A Secure Electronic Prescription System

Hugo Rodrigues
Faculty of Medicine of Porto, Portugal

Manuel Eduardo Correia
Faculty of Sciences of Porto, Portugal

Luís Antunes
Instituto de Telecomunicações, Faculty of Sciences of Porto, Portugal

Abstract

Abstract — Since 2011, is 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. 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. 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.

1. 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. Data should circulate anonymously and 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 smart cards 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 medicines and financial management. It helps to prevent medicines reactions, allergies and polymedication errors but "the integrity, security and confidentiality of data must be ensured". [4]

There are different standards that allow health information exchange and interoperability between Health Information Systems, such as HL7 or openEHR that may be used for prescriptions' data storage and transmission. How ever, these standards documentation assumed that encryption happens below the application layer (via IPSec or TLS) or using Web Services Security Features [5] and not within HL7 messages. In order to protect the medical information is necessary a whole new classes of administrative and infrastructure messages to establish and maintain organizational trust, communicate shared secrets (keys), user/entity authentication, etc. [6]

Other hypothesis is to use a pseudo-anonymous identification to minimize security and confidentiality problems of the involved data [4, 7]. 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). [8]

Another possible solution is the use of smart cards and digital signing. The smart cards in the health area may assume different functions and be

used as an ID card, a simple device to store patients' information or an authentication token to access the system. From a technological point of view, smart cards allow the professionals to be authenticated, documents to be digital signed and encrypted.

This technology is being implemented in several health projects for more than one decade [9] and it represents an asset to the current prescription systems. It can be found is some EPS [10], either as a data storage device, as an authentication card.

This paper intends to focus on security during the transmission of the prescription data and the possibility to protect patients' information from third-party entities involved in the EPS.

2. The Problem

Electronic prescribing became mandatory in Portugal, according to its legislation, since 2011 in order to reduce costs and start to dematerialize the prescribing processes. It's also believed that logging and tracking prescription activities will help in fraud prevention. [11]

Portuguese government stimulated software houses to develop software and services that would send data from public and private institutions directly to the Health Services Central Administration (ACSS). Consequently, many software houses developed numerous sets of e-prescribing software and web-services that were submitted for ACSS to approval, resulting in a variety of applications available on the market. [8]

Francis France considers the Heath care environment physically very open, vulnerable to theft, damage and unauthorized access. [12] Comparing to other kind of data (financial, academic, scientific, etc.), clinical information is required to be accessible in any time and its storage is also retained for a long time. [13]

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. [14] For this kind of scenarios, is important to invest in a system with safe communications between the various health entities.

Figure 1 represents e-prescribing stakeholders and their roles. Physicians are responsible for prescription filling and delivering to patients in a printed format. At the same time, that information is transmitted to ACSS National Database through the e-prescription application. The patient withdraws the drugs at the pharmacy and is confirmed at ACSS. The prescription's data is valuable for the organizations mentioned before, what turns them stakeholders too.

The facility to establish direct connections between some medicines and active pathologies, if a data leakage occurs on a TPC, makes the prescription data to 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...

