Proposal of a Secure Electronic Prescription System

Hugo André Malheiro Rodrigues
Faculty of Medicine of Porto, Portugal
hugoamrodrigues@gmail.com

Luís Antunes
Faculty of Sciences of Porto, Portugaal
antunes.lfa@gmail.com

Manuel Eduardo Correia
Faculty of Sciences of Porto, Portugal
mdcorreia@gmail.com

Abstract — Since 2011, it's mandatory to prescribe through an electronic system in Portugal. Several third party companies start to develop prescribing software/interfaces that act as gateways to transmit the prescription data from the practitioners to the Health Ministry. The use of those companies in this circuit weakens the Prescription System's security levels and compromises the confidentiality and privacy of doctors and patients' personal data.
Aim: The main aim is to propose a secure and safer Prescribing System that allows prescriptions' authentication and protects the patient data, keeping their identity confidential.
Results: By protecting several system flaws, this proposed increases greatly the Prescription System security levels, protects patient data, and avoid its collection from Third Party Companies. Also the physical model of the electronic Prescription appears to have all the security and applicability requirements needed to function during a communication network dysfunction.

Keywords-component; electronic prescribing, patient data, security, data encription, confidentiality, smartcard.

I. INTRODUCTION

The electronic prescription systems (EPS) brought the concept of a safer, smarter, and cheaper medication-management systems. The EPS's functionality demands immediate access to the patients' information from several health entities, which brings risks related with privacy, confidentiality and security of patients' clinical data. The potential of future EPS may be compromised if no policy refinements are established in order to let physicians confident about a networked sharing of patient health information [1].

Data privacy requires a special highlight in the context of clinical information protection: on first place, more non-medical entities involved implies a more complex and hard to manage system; on second place, prescribers and patients' involvement must be protected, specially their identity and the information traded between. However, there shouldn't be completely anonymous prescriptions because there are certain scenarios that demand the intervenients' identification, for example in case of lawsuits. The data should circulate anonymously but remain the capability to be restored in the network's mainframe (under the Health Ministry's protection), in order to allow researches, processes and resolve responsibilities [2].

Properly implemented medication registry systems are rare today and the fragmented information into several systems and organizations requires an additional preoccupation about the security used on the clinical data transmitted. Clinical data's security is easily overlooked by the public health entities, since it does not have a direct impact in the organizations' finances or management. But if this information is exploited, it can represent catastrophic damages to the individuals involved, especially if related to private insurers, credit companies and even the professional levels [3].

The idea of use smartcards for digital identification appears described in the literature since 1997 by Jaakko Niinima and Jari Forsstro (medical informatics' specialists from Finland) [3,4]. The concept of electronic prescription is also an assessment for drugs and financial management. It helps to prevent drugs reactions, allergies and poli-medication errors but "the integrity, security and confidentiality of data must be ensured" [4]. The smartcards seems to be the easier authentication and encryption method to be implemented in a EPS. Other hypothesis would use a pseudo-anonymous identification to minimize the security and confidentiality problems of the involved data [4,5]. Another study from in Thailand, proposed a Service-Oriented Architecture Prescription System to ease communications between the numerous information systems and, at the same time, protect the anonymity of the involved people (with pseudonyms and proxy signatures) and control the prescriptions emitted (to avoid eventual scenarios of corruption) [6].

II. THE PROBLEM

The propose described in this paper aims to improve an EPS that interacts with several electronic prescription software developed by third party companies (TPC), more specifically the Portuguese EPS [7]. For this kind of scenarios, it's important to invest in a system with safe communications between the various health entities.

Because it's easy to establish direct connections between some medicines and active pathologies, if a data leakage occurs on a TPC, the prescription data will be very valuable to some organizations (Figure 1), for example:

- Pharmaceutical laboratories (marketing);
- Insurance companies (life insurance);
- Banking institutions (bank loans);
- Companies wishing to hire new employees (physical and psychological ability);
- Among other reasons and examples...

