Privacy Oriented Clearing for the German Health-Care System

Gerrit Bleumer, Matthias Schunter
Universität Hildesheim, Institut für Informatik
Marienburger Platz 22, 31141 Hildesheim
{bleumer, schunter}@acm.org

Abstract. We present a clearing scheme for health-care in Germany that allows for the specific privacy interests of all participants, including the patient. Health insurance plays a key role in the German clearing system and it is their vital interest to reduce their overall cost as much as possible. Our scheme supports these interests while protecting the privacy of the insured persons and medical professionals.

1 Introduction

In most western democracies the increasing diversification of health-care providers and their ongoing competition enforce lean administration procedures including charging and accounting. However, simply simulating paper-based procedures by distributed computer systems will endanger the legitimate privacy interests of the participants. In this paper we show that charging, clearing and an effective control of the total remuneration of the health-care system are possible while privacy for all participants is provided.

Former and current paper-based procedures relied on much identifying patient data in order to ensure integrity. The applicable law on data protection limited the leakage of identifiable information only to the extent that getting hold of such data, transferring or storing it was relatively bothering. The inevitable consequence was that patients lacked privacy against all parties involved in their treatment but were slightly protected against outsiders since copying the paper documents is costly. This does not hold for digital documents. Therefore, the easier it is to acquire data illegitimately, the more need protection measures be integrated into the technical infrastructures themselves.

On the one hand, new technologies bear new potentials of surveillance and control (computer aided evaluation, medical data warehouses), on the other hand they also facilitate a new quality of security — including security of *all* participants — by avoiding the storage of large amounts of personal data in central places (chipcards, electronic wallets, and personal digital assistants with keyboard and display [21]). Health-care providers are about to invest millions into new communication and computing infrastructures. These investments will pay only if the technologies respect the actual legal regulations and if their implications are tolerated or at least accepted by all participants affected, e.g., patients, medical professionals, health insurances, etc. The G7 and some national initiatives [8] have stimulated such technologies, the topic has been suggested for further research to the Commission of the European Communities [2, 3] and, for example, specific solutions for the US market are under development [17, 18].

In order to derive an acceptable solution we state the (professional) duties and goals of each participant and then answer the key question:

Who needs which data in order to fulfil their duties and meet their goals?

Depending on the answer, we will select suitable technical and cryptographic measures to build our protocols. In comparison to existing solutions [23, 24], our protocols do not only provide integrity, but also full privacy to all participants.

2 Contractual Framework

We introduce the participants and business transactions of the German health-care system [1, 7, 16] with respect to charging and clearing of medical services. Afterwards we deduce the security interests of the participants involved.

The German health-care system[1] consists of five supply sectors [1, 9]. *Medical Outpatient Treatment* includes registered physicians (GPs) and specialists, e.g., dentists, who have their own independent practices. *Paramedical Outpatient Treatment* includes professionals allied to medicine like physio-therapists, speech therapists, etc. The *Inpatient Treatment* consists of all hospitals for acute cases and special hospitals. The *Public Health Services* are provided by state and local public health departments and by the departments of chemical examinations. The *Pharmaceutical Supply* is provided by pharmacists.

The health insurers are the clearing houses of the health-care system. In practice they delegate the clearing tasks to several client-specific organizations (*actual clearing houses*). There are compulsory and private health insurances. 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 insurance is compulsory. 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. They pay about one half of the total cost in health-care.

Throughout this paper we distinguish three kinds of *health-care providers* (Fig. 1.) and draft their modes of charging.

1) Outpatient physicians registered by compulsory health insurers (*registered physicians*) may issue prescriptions for medical treatment and write letters of referral. They do not claim directly to the health insurers. Their actual clearing houses are the local associations of registered physicians: Kassenärztliche Vereinigungen (KV). Each KV gets a lump sum from the compulsory health insurers and reimburses the invoices of registered physicians. The registration is done by a joint registration committee of the health insurances and the KVs.
2) *Pharmacists* and *paramedical professionals* serve patients more or less according to what registered physicians have prescribed. Their actual clearing houses are the health insurers.
3) *Inpatient physicians*, analogously to outpatient physicians, do not claim directly to the health insurers. Their clearing houses are their respective hospitals which in turn are reimbursed by the health insurers.

3 Paper-based Charging and Clearing

We consider in more detail how expenses for medical treatment and medicaments are claimed in the German health-care system. Interactions between two participants consist

1) A German-English and English-German glossary about the German health-care system can be found in [1].