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

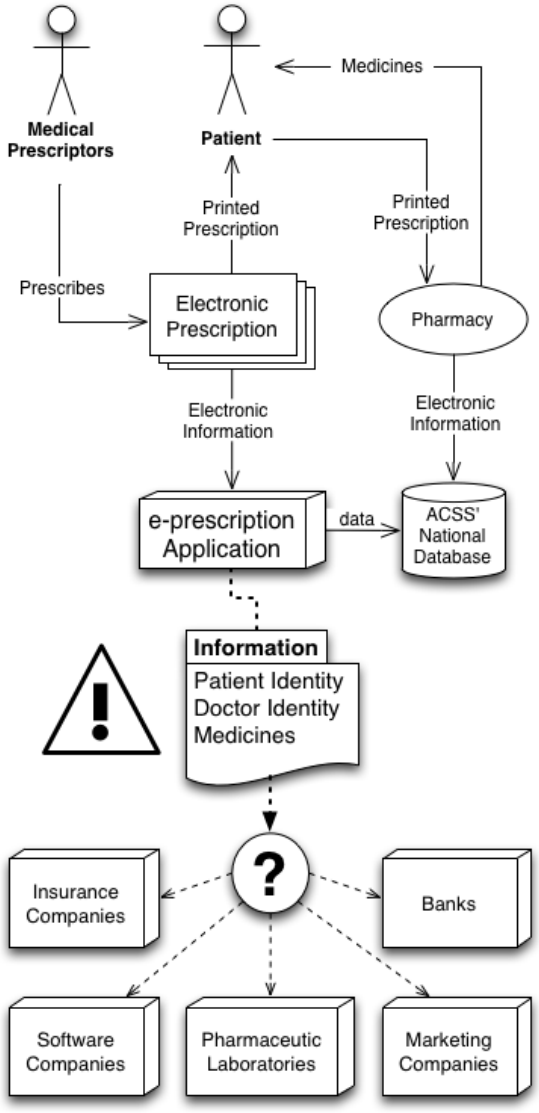


Figure 1. EPS and TPC and its potential risk of information leakage

An example of this situation (clinical data access) may happen this year in England, once national medical data database has been created. Drugs Companies and Insurance Companies may be able to buy and access information about patients (from

medical diagnosis to daily habits, including mental health conditions, cancer). [15] Fortunately, privacy experts are concerned about this announcement because of patient's confidentiality and privacy, even if the data is pseudo-anonymized.

3. Electronic Prescription System

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 is 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.

3.1. Requirements

This model needs some technical requirements, such as:

- Professional electronic cards (smart cards) prepared with a mechanism for accreditation, using public and private keys to identify and authenticate the prescriber medical professional, and permit digital signing;
- Certification system, with Certificated Authorities, responsible for distributing the medical certificates;
- Smart cards readers on the doctor's workstations to read the Professional electronic cards;
- National prescription database, for consulting previous medications, since the new model intends to protect the prescriptions and avoid any other history service to operate;
- Online platform to manage professional personal data, access codes and to associate the professional credentials to the prescription systems or work places; it may act as a portal to access the national prescription history database.

3.2. Distributing the Professional Certificates

Since every medical doctor must be member of the National Medical Board, this organization would be the responsible for validate and certify the professionals in order to authorize them to prescribe.

This validation must be in person and, one by one, the professional must fill and sign the required documentation, in order to update their personal information and to generate a qualified digital certificate by a certificate authority. The doctors' personal data will be stored in the National Medical Board system and will remain secure and confidential.

The certificate authority, will generate the certificates to be included in the professionals smart card, among other professional information like license number, specialty, sub-specialties or other relevant skills the professional have achieved.

The certificates include a public-key and private-key pair. The professional public-keys will be stored in a Public Key Infrastructure (PKI) and accessed by a Online Certificate Status Protocol server to validate either the professionals identity, either the electronic prescriptions veracity. If a professional is not allowed to prescribe, the certificate will be revoked and the system will refuse any attempt to generate electronic prescriptions.

The professional smart card (Figure 2) has a chip where the public-private keys are stored and protected by a PIN code. It can be used as a regular ID card (for visual identification) and an electronic ID (for electronic authentication). It consists in a Java Card technology-enabled smart card that allows applets written in the Java language to be executed within the card (in a Java Card Runtime Environment). [16]

The medical doctor is able to use the card, not only to authenticate in the system but also to digitally sign documents and avoid information repudiation by the author. The card reader technology and public-key cryptography standards are quite spread