978-1-908320-13/1/$25.00©2013 IEEE

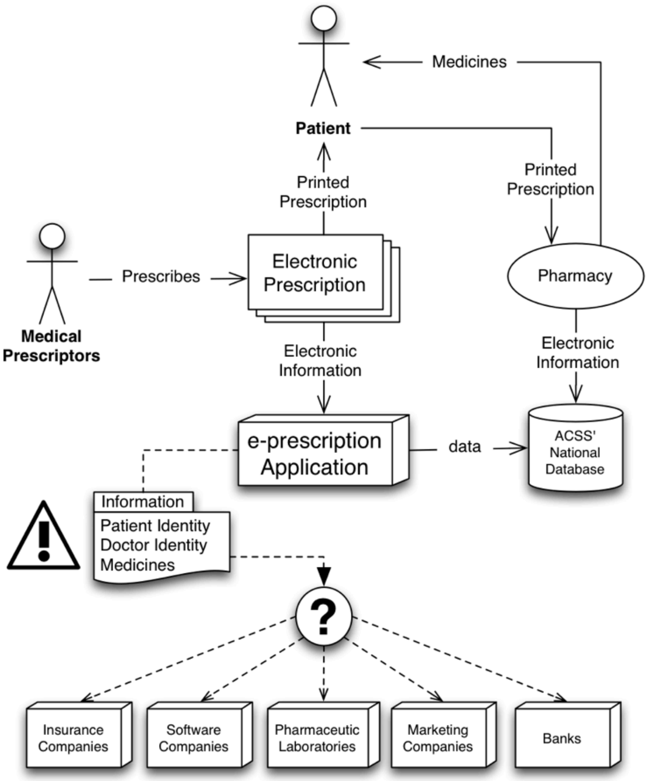


Figure 1. EPS and TPC and its potential risk of information leakage

This situation, although it seems a simple health services evolution, is a potential weakness in a delicate established and it should be avoided or corrected as soon as possible.

III. EPS Proposal

The most viable solution for an EPS already implemented that presents follows the previous conditions would be to implement communication protocols and the technological devices to correct the identified flaws. To regain the confidence of health professionals it's important to prepare a certification system able to provide a transparent and reliable solution and maintain the confidentiality and authenticity of clinical and personal data.

This model needs some technical requirements, such as professional electronic cards (prepared with a mechanism for accreditation, using public and private keys to identify the prescriber medical professional), a certification system (with Certificated Authorities, responsible for distributing the medical certificates) and smartcards readers on the doctor's workstations.

A national database for consulting previous medications would be previously prepared since the new model intends to protect the prescriptions and avoid any other history service to operate.

A. EPS – Registration

The first step would be the registration of the professional on the Health Ministry's platform, only possible after authentication with the EPC. At this moment it's validated the doctor's identity in the National Medical Association (NMA) and his current status (to check if is authorized to prescribe). After this verification, is created a secure channel for data transmission where the practitioner has to introduce his identification data and professional details (or import it from NMA records) with discrimination of establishments where he actually practices medicine. This process finishes with a random 256-bit password generation, encrypted with the doctors EPC's public key, transmitted to the doctor's computer and written with only-read permissions on the EPC (Figure 2). In this way, the Health Ministry's encrypted key can only be used after entering the doctor's PIN code, which protects the certificate and decrypt it with the private key, preventing the doctor from having knowledge of the real key has been assigned (Figure 3).

This method has the advantage of use a fast computing symmetric key that is only stores in two locations: the Doctor's EPC and the Health Ministry's Server.

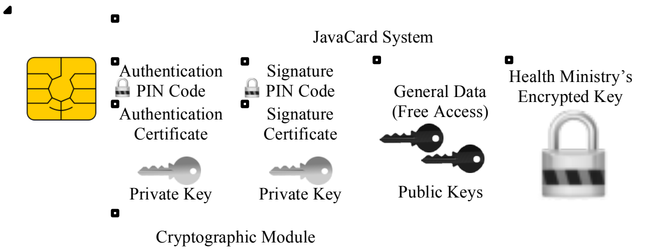


Figure 2. Electronic Professional Card Model

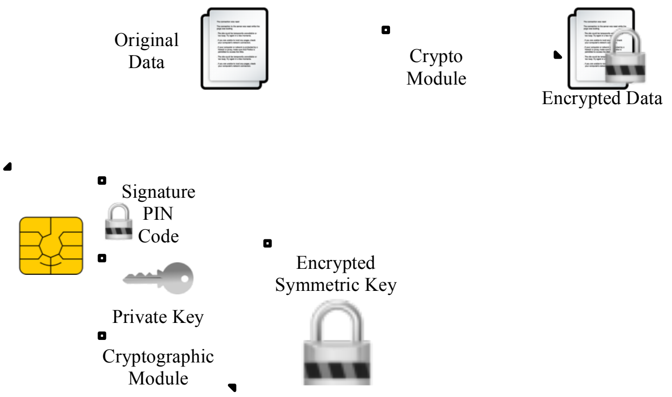


Figure 3. Data encryption model with the EPC

B. EPS – Company Contract

The second step is the dematerialization of the TPC contracts with the prescribers, also done online using EPC. After the doctor confirms his identity and current professional status authorization of prescription, the company would send the doctors identification to the Health Ministry server who would generate an one-time pad password and send it to the professional's profile associated contact (telephone, e-mail or regular mail store in the Health Ministry database). The submission of the correct password would associate the physician to the TPC and the Ministry of health would be notified of the recruitment. This step requires the establishment of communication protocol between the companies and the Ministry to allow a real-time secure registration.

