An improvement of NFC-SEC with signed exchanges for an e-prescription-based application

Mohamad Hamze, Fabrice Peyrard, Emmanuel Conchon

An improvement of NFC-SEC with signed exchanges for an e-prescription-based application

Mohamad Hamze[1], Fabrice Peyrard[2], Emmanuel Conchon[3]

[1] University of Burgundy, Le2i
9 avenue Alain Savary, BP 47870, 21078 Dijon France
Mohamad.Hamze@u-bourgogne.fr
[2] University of Toulouse, IRIT/ENSEEIHT
2 rue Charles Camichel, BP 7122, 31071 Toulouse Cedex 7 France
Fabrice.Peyrard@irit.fr
[3] University of Toulouse, IRIT/ISIS
Rue Firmin Oules, 81100 Castres, France
Emmanuel.Conchon@irit.fr

Abstract. In the context of an aging population, drug intake can be a potential source of errors leading to death in some cases. Almost all of these errors are unintentional and come from incorrect prescriptions, unsuitable dosages for the patient or incompatibility with other treatments. To limit these risks which are especially important in the elderly or predependency, we propose a secure system for drug treatment through the NFC (Near Field Communication) contact-less communication technology. The proposed system provides security mechanisms such as integrity, authentication, encryption and non-repudiation. To ensure this security, an extension of the international standard ISO/IED 13157 (NFC-SEC) is proposed to handle electronic signature based on a public key infrastructure.

Key words: NFC, e-prescription, Security, e-signature, ISO/IEC 13157, healthcare application

1 INTRODUCTION

Everyday our health system is improving so that elders can now have a longer life expectancy. Nonetheless, for many of them, seniors require an assistance to improve their quality of life leading to a strong effort in this direction by the research community. In this context, to support the autonomy of elderly people, we choose to focus on the risk of medication errors. More specifically, we choose to highlight three common sources of medication error. First is when the physician is writing his prescription: the patient may inadvertently omit to tell the doctor about another medication he is taking for the treatment of another disease. Second, during the pharmacist dispensation, a prescription may be poorly written so that the pharmacist may misread the prescription leading to the dispensation of the wrong drug or of the wrong dosage for instance. Third, when taking his medication, the patient can make an error with the dosage,

the schedule or even with the drug he takes. The risk associated with each of these three sources is very different from one to another with a probability of occurrence which increases from source 1 to source 3. Indeed, a good physician (doctor) and a good pharmacist should ask the relevant questions to avoid most of these risks. However, the third case depends only of the patient and has therefore a great probability to occur especially in the case of the elderly.

We present in this paper a process of development and use of electronic prescribing (e-prescribing) in an ubiquitous environment to reduce the risk of medication errors. Indeed, potential errors induced by the prescriber or pharmacist can be limited with the use of an electronic prescription (e-Rx) system. The drug intake phase is assisted by an ambient intelligence system in order to reduce the associated risks.

The ubiquitous system is based on electronic prescription and on a NFC (Near Field Communication) contact-less communications technology between patient, prescriber, pharmacist and drug boxes. The originality of our contribution relies on the following points: (1) the use of a single wireless technology NFC throughout the overall process, (2) a natural behavior of the patient through the process by being vigilant at every stage at the acceptability of the system, (3) a secure design ensuring the confidentiality of patients personal data (ethics), the traceability and the non-repudiation of the data exchanges.

In this paper, it has been chosen to highlight the security issues of the NFC technology and to propose a solution that tackles these issues for a healthcare system. A big part to ensure the patient safety is the necessity to track every people, devices and medication involved in the medical treatment. Indeed, misidentified patient or medications can cause serious, or even fatal, errors in medication care [25]. In addition, for a secure system several other requirements have to be filled: confidentiality, integrity, availability and non-repudiation of the exchanged data.

An NFC communication is usually done through an insecure channel which is not satisfactory from a security standpoint as shown as in [18][27]. To tackle this issue, several security standards have been published. For example, the International Standard ISO/IEC 13157 (NFC-SEC) [2][3] published in 2010 enables two NFC devices to establish a secure channel in Peer-to-Peer mode. Nonetheless, they still do not provide a solution for every security requirements. For instance, the NFC-SEC standard does not provide entity authentication. In addition, it cannot ensure non-repudiation because it does not contain any functionalities to sign the exchanged data. To deal with this problem, we propose to extend the NFC-SEC standard with the use of an electronic signature delivered by a Public Key Infrastructure (PKI).

The remaining of this paper is organized as follows: in section 2, the proposed ubiquitous system to improve drug intake based on e-Rx is presented; in section 3, the NFC technology is introduced with a focus on the security issues for healthcare applications; in section 4, the proposed security architecture and the extension of the NFC-SEC standard are presented; finally, a conclusion and some future works are provided.

2 PROPOSED COMMUNICATION PROCESS

2.1 System overview

The proposed system is based on a recommendation made in 2012 by the CLIO (Comité de Liaison Inter-Ordres) Santé, which is the liaison committee of French medical regulatory authorities. In this note, the CLIO has presented a solution for the introduction of e-prescription (e-Rx) in the French e-health organization.

Currently, this system mainly relies on two electronic health records (EHR): The shared personal medical record (DMP) and the pharmaceutical record (DP).

- The DMP is the French shared patient record where the health professionals (medical doctor, surgeon etc.) can exchange medical information about the patient. This EHR stores labs exams, medical background, letters between physicians, medical images but no e-Rx. It has to be noticed that the patient can hide some information in this record and, for instance, only allow the access to a small subset of information for a specific doctor.
- The DP is handled by pharmacists and stores information about every medication that have been delivered to the patient in the last 36 months.

The information is split between the DMP and DP and a e-Rx system should be suitable to establish a link between them to carry the information between doctors and pharmacists. Therefore, the CLIO recommendation is to have a third repository dedicated to e-Rx.

