its files, sums them up into global invoices and sends them to the health insurer on a regular basis. When the health insurer reimburses a lump sum, the KV pays the physicians.

Alternatively, physicians could send their invoices directly and anonymously to the health insurer by signing with a group signature. The anonymous channel between physicians and health insurer can be implemented by various redirecting techniques such as MIXes [15], crowds [32], and anonymous remailers [2]. The KV could also provide such a service. This latter solutions is likely to achieve more timely reimbursements than the former.

If health insurers want more control, they could ask their policy holders to consent to each medical treatment as a condition of reimbursement. Here are two implementations, the first more patient privacy protecting than the second:

- Patients provide a proof of enrollment that is customised to the treatment they consent to. The customised proof can be obtained by implementing enrollment authorisations by check credentials that can be filled in by the patients before use.

- Patients consent by signing their treatment with an ordinary digital signature. The physicians keep the signed reports with the patient's record. If a health insurer detects that some budget is exceeded, it may ask for patients' signed consent. In addition, the KVs may spot-check physicians, i.e., ask for the consent of randomly selected patients.

In any case, some exception handling is necessary if a patient cannot or will not consent to a treatment.

4.6 Charging of Specialist Treatment, Medication and Paramedical Treatment

When visiting a specialist, the patient must use referral and enrollment authorisations. Similarly, when visiting a pharmacy or a paramedical provider, he must present a prescription and an enrollment authorisation. In each case, both authorisations will be accepted only if they are used for the same target pseudonym. Otherwise, collusions of policy holders could join all of their authorisations even without breaking the tamper resistance of their observers. The idea of matching pseudonyms is sketched in Fig. 4. An enrollment authorisation E is issued to a policy holder for a source pseudonym $\triangle$. Later a physician issues a referral or prescription authorisation R/P to the same policy holder for source pseudonym $\bigtriangledown$. Finally, the patient can use both authorisations only for the same target pseudonym $\circ$.

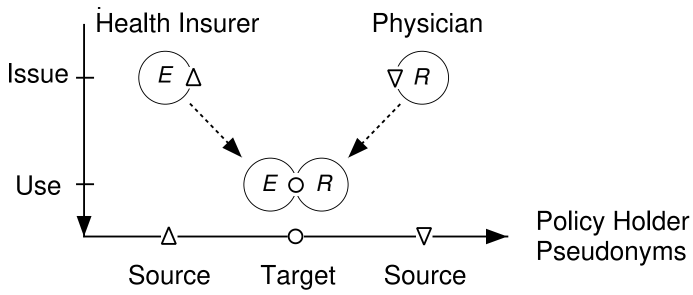

Figure 4: Using Two Authorisations for the same Target Pseudonym

In principle, enrollment authorisations can be implemented by personal or coin credentials, whereas referral and prescription authorisations can be implemented by group signatures or group coin credentials.

Double-use of referral and prescription authorisations can be prevented online by checking the health insurer's database of all referral or prescription authorisations ever used. Alternatively, double use can be prevented offline by the observer inside a digital patient assistant. In this case, double use prevention relies only on the tamper resistance of observers, and tamper resistance is hard to implement, so it is recommended that double users are still detectable after the fact. Double users can only be detected by the target pseudonym they use more than once, so these must somehow contain their identity (cf. coin credentials). As referral and prescription authorisations need to be used for the same target pseudonyms as the accompanying enrollment authorisations, the policy holders' identities must be encoded into the source pseudonyms of the relevant authorisations by either the insurer or the physician. The latter option raises an inevitable conflict with patient privacy, because it requires patients to reveal their policy holder identities to their physicians, which in turn makes all of their visits to physicians linkable.

Online authorisations require the health insurer's database to be available continually and also gives the insurer timing information about authorisation use. We therefore want to avoid any need for online access to the health insurer during patient visits to a physician. We therefore consider only enrollment authorisations that can be used offline, and consider the implementation options for referral and prescription authorisations orthogonally (Fig. 5).

Important Advantages (+) and Disadvantages (−)		Referral or Prescription Authorisations			
		Group Signatures		Group Coin Credentials	
		offline	online	offline	online
Enrollment Authorisations	Personal Credential	relies totally on tamper resistance	+ efficient − online − traceable[a]	+ offline + untraceable	+ untraceable − online
	Coin Credential	+ efficient − traceable − transferable[b]	less interesting[c]	+ offline + untraceable − transferable	less interesting[c]

[a] Collaborating health care providers can trace referral or prescription authorisations.
[b] Without non-digital means, enrollment authorisations are easy to transfer between individuals.
[c] Like option to the left, but enrollment authorisations can be used online only.

Figure 5: Combinations of Implementations and their Characteristics

4.6.1 Enrollment Authorisations by Personal Credentials

If referral or prescription authorisations are implemented by group signatures, then the content of a referral or prescription can simply be signed just as any other message[4] (in contrast to an implementation by group coin credentials). This is efficient, but leaves referral or prescription authorisations traceable by collaborating physicians and hospitals or by physicians and non-medical providers, respectively[5], because they can link any issuing and use of these authorisations. In most cases, this appears to be a minor issue. Double use can easily be detected if the physicians are required to include a target pseudonym in their referrals or prescriptions. This can be checked online when the prescription is used. An offline solution however must rely on the tamper resistance of observers because any identification of the dishonest patient can only be enforced by the observer inside the patient's digital assistant.

If referral or prescription authorisations are implemented by group coin credentials, then the only known way of enclosing different contents of referrals or prescriptions is by using a different group signing key for each issuing physician and each prescription. However, the prescription must be kept separate from the issuing physician's identity, because the former shall remain visible while the latter shall be kept anonymous. Therefore we suggest to form *referral groups* and *prescription groups*, i.e., one group of physicians for each possible referral content or prescription content. The group signature for a referral or prescription authorisation is then to be verified with the respective group's public verification key. Coin credentials add an extra layer of privacy for the patients, because

[4] We assume that the signatures are randomised, i.e., that any two signatures for the same prescription are different.

[5] Powerful health insurers who may try to bribe or blackmail health care providers.

even if the health insurer and all healthcare providers collaborate, they cannot determine which referral or prescription authorisations are used by the same patient(s).

This solution may or may not be appropriate for an entire national health system. For example, on the German pharmaceutical market there are about 80,000 medications[6] that are available only on prescription or at a pharmacy. Combinations, dosages and other treatments mean that there are at least several hundred thousand possible prescription contents. The situation is probably similar for referral contents. Maintaining a referral or a prescription group for each content is probably practical for smaller subsets of contents, but it is unclear how this solution scales.