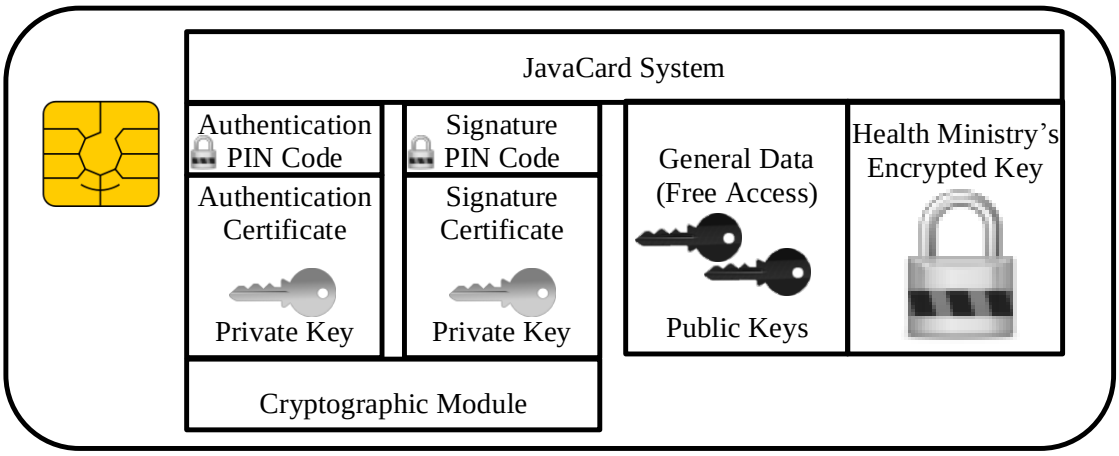


Figure 2. Electronic Professional Card

over the Europe and by using an authenticated authority their credentials are valid in different countries.

After manufacturing, the smart cards can be received in person (at the National Medical Board) or at home (by registered letter, with all the security levels used for delivering a bank card).

The professionals can change the PIN code and personal data by accessing the online platform with the smart card.

3.3. Sharing the Symmetric Key

When the smart cards are delivered and the professional PKI is created, it's possible to advance to the next step of this model and associate the medical certificates with work places or prescription systems used in the country.

The professional can sign-in at the online platform, using their professional electronic card and a smart card reader. During the sign in process, doctor's identity and current status (is authorized to prescribe?) are verified through the National Medical Board PKI. After this verification, is created a secure channel for data transmission and it's generated a random 256-bit key 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).

By sharing the encrypted symmetric password we guarantee that it only relies in two locations (the Doctor's EPC and the National Medical Board server.

This process allows the combination of a 256 bits generated symmetric key and the professional's asymmetric keys (public-private keys). Symmetric keys allow a simpler and faster encryption process. Asymmetric keys advantages are authentication, detection of tampering and non-repudiation of the transmitted information. By combining both methods it's possible to use the best potentialities of each.

Since the generated key is encrypted with the professional public key and stored in the smart card memory chip, it cannot be directly accessed. However, applets executed inside the card can access the symmetric encrypted key, decrypt it using the private key (Figure 3-A) and use it to encrypt the information to be transmitted (Figure 3-B). To access this routine, the card owner must insert the 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).

When the professionals signs in to their personal account at the online platform, they can: manage some of their personal information (like address, phone contact, email); subscribe

3.4. Subscribing the Electronic Prescription Systems

After receiving the symmetric password, the practitioner has access to his account section (for managing the personal information like address, phone contact, email) and the subscription section. The subscription section is designed for subscribe or revoke the health establishments where the professional practices medicine). The third party prescription systems (certified by the Health System) are also on the list, if the doctor wants to prescribe at home or as member of a private institution. Each institution and prescription system are identified by a