C. EPS – The Electronic Model

All the software from the TPC must have to be equipped with an authentication mechanism through the EPC, protected by the corresponding PIN. This mechanism is easily implementable in primary care, hospitals and other healthcare facilities and it solves the credentials' sharing problem at the computer terminals. By removing the CPE, the session would suspend, and after some minutes of inactivity it would record the working data and would sign-out the session.

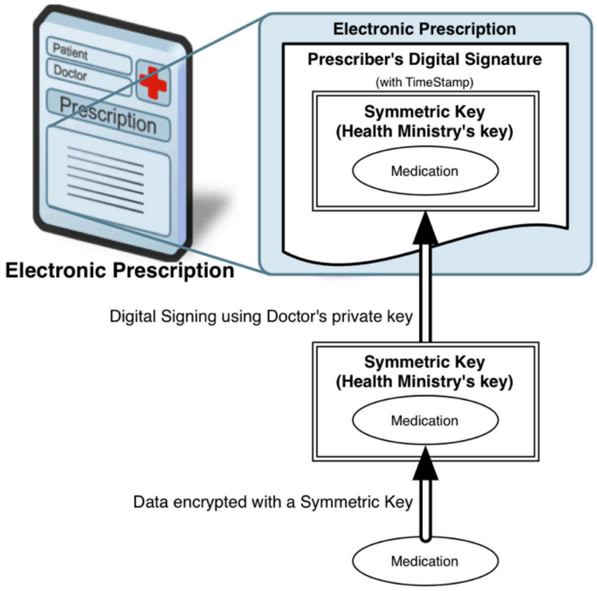


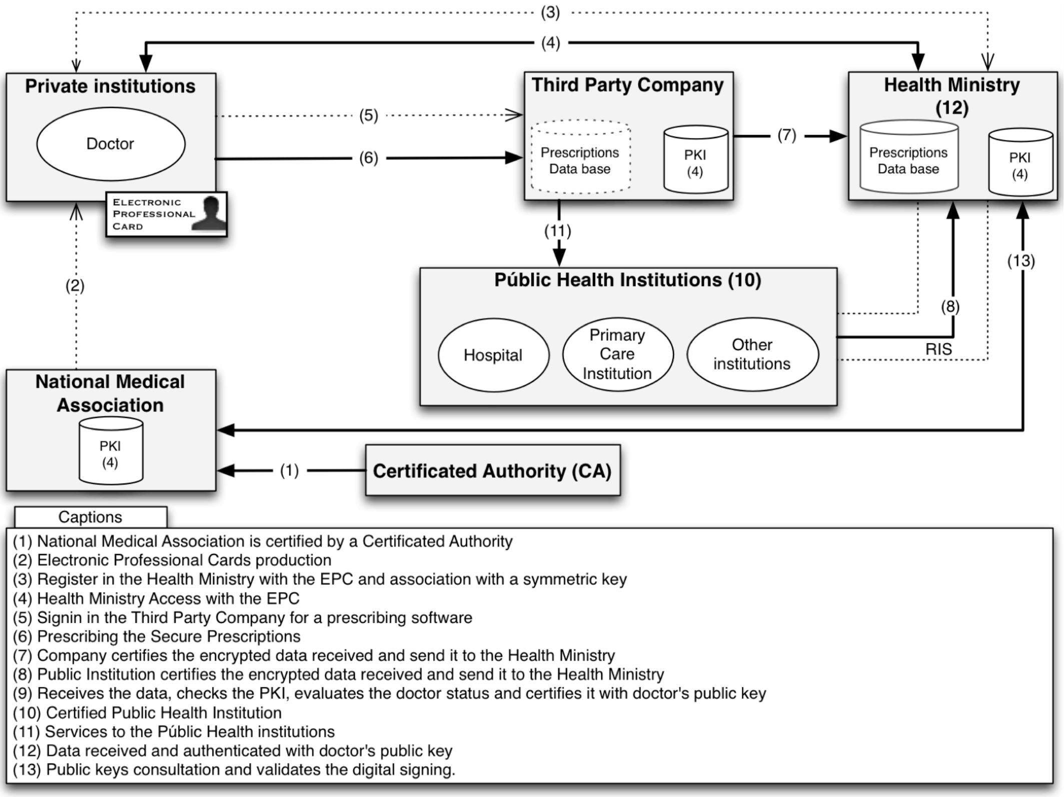
Figure 4. Secure Prescription's Model

The model previously described includes in the same smartcard a symmetric key and an asymmetric key allows secure data authentication (using digital signature) and data encryption (using the Health Ministry's key). With these functionalities, it's possible to create a prescription, encrypted by the Health Ministry's key and encapsulated with a time-stamp digital signature (Figure 4).