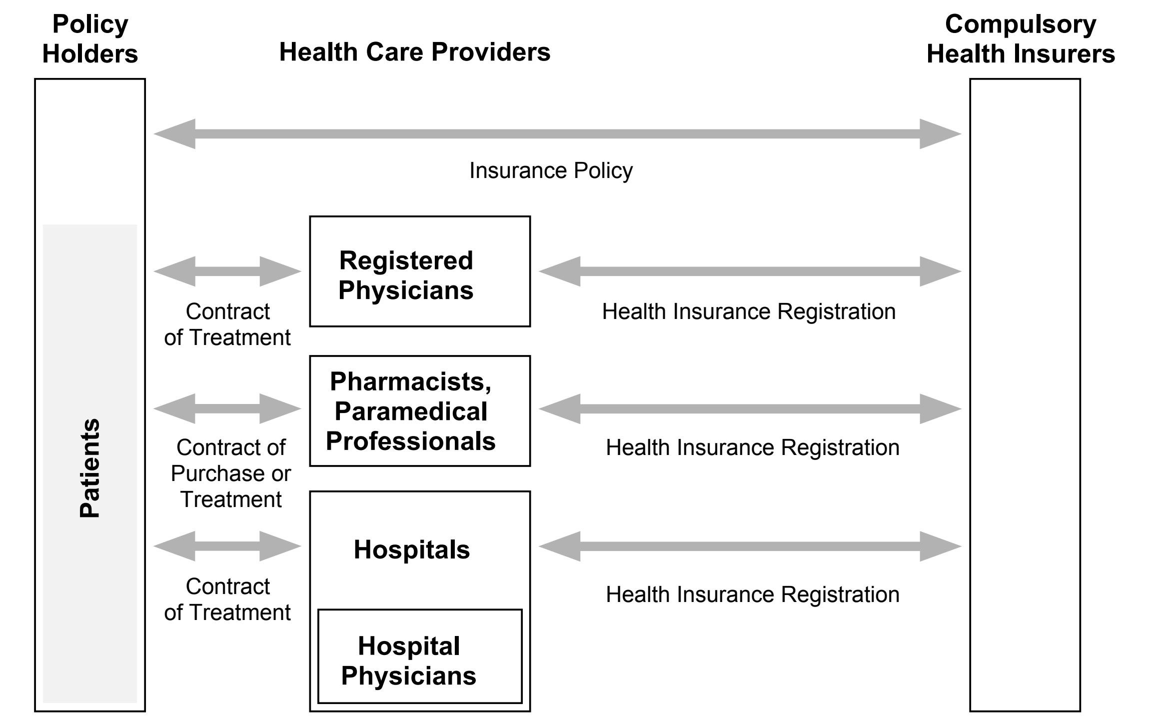

Fig. 1. Contractual Framework

of "real" actions and of "paper" actions. For example, a physician treats a patient, sends an invoice for the treatment and is finally refunded. 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 process of treatment: A patient requests treatment from his GP by handing over a signed health insurance record card (Krankenschein) and includes the data necessary for accounting. The GP may provide some treatment on his own and in addition:

1) prescribe some medicament, and
2) refer the patient to a specialist or hospital.

During the process of health-care, 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 possibly diagnostic, therapeutic or prognostic information about the patient. Usually, the patient passes a relevant excerpt of this record to the next health-care provider, who then continues the process of treatment. Each health-care provider copies the respective part of the patient's record and forwards it to the respective actual clearing house in order to legitimate his invoice.

3.1 Analysis

Since 1992 the compulsory health insurers have equipped their policy holders with personal health insurance cards ("Versichertenkarte"). These are memory chip cards containing the administrative data of a patient that had previously been communicated by a paper-based health insurance record card. If a patient requests a medical service from a health-

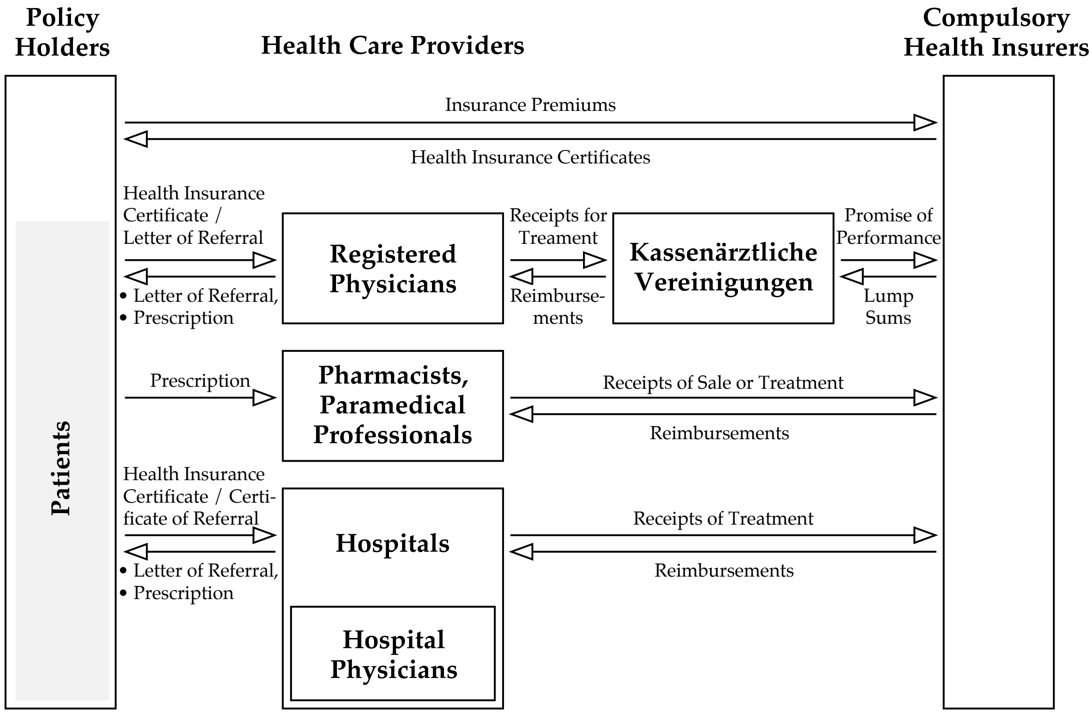

Fig. 2. Flow of Information Between the Participants of the German Health-care System

care provider, he has to identify himself by his health insurance card. Clearly, this is an almost perfect means to efficiently and reliably enforce the complete identification of patients — the primary requirement of health insurers. The privacy requirements of patients, however, have simply been ignored.

The paper-based refund system implements a kind of postpaid system. Forms for health insurance record cards can be regarded as special kinds of credit cards. Filling in such a form legitimates a patient to get, e.g., medical treatment. The health insurer of the patient acts as the clearing house. It pays lump sums to the actual clearing houses and these reimburse the expenses that are properly supported with receipts.

Alternatively, health-care providers could also claim directly to the patients, as most insurers do, e.g., private health or car insurances. In this case, policy holders get to know the detailed cost of their treatments and could act in a more cost-saving way. On the one hand, they could ask their health-care providers for less expensive services and could check all invoices. On the other hand, they could occasionally decide whether to use their health insurer or whether they like to pay by themselves.

Usually, receipts for everyday's commercial transactions do not contain much personal information about the payer; receipts in health-care are different. In paper-based systems the invoices of the health-care providers (and the receipts of the actual clearing houses) contain a tremendous amount of highly personal and sensitive information about patients and physicians. The mere existence of charging documents containing identifying information about patients tempts people to use this information for secondary purposes. Every participant involved gets to know the complete prescription for a patient and all documents referring to a patient are linked from the treating physician at the front end to the health insurer at the other end.

3.2 Participants and Their Specific Security Requirements

In order to motivate our alternative, we settle the question which participants really need to have which information in order to fulfil their tasks. We recall the services to be provided by each participant (Section 3.2.1) and consider additional constraints posed by the specific confidentiality and privacy needs of all participants (Section 3.2.2).