If group coin credentials are used offline, then the observer inside the patient's digital assistant is supposed to prevent the patient from using a referral or prescription authorisation twice. If the tamper resistance is defeated, the health insurer should still be capable to detect double use after the fact. Hence, enrollment authorisations are implemented by personal credentials that bear a patient's identity in their source and target pseudonyms just like coin credentials. Since a coin credential can be used only for the same target pseudonym as a personal credential, the health insurer can detect double use after the fact.

If double use detection of group coin credentials is done online, then the recipient simply checks with the health provider if the group coin credential at hand is still unused.

4.6.2 Enrollment Authorisations by Coin Credentials

If enrollment authorisations are implemented by coin credentials, then double use prevention of referral or prescription authorisations can be enforced offline. Online solutions can be derived by replacing the role of the observer inside the patients' personal devices by an online request to the insurer. This appears to be less interesting because it requires all non-medical providers to be online and tends to reduce service availability of the system without adding advantages.

If referral or prescription authorisations are implemented by group signatures, then double use can be prevented by requiring physicians to include the patients' target pseudonyms into the referral or prescription content. If we assume that patients can never use two coin credentials for the same pseudonym, then they cannot use any prescription twice. This assumption holds for most existing coin credential schemes [9, 18]. If referral or prescription authorisations are implemented by group coin credentials, then double use of a prescription reveals the policy holder's identity because the prescriptions must be used for the same target pseudonym as the accompanying enrollment coin credential. Note that the double use detection of the group coin credential scheme is not needed since it is already provided by the coin credentials implementing the enrollment authorisations. This solution has been presented in earlier versions of this paper [6, 7].

4.6.3 Delegating Purchase of Medications

Next we consider the case of patients who want friends or relatives to go and buy medications for them. If enrollment authorisations are implemented by personal credentials, delegation to buy medications can be done by giving away one's digital assistant to the

[6] Not counting homeopathic medications.

delegate. In order to prevent misuse of the digital patient assistant, either the patients could block their assistants for everything but the intended purchase, or the patients could have pre-established pseudonyms with their pharmacies, so that the delegates can later reuse the established pseudonyms without being asked for a second biometric verification. The latter solution presumes more trust in the delegate because there might be other pre-established pseudonyms, which the delegate might use as well. The other way to delegate buying medications is by transferring a copy of the enrollment credential and of the prescription credential from the patient's digital assistant directly into the delegate's digital assistant. The delegate must then be able to use both authorisations for the same pseudonym without biometric verification.

If enrollment authorisations are implemented by coin credentials, then the patient needs to transfer one of these coins and the prescription authorisation into the delegate's digital assistant. For the coin credential, a transfer protocol is needed that moves the coin directly from the patient's digital assistant into the delegate's. If the prescription authorisation is implemented by a group signature, this can simply be copied. If the prescription authorisation is implemented by a group coin credential, then this too needs to be transferred.

4.7 Capping the Total Reimbursement

The simplest method of enforcing cost control with this system is for the insurer to track the budget of each physicians' group. If this is exceeded, the group is asked to re-identify some of the authorisations in order to find out who caused the trouble.

Another way of enforcing, for example, a yearly cap of $\$L$ is to let physicians claim their expenses in a virtual currency. At the end of the year the exchange rate of the virtual currency is calculated as the quotient of L over the sum of all claims. Each physician then gets reimbursed according to this exchange rate. Of course, shorter intervals of reimbursement are possible. This is how German compulsory health insurers operate today.

4.8 Discussion

If compulsory health insurers provide specialised health plans so that policy holders may enroll in the plans of several insurers at the same time, then a common clearing center can be used to cap the overall cost. As well as consenting to treatment, patients must also decide which insurer to bill for a treatment. We are then concerned about whether the common clearing center needs to be online, e.g. to check if prescription authorisations for double use.

What are the most suitable implementation options?

For enrollment authorisations, personal credentials appear to be the most suitable implementation. They cannot be transferred between individuals, yet it is easy to delegate personal credentials to a friend or relative. Besides, only one personal credential needs to be issued to each policy holder for each insurance plan. This solution is presented in more detail in Section 5.2. A problem of personal credentials is that no implementations are known yet that allow patients to authorise their treatments using their enrollment authorisations alone. The main advantages of coin credentials are that health insurers keep more control over the number of enrollment authorisations for each policy holder, while extending them to check credentials enables patients to authorise their treatments in a privacy protecting way. Their main disadvantage is transferability between individuals (at least by lending or sharing personal devices).

For referral authorisations, group coin credentials with offline use are promising. They provide an additional level of untraceability, do not require the health insurer to be online every time a specialist is visited, and their double use must probably not be strictly prevented. The combination with enrollment authorisations implemented by personal credentials, however, reduces privacy for patients because physicians need to know the identities by which their patients are enrolled in a health plan. In such a combination, the ideal implementation of enrollment authorisations are personal credentials with offline use that are issued for source pseudonyms that bear a policy holder's identity in much the same way as coin credentials do, and maintain those identities in their target pseudonyms. In this case, group coin credentials could achieve full privacy and untraceability. This solution is also presented in Section 5.2.

For prescription authorisations, group signatures appear most appropriate. Their double use can be strictly prevented regardless of whether enrollment authorisations are implemented by personal or coin credentials; untraceability and offline use are not important; and they do not make delegation any more difficult. Enrollment authorisations can be implemented efficiently by personal credentials or by coin credentials.

5 Offline Implementation of the Clearing Process

The discussion of implementation options in Section 4.8 has identified a practical solution that yields strong privacy for patients and physicians. The enrollment authorisations are implemented by personal credentials with identity based pseudonyms, referral authorisations by group coin credentials, and prescription authorisations by group signatures (see Section 4.6). The required cryptographic primitives are introduced in more detail in Section 5.1. The implementation of the charging and clearing process is sketched in Section 5.2.

5.1 Cryptographic Primitives

We employ four cryptographic primitives: *ordinary digital signatures* (Section 5.1.1), *personal credentials* (Section 5.1.2), *group signatures* (Section 5.1.3) and *group coin credentials* (Section 5.1.4). Each of these primitives has its own set of operations and security features. In order to indicate how the operations are going to be applied, we introduce them by referring to the now familiar participants: Health insurer H, physician D, specialist E, pharmacy or paramedical provider F and policy holder P. Some operations are to be implemented by two party protocols. This is indicated structured input and output parameter lists. All input and output parameters of one participant X are enclosed in square brackets, which are annotated with the respective participant's initial, i.e., the list $(\ldots, {}^{X}[a, b], \ldots)$ indicates that a and b are parameters of $X \in \{H, D, E, P\}$.