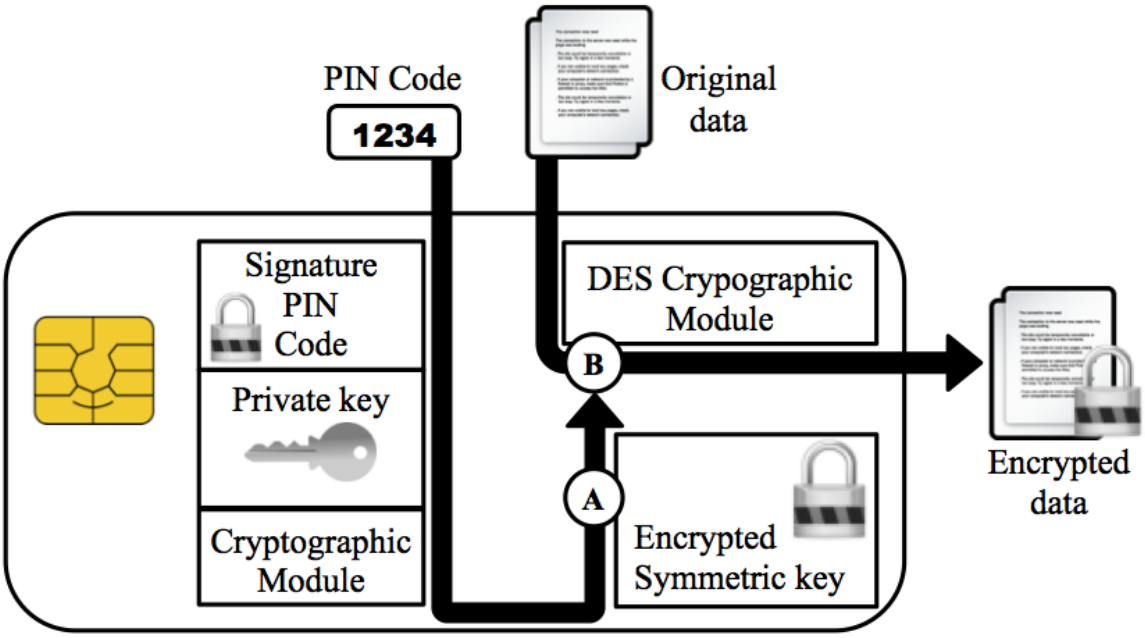


Figure 3. Data encryption in the Electronic Professional Card using the symmetric key

unique identification code.

When a work place is subscribed, the institution is informed and if the doctor has contract with it, the subscription is complete and the professional may prescribe using the institution EPS.

The electronic subscription may represent the dematerialization of the TPC contracts with the prescribers. When the doctor accesses the online platform, is identified as a legit and authorized professional. By choosing a system, it's generated a specific password to complete and officialize the contract with the companies. If the password is not activated, it expires in a few hours. The user may request more codes in order to access two or more EPS.

When the professional provides the specific password during the services agreement, the company is informed that a valid and authorized prescriber is contracting their services. The professional is identified by the electronic authentication plus the access code and his personal data (as contact phone number, address, email, signature, ID card) is protected.

When the contract is complete, the company returns confirmation to the online platform and the EPS is flagged as subscribed. The EPS is associated to the physician account and the Health Ministry is notified about the recruitment. From this moment the electronic prescriptions generated by that professional in that system are accepted by the system.

3.5. Electronic Prescribing

All the software from the TPC must be equipped with an applet to permit user authentication using the professional smart card and access the cryptographic module, protected by a PIN code.

Such mechanism is easily implementable in primary care, hospitals and other healthcare facilities and it solves the credentials' sharing problem in the health sector. The prescriber connects to the national database by inserting the EPC in the card reader, typing the PIN code and authenticating in the electronic health system.

Every time a prescription is generated, the signature PIN code is requested for digital qualified signing, which replaces handwriting signatures and supports the prescribing system dematerialization (Figure 4-A).

Since the EPC is the only legal ID document, it's assumed that the professionals will be concerned about the card and its location. When the doctor leaves the work terminal, must withdraw the card and carry it personally (because it's the professional visual ID card). Once the EPC is removed from the card reader, the terminal is locked, the session is suspended and, after some minutes of inactivity, all