3.2.1 Availability and Integrity Requirements

Physician: Each patient shall receive exactly the treatment and medicament as is prescribed. In particular, each prescription shall be used at most once. In some cases an extended validity of prescriptions is required according to a therapy plan.

Policy holder: If he presents a valid health-insurance certificate, letter of referral, or prescription to a health-care provider of his choice, the provider shall indeed offer the requested service or perform the treatment prescribed.

Pharmacies and Paramedical professionals: Any of their expenses should be reimbursed by the health insurers if the health-care provider is registered and if the claims are properly supported by proofs 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 limit the total reimbursement per year (“Deckelungsprinzip”).

Clearly, the health-care providers usually need few administrative data of the patients they treat or sell medicine to. Even less administrative data about patients needs to be communicated between health-care providers. The patients need non-repudiable prescriptions of their physicians. The health service providers need to verify the prescriptions before giving any treatments or medicines. Afterwards, they need to obtain receipts for the services provided. In paper-based practice, the medical prescription serves for both purposes. What we learn from this summary is that the patients’ real names need to be included only in their health insurance policies.

3.2.2 Confidentiality and Privacy Requirements

Physician and Patient: Medical treatment requires a relationship based on trust between patient and physician. Their relationship has to be protected comprehensively against third parties’ interests; diagnoses and therapies should be strictly confidential. This specific 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.

Physician: At least by default, health insurers should not be able to monitor the physicians’ habits to treat their patients and to prescribe medicaments. The interest and obligation of health insurers to save cost of health-care hardly justifies more control than spot-checking physicians.

Policy holder: The policy holder's right to ask a health-care provider of his choice for second opinions implies that different health-care providers should not monitor policy holders by exchanging their local views on them.

Obviously, the above requirements can be met by legal regulations, but technical means are more effective; even more so 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 any charging interaction of physicians and policy holders [19, 20].

4 Digital Charging and Clearing Procedures

We now show how the whole process of treatment can be organized in a privacy-oriented way. The underlying idea is to use a modified prepay system rather than simulating the postpaid system of the paper world. Each health insurance maintains its own digital currency. The coins are labelled and represent Health Insurance certificates (***I*-certificates**), which legitimate for certain treatments (e.g., visiting a GP, dentist, etc.). Health-care providers maintain their own digital currency. These coins are also labelled and represent Medical certificates (***M*-certificates**) that we use as a generic term for prescriptions, letters of referral, etc. *M*-certificates can be issued such that they only reveal a group to which the actual issuer belongs — not the issuer himself. We assume that each policy holder is equipped with a personal user device [21] capable to manage his or her certificates and that each health-care provider offers appropriate stationary equipment to interact with personal devices. Note that this fulfilled by smartcards which will be introduced, except for a missing secure user interface.

4.1 Initialization

There are three initializing steps as illustrated in Fig. 3.. Since these steps are independent, they may be executed in any order.

<i> In order to facilitate their policy holders to receive treatment anonymously, each health insurer issues batches of *I*-certificates to its policy holders. *I*-certificates have the following properties:

a) From a given *I*-certificate one can determine the actual health insurer of a policy holder but learns nothing more about the holder's identity.

b) *I*-certificates can be used at most once. Using one twice in order to receive a service twice, reveals the policy holder's identity. Observe that copying an I-certificate is not prevented, but if the original owner would use it, too, the double-show detection mechanism will identify him.

<ii> Physicians can form groups that could be administered, e.g., by the respective KV or hospital. Members of a group can claim their expenses anonymously, i.e., relative to their group. Examples for such groups are the GPs of a geographical region, or the physicians of a hospital department. The size and structure of these groups is subject to balancing the monitoring interests of health insurers and the privacy interests of the physicians.

<iii> Each health-care provider has his specific signature key by which he signs his invoices later on. Health-care providers are registered by a committee of the health

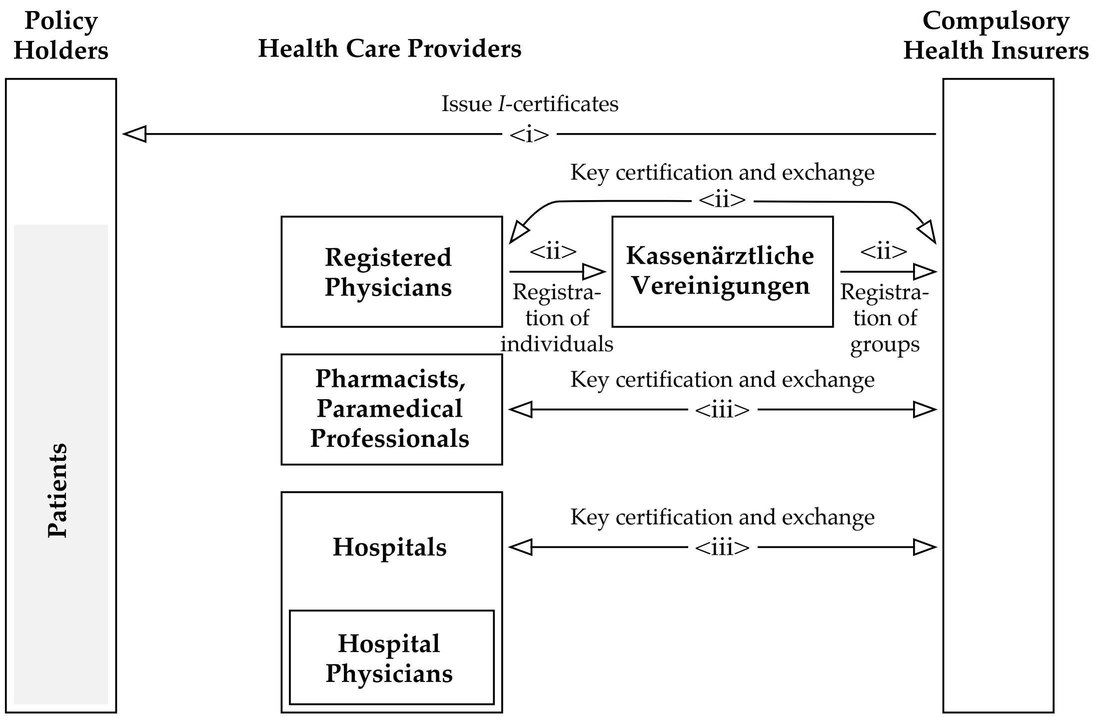

Fig. 3. Initialization

insurers by having their corresponding public keys registered. Alternatively, the committee may delegate this registration to the KV.

