Prescriptions Management

Pharmacy module

Olga Dzięgielewska
Marcin Klepaczka
Andrzej Rybczak
Jan Szajda

Wrocław, 2014

Contents

Chapter 1

Current Situation

The main element of the currently used system is a paper prescription. There are all the informations, which allow a patient to buy specific medicines, e.g.:

- prescription's creation date,
- patient's personal data:
  - name and surname
  - address
  - PESEL
- number of the prescription, specific for each doctor [1],
- list of medicines with refoundation level,
- signature and stamp of the doctor.

The patient, who was given the prescription by the doctor, goes to the pharmacy to buy the medicines. He gives his prescription to a pharmacist and says which of the medicines from the list he wants to buy. The pharmacist checks if the medicines are

[1] NFZ generates a list of prescription for each doctor. Every prescription has the unique identifier number. During the refoundation process, NFZ checks, if the number on the prescription, the doctor name, signature and stamp are correct. Only if thy are valid, the refoundation is granted.

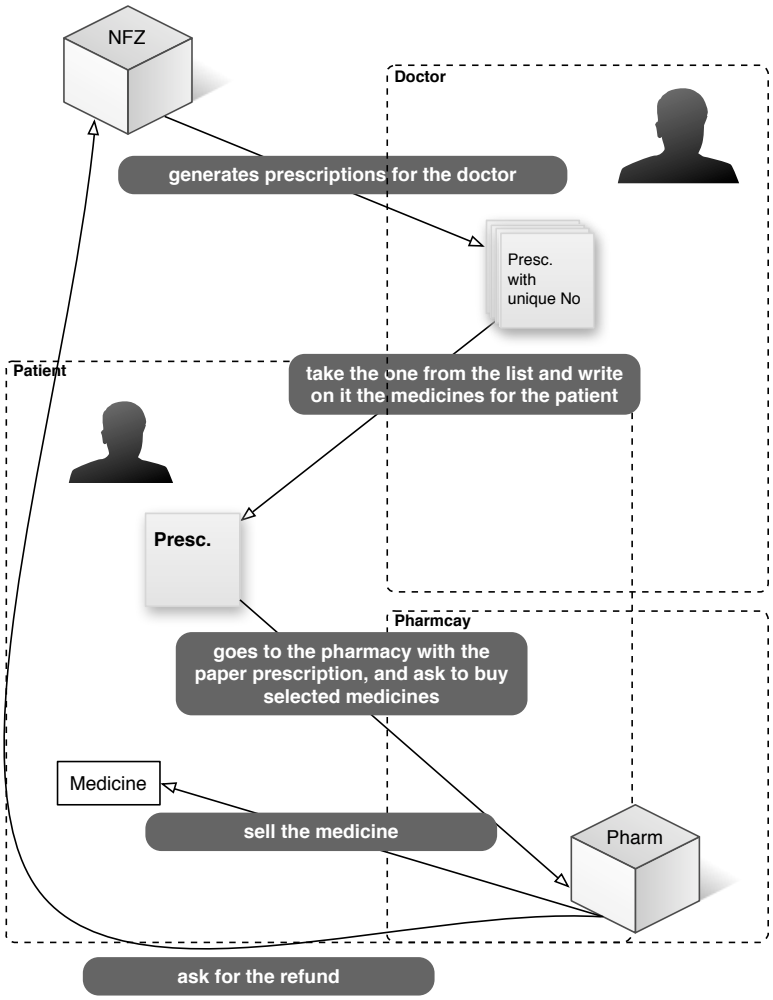

Figure 1.1: The main points of currently used system

available and if yes, he sells them. Next, he takes the prescription and makes a signature next to the each of the medicine he sold. He also inputs to the software installed on computers in the pharmacy, which of the medicine was sold, for who, who gave the prescription and what are the refoundation costs.

Each month in every pharmacy a report, consisting of the set of the information about each prescription sold in the pharmacy is generated. This report is sent to the NFZ central database. Based on this, the NFZ refunds costs of the medicines. Each prescription has to be kept for at least five years in the pharmacy, and be ready for checking during controls made by NFZ representatives.

Chapter 2

Threats and Inconveniences

The way prescriptions are currently processed is vulnerable to many threats, and brings many inconveniences. The most important ones are listed below.