The new CLIO healthcare pathway is presented in Figure 1 from step (1) to step (6). Once the doctor is authenticated on the system, he can access to the DMP of his patient to collect information (step (1)). Both the identity of the patient and of the doctor are ensured with a smart card (see section 2.3). After the medical exam, the doctor can edit a new e-prescription (e-Rx) and sends it to the e-Rx national repository (step (2)). He also gives a paper-based prescription to the patient. With his prescription, the patient goes to the pharmacy of his choice to receive his medication. In the pharmacy, the patient gives his smart card to the pharmacist who can then access to the DP and can receive the e-Rx to deliver (step (3) and (4)). He can substitute some drugs for generic ones. If so, he updates both the DP and the e-Rx registries (step (5) and (6)).

This system seems to be an effective and cost-saving way to reduce several errors (transcription for instance) and to ease the exchange of information between the doctor and the pharmacist. But, this system has no direct impact on the way the patient deals with his own medication.

As depicted on Figure 1, we propose to extend this proposition with a dedicated solution to provide new services to the patient among which is the possibility to make the intake of medicines easier. This solution is not to be opposed to the centralized e-Rx repository but can rather be viewed has a complementary tool to enforce the patient safety and security.

To provide these new functionalities, the patient has to received the e-Rx. To do that, we choose to use a NFC contact-less technology (see section 3.1). Indeed, the NFC technology is of growing interest and is present in most of modern

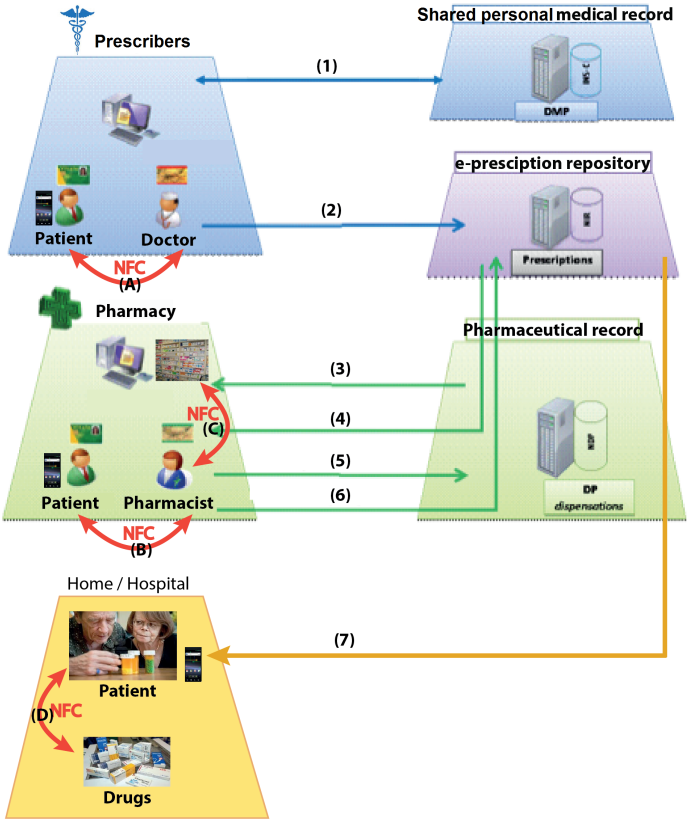

Fig. 1. Global system architecture

phones. This technology is an extension of the RFID technology and provides a peer-to-peer communication mode which can be used for the exchange of e-Rx. Moreover, the range of communication is very short (below 10cm) so that the communication link has to be willingly established keeping the social interactions that currently exist and helping in the memorization of the transmission by the patient.

This e-Rx is then stored on the patient smartphone and can then be used to have reminders of his drug intakes for instance. Nonetheless, this NFC system has to be as secure as the system based on the centralized repository for e-Rx.

2.2 System communication architecture

Three kinds of actors have been defined: the patient, the prescriber (i.e. the health professional which can be a doctor or a nurse for instance) and the pharmacist. In addition to this three actors, the drug box also has a preeminent role as it contains a big part of the information (i.e. the intelligence) of the ambient system. The system is split in three parts where different interactions can occur:

– interactions between the patient and the prescriber (step (A)),
– interactions between the patient, the pharmacist and the drug box (step (B) and (C)),
– interactions between the patient and the drug box (step (D)).

Interactions between the patient and the prescriber After the medical exam, the e-Rx is provided by the prescriber to the patient via NFC (see step (A) on Figure 1). This e-Rx has the same level of security as the paper one and has to be digitally signed by the prescriber to ensure the non-repudiation of the contained data.

Note that the patient can also give the prescriber an access to his previous prescriptions (or a subset) so that the prescriber can have valuable information to write his e-Rx.

Interactions between the patient, the pharmacist and the drug box With his e-Rx on his smartphone, the patient or his helper goes to his usual pharmacy to receive his medication. The pharmacist consults the national e-Rx repository based on the e-Rx id provided via NFC. Note that this proposition enforces the CLIO system in terms of confidentiality. Indeed, the pharmacist has only access to the e-Rx to deliver and not to every e-Rx stored in the repository. If a substitution is made, the e-Rx is updated and then transmitted both to the national repository and to the patient mobile phone with NFC. This e-Rx has information about the current date, the substituted drugs, the drug box that are given to the patient (Unique ID, type etc.) and about the pharmacist identity for traceability purpose.

Moreover, the e-Rx can be used by the pharmacist to store on the drug box memory, information that are usually written on it. Indeed, we propose to add a NFC-tag to the drug box to store information about the patient, the prescriber, the dosage and the date of the prescription as well as the date of the dispensation.

At the end of this step, the patient has an updated e-Rx on his mobile phone and has received several smart drug boxes. All of these elements will allow the proposition of new services for the patient.

