# SECURITY SCHEME FOR ELECTRONIC PATIENT'S RECORDS INCORPORATING FULL PRIVACY

Kosmas Kapis, Jan C.A. van der Lubbe, Kathy Cartrysse, Bartek Gedrojc
{K.Kapis; J.C.A.vanderLubbe; K.Cartrysse; B.Gedrojc}@ewi.tudelft.nl
DELFT UNIVERSITY OF TECHNOLOGY

*This paper presents an electronic patient record (EPR) security scheme that covers the privacy of patients and health care practitioners (HCPs). The scheme is designed such that it provides HCP's privacy towards another HCP but revealable in disputes. Forward signature and encryption schemes are used to provide EPR integrity and confidentiality respectively. Furthermore, forward group signatures are used to provide privacy between HCPs.*

## INTRODUCTION

Currently, most of the patient's medical records are stored in digital form in the storages called Electronic Patient Record (EPR). An EPR can be defined as a collection of a patient's medical information in electronic form that is accessible online from many separate, inter-operable automated systems within an electronic network [3]. In these electronic networks large amounts of information are processed. This poses a threat to the patient's privacy especially, in the current situation where the availability of electronic medical record is well enhanced and the records are fully owned by hospitals and their respective health care practitioners (HCPs).

In the existing running of health care services, only HCPs own EPRs and control their access. In a way, patients are deprived of their right to control their privacy. The patient's accountability to his medical records is realized in a few situations. For example, when a conscious patient is advised to take a medication that might be life threatening. In such cases a patient is required to give his consent in writing before accepting the medication. This calls for the need for patients to control their privacy and shared responsibility of EPRs handling. Hence sharing EPR access accountability. This paper shows an EPR security scheme that ensures that a patient remains himself the part-owner of and the jointly responsible of his own EPR. The scheme protects the privacy between HCPs and incorporates the capabilities to hold either the patient or the HCP accountable in situations where disputes can occur. The achievement of this goal is based on the way the

parties participating in the functionality of the scheme are registered. For the scheme to work the following requirements have to be met: the protection of EPR confidentiality and integrity, and patient's consent; provision of HCP's privacy towards another HCP (i.e. elimination of control between HCPs); registration of patients and HCPs must be done via their respective hospital; and provision of shared EPR accountability between patients and HCPs.

## RELATED WORK

In the literature, few studies have been done on schemes for protecting the privacy of patients and HCPs. The first approach to reduce the privacy vulnerabilities was addressed in [1]. In this scheme the patient is conscious and able to communicate. The privacy and confidentiality of the patient and HCP is secured by using ordinary digital signatures (ODS) and group signatures (GS). The scheme uses one show credentials for ODS and GS to protect patient's and HCP's identities respectively, leaving the EPR in a clear text. An emergency case, when the patient is unconscious is considered in [5]. This scheme is based on a forward signature scheme [4]. It bypasses patient's consent and allows access to the patient's EPR in emergency situations, and has a capability of restoring EPR consent after the patient gains consciousness and ability to communicate.
A scheme for protecting privacy of patients and HCPs in normal and emergency situations was considered previously; in particular, [2] proposed a system using nameless patients' identities called *anonymous credentials* to provide patients and HCPs privacy. This scheme requires the patients to create and distribute the emergency record access tokens to several authorized entities immediately after registration. The medical record is stored in plain text readable by anyone with a token. This again increases vulnerability of compromising patient's confidentiality and invalidates the need for patient's consent. We show a scheme that protects the patient's and HCP's privacy when a patient can communicate and guarantees the EPR access in emergency situations. The scheme can be used to demonstrate evidence where disputes may arise between the patients and HCPs.

## THE PRIVACY PROTECTION SCHEME

To meet the defined requirements, some assumptions are made. Firstly, several entities participate in the scheme(see figure 1), namely *Trusted Third Party*, (TTP),*hospital owner* (HO), the patient $u_j$, the HCP $v_{j'}$, and the storage of EPR

access keys and EPRs called (EPRHost), ($j$ and $j'$ represent the numerical position of the patient and HCP respectively). Secondly, each HCP is a part of the group. Thirdly, patients and HCPs use smartcards provided by the TTP as means of identification and access to the EPR. Finally, for facilitation of the healthcare services mobility , smart gateways are introduced. They include a *mobile gateway* $G_\Omega$ and *hospital gateway* $G_\mathcal{H}$. The mobile gateway is part of the TTP while the hospital gateway belongs to the hospital. It is also assumed that, the TTP has a public key $P_{ttp}$, private key $S_{ttp}$ and an identifier $I_{ttp}$ and, the $HO$ has a valid hospital license and other credentials.