Party	Threats and Inconveniences
patient	• the patient can lose the prescription and he cannot buy the medicines, even if they are life-saving, he has to go to the doctor again and ask for the new prescription • the patient can lose his prescription, then, the person who found this prescription can buy this medicines; what is more, this person can get to know, who takes which medicines and in this way, he can get to know, what is wrong with the person described on the prescription

pharmacy	• the pharmacy has to wait long time to refund costs for the medicines from NFZ on • the prescription are often mistakes, which make the prescription useless. In this situation, the patient has to go to the doctor again and ask him to fix the mistakes
NFZ	• significant amount of money is being defrauded from NZF, because the current system does not verify if the patient himself has bought the medicine or the pharmacists has made a false call for the medicine having some patient's prescription, prepared by the doctor (who is also a part of the defraudation scheme)
system	• the patient can try to copy the prescription and try to buy the medicines few times in different pharmacies • the patient can claim that he has lost his prescription and ask the doctor to give him another one, then, he can buy the medicines twice instead of once

Chapter 3

Project

3.1 The Main Objectives

The main objectives of our new design of the pharmacy module is to limit the impact of the threats listed above and improve the usability of the current system.
The patient has to be sure that his sensitive data is stored in a secure way, and unauthorized person cannot get to know anything about his medicines and illnesses.
The pharmacist has to be sure that he sells the right medicines only for the right patient.
The refund process should be quicker and easier.
The possibility of making **mistakes** on the prescription should be eliminated.
The number of **defraudations** should be significantly limited.

3.2 Environment Requirements

3.2.1 Smart Cards

The main reason we decided to use smart cards is that smart card solutions, which employs two factor authentication, i.e. "something you have and something you know", provide a high security level which is crucial for the health's systems sensitive data.

All the system's users will be given personalized smart cards which will store their identification data: names, surnames, PESEL and digital certificates. Each card will be assigned PIN and PUK numbers. The first one will be used to initialize authentication process, the second one will be used for unblocking a card[1].

To improve the security level of the system, the data stored on smart cards should be enciphered. Users' private keys need to be stored in a secure memory which cannot be directly read out.

In case of loosing a smart card, a user should perform a standardized revocation procedure. First, he should block a card in the assigned institution and while doing this he should be able to select whether he want to block the card temporarily or permanently. In the first case, after finding the card it is possible to unblock it with card's PUK number. In the second case it is necessary to generate new user's card and even after finding the card it will not be possible to unblock it.

3.2.2 Certificates

Each user has his digital certificate on his smart card. All the user's certificates must be given by a defined certification authority and regularly[2] updated.

In case of selecting permanent blocking option during the revocation procedure, a new certificate is generated for such user.

The certificate's validity should be checked at each use of the user's smartcard. The validity check is performed in the database module.

3.2.3 Pharmacy

All the pharmacies which will be using the system must have broadband internet access, two smart card readers and two terminals: one for a pharmacist and one for a customer.

[1] Unblocking procedure can be performed in the two following situation: when a user inputs wrong PIN number three times in a row or when he blocks his card after loosing it.

[2] The CA should define a standard validity period for the patient's, pharmacist's and doctor's certificates.

The terminals apart from displaying the data need to handle all the confirmation actions on both sides.

3.3 Architecture

The pharmacy module architecture consists of the following elements:

1. **smart cards** with personal certificate, used for the authentication and signing, and an application which allows to read certain data from the card;
2. **pharmacist's PC** with a pharmacy module application which provides all of the functionalities which satisfy all the operation performed in a pharmacy; provides two user-friendly interfaces: one for a patient and one for a pharmacist; is connected with patient's and pharmacist's terminals and the central database; is able to execute SIGMA protocol, handle secure keys storage and establish SSL connection;
3. **central DB** is a central element of the whole system; stores the data and handles all the necessary database I/O functions.

Chapter 4

Data Flows

4.1 Use Cases

The way prescriptions are currently processed is vulnerable to many threats, and brings many inconveniences. The most important ones are listed below.

1. **System:**
    - **pharmacist's verification** - system is ableto check that pharmacist has permissions to sell the drugs;
    - **buyer's verification** - system is able to check that the buye's card is valid and entered PIN number was correct;
    - **prescriptions update** - system can change the state of prescriptions(to either 'bought' or 'invalid') or attach additional info to them, like the fact that drug's substitute was sold instead of prescribed one;
2. **Pharmacist:**
    - **reading available prescriptions** - a pharmacist is able to seebuyer's prescriptions
    - **modifying the prescriptions** - a pharmacist is able to update the prescriptions (changing their state/attaching info that substitute was sold instead)

- **signing the prescriptions** - a pharmacist is able to sign prescription to confirm that he's the one who sold them

3. **Customer:**

- **reading available prescriptions** - a customer is able to see/select prescriptions that haven't yet been bought
- **confirming pharmacist's changes** - a customer is obliged to confirm possible changes made to the prescriptions by the pharmacist
- **signing the prescriptions** - a customer is able to sign prescription to confirm that he got the certain medicines

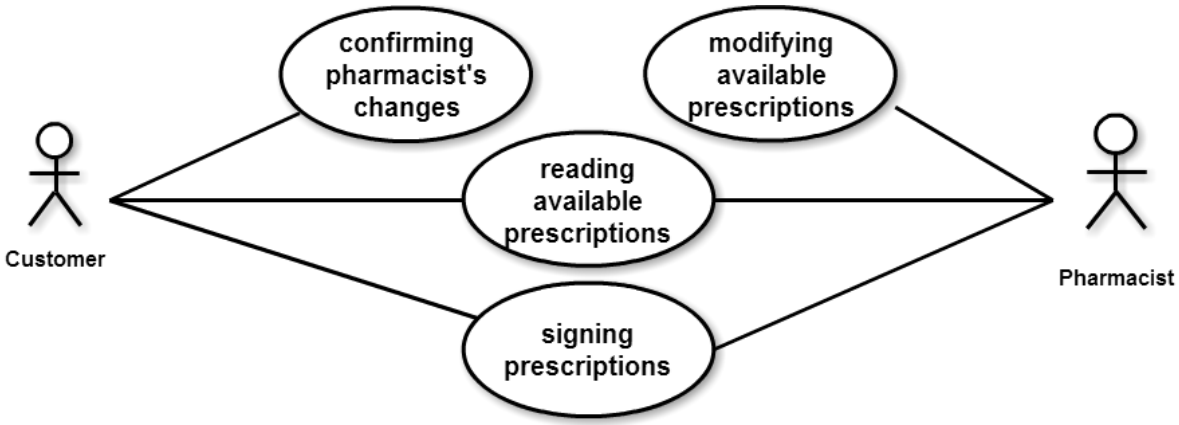

Figure 4.1: Patient's and pharmacist's use cases

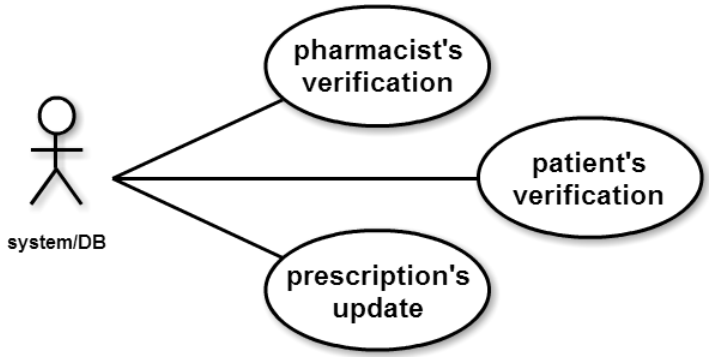

Figure 4.2: System's use cases

4.2 Scenario

1. Customer inserts his card into the reader and enters PIN number.
   (a) System checks whether PIN is correct (if it is not, an appropriate message is displayed and the process cannot be continued).
2. Terminal displays list of active prescriptions to both buyer and pharmacist.
3. Buyer selects prescriptions to buy.
4. Pharmacist inserts his card into his reader and authenticates himself to the system (assuming that the card is not already inserted).
   (a) If authentication is not possible (eg. card of the pharmacist is invalid), an appropriate error message appears on the screen and the process can't be continued.
5. The pharmacist marks prescriptions selected by the customers as 'to be bought'.
6. System checks whether prescriptions have already been bought.
7. System verifies validity of prescriptions (expiration date, credentials of the doctor etc.)
   (a) If some prescriptions are invalid, an appropriate message appears on the screen and system marks the prescriptions as 'invalid'.
8. If the drug from the prescription is not available (or the buyer does not want it for some reason), pharmacist can instead sell a substitute. For that, he is able to write information about selling a substitute to the system.
9. Buyer confirms the prescriptions to be bought (including possible substitute replacements).
10. Pharmacist gives the drugs to the buyer, confirms the selling and the system marks the prescriptions as 'bought'.
11. Buyer takes the drugs and removes his card from the reader.

If the customer's or pharmacist's card is removed from the reader before the step 10, the process is aborted and the initial state of the prescriptions is not changed.

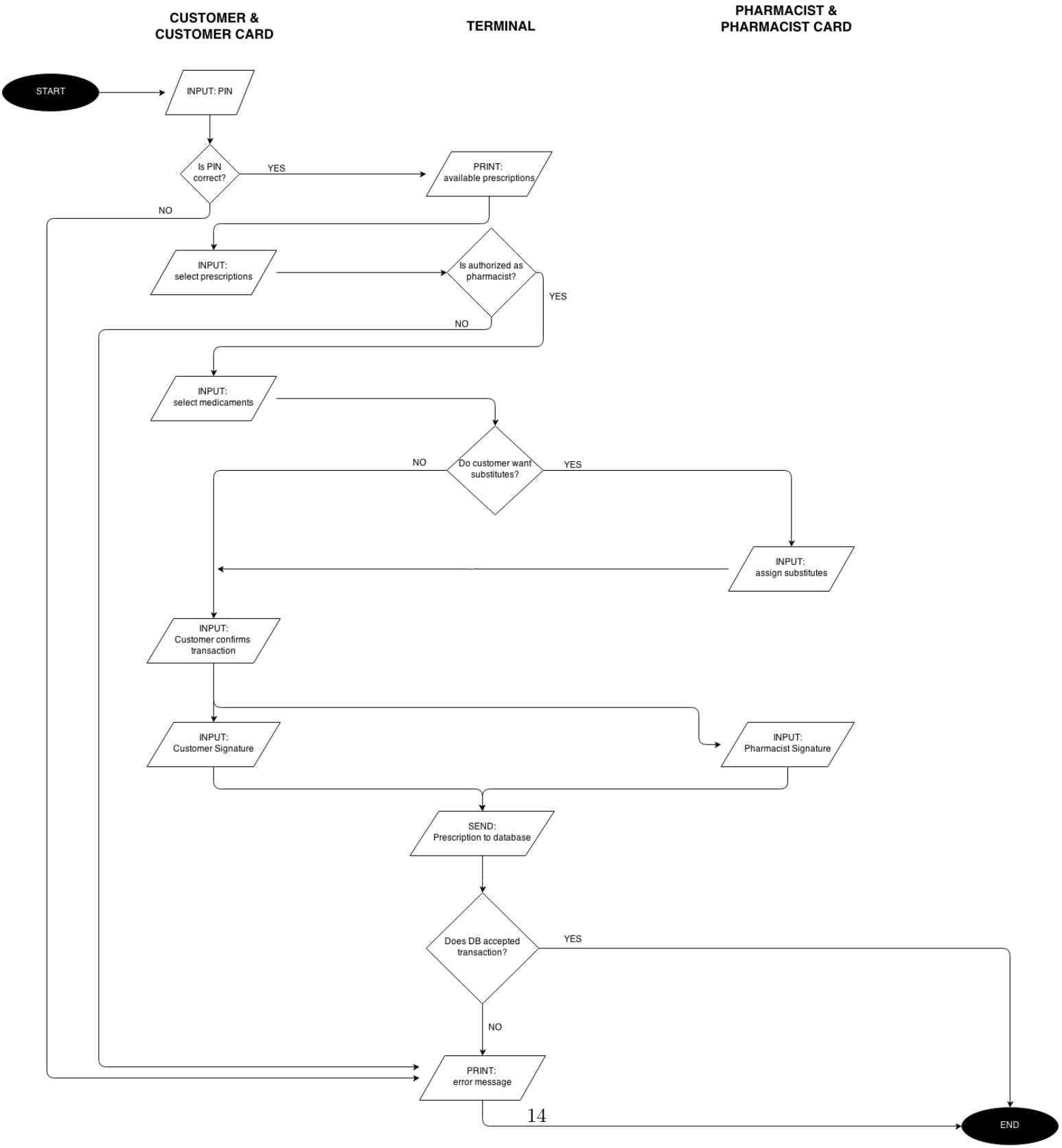

Figure 4.3: Flow chart

Chapter 5

Protection and Security

This chapter describes entities used in the system, how we choose to protect them and why.

5.1 Protection methods

5.1.1 Card

Entity	Description
Patient's card	Patient's card stores private key along with the certificate. Elements of the certificate are as follows (*text in parentheses describes what is used*): • **Serial Number**: Used to uniquely identify the certificate. • **Subject**: The person, or entity identified (*personal data of the patient*). • **Signature Algorithm**: The algorithm used to create the signature (*RSA*). • **Signature**: The actual signature to verify that it came from the issuer. • **Issuer**: The entity that verified the information and issued the certificate (*CA for the patient*). • **Valid-From**: The date the certificate is first valid from. • **Valid-To**: The expiration date. • **Public Key**: The public key. • **Thumbprint Algorithm**: The algorithm used to hash the public key certificate (*SHA256*). • **Thumbprint (also known as fingerprint)**: The hash itself, used as an abbreviated form of the public key certificate.
Pharmacist's card	Pharmacist's card stores the same information as patient's card, with exception to several certificate fields being different: • **Subject:** *Personal data + entity (pharmacy)* • **Issuer:** *CA for the pharmacies*

Card's data access	Card is read only is the sense that patients/pharmacists are not able to modify the data that is stored on it. They do, however (after successful authentication), have access to certificate stored on the card as well as the function to sign arbitrary input data with its private key.
PIN	The certificate access/signing input data can be performed after inputting a PIN. The user is given 4-digit PIN number and the verification system will allow three attempts of typing the correct number before the card is blocked.

5.1.2 Authentication

Entity	**Description**
Patient	Two factor authentication is used: • Something you have - smart card (containing user's certificate) • Something you know - PIN number used to access the certificate on the card
Pharmacist	Two factor authentication is used: • Something you have - smart card (containing pharmacist's certificate) • Something you know - PIN number used to access the certificate on the card

5.1.3 Connection

We assume that if the connection was lost, the whole authentication process needs to be repeated.

Connection	Description
card – PC	After successful authentication we establish a session key and the communication is encrypted with it (for that AKE protocol „SIGMA" is utilized).
application – DB	Two-way SSL connection is used.

5.2 Justification

5.2.1 PIN protection

The PIN number is used to authenticate the card holder. In case the card was lost and found by someone else, he won't be able to use the card without knowing the PIN. We propose 4-digit PIN number with three subsequent incorrect attempts before the card is blocked as it's already used e.g. in ATM cards and proven to work there.

5.2.2 SIGMA protocol

This AKE protocol (we choose to use SIGMA, but that is by no means the ultimate choice. It's been chosen due to convenience of having the implementation already in place. If one wishes, it can be replaced by other AKE protocol, e.g. NAXOS) will be used to secure the communication channels between parties existing in the pharmacy, i.e. cards and application. AKE protocols provide not only secure communication but also authentication mechanism, preventing not only eavesdropping or man-in-the-middle attacks but also party substitution.

5.2.3 Secure key disposal

All short term keys, i.e. ephemeral keys used using AKE protocol or session keys which are the result of the protocol are erased from memory immediately after they are no longer needed.

5.2.4 Secure communication with the database

The communication channel between database and pharmacy is secured with an SSL connection. We assume the SSL provides all the necessary mechanisms to protect the channel from attacks. To strengthen the security of the channel all the requests from any valid party must contain the signature (RSA signature) over the nonce provided by database system. This solution ensure that no unauthorized party is able to get access to database.

5.2.5 Protection against defraudation

Each transaction has to be signed by all the participating parties. In this setting it is impossible for the doctor/pharmacist to fake the medicaments sale and deceive NFZ into giving them money for refunding the nonexistent costs, as signature of the patient is also required.

Chapter 6

Sequence Diagram

In his chapter we present sequence diagram of the actions performed in the range of Pharmacy Module. Each step is described in details. Not all the actions are obligatory, i.e. some procedures can be performed or omitted depending on the required security level and a budget.

6.1 Communication initialization

The first step is communication initialization. Actions performed in this step by the system elements are presented in the figure 6.1

At the beginning, a patient puts his personal card to a terminal and he enters his PIN as usual, e.g. in the ATM. If the PIN is correct, the user can see appropriate message on the terminal screen. Also a pharmacist have to use his card and enters his PIN in the second terminal. Then, the system is ready to work.

PINs are preventing from unauthorized usage of cards, e.g. when a card was stolen or lost.

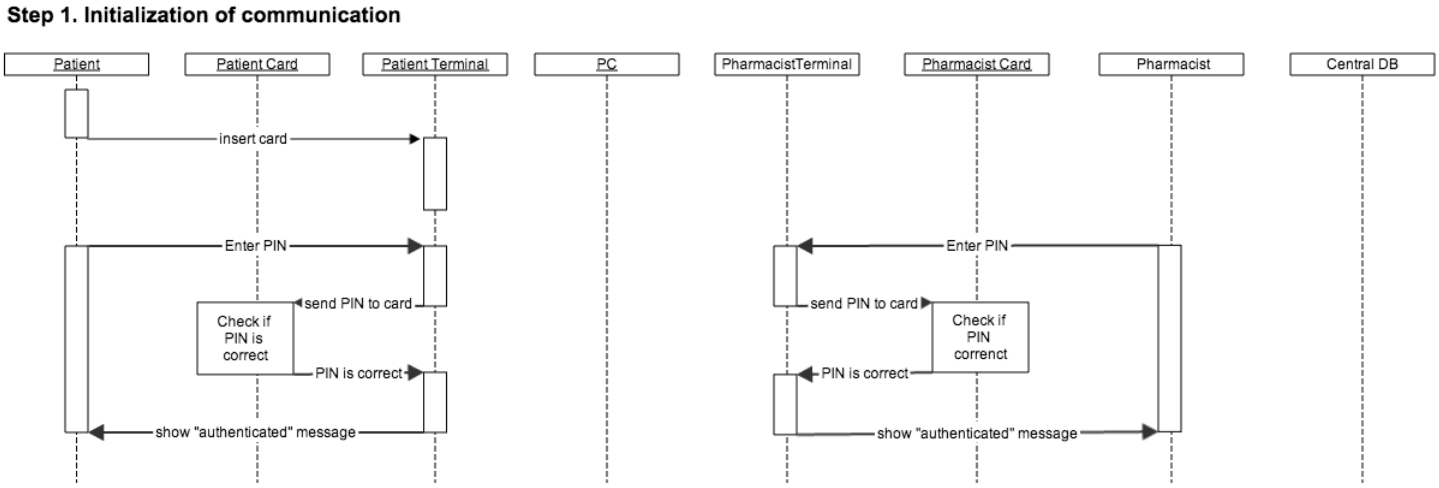

Figure 6.1: Sequence diagram - step 1

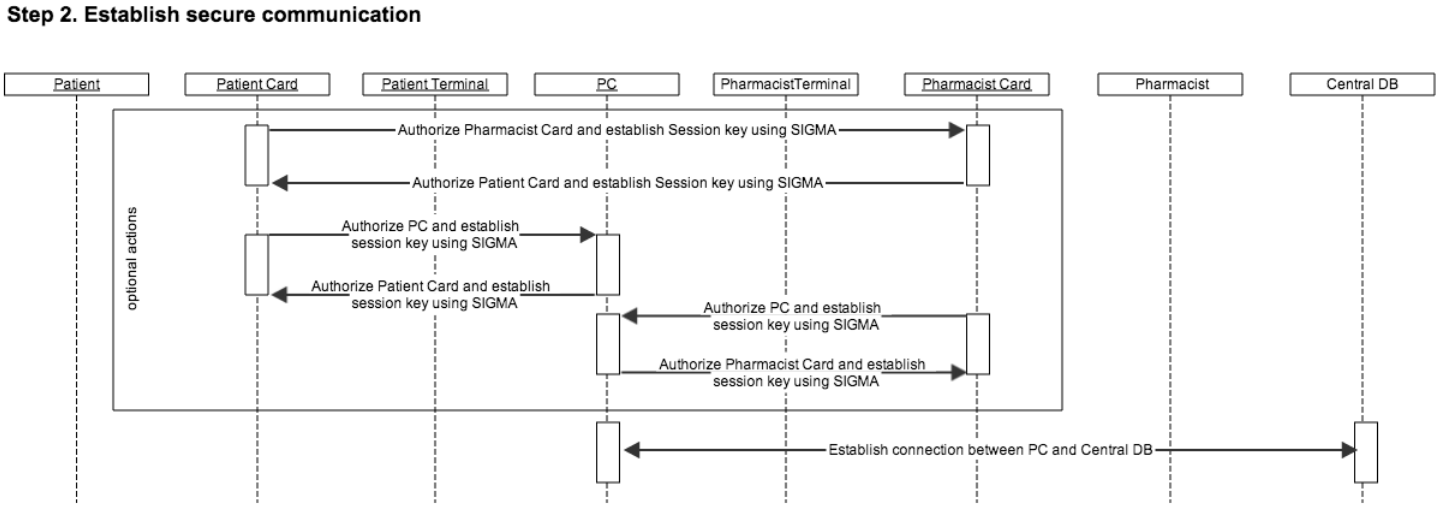

Figure 6.2: Sequence diagram - step 2

6.2 Establish a secure communication

The second step, presented on the figure 6.2, contains actions related with establishing secure communication between the system parties. Part of the actions marked there, are optional and are not required for the system to work properly. Establishing a secure communication between the cards allows the participant to be sure, that the patient's and pharmacist's cards are not forged and they are authenticated to each other. Similarly, suing the SIGMA protocol between a card (patient's or pharmacist's) and the application installed on the PC, allows to authorize the application by the card and the card by the application. These two sub-steps can be implemented, if a very-high level of the security is required.

The communication between the application on the PC and the Central Database is performed in the way described in the Central Database Module Documentation.

6.3 Select prescription to buy

The figure 6.3 presents a point in the protocol, in which user's prescriptions are downloaded from the Central Database and are shown on the screen. After that the patient selects one or more of them to realize them. User's identification data are stored on his card. They are used to authenticate the patient and to download appropriate prescriptions.

6.4 Realize prescription

The last step is presented on the figure 6.4. This scheme is repeated for the each prescription. At the beginning, the system shows available substitutions for the medicine. Then, the pharmacist can select original medicine or one of the substitutions and the patient can confirm this choose.

Then, the application ask the patient and pharmacist cards to sign selected data. After it receives a response, it sends this signed data to the Central Database. The data

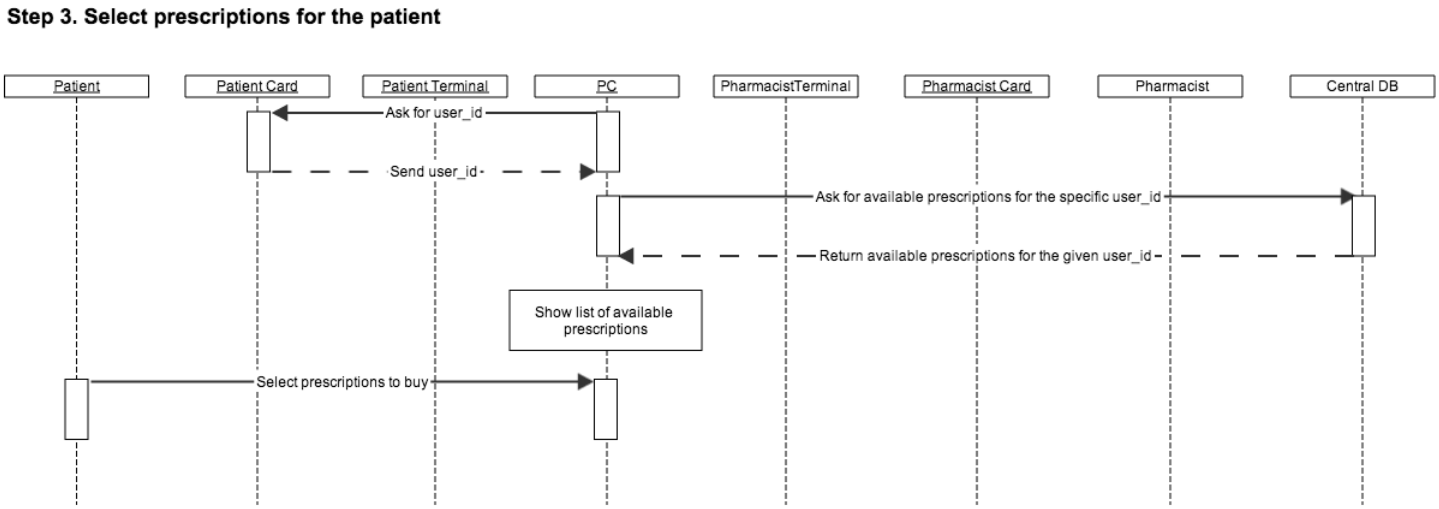

Figure 6.3: Sequence diagram - step 3

are saved there. Because of that, it is impossible to simulate buying process, without patient's personal card. The prescription's data have to be signed by the patient to be inserted into a database as a bought prescription. Without a valid insert, the refund will not be granted.

6.5 End of the protocol

At the end of the protocol, the communications channels are closed and all ephemeral keys are destroyed.

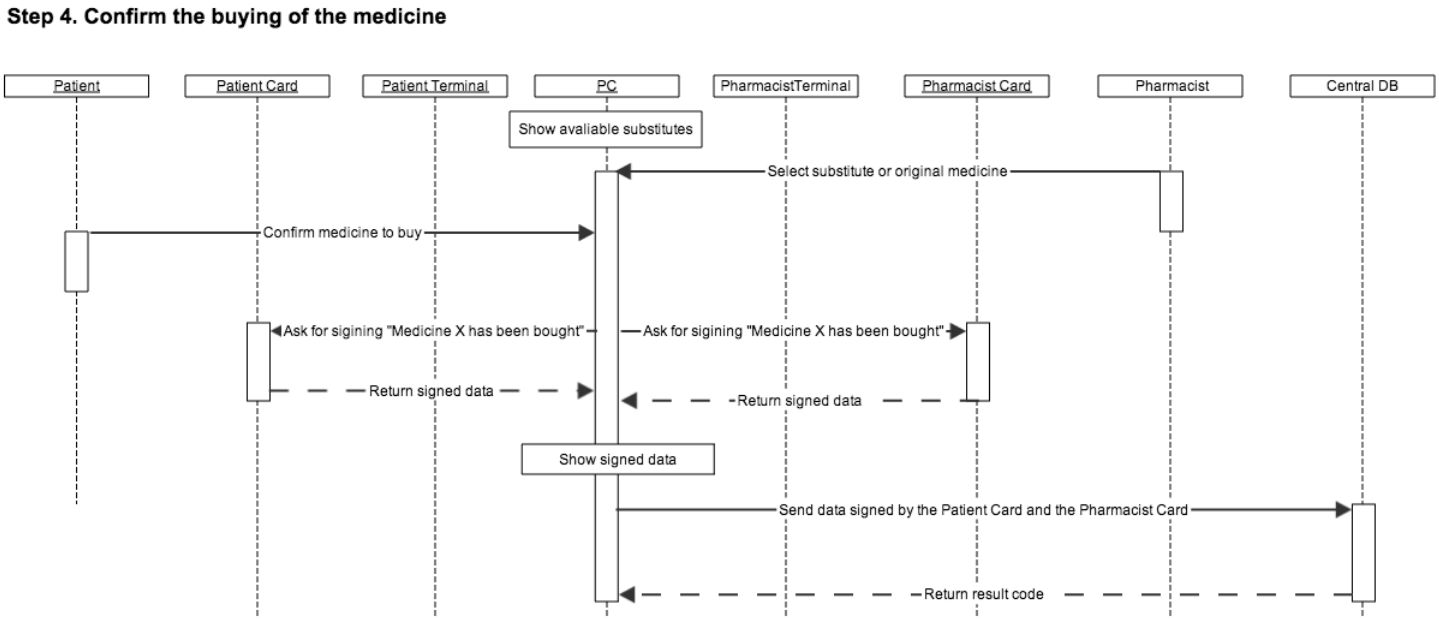

Figure 6.4: Sequence diagram - step 4