Interactions between the patient and the drug box With the e-Rx on his smartphone, the patient will then be allowed to receive scheduled reminders to take his drugs. When an alert is received, the patient has to pass the phone over the drug box (i.e. to tag) to acknowledge the drug intake. The drug box tag is read by the smart-phone to ensure first that the box contains the drug the patient is supposed to take and second that the box belongs to him. Alzheimer patients for instance can forget what their medication box looks like even after years of usage of this same drug. If the patient uses the correct drug box, the time and date are stored in the box tag. If a box is tagged without any reminder issued by the smart-phone, this date is used to compute the time between the last intake and the current one. If this time interval is too short leading to a risk for the patient health, an alert is generated in order to cancel the drug intake.

Every validated drug intake is then logged on the smart-phone to provide a historical overview of the patient behavior. This overview can be used by

the doctor to adjust the medical treatment with more information than with an interview only. For Alzheimer patients, this overview can also be used by helpers to keep a track of the drugs taken. Moreover, a functionality is provided to allow the patient to add specific information during every drug intakes explaining why he did or did not take the prescribed drug (side effects for instance).

Information stored on the drug box can also be used to enforce the overall traceability from the dispensation standpoint (to recover some box within a contaminated lot for instance) and from the drug intake standpoint. Indeed, this information can be used by the patient to start over a new overview even if he looses his smart-phone or his e-Rx. Without an e-Rx, the patient will still be able to know if a drug box belongs to him, if the drug intake is possible at the current time and even find the prescribed dosage on the drug box.

To sum up, two kinds of communication can occur. Peer-to-peer communications between the doctor (e.g the pharmacist) and the patient and communications between the patient and the drug box.

2.3 Security considerations

In the proposed system several security issues can be pointed out. First, as the e-Rx is considered in France as a medical information, it has to be encrypted and transmitted in a secure way to prevent eavesdropping. Similarly, the data stored on the box has to be encrypted. Moreover, every actors of the system has to be identified. For every communication the exchanged data has to be signed in order to ensure the non-repudiation. Furthermore, the use of the digital signature will help to detect potential modification of the information stored in the e-Rx or on the drug box.

In the French health system, health professionals and patients are equipped with a smart card that can be used to ensure the basic operation for our system: the 'CPS Card' and the 'Carte Vitale 2'.

CPS Card *ASIP santé* is a national registration and certification authority that ensures trust in the exchange of health data. It delivers to each health professional a smart card called CPS (Carte des Professionnels de Santé) used as an electronic certificate. A CPS card is a professional electronic identity card. It helps holders to prove their identities and their professional qualifications. It is protected by an individual PIN code. A CPS card is the key for e-health services now and in the future in France. It enables healthcare professionals to: (1) Identify themselves and avoid identity theft; (2) Add electronic signatures to documents; (3) Send electronic treatment forms to the mandatory state health and supplementary insurance organizations; (4) Create, add to and refer to the electronic health records of their patients; (5) telemedicine; (6) Use a secure messaging service for healthcare professionals; (7) Thanks to contact-less technology, it can also be used for other applications such as accessing premises .

Carte Vitale 2 The *Carte Vitale 2* is the health insurance card in France used for the reimbursement of treatment costs by the national social security

agency. With the *Carte Vitale 2*, health professionals can electronically transmit sheets to care health insurance. The *Carte Vitale 2* is supposed to guarantee the identification of the insured person and allows him to sign the electronic care sheet. It must be presented for each visit to the doctor and for every purchase of medication. At the time of writing, the identification is made by the health professional based on the name of the card holder and his photography printed on the card. But, it can be noticed that the card already offer cryptographic functionalities which could be used to ensure security of the exchange and the holder authentication if activated.

So, the CPS card empowered every health professional with digital certificates that can be used for encryption or signature. But, the communication technology has to support also encryption and signature to ensure the overall security of the system.

3 BACKGROUNDS

3.1 Near Field Communication (NFC) Technology

NFC is an extension of RFID based on contactless communication standards. NFC provides short-range communication on a high frequency (13.56 MHz) and is used by devices with low capacity of memory and of computing. It allows data to be exchanged between devices that are within a few centimeters (10 cm) and supports data transfer rates of 106, 216, 424, and 848 Kbit/s. NFC allows the use of small tags that made it possible to be used with small products. Moreover the communication does not require a direct line of sight.

NFC in mobiles can operate in three different modes determined by the application used; it can communicate with another active NFC mobile in Peer-to-Peer mode, or communicate with a passive RFID/NFC tag in reader/writer mode, or communicate with an NFC reader in card emulation mode [30]. Our work in this paper concerns NFC mobiles in Peer-to-Peer communication mode.

Standardization NFC is standardized in ISO/IEC 18092 [6] and ISO/IEC 21481 [7] that define communication interfaces and protocols between two NFC devices. For easier integration, NFC has been derived from the same platform as ISO/IEC 14443 [4][5], or from *proximity cards* that define the communication with contact-less integrated circuits (IC). NDEF (NFC Data Exchange Format) defines the logical formats for data exchanges.

3.2 NFC survey

In healthcare : Alemdar [8] presents in 2010 a state of the art of sensor networks for healthcare where the BAN (Body Area Network), PAN (Personal Area Network), gateway to wide networks, wide networks, and end-user health-care monitoring application are described. This study is a large overview of the different wireless technologies. The presented work on contact-less technology in

particular RFID and NFC, highlights the support for activities of daily living detection , the support of location tracking and the support of medication intake.

On this last point, Ho [19] is one of the first to propose a prototype integrating a sensor network and RFID technology for the in-home medication monitoring. Pang [28] recently proposed iPackage: a pervasive healthcare solution for medication noncompliance problem . This prototype allows to tag individual tablets of a medicine box. The proposed solution is cumbersome and the performances obtained do not fully meet the authors expectations.

Ilie-Zudor [20] published in 2011 a journal article which is also a state of the art of applications with unique identifications. It categorizes fifteen application areas including healthcare. The advantages of RFID-based applications are presented including pharmaceutics where RFID can be used as a substitute of bar-codes or can be used for hospital equipment and personnel tracking, for patient medical history or for implant prosthetic and elderly care. It is stated that RFID technology can reduce human errors in the process.

