Prescriptions Management

Wrocław, 2014

Authors

Database Group

Michał Kaczmarek

Paweł Kędzia

Jakub Płaskonka

Mateusz Płatek

Patient Group

Zbginiew Dobosiewicz

Maciej Niemczyk

Paweł Nużka

Bartłomiej Paciorek

Bartosz Piwowarski

Doctor Group

Krystian Krakowiak

Piotr Lipiak

Pharmacy Group

Olga Dzięgielewska

Marcin Klepaczka

Andrzej Rybczak

Jan Szajda

Supervisor

Ph.D. Łukasz Krzywiecki

Contents

Part I

Introduction

Chapter 1

Current Situation

Current system strongly depends on paper prescriptions. Each prescriptions carries a lot of data, which some can be treated as private data of patients:

- 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.

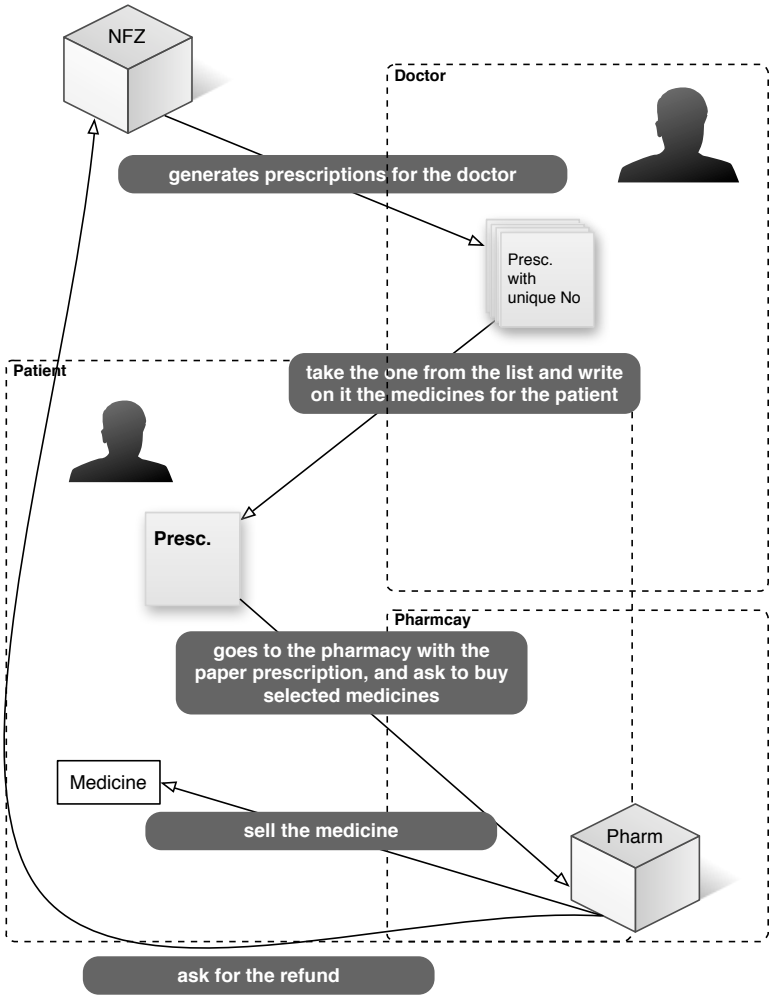


Figure 1.1: The main points of currently used system

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.

2.1 NFZ

2.1.1 Defraudation

Significant amount of money is being defrauded from NFZ 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).

2.2 Patient

2.2.1 Losing a prescription

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.

If someone finds lost prescription, he 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.

2.3 Pharmacy

2.3.1 Refundation delay

The pharmacy has to wait long time to refund costs for the medicines from NFZ.

2.3.2 Prescriptions with mistakes

Prescription tend to contain mistakes which makes it useless. In this situation the patient has to go to the doctor again so it's fixed.

2.4 System

2.4.1 Prescription forgery

Patient can try to copy the prescription and try to buy the medicines few times in different pharmacies.

2.4.2 Pretending that prescription was lost

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.

Chapter 3

System Goals

The system has to eliminate each of the flaws described in previous chapter. It will meet each of following requirements:

1. Prescriptions will be digitalized.
2. Prescriptions will be hard to forge.
3. Doctors won't be able to create prescriptions without knowledge of patient.
4. Prescriptions will be realized only by users with right credentials.
5. Patients and doctors will be able to browse history of prescriptions.
6. System will be secured with most up-to-date measures.
7. System will provide anonymous big data statistics.

3.1 Central Server Objectives

The central server will be the core component of the whole digital prescriptions system. Key features of central server are:

- Holding data of patients, doctors and pharmacists
- Allowing doctors to create prescriptions
- Allowing doctors and patients to review history of created prescriptions
- Allowing patients to transfer the ownership of prescription in secure, controlable manner
- Allowing pharmacists to review prescriptions yet to be realized
- Allowing prescription realization only if patient will be present at this event
- Validating the signatures of each party
- Providing annonymous statistics

3.2 Pharmacy Module Objectives

The main objectives of our new design of the pharmacy module is to limit the impact of the threats listed in Chapter 2 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.

Part II

Project

Chapter 4

Project

4.1 Environment Requirements

4.1.1 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.

Keys used for connecting and authorising should have sufficient length to provide security. If the RSA key is used it should have length of at least 2048 bits.

[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.

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.

4.1.2 Two-Way SSL

Two-Way SSL provides the same functionalities as SSL, with the addition of authentication and non-repudiation of the client authentication, using digital signatures. When mutual authentication is used the server would request the client to provide a certificate in addition to the server certificate issued to the client. The main advantages of client-certificate authentication are:

1. The private information (the private key) is never sent to the server. The client doesn't let its secret out at all during the authentication.
2. A server that doesn't know a user with that certificate can still authenticate that user, provided it trusts the CA (Certificate Authority) that issued the certificate (and that the certificate is valid). This is very similar to the way passports are used: you may have never met a person showing you a passport, but because you trust the issuing authority, you're able to link the identity to the person.

4.1.3 Certificates

In Two-Way SSL both parties (client and server) need the 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. The CA also generates a keypair for the database server.

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

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

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

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

4.2 Architecture

4.2.1 Central Server Architecture

Central server will be constructed of several components. In order to provide all necessary data and functionalities to the users this is system will be a cooperation of system's logic, specific APIs and database. In the project the following components were chosen:

1. **server layer** - Apache HTTP Server ("Apache") version 2.4.9
2. **database layer** - PostgreSQL version 9.3

4.2.2 The Pharmacy Module

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.

4.3 Protection and Security

Below we describe entities used in the system, how we choose to protect them and why.

4.3.1 Protection methods

4.3.1.1 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.

4.3.1.2 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 of the pharmacist and pharmacy*
- **Issuer:** *CA for the pharmacies*

4.3.1.3 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.

4.3.1.4 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.

4.3.1.5 Patient authentication

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

4.3.1.6 Pharmacist authentication

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

4.3.1.7 Connection between card and application

After successful authentication we establish a session key and the communication is encrypted with it. For that AKE protocol „SIGMA" is utilized. (Note that encryption is optional if we assume that no eavesdropping can take place or the data exchanged isn't considered confidential).

4.3.1.8 Connection between application and central database

Two-way SSL connection is used along with additional nonce-based authentication.

4.3.2 Justification

4.3.2.1 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.

4.3.2.2 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.

4.3.2.3 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.

4.3.2.4 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.

4.3.2.5 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. Additionally a token that has to be signed changes with each transaction, so protection from repetition attacks is also gained.

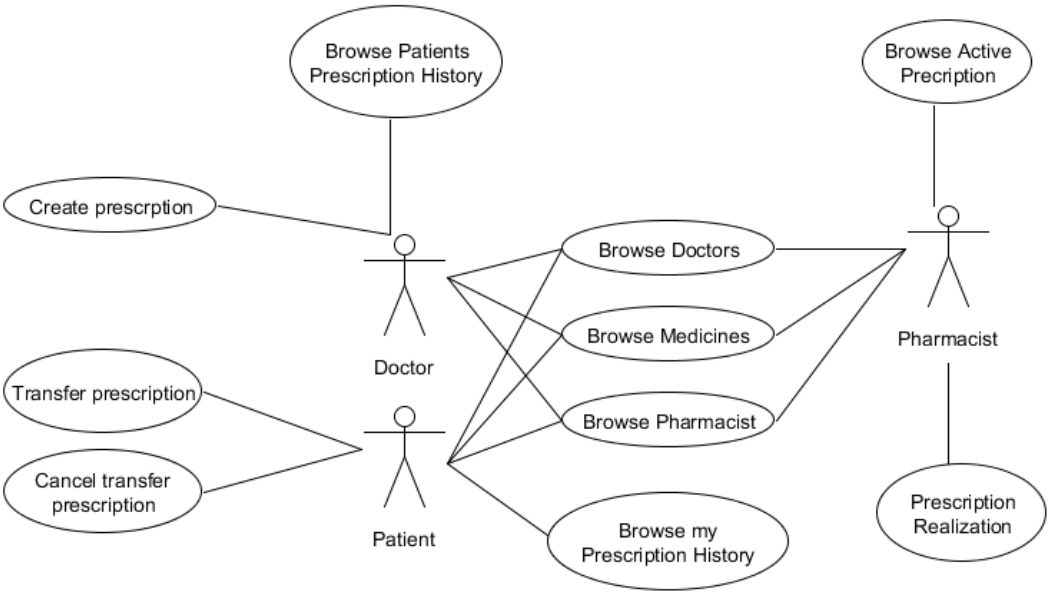
Part III

Database

Chapter 5

Use cases

We define two groups of actors - clients like patients, doctors and pharmacists which benefit from the system on daily basis and third parties - administrators, analytic tools and goverment authorities which cope with the system on special ocassions.



Every use case requires the users to establish secure channel of communication with central server and have to be logged in which will be described more thorougly in section 6.1.

5.1 Shared use cases

Three use cases are applicable for patient, pharmacist and doctors and they consider browsing informations which can be publicly accessible, that is:

- Browse Doctors
- Browse Medicines
- Browse Pharmacists

Rest of use cases which are applicable to only one actor is described in their respective subsections.