5.1.1 Ordinary Digital Signatures

An ordinary digital signature for a message achieves non-repudiation of origin for the recipient [21, 33]. An ordinary digital signature can be checked by anybody and, thus, can provide legal evidence for authorship of a message (cf. Section 4.3). There are three operations:

Generating Keys A pharmacy F can generate a *private key* rk and a corresponding public key pk. The private key is used to sign digital messages. The public key needs to be distributed in an authentic way, such by means of trust centers, and lets other principals verify ordinary digital signatures.[7]

$$(rk, pk) \leftarrow \mathrm{genKey}(\bullet) \ .$$

Signing The pharmacy F signs a message m and obtains a signature σ.

$$\sigma \leftarrow \mathrm{sign}(rk, m) \ .$$

Verifying Everyone can verify the signature σ for message m by looking up F's public key pk. If the verification yields $ok = \mathrm{True}$, then we call the signature σ valid for message m with respect to public key pk.

$$ok \leftarrow \mathrm{verify}(pk, \sigma, m) \ .$$

5.1.2 Personal Credentials

A personal credential (Section 4.3) is the digital analogue of a personal document like a membership card, passport or driver's license [5, 18]. Personal credentials reveal the identity of their issuer, e.g., the health insurer, but keep their holders anonymous against both issuers and recipients. Personal credentials can be used arbitrarily often. Everybody can verify a personal credential and so it provides legal evidence for its holder's authorisation. There are four operations:

Generating Keys The health insurer H, can generate a *private key* rk and a corresponding public key pk. The private key is used to issue personal credentials. The public key is published just as for ordinary digital signatures and is needed to verify personal credentials:[7]

$$(rk, pk) \leftarrow \mathrm{genKeyCred}(\bullet) \ .$$

[7] All (individual) key generating operations are probabilistic algorithms, so that their outcome cannot be predicted. The bullet in the parameter list is a place holder for one or more security parameters, which are not important in this context.

Issuing Personal Credentials The health insurer H with private key rk_H issues a personal credential to a policy holder P. The policy holder and health insurer agree on a source pseudonym $\triangle$ into which the policy holder's identity is encoded, the health insurer inputs the issuing key rk_H and the policy holder ends up with a personal credential EC within her digital patient assistant:

$$^{P}[EC] \leftarrow \text{issue}(^{H}[rk_H, \triangle], ^{P}[\triangle]) \ .$$

Using Personal Credentials The policy holder P can use the personal credential EC at some physician D. D verifies EC by using the public key pk_H of the issuer H. If the operation succeeds, then physician D learns the target pseudonym $\bigcirc$ of patient P and obtains a transcript t that he can later use to prove that he has received EC.

$$^{E}[t, \bigcirc] \leftarrow \text{use}(^{E}[pk_H], ^{P}[EC]) \ .$$

The target pseudonym is chosen by probabilistic choices of the digital patient assistant and its observer. If patients want to reuse any of their target pseudonyms, they can ask their observer to re-use their previous choices instead of making new ones.

Depositing Credentials A physician D who has received a credential EC can prove so to the insurer H by providing the transcript t and the corresponding target pseudonym. The insurer checks the validity of t by using its public key pk_H.

$$^{H}[t, \bigcirc] \leftarrow \text{deposit}(^{H}[pk_H], ^{E}[t, \bigcirc]) \ .$$

Upon successful termination of the protocol, H receives the transcript and corresponding target pseudonym $\bigcirc$.

5.1.3 Group Signatures

Group Signatures [13, 17, 19] can be described as anonymous digital signatures. Signers can dynamically form groups administered by a group center and sign in behalf of their group(s). Each group publishes a public group key by which everyone can verify whether a signature originates from a member of that group, but not from which. However, a group signature contains enough information to re-identify the actual signer if a dispute arises later on. A dedicated center in each group manages registration and suspension of members as well as re-identifications (cf. Section 4.3). There are five operations:

Generating Keys and Managing Groups Every physician D who has a need to sign anonymously can generate a private individual key ri_p and a corresponding public individual key pi_D:[7]

$$(ri_D, pi_D) \leftarrow \text{genKey}(\bullet) \ .$$

Registration as a member of a group G is done by giving one's public individual key to the group center and receiving the public group key pk_G in return. (The public individual keys are known by the respective group center(s) only, not by the general public.) In addition, the group center maintains a private group key rk_G that is used for identification of group members only:[8]

$$(rk_G, pk_G) \leftarrow \text{genGKey}(\bullet) \ .$$

Signing A member D of group G, on input the private and public individual keys and the group's public key, signs a message m anonymously. The group signature is returned:

$$\sigma \leftarrow \text{gSign}(ri_D, pi_D, pk_G, m) \ .$$

Verifying Everyone can verify a group signature σ for message m by looking up the public key pk_G of the group G. If the result is $ok = \text{True}$, then the verifier is assured that the message has originated from one of the members of G, but does not learn from which one. In this case we say that the signature σ is *valid* for message m with respect to public group key pk_G.

Identifying Signers Given a message m signed by a member D of group G, the center of G can identify the signer D by determining his public individual key:

$$pi_D \leftarrow \text{identifySigner}(rk_G, pk_G, \sigma, m) \ .$$

5.1.4 Group Coin Credentials

Group coin credentials are coin credentials (alias untraceable electronic cash) [16, 9, 18] that do not reveal their actual issuer, but only a group in which the issuer is registered. Each group coin credential can be used only once. In case of a dispute, the issuer of a group coin credential can be identified by the center of the respective group. There are seven operations (cf. Section 4.3):

Generating Keys and Managing Groups Every physician D who has a need to issue group coin credentials can generate an individual key pair of a private key ri_D and a corresponding public key pi_D:[7]

$$(ri_D, pi_D) \leftarrow \text{genIKeyCred}(\bullet) \ .$$

Registration as a member of a group G is done by giving one's public individual key to a group center and receiving for it the public group key pk_G in return. In addition, the group center maintains a private group key rk_G that is used for identification of group members only:[8]

$$(rk_G, pk_G) \leftarrow \text{genGKeyCred}(\bullet) \ .$$

[8]Here, the bullet indicates an input of one or more individual public keys. The group key pair can be constructed at once if the individual public keys of all group members are available for input. Otherwise, it can be constructed iteratively by updating the group key by one individual public key after another.