In their work Jara and al. [22, 21, 23] present architectures for AAL (Ambient Assisted Living) based on IoT (Internet of Things). In [22], Jara and al. present the need for secure communications in a medical environment based on symmetric ciphers and on DESFire tag for specific smartphones applications. In [21], the focus is on IoT with the use of NFC to ensure compatibility between drugs. Finally, in 2011, they published [23] a very interesting journal article where a system for diabetes therapy management has been proposed. This system defines a solution for a secure therapeutic monitoring based on a personal health NFC card of the patient.

Garcia and Bravo [16] proposed in 2011 a solution to assist the intake of medication for elderly people with cognitive disabilities. The objective of the system is to remind, guide and motivate the person to take his medication. NFC technology is used as a carrier to help identify boxes of drug.

In [10, 11] Bravo and al. use NFC technology to assist people with Alzheimer's disease in their daily lives. It is based on tags that are embedded in the environment of the person enabling him to be guided and assisted thanks to a NFC smartphone.

Finally, the work of Lahtela [25] deals with a secure mechanism for the use of medications in a hospital environment. With NFC technology identification, the proposed system can reduce human errors in medication.

The closest work with our solution has been proposed by Vergara and al.[31]. In this work, the authors provide a mobile prescribing solution using a smartphone with interaction between the medical doctor and drug boxes. However, it does not consider the process as a whole (patient, doctor, pharmacist, drug manufacturer). Moreover, the security of exchanged data is not taken into consideration neither is the traceability of exchanged documents with NFC.

It can also be noted that Garcia and Bravo [16] project which supports strategies to improve the treatment compliance of elderly with ambient intelligent systems could be coupled with our own support and control system of e-prescribing and drug intake solution to have a complete system dedicated to the elderly

with cognitive disabilities resulting from Alzheimer or Parkinson disease as well as people with head trauma.

Security issues : Although the NFC communication range is limited to a few centimeters, it is not enough to ensure security. Indeed, three safety axis for NFC are to ensure: (1) Security of mobiles (NFC devices and applications); (2) Safety of the communication channel; (3) System Security (reader and tag).

Mifare Classic cards are one of the most popular solution with more than 200 million copies worldwide. These inexpensive cards implement the symmetric security algorithm Crypto-1 whose vulnerability was demonstrated in 2009 by Garcia [15]. He showed four possible attacks on this kind of card. The most significant result is the attack of the secret key in less than a second. Courtois [12] has also shown how to clone this type of card in 1 second. With such a low time rate, the spoofing of an ID tag can be easily done for instance.

In 2006, Hancke [17] proposed relay attack on an RFID system (tag/reader). In 2010, Francis et al. [13] showed the feasibility of this same relay attack between NFC smartphones. They proposed the use of an information system based on the mobile devices location coupled with a digital signature to counter this attack.

Madlmayr et al. [26] studied the security and the confidentiality of NFC devices. They call for the integration in applications of encryption and authentication mechanisms not only of terminals but also of people. More recently Roland [29] in 2010 proposes in his paper a digital signature records for NDEF NFC layer to ensure messages integrity and authenticity. In other works, Francis et al. [14] offer a Security applications Framework for e-identification, e-payment and e-ticketing with NFC reader/tag mode. This framework offers a CPTI (Communication Protocol Translator Interface) protocol for secure P2P transactions with token between terminal and cards. It is based on an asymmetric encryption mechanism and digital signature.

In addition, commonly known threats to the NFC security [24] are: (1) Eavesdropping, where a third party can receive a signal using an antenna. (2) Unwanted activation, which is somewhat similar to eavesdropping. Third party attacker tries to activate the card without the owner's knowledge; (3) Data Corruption, or modification of transmitted data using an NFC device working with the valid frequency; (4) Data Modification, where the attacker is sending valid, but altered data to the receiving NFC device; (5) Data Insertion, where attacker tries to insert a new message into a NFC communication; (6) Man-in-The-Middle-Attack, where two parties who want to establish communication are tricked into communicating with or via the third party which is therefore enabled to record the entire conversation; (7) Denial of service, where the attacker tries to interfere with the RF field, in order to prevent the transaction. Also, Haselsteiner and BreitfuB [18] show multiple attacks against NFC-based systems that rely on the lack of link level security of the NFC technology.

3.3 NFC Security standard ISO/IEC 13157

NFC (Near Field Communication) data exchanges pose a security problem that the International Standard ISO/IEC 13157 published in June 2010 addresses. It consists of two parts: 'NFC-SEC: NFCIP-1 security services and protocol' [2] and 'NFC-SEC cryptography standard using ECDH and AES' [3]. This NFC-SEC cryptography Standard specifies cryptographic mechanisms based on the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity.

This standard enables the encryption of exchanged data based on a symmetric algorithm where the shared secret is generated from digital certificates of the communicating entities. This process can be split in four steps as depicted as in Figure 2.

- *Step 1:* Key agreement: enables the establishment of the shared secret (z) from the derivation of a part of the private key of the transmitter and derivation a part of the receiver's public key. It begins with the generation of an Elliptic Curve (EC) Key Pair and the validation of the EC public key. Each NFC-SEC entity generates a random nonce (N) which will be used to provide more entropy for the keys derivation. N is then concatenated ($\|$) with the EC public key (Q) and the result is sent to the other entity (Fig. 3). z is then computed by the ECDH derivation Primitive [1] from the user's private key and the public key of the other entity.
  With the properties defined in Table 1, two Key Derivation Functions (KDF) are specified; one for the Shared Secret Service (SSE) and one for the Secure Channel Service (SCH).
  1. SSE establishes a shared secret MK_{SSE} between two NFC-SEC entities. This secret must be cryptographically uncorrelated from any shared secrets established beforehand or afterwards (Fig. 3);

$$MK_{SSE} = KDF_{SSE}(N_S, N_R, z, ID_S, ID_R) \tag{1}$$

  2. SCH provides a secure channel between two NFC-SEC entities with link keys MK_{SCH}, KE_{SCH}, KI_{SCH}, and subsequently protect all communications in both direction across the channel.