An overview over the stages of charging and clearing is shown in Fig. 4..

4.2 Issuing Prescriptions

<1> When a policy holder —now acting as a patient— is to receive a prescription, he pays a fresh *I*-certificate to his physician and gets a respective *M*-certificate in return. Physicians record all treatment and prescriptions they have provided to their patients.

4.3 Showing Prescriptions

<2> The patient shows a new *I*-certificate as a proof of being member of a health insurance together with the *M*-certificate received in order to show his prescription to an provider (e.g. a pharmacist). The provider checks both certificates and provides the prescribed treatment or medicament(s). In the next section we show how this can be implemented by means of one-show group credentials [4, 10].

4.4 Digital Clearing of Prescriptions

<3> The health-care provider sends the transcripts of the received certificates to the respective health insurer in order to prove his expenses. The health insurer checks the validity of the transcripts and checks for double showing. The health insurer also checks for the budgeting of the groups. If a group of health-care providers exceeds a certain budget, its group center can be asked to deanonymize some or all of the transcripts of a group to find out which provider(s) caused the trouble.

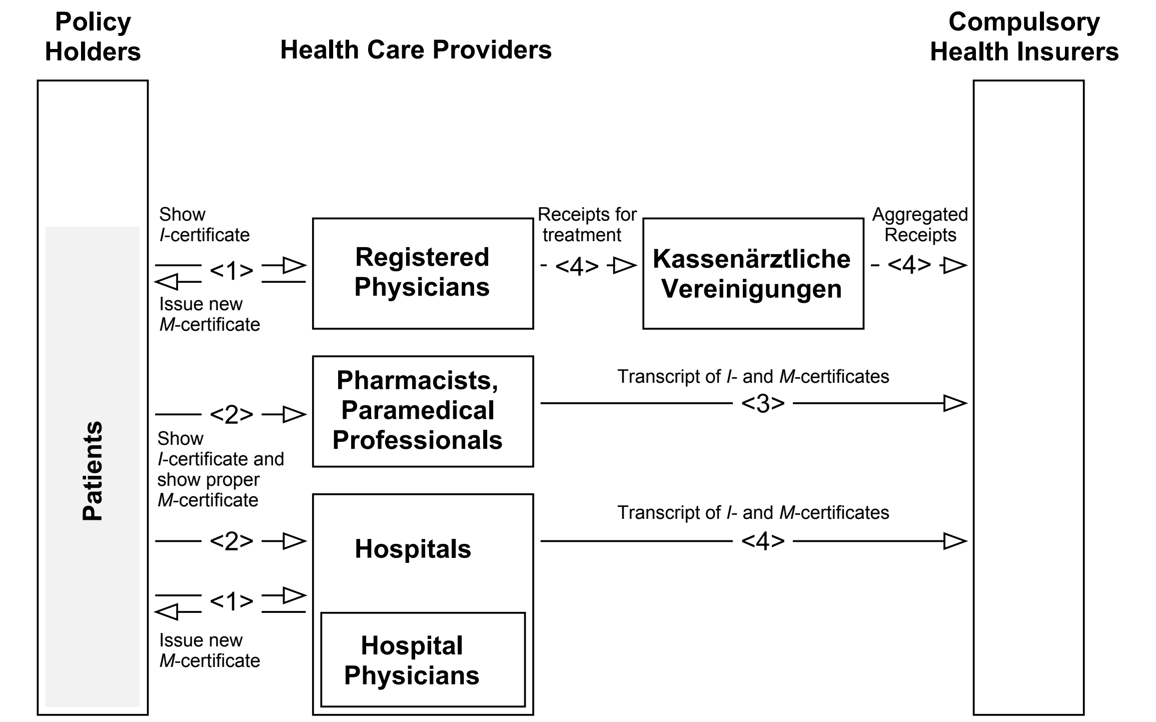

Fig. 4. Digital Charging of Medical Services.

The health-care providers need not trust the health insurers, because, if need be, the providers can prove all their claims to an arbiter or a court.

4.5 Digital Clearing of Medical Treatment

Different from pharmacists and paramedical professionals, physicians decide autonomously about therapies they perform or prescribe and thereby determine the amounts claimed. In the current paper-based system this autonomy is hardly controlled; even the compulsory insured patients cannot check if the expenses claimed correlate to the treatment they received. This can be implemented straightforwardly. Health insurers simply accept the transcripts of *M*-certificates containing the corresponding *I*-certificates as valid proof of treatment. If health insurers request more control, they could ask the physicians to have their invoices signed (anonymously) by their respective patients (see Section 3.1).

According to Section 3.2, we must consider the following requirements:

1) The trust relationship between physician and patient must be protected. Transcripts or combinations of transcripts resulting from this relationship (prescriptions, etc.) must not reveal the identity of physician or patient.
2) Exceptional rules must be supported because the physician in charge of a patient is ultimately responsible and liable for how the patient is treated and what he is told. For example, in case of an emergency, a physician's expenses must be reimbursed even if the patient is not able to confirm or consent to anything. Another case occurs when a physician decides not to tell the whole story to his patient.

A possible trade-off is the following:

<4> Patients confirm and sign the medical reports about their treatment. The physicians keep the signed reports with the patient's record. The physicians write anonymous invoices and claim to the respective KV or their employing hospital, e.g., every quarter of a year. After checking the budgets, all reimbursements are payed.

The physicians record the signed confirmations of their patients. If a health insurer detects that some budget is exceeded, it may ask for these confirmations. These confirmations may be signed anonymously (see Section 4.5) using a group signature scheme to protect the privacy of the patients even in the presence of extensive spot-checking. In addition, the KVs may spot-check physicians, i.e., ask for these confirmations of randomly selected patients, too.

4.6 Security

We explicate why the proposed solution meets the requirements described in Section 3.2:

4.6.1 Availability and Integrity Requirements

Physician: Each patient shall receive exactly the treatment and medicaments as is prescribed. In particular, each prescription shall be received once and only once. In some cases an extended validity of prescriptions is required according to a therapy plan.