Issuing Group Coin Credentials A physician D registered as a member of group G issues a credential for source pseudonym $\triangle$ to a policy holder P. Both have previously agreed on the source pseudonym $\triangle$ into which the policy holder's identity is encoded. The result is a group coin credential PC:

$$^{H}[PC] \leftarrow \mathrm{gIssue}(^{D}[ri_D, pi_D, pk_G, \triangle], {}^{P}[\triangle]) \ .$$

Using Group Coin Credentials Having received a group coin credential PC, the policy holder P can use it at some specialist E. The specialist inputs the public key pk_G of the issuer's group, the policy holder inputs PC, and the specialist receives a transcript t and the policy holder's target pseudonym $\bigcirc$. Both are used later to deposit the received group coin credential and get a corresponding reimbursement:

$$^{E}[t, \bigcirc] \leftarrow \mathrm{gUse}(^{E}[pk_G], {}^{P}[PC]) \ .$$

The digital patient assistant and its observer construct the target pseudonym by using random choices. This can be done at issuing time. If patients want to reuse any of their target pseudonyms, they can ask their observers to re-use their previous choices instead of making new ones.

Depositing Group Coin Credentials A specialist E who has received a group coin credential PC proves so to the health insurer H. The health insurer H inputs the public key pk_G of the issuer's group. The specialist inputs a transcript t and a corresponding target pseudonym $\bigcirc$. If the operation succeeds, the health insurer obtains the policy holder's transcript and target pseudonym:

$$^{H}[t, \bigcirc] \leftarrow \mathrm{gUse}(^{H}[pk_G], {}^{E}[t, \bigcirc]) \ .$$

Identifying Issuers The group center of G can re-identify any group member. On being given the private and public group key and a transcript for a target pseudonym, the group center calculates the individual public key pi_D of the physician D who has issued the credential that produced the transcript t:

$$pi_D \leftarrow \mathrm{identifyIssuer}(rk_G, pk_G, t, \bigcirc) \ .$$

Identifying Users The health insurer maintains a database of all group coin credentials ever reimbursed since the issuing key of group G was set up. If a group coin credential is successfully deposited, the health insurer checks whether the target pseudonym has been used before. If not, it puts the new target pseudonym into its database and pays the bill. Otherwise, it identifies the double user of pseudonym $\bigcirc$ by comparing the transcript t with the old one t' from its database and obtains the identity id of a policy holder:

$$id \leftarrow \mathrm{identifyUser}(t, t', \bigcirc) \ .$$

5.2 Draft Protocols

As discussed in Section 4.8, enrollment authorisations are implemented by personal credentials, referral authorisations by group coin credentials and prescription authorisations by group signatures. In order to sign their invoices, registered and hospital physicians use group signatures whereas pharmacies and paramedical providers use ordinary digital signatures.

5.2.1 Initialisation

The health insurer H generates issuing keys for a personal credential scheme, usually one key for each type of health insurance plan. Policy holders and health care providers are initialised as follows (Figure 6):

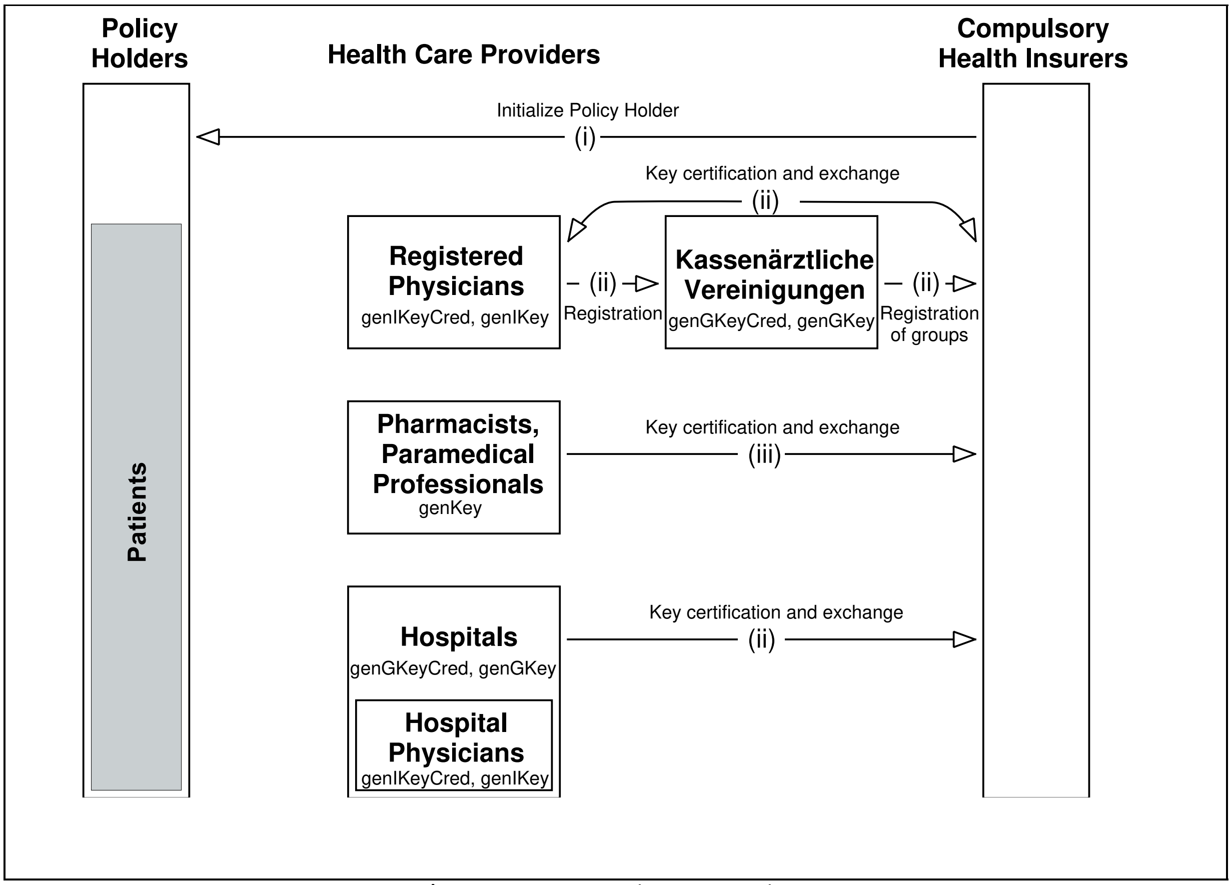

Figure 6: Initialisation Phase

Initialisation of Policy Holders (i) Initially, the health insurer equips every policy holder with a tamper resistant observer that fits into their digital patient assistant. The policy holders then personalise their observers with their biometric identity. The tamper resistance assumption about observers includes the irreversibility of personalisation; thereafter, observers can verify their holders' identity.