During the prescribing, the doctor may select from a list the medicines he pretends, its dosage and posology. To confirm the prescription, the signing PIN code which must be entered to unlocked the access to the module that contains the private key, access the stored password and encapsulate the encrypted information with doctor's digital signature.

This format has the advantage of allow any intervenient in the prescription transmission to check the authenticity of the information received (by using the public key of the doctor). Though, the content of the prescription can only be accessed in the Health Ministry Server where is store the other copy of the password that encrypt all data

Since the key is shared only by two intervenients, as outlined in Figure 5, the TPC can continue to promote and assist the electronic prescribing with data confidentiality of patients.



(1) National Medical Association is certified by a Certificated Authority
(2) Electronic Professional Cards production
(3) Register in the Health Ministry with the EPC and association with a symmetric key
(4) Health Ministry Access with the EPC
(5) Signin in the Third Party Company for a prescribing software
(6) Prescribing the Secure Prescriptions
(7) Company certifies the encrypted data received and send it to the Health Ministry
(8) Public Institution certifies the encrypted data received and send it to the Health Ministry
(9) Receives the data, checks the PKI, evaluates the doctor status and certifies it with doctor's public key
(10) Certified Public Health Institution
(11) Services to the Públic Health institutions
(12) Data received and authenticated with doctor's public key
(13) Public keys consultation and validates the digital signing.

Figure 5. EPS scheme with the Secure Prescription Model

IV. Discussion

This work was intended to draw attention to the various existing flaws in the electronic prescription system and to the aspects of security and data privacy, which are recognized worldwide as a major concern.

The proposal of a prescription system serves to demonstrate that the imperfections can always be improved.

However, the system described here is not perfect, and there are always flaws that will depend on others and the level of civility of their stakeholders.

As with any authentication system without communication with the network, it is not possible to exclude the possibility of multiple layoffs in the same prescription, why keep the signature as a means of legitimizing the medical prescription.

With this method is not possible to access to the prescription's history from the TPC servers, neither from other prescribers, neither from the own doctor history. It may sound a disadvantage from the practitioner's point of view but represents a major security advantage. The logical solution would be prepared a secure national network for consultation of the prescription history with digital authentication to trace the system users and what information they consulted.

The necessity of an additional programs or driver may also represent some difficulties for the TPC, especially the ones who provide a web interface system because it would be dependent of the installation of a middleware, for example, to access the smartcard modules, perform the encryption and apply the doctors signature.

The positive points are: access to prescription software through the EPC; real-time validation of doctors' professional status; implementation of a safe enrolment with dematerialization of hiring medical software companies; validation of the prescription by any of the intervenients; create secure prescriptions that keep the patients data private and confidential.

References

[1] M. D. Greenberg, M. S. Ridgely, and D. S. Bell, "Electronic prescribing and HIPAA privacy regulation," Inquiry, vol. 41, pp. 461-8, Winter 2004.

[2] Y. Yang, X. Han, F. Bao, and R. H. Deng, "A smart-card-enabled privacy preserving E-prescription system," IEEE Trans Inf Technol Biomed, vol. 8, pp. 47-58, Mar 2004.

[3] J. Niinimaki, M. Savolainen, and J. J. Forsstrom, "Methodology for security development of an electronic prescription system," Proc AMIA Symp, pp. 245-9, 1998.

[4] J. Niinimaki and J. Forsstrom, "Approaches for certification of electronic prescription software," Int J Med Inform, vol. 47, pp. 175-82, Dec 1997.

[5] V. M. Brannigan and B. R. Beier, "Patient privacy in the era of medical computer networks: a new paradigm for a new technology," Medinfo, vol. 8 Pt 1, pp. 640-3, 1995.

[6] T. C. Hsiao, Z. Y. Wu, Y. F. Chung, T. S. Chen, and G. B. Horng, "A secure integrated medical information system," J Med Syst, vol. 36, pp. 3103-13, Oct 2012.

[7] ACSS, Software para prescrição eletrónica de medicamentos, 2012. – Link: http://www.acss.min-saude.pt/Portals/0/Emp_sw_ certificado _2012-01-09.pdf