Any modification of a M-certificate's label invalidates the certificate itself because it invalidates the digital signature involved in the cryptographic implementation of certificates. The one-time property of M-certificates ensures that each prescription can be used only once.

Policy holder: If he presents a valid health-insurance certificate, letter of referral, or prescription to a health-care provider of his choice, the provider shall indeed offer the requested service or perform the treatment prescribed.

The integrity requirement is met since the employed credential scheme is correct. The availability requirement cannot be enforced, it is "only" supported by the legal contract between health-care providers and health insurers: If a patient shows a valid prescription, the provider is obliged to provide the prescribed treatment.

Pharmacist and Paramedical professionals: Any of their expenses should be reimbursed by the health insurers if the health-care provider is registered and the expenses claimed are properly supported by proofs of treatment.

Providers use M-certificate transcripts as receipts to the health insurers. As M-certificates as well as their transcripts reveal a group of their issuer, health insurers can make sure to accept only M-certificates that have been issued by physicians.

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 limit the total reimbursement per year ("Deckelungsprinzip").

Registrations of physicians are checked in the same way as those of pharmacies and paramedical professionals. Showing prescriptions more than once will be recognized by the health insurers when performing a double show detection.

Reimbursement of expenses for own policy holders cannot be enforced strictly in the paper-based system. The same holds for our digital scheme: Two potential attackers need to be addressed, policy holders and non-policy holders, and collusions thereof. Non-policy holders could get hold of the personal user device of a policy holder and thus of his certificates. Potential damage of this attack could be limited by two measures: Each personal user device should identify its owner, e.g., by means of biometrics, and all critical operations should be protected by means of passwords, PINs, etc. More dangerously, policy holders could try to sell their certificates or their whole personal user devices together with passwords and PINs. This may be prevented by means of a printed photographs on the device. This kind of insurance fraud cannot be strictly prevented, but health insurers can limit the number of *I*-certificates issued just like banks do with usual checks.

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

4.6.2 Privacy Requirements

Physician and Patient: Medical treatment requires a relationship based on trust between patient and physician. This relationship should be protected comprehensively against third parties' interests; diagnoses, therapies and prognoses should be strictly private. This specific 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 relative to one of their groups, and patients enforce their privacy by using a fresh certificate for every transaction. 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' habits to treat their patients or to prescribe medicaments. The interest and obligation of health insurers to save cost of health-care hardly justifies more control than spot checking physicians.

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

Policy holder: The policy holder's right to ask a health-care provider of his choice for second opinions implies that different health-care providers should not monitor policy holders by exchanging their local views on them.

Since the patient uses a fresh pseudonym for each transaction, no two of his transactions can be linked (from the data he provides himself). This feature is supported by the personal user devices being indistinguishable on the network, e.g., no machine readable serial numbers must be present.

5 Implementing the Clearing Process

We show how to implement the clearing process described in Section 4 by four primitive schemes. The primitive schemes are introduced in Section 5.1, an implementation of the clearing process is sketched in Section 5.2 and the means to control cost are revisited in Section 5.2.9.

5.1 Primitive Schemes

We employ four primitive schemes: *ordinary digital signatures* (Section 5.1.1), *one-show credentials* (also called digital cash, Section 5.1.2), *group signatures* (Section 5.1.3) and *one-show group credentials* (Section 5.1.4). Each of these schemes 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*), pharmacist or paramedical professional (*E*) and policy holder (*P*). Some operations are to be implemented by two party protocols. In this case the last parameter of the formal parameter list of the operation is an address of the peer party.

5.1.1 Ordinary Digital Signatures

An ordinary digital signature under a message achieves non-repudiation of origin for the recipient of the message [15, 22]. An ordinary digital signature can be checked by anybody and, thus, can provide legal evidence for authorship of a message. The primitive offers three operations:

Generating Keys

Everyone who has a need to sign 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, for example, by means of trust centers, and enables to test ordinary digital signatures. Everyone holding a signed message and the public key of the claimed signer can test whether the signature is valid or not.

$$(rk, pk) = \text{genKey}(\bullet)$$ [2]

Signing

Someone who has generated a private key can later sign a message m and obtain a signature σ.

$$\sigma = \text{sign}(rk, m)$$

Testing

Everyone can test the signature σ on message m by looking up the public key pk of the claimed signer.

$$ok = \text{test}(pk, \sigma, m)$$

5.1.2 One-Show Credentials

A one-show credential scheme (also called digital cash scheme) provides the digital analogue of coins of some currency [5, 6, 11]. Credentials reveal the identity of their issuer, e.g., a health insurer, but keep the holder anonymous against both the issuer and the recipient to whom the credential is shown. A credential can be checked by anybody and, thus, can provide legal evidence for an authorization of the holder. The primitive offers five operations:

2) All 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.

Generating Keys

The health insurer H, which has to issue some kind of currency, can generate a *private key* (*rk*) and a corresponding public key (*pk*). The private key is used to create and issue credentials. The public key needs to be distributed just as for ordinary digital signatures, and enables to check credentials.

$$(rk, pk) = \text{genKeyCred}(\bullet)$$

Issuing Credentials

A health insurer H with private key rk_H issues a credential labelled with a type identifier l to a policy holder P. The result is a one-show credential I, which later represents an I-certificate:

$$I = \text{issue}(rk_H, l, P)$$

Showing Credentials

Having received a credential I, a policy holder P can show it to some physician D. D checks the credential by using the public key *pk* of the claimed issuer I. If physician D accepts the credential, he ends up with a transcript t_I that he uses later to deposit the received credential.

$$t_I = \text{show}(pk_H, I, D)$$

Depositing Credentials

A physician D who has received a credential I proves this fact to an insurer H by providing a transcript t_I. The insurer checks the validity of t_I by using the insurer's public key pk_H.

$$ok = \text{deposit}(pk_H, t_I, H)$$

Double Showing Detection

As an integral part of checking the validity of a transcript, the health insurer checks if the credential has been spent and claimed previously. If so, the insurer can determine the identity of the policy holder who once received that credential. This requires only the two different transcripts t_I, t_I' that resulted from showing the credential twice. The parameter list contains the actual transcript t_I and the history of all transcripts deposited before (indicated by •)

$$id = \text{identifyShower}(t_I, \bullet)$$

Instead of detecting double-showers after the fact, such fraud can also be prevented by using wallets with observer for the user devices [12]. Double deposits of an identical transcript are usually prevented by randomizing the signatures and rejecting the second deposit after showing the first signature.