Initialisation of registered and hospital physicians Physicians get organised in groups, managed by the KVs and hospitals, which issue referrals and charge for medical treatment. To keep things simple, we consider only one referral content and therefore only one referral group G.

(ii) Each registered physician D and hospital physician E generates an individual key pair for a group credential scheme and for each referral content an individual key pair of a group signature scheme:[7]

$$(ri_D, pi_D) \leftarrow \text{genIKey}(\bullet) \ , \qquad (ri'_D, pi'_D) \leftarrow \text{genIKeyCred}(\bullet) \ ,$$
$$(ri_E, pi_E) \leftarrow \text{genIKey}(\bullet) \ , \qquad (ri'_E, pi'_E) \leftarrow \text{genIKeyCred}(\bullet) \ .$$

The KV generates the group key pair from the individual public keys:[8]

$$(ri'_D, pi'_D) \leftarrow \text{genIKey}(\bullet) \ , \qquad (ri_D, pi_D) \leftarrow \text{genIKeyCred}(\bullet)$$

Finally, the health insurer registers each group by certifying its public group key.

Initialisation of Pharmacies and Paramedical Providers (iii) Each pharmacy and paramedical provider F generates a key pair for an ordinary digital signature scheme and publishes the public key pk_F.

The health insurer registers each pharmacy and paramedical provider F by certifying their public keys.

5.2.2 Policy Holders' View

We are going to walk through a complete charging and clearing example including one health insurer H, one of its policy holders P, a physician D, a specialist E and a pharmacy or paramedical provider F. This Section 5.2.2 contains all actions in which the policy holder participates, and the following Section 5.2.3 contain the actual charging of health care provider expenses to the health insurer. An overview is given in Figure 7. Finally, Section 5.2.4 shows how the health insurer can cap the total cost.

Enrolling Policy Holders (1) To enroll a new policy holder in a health insurance plan, the health insurer issues a personal credential to the policy holder P with a source pseudonym $\triangle$ which is chosen randomly by the policy holder and the insurer together but encoding the holder's identity. As long as the holder honestly follows the subsequent protocols, the pseudonym will protect his identity, but if he deviates from the protocols, then the health insurer can later identify him.

$${}^{P}[EC] \leftarrow \text{issue}({}^{H}[rk_H, \triangle], {}^{P}[\triangle]) \ .$$

Getting a Referral or Prescription Authorisation (2) When patient P visits physician D, he first proves enrollment in a suitable health plan by using the personal credential EC for a target pseudonym $\bigtriangledown$:

$${}^{D}[t_D, \bigtriangledown] \leftarrow \text{use}({}^{D}[pk_H], {}^{P}[EC]) \ .$$

If during the course of treatment, D wants to write a letter of referral he issues a group coin credential PC to the patient P for the pseudonym, which is now used as a source pseudonym. The actual referral content is encoded in D's issuing key:

$${}^{P}[PC] \leftarrow \text{gIssue}({}^{D}[ri_D, pi_D, pk_G, \bigtriangledown], {}^{P}[\bigtriangledown]) \ .$$

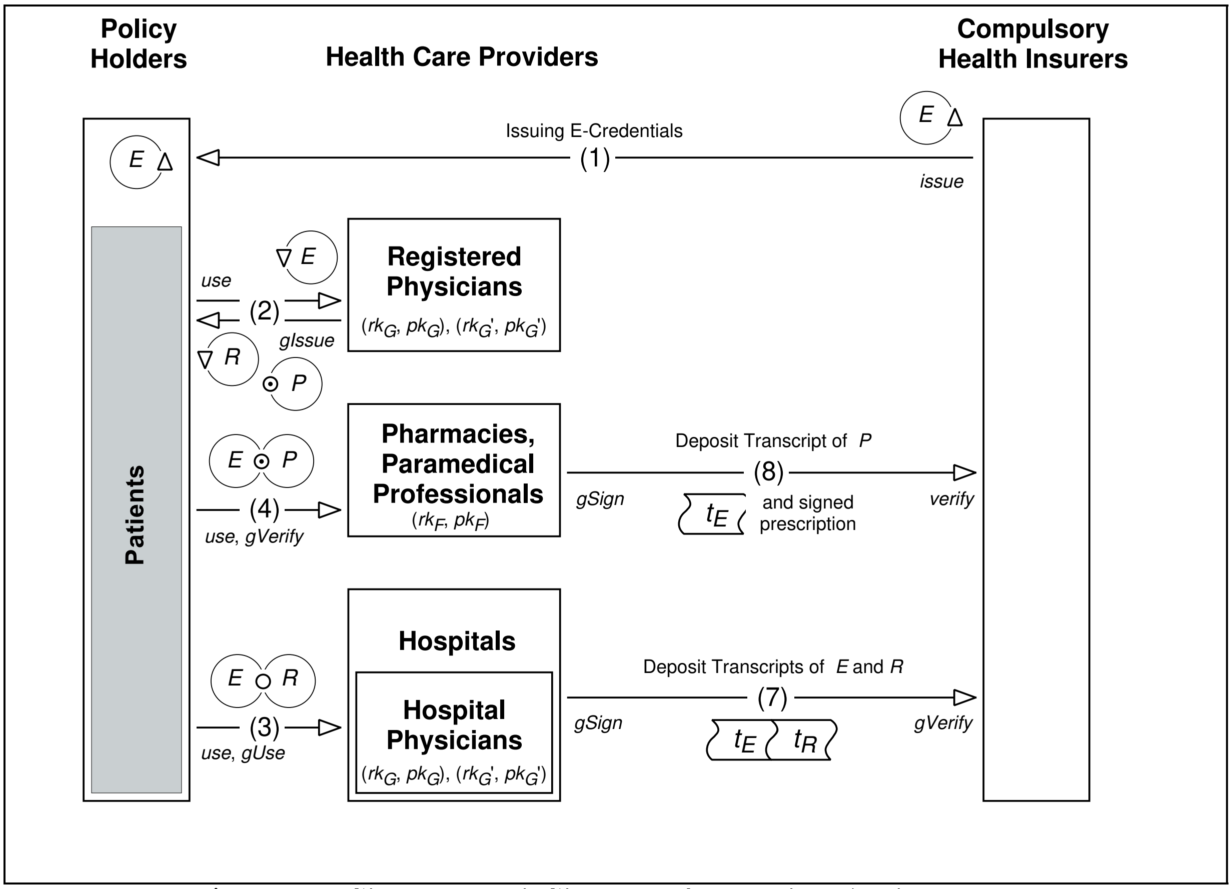

Figure 7: Charging and Clearing of R- and P-Authorisations

Similarly, if D wants to write a prescription, he first asks P for a pharmacy target pseudonym $\odot$, and then signs the prescription content plus the anticipated target pseudonym $\odot$ using a group signature (In Figure 7 this signed prescription is denoted by a circle annotated with the anticipated target pseudonym):

$$\sigma \leftarrow \mathrm{gSign}(ri_D, pi_D, pk_G, (\mathrm{prescription}, \odot)) \ .$$

If the patient visits a specialist E, then the specialist will run the same transactions using his own keys instead of D's.