$$\{MK_{SCH}, KE_{SCH}, KI_{SSH}\} = KDF_{SCH}(N_S, N_R, z, ID_S, ID_R) \tag{2}$$

- *Step 2:* Key confirmation: Both NFC-SEC entities check that they indeed share the same key. Each entity generates a key confirmation tag (MacTag) based on a Message Authentication Code (MAC) and sends it to the other entity. Both then verify the key confirmation tag upon reception.
- *Step 3:* PDU security: The NFC-SEC entities (Fig. 4) protect data exchange using encryption. This mechanism involves (a) Sequence Integrity, (b) Confidentiality and Origin authentication and (c) Data integrity. **No signature mechanism of packets is supported in the standard**.
  (a) NFC-SEC provides a sequence integrity mechanism in accordance with the

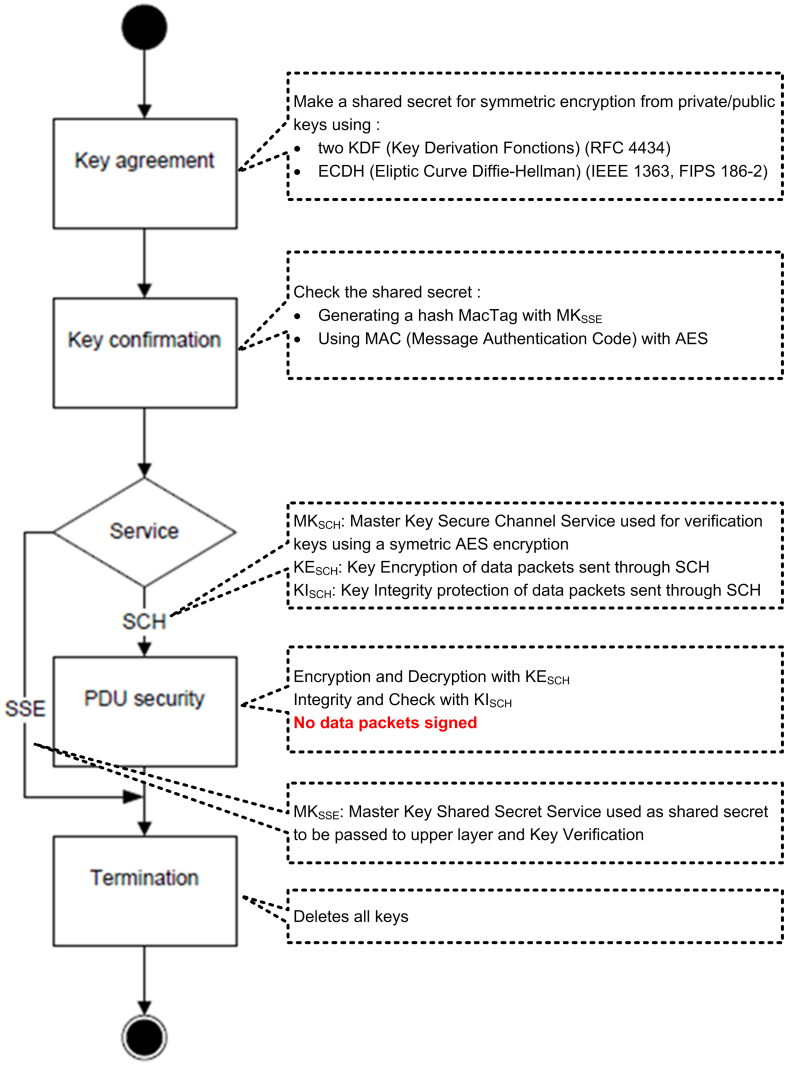

Fig. 2. General flow of the NFC-SEC services

following: each NFC-SEC Entity maintains its SNV (Sequence Number Variable), then upon SCH establishment, the receiving entity initializes its SNV to the same initial value as the Sender's SNV. This SNV is then enclosed in every exchanged data to ensure the sequence integrity.
(b) As previously mentioned, the data encryption algorithm used is AES with counter CTR mode. At first, to avoid the exchange of the initial value (IV) of the CTR counter, the IV must be computed by both entities from the exchanged nonces with equation:

Table 1. Cryptographic properties of standard NFC 13157

Actions	Algorithms
Key agreement	ECDH P-192, IEEE 1363 and FIPS 186-3
Key Derivation Fonction	AES-XCBC-PRF-128, RFC 4434 (IPSEC v2)
Key confirmation	AES-XCBC-MAC-96, RFC 3566 (IPSEC v2)
Encryption	AES-128-CTR, IV init: AES-XCBC-PRF-128
Integrity	AES-XCBC-MAC-96

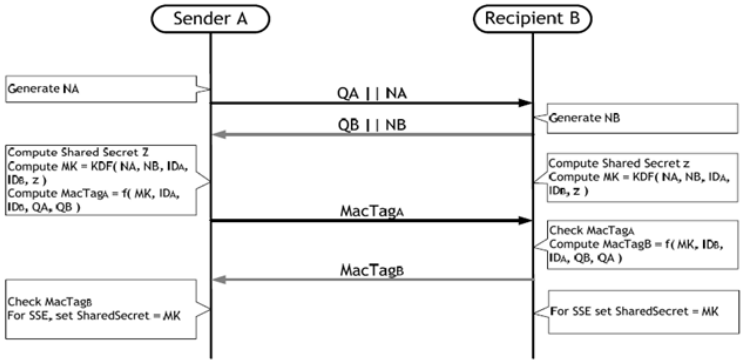

Fig. 3. MSC of establishing of a shared secret MK_{SSE}

$$MAC\text{-}IV(MK_{SCH}, KI_{SCH}, N_S, N_R) \tag{3}$$

The data must be encrypted or decrypted using the symmetric encryption key KE_{SCH} :

$$EncData = ENC_{KE_{SCH}}(Data) \tag{4}$$

$$Data' = DEC_{KE_{SCH}}(EncData) \tag{5}$$

(c) Integrity of all encrypted data transferred on the SCH is preserved through a MAC (Message Authentication Code) (i.e a fingerprint) generated with the symmetric key KI_{SCH} and the AES algorithm.