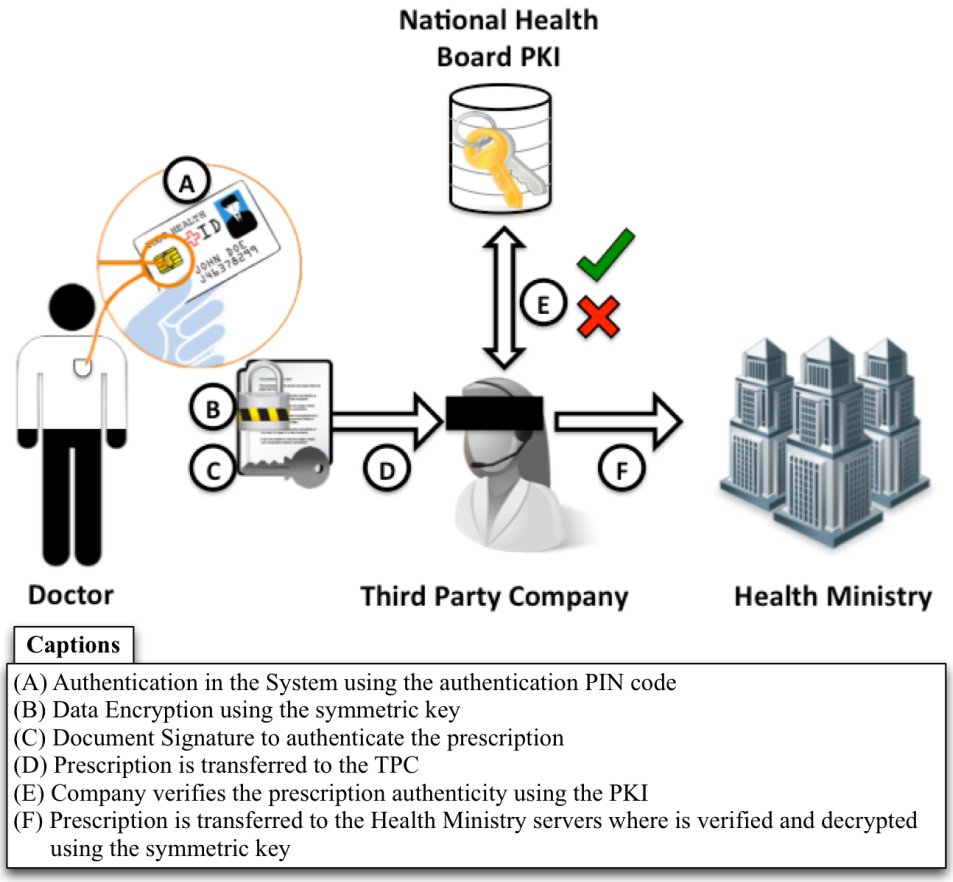


Figure 4. Electronic Prescribing using the symmetric key and digital signature

non-saved data is recorded (presented to the professional in the next time login to decides if it should be saved or discarded) and the doctor is logged out system. In case of a second session is started, the first session is closed.