Using a Referral Authorisation (3) In order to obtain specialist treatment, patient P uses both her enrollment and referral authorisations at a specialist E:

$$^{E}[t_E, \bigcirc] \leftarrow \mathrm{use}(^{E}[pk_H], {}^{P}[EC]) \ , \qquad ^{E}[t_R, \bigcirc'] \leftarrow \mathrm{gUse}(^{E}[pk_G], {}^{P}[PC]) \ .$$

If the target pseudonym $\bigcirc$ has been used before, then the patient's observer will not use it again. If the observer's tamper resistance is defeated, the health insurer can still identify the policy holders who use credentials twice (see Section 5.2.3-Charging for Specialist Treatment). E accepts only if both operations succeed and reveal the same target pseudonym $\bigcirc = \bigcirc'$. The specialist obtains a transcript from each transaction for charging purposes.

Using a Prescription Authorisation (4) In order to obtain her medications, patient P uses her enrollment authorisation at the pharmacy F and let it verify her prescription:

$$^{E}[t_F, \odot] \leftarrow \text{use}(^{E}[pk_H], {}^{P}[EC]) \ , \qquad \text{gVerify}(pk_G, \sigma, (\text{prescription}, \odot')) = \text{True} \ .$$

This is accepted only if both operations succeed, the target pseudonyms are equal ($\odot = \odot'$) and have not been used before. The latter is checked online by contacting the insurer. F obtains the transcript t_F and the signed prescription for charging purposes. The same protocol is used by paramedical providers.

5.2.3 Healthcare Providers' View

Charging for Medical Treatment (5) The physician D claims payment for medical treatment anonymously. Essentially, D uses a group signature, sends the invoice directly to the health insurer and deposits the endorsing transcript:

$$\sigma \leftarrow \text{gSign}(ri_D, pi_D, pk_G, (\text{invoice}, t_E)) \ , \qquad ^{H}[t_R, \bigtriangledown] \leftarrow \text{deposit}(^{H}[pk_H], {}^{E}[t_E, \bigtriangledown]) \ .$$

The transcript t_E tells the health insurer that a patient has seen the physician. In order not to allow physicians to simply reuse transcripts, the health insurer will check if the pseudonym $\bigtriangledown$ has been used before. It might be even more desirable if the transcripts also carried some kind of patient's consent to the treatment to be reimbursed (cf. Section 4.5).

The relevant amount is included in the next lump sum to be reimbursed to the KV that manages the group G:

$$\text{gVerify}(pk_G, \sigma, (\text{invoice}, t_E)) = \text{True} \ .$$

(6) The KV obtains a lump sum reimbursement from the health insurer together with the invoices covered. The KV verifies the invoices, re-identifies the claiming physicians and refunds their expenses accordingly:

$$\begin{aligned} \text{gVerify}(pk_G, \sigma, (\text{invoice}, t_E)) &= \text{True} \ , \\ \text{identifySigner}(rk_G, pk_G, \sigma, (\text{invoice}, t_E)) &= pi \ . \end{aligned}$$

The charging and clearing of medical treatment is summarised in Figure 8.

Charging for Specialist Treatment (7) The specialist E claims expenses in much the same way as physician D, but includes a transcript of the patient's referral authorisation. E's invoice is endorsed by the transcripts t_E of the enrollment authorisation and t_R of the referral authorisation. The specialist signs the invoice and the transcripts with his group signing key and deposits both of them:

$$\begin{aligned} \sigma &\leftarrow \text{gSign}(rk_E, (\text{invoice}, t_E, t_R)) \ , \\ ^{H}[t_E, \bigcirc] &\leftarrow \text{deposit}(^{H}[pk_H], {}^{E}[t_E, \bigcirc]) \ , \\ ^{H}[t_R, \bigcirc'] &\leftarrow \text{gDeposit}(^{H}[pk_G], {}^{E}[t_R, \bigcirc']) \ . \end{aligned}$$

The insurer accepts them if the signature σ is valid, the target pseudonyms are equal ($\bigcirc = \bigcirc'$) and the referral authorisation t_R has not been used before:

$$\text{gVerify}(pk_E, \sigma, (\text{invoice}, t_E, t_R)) = \text{True} \ .$$

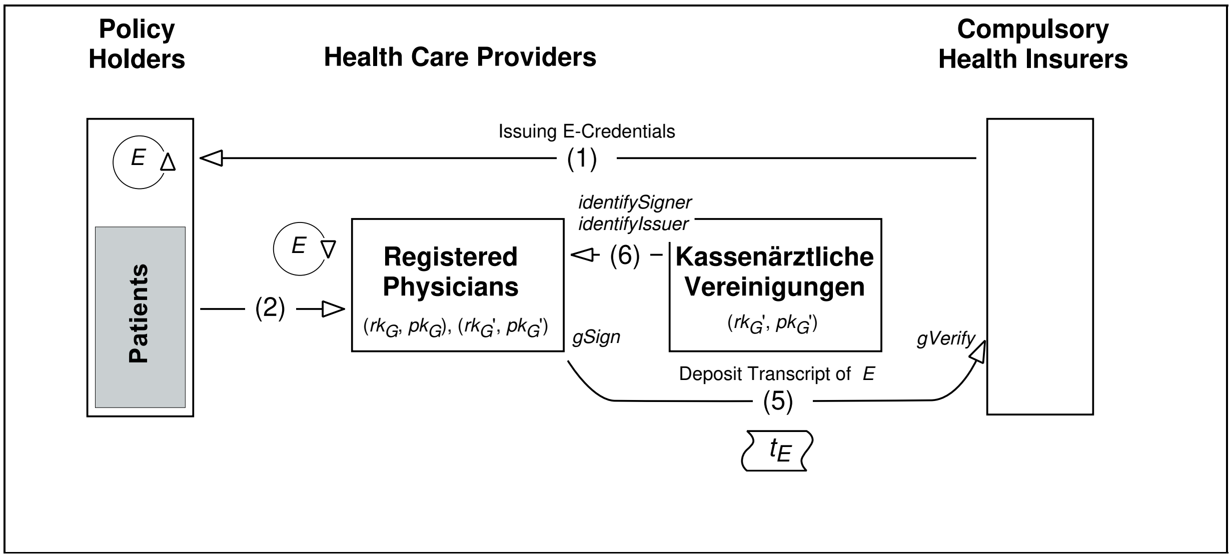

Figure 8: Charging and Clearing of Medical Treatment

The insurer can check for double use by looking up the target pseudonym it its database. If it is found, then comparison with the previous transcript will re-identify the cheater:

$$id = \text{identifyUser}(t_R, t'_R, \bigcirc) \enspace .$$

Charging for Medication and Paramedical Treatment (8) The pharmacy or paramedical provider F claims expenses in much the same way as a specialist, only the signed prescription is not a group coin credential and therefore is simply sent to the health insurer instead of using an interactive protocol (gDeposit()).