– *Step 4:* Finally, The NFC-SEC entities terminate SSE and SCH and destroy the associated shared secret and the link keys. Indeed, the MK_{SSE}, MK_{SCH}, KE_{SCH} and KI_{SCH} keys must be different for every NFC-SEC transaction.

More details on the standard can be found in [3].

4 PROPOSED SECURE AND TRUST ARCHITECTURE

4.1 A need for secure communications

According to the architecture presented in Fig. 1, we propose to use NFC technology to transmit e-Rx between doctors (or pharmacists) and patients. However,

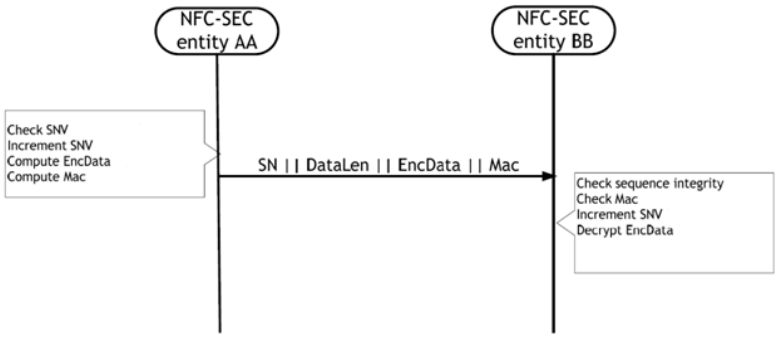

Fig. 4. MSC of data security exchange

NFC communication is done via an insecure channel. NFC tags can be read and legitimate transactions with readers can be heard by a third party attacker. Therefore, we need to protect privacy, personal devices, and exchanged data to prevent eavesdropping and ensure trust between the patient, the doctor and the pharmacist. As a result, establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping and any kind of data modification attack.

We propose the use of NFC-SEC to ensure security communication. The confidentiality and integrity are ensured by the symmetric keys MK_{SCH}, KE_{SCH} and KI_{SCH} that are derived from equation (2) and used in equations (4) and (5) and by the MAC computed from equation (3). This is ensured because if the attacker can find N_A, N_B, ID_A and ID_B, he still can't find the shared secret z. Indeed, the shared secret z is calculated from a user's private key and the public key of the other. Without the private key, the attacker can't reverse the process.

NFC-SEC enables two NFC devices in Peer-to-Peer mode to establish a secure channel but does not provide all requested security features.

Firstly, NFC-SEC standard does not provide authentication [9] mechanisms which is a strong weakness to fight against Man-In-The-Middle attacks as demonstrated by Haselsteiner and al. [18].

Secondly, doctor or pharmacist or patient must not be able to deny that they exchanged information at some point (to respect non-repudiation). In addition, '*e-Rx*' must not be modified by an attacker when exchanged or stored in the patient smartphone (to respect integrity). Thus, when the patient goes to the pharmacy, the pharmacist must ensure that the received '*e-Rx*' is not altered and is delivered by a doctor. Therefore, any data exchanged between users has to be signed.

As previously, stated NFC-SEC does not provide functionality to sign the exchanged nor stored data failing to ensure authentication and non-repudiation.

4.2 Proposed trust architecture

To deal with this problem, we proposed to use a digital signature (e-signature) to sign every exchanged of e-Rx at communication time. This method ensures a trust between the different parts of the communication due to the reliability of the signature checks, authentication and authorization required for both receiver and sender. It insures integrity of data, easily traces transactions between parties, and insures that any actor can not deny that he sends a signed information.

The e-signature relies on the utilization of a public-private key pair with a hash function. First, the sender uses the hash function to calculate a footprint of data to be signed. He uses the private key to encrypt (i.e. sign) this footprint. Then, he sends the message containing the clear data and the signature to the receiver. Upon receiving this message, the receiver decrypts the signed footprint using the public key of the sender. He calculates the footprint of the clear data with the hash function and compares the result with the decrypted footprint. If they are equals then the receiver is sure that the data were not altered (integrity) during the communication and that the sender is who he claims to be (non-repudiation).

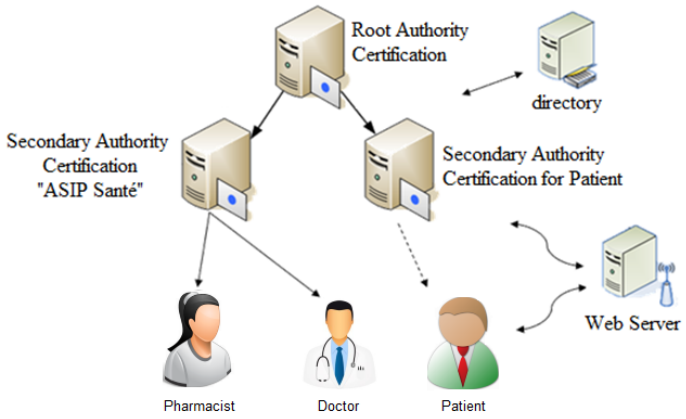

Fig. 5. Architecture of Public Key Infrastructure

Public Key Infrastructure (PKI) We propose a PKI (Fig. 5) to deliver e-signatures. This PKI is composed of the following equipments:

1. A root Certification Authority (AC_root) that self-generates its own certificate (key pair).
2. Two secondary certification authorities (AC_sec) which could be integrated into the social security system:
   – The *ASIP santé* (section 2.3) which delivers certificates for CPS user and which already exists.