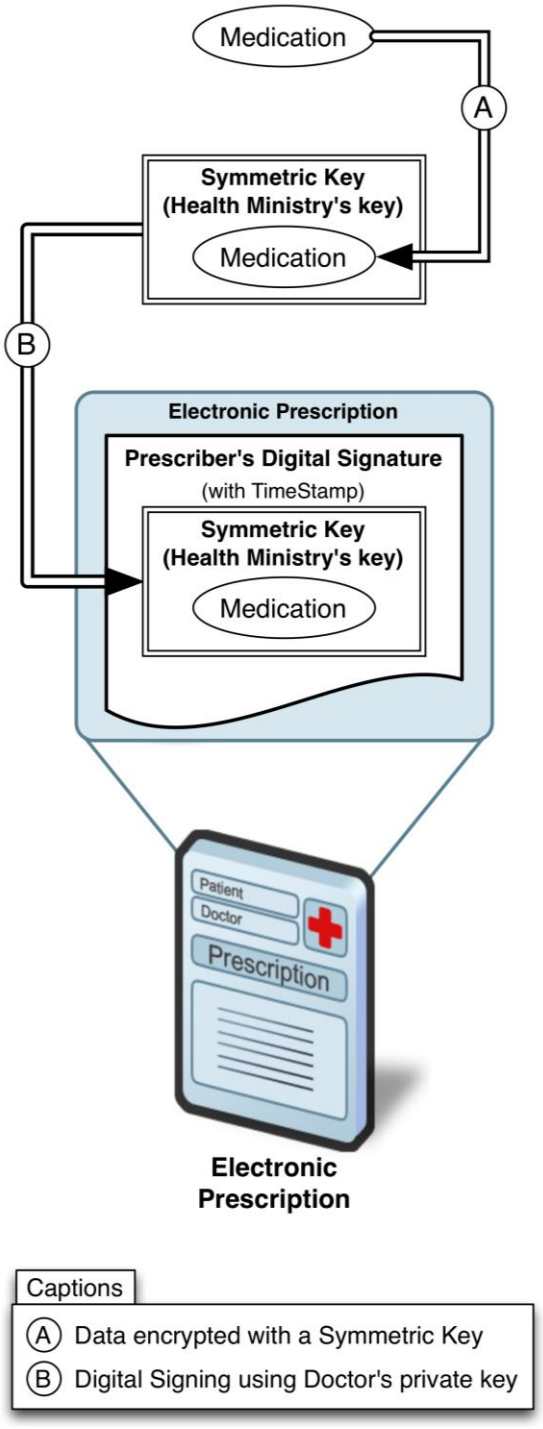


Figure 5. Secure Prescription's Model

The model previously described includes in the same smart card a symmetric key and an asymmetric key. It allows a fast data encryption and a secure data authentication, respectively. All these functionalities, allows to create a prescription, encrypted by the symmetric key (Figure 5-A) and encapsulated with a time-stamp digital signature (Figure 5-B).

The doctor may select from a list, the medicines he pretends, its dosage and posology. To confirm the prescription, the signature PIN code is requested to unlock 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 allows to check the authenticity of the information received by any intervenient in the prescription transmission by consulting the PKI (Figure 4-E). 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.

4. Discussion

This work was intended to draw attention to the several existing flaws in the EPS and to the aspects of security and data privacy, which are recognized worldwide as a major concern. The system described is not perfect and serves to demonstrate that the imperfections can always be improved. There are always flaws that will depend on others and the level of civility of their stakeholders.

Is necessary to connect electronically the private institutions to the health ministry. But, without communication with the intra network, must be implemented a secure system that protects the prescription data.

The described method makes impossible to the TPC to collect patients prescription data for history proposes, 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 best solution is to create a secure national network for prescription history consult, with digital authentication to trace the system users and what information have been consulted.

The necessity of an additional programs or drivers 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 smart card modules, perform the encryption and apply the doctors signature.

Since the symmetric key is shared only by two intervenients, as outlined in Figure 6-(3), the third party companies may continue to promote and assist the electronic prescribing without compromising patients data confidentiality.

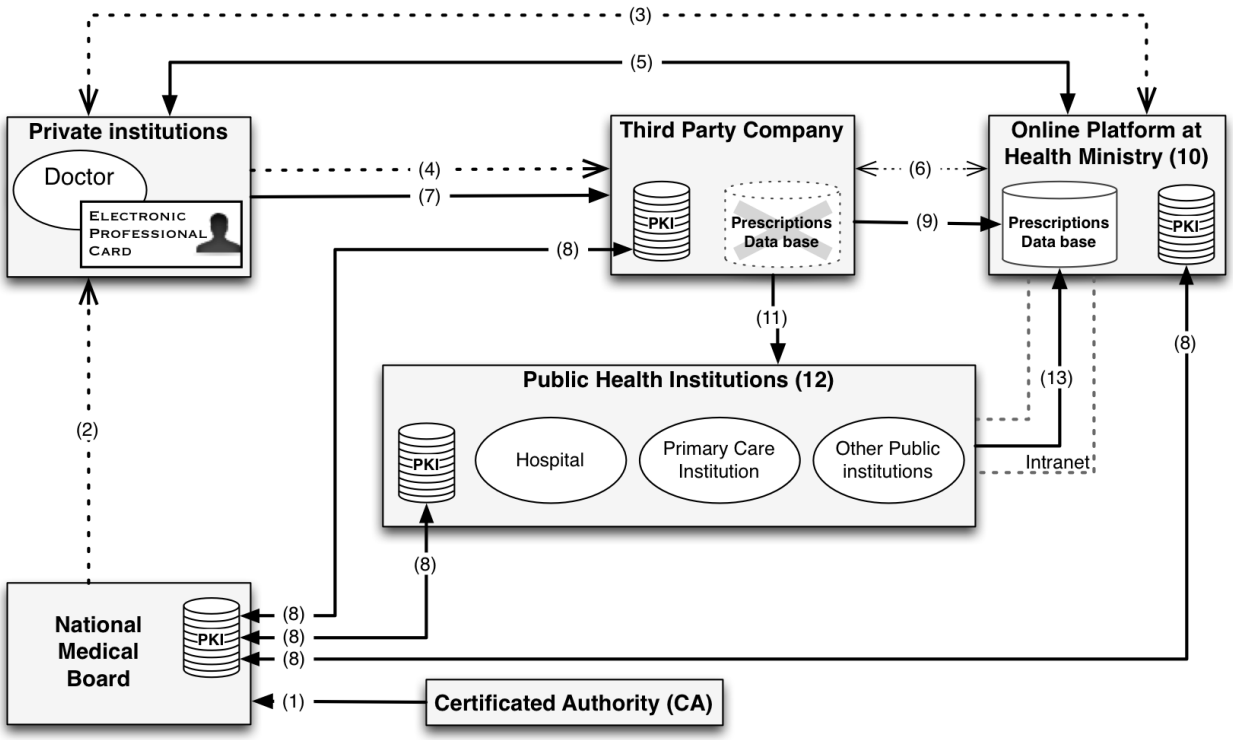
The global view of the system is represented in Figure 6, with all its intervenients and interactions.