Actors: Patient, Doctor, Pharmacist	Title: Browse Doctors
Goal:	Allows to find doctor with specific name, address or license number.
Scenario:	User enters any or all of name, address and license number of searched doctor.
Result:	List of doctors corresponding to the query.
Database method:	browse_doctors

Actors: Patient, Doctor, Pharmacist	Title: Browse Pharmacies
Goal:	Allows to find pharmacist and pharmacy with specific name, address or license number.
Scenario:	User enters any or all of name, address, license number of searched pharmacist or pharmacy name.
Result:	List of pharmacists corresponding to the query.
Database method:	browse_pharmacies

Actors: Patient, Doctor, Pharmacist	Title: Browse Medicines
Goal:	Allows to find medicine with specific name or type.
Scenario:	User enters name or/and type of medicine he is searching.
Result:	List of medicines corresponding to the query.
Database method:	browse_medicines

5.2 Patient

Actors: Patient	Title: Transfer prescription
Goal:	Allows to transfer a prescription to another patient and give him credentials to realize this prescription. Patient who transferred the prescription losses his right to realize it by himself. If he wants the prescription back he has to cancel the transfer (next use case).
Scenario:	Patient enters his id, id of new owner, the prescription id he wants to transfer and his signature.
Result:	OK response from database and iId of new owner of prescription.
Database method:	transfer_prescription

Actors: Patient	Title: Cancel Transfer Prescription
Goal:	Allows to revert transfering of prescription to another patient.
Scenario:	Patient enters his id, prescription id he wants transfers to revert and his signature.
Result:	OK response from database.
Database method:	cancel_prescription_transfer

Actors: Patient	Title: Browse My Prescriptions History
Goal:	Patient can see his history of realized and created prescriptions.
Scenario:	Patient sends his id which is signed by his key from smartcard. Patient can define the time span of returned prescriptions as also a filter to only return prescriptions which aren't realized yet.
Result:	List of prescriptions for the patient.
Database method:	browse_prescription_history

5.3 Doctor

Actors: Doctor	Title: Create prescription
Goal:	Allows to create a new prescription in database for selected patient..
Scenario:	Doctor enters his and patients ids, as well as the data specific to the medicine - id, dosage, unit and quanitity. Everything is signed by his key.
Result:	OK response from database.
Database method:	create_prescription

Actors: Doctor	Title: Browse Patients Prescriptions History
Goal:	Doctor can see patient history of realized and created prescriptions..
Scenario:	Doctor sends his id - he will see all prescriptions created by him. If he will add the id of patient with patients signature, he will see the full history of prescriptions of current patient. Doctor can define the time span of returned prescriptions as also a filter to only return prescriptions which aren't realized yet.
Result:	List of prescriptions for the patient.
Database method:	browse_patient_prescription_history

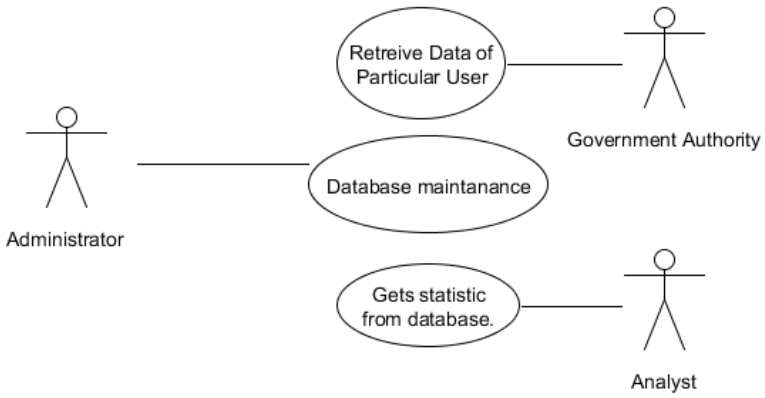
5.4 Pharmacist

Actors: Pharmacist	Title: Prescription realization
Goal:	Pharmacist realizes the prescription. DB checks if the request can be verified and if the prescription is valid.
Scenario:	Pharmacist enters his id, prescription id as well as drugs id, dosage and qunatity of medicine. Everything is signed by pharmacist key.
Result:	OK response from database if operation was successful.
Database method:	prescription_realization

Actors: Pharmacist	Title: Browse Active Prescriptions
Goal:	Pharmacist can see prescriptions which are not yet realized.
Scenario:	Pharmacist sends his id and id of current patient which are signed by both of their keys. Pharmacist can see only prescriptions which are not yet realized.
Result:	List of prescriptions for the patient.
Database method:	browse_active_prescriptions

5.5 Special Users

There are also defined three other users which cope with the system on special ocassions. These are - administrator, which maintains the system, analytic tools which can be used to obtain statistical data and the goverment authority which has super access to all the data after acquiring proper permissions from court or police.



Actor: Administrator	Title: Central Server maintenance
Goal:	Administrator modifies the database, upgrades software etc.

Actor: Goverment Authority	Title: Retreive Data Of Particular User
Goal:	Goverment Authority (GA) can retreive all sensitive data of every user after showing permission to do so e.g. court order. GA account password can be separated into several pieces to ensure that one attacker won't be in possesion of the key.

Actor: Analytic tools	Title: Obtaining statistics from DB
Goal:	Analyst can query the database for statistical data e.g. number of medicines sold in last month. Analyst can't query patients or link prescriptions data to particular person.

Chapter 6

Communication

Every communication with database can be described by one abstract scenario. First central server and client establish session via SSL. After correct establishment of session, client chooses one of database functions that he can execute with appropriate arguments. Before using methods requiring signatures, client has to ask server for nonce, generated specially for the user. After obtaining the nonce, client can execute selected function. Database verifies the correctness of signature and data passed in arguments and returns the result, or if one of the verification steps failed, error message.

6.1 Connecting to Central Server

1. Enter smartcard with users private key and certificate (or establish paths to them)
2. set path of PostgreSQL to environment variable PATH.
3. in command line write $psql\ 'host = hosts_ip\ port = port\_address\ dbname = database\_name\ user = username\ sslmode = require\ sslcert = user.crt\ sslkey = user.key\ sslrootcert = ca.crt'$ where:
   - *host* - IP of server where database is
   - *dbname* - is the name of database to which we want to connect
   - *user* - name of user which want to connect. Each part will have its own user name.

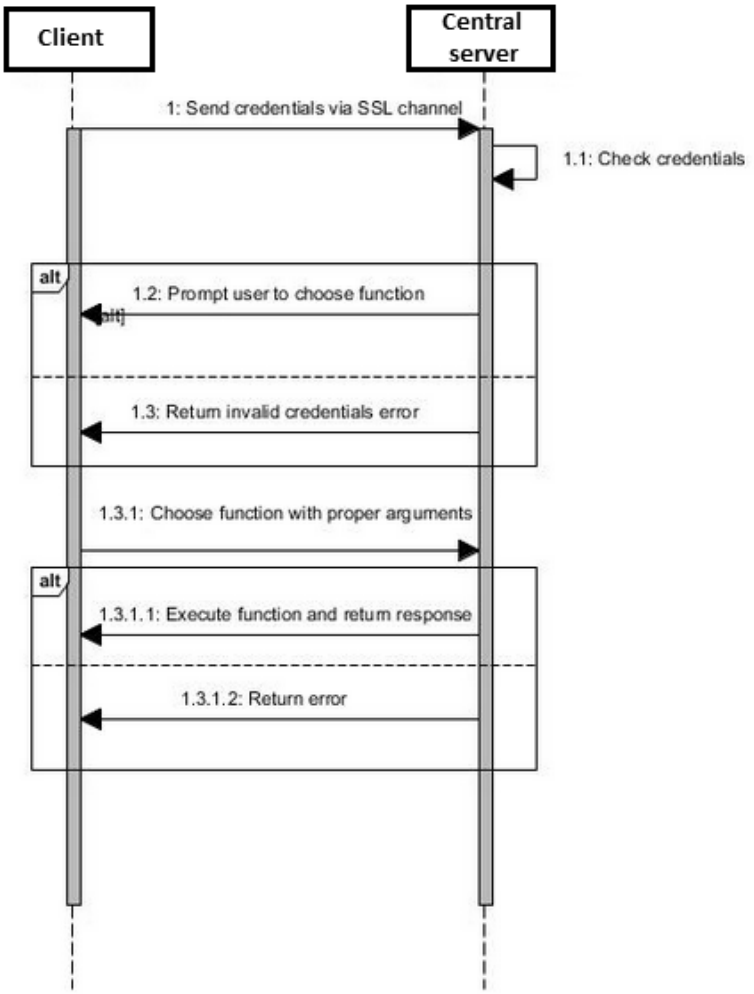


Figure 6.1: General communication diagram for patient, pharmacist and doctor

- *sslcert* - certificate of user.
- *sslkey* - private key of user.
- *sslrootcert* - Certificate of CA.

Example login: $psql\ 'host = 95.85.28.156\ port = 5432\ dbname = PrescriptionSystemMk2\ user = patient\ sslmode = require\ sslcert = patient.crt\ sslkey = patient.key\ sslrootcert = ca.crt'$

4. enter password

6.2 Nonces & Verification Proccess

Randomly generated nonces are part of challenge-response protocol used in communication with database layer. Nonce are security measure against the replay attack. If a request require signature of any party, client has to ask database for generated nonce for given ID. After nonce is return, client has to:

1. Conacatenate function name,
2. function arguments,
3. nonce.
4. Calculate SHA-1 sum over the concatenated elements.
5. Sign the with appropriate key[1].
6. Add the signature as the corresponding argument in function.
7. Send the request.

When the server obtains the request:

1. Takes users key from the database
2. Validates the signature
3. If the signature is validated, constructs SHA-1 sum in the same way as user
4. compares the verified, signed sum with one calculated in previous point
5. Executes the query if the sums are equal
6. Returns the result to the user

[1]Signing method should be equal to invoking openssl command "openssl rsautl sign" with necessary parameters only

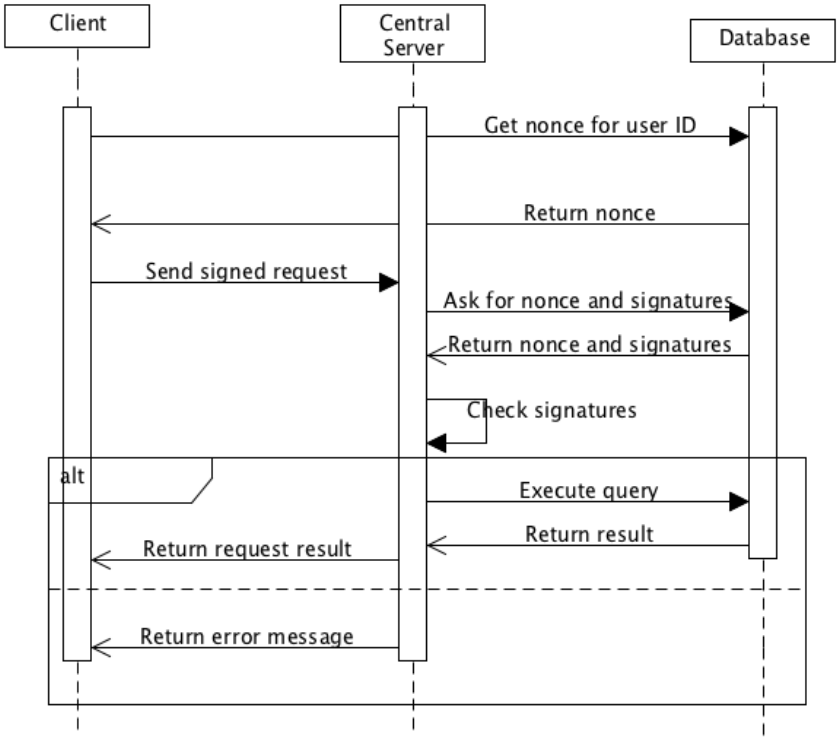


Figure 6.2: Sequence diagram of executing request with nonce signature

Chapter 7

Database Functions and Schema

7.1 Database Functions

After veryfing credentials sent by user to Central Server via SSL secure channel, user, depending on its role, will be able to execute set of functions, which will serve single purpose each (e.g. creation of new prescription).

7.1.1 Shared Functions

	browse_medicines
Arguments:	• name (string, optional, default = None) • type (string, optional, default = None)
Usage:	Pharmacist sends his id and id of current patient which are signed by both of their keys. Pharmacist can see only prescriptions which are not yet realized.

Result:	• medicine_id • name • prescription requirement • medicine type • maximum dosage • unit

Note: Multiple records may be returned at single request.

	browse_doctors
Arguments:	• name (string, optional, default = None) • address (string, optional, default = None) • license_number (string, optional, default = None)
Usage:	Entity using this function performs simple query which return all public data regarding registered doctors stored in DB. Arguments name, adress and license_number narrows down result applying filters to the executed query.
Result:	• doctor_id • name • address • license_number • certificate • public_key

Note: Multiple records may be returned at single request.

	browse_pharmacists
Arguments:	• pharmacist_name (string, optional, default = None) • address (string, optional, default = None) • license_number (string, optional, default = None) • pharmacy_name (string, optional, default = None)
Usage:	Entity using this function performs simple query which return all public data regarding registered pharmacists stored in DB. Arguments name, adress and license_number narrows down result applying filters to the executed query.
Result:	• pharmacist_id • name • address • license_number • certificate • public_key • pharmacy_name

Note: Multiple records may be returned at single request.

7.1.2 Patient Functions

	get_patient_nonce
Arguments:	• patient_id (integer, mandatory)
Usage:	Function returns 1024 bit nonce for given patient_id.
Result:	• nonce
Comment:	New nonce is generated only if the last request was successfully verified.

	browse_my_prescriptions_history
Arguments:	• patient_id (integer, mandatory) • executed (boolean, optional, default = None) • start (date, optional, default = None) • end (date, optional, default = None) • patient_signature (byte, mandatory)
Usage:	Patient requires history of his prescriptions. In order to get access to this kind of data, patient needs to sign his request using his secret key. Next, the signature will be veryfied by database. If signature will be acknowledged as genuine, database will return data about patient prescription history. Database provides patient the ability to filter his history by mean of time span and by the information about execution of prescriptions.
Result:	• prescription_id • doctor_id • doctor name • doctor address • doctor license number • prescription_owner_id • drug id • dosage • max dosage • unit • quantity • execution • time of execution • pharmacy_id • pharmacy_name • pharmacy_adress

Note: Multiple records may be returned at single request.

	transfer_prescription
Arguments:	• patient_id (integer, mandatory) • owner_PESEL (integer, mandatory) • prescription_id (integer, mandatory) • patient_signature (byte, mandatory)
Usage:	Patient changes prescription owner to another patient, therefore allowing him to buy out specific prescription. It is important note, that after changing owner of prescription, original owner is NOT able to buy out his prescription until transfer is cancelled.
Result:	• new_owner_id • "OK"
Comment:	Prescription in database structure has two fields indicating prescription ownership - patientID (non-changeable, indicates the patient to which the medicine was prescribed) and owner_PESEL (patient which will may realize the prescription). Transfering the right will only apply if both of these fields point to same id - thus we exclude the scenario when patients can pass the prescription to yet another person. After this operation the transferring patient losses right to realize the prescription - prevention from cloning the prescription.

	cancel_prescription_transfer
Arguments:	• patient_id (integer, mandatory) • prescription_id (integer, mandatory) • patient_signature (byte, mandatory)
Usage:	Patient changes actual owner of his prescription back to the original one (the patient himself) allowing him to buy out prescription and disallowing former owner of prescription to do so.
Result:	• "OK"

Comment:	Prescription in database structure has two fields indicating prescription ownership - patientID (non-changeable, indicates the patient to which the medicine was prescribed) and ownerID (patient which will may realize the prescription). Cancelling will only work if patientID and ownerID are different and the signature over request is verified.

7.1.3 Doctor Functions

	get_doctor_nonce
Arguments:	• doctor_id (integer, mandatory)
Usage:	Function returns 1024 bit nonce for given doctor_id.
Result:	• nonce
Comment:	New nonce is generated only if the last request was successfully verified.

	create_prescription
Arguments:	• doctor_id (integer, mandatory) • patient_id (integer, mandatory) • drug_id (integer, mandatory) • dosage (integer, mandatory) • unit (integer, mandatory) • quantity (integer, mandatory) • doctor_signature (byte, mandatory)
Usage:	Doctor prescribe single medicine to the patient, describing medicine, quantity and dosage.
Result:	• "OK"

Comment:	Database does not requires patient signature to create a prescription for him - Prescription realization will require his key (thus his smartcard) so the medicine can't be bought without his knowledge. Also the doctor can create prescription without the need of meeting the patient face to face - which is and advantage for chronically ill patients.

	browse_patient_prescription_history
Arguments:	• doctor_id (integer, mandatory) • patient_id (integer, mandatory) • start (date, optional, default = None) • end (date, optional, default = None) • bought(boolean, optional, default = None) • doctor_signature (byte, mandatory) • patient_signature (byte, optional)
Usage:	Doctor downloads patient prescription history. Doctor (unlike pharmacist) do not needs patient signature to browse history od prescription that he has created. If he wants the full history, patients signature is needed.

Result:	• prescription_id • doctor_id • doctor name • doctor address • doctor license number • prescription_owner_id • drug id • dosage • max dosage • unit • quantity • execution • time of execution • pharmacy_id • pharmacy_name • pharmacy_adress
Comment:	If the patient signature is missing, database will only return prescriptions which were created by the doctor. If the patient signature is present and can be verified, doctor will receive the full history of patient. In case of any errors on verification, the request will be canceled.

Note: Multiple records may be returned at single request.

7.1.4 Pharmacist functions

	get_pharmacist_nonce
Arguments:	• pharmacist_id (integer, mandatory)
Usage:	Function returns 1024 bit nonce for given pharmacist_id.
Result:	• nonce

Comment:	New nonce is generated only if the last request was successfully verified.

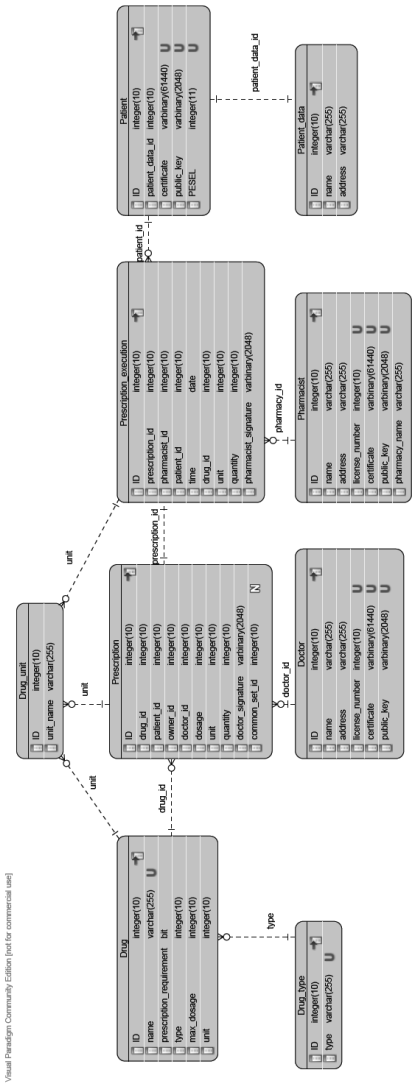
	prescription_realization
Arguments:	• prescription_id (integer, mandatory) • pharmacist_id (integer, mandatory) • drug_id (integer, mandatory) • unit (integer, mandatory) • quantity (integer, mandatory) • pharmacist_signature (byte, mandatory) • patient_signature (byte, mandatory)
Usage:	Pharmacist will be able to realize patient prescription by pointing right prescription by giving its id, choose proper medicine (not necessarily the same as medicine prescribed by doctor, this check will be done by database), describe how many medicine is sold.
Result:	• "OK"
Comment:	Request has to be signed by both patient's and pharmacist's keys. If the signature is incorrect, the database will return error message and the medicine shouldn't be given away.

	browse_active_prescriptions
Arguments:	• pharmacist_id (integer, mandatory) • patient_id (integer, mandatory) • pharmacist_signature (byte, mandatory) • patient_signature (byte, mandatory)
Usage:	Pharmacy is able to see all active (not bought) prescriptions of current patient, which agrees to show this data to the pharmacy by signing request.

Result:	• prescription_id • doctor_id • doctor name • doctor address • doctor license number • prescription_owner_id • drug id • dosage • max dosage • unit • quantity • execution • time of execution
Comment:	If the signatures of patient or pharmacist are incorrect, database will return an error. If there are no non-realized prescriptions, database will return empty list.

Note: Multiple records may be returned at single request.

7.2 Database schema



Chapter 8

Central Server Security Standards

8.1 Physical Security

- Servers is protected by backup and offsite data storage. The offsite storage of backup media is in a secure backup-vendor secure facility.
- A facility with Uninterruptible Power Supply (UPS) supporting all servers and essential peripheral equipment (console servers, etc).
- A facility with a climate controlled environment separate from the building HVAC, (dedicated air conditioning with in-room temperature controls).
- A facility with cooling and electrical capacity that is planned and monitored for outages.
- Secured access to the facility with documentation listing all individuals who currently have access and monitoring/auditing of ingress/egress via staff/video/etc.
- Servers in the facility must require authentication for local access (i.e. consoles are not left logged in while unattended).
- For facilities that use access codes, the capability to quickly change the access codes if personnel changes warrant is required. Access codes must be changed at least annually.
- A facility with automated fire detection and suppression systems.

8.2 Data Encryption

- Hard disks, on which are stored databases, will be encrypted by external program TrueCrypt. TrueCrypt encrypts whole data on hard disk in real time.
- Databases will be encrypted by TDE (Transparent Data Encryption). TDE encrypts:
  - Database files
  - Database Snapshots
  - Transaction Log File
  - Backups

  using DEK (Database Encryption Key) which is protected by certificate.

8.3 Backup Procedure

- To ensure no data loss, database is replicated in real-time to a server in another location - this location meets conditions mentioned in section 5.1.
- Additionally, regular backups are made every day.
- Backups are kept for reasonable amount of time:
  - Daily backups - 1 week
  - Weekly backups - 1 month
  - Monthly backups - 1 year
  - Annual backups - forever
- All backups are encrypted with measures described in section 5.2.

Part IV

Pharmacy Module

Chapter 9

Data Flows

9.1 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 9.1: Patient's and pharmacist's use cases

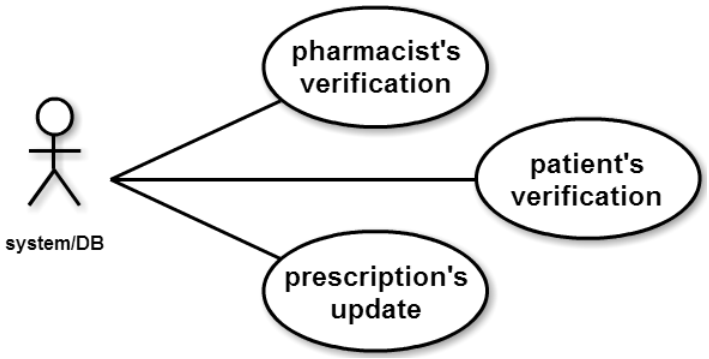


Figure 9.2: System's use cases

9.2 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.

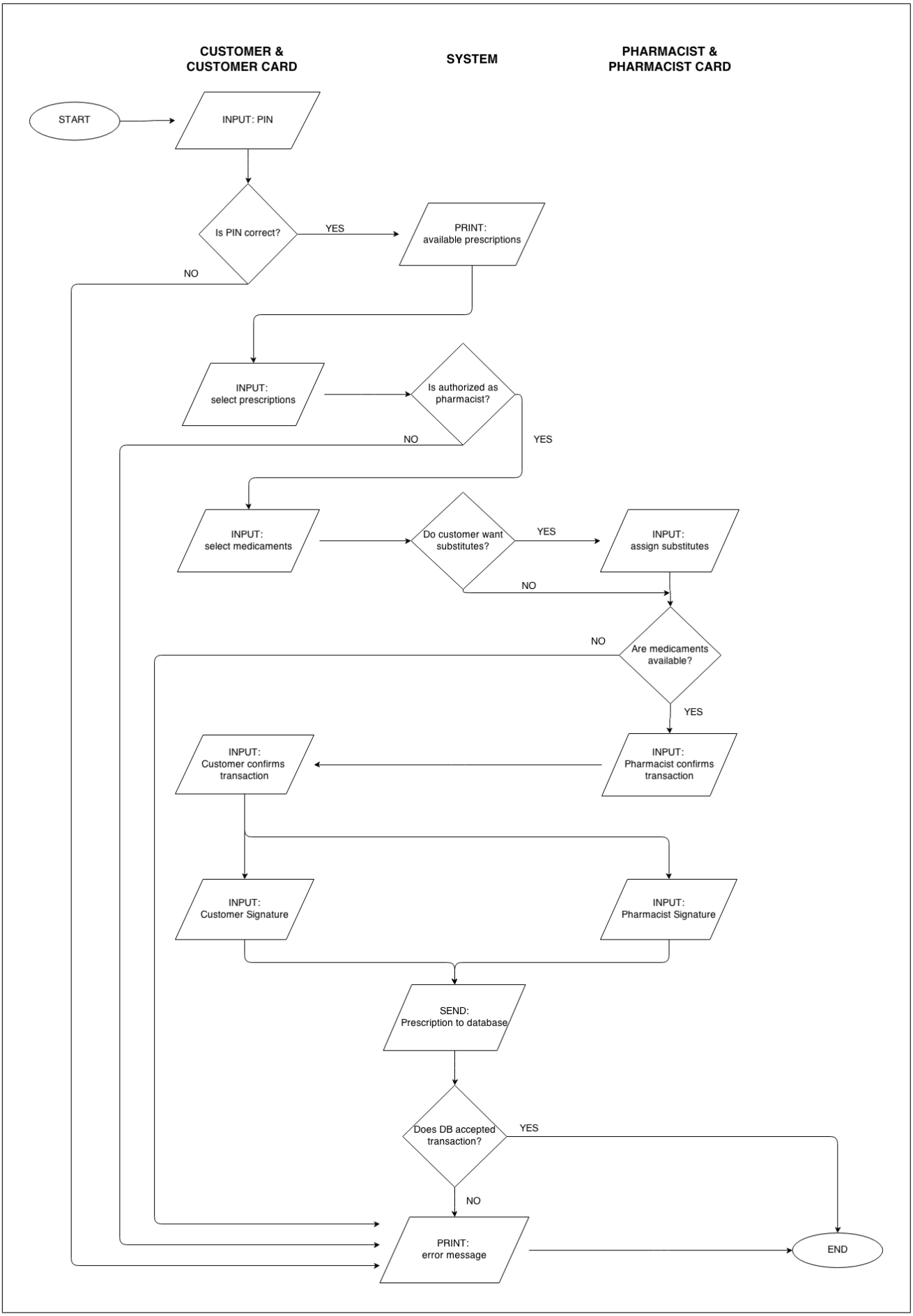


Figure 9.3: Flow chart

Chapter 10

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.

10.1 Communication initialization

The first step is communication initialization. Actions performed in this step by the system elements are presented in the figure 10.1

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.

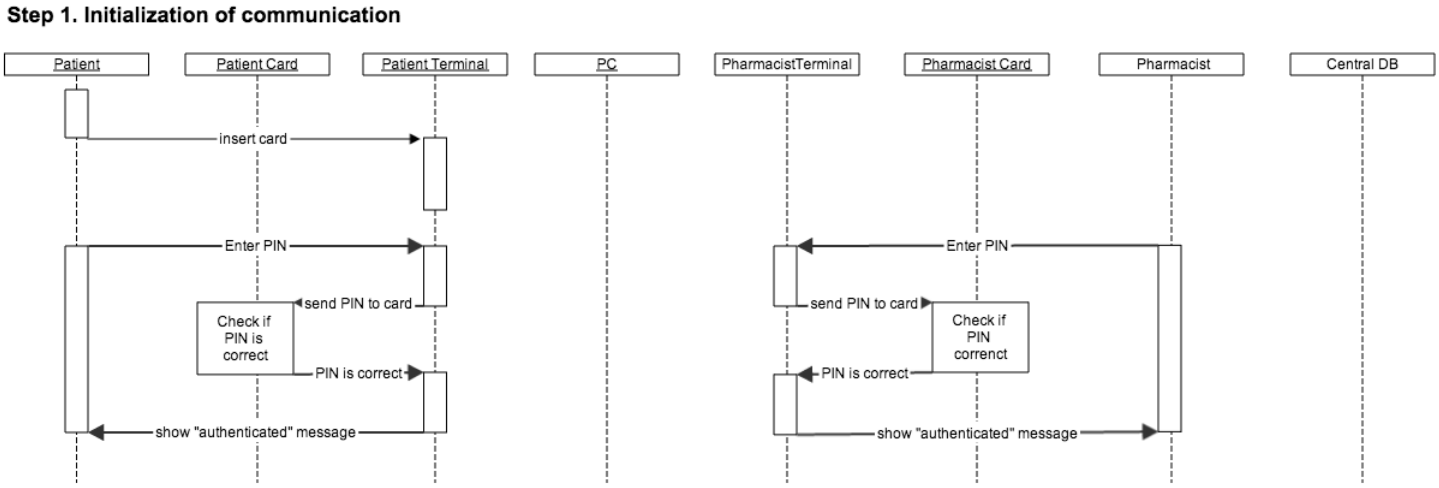


Figure 10.1: Sequence diagram - step 1

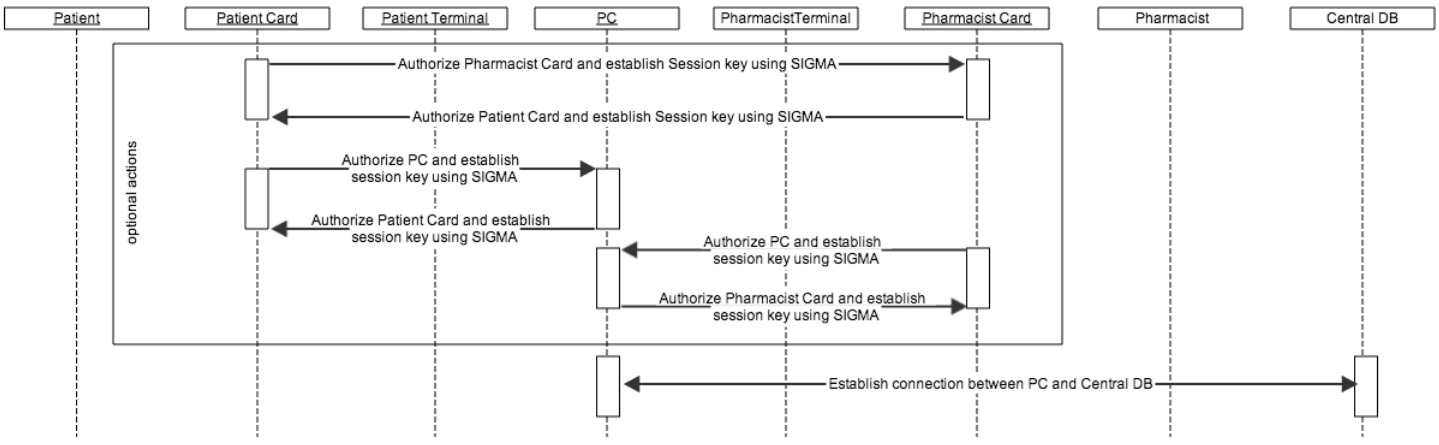


Figure 10.2: Sequence diagram - step 2

10.2 Establish a secure communication

The second step, presented on the figure 10.2, 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.

10.3 Select prescription to buy

The figure 10.3 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.

10.4 Realize prescription

The last step is presented on the figure 10.4. 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

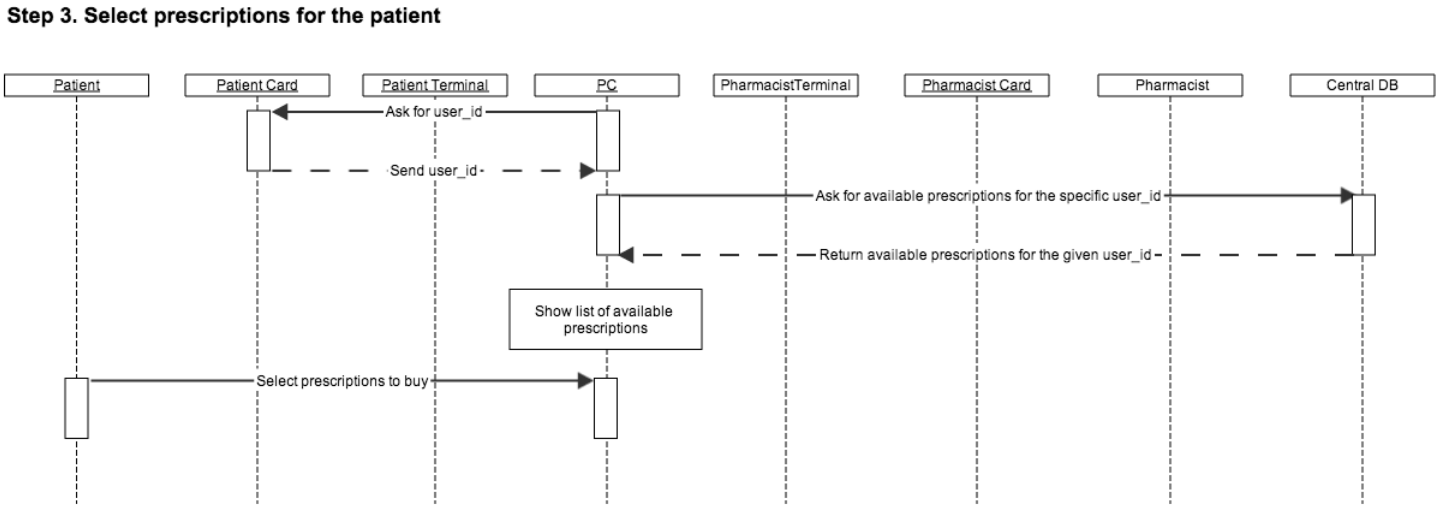


Figure 10.3: Sequence diagram - step 3

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.

10.5 End of the protocol

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

Step 4. Confirm the buying of the medicine

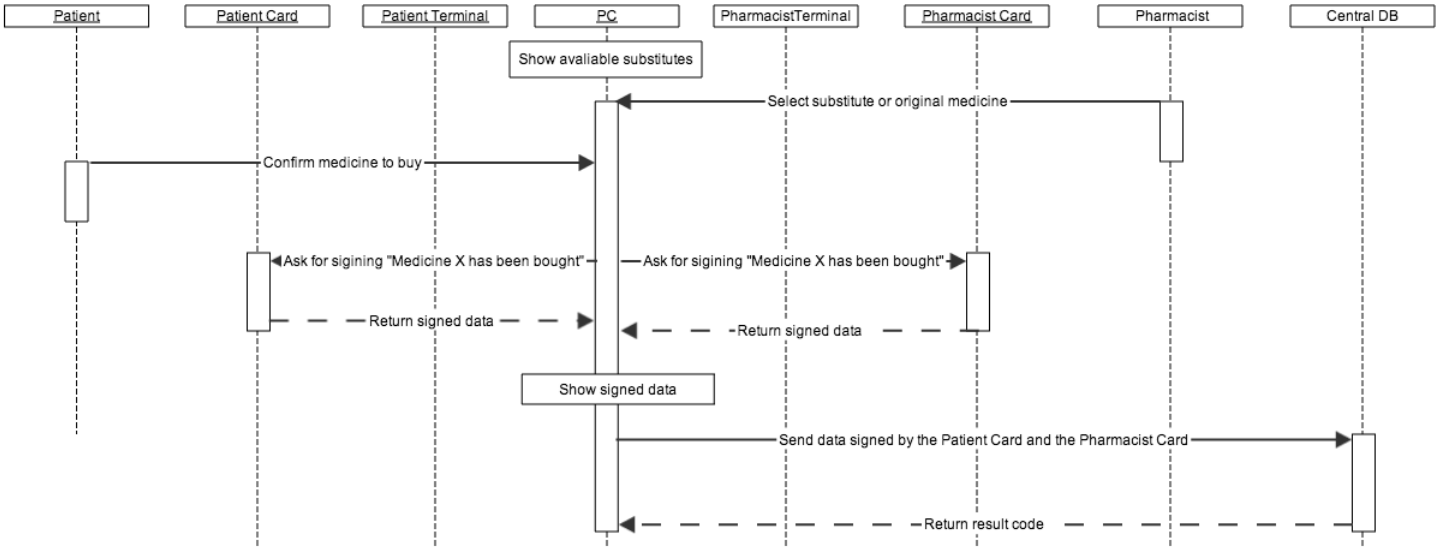


Figure 10.4: Sequence diagram - step 4

Part V

Patient

Chapter 11

Patient's module

11.1 Module description

The prescription system from the patient point of view is based on smart cards. Each patient has a unique card with ID and a pair of cryptographic keys used to create a signature. The system could be easily combined with electronic IDs, when they become available in Poland.

The benefit of our system is that the patient could get the prescription without leaving home. He could request medicines by calling the doctor, who would prescribe them and make available on patient's account. In order to decrease the refund fraud problem, the patient has to realize the prescription in pharmacy by himself. If he is unable to realize it, he would be able to transfer it onto another person's account. Realization of a transferred prescription would only be possible for the person designed by the patient. However, if the patient would like to change the designed person or make the prescription again available for him to realize, he would be able to cancel the transfer.

Both the patient and the doctor (with patient's permission) are able to browse all of the patient's previous prescriptions. It could be helpful to reduce possibility of interactions between drugs prescribed by different specialists. Also, doctors would not be able

to abuse this functionality, because it would require the patient to insert his smart card into the terminal in doctor's office.

Patient is able to browse the list of medicines, doctors and pharmacies. Thanks to this, he could easily check the leaflet of the medicine, find the phone number to the doctor or check the opening hours of the pharmacy.

11.2 Goals of the patient module

- Protection from the refund fraud problem
- Possibility to get prescriptions without leaving home
- Functionality of transferring prescription to another person's account
- Availability of prescription history for a doctor
- Possibility to browse the list of medicines, doctors and pharmacies

Chapter 12

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 lifesaving, 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
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

12.1 Protection methods

12.1.1 Smart Card

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

All of the system's users will be given personalized smart cards which will store their identification data: names, surnames, PESEL and digital certificates. Each card would have PIN number associated with it, that will be used to initialize authentication process.

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

In case of loosing a smart card, the user should perform a standardized revocation procedure, i.e. he should block a card in the assigned institution. The user should enroll for a new card afterwards

12.1.2 Certificates

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

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

Chapter 13

System architecture

The patient's module architecture consists of the following elements:

- smart card with personal certificate and secure key storage, used for the authentication and signing
- patient's application, providing all of the functionalities required by patient's module:
  - provides user-friendly interface
  - is connected with patient's card and the database
  - establishes two way SSL connection
- database is a central element of the whole system; stores the data and handles all the necessary database I/O functions; the database is described in greater detail in Database & Server Documentation'

Chapter 14

Use Cases

Patients have access to the system by dedicated patient's application. Each patient is given unique, personal smart card that is being used for authentication.

14.1 Use cases for patient's application

The patient's application is a graphical interface to the patient's module. It includes six use cases that are available for the patient:

browse medicines
: The patient is able to browse all medicines available in the database. There is a leaflet attached to each medicine's description, that contains at least dosage and contraindications.

browse pharmacies
: The patient is able to browse all pharmacies available in the database. Each pharmacy has its address and opening hours listed for patient's convenience.

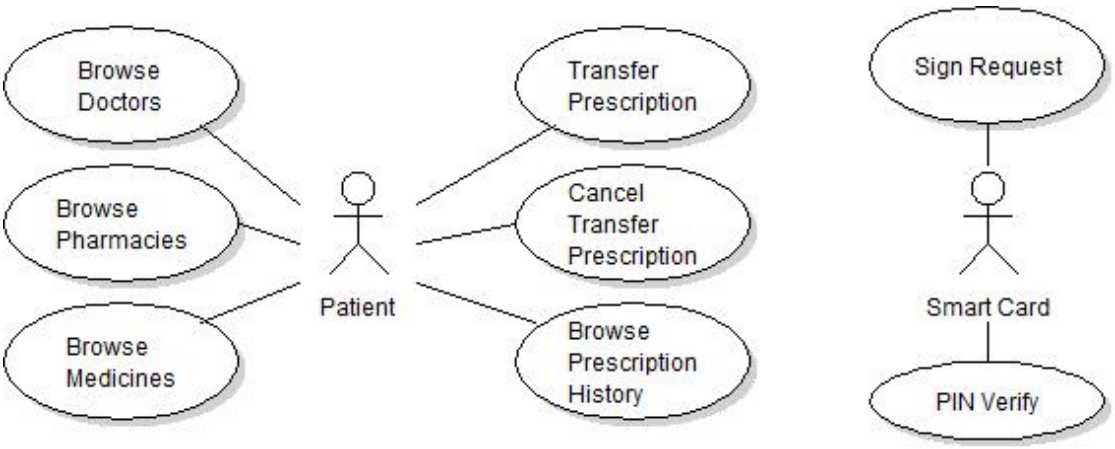


Figure 14.1: Use cases

browse doctors

The patient is able to browse all doctors available in the database. He can find phone number and office address for each doctor.

browse prescription history

The patient can browse all of his prescriptions, differentiated on active and already realized.

transfer prescription

If the patient cannot realize prescription, he is able to transfer his prescription buying rights to somebody else.

cancel prescription transfer

The patient can cancel transfer of prescription and realize it by himself or transfer it again.

14.2 Smart card use cases

The smart card, introduced into the system for security reasons, includes two use cases.

sign message

The smart card signs a message produced by patient's application. The signature would be used in calls to database procedures.

verify PIN

The smart card verifies PIN, that the patient has entered, in order to access any functionalities of the system.

14.3 Flow chart for transfer prescription use case

To transfer the prescription user has to enter correct PIN. Application establish connection with database and retrieve the list of prescription available to transfer. The list contains only prescriptions which can be transferred by the patient. Then the patient is able to select prescription to transfer from the list and enter the new owner's ID. After the patient's confirm transfer, application create and send request to the database. If the signature under the request concatenated with nonce is valid and request contains required data database transfers the prescription to the new owner.

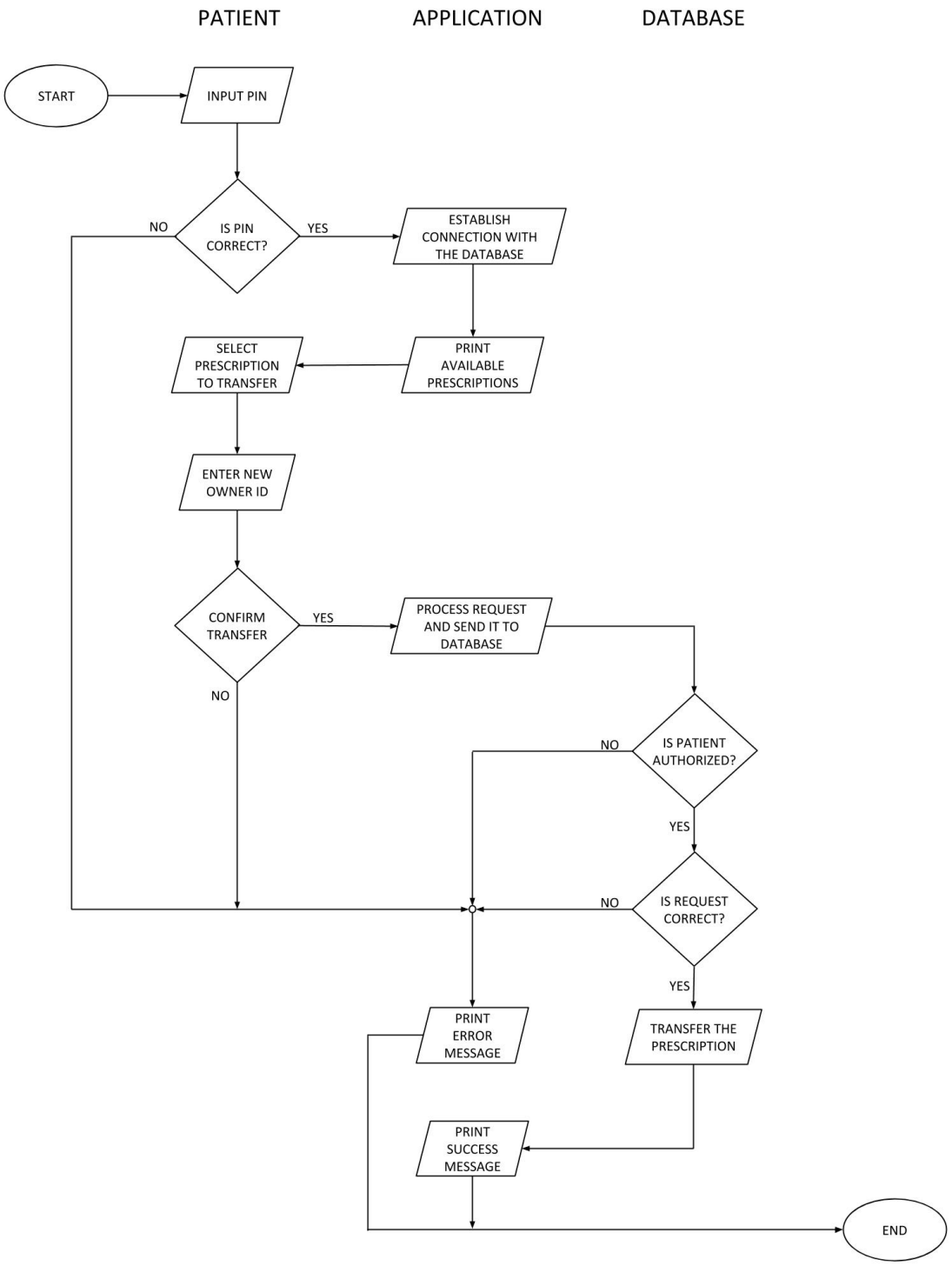


Figure 14.2: Transfer prescription flow chart

Chapter 15

Functionalities of application

The application implements following functions:

- `browse_medicines`
- `browse_pharmacies`
- `browse_doctors`
- `browse_prescription_history`
- `transfer_prescription`
- `cancel_prescription_transfer`

They are discussed in greater detail below.

15.1 Browse medicines

	`browse_medicines`
argumets	• `name` • `type`
description	The patient is able to browse all medicines available in database.
action	After entering name of medicine, function is querying database for results.
display	• `name` • `prescription requirement` • `patient information leaflet`

15.2 Browse pharmacies

	`browse_pharmacies`
argumets	• `name` • `address`
description	The patient is able to browse all pharmacies available in database.
action	After entering name or address of pharmacy, function is querying database for results.
display	• `name` • `address` • `phone` • `opening hours`

15.3 Browse doctors

	`browse_doctors`
argumets	• `name` • `address` • `license number`
description	The patient is able to browse all doctors available in database.
action	After entering name of doctor or address, function is querying database for results.
display	• `name` • `address` • `phone`

15.4 Browse prescription history

	`browse_prescription_history`
argumets	• `time interval` • `isExecuted`
description	The patient is able to browse all of his previous prescriptions.
action	Function is querying database for results, using patient's ID and signature created by the smart card.
display	• `medicine name` • `quantity` • `unit` • `dosage` • `execution` • `time of execution` • `doctor name` • `doctor signature` • `pharmacist name` • `pharmacy signature`

15.5 Transfer prescription

	`transfer_prescription`
argumets	• `new owner ID` • `prescription ID`
description	The patient can transfer the prescription to another person.
action	After entering ID of designed person and choosing the prescription, function that transfers it is called, using patient's ID and signature created by the smart card.
display	• `new owner ID` • `exit status`

15.6 Cancel prescription transfer

	`cancel_prescription_transfer`
argumets	• `prescription ID`
description	The patient is able to transfer his prescription back into his account.
action	After choosing the prescription, function that rolls back the transfer is called, using patient's ID and signature created by the smart card.
display	• `exit status`

Chapter 16

Functionalites of patient's card

The patient's card implements following functions:

- `sign`
- `PIN verify`

They are discussed in greater detail below.

16.1 Sign request

	`sign`
argumets	• `message`
description	The patient's card signs doctor or pharmacist request.
action	The patient's card makes a signature under doctor or pharmacist message using its secret key.
result	• `signature` • `exit status`

16.2 PIN verification

	`PIN_verify`
argumets	• `PIN`
description	The card verifies the PIN given by patient.
action	The patient's card verifies correctness of the PIN entered by the patient.
result	• `exit status`

Chapter 17

Sequence diagrams

17.1 Sequence diagram for connection initialization

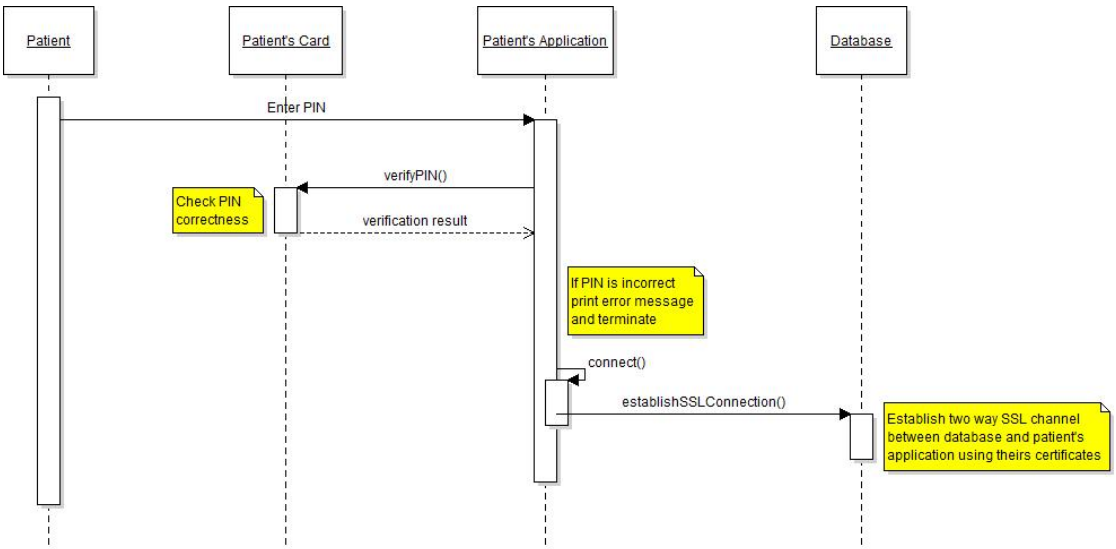


Figure 17.1: Connection initialization

When the patient connects to the system, he needs to enter the PIN. Then, the PIN is verified by the Patient's Card. If the verification fails, an error message is printed and the connection is terminated. Otherwise, the Patient's Application establishes a two-way SSL channel with the database. From this point, the communication between

the Patient's Application and the database is done through SSL encrypted channel.

17.2 Sequence diagram for transfer prescription functionality

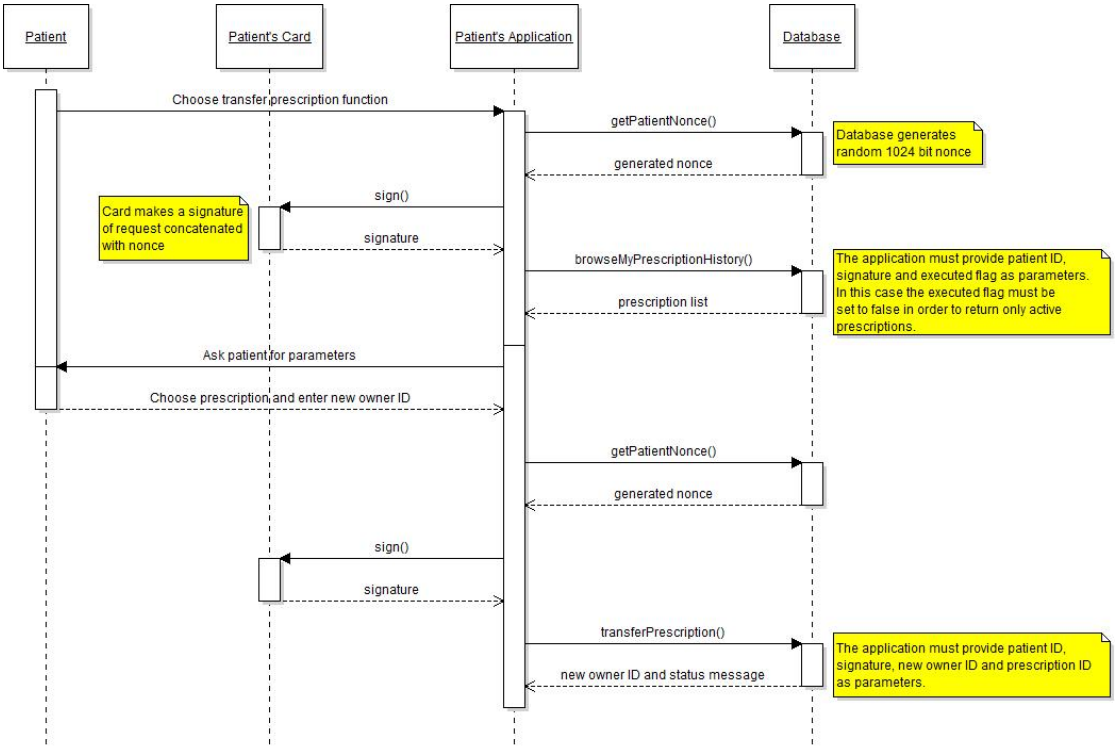


Figure 17.2: Transfer prescription

This sequence is executed after establishing a secure connection with the database.

To transfer a prescription, the patient has to choose transfer prescription functionality in the Patient's Application (PA). PA sends patient's ID to the database and receives a random 1024 bit nonce. Afterwards, PA sends created browse prescriptions request to the Patient's Card (PC) for signing. PA sends the signed request to the database (DB) and receives a list of available prescriptions. Then the patient chooses a prescription he wants to transfer from the list, and enters new owner's ID. Next, PA requests new nonce from DB and creates a valid transfer prescription request, which is signed by PC. The request with a signature is sent to DB afterwards. DB verifies both the request and the signature. If the verification was successful, DB transfers the prescription to the new owner and returns a status message and the ID of new owner.

17.3 Sequence diagram for browse medicines functionality

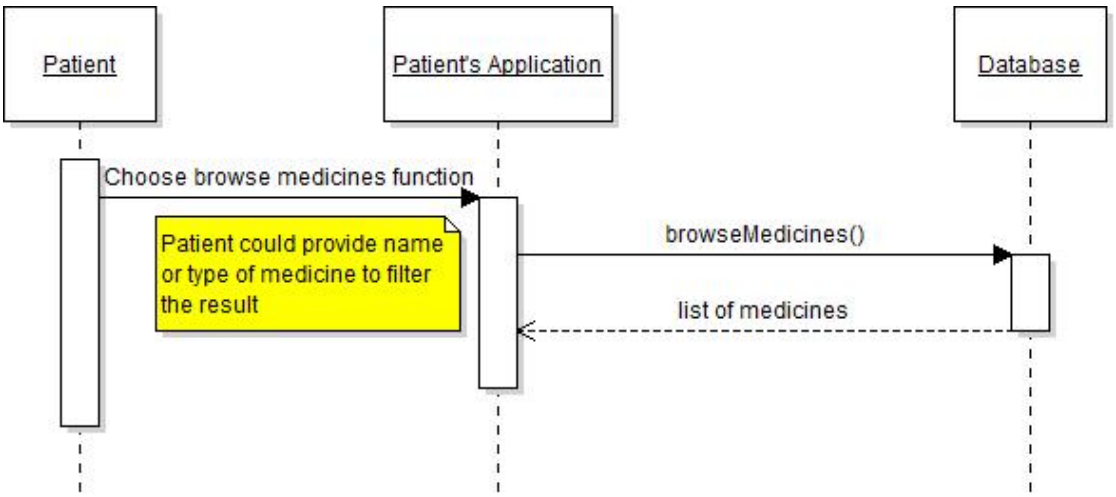


Figure 17.3: Browse medicines

To browse medicines, the patient needs to choose browse medicines functionality in the Patient's Application. Then, the Patient's Application prepares a request with parameters either default or provided by the patient. The request is sent to the database afterwards. The database returns a list of medicines which is displayed to the patient in the Patient's Application.

Chapter 18

Security

Both security mechanisms used in the patient's module and their justification are described in the following sections.

18.0.1 Used security mechanisms

18.0.2 Smart 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.
Card's data access	• Card is read only is the sense that patients 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 entering PIN. The user is given 4-digit PIN and the verification system will allow three attempts before blocking the card.

18.0.3 Authentication

Patient's authentication is constructed as a two factor process. It includes the following points:

- Something you have - smart card (containing user's certificate)
- Something you know - PIN needed to access smart card's functionalities

18.0.4 Connection

The connection between the application and the database is established by two-way SSL protocol. Whole communication afterwards would be sent by encrypted SSL channel. We assume that if the connection was lost, the whole authentication process needs to be repeated.

18.1 Justification

18.1.1 PIN protection

The PIN number is used to authenticate the cardholder. We propose 4-digit PIN number. Three subsequent incorrect attempts will block the card. Similar mechanism is already used e.g. in ATM cards.

18.1.2 Secure communication with the database

The communication channel between the database and the application is secured with a two way SSL protocol. We assume that SSL provides all necessary mechanisms to protect the channel from attacks.

18.1.3 Protection against prescription overtaking

Transfer prescription request have to be signed by the patient using his private key in order to not give buying rights to unauthorized person. If the patient has made a mistake during prescription transfer, he is able to cancel and redo the transfer correctly.

18.1.4 Protection against prescription duplication

Transfer and cancel transfer prescription functionalities have to be performed in transaction environment by the database. In this way, there would be no possibility that both the patient and new owner could buy the prescription simultaneously.

18.2 Advantages of system

Our system is designed in way that any defraudation of purchasing not prescribed medicine is impossible, pharmacist can not do any defraudation on transaction of seeling drugs to the patient which were not previously prescribed by the doctor, because to every transaction our system demands patient's smart card with previously issued prescription by the doctor and signed by his smart card.

The above security assure very secure system of digital signatures and certificates which will be implemented in our application on smart cards and users programs. This system will prevent any defraudation from users (patient/ pharmacist/ doctor) and also simplify any financial settlement between pharmacist and NFZ, furthermore system will be very comfortable and easy to use for every user.

Part VI

Doctor

Chapter 19

Introduction

First of all we describe current system - his advantages and disadvantages, the biggest problems from the point of view that presents the final recipient. Our part is ”doctor module” so we will focus only on this part of the system.

19.1 Current situation

19.1.1 Uncontrolled money flow and embezzlement of public money

Let say that we have 2 corrupted parties in current system - doctor and pharmacist. In that situation doctor can create fake prescription for any of his patient, then send them to pharmacist and he - as second partie - can declare that prescription that is financing by NFZ as completed. It is the way how today polish money goes abroad.

19.1.2 Digitalization of prescription

There is a lot of problems with paper prescription - the biggest is that sometime - when we are serious illness - we have a lot of prescription, and then there is big opportunity to lost few of them, and that is a quite big problem because we need to go back to a doctor for new visit and get copy of them. There is another opportunity for a patient to

get prescription for some medicine but what if he really did not lost a prescription? He can buy a medicine twice and i.e. sell them on black market. We want to exclude that opportunity.

19.1.3 Internet shopping

Today we can only buy in online pharmacy medicines that can be bought without prescription. There are people that prefer online shopping because it is easier and faster than basic shopping in pharmacy when we have to go there, stay in a queue. We want to create possibility to buy every medicine in online pharmacy in secure way.

19.1.4 Prescription pad has been lost

We would like to pay attention to a situation when a doctor lost his prescription pad. We do not know how it works today but it is a situation that makes the system unsecure. e-prescription does not have that lack of security.