5.1.3 Group Signatures

Group Signatures [12, 14] can be regarded as anonymous ordinary digital signatures. Signers can dynamically form groups and sign in behalf of their group(s). Each group publishes a public group key by which outsiders can test whether a signature originates from a member of that group, but not from whom. However, a group signature contains enough information to identify the actual signer if a dispute arises later on. A dedicated center in each group could manage registration and suspension of members as well as re-identifications. The primitive offers five operations:

Generating Keys and Managing Groups

Every physician D who has a need to sign anonymously can generate a private individual key (ri_D) and corresponding public individual key pi_D:

$$(ri_D, pi_D) = \text{genIKey}(\bullet)$$

Registration as a member of a group G is done by handing over one's public individual key 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 (The public individual keys of all group members are one input to this procedure.):

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

Signing

A member D of group G can sign a message m anonymously on input her or his private and public individual keys and the group's public key. The following group signature is obtained:

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

Testing

Everyone can test a signature σ on message m by looking up the public key pk_G of the group G by what the message is claimed to be signed. A positive result assures the verifier that the signer is a member of group G, but gives no further indication who the signer is.

$$ok = \text{gTest}(pk_G, \sigma, m)$$

Identifying

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

$$pi = \text{identifySigner}(rk_G, pk_G, \sigma, m)$$

5.1.4 One-Show Group Credentials

This primitive extends one-show credentials in much the same way as group signature schemes extend ordinary digital signature schemes. Group credentials do not reveal their actual issuer, but only a group to which the issuer is registered. In case of a dispute, the actual issuer can later be identified by the center of the respective group. Group credentials offer seven operations:

Generating Keys and Managing Groups

Every physician D who has a need to issue group credentials can generate a pair of individual keys, a private (ri_{pD}) and corresponding public one pi_D:

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

Registration as a member of a group G is done by handing over one's public individual key 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:

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

Issuing Group Credentials

A physician D registered as a member of group G issues a credential labelled l to a policy holder P. The result is a one-show group credential M, later representing an M-certificate:

$$M = \text{gIssue}(ri_D, pi_D, pk_G, l, P)$$

Showing Group Credentials

Having received a group credential M, a policy holder P can show it to some physician D. D checks the credential by using the public key pk_G of the claimed issuer group. If physician D accepts the credential, he ends up with a transcript t_M that he uses later to deposit the received credential and get reimbursed.

$$t_M = \text{gShow}(pk_G, M, D)$$

Depositing Group Credentials

A physician D who has received a group credential M proves this fact to an insurer H by providing a transcript t_M. The insurer H checks the validity of t_M by using the public key pk_G of the group G of the issuer.

$$ok = \text{gDeposit}(pk_G, t_M, H)$$

Identifying Issuers

Given a group credential M issued by any of the members of group G, the center of G can identify the issuer D by determining his public individual key:

$$pi_D = \text{identifyIssuer}(rk_G, pk_G, M)$$

Double Showing Detection

As an integral part of checking the validity of a transcript, the health insurer checks if the credential has been shown or deposited before. If so, the insurer can determine the identity of the policy holder who once received that credential. This requires only the two different transcripts t_M, t_M' that resulted from showing the credential twice. The parameter list contains the actual transcript t_M, and the history of all transcripts deposited before (indicated by •):

$$id = \text{gIdentifyShower}(t_M, \bullet)$$

5.2 Draft Protocols

The idea underlying our proposal is to implement I-certificates by one-show credentials (depicted as white coins in the following figures) and M-certificates by one-show group credentials (depicted as shaded coins). In order to sign their invoices, physicians use group signatures and all other health-care providers use ordinary digital signatures.

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* and a pharmacist or paramedical professional *E*. Each step is implemented by means of the primitives of Section 5.1. The initialization phase is depicted in Fig. 5. (Section 5.2.1 through 5.2.4). The subsequent actions for charging and clearing of medical treatment and accounting are depicted in Fig. 6. (Section 5.2.5 through 5.2.8).

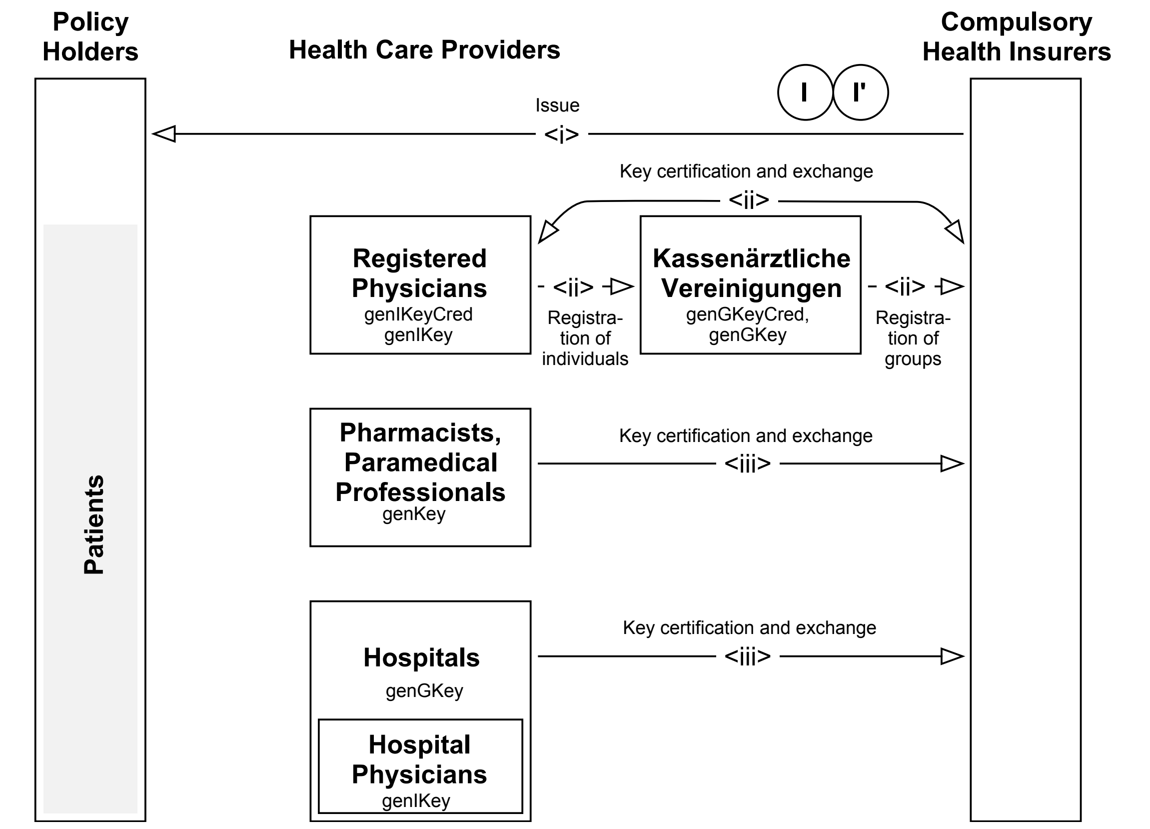

Fig. 5. Initialization Phase

5.2.1 Initialization

Physicians have to generate a pair of individual keys for a group signature scheme and one for a group credential scheme. The former is to claim the expenses for their medical treatment, the latter is to issue prescriptions to their patients. Pharmacies and paramedical professionals have to generate an individual pair of keys for an ordinary digital signature scheme.

5.2.2 Generating Health Insurance Record Cards

Health insurers issue batches of one-time credentials to their policy holders. For every health insurance record card a policy holder needs, he uses a fresh credential later on (Section 5.1.4).

<i> A health insurer using private key rk_H issues to its policy holder *P* a batch of credentials that facilitate to visit a GP:

$$(I, I', \ldots) = \text{issue}(rk_H, \text{‘GP’}, P)$$

5.2.3 Generating Provider Licenses for Medical Professions

Before physicians can issue prescription or claim expenses for medical treatment, they have to be registered to respective groups of physicians. These groups could be managed, e.g., by the KVs. Registration to a physicians' group serves as a legitimation to claim expenses for medical treatment to a health insurer and, thus, is an analogue to provider licenses of physicians. Registration is by generating two individual keys and having their public parts registered by the group center. One is of a group credential scheme in order to issue *M*-certificates (Section 5.1.4), the other is of a group signature scheme in order to claim expenses for medical treatment (Section 5.1.3). We see no disadvantage in using the same groups for both purposes:

<ii> Physician *D* generates a pair of individual group credential keys and another pair of individual group signature keys:

$$(ri_D, pi_D) = \mathrm{genIKeyCred}(\bullet)$$

$$(ri_D', pi_D') = \mathrm{genIKey}(\bullet)$$

The group center (KV) generates the group keys from the individual keys submitted. The private group keys remain at the KV, whereas the public group keys are published:

$$(rk_G, pk_G) = \mathrm{genGKeyCred}(\bullet).$$

$$(rk_G', pk_G') = \mathrm{genGKey}(\bullet)$$

5.2.4 Generating Provider Licenses for Paramedical Professionals

.

<ii> Each pharmacist and paramedical professional *E* needs to generate a pair of keys for an ordinary digital signature scheme and publishes the public key pk_E:

$$(rk_E, pk_E) = \mathrm{genKey}(\bullet)$$

Fig. 6. illustrates the processes of issuing prescriptions, charging medicaments and medical treatment.

5.2.5 Issuing a Prescription

<1> After examining his patient *P*, physician *D* can issue a prescription *m* to *P* by means of a one-show group credential *M*:

$$M = \mathrm{gIssue}(ri_D, pi_D, pk_G, m, P),$$

5.2.6 Showing a Prescription

<2> Patient *P* who has received a group credential *M* can show it to a pharmacist or paramedical professional *E*. In addition, he shows a fresh credential I' in order to prove his membership in a health insurance. If *E* accepts, he is left with two transcripts $t_{I'}$ and t_M.

$$t_{I'} = \mathrm{show}(pk_H, I', E), \quad t_M = \mathrm{gShow}(pk_G, M, E)$$

If a patient shows the same (group) credential twice, the fraud will be detected at clearing time. If, for example, duplicate delivery of drugs is to be prevented, the pharmacy needs to check on-line whether the M-certificate has been shown before.

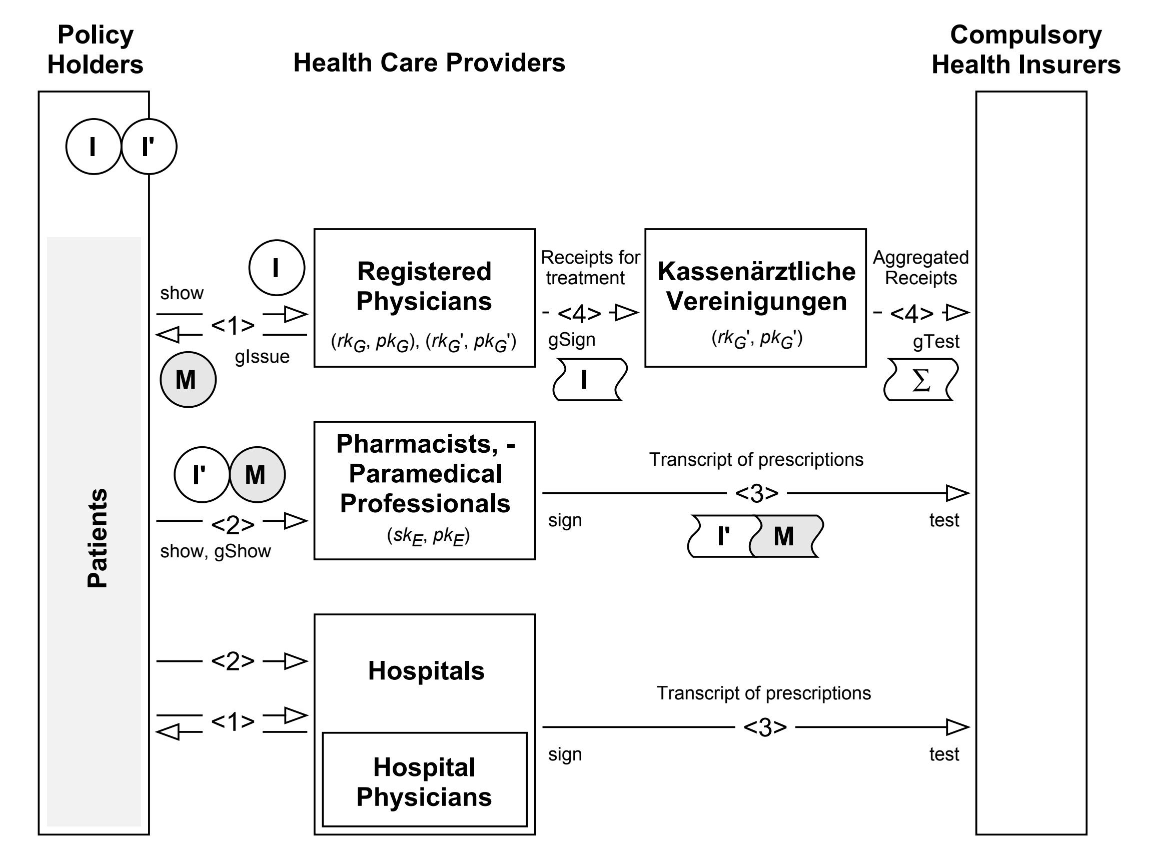

Fig. 6. Charging Medical Treatment and Prescriptions and Clearing

5.2.7 Depositing Prescriptions on Health Insurers' Accounts

<3> A pharmacist or paramedical professional E claims his expenses for a prescribed service m to the respective health insurer H by forwarding his signed invoice including both the credential transcript (I-certificate) and the group credential transcript (M-certificate):

$$\sigma = \mathrm{sign}(rk_E, (\mathrm{invoice}, t_{I'}, t_M)),$$

$$ok = \mathrm{deposit}(pk_H, t_{I'}, H)$$

$$ok = \mathrm{gDeposit}(pk_G, t_M, H)$$

The health insurer accepts if the signature is valid and the double show detection fails for both transcripts:

$$ok = \mathrm{test}(pk_E, \sigma, (\mathrm{invoice}, t_{I'}, t_M)),$$

$$\mathrm{identifyShower}(t_{I'}, \bullet),$$

$$\mathrm{gIdentifyShower}(t_M, \bullet)$$

Recall that prescriptions of risky or expensive medicaments like drugs that should not be delivered twice for one prescription require double show prevention after step <2> already.

5.2.8 Placing Medical Treatment on the Account of a KV

<4> A physician D claims his expenses for medical treatment m to a KV in a similar way as pharmacists and paramedical professionals do to health insurers. The only difference is that physicians confirm their treatments anonymously by using a group signature:

$$\sigma = \text{gSign}(ri_D, pi_D, pk_G, (\text{invoice}, t_\Gamma)), \quad ok = \text{deposit}(pk_G, t_\Gamma, H)$$

The health insurer accepts if the group signature is valid and no double-deposit occurred. Afterwards, a double-spending check is done:

$$ok = \text{gTest}(pk_G, \sigma, (\text{invoice}, t_\Gamma)), \quad \text{identifyShower}(t_\Gamma, \bullet)$$

If the health insurer is not willing to bear the risk of double-spending, on-line checks must be mandatory.

5.2.9 Limiting the Total Cost

The above concept of charging and clearing enables the health insurers to limit the overall cost of the system. Health insurers can monitor the sum of M-certificates issued by each group of physicians. If certain groups exceed their budget, the KVs or hospitals can be asked to identify those physicians issuing significantly above average:
<3> KVs:

$$D = \text{identifyIssuer}(rk_G, pk_G, M)$$

Furthermore, the KVs could recommend practices for subsequent spot-checking.

The health insurers can also limit the cost of medical services. The expenses claimed by pharmacies and paramedical professionals can be monitored individually. Those of physicians can be monitored with respect to the groups maintained. Health-care providers who have over-claimed can be identified similar as above.
<3> KVs:

$$D = \text{identifySigner}(rk_G, pk_G, \sigma, m)$$

The health insurers can coarsely limit the overall cost by limiting the amount of I-certificates they issue. If a certain overall limit L per year must not be exceeded at all, any cost could be claimed in a virtual currency. At the end of a year the value of a unit of this virtual currency is calculated and all health-care providers are reimbursed according to this actual exchange rate. In addition, a small percentage of policy holders might be asked to participate in cross-section studies, etc.

6 Conclusions

We have shown that charging and clearing in the German health-care system can be done while the security and privacy interests of all participants and, particularly, of the patient-physician relation are respected. The proposal should be transferable to clearing systems of other solidarity-based reimbursement systems.

7 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 have further appreciated the constructive criticism of Birgit Pfitzmann, Joachim Biskup and Simon Jenkins. This work has partially been supported by the German Research Foundation (DFG) and by the Commission of the European Union through their project SEMPER (Secure Electronic MarketPlace for EuRope).

8 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] 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.

[3] 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.

[4] Bleumer G: Group Credentials; Hildesheimer Informatik Bericht (to appear in July 1996).

[5] 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.

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

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

[8] 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.

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

[10] 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.

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

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

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

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

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

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

[17] 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.
[18] Maxemchuk NF, Low SH: The Use of Communication Networks to Increase Personel Privacy in a Health Insurance Architecture; Manuscript, 1995
[19] 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.
[20] Pommerening K: Chipkarten und Pseudonyme; F!FF Kommunikation 1/96, 9-12.
[21] Pfitzmann A, Pfitzmann B, Schunter M, Waidner M: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule; Brüggemann HH, Gerhardt-Häckl W (ed.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS'95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 329-350.
[22] 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.
[23] Struif B: Das elektronische Rezept mit digitaler Unterschrift; Reimer H, Struif B (eds.): Kommunikation & Sicherheit, TeleTrust Deutschland e.V., Darmstadt 1992, 71-75.
[24] Struif B: Sicherheit und Datenschutz bei elektronischen Rezepten; Multicard'94, Elektronische Kartensysteme - Anspruch und Wirklichkeit, Kongreßdokument I, 23.-25. Februar 1994, Berlin, 71-80.