In a few words, this system permits:

- control and easily update professionals' permissions to prescribe;
- access to prescription software with a smart card integration;
- establish a real-time validation of doctors' professional status;
- implement a safe enrolment capable of TPC contracts dematerialization;
- increasing professionals personal data privacy;
- validate of the prescription by any of the intervenients;
- avoid third party companies to collect patients clinical data and professionals personal data;
- create secure prescriptions that keep the patients data private and confidential.

5. Acknowledgments

This work is supported by the Master Degree in Medical Informatics of the University of Porto (http://mim.med.up.pt) and by the National Science Foundation, Fundação para a Ciência e Tecnologia (FCT), through FEDER funds through Programa Operacional Factores de Competitividade – COMPETE through the project CSI2 with the reference PTDC/EIA-CCO/099951/2008, through



Captions

(1) Certification of the National Medical Association by a Certificated Authority
(2) Production and distribution of the Electronic Professional Cards (EPC)
(3) Registration at the online platform, Symmetric key transference and subscription of the Electronic Prescription System (EPS)
(4) Contract with a Third Party Company (TPC) for a EPS using the specific password requested at the online platform
(5) Access to the professional personal account, prescription history, and EPS management, using the EPC
(6) Association of the contract number and the prescriber's account
(7) Electronic prescribing, after doctor status verification, encrypted with the symmetric key, digitally signed and sent to the TPC
(8) Checks the PKI, evaluates the doctor status and if is authorised to prescribe
(9) Encrypted data transmitted to the Health Ministry
(10) Data received, authenticated with prescriber's public key, decrypted with symmetric key and stored in the prescription database
(11) Services to the Public Health institutions
(12) Certified Public Health Institution
(13) Public Institutions verify the encrypted data received and send it trough the National Health System intra-network

Figure 6. Secure Electronic Prescription System

the project with the reference PEST-C/SAU/UI0753/2011.

6. 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] J. Voos, G. Riva, C. Zerbini, C. Centeno, and E. Gonzalez, Custom HL7 V3 message provider using web services security features vol. 1, 2010.

[6] HL7, "Implementation FAQ:Encryption and Security," http://wiki.hl7.org/index.php?title=Implementation_FAQ:Encryption_and_Security&oldid=13925 (25th January 2014).

[7] 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.

[8] 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.

[9] C. Pagetti, "A European Health Card Final Report," 2001.

[10] P. Kierkegaard, E-Prescription across Europe vol. 3. Heidelberg, Germany: Springer, 2013.

[11] Diário da República, nº 96, 18 de Maio de 2011 http://dre.pt/pdf1sdip/2011/05/09600/0279202796.pdf (25th January 2014)

[12] F. H. France and P. N. Gaunt, The need for security - a clinical view vol. 35 Suppl, 1994.

[13] F. H. Roger France, "Control and use of health information: a doctor's perspective," International journal of bio-medical computing, vol. 43, pp. 19-25, 1996.

[14] ACSS, "Software para prescrição eletrónica de medicamentos," 2012, http://www.acss.min-saude.pt/Portals/0/Emp_sw_certificado_2012-01-09.pdf (25th January 2014).

[15] R. Ramesh, "NHS patient data to be made available for sale to drug and insurance firms," in The Guardian, ed. Sunday 19 January, 2014, http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy (25th January 2014).

[16] Oracle, "About Java Card Technology," http://www.oracle.com/technetwork/java/javame/javacard/overview/about/index.html (25th January 2014).