19.2 Requirements

We want to eliminate as much as possible of that issues, but still we need to fulfill the requirements, which are:

- It should be impossible to create a prescription without patient‘s present and knowledge item All prescriptions should be kept in digital form in central database
- Prescription‘s owner should be verified in pharmacy and only the owner can realize the prescription
- Patient should be able to overview his own prescription history
- Doctor is allowed to overview prescriptions history of all his patients and moreover all prescriptions of patient during examination(patient present should be required)

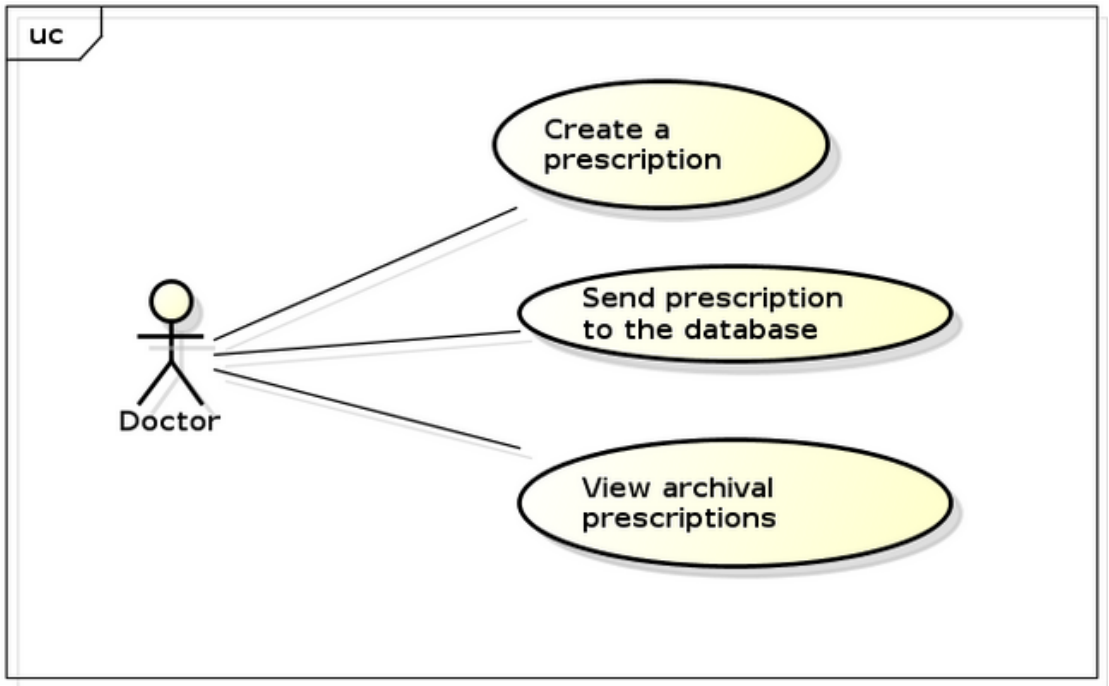
- System should be secure and provide anonymous statistics

Chapter 20

UML Diagrams

In this section we present diagrams that are needed to describe part of the system.

20.1 Use cases



We mark out 3 use cases:

- create a prescription - Doctor is generating prescription by collect all needed data and then signature is forged
- send prescription to the database - prescription sending to database(in some database friendly format)
- view archival prescriptions - Doctor can check archival prescription of his current patient

20.2 Activity diagram

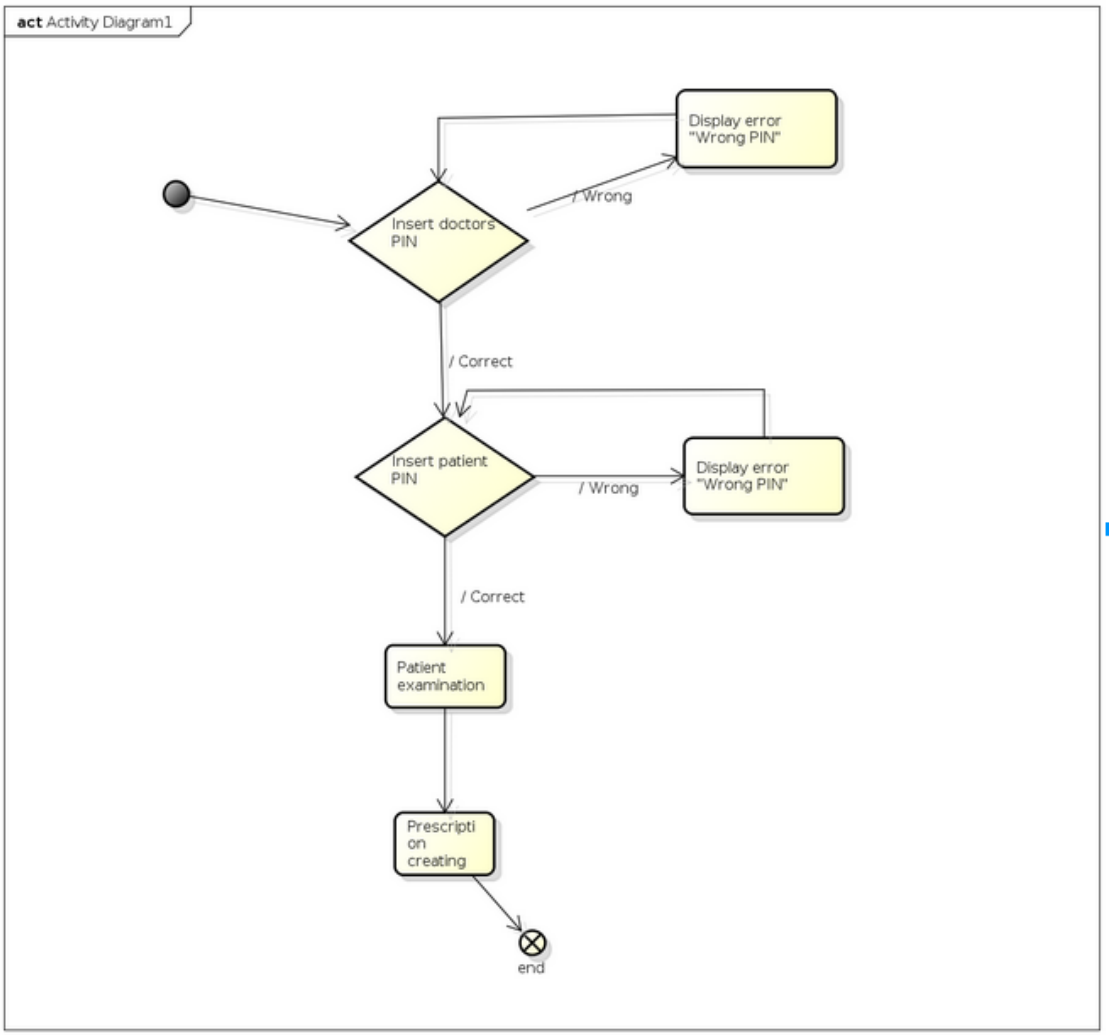
It presents system scheme from high level layer and has to show the overall flow of control

20.3 Sequence diagram

We present detailed scheme of the system. THe mail goal of this diagram is to present communication between out part, and other parts of the system

Writing out a prescription is initialized by the doctor. He can create a prescription on demand or load one previously saved from the csv file. During creation process patients ID should be obtained(from reading patients card or returned by database query). Having newly created prescription, Doctors computer is establishing SSL connection to the database. After this stage, computer requests new value of nonce, by the SQL statement $getnoncefor(patientid)$. This nonce and entire prescription should be signed be the doctors card. At the end of the process query to database is made. It should include: nonce, signature over nonce, prescription and signature over prescription.

Database validates both signatures and nonce before inserting any records. Only information inside database can be considered as valid.



20.3.1 View entire patient's history

View entire patient's history is initialized by the doctor. First of all, doctor creates overview request. During the process patient's ID should be obtained(from reading patient's card or returned by database query). Having the request, Doctor's computer is establishing SSL connection to the database. After this stage, computer requests new value of nonce, by the SQL statement $getnoncefor(patientid)$. This nonce and entire prescription should be signed be the doctor's card.

At the end of the process query to database is made. It should include: nonce, signature over nonce, request and signature over request. Database after successful validation

return patient‘s records.

Chapter 21

Notes

There is no need to require doctor‘s signature in this procedure. Process requires the presence of a patient and his willingness, so only the owner of the card should be verified. Adding doctor‘s signature doesn‘t change anything. It only increase computation time and data amount sended across the internet.

Chapter 22

Prescription

In this part we propose structure of prescription defined using ASN.1. We do not specify format of records in database, it is just a formal specification of object ?Prescription? with information that it has to contain(i.e. it can be even concatenation of all fields specified lower splited by ;¨).

In this model it is obvious that pharmacist‘s signature is equal to fully realized prescription

```
Prescription ::= SEQUENCE {
        CertBody ::= SEQUENCE{
                MetaData ::= SEQUENCE{
                        PrescriptionID          INTEGER, //Unique in DB
                        MagicID                 INTEGER, //Made for DB
                        Created_at              UTCTime //Timestamp
                },
                PatientsData            PersonalDataType,
                DoctorsData             PersonalDataType,
                Medicines ::= CHOICE{
                        SelfMadeMedicine,
                        Medicine
                }
        },
        Signature ::= CHOICE{
                X9.62Signature,         //For EC
                PKCS#7Signature         //For RSA
        }
}
PersonalDataType ::= SEQUENCE{
        Id              BIT STRING
}
SelfMadeMedicine ::= SET OF Ingredient

Ingredient ::= SEQUENCE{
        Name            UTF8String,
        Amount          REAL
        Unit            UTF8String
}
Medicine ::= SEQUENCE{
        Id_medicine     BIT STRING,
        Name            UTF8String,
        Quantity        INTEGER
        Dosage          UTF8String
}
```

Chapter 23

Signature

There is a lot of signature schemes that can be used according to standards (like PKCS# or X9.63) so we do not specify which should be used yet. We want to mark a situations in protocols that has to be signed.

23.1 Doctor signature over prescription, and pharmacist signature as a proof that prescription is realized.

Prescription as a tuple of data and signature can be signed by doctor and then creating prescription process has been completed. Now when pharmacist is realizing prescription, he has to generate another signature over that tuple with some pharmacist personal data and concat it to prescription. If pharmacist sign prescription, it means that prescription is realized (fully because there is only 1 medicine per prescription)

In this scenario there is still possibility to generate prescription without patient knowledge, but it can not be realized without him, so this scheme is still secure.

Doctor has to compute signature, because it is a proof that prescription is valid and is signed by specified person. Without it, there is possibility to craft a lot of prescription without knowledge who is trying to spam database.

Chapter 24

Patient needs to generate signature when patient archival prescription has to be available

There is a use case, when a doctor wants to look into archival prescription of a patient. Core of a system sends then a nounce (random generated byte‘s array) that has to be signed by a patient as a proof that patient allow doctor to check his archival prescription. The Core is not signing a nounce so there is possibility to Adversary (i.e. doctor) to make chosen message attack, so we need to choose digital signature scheme that is unbreakable by chosen-message attack(should we specify what is this?).

Patient needs to generate signature because he is computing a request that says to DB that he want access to archival prescription. Without it, we do not have a mechanism to confirm this request by patient, so there is opportunity to make request for access without a patient knowledge.

Chapter 25

Database integration

The connection to database is authenticated by Two-way SSL and password. Each party in this process have their own X.509 certificate signed by the CA authority. During authentication process each party verifies certificate of another entity, to be sure that entity is exactly who claims to be. Password is required for specify the username to the database.

Whenever prescription is created by the doctor it has to be send to the database and only the prescription inside database can be valid. Sending process requires to be authenticated and it‘s done by the invoke of stored procedure inside database. Procedure takes all information about a prescription at once (specified in section 3).