5.2.4 Limiting the Total Cost

The above concept of charging and clearing enables the health insurer to limit the overall cost of the system. The health insurer can monitor the sum of referral and prescription authorisations issued by each group of physicians. If certain groups exceed their budgets, the KVs or hospitals can be asked to re-negotiate the reimbursements for its group members, or re-identify those physicians who issue significantly above average:

$$pi_D = \text{identifyIssuer}(rk_G, pk_G, t_P, \bigcirc) \enspace .$$

In addition, the KVs could also recommend practices for subsequent spot-checking and a small percentage of policy holders can be asked to participate in cross-section studies.

Insurers can also monitor pharmacies and paramedical providers individually.

6 Security

A rigorous security analysis would have to formalise the security requirements as well as the security properties of the cryptographic primitives, and many assumptions about the real world implementation would have to be made. This section shall only summarise the evidence that the cryptographic kernel of the proposed implementation would satisfy a more rigorous proof.

6.1 Availability and Integrity Requirements

Physician: Each patient shall receive only the treatment and medication prescribed. In particular, each prescribed treatment shall be received only once (unless repeat prescriptions are given).

Referral and prescription authorizations are implemented by group coin credentials and group signatures, respectively. These in turn are based on digital signatures and therefore inherit effectiveness and unforgeability. Double use of referral and prescription authorisations is prevented by each patient's observer. If the observer's tamper resistance is defeated, double use of group coin credentials can still be detected and the cheaters identified after the fact. Double use of group signatures can also be detected because pharmacies and paramedical providers check the health insurer's pseudonym database online.

Policy holder: If she presents a valid insurance certificate, letter of referral, or prescription to a healthcare provider of her choice, the provider shall offer the requested product or service.

Again, effectiveness and unforgeability of enrollment, referral and prescription authorisations follow from the underlying digital signature. Availability of medical or paramedical services is a contractual rather than a technical matter.

Pharmacies and Paramedical providers: Their bills should be paid by the insurers if they are registered and their bills properly supported by proofs of treatment or purchase of medication.

Healthcare providers use transcripts of referral or prescription authorisations to prove referral; proofs that the product or service was covered by the patient's health plan is embedded in the prescription or transcript of enrollment authorisation. These transcripts also reveal their issuers' group and so insurers can verify physician registration.

Health insurers: Only registered physicians should be able to issue prescriptions. Each policy holder should be able to use prescriptions at most once (or according to a therapy plan). Each health insurer should reimburse expenses only once and only if they have been spent for its own policy holders. Health insurers should be able to cap the total reimbursement per year ("Deckelungsprinzip").

Health insurers accept only invoices from registered groups of physicians, pharmacies etc because these providers have to submit their public keys during initialisation. Unforgeability and double use prevention of enrollment, referral and prescription authorisations have been discussed above.

As personal credentials can only be used with the same observer present as the time of issue, and as the observer is personalised to exactly one biometric identity, it is infeasible to use someone else's authorisations unless the tamper-resistance of observers is broken, and even in that case cheaters can be detected after the fact. And as the defeat of an observer only allows the abuse of the credentials issued to its holder, such a defeat does not allow widespread fraud. It is also to be expected that insurers may limit the lifetime of enrollment credentials by issuing new keys periodically.

The total reimbursement per year can be controlled by monitoring and budgeting the groups of physicians.

6.2 Privacy Requirements

Physician and Patient: Medical treatment requires trust between patient and physician. This relationship must be protected against third parties' interests; diagnoses, therapies and prognoses should be strictly private. This rule should override, for example, a general obligation to escrow cryptographic keys. In general, health insurers do not need to know and thus should not know which physicians their policy holders visit.

Physicians achieve their privacy by charging and prescribing anonymously in one or more groups, and patients enforce their privacy by using different pseudonyms for different health care providers. This combination guarantees that no participant other than the patient and the physician can link any two of their visits.

Physician: At least by default, health insurers should not be able to monitor the physicians' prescription and other treatment habits. The interest of health insurers in cost control only justifies aggregate and spot checks.

In our proposal, insurers can profile only groups of physicians, not individual physicians.

Policy holder: The policy holder's right to ask a for second opinions implies that different healthcare providers should not monitor policy holders by exchanging views on them.

Since a policy holder can use different pseudonyms for each visit to a provider, no two visits or purchases can be linked from the data she provides. This feature is supported by the personal user devices being indistinguishable on the network, e.g., no machine readable serial numbers must be present.

7 Conclusions

We have shown that charging and clearing in the German healthcare system can be done electronically in a way that protects the legitimate security and privacy interests of all participants and, particularly, the patient-physician relationship. Given the tremendous amount of criticism against the German health insurance card (Versichertenkarte) introduced in 1992, there may well be a need for a more advanced solution. The original proposal of a health insurance card in Germany suggested the card as a medium to communicate administrative and medical data between physicians, pharmacies and other health care providers. Patients and patient advocates appreciated the increased reliability of chip-cards technology, but harshly criticised patients' lack of control over what is stored or communicated by their cards. So patients rightfully see little added value in any smart card solution. Our proposals suggest a technological leap towards digital patient assistants, which give patients appropriate control over both administrative and medical data.

8 Acknowledgments

This work has been supported by many parties. We would like to thank the working group on security in hospital information systems of the German GMDS and in particular Bernd Blobel and Klaus Pommerening for their motivation and support of this work. We also thank Birgit Pfitzmann, Joachim Biskup and Simon Jenkins for their interest and comments. This work has partially been supported by the German Research Foundation (DFG) and by the Commission of the European Union through their project ACTS.SEMPER (Secure Electronic MarketPlace for EuRope); however, it represents only the view of the authors. We appreciate Ross Anderson's efficient editorial help.

References

[1] Arnold M, Brauer HP, Deneke V, Fiedler E: The Medical Profession in the Federal Republic of Germany; Deutscher Ärzte-Verlag, Köln-Lövenich 1982.