The TTP is legal entrusted party that is responsible for registering patients, HCPs, hospitals and creating smartcards for patients and HCPs. It also receives and checks HO's credentials, creates and distributes keys to all entities except the HO, whose role is to generate temporary transport keys. These keys are physically submitted to the TTP and are used initialize the registration process only. The function of the scheme is such that, when a patient is conscious and physically able to communicate, the HCP $v_{j'}$ and a patient $u_j$ are both needed to sign the same newly entered medical record, $M$. They sign $M$ using forward signatures. These are signatures which when used are such that, if the current signing is compromised, signatures in the past remain valid. In this case, M is signed by the patient and HCP using forward ODS key $S_{u_j,t}$ [4] and forward GS key $\bar{S}_{v_{j'},t''}$ [6] respectively. Moreover, for efficiency enhancement purposes, $M$ has to be hashed before being signed. In order to provide confidentiality, the patient encrypts $M$ using his symmetric encryption key. Where $t$ and $t''$ represent time instants for forward ODS and forward GS respectively. The function of this scheme is based on the availability of the smartcard and involves; the registration of entities, EPR access, and update of patient's secret keys. In this case we focus on the registration of entities, and show how the set requirements are met.

The registration process starts by the HO submitting all required information to the TTP. If documents are approved, the TTP registers the hospital and the group of HCPs. Every HCPs must be a part of the group for privacy reasons. When executing tasks, HCPs have to identify themselves by their group. Next, the HCP and patient register with the TTP via their hospital. The TTP creates smartcards and sends them to the hospital, ready for collection. At this stage, the HCP has to register first with the hospital EPRHost, followed by the patient. The patient's registration with the hospital EPRHost is such that, for the patient to be registered with the hospital EPRHost, his permission must first be

obtained. The patient's registration with the hospital EPRHost results in the creation of an EPR, which requires the HCP's and patients involvement. This ensures that the patient remains a co-owner and responsible for his EPR. The registration protocols are described in the next section.

## Interactions Protocols

Registration protocols are shown in figure 1. Firstly, the hospital $\mathcal{H}$, and the group of HCPs are registered with the TTP by the hospital owner HO (I). Secondly, HCPs are registered with the TTP (II) and EPRHost (III). And finally, patients are also registered with TTP (IV) and EPRHost (V). The registration of HCPs and patients with the TTP is done via the hospital. Protocol (V) shows how the patient and HCP together create the EPR while ensuring EPR confidentiality and integrity, and HCP's privacy. It also shows that, for the patient to be registered with the hospital EPRHost, his consent must first be obtained. Following is a description of the protocols.

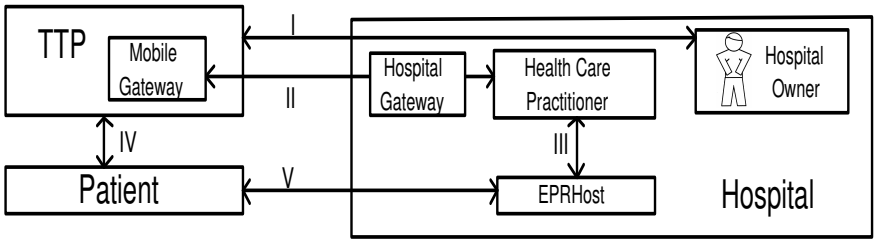


Figure 1: Participating Entities and Registration Protocols

I. ***Hospital and HCPs Group Registration with TTP.*** Using the hospital EPRHost computer system, the HO generates and stores symmetric shared secret keys $K_{HO_1}$and $K_{HO_2}$. The HO submits $K_{HO_1}, K_{HO_2}$ and his credentials to the TTP. The TTP checks the HO credentials and the hospital license, and then generates the hospital $\mathcal{H}$ keys $(P_{\mathcal{H}}, S_{\mathcal{H}}, I_{\mathcal{H}})$ and HCPs' group public key $\bar{P}_v$. The TTP uses a message authentication code (MAC) together with keys $K_{HO_1}, K_{HO_2}$ to transport keys from the TTP to the hospital EPRHost. The MAC is used to guarantee message authenticity and confidentiality of the keys transported from the TTP to the hospital EPRHost. The registration protocol of the hospital and the HCP group is as follows;

1. $TTP \rightarrow EPRHost : r_1$ (A random challenge)

2. $EPRHost \rightarrow TTP : \mathbf{e}K_{HO_2}(r_1, r_2), h_{K_{HO_1}}(\mathbf{e}K_{HO_2}(r_1, r_2))$ Where $h_{K_{HO_1}}$ is a MAC computed using secret key $K_{HO_1}$

3. $TTP \rightarrow EPRHost : \mathbf{e}K_{HO_2}(\bar{P}_v, P_{ttp}, I_{ttp}, P_{\mathcal{H}}, S_{\mathcal{H}}, I_{\mathcal{H}}, r_2)$,
$h_{K_{HO_1}}(\mathbf{e}K_{HO_2}(\bar{P}_v, P_{ttp}, I_{ttp}, P_{\mathcal{H}}, S_{\mathcal{H}}, I_{\mathcal{H}}, r_2))$

II. ***HCP Registration with TTP.*** The HCP $v_{j'}$ physically submits his credentials to the hospital authority to be checked. If credential are valid, the hospital securely sends an application form for the HCP's smartcard $AF_{v_{j'}}$ to the TTP. The TTP assigns a smartcard with a card number $NC_{v_{j'}}$ and generates all keys necessary for the HCP to interact with other entities. The TTP creates the smartcard and assigns the HCP's personal identification number PIN, $\pi_{v_{j'}}$. Then the TTP securely mails the created smartcard and $\pi_{v_{j'}}$ separately to the hospital. Finally, the HCP is informed that the card and $\pi_{v_{j'}}$ are ready for collection. Following are the HCPs' registration steps with the TTP.

1. The HCP physically contacts the Hospital and submits his credentials (Certificates, Identity, license, insurance).

2. The Hospital checks HCP's credentials and sends $\mathbf{e}P_{ttp}(AF_{v_{j'}}, I_{\mathcal{H}})$ to the TTP.

3. The TTP assigns to the HCP's smartcard , a forward individual's group signature key $\bar{S}_{v_{j'},t''}$, public and private keys pair $P_{v_{j'}}, S_{v_{j'}}$, identification $I_{v_{j'}}$ and card number $NC_{v_{j'}}$.

4. The TTP creates a smartcard for the HCP. Using the smartcard and TTP system, the TTP selects $\pi_{v_{j'}}$. Upon interaction between TTP system and the smartcard, $\pi_{v_{j'}}$ is converted into $h(\pi_{v_{j'}})$ using a hash function $h$. The TTP temporarily keeps $h(\pi_{v_{j'}}) = K_{\pi_{v_{j'}}}$ and uses it as an encryption key. The TTP stores in smartcard $h(h(\pi_{v_{j'}})) = h(K_{\pi_{v_{j'}}})$, $\mathbf{e}K_{\pi,v_{j'}}(\bar{S}_{v_{j'},t''}, S_{v_{j'}}, I_{v_{j'}})$. It also stores in the smartcard HCP's public key $P_{\mathcal{H}}$ and Card number $NC_{v_{j'}}$.

5. The TTP sends $\mathbf{e}P_H(P_{v_{j'}}, NC_{v_{j'}}, I_{v_{j'}}, I_{ttp})$ to the hospital EPRHost.

6. The TTP securely mails the smartcard and a protected HCP's $\pi_{v_{j'}}$ separately to the hospital. The mail containing the PIN is secured in such a way that once $\pi_{v_{j'}}$ security seal is damaged it cannot be repaired(e.g. prepaid phone cards). $\pi_{v_{j'}}$ can be disclosed only by the owner.

7. The hospital receives the mails and informs the HCP.

8. The HCP receives the two mails at the hospital after showing credentials proving that the two sealed mails belong to him.

III. ***HCP Registration with EPRHost.*** The goal of this stage is to enable the HCP be recognized by the EPR-Host during the provision of medical care services to patients. Having registered, it should be possible to confirm that the

HCP claiming to be an employee of the hospital is one who claims to be. In this stage the HCP's and EPR-Host's information previously distributed by TTP to HCP and EPRHost is used to approve the HCP's registration with the EPR-Host. This registration is done once. The identity authentication protocol is used and two different challenges are used to prevent a replay attack. The HCP uses his $\pi_{v_{j'}}$ and smartcard to log into the hospital system to register with EPR-Host. Then the registration procedure continues as follows;

1. $HCP \rightarrow EPRHost : I_{v_{j'}}, NC_{v_{j'}}$
2. $EPRHost \rightarrow HCP : r_1$
3. $HCP \rightarrow EPRHost : \mathbf{sign} S_{v_{j'}}(r_1), r_1$
4. $EPRHost \rightarrow HCP : \mathbf{sign} S_{\mathcal{H}}(r_2), r_2$
5. $HCP \rightarrow EPRHost : Yes/No$. The HCP receives the second challenge $r_2$, and registers if confirmed using verification key $P_{\mathcal{H}}$ (stored in his smartcard), that the challenge is indeed from the EPRHost.

In this protocol, challenges are signed using the private keys to prevent an attack of a man in the middle.

IV. ***Patient's Registration with TTP.*** The patient $u_j$, physically submits his credentials to the hospital authority for approval. If credentials are valid, the hospital securely sends an application form for the patient's smartcard $AF_{u_j}$ to the TTP. The TTP assigns the smartcard with a card number $NC_{u_j}$ and generates the patient's forward signature key pairs $(S_{u_j,t}, P_{u_j}), (\tilde{S}_{u_j,t'}, \tilde{P_{u_j}})$, identifier $I_{u_j}$, and the patient's mobile symmetric key $K_{\Omega,u_j}$. $K_{\Omega,u_j}$ is used to facilitate EPR emergency access. Where $P_{u_j}, \tilde{P_{u_j}}$ are patient's verification and master keys respectively. The two keys are also used for decryption hence must be kept secret. The TTP then assigns the patient's personal identification number PIN, $\pi_{u_j}$ and creates the patient's smartcard. Thereafter, the TTP securely mails the card and PIN separately to the hospital. Finally, the patient is informed that the card and $\pi_{u_j}$ are ready for collection. Following are the steps used by the hospital to register the patient with the TTP.

1. Steps $1, 2$ in protocol II are first repeated (use $AF_{u_j}$), then the TTP assigns to the patient's smartcard; pairs of forward signature and encryption keys $(S_{u_j,t}, P_{u_j})$, $\tilde{S}_{u_j,t'}, \tilde{P_{u_j}}$, an identifier $I_{u_j}$, and a smartcard number $NC_{u_j}$. The TTP assigns also $K_{\Omega,u_j}$.
2. The TTP creates a smartcard for the patient. Using the smartcard and its computer system, the TTP selects the patient's PIN, $\pi_{u_j}$. Upon interaction between TTP system and the smartcard, $\pi_{u_j}$ is converted into $h(\pi_{u_j})$. The TTP temporar-

ily keeps $h(\pi_{u_j}) = K_{\pi_{u_j}}$ and uses it as an encryption key. Then the TTP permanently stores $h(h(\pi_{u_j}))$ in the smartcard for integrity check purposes. Where, $K_{\pi,u_j}$ is a patient's symmetric encryption key. The TTP sends to the smartcard; the card number $NC_{u_j}$, signed patient identifier $\mathbf{sign}S_{u_j,t}(I_{u_j})$, encrypted master key $\mathbf{e}K_{\Omega,u_j}(\tilde{P_{u_j}})$,$\mathbf{e}K_{\pi,u_j}(\tilde{P_{u_j}})$ , encrypted generation key $\mathbf{e}K_{\pi,u_j}(\tilde{S}_{u_j,t'})$, and encrypted patient's identifier $\mathbf{e}K_{\pi,u_j}(I_{u_j})$. It also enters in the smartcard $h(\tilde{P_{u_j}})$ for the master key integrity check. The key $\tilde{S}_{u_j,t'}$ is used to generate EPR encryption keys.

3. The TTP stores in its records the patient's; $NC_{u_j}$, credentials, Signature key $S_{u_j,t}$, identifier $I_{u_j}$, and symmetric mobile encryption key $K_{\Omega,u_j}$.

4. The TTP sends to the mobile gateway the patient's; public key $P_{u_j}$, identifier $I_{u_j}$, Card number $NC_{u_j}$, and mobile symmetric key $K_{\Omega,u_j}$. Finally, steps $6, 7, 8$ in protocol II are repeated.

V. ***Patient's Registration with EPRHost.*** Having registered with the TTP, a patient is required to prove to the hospital that he is the one registered with the TTP and is entitled to get medical care services from a given hospital. It only after such verification, the HCP can facilitate the creation of electronic patient record in the EPR-Host. The registration procedure is as follows;

1. The patient firstly physically interacts with HCP and then is requested to insert his smartcard into the HCP's system followed by keying in his PIN $\pi_{u_j}$.

2. The HCP's system retrieves from the patient's smartcard; $NC_{u_j}$, $\mathbf{sign}S_{u_j,t}(I_{u_j})$ and assigns a file number $NF$ to be used as a reference number of the EPR to be created. The HCP system sends these parameters to the mobile gateway $\mathcal{G}_\Omega$ through the hospital gateway $\mathcal{G}_\mathcal{H}$. The hospital gateway extracts $NF$ and stores it. The remaining parameters are passed to the mobile gateway where the patient's identification $I_{u_j}$ is verified using the patient's public key, $\mathbf{ver}P_{u_j}(\mathbf{sign}S_{u_j,t}(I_{u_j}))$; and the card number $NC_{u_j}$ is authenticated.

3. The mobile gateway confirms the existence of such a patient and sends to the HCP a message permitting the creation of an EPR. The HCP sends the $NF$ to the EPRHost. The EPRHost creates an EPR form for a given patient.

4. If there are records entered, the HCP the system facilitates the signing of the record using HCP's private group signature key $\bar{S}_{v_{j'},t''}$ and the patient's key $\tilde{S}_{u_j,t'}$. The system enables encryption of the medical records using the patient's EPR encryption key and stores the records in the EPR-Host.

5. The HCP's system compresses (takes a hash of) the entered patient's the medical record and sends the $h(M_i) = \sigma_{M_i}$ to the hospital gateway for future medical

record integrity check purposes.

## CONCLUSION

This paper has shown the scheme that insures privacy of patients and HCPs. This is based on the fact that, for the patient to be registered with the hospital EPRHost, his consent (PIN) must first be obtained. The patient's registration with the hospital EPRHost results in the creation of an EPR, which requires the HCP's and patients involvement. The HCP can create the patient's EPR only with the patient's consent availability. This ensures that the patient remains a co-owner and responsible for his EPR. The need for both HCPs and patient to sign the EPR ensures the sharing of accountability between them. These signatures are put on the message digest of the EPR which also guarantees the EPR integrity and efficiency of the scheme. This scheme can also be used in an emergency situation [5].

## REFERENCES


[1] M.S. Bleumer. Privacy oriented clearing for the german health care system. In *Personal Information Security, Engineering and Ethics*. Springer-Verlag, 1997.

[2] B. de Meideiros, G. Ateniese, and R. Cutmola. Medical information privacy assurance: Cryptographic and system aspects. In *SCN02, Third Conference on Security in Communication Networks*. Springer, 2002.

[3] D. Gordon. What is an electronic patient record? In *American Medical Informatics Association Annual Symposium*. AMIA, 1998.

[4] Gene Itkis and Leonid Reyzin. Forward-secure signatures with optimal signing and verifying. *Advances in Cryptology, LNCS*, 2139:332–354, 2001.

[5] Kosmas Kapis, Jan C.A.vander Lubbe, and Kathy Cartrysse. Cryptographic approach to patient records privacy protection in emergency situations. In *Twenty-fifth Symposium on Information Theory in the Benelux*, pages 177–184, June 2004.

[6] Dawn Xiaodong Song. Practical forward secure group signature schemes. In *ACM2001, 8th ACM Conference on Computer and Communication Security*, pages 225–234, 2001.