   - An authority that distributes electronic certificates to patients.
3. A directory to manage valid and usable public keys and those which are on the CRL (Certificate Revocation List).
4. A Web server is used for:
   a) The reception of a request for a certificate from the user, and its sending to the secondary authority.
   b) Sending a certificate received from the secondary authority to the user with the addition of the public key in the directory.
   c) Receiving information (public key, identifier...) sent by a user to check :
      - If a public key is on the CRL or is under use
      - If it is signed by the secondary authority, and if the authority's public key is signed by the root authority.
   d) Sending a user public key based on the request of another user.
   e) The return of the verification results.

These authorities distribute signing certificates (C_{sig_pat}, C_{sig_doc}, C_{sig_pha}) for (patient, physician, pharmacist) that contains actor key pair ($K_{pub\_sig_{pat}}$ / $K_{pri\_sig_{pat}}$, $K_{pub\_sig_{doc}}$ / $K_{pri\_sig_{doc}}$, $K_{pub\_sig_{pha}}$ / $K_{pri\_sig_{pha}}$).

These certificates are stored as follow: For the doctor and pharmacist, they are stored on the CPS card. While for the patient, they are stored in the smartphone. Note that we could store the patient certificates in '*Carte Vitale 2*' if the cryptography functionalities were activated.

Authentication. At the beginning of a NFC communication, N and Q are exchanged among peers to generate the shared secret z in order to establish the secure channel. Therefore, to avoid the classical threat in unauthenticated key agreement protocols and to insure authentication between different entities before establishing a secure channel, we propose to use e-signatures (Fig. 6). First, each entity generates N then signs the concatenation of N and Q and append the resulting e-signature to the data to transmit. Next, each entity sends the result to the other for verification. Finally, if there were no alteration during the communication (verification of the fingerprint and of the e-signature), they compute the shared secret z and establish a secure and trust channel.

Trust exchange and data storage. Next, the patient is going to exchange and store the signed data such as '*e-Rx*'. Therefore, we propose to sign these data first and then send them in a secured manner with NFC-SEC (Fig. 7). After signing the '*data*', we obtain '*SigData*'. Then, we encrypt '*SigData*' using the NFC-SEC encryption protocol and we obtain '*EncSigData*'. Finally, we apply the MAC on information and send them to the receiver using NFC-SEC. Finally at the reception, by applying the protocol NFC-SEC, we obtain the initial signed data '*SigData*' that can be verified or stored for a later check.

5 CONCLUSION

In this paper, we have presented a new system based on e-Rx to assist people with their daily medication intakes. This system relies on the NFC technology which

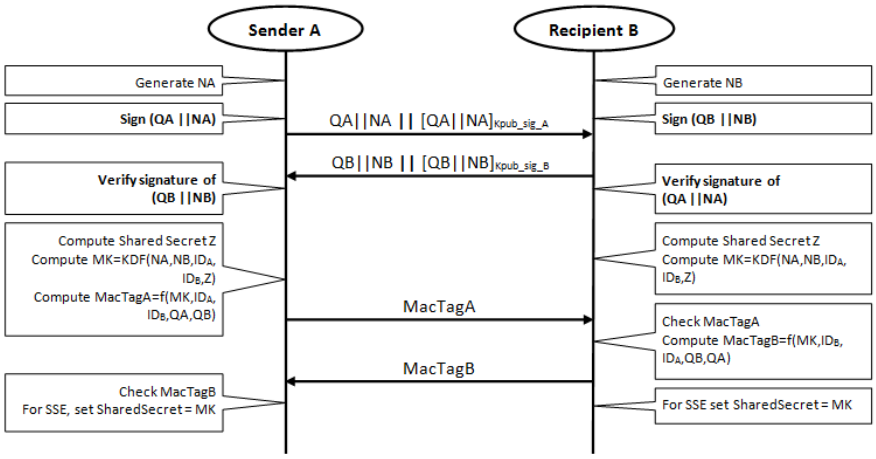

Fig. 6. MSC of authentication entities before communication.

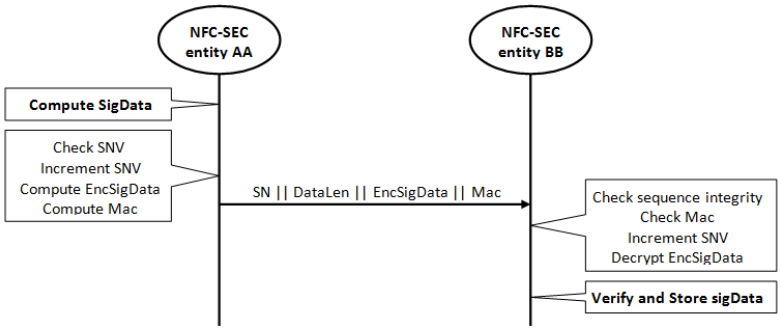

Fig. 7. MSC of trust exchange and data storage.

has been enhanced to provide all requirements for a secure healthcare application (among which is confidentiality, authentication and non-repudiation). We have proposed an extension of the NFC-SEC standard to support electronic signature in order to authenticate and to ensure the non-repudiation every exchanged data. This extension relies on a PKI which can be seamlessly integrated in the existing French e-health system to deliver electronic certificate to every actors.

At the time of writing, an Android prototype has been developed and it is planned in future works to evaluate the impact of the e-signature extension on the communication process in terms of energy consumption, bandwidth and delays and to compare it with the NDEF e-signature mechanism. Finally, we are planning to extend our proposition to enable a e-signature support in reader tag communication in order to strengthen security in the communication between user and drug box.

References

1. IEEE 1363:2000, Standard Specifications for Public-Key Cryptography
2. ISO/IEC 13157-1:2010 Information technology – Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SEC NFCIP-1 security services and protocol
3. ISO/IEC 13157-2:2010 Information technology – Telecommunications and information exchange between systems – NFC Security – Part 2: NFC-SEC cryptography standard using ECDH and AES
4. ISO/IEC 1443-1:2008, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics
5. ISO/IEC 1443-2:2001, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio Frequency power and signal interface
6. ISO/IEC 18092:2004, Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)
7. ISO/IEC 21481:2004, Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-2)
8. Alemdar, H., Ersoy, C.: Wireless sensor networks for healthcare: A survey. Computer Networks 54(15), 2688 – 2710 (2010)
9. Alshehri, A., B.J.S.S.W.S.: Formal security analysis of nfc m-coupon protocols using casper/fdr. In: 5th International Workshop on Near Field Communication, Zurich, Switzerland (2013)
10. Bravo, J., Hervas, R., Fuentes, C., Chavira, G., Nava, S.: Tagging for nursing care. In: Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on. pp. 305 –307 (30 2008-feb 1 2008)
11. Bravo, J., Hervás, R., Gallego, R., Casero, G., Vergara, M., Carmona, T., Fuentes, C., Nava, S.W., Chavira, G., Villarreal, V.: Enabling nfc technology to support activities in an alzheimer's day center. In: Proceedings of the 1st international conference on PErvasive Technologies Related to Assistive Environments. pp. 81:1–81:5. PETRA '08, ACM, New York, NY, USA (2008)
12. Courtois, N.: The dark side of security by obscurity - and cloning mifare classic rail and building passes, anywhere, anytime. In: Fernandez-Medina, E., Malek, M., Hernando, J. (eds.) Proceedings of the International Conference on Security and Cryptography (SECRYPT 2009). pp. 331–338. INSTICC Press, Milan, Italy (July 2009)
13. Francis, L., Hancke, G., Mayes, K., Markantonakis, K.: Practical nfc peer-to-peer relay attack using mobile phones. In: Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues. pp. 35–49. RFIDSec'10, Springer-Verlag, Berlin, Heidelberg (2010)
14. Francis, L., Hancke, G., Mayes, K., Markantonakis, K.: A security framework model with communication protocol translator interface for enhancing nfc transactions. In: Proceedings of the 2010 Sixth Advanced International Conference on Telecommunications. pp. 452–461. AICT '10, IEEE Computer Society, Washington, DC, USA (2010)
15. Garcia, F.D., Rossum, P.v., Verdult, R., Schreur, R.W.: Wirelessly pickpocketing a mifare classic card. In: Proceedings of the 30th IEEE Symposium on Security and Privacy. pp. 3–15. SP '09, IEEE Computer Society, Washington, DC, USA (2009)

16. García-Vázquez, J.P., Rodríguez, M.D., Andrade, A.G., Bravo, J.: Supporting the strategies to improve elders' medication compliance by providing ambient aids. Personal Ubiquitous Computing 15(4), 389–397 (April 2011)
17. Hancke, G.: Practical attacks on proximity identification systems. In: IEEE Symposium on Security and Privacy. pp. 328–333 (may 2006)
18. Haselsteiner, E., B.K.: Security in near eld communication (nfc). In: Workshop on RFID and Lightweight Crypto (RFIDSec06) (2006)
19. Ho, L., Moh, M., Walker, Z., Hamada, T., Su, C.F.: A prototype on rfid and sensor networks for elder healthcare: progress report. In: Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis. pp. 70–75. E-WIND '05, ACM, New York, NY, USA (2005)
20. Ilie-Zudor, E., Kemény, Z., van Blommestein, F., Monostori, L., van der Meulen, A.: A survey of applications and requirements of unique identification systems and rfid techniques. Computers in Industry 62(3), 227 – 252 (2011)
21. Jara, A., Alcolea, A., Zamora, M., Skarmeta, A., Alsaedy, M.: Drugs interaction checker based on iot. In: Internet of Things (IOT 2010). pp. 1 –8 (dec 2010)
22. Jara, A., Zamora, M., Skarmeta, A.: An architecture based on internet of things to support mobility and security in medical environments. In: 7th IEEE Consumer Communications and Networking Conference (CCNC 2010). pp. 1 –5 (jan 2010)
23. Jara, A.J., Zamora, M.A., Skarmeta, A.F.: An internet of things—based personal device for diabetes therapy management in ambient assisted living (aal). Personal Ubiquitous Computing 15(4), 431–440 (Apr 2011)
24. Jovanovic, M., O.M.: Analysis of the latest trends in mobile commerce using the nfc technology. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT) May Edition, 1–12 (2011)
25. Lahtela, A., Hassinen, M., Jylha, V.: Rfid and nfc in healthcare: Safety of hospitals medication care. In: Second International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth 2008). pp. 241 –244 (February 2008)
26. Madlmayr, G., Langer, J., Kantner, C., Scharinger, J.: Nfc devices: Security and privacy. In: Third International Conference on Availability, Reliability and Security (ARES 08). pp. 642 –647 (march 2008)
27. Mulliner, C.: Vulnerability analysis and attacks on nfc-enabled mobile phones. In: 1st International Workshop on Sensor Security. p. 695700 (2009)
28. Pang, Z., Chen, Q., Zheng, L.: A pervasive and preventive healthcare solution for medication noncompliance and daily monitoring. In: 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2009). pp. 1 –6 (nov 2009)
29. Roland, M., Langer, J.: Digital signature records for the nfc data exchange format. In: Second International Workshop on Near Field Communication. pp. 71 –76 (april 2010)
30. Vedat Coskun, Kerem Ok, B.O.: Near Field Communication: from theory to practice. Wiley (2012)
31. Vergara, M., Diaz-Hellin, P., Fontecha, J., Hervas and, R., Sanchez-Barba, C., Fuentes, C., Bravo, J.: Mobile prescription: An nfc-based proposal for aal. In: Near Field Communication (NFC), 2010 Second International Workshop on. pp. 27 –32 (2010)