[2] Bacard A: Anonymous Remailers; FAQ, Version Nov 15, 1996, `http://www.well.com/user/abacard/remail.html`.

[3] Biskup J: Medical Database Security; Data Protection and Confidentiality in Health Informatics - Handling Health Data in Europe in the Future, Edited by the Commission of the European Communities DG XIII/F AIM, Proc. of the AIM Working Conference, Brussels, 19-21 March 1990, IOS Press, Amsterdam 1991, 214-230.

[4] Biskup J: Protection of privacy and confidentiality in medical information systems; Database Security, III: Status and Prospects (eds.: Spooner DL, Landwehr CE), North-Holland, 1990, 13 - 23.

[5] Bleumer G: Biometric yet Privacy Protecting Person Authentication; Information Hiding Workshop '98, LNCS 1525, Springer-Verlag, Berlin 1998, 101-112.

[6] Bleumer G, Schunter M: Privacy Oriented Clearing for the German Healthcare System; in Ross Anderson (ed.): Personal Information Security, Engineering and Ethics, Springer-Verlag 1997, 175-194.

[7] Bleumer G, Schunter M: Datenschutzorientierte Abrechnung medizinischer Leistungen; Datenschutz und Datensicherheit DuD 21/2 (1997) 88-97.

[8] Brands S: An Efficient Off-line Electronic Cash System Based On The Representation Problem; Centrum voor Wiskunde en Informatica, Computer Science/Departement of Algorithmics and Architecture, Report CS-R9323, March 1993.

[9] Brands S: Untraceable Off-line Cash in Wallet with Observers; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994 302-318.

[10] Buchholz EH: Unser Gesundheitswesen: Ein einführender Überblick zum Gesundheitswesen der Bundesrepublik Deutschland, Springer-Verlag, Berlin, 1988.

[11] Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie: INFORMATIONSGESELLSCHAFT: Chancen, Innovationen und Herausforderungen; Rat für Forschung, Technologie und Innovation, Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, 1995.

[12] Bundesamt für Sicherheit in der Informationstechnik: Chipkarten im Gesundheitswesen; Schriftenreihe zur IT-Sicherheit Band 5, Bundesanzeiger Verlag, Köln 1995.

[13] Camenisch J, Stadler M: Efficient Group Signature Schemes for Large Groups; Crypto '97, LNCS 1294, Springer-Verlag, Berlin 1997, 410-424.

[14] Chaum D: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; AUSCRYPT'90, Sydney, Australia, January 1990, LNCS 453, Springer-Verlag, Berlin 1990, 246-264.

[15] Chaum D: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

[16] Chaum D, Fiat A, Naor M: Untraceable Electronic Cash, Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 319-327.

[17] Chaum D, van Heijst E: Group Signatures; Eurocrypt '91, LNCS 547, Springer-Verlag, Berlin 1991, 257-265.

[18] Chaum D, Pedersen TP: Wallet Databases with Observers; Crypto '92, LNCS 740, Springer Verlag, Berlin 1993, 89-105.

[19] Chen L, Pedersen TP: New Group Signature Schemes; EUROCRYPT '94, Proceedings, LNCS 950, Springer-Verlag, Berlin 1995, 171-181.

[20] DiabCard: Improved Communication in Diabetes Care Based on Chip Card Technology; `http://www.med.auth.gr/localsrv/medical/projects/lomi-pro/diabcard.htm`.

[21] Diffie W, Hellman ME: New Directions in Cryptography; IEEE Transactions on Information Theory 22/6 (1976) 644-654.

[22] Famulla R, Gerlof H: Das Kartenhaus in der Medizin wächst viel langsamer als gedacht; Arzt Online Nr. 6, das Computermagazin der Ärzte Zeitung, Oktober 1996. `http://www2.aerztezeitung.de/de/htm/medpc/karten/06ao1201.htm`.

[23] Häußler S, Liebold R, Narr H: Die Kassenärztliche Tätigkeit; Springer-Verlag, Berlin, 1984.

[24] Low SH, Maxemchuk NF: Anonymous Credit Cards; 2nd ACM Conference on Computer and Communications Security, Fairfax, November 1994, ACM Press, New York 1994, 108-117.

[25] Maxemchuk NF, Low SH: The Use of Communication Networks to Increase Personel Privacy in a Health Insurance Architecture; Manuscript, 1995.

[26] Neumann PG: Computer Related Risks; Addison Wesley - ACM Press, Reading Massachusetts 1995.

[27] Neumann PG: Risks of Surveillance; Communications of the ACM 36/8 (1993) 122.

[28] Pommerening K: Pseudonyme - ein Kompromiß zwischen Anonymisierung und Personenbezug; in: Trampisch HJ, Lange S (Hrsg.): Medizinische Forschung - Ärztliches Handeln; 40. Jahrestagung der GMDS, Bochum, September 1995, MMV Medizin Verlag, München 1995, 329-333.

[29] Pommerening K: Chipkarten und Pseudonyme; F!FF Kommunikation 1/96, 9-12.

[30] Pfitzmann A, Pfitzmann B, Schunter M, Waidner M: Trusting Mobile User Devices and Security Modules; Computer 30/2 (1997) 61-68.

[31] Sudhakaran Ram: Medical Prescription Dispensing Robot; RISKS-17.73 (1996) `ftp://unix.sri.com/risks`,

[32] Reiter MK, Rubin AD: Crowds: Anonymity for Web Transactions; DIMACS Technical Report 97-15, April 1997, revised August 1997, `http://www.research.att.com/~reiter/papers/dimacs-tr9715-revised. ps.gz`, to appear in ACM Transactions on Information and Sytem Security 1/1 (1998).

[33] Rivest RL, Shamir A, Adleman L: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21/2 (1978) 120-126, reprinted: 26/1 (1983) 96-99.

[34] Seecof M: Marketing use of medical DB; RISKS-17.13 (1996) `ftp://unix.sri.com/risks`.

[35] Struif B: Das elektronische Rezept mit digitaler Unterschrift; Reimer H, Struif B (eds.): Kommunikation & Sicherheit, TeleTrust Deutschland e.V., Darmstadt 1992, 71-75.

[36] Struif B: Sicherheit und Datenschutz bei elektronischen Rezepten; Multicard '94, Elektronische Kartensysteme - Anspruch und Wirklichkeit, Kongreßdokument I, 23.-25. Februar 1994, Berlin, 71-80.

[37] The Clinical Information Consultancy: Healthcards; `http://www.compulink.co.uk/~cic/euhci.htm`.