Final Year Project

SecureMed

Blockchain Based Medical Document Sharing

FYP Team

Haseeb Ijaz i15-0172

Hafiz Mian M Waqas i15-0107

Danyal Ahmad i15-0300

Supervised by

Mr. Muhammad Ali Nasir

Department of Computer Science
National University of Computer and Emerging Sciences

Islamabad, Pakistan

2019

Anti-Plagiarism Declaration

This is to declare that the above publication produced under the:

Title: _____

is the sole contribution of the authors and no part hereof has been reproduced on as it is basis (cut and paste) which can be considered as **Plagiarism** All referenced parts have been used to argue the idea and have been cited properly. The work presented in the report is our own and it has not been submitted/presented previously to any other institution or organization. We will be responsible and liable for any consequence if violation of this declaration is determined.

Date: _____

Student 1
Name: _____

Signature: _____

Student 2
Name: _____

Signature: _____

Student 3
Name: _____

Signature: _____

Supervisor (Faculty)

Name: _____

Signature: _____

Executive Summary:

This report embodies all the requirements as well as the object-oriented designs for system development of SecureMed. This report completely describes the utility that the system provides by defining the roles of the system users, the goals that are met by interacting with the system and in what way or by following what sequence of steps and operations those specified goals are met. The document attempts to provide a brief description of the Constraints and the Stakeholders involved.

The report contains detailed description of the activities, which the Patient and the Hospital staff performs, by providing detailed description on the use cases. There are some sections which describe how the system behaves to every input. The document further contains a plan to execute the development of the system. A section is dedicated to the detailed description of the iteration plan.

Designed Artifacts including the Use Case Diagram, Activity Diagram, Domain Model, System Sequence Diagram, Sequence Diagrams, and Class Diagram to give a description on the Object-Oriented Design. The document further contains the description of the artifacts in textual form for the clarification of the big picture.

Table OF Contents:

1. Introduction

SecureMed provides a secure communication channel between health centers and third-party organizations by making the process more efficient and reliable from the usage perspective and private from the security perspective.

The traditional systems have failed to meet the standards of trust and data confidentiality, these systems are basically deployed for the inter-organizational communication which often requires a Cloud Service Provider to become a trusted party. This trust gives that third-party Cloud Service Providers the power to control the systems of records and control the identity of entities involved in the system. There are two parts of the problem:

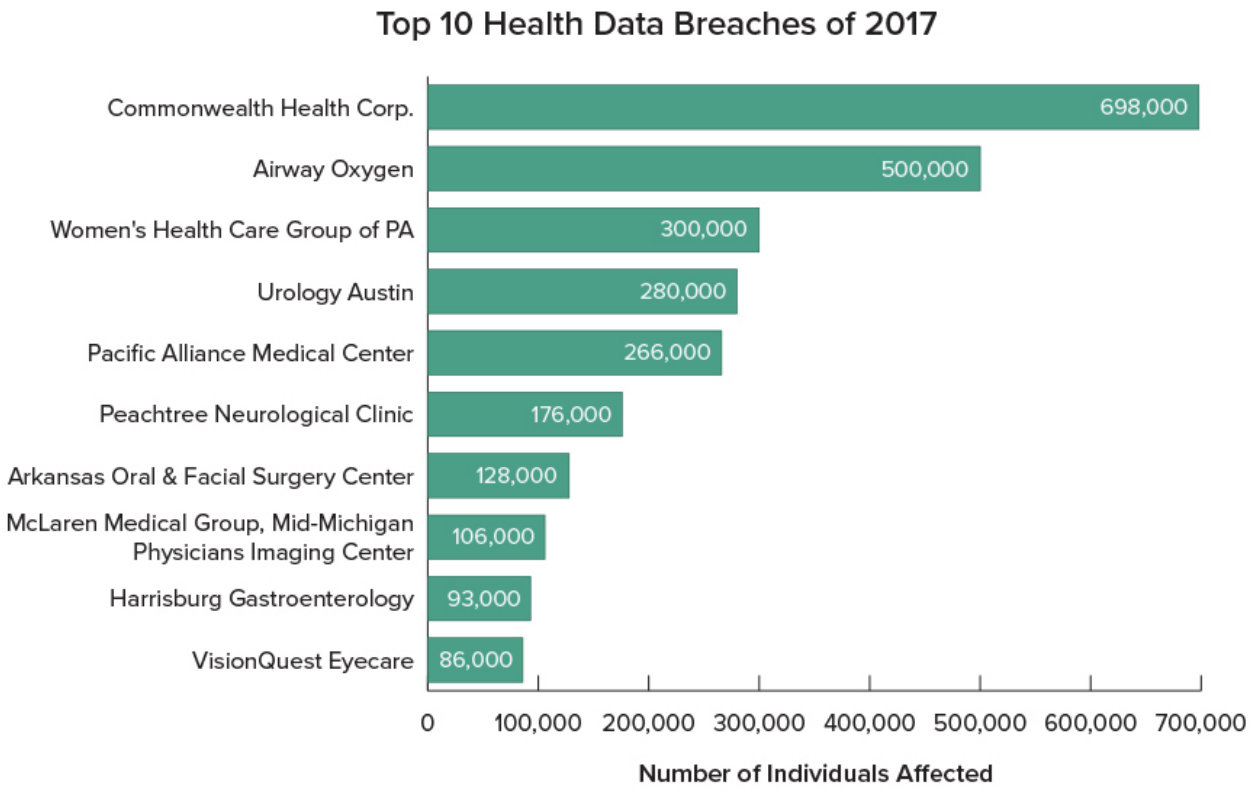
Firstly, the problem starts when the trust laid up on the CSP leads to record tempering and the undesirable disclosure of personal information to the admin. This trust factor is also a risk for Privacy and confidentiality since the medical record is an information that is sensitive and personal to the patients. This involves all kinds of risks from identity control to data tempering.

Secondly, the interactions with PHI or EPHI which are medical records requires the CSP to ensure the privacy of the data which is done by using various encryption schemes. This seems to be solving the privacy issues by not storing the data in its original form and keeping the encryption key away from the admin but various cases of the key leakage, which ultimately lead to privacy breach, have been marked in history.

This problem led us to think about designing a system which makes the use of a trustless mechanism and cryptography to solve the above-mentioned problems. This is done by calculating the hash of the records and storing it on the blockchain which a tamper proof is means of storing records. So that the trust factor is removed, and privacy is ensured.

2. Literature Review

The sharing of health data is being done by manual means which makes the process to be slow and hectic in nature. Such situations require the formation of Trust entities for dedicated purposes. In Pakistan, no existence of such system which can be used for both dedicated and general purposes have been reported till now. The systems which exist so far do not, in any way, involve the consent of Patient to be involved. Also, the software systems, from time to time, have been victimized by malicious attackers leading to privacy breaches. The following picture shows some facts and figures about the breaches:



Some systems for the same purpose exist but they are under development and do not provide services in this region. One such system is MedChain which is providing the services on the same lines but the range of services they are providing is very vast. Also, they involve a payment and service usage mechanism which involves cryptocurrencies which is not a legal tender in Pakistan.

3.Project Vision

The vision behind SecureMed is to provide a secure platform for interoperability between organizations, where every chunk of health information being shared involves the consent of the relevant patient and guarantees the privacy at the same time.

3.1 Problem Statement

The main problem that we are targeting is Document Forgery. Forgery is the action of forging a copy or imitation of a document, signature, banknote, or work of art. There a few types of forgery and some of them are deeds, checks, patents, prescriptions etc.

Simply falsifying a letter or document does not constitute forgery unless the person does so in attempt to defraud a person or entity. For example, if you were to receive a check for a car you sold, and the check was forged, you would not be held criminally liable unless you knew that the check had been falsified. If you knew that the check was forged, this constitutes fraud in many states.

Modern identity documents consist of a magnetic stripe on their back. These strips undergo scanning for verification purposes. Ultraviolet light is also used to view the images printed on the identification card. These images are only visible under ultraviolet light.

Forging Medical Records:

Patient records are legal documents, and the courts do not respond favorably to accusations that they have been falsified or tampered with. "Doctored" data can throw into doubt the basis of a diagnosis, the treatment plan and communications with the patient, which in turn can have serious implications for the quality of patient care. Altering a medical record can lead to a world of trouble for the medical practitioner, even if the alteration just clarifies what occurred trouble for the medical practitioner, even if the alteration just clarifies what occurred.

3.2 Business Opportunity

Every Third-Party Organization, which requires the validation of health claims, has its own business process for that purpose. There lies a communication gap between these organizations and the Health Centers, SecureMed aims to bridge the gap by providing a communication channel which is private essentially.

This application in Healthcare domain covers a huge target market and can become a lucrative opportunity by becoming the first mover in the market.

3.3 Objectives

We intend:

- To ease the already existing procedure of document authentication
- To secure the patient's medical records
- To put an end to document forging
- To reduce load management

3.4 Project Scope

Stakeholders: Health Centre, Patient, Third Party Organization (e.g. visa office)
Requirements: Defining of Roles, Representation of Assets, Defining of Participants, Defining of the Rights and Privileges of each Participants, Defining of Contracts and interactions between Participants
Scope: Corporate Usage, Health Centers
Process: Third Party Organization (TPO) wants a verified document of the health status of its client and for that it asks him to visit the relevant Health Centre and request for the verification by digitally signing the document. After the hospital goes through the Verification Process, the Document's hash is available on the Blockchain, and now the TPO is able to authenticate the concerned document instantly.

3.5 Constraints

- Health Centers working on manual systems
- Documents in Hard form

3.6 Stakeholders Description

3.6.1. Stakeholders Summary

The stakeholders of SecureMed are as follows:

- Admin
- Hospital Registrar
- Hospital Manager
- Patient
- Third Party officer
- Third Party registrar
- Receptionist
- Doctor

3.6.2. Key High-Level Goals and Problems of Stakeholders

Stakeholder	**Goal**	**Problems**
Admin	Registration of Organizations, Owners and Registrars.	Excessive Right and Privileges.
Hospital Registrar	Registration of doctors, receptionist	None
Third Party Officer	Cross-checking of medical documents	Health Claim Authentication
Patient	Request generation for document, Authentication of requested document	Complicated and Long Processes
Third Party Registrar	Registration of visa officers	None
Receptionist	Tackling a document request from a patient	Complicated and Long Processes
Doctor	Authentication of requested document	None
Hospital Manager	Tracking of document request	Complicated and Long Processes

4. Software Requirement Specifications

4.1. List of Features

Following are the features that cover the whole project of SecureMed:

- Document Request Handling
- Blockchain Transaction Handling
- Membership Service Provision
- Web Application
- Byzantine Fault Tolerant System
- Guaranteed Privacy in case of System Breach

4.2. Functional Requirements

- Register Patients, Health Centers, Third Party Organizations and the relevant staff.
- Allow Patients to submit a Request for Document.
- Allow Receptionists to handle the Request.
- Enable Doctor to authenticate the Document.
- Enable Patient to share the Document with multiple Third-Party Organizations
- Allow Third Party Participant to check the accuracy of the Document.

4.3. Quality Attributes

Attribute	**Description**
Usability	The system will provide a consistent User Interface for user to learn the system easily and in a satisfying manner
Performance	The system has a high throughput in terms of Transaction Processing. However, the Document Request Completion will significantly depend on the availability and responsiveness of the external actors involved in the process

Reliability	The chances of failure should be significantly low.
Security	The system will provide security against unauthorized access.
Availability	The underlying architecture should be available for access all the time.
Fault Tolerance	The system will be Byzantine Fault Tolerant in nature.
Scalability	The system will be easy to scale horizontally.

4.4. Non-Functional Requirements

- The application will be connected to the internet when in use.
- The patients will be required to visit the easily accessible Health Centre for the purpose Identity vetting.
- The application may optionally be able to maintain the log of activities
- The Patient will be required to have a personal copy of the health record in soft from.
- The Third-Party Officer will be required to have a copy of the health record in soft form.
- The Patient will be required to provide an identical copy of his health record in soft form to the Third-Party Officer.

5. High level Use cases

Use case	Register Organization
Actors	Admin
Type	Primary
Description	The Admin collects the information of the organization and registers the organization in the system of records.

Use case	Register Owner
Actors	Admin
Type	Primary
Description	The Admin collects the information of the owners of the organization and registers the owners in the system of records.

Use case	Register Registrar
Actors	Admin
Type	Primary
Description	The Admin collects the information of the Registrar of the organization and registers the registrar in the system of records

Use case	Login
Actors	All
Type	Primary
Description	All actors of the system are required to authenticate their Id via Login before making any transaction.

Use case	Register User
Actors	Registrar
Type	Primary
Description	The Registrar is a Power User and registers other relevant users in the organization.

Use case	Track Request
Actors	Manager
Type	Primary
Description	The Manager tracks the status of any Document Request that is present in the system of records using MRN or any related information.

Use case	Register Patient
Actors	Patient, Receptionist
Type	Primary
Description	The Patient signs up in the system and visits the easily available Health Centre for the vetting of his identity. The receptionist vets his identity to complete Registration.

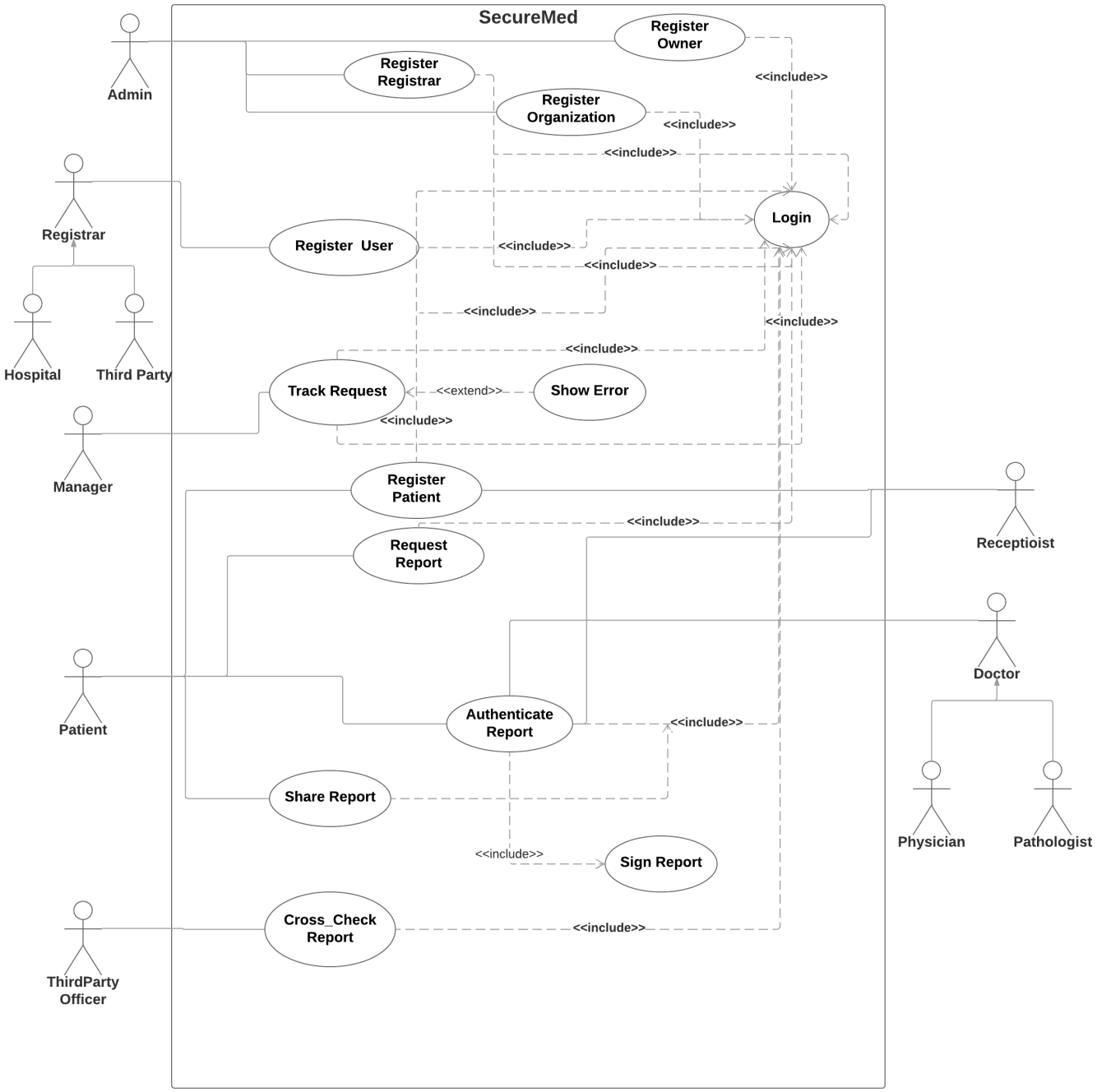
Use case	Request Report
Actors	Patient
Type	Primary
Description	The Patient makes a request to the relevant Health Centre for the report that is available at the Health Centre.

Use case	Authenticate Report
Actors	Patient
Type	Primary
Description	The patient authenticates the report and signs if he finds the information to be true.

Use case	Share Report
Actors	Patient
Type	Primary
Description	The patient shares the report with any of the third party available on the screen.

Use case	Cross-check Report
Actors	Third Party Officer
Type	Primary
Description	The Officer or the User working at the Third-Party Organization uploads the copy available to him and cross-checks the report against the records available to him.

5.1 Use case diagram:



6. Iteration Plan:

SecureMed has been divided into four iterations considering the nature of the work and familiarity with the tools. However, the plan can be subjected to change on meeting of certain conditions. The Four iterations are as follows:

1.Designing:
Iteration 1 is about the creation of the object-oriented designs and mapping them at the system level. At system level, it involves creating a design using CTO Modeling language of Hyperledger Composer.

2.Model Deployment:
Iteration 2 is about creation of the complete design independent of the Third-Party Organization and deployment of it on instance of Hyperledger Fabric.

3.Consensus:
Iteration 3 is about consensus on the issued document contents by the Patient, Doctor and the Receptionist.

4.Permissioned Sharing:
Iteration 4 is about sharing of the instance of consensus with the third present in the system which also makes creation of support for Third Party Organizations

7. Iteration 1:

Iteration 1 of SecureMed is majorly focused on the designing of the system which involves the development of the Object-oriented designs and Use cases. The iteration also involves the modeling of the business network on Hyperledger Composer which briefly includes the creation of participants and assets involved.

7.1. Expanded Use Cases:

UC01: Register Organization

Scope: SecureMed

Level: User Goal

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Organization registrar is registered

Main Success Scenario:

Actor Action	System Response
1. The admin of SecureMed logs into SecureMed	
	2. SecureMed opens the main page
3. The admin registers organization	
	4. SecureMed asks about the organization
5. The admin issues the certificate to the organization	
	6. The system identifies the organization

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be user friendly.

Technology and Data Variation List: Web page.

UC02: Register Owner

Scope: SecureMed

Level: Business requirement

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Owner of organization is registered

Main Success Scenario:

Actor Action	System Response
1. The admin of SecureMed logs into SecureMed	
	2. SecureMed opens the main page
3. The admin registers owner of the organization	
	4. SecureMed asks about the Owner
5. The admin enters owner's information	
	6. The system stores information in system of records

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be clear and user friendly.

Technology and Data Variation List: Web page.

UC03: Register Registrar

Scope: SecureMed

Level: Business requirement

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Default registrar of the organization is registered

Main Success Scenario:

Actor Action	System Response
1. The admin of SecureMed logs into SecureMed	
	2. SecureMed opens the main page
3. The admin registers default registrar of the organization	
	4. SecureMed asks about the registrar and the privileges
5. The admin enters the required information	
	6. The system maintains the record for the information

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be clear and user friendly.

Technology and Data Variation List: Web page

UC04: Issue Certificates

Scope: SecureMed

Level: Business requirement

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Default registrar of the organization is registered

Main Success Scenario:

Actor Action	System Response
1. The admin of SecureMed logs into SecureMed	
	2. SecureMed opens the main page
3. The admin asks system to issue the certificate to the relevant Registrar	
	4. SecureMed asks about the organization and the Registrar
5. The admin enters the required information	
	6. The system issues the certificate accordingly

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be clear and user friendly.

Technology and Data Variation List: Web page

UC05: Login

Scope: SecureMed Goal

Level: Security Goal

Primary Actor: Admin, Registrar, Manager, Patient, Third Party Officer, Receptionist, Doctor

Pre-Conditions: System must be on

Success Guarantee: Login to the system

Main Success Scenario:

Actor Action	System Response
1. The user opens the SecureMed	
	2. SecureMed show the main page having different roles
3. The user selects his role and enter	
	4. The system asks for the credentials.
5. The admin enters the required information	
	6. The system logs in

Extensions: May be the credentials entered by the user are not correct.

Special Requirements: Log in box should be clear and visible.

Technology and Data Variation List: Login Web Page

UC06: Register User

Scope: SecureMed

Level: Business requirement

Primary Actor: Registrar

Pre-Conditions: Registrar must login and registrar should be registered

Success Guarantee: Registrar registers defined users of the organization.

Main Success Scenario:

Actor Action	System Response
1. The registrar of organization logs into SecureMed	
	2. SecureMed opens the main page
3. The registrar selects register user option and select the user	
	4. System confirms the user
5. The registrar enters the required information of user.	
	6. The system stores the information of users and create a user account

Extensions: May be something not present on menu that registrar wants.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC07: Issue Certificate

Scope: SecureMed

Level: Business requirement

Primary Actor: Registrar

Pre-Conditions: Registrar must login and registrar should be registered

Success Guarantee: Registrar issues certificates to the registered users of the organization

Main Success Scenario:

Actor Action	System Response
1. The registrar of organization logs into SecureMed	
	2. SecureMed opens the main page
3. The registrar selects registered user option and select the user	
	4. System confirms the user
5. The registrar enters the required information of user.	
	6. The system issues the certificate to the requested user.

Extensions: May be some users don't have the privilege of certificate

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen.

Technology and Data Variation List: Web page

UC08: Track Request

Scope: SecureMed

Level: Business requirement

Primary Actor: Manager

Pre-Conditions: Manager must login

Success Guarantee: Manager of the organization can track the request of patient and other users as well

Main Success Scenario:

Actor Action	System Response
1. The Manager of organization logs into SecureMed	
	2. SecureMed opens the main page
3. The Manager opens the requests	
4. The Manager track the requested request	
	5. The system shows the information of the request

Extensions: May be some requests cannot be tracked.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC09: Register Patient

Scope: SecureMed

Level: Business requirement

Primary Actor: Patient, Receptionist

Pre-Conditions: Patient, Receptionist must login, Receptionist should be registered by the registrar.

Success Guarantee: Receptionist registers the patient.

Main Success Scenario:

Actor Action	System Response
1. The receptionist of organization logs into SecureMed	
	2. SecureMed opens the main page
3. The receptionist checks the request log of the patients.	
4. The receptionist confirms the request.	
	5. The system accepts the request and update the system of records.

Extensions: May be some patient cannot be registered due to some limitations

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC10: Request Report

Scope: SecureMed

Level: Business requirement

Primary Actor: Patient

Pre-Conditions: Patient must login and Patient should have been vetted by the receptionist of the hospital(organization)

Success Guarantee: Patient requests for medical report.

Main Success Scenario:

Actor Action	System Response
1. The patient logs into SecureMed	
	2. SecureMed opens the main page
3. The patient selects the report request option.	
	4. The system opens the MRN page
5. The patient enters his/her MRN	
	6. System send the MRN to the receptionist of the hospital

Extensions: MRN may not be exist.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC11: Authenticate Report

Scope: SecureMed

Level: Security Goal

Primary Actor: Patient

Pre-Conditions: Patient must login and receptionist should send the report to the patient for cross check

Success Guarantee: Patient signs the report sent by the receptionist.

Main Success Scenario:

Actor Action	System Response
1. The patient logs into SecureMed	
	2. SecureMed opens the main page
3. The patient checks the report by clicking requested reports	
	4. System shows the report
5. The patient confirms the report	
	6. The system sends the confirmation message and hash of the report to the receptionist.

Extensions: May be the report is not that, that was expected by the patient

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen.

Technology and Data Variation List: UML model may be produced

UC12: Share Report

Scope: SecureMed

Level: User Goal

Primary Actor: Patient

Pre-Conditions: Patient must login and Patient should be registered having some medical reports.

Success Guarantee: Patient shares the report with the third party (visa officer)

Main Success Scenario:

Actor Action	System Response
1. The patient logs into SecureMed	
	2. SecureMed opens the main page having third party list
3. The patient selects the desired party and enters	
	4. System confirms the third party
	5. The system accepts the request and update the system of records.

Extensions: May be some patients cannot share the report due to the privilege issues.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen. Up to 98% accuracy

Technology and Data Variation List: Web page

UC13: Cross-check Report

Scope: Security goal

Level: User Goal

Primary Actor: Third Party Officer

Pre-Conditions: Third Party Officer must login and Third-party officer should be registered

Success Guarantee: Third-party officer cross checks the shared medical document by the patient.

Main Success Scenario:

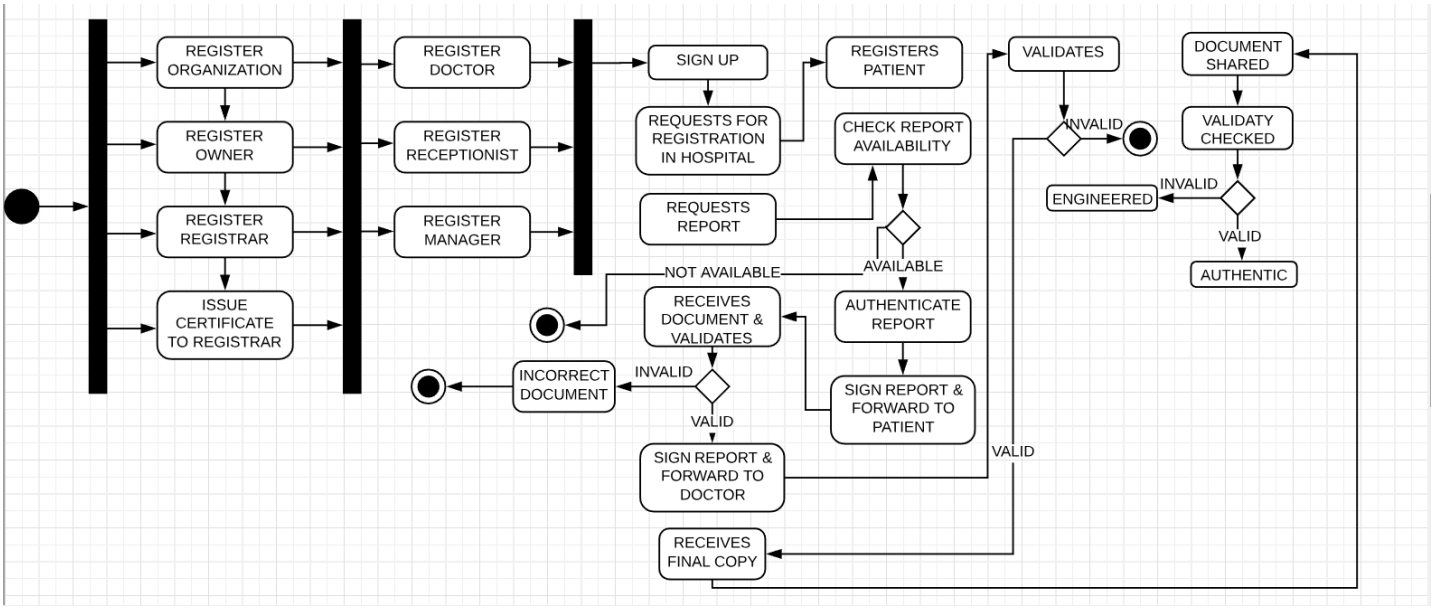
Actor Action	System Response
1. The officer logs into SecureMed	
	2. SecureMed opens the main page.
3. The officer checks the shared reports and select the desired one.	
	4. System opens the document
5. The officer hashes the document and check it on the ledger (Blockchain)	
	6. The system checks the report on the ledger and confirms the report

Extensions: Shared report may not be original or not on blockchain. So, can't be cross check by the visa officer.

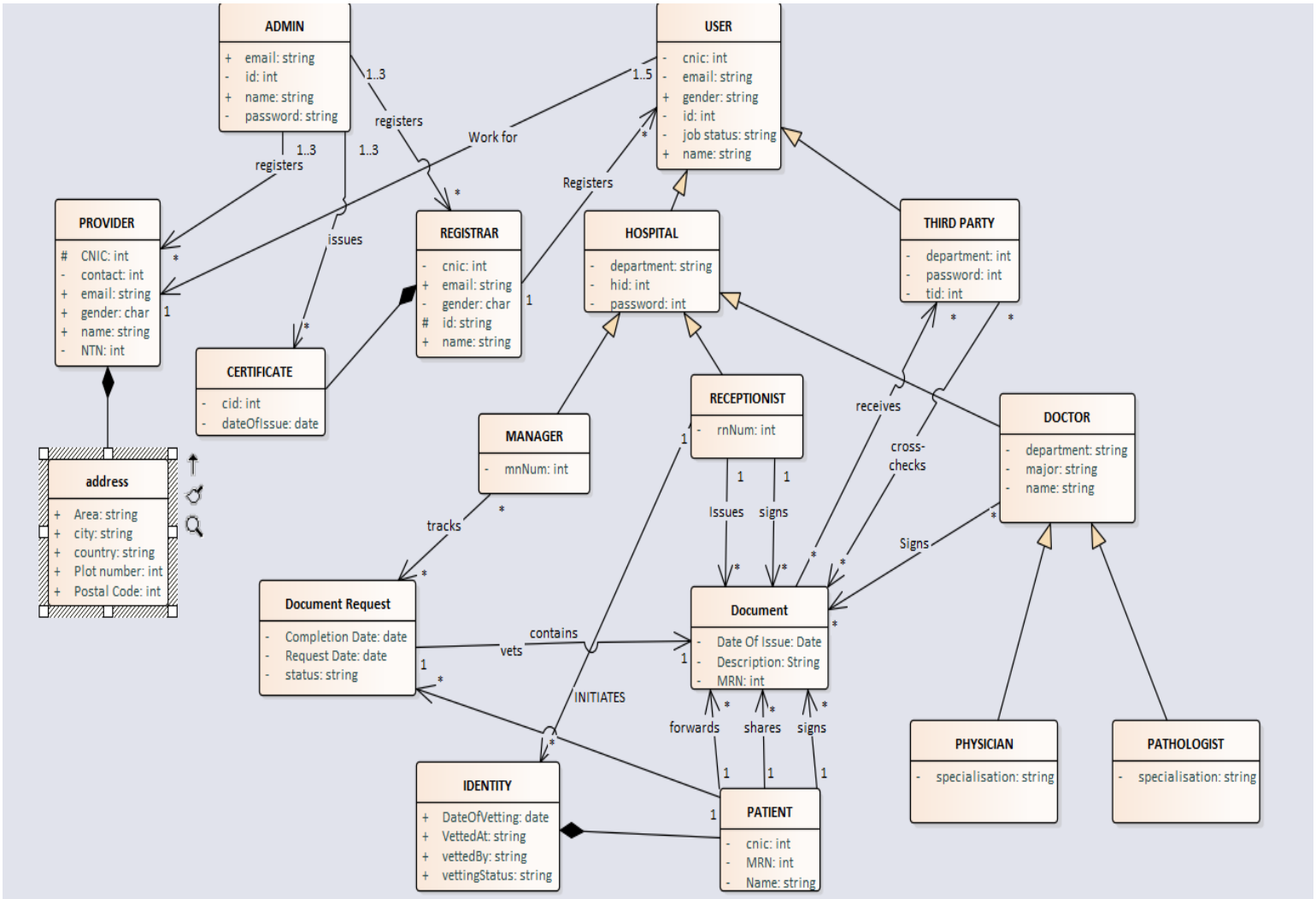
Special Requirements: Menu should be clear and user friendly. User should be defined on the screen. Up to 98% accuracy.

Technology and Data Variation List: Web page

7.2. Activity Diagram

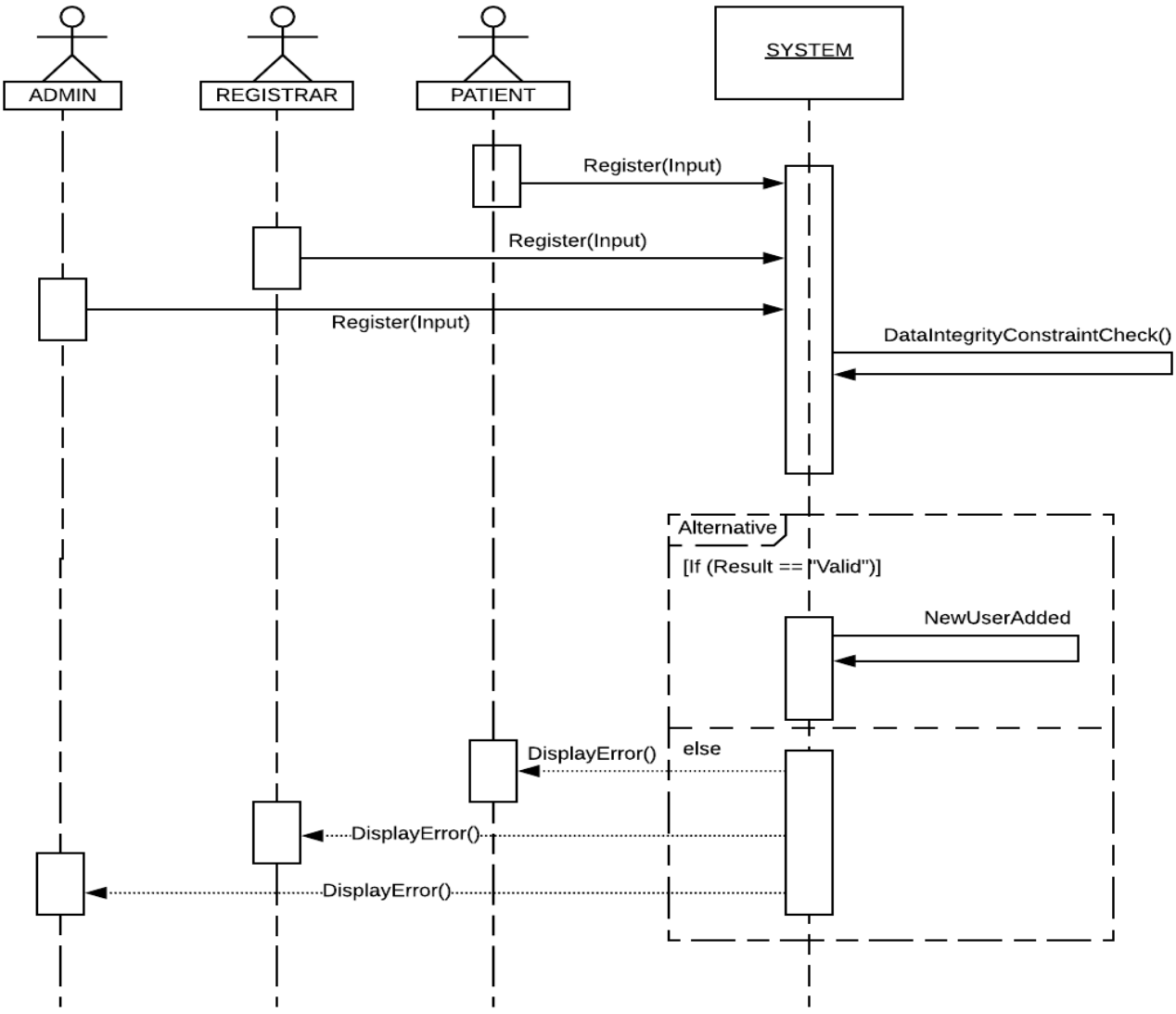


7.3. Domain Model

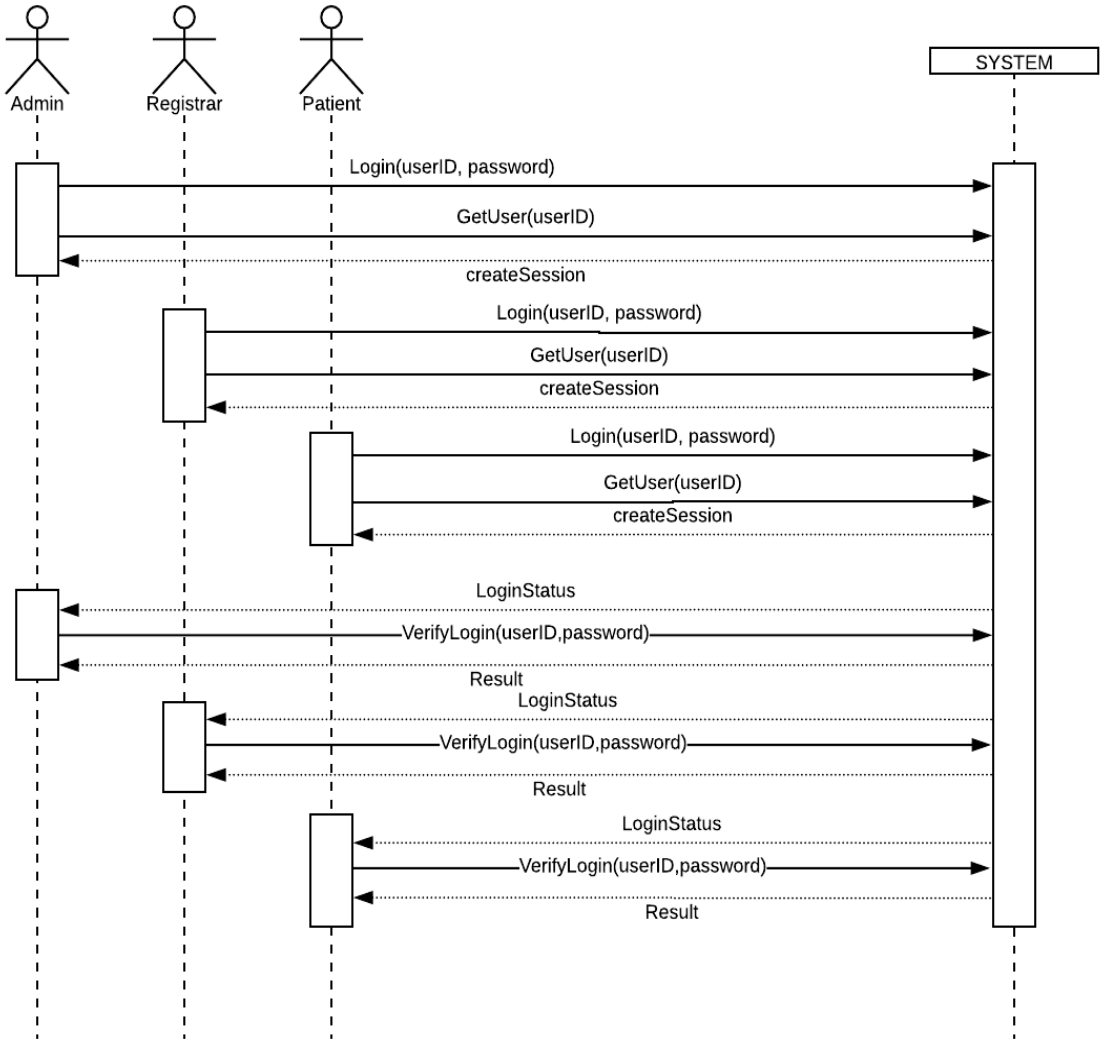


7.4. System Sequence Diagram

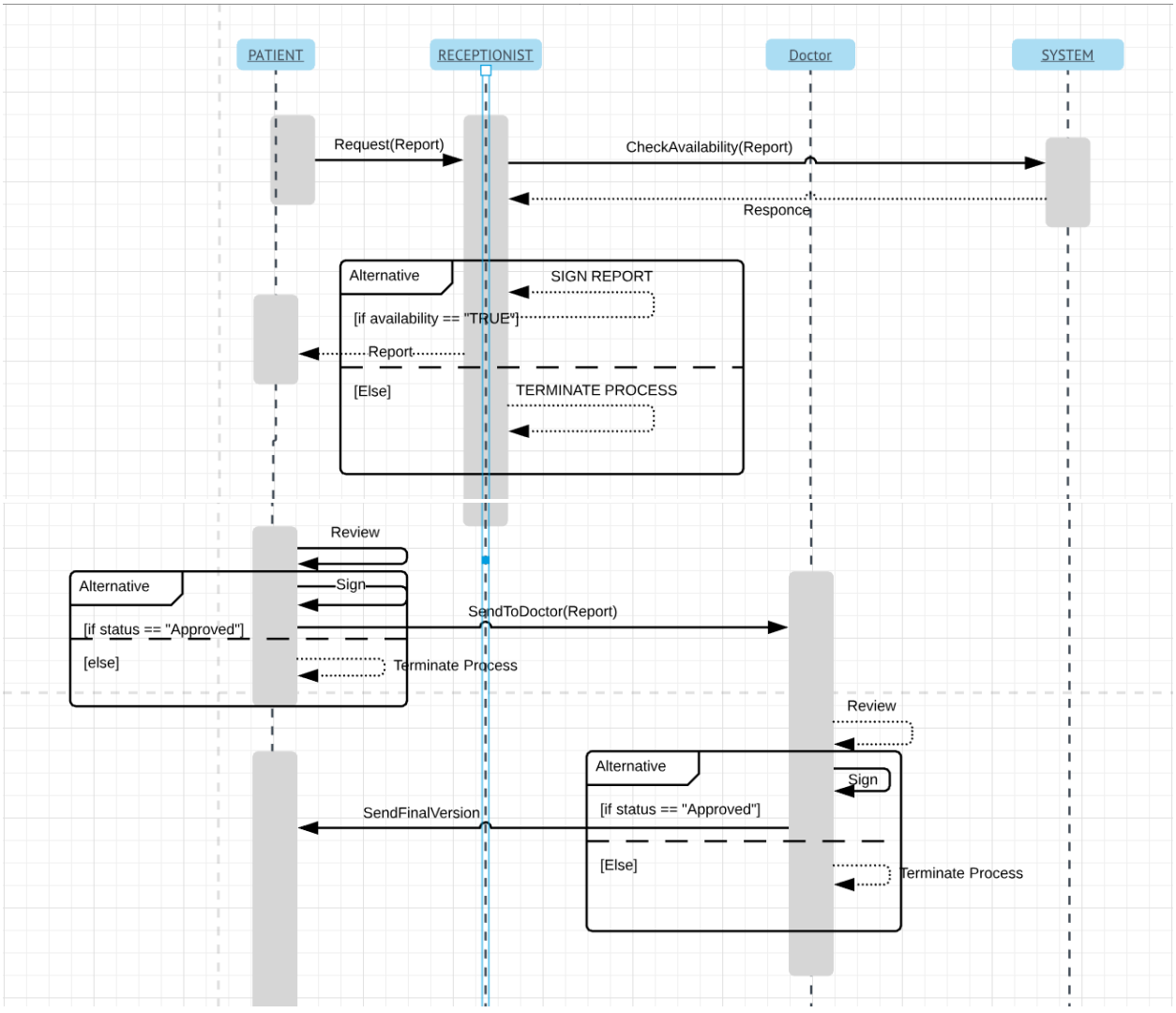
REGISTRATION:



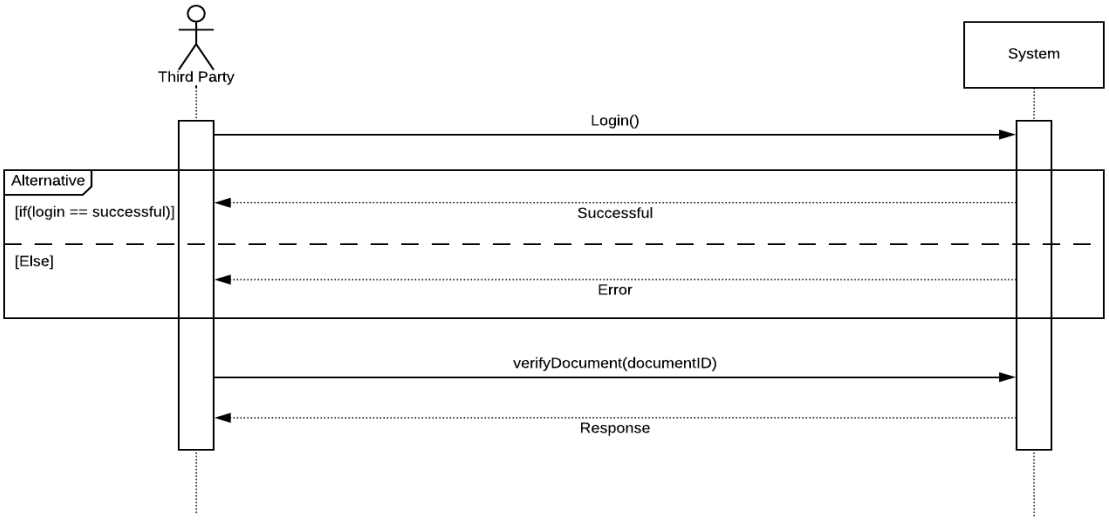
Login


Admin
Registrar
Patient
SYSTEM
Login(userID, password)
GetUser(userID)
createSession
Login(userID, password)
GetUser(userID)
createSession
Login(userID, password)
GetUser(userID)
createSession
LoginStatus
VerifyLogin(userID,password)
Result
LoginStatus
VerifyLogin(userID,password)
Result
LoginStatus
VerifyLogin(userID,password)
Result

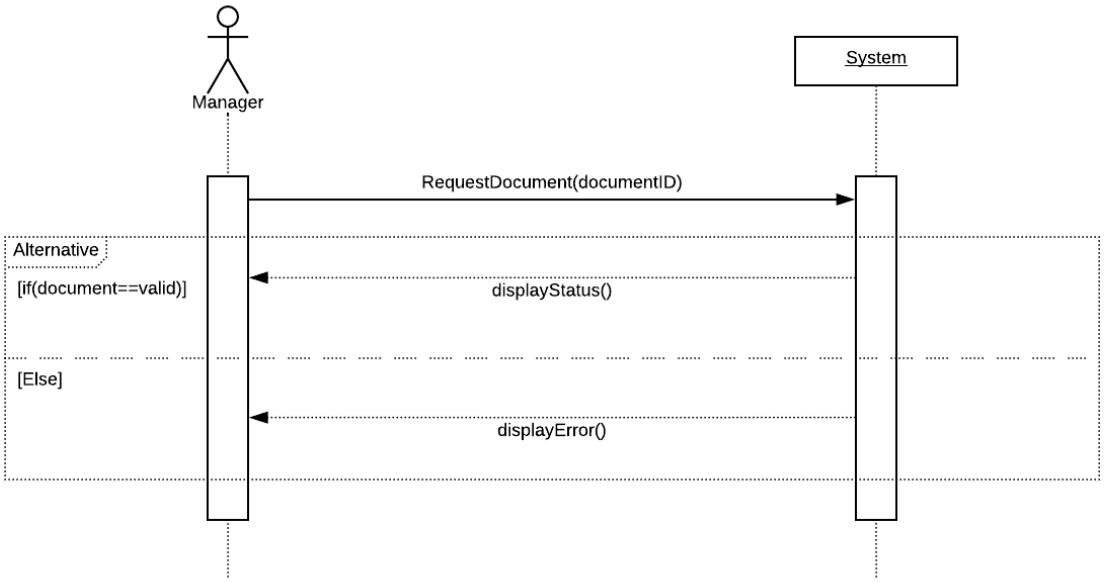
Authentication, signing, request & validity (patient, receptionist):



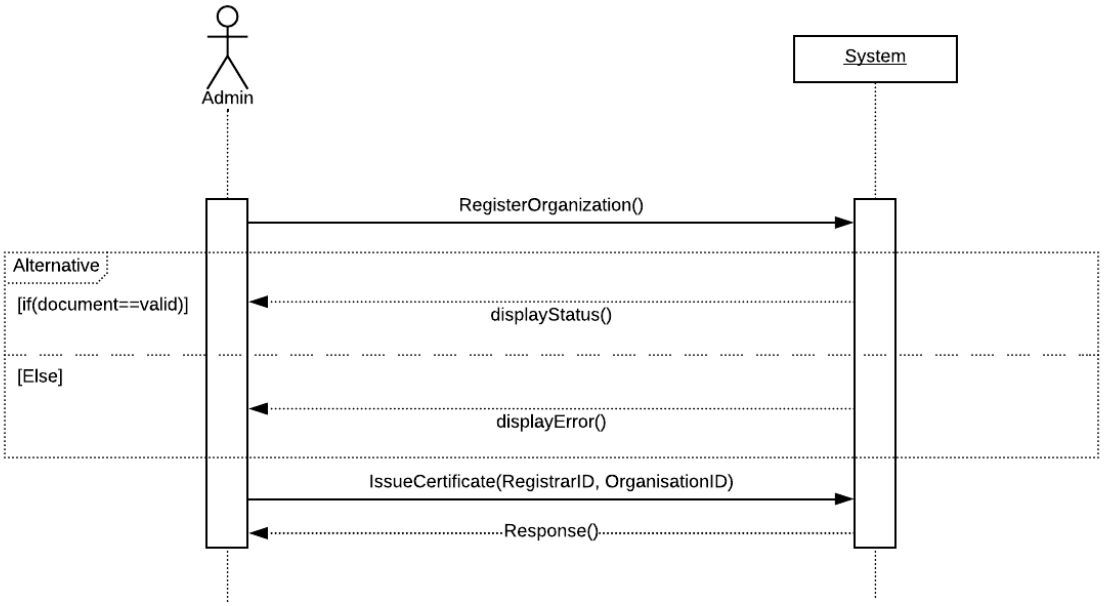
Third Party Authentication



CHECKING STATUS:



ISSUE CERTIFICATE:



7.5. Operation contracts

Name:	Register(input)
Responsibility:	Register users of the system
Type:	System.
Cross Reference:	Register User
Pre-Conditions:	User must be stakeholder of the system
Post-Conditions:	New instance was instantiated of user User. Status was updated by registrar or admin User was saved to the database

Name:	dataIntegrityConstraintCheck ()
Responsibility:	Check the credential of the user
Type:	System.
Cross Reference:	Register User
Pre-Conditions:	This is a registration process underway
Post-Conditions:	New instance was instantiated of user User. Status was updated by registrar or admin User was saved to the database

Name:	DisplayError()
Responsibility:	Customer places order.
Type:	System.
Cross Reference:	Register User, register organization, Register Owner
Pre-Conditions:	This is a registration process underway
Post-Conditions:	New instance was not instantiated of user User. Status was not updated by registrar or admin User was not saved to the database Error message was displayed

Name:	Login (UserID, password)
Responsibility:	User must be login in order to proceed further
Type:	System.
Cross Reference:	Every user
Pre-Conditions:	User must be registered
Post-Conditions:	A main page was opened

Name:	GetUser (UserID)
Responsibility:	Check the user status
Type:	System.
Cross Reference:	Track request
Pre-Conditions:	User must be registered
Post-Conditions:	New instance of user was instantiated of user User. Status was updated by registrar or admin UserID was got by the manager object

Name:	verifyLogin (UserID, password)
Responsibility:	System verify user
Type:	System.
Cross Reference:	Login
Pre-Conditions:	User must be registered. User ID must be present in the system
Post-Conditions:	New instance of user was instantiated of user User. Status was updated User was associated with the current scenario.

Name:	Request (Report)
Responsibility:	User wants to share the report with the officer of third party
Type:	System.
Cross Reference:	Cross-check Report
Pre-Conditions:	Officer and patient are the part of the system
Post-Conditions:	Patient instance was created Officer instance was created Patient was associated with the officer and receptionist

Name:	CheckAvailability(Report)
Responsibility:	User wants to share the report with the officer of third party
Type:	System.
Cross Reference:	Authentication + signing + request & validity(patient + receptionist):
Pre-Conditions:	Instance of report is instantiated. Patient have MRN
Post-Conditions:	A report was made by system Report was instantiated.

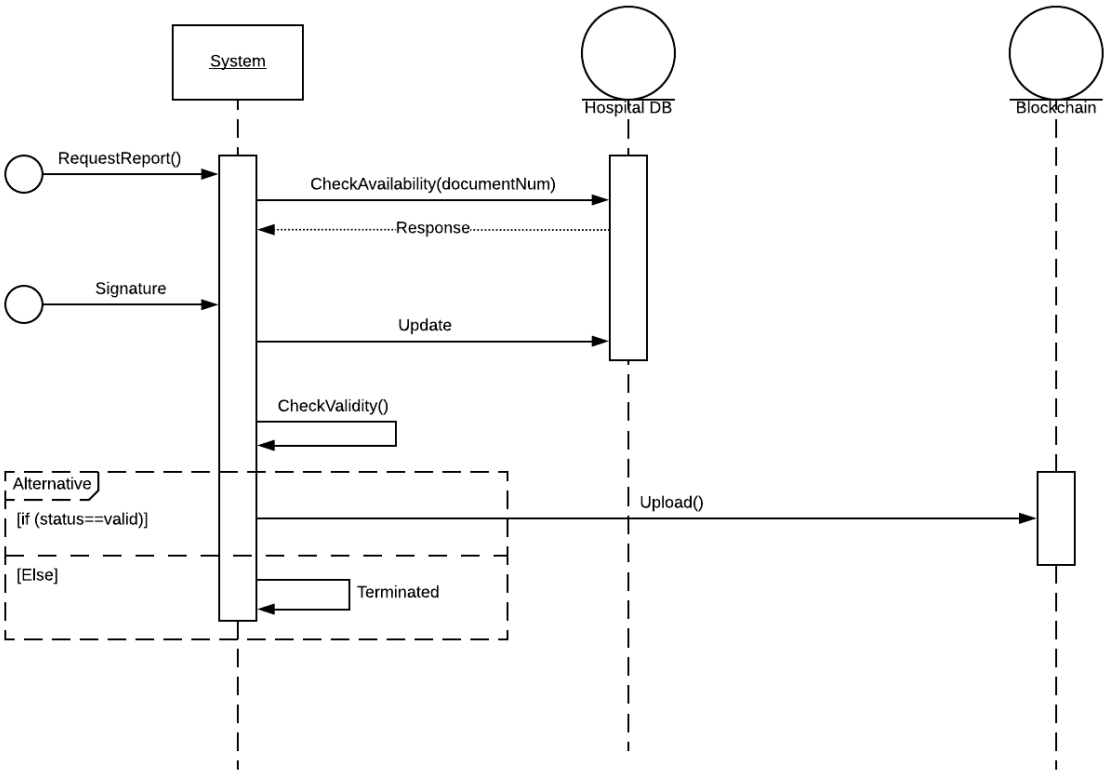
Name:	sentToDoctor(Report)
Responsibility:	Report send to the doctor
Type:	System.
Cross Reference:	Authentication + signing + request & validity(patient + receptionist):
Pre-Conditions:	New request made by the patient
Post-Conditions:	Instance of doctor was created Report instance was associated with the doctor.

Name:	verifyDocument(documentID)
Responsibility:	Third party authentication
Type:	System.
Cross Reference:	Third party authentication
Pre-Conditions:	Patient make a request
Post-Conditions:	Officer was instantiated. Officer was associated with the patient

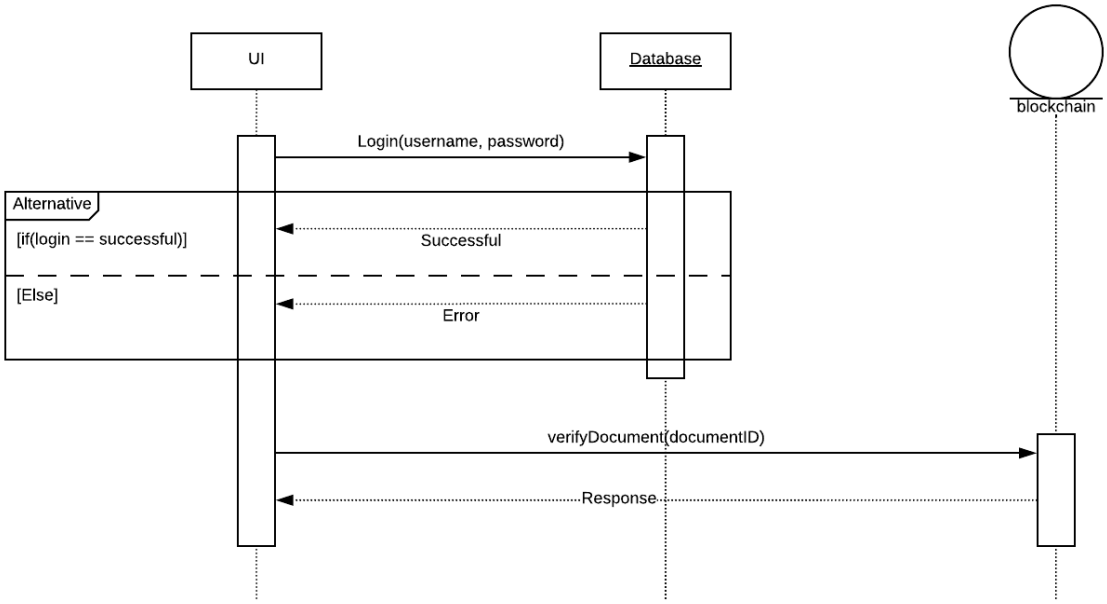
Name:	**IssueCertificate(registrarID, organizationID)**
Responsibility:	**Customer places order.**
Type:	**System.**
Cross Reference:	**Issue certificate**
Pre-Conditions:	**Organizations is registered**
Post-Conditions:	**Hospital was instantiated.** **Hospital was associated with the Admin of the system.** **Organization. Certificate was called**

7.6. Sequence Diagrams

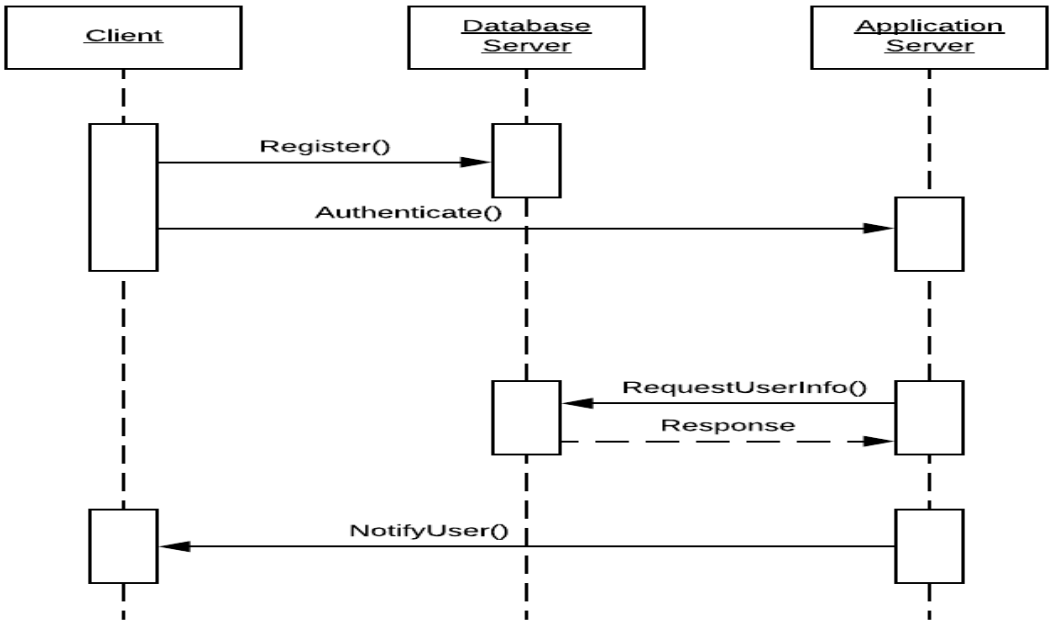
Authentication, signing, request & validity (patient, receptionist):



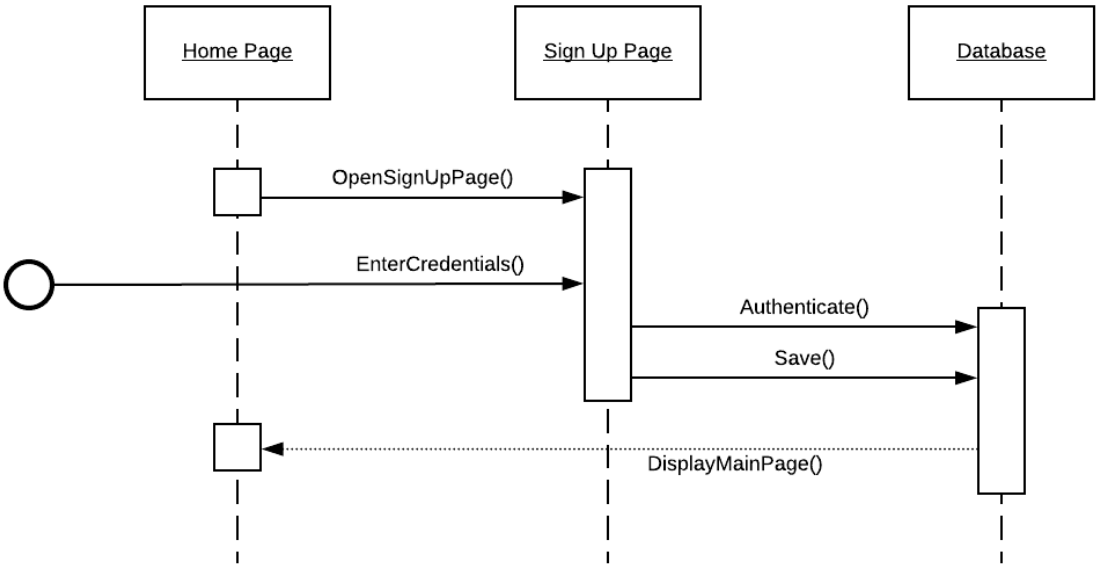
THIRD-PARTY VERIFICATION:



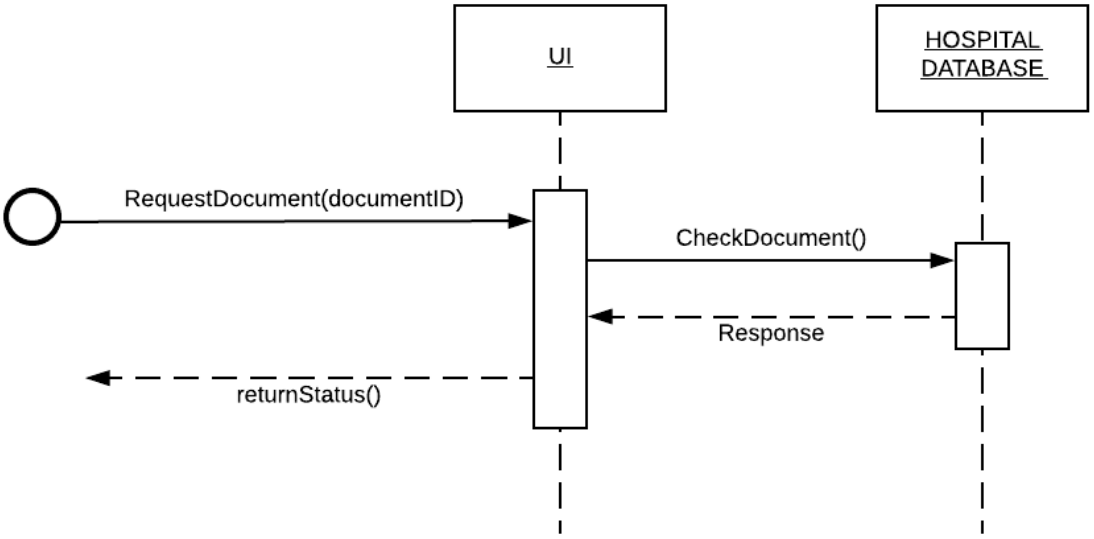
LOGIN:



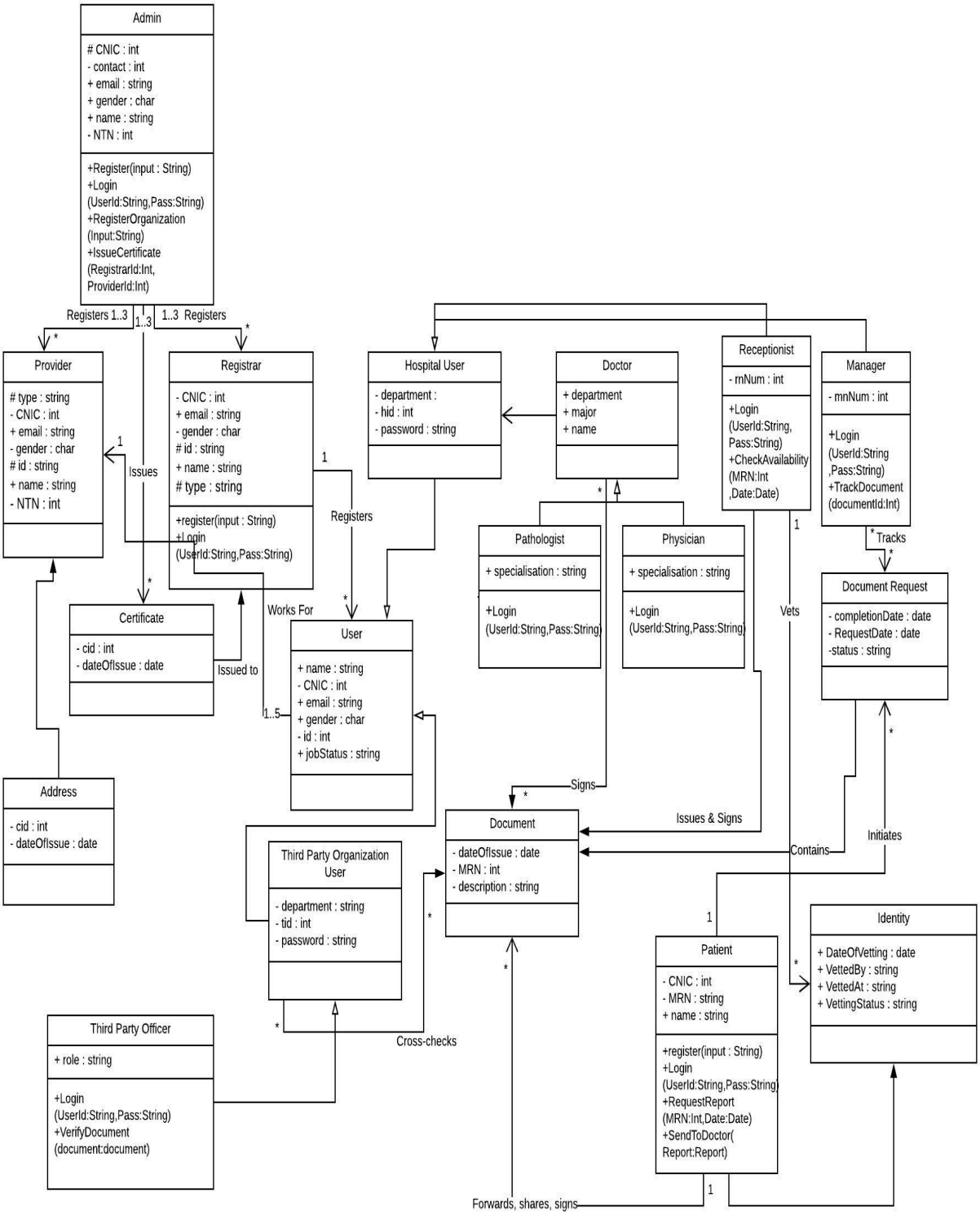
REGISTRATION:



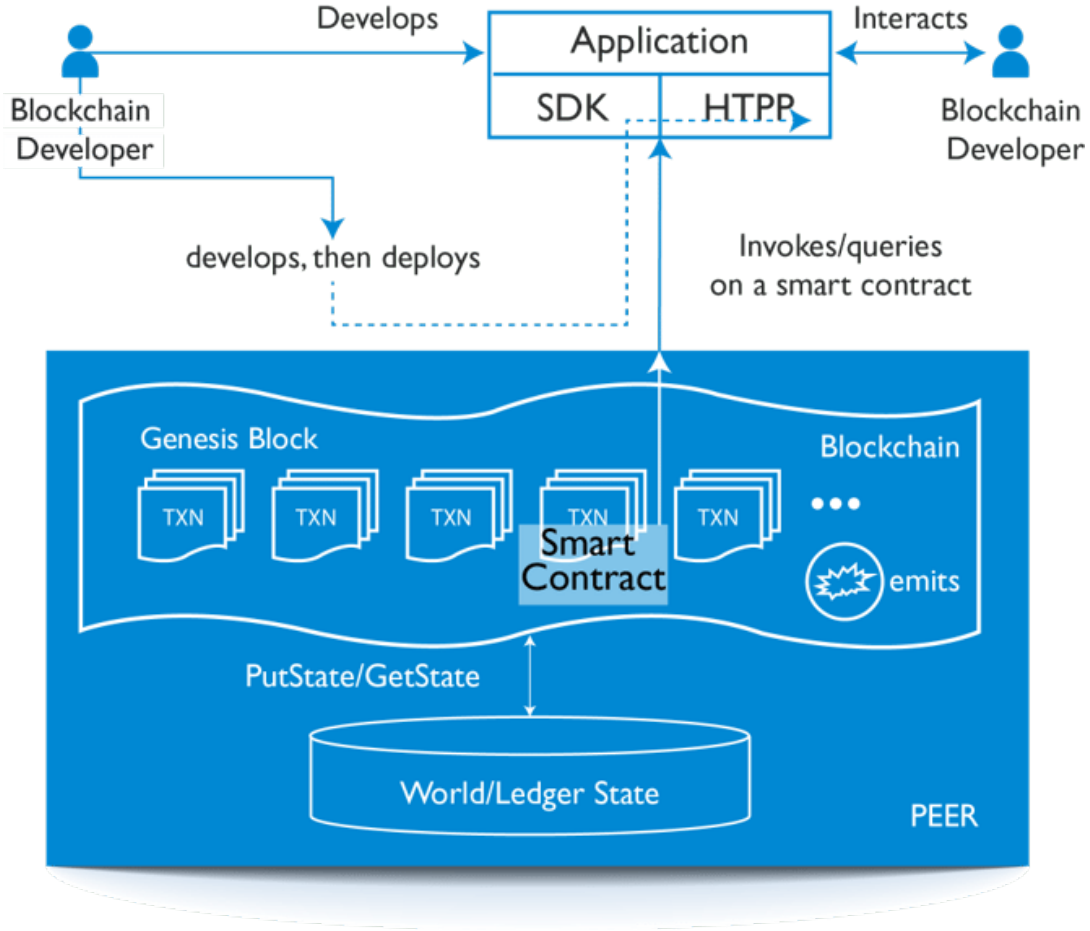
DOCUMENT TRACKING:

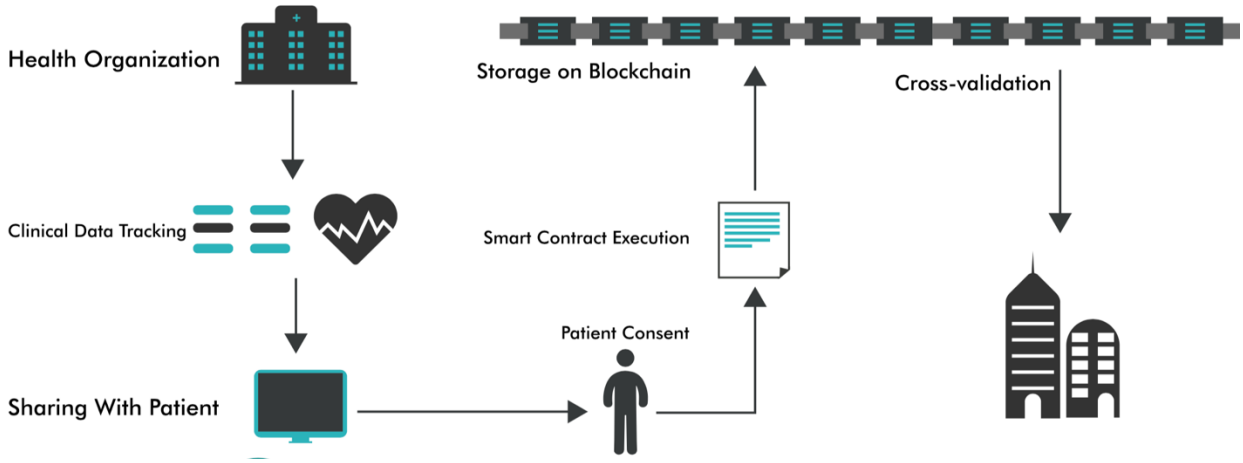


7.7. Class Diagram



7.8. Architecture Diagram





8. Iteration 2:

Iteration 2 of SecureMed is majorly focused on the creation of the complete design independent of the Third-Party Organization and deployment of it on instance of Hyperledger Fabric.

8.1. Expanded Use Cases:

UC01: Register Organization

Scope: SecureMed

Level: User Goal

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Organization registrar is registered

Main Success Scenario:

Actor Action	System Response
7. The admin of SecureMed logs into SecureMed	
	8. SecureMed opens the main page
9. The admin registers organization	
	10. SecureMed asks about the organization
11. The admin issues the certificate to the organization	
	12. The system identifies the organization

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be user friendly.

Technology and Data Variation List: Web page.

UC02: Register Owner

Scope: SecureMed

Level: Business requirement

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Owner of organization is registered

Main Success Scenario:

Actor Action	System Response
7. The admin of SecureMed logs into SecureMed	
	8. SecureMed opens the main page
9. The admin registers owner of the organization	
	10. SecureMed asks about the Owner
11. The admin enters owner's information	
	12. The system stores information in system of records

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be clear and user friendly.

Technology and Data Variation List: Web page.

UC03: Register Registrar

Scope: SecureMed

Level: Business requirement

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Default registrar of the organization is registered

Main Success Scenario:

Actor Action	System Response
7. The admin of SecureMed logs into SecureMed	
	8. SecureMed opens the main page
9. The admin registers default registrar of the organization	
	10. SecureMed asks about the registrar and the privileges
11. The admin enters the required information	
	12. The system maintains the record for the information

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be clear and user friendly.

Technology and Data Variation List: Web page

UC04: Login

Scope: SecureMed Goal

Level: Security Goal

Primary Actor: Admin, Registrar, Manager, Patient, Third Party Officer, Receptionist, Doctor

Pre-Conditions: System must be on

Success Guarantee: Login to the system

Main Success Scenario:

Actor Action	System Response
7. The user opens the SecureMed	
	8. SecureMed show the main page having different roles
9. The user selects his role and enter	
	10. The system asks for the credentials.
11. The admin enters the required information	
	12. The system logs in

Extensions: May be the credentials entered by the user are not correct.

Special Requirements: Log in box should be clear and visible.

Technology and Data Variation List: Login Web Page

UC05: Register User

Scope: SecureMed

Level: Business requirement

Primary Actor: Registrar

Pre-Conditions: Registrar must login and registrar should be registered

Success Guarantee: Registrar registers defined users of the organization.

Main Success Scenario:

Actor Action	System Response
7. The registrar of organization logs into SecureMed	
	8. SecureMed opens the main page
9. The registrar selects register user option and select the user	
	10. System confirms the user
11. The registrar enters the required information of user.	
	12. The system stores the information of users and create a user account

Extensions: May be something not present on menu that registrar wants.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC06: Issue Certificate

Scope: SecureMed

Level: Business requirement

Primary Actor: Registrar

Pre-Conditions: Registrar must login and registrar should be registered

Success Guarantee: Registrar issues certificates to the registered users of the organization

Main Success Scenario:

Actor Action	System Response
7. The registrar of organization logs into SecureMed	
	8. SecureMed opens the main page
9. The registrar selects registered user option and select the user	
	10. System confirms the user
11. The registrar enters the required information of user.	
	12. The system issues the certificate to the requested user.

Extensions: May be some users don't have the privilege of certificate

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen.

Technology and Data Variation List: Web page

UC07: Track Request

Scope: SecureMed

Level: Business requirement

Primary Actor: Manager

Pre-Conditions: Manager must login

Success Guarantee: Manager of the organization can track the request of patient and other users as well

Main Success Scenario:

Actor Action	System Response
6. The Manager of organization logs into SecureMed	
	7. SecureMed opens the main page
8. The Manager opens the requests	
9. The Manager track the requested request	
	10. The system shows the information of the request

Extensions: May be some requests cannot be tracked.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC08: Register Patient

Scope: SecureMed

Level: Business requirement

Primary Actor: Patient, Receptionist

Pre-Conditions: Patient, Receptionist must login, Receptionist should be registered by the registrar.

Success Guarantee: Receptionist registers the patient.

Main Success Scenario:

Actor Action	System Response
6. The receptionist of organization logs into SecureMed	
	7. SecureMed opens the main page
8. The receptionist checks the request log of the patients.	
9. The receptionist confirms the request.	
	10. The system accepts the request and update the system of records.

Extensions: May be some patient cannot be registered due to some limitations

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC9: Request Report

Scope: SecureMed

Level: Business requirement

Primary Actor: Patient

Pre-Conditions: Patient must login and Patient should have been vetted by the receptionist of the hospital(organization)

Success Guarantee: Patient requests for medical report.

Main Success Scenario:

Actor Action	System Response
7. The patient logs into SecureMed	
	8. SecureMed opens the main page
9. The patient selects the report request option.	
	10. The system opens the MRN page
11. The patient enters his/her MRN	
	12. System send the MRN to the receptionist of the hospital

Extensions: MRN may not be exist.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC10: Authenticate Report

Scope: SecureMed

Level: Security Goal

Primary Actor: Patient

Pre-Conditions: Patient must login and receptionist should send the report to the patient for cross check

Success Guarantee: Patient signs the report sent by the receptionist.

Main Success Scenario:

Actor Action	System Response
7. The patient logs into SecureMed	
	8. SecureMed opens the main page
9. The patient checks the report by clicking requested reports	
	10. System shows the report
11. The patient confirms the report	
	12. The system sends the confirmation message and hash of the report to the receptionist.

Extensions: May be the report is not that, that was expected by the patient

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen.

Technology and Data Variation List: UML model may be produced

UC11: Share Report

Scope: SecureMed

Level: User Goal

Primary Actor: Patient

Pre-Conditions: Patient must login and Patient should be registered having some medical reports.

Success Guarantee: Patient shares the report with the third party (visa officer)

Main Success Scenario:

Actor Action	System Response
6. The patient logs into SecureMed	
	7. SecureMed opens the main page having third party list
8. The patient selects the desired party and enters	
	9. System confirms the third party
	10. The system accepts the request and update the system of records.

Extensions: May be some patients cannot share the report due to the privilege issues.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen. Up to 98% accuracy

Technology and Data Variation List: Web page

UC12: Cross-check Report

Scope: Security goal

Level: User Goal

Primary Actor: Third Party Officer

Pre-Conditions: Third Party Officer must login and Third-party officer should be registered

Success Guarantee: Third-party officer cross checks the shared medical document by the patient.

Main Success Scenario:

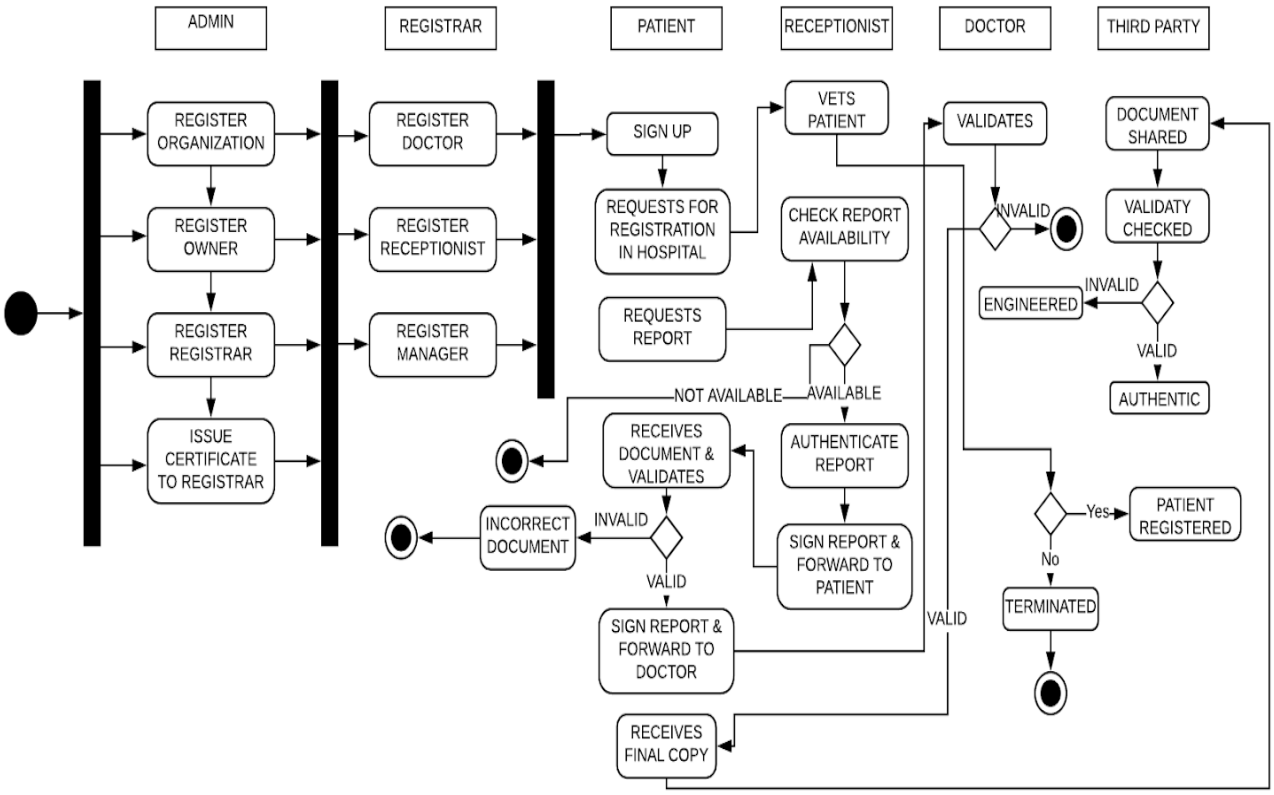
Actor Action	System Response
7. The officer logs into SecureMed	
	8. SecureMed opens the main page.
9. The officer checks the shared reports and select the desired one.	
	10. System opens the document
11. The officer hashes the document and check it on the ledger (Blockchain)	
	12. The system checks the report on the ledger and confirms the report

Extensions: Shared report may not be original or not on blockchain. So, can't be cross check by the visa officer.

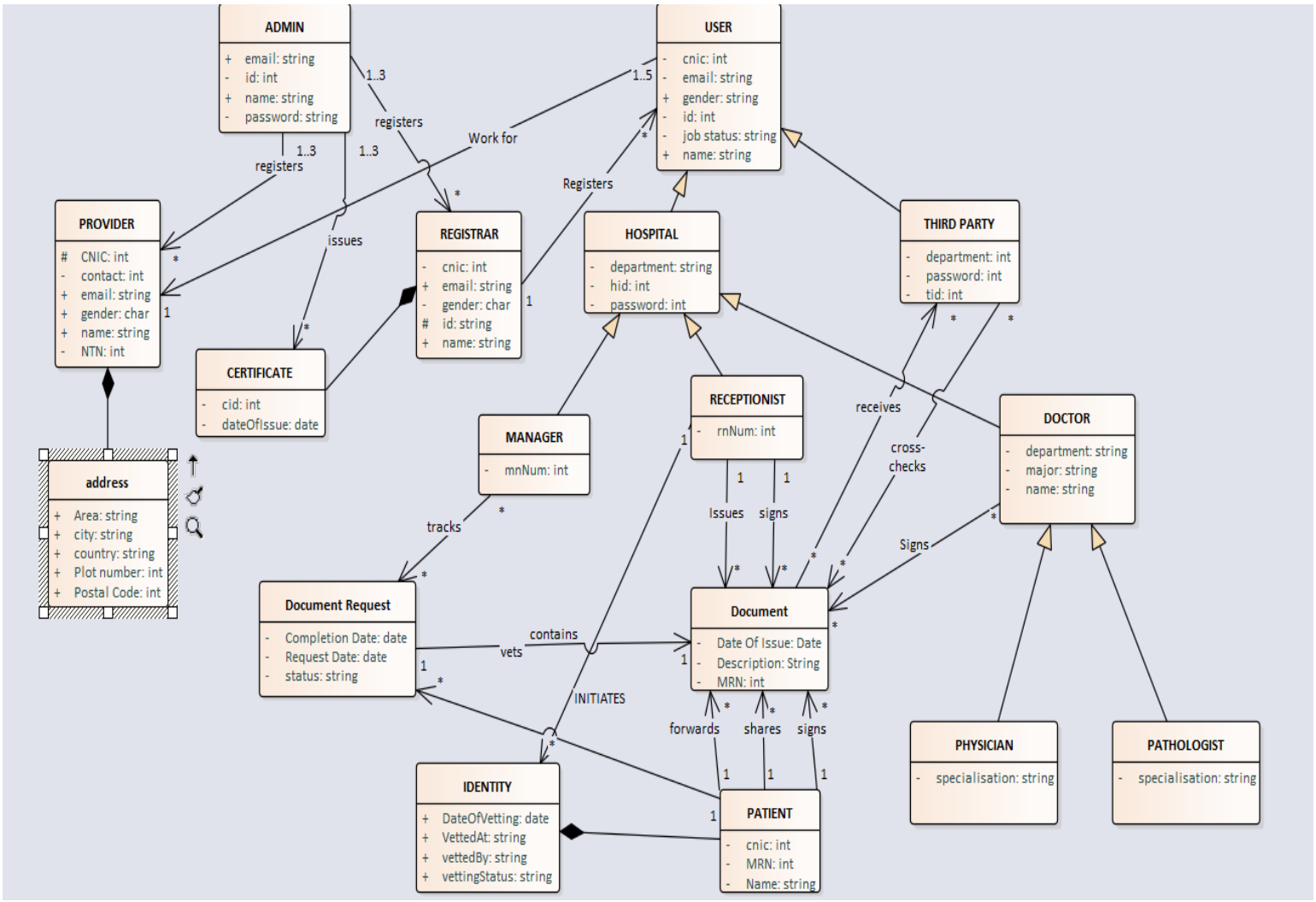
Special Requirements: Menu should be clear and user friendly. User should be defined on the screen. Up to 98% accuracy.

Technology and Data Variation List: Web page

8.2. Activity Diagram

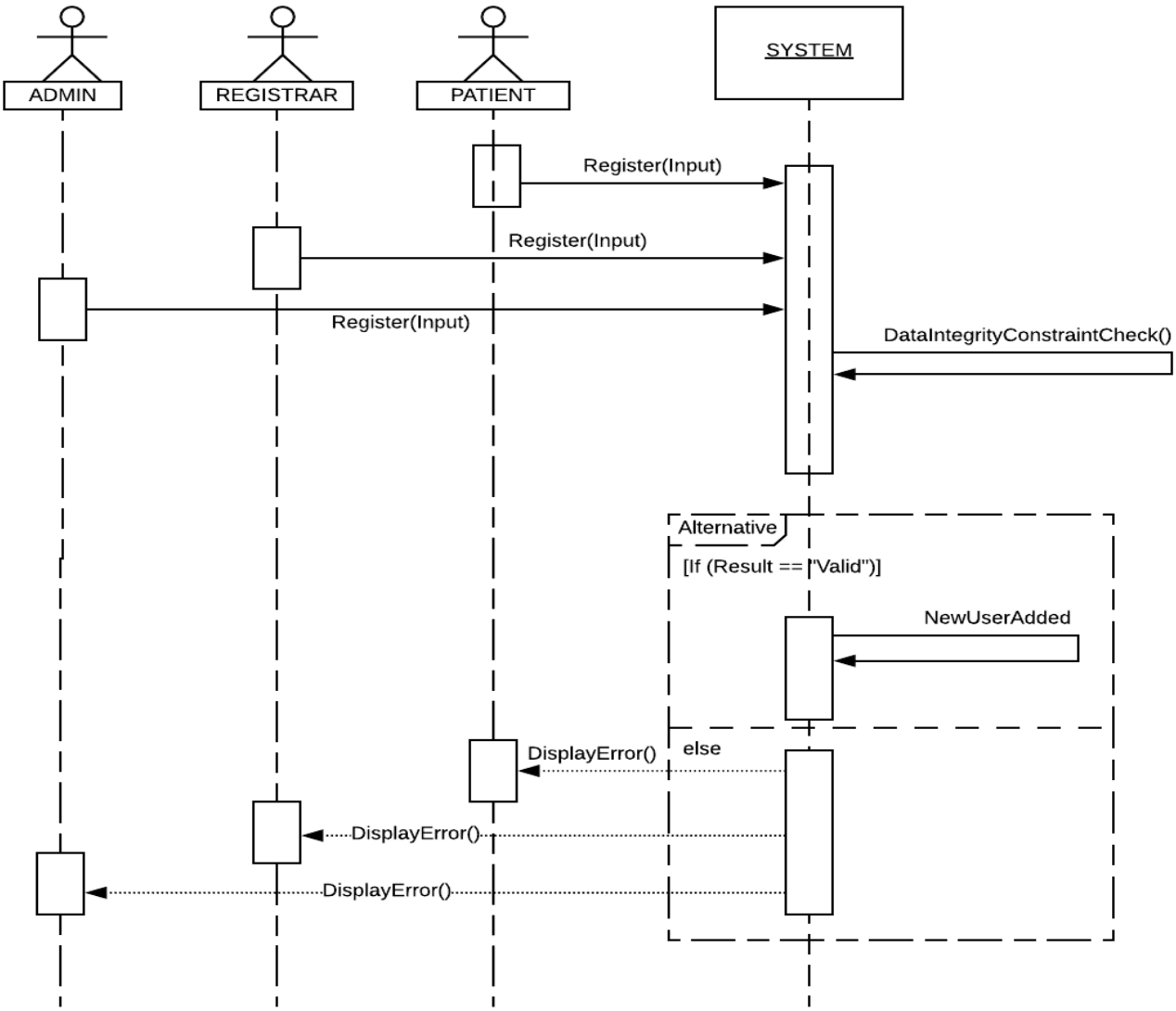


8.3. Domain Model

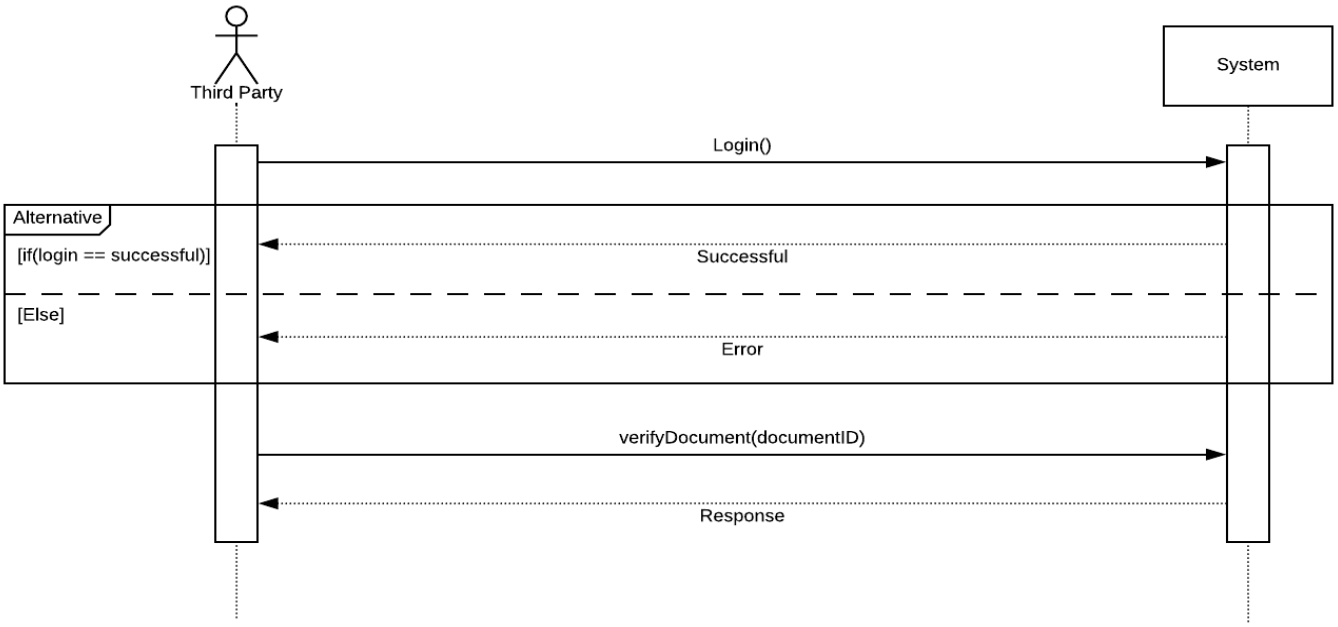


8.4. System Sequence Diagram

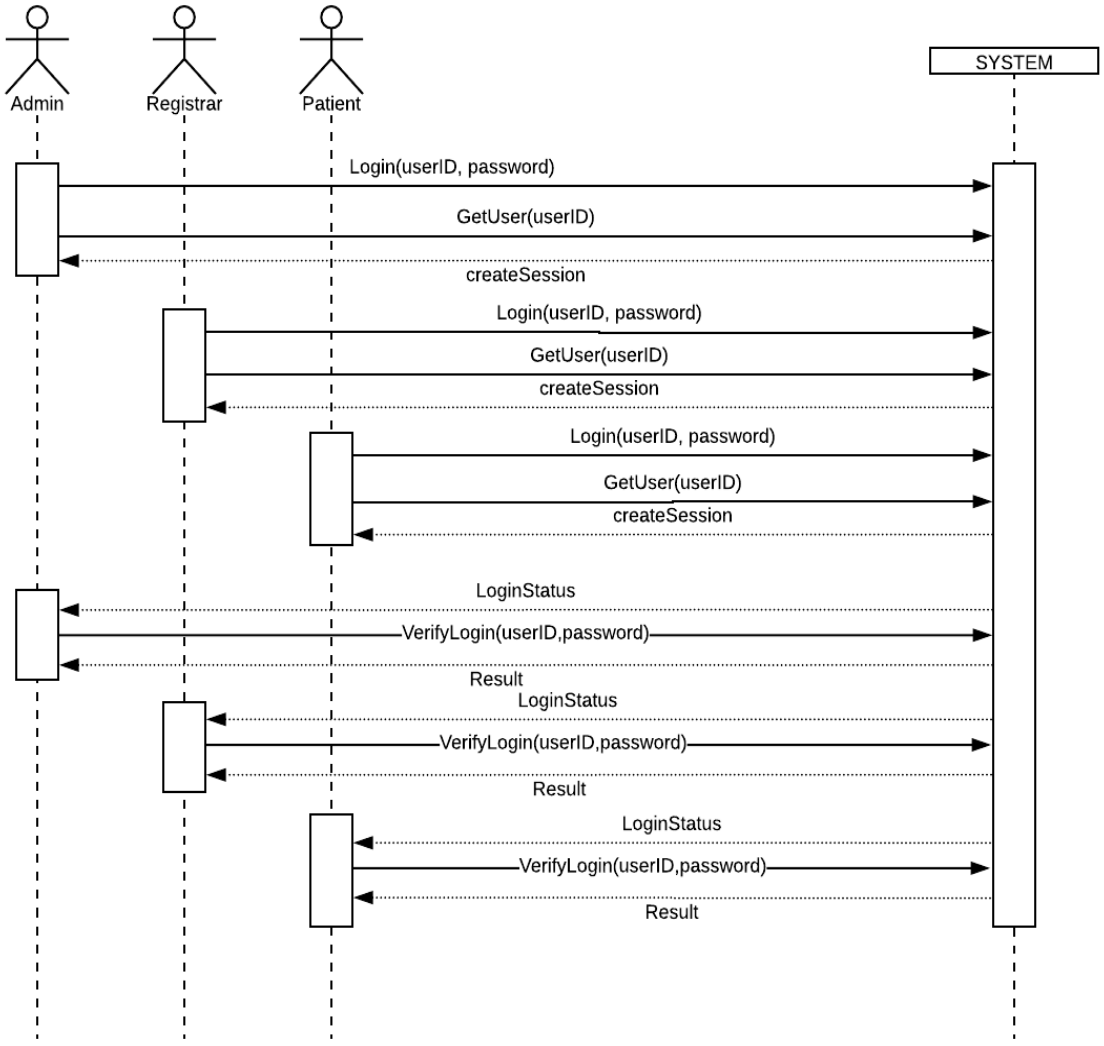
REGISTRATION:



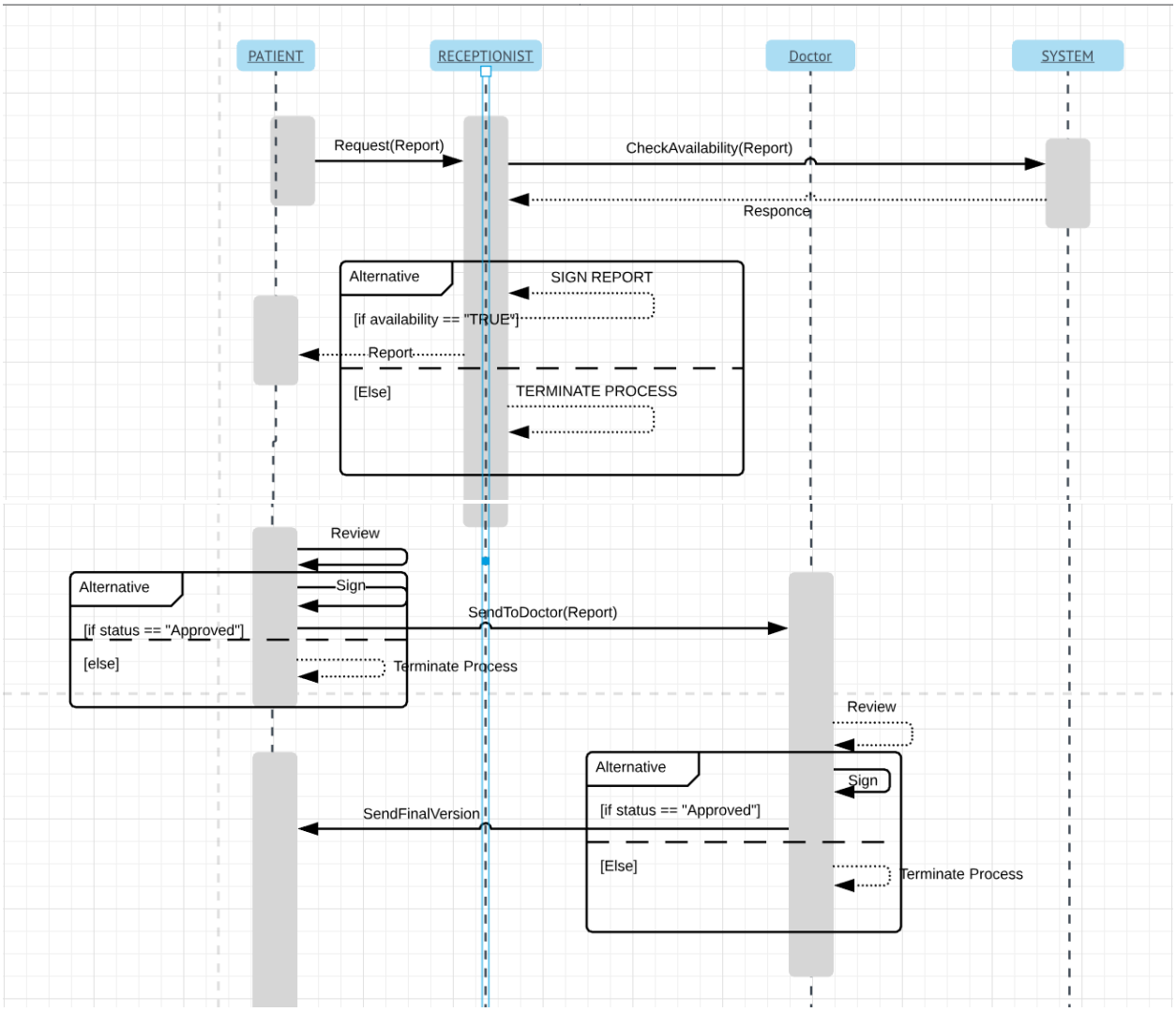
Third Party Authentication



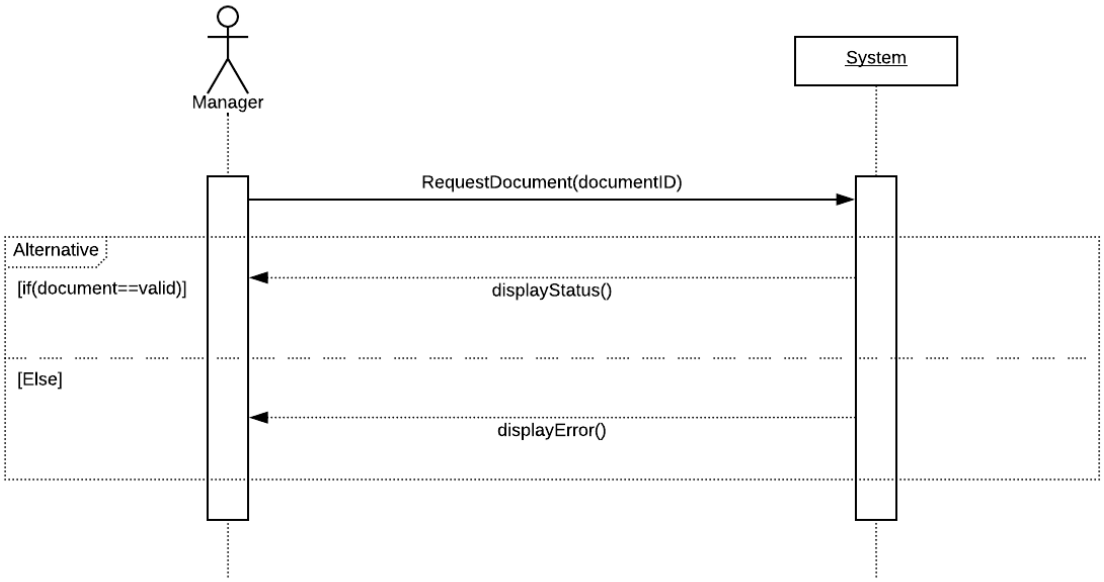
Login


Admin
Registrar
Patient
SYSTEM
Login(userID, password)
GetUser(userID)
createSession
Login(userID, password)
GetUser(userID)
createSession
Login(userID, password)
GetUser(userID)
createSession
LoginStatus
VerifyLogin(userID,password)
Result
LoginStatus
VerifyLogin(userID,password)
Result
LoginStatus
VerifyLogin(userID,password)
Result

Authentication, signing, request & validity (patient, receptionist):



CHECKING STATUS:



8.5. Operation contracts

Name:	Register(input)
Responsibility:	Register users of the system
Type:	System.
Cross Reference:	Register User
Pre-Conditions:	User must be stakeholder of the system
Post-Conditions:	New instance was instantiated of user User. Status was updated by registrar or admin User was saved to the database

Name:	dataIntegrityConstraintCheck ()
Responsibility:	Check the credential of the user
Type:	System.
Cross Reference:	Register User
Pre-Conditions:	This is a registration process underway
Post-Conditions:	New instance was instantiated of user User. Status was updated by registrar or admin User was saved to the database

Name:	DisplayError()
Responsibility:	Customer places order.
Type:	System.
Cross Reference:	Register User, register organization, Register Owner
Pre-Conditions:	This is a registration process underway
Post-Conditions:	New instance was not instantiated of user User. Status was not updated by registrar or admin User was not saved to the database Error message was displayed

Name:	GetUser (UserID)
Responsibility:	Check the user status
Type:	System.
Cross Reference:	Track request
Pre-Conditions:	User must be registered
Post-Conditions:	New instance of user was instantiated of user User. Status was updated by registrar or admin UserID was got by the manager object

Name:	verifyLogin (UserID, password)
Responsibility:	System verify user
Type:	System.
Cross Reference:	Login
Pre-Conditions:	User must be registered. User ID must be present in the system
Post-Conditions:	New instance of user was instantiated of user User. Status was updated User was associated with the current scenario.

Name:	Request (Report)
Responsibility:	User wants to share the report with the officer of third party
Type:	System.
Cross Reference:	Cross-check Report
Pre-Conditions:	Officer and patient are the part of the system
Post-Conditions:	Patient instance was created Officer instance was created Patient was associated with the officer and receptionist

Name:	CheckAvailability(Report)
Responsibility:	User wants to share the report with the officer of third party
Type:	System.
Cross Reference:	Authentication + signing + request & validity(patient + receptionist):
Pre-Conditions:	Instance of report is instantiated. Patient have MRN
Post-Conditions:	A report was made by system Report was instantiated.

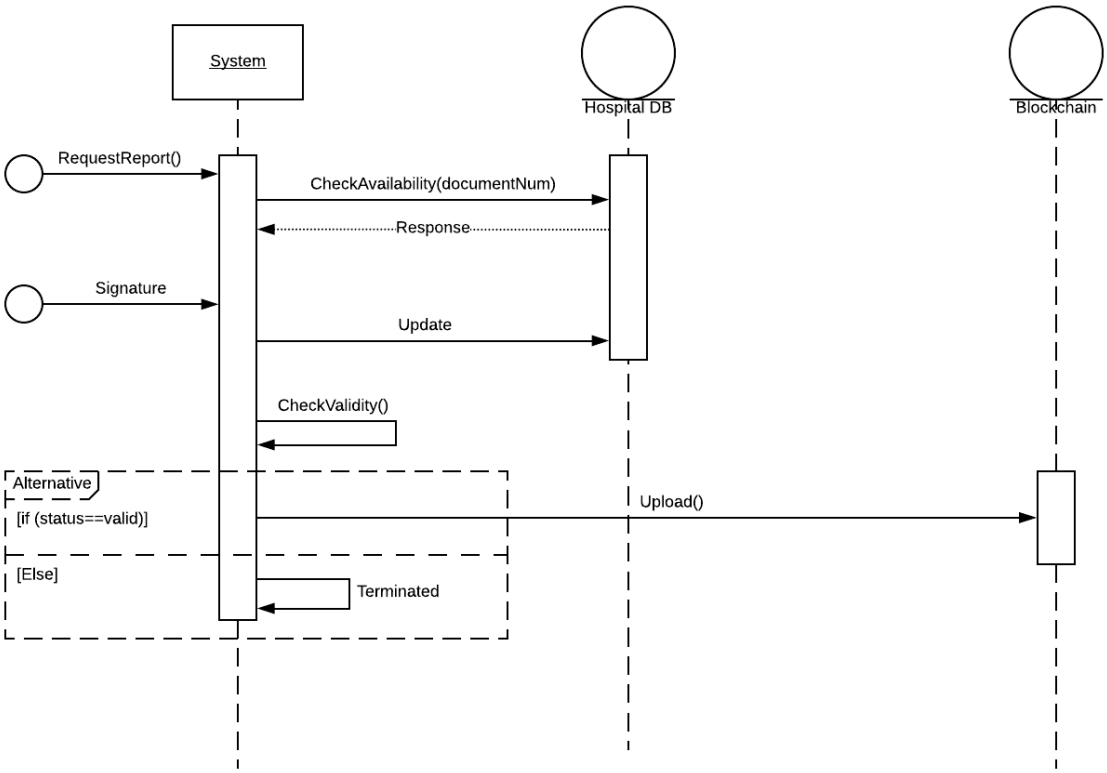
Name:	sentToDoctor(Report)
Responsibility:	Report send to the doctor
Type:	System.
Cross Reference:	Authentication + signing + request & validity(patient + receptionist):
Pre-Conditions:	New request made by the patient
Post-Conditions:	Instance of doctor was created Report instance was associated with the doctor.

Name:	verifyDocument(documentID)
Responsibility:	Third party authentication
Type:	System.
Cross Reference:	Third party authentication
Pre-Conditions:	Patient make a request
Post-Conditions:	Officer was instantiated. Officer was associated with the patient

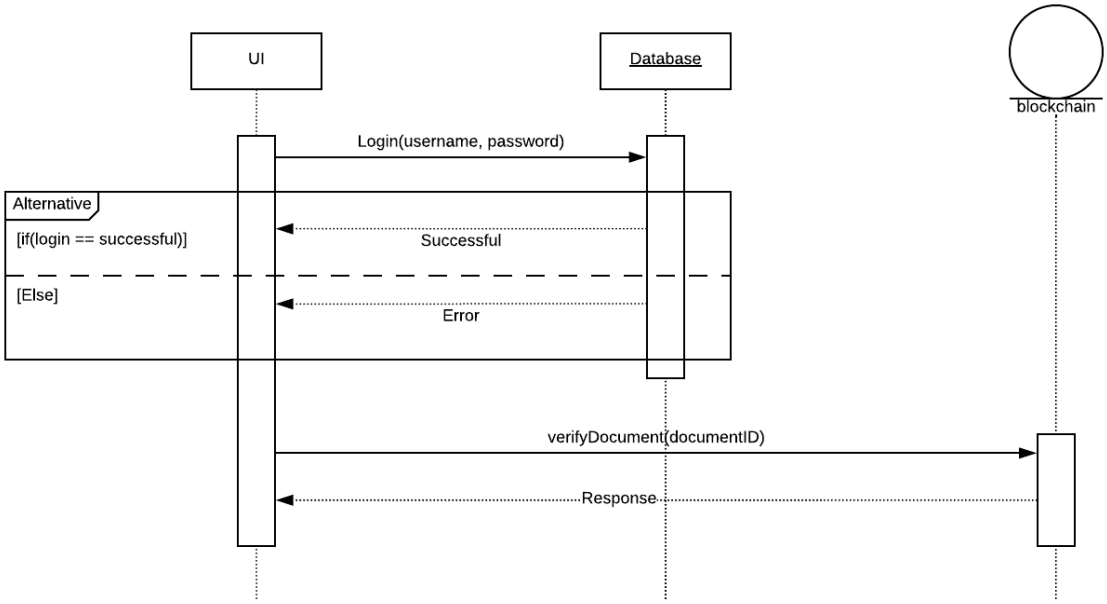
Name:	IssueCertificate(registrarID, organizationID)
Responsibility:	Customer places order.
Type:	System.
Cross Reference:	Issue certificate
Pre-Conditions:	Organizations is registered
Post-Conditions:	Hospital was instantiated. Hospital was associated with the Admin of the system. Organization. Certificate was called

8.6. Sequence Diagrams

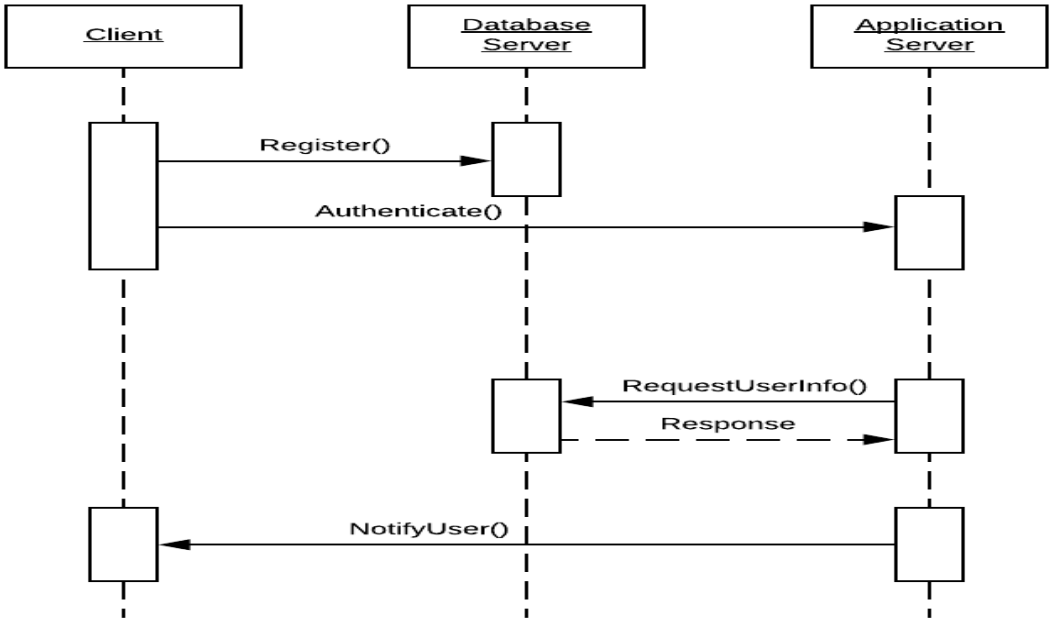
Authentication, signing, request & validity (patient, receptionist):



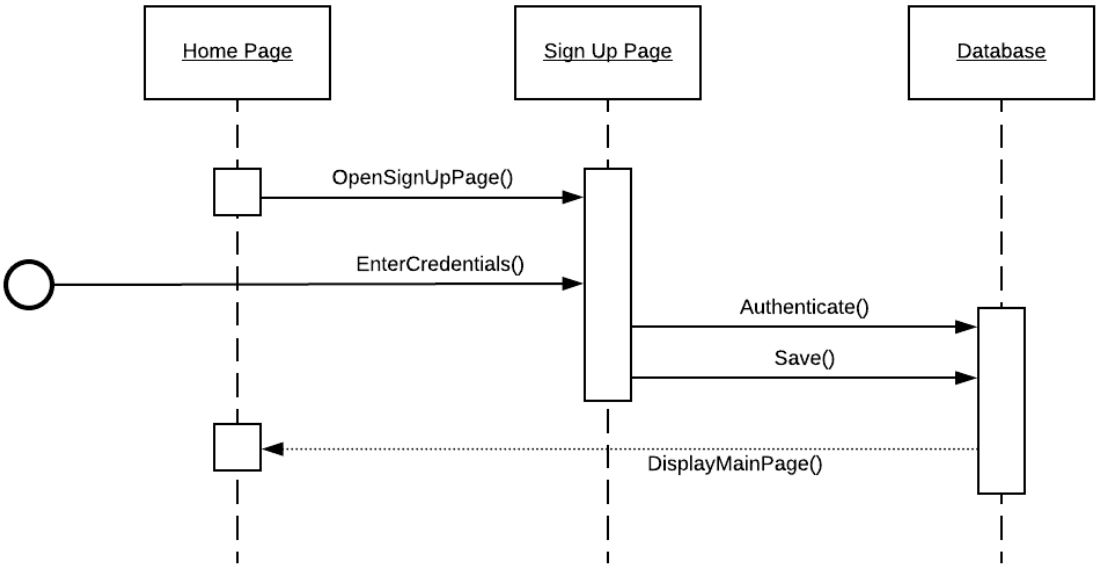
THIRD-PARTY VERIFICATION:



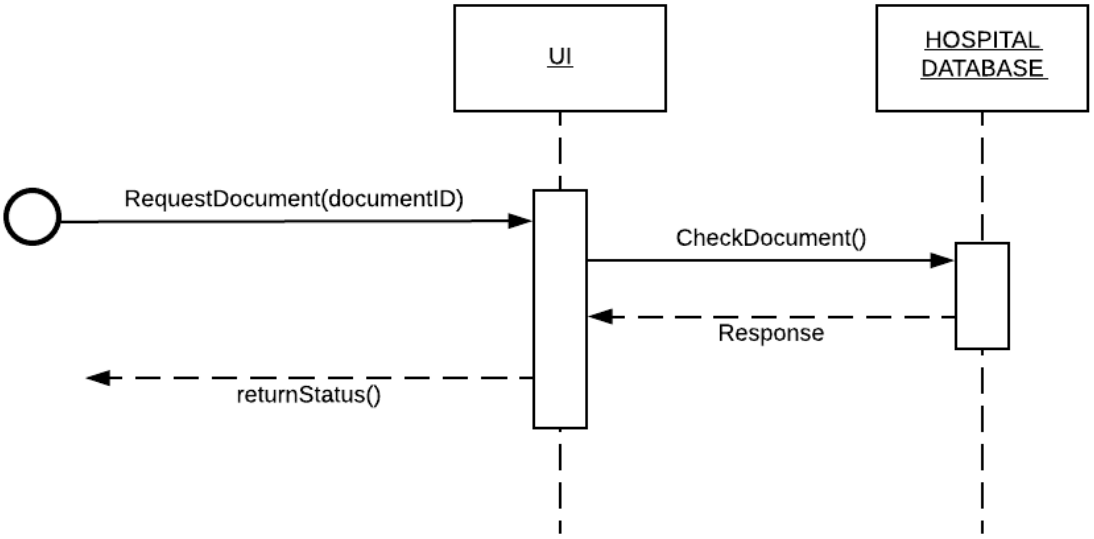
LOGIN:



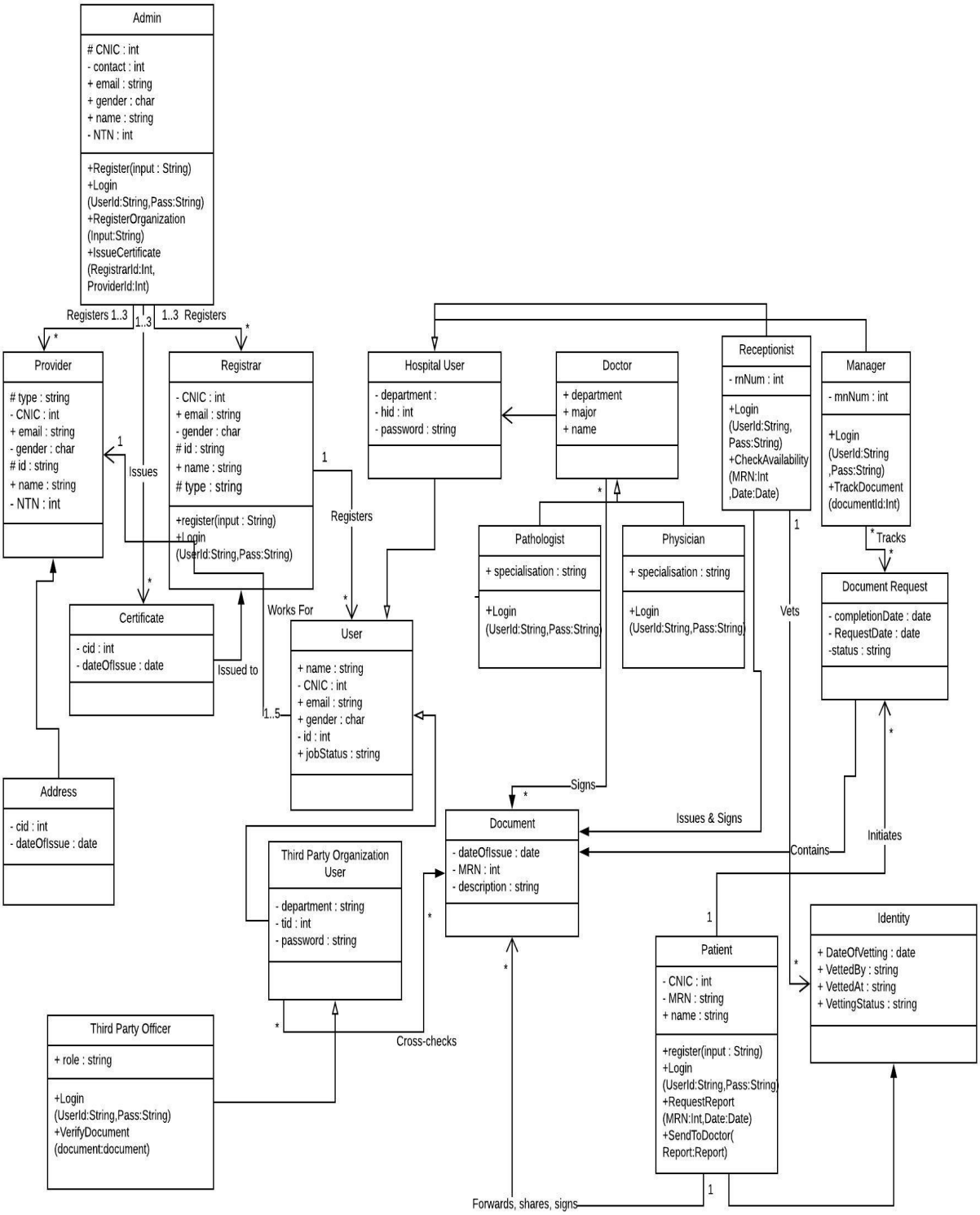
REGISTRATION:



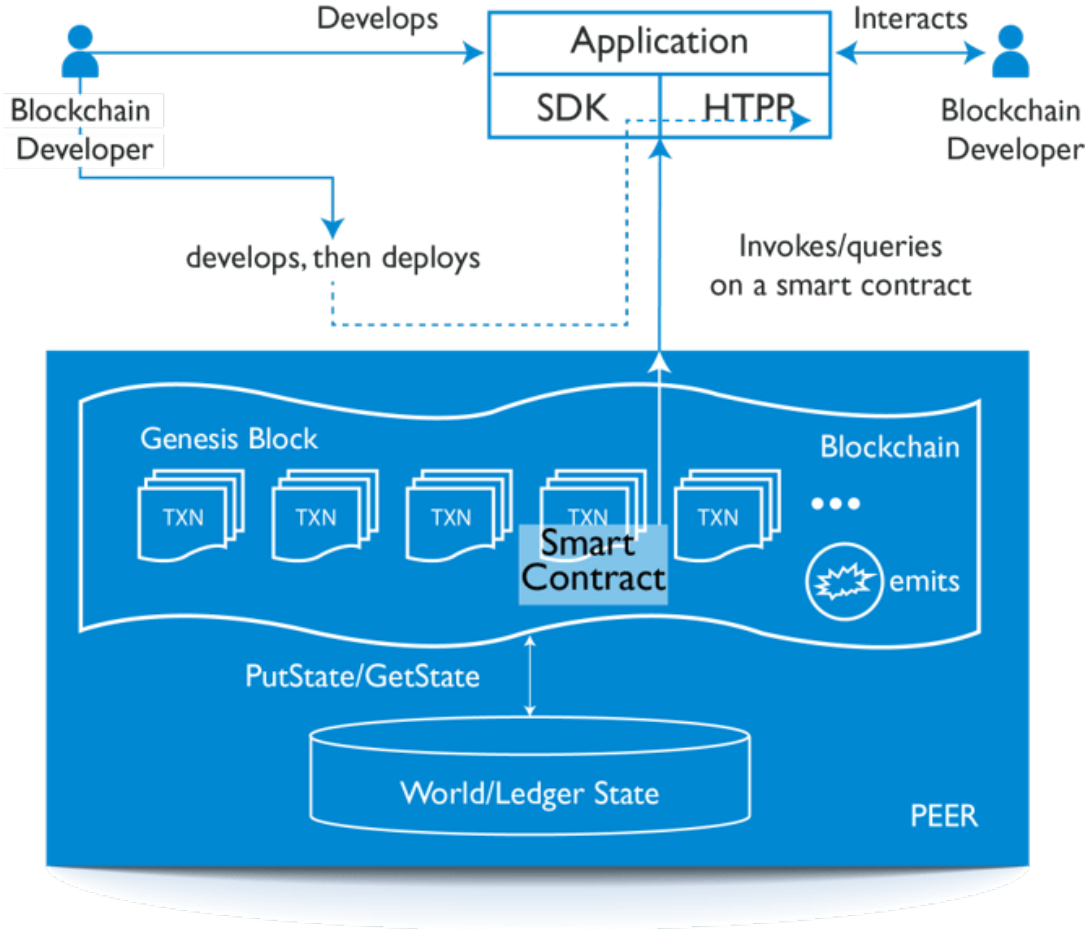
DOCUMENT TRACKING:

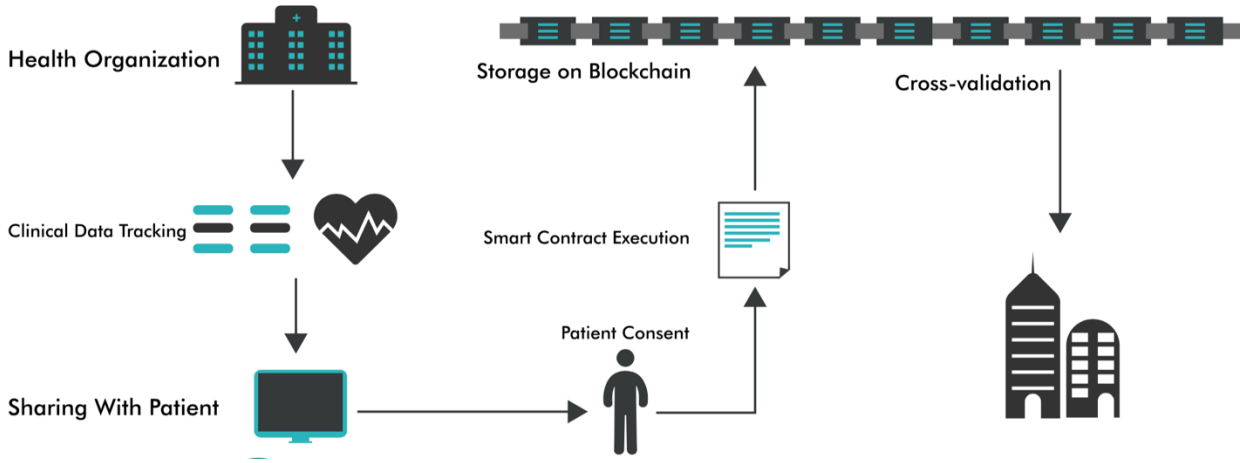


8.7. Class Diagram

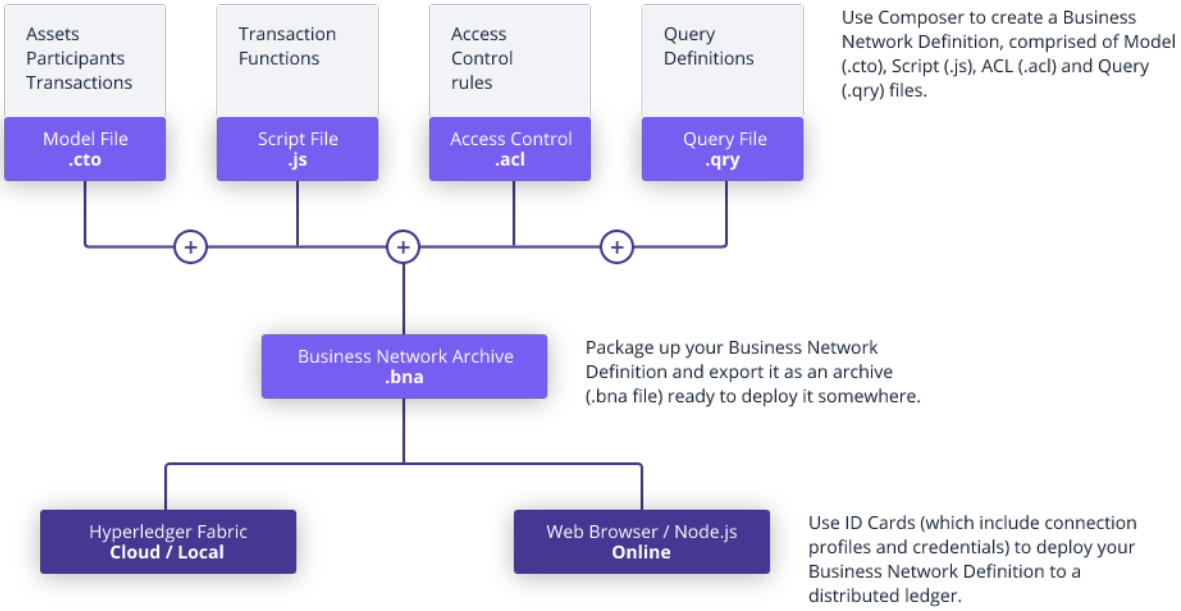


8.8. Architecture Diagram





8.9. Package and Deployment Diagram



8.10. Design Description

Assets:

- Patient Identity
- Document Request
- Document

Participants:

- Admin
- Provider
- Owner Of Organization
- Registrar
- Doctor
- Manager
- Receptionist
- Patient
- Third Party Officer

Transactions:

- CreatePatientIdentity
- ForwardPatientIdentityToHospital
- VetPatientIdentity
- RejectPatientIdentity
- DocumentRequestForwarding
- DocumentRequestNotAvailable
- DocumentRequestIrrelevant
- DocumentRequestForwardingToDoctor

- DocumentRequestCompletion
- DocumentRequestCanceledByDoctor
- DocumentCanceledByPatient
- DocumentAcceptance
- OurSetupDemo

Asset States:

Patient Identity :

- SIGNED_UP_IDENTIY
- FORWARDED_TO_HOSPITAL
- VETTED

Document Request Status:

- FORWARDED_TO_RECEPTIONIST
- FORWARDED_TO_PATIENT
- FORWARDED_TO_DOCTOR
- CANCELED_BY_RECEPTIONIST_UNAVAILABLE_DOCUMENT
- CANCELED_BY_RECEPTIONIST_IRRELEVANT_DOCUMENT
- CANCELED_BY_DOCTOR
- COMPLETED

Document:

- SIGNED_BY_RECEPTIONIST
- SIGNED_BY_RECEPTIONIST_AND_DOCTOR
- SIGNED_BY_PATIENT_RECEPTIONIST_AND_DOCTOR
- RECORD_CONFLICT
- CANCELED_BY_PATIENT_IRRELEVANT_DOCUMENT

Participants : Patient - Receptionist

Asset: PatientIdentity

1. Patient Signups by filling all the fields and the asset **PatientIdentity** is created and given the state
    - As soon as the patient creates the identity , it is assigned the state:
        - **PatientIdentity → SIGNED_UP_IDENTIY**

2. Patient selects a health centre from a list of specified Health Centres and forwards a request for identity vetting to the Health Center
    - **PatientIdentity → FORWARDED_TO_RECEPTIONIST**

3. Patient visits the Health centre and reaches the counter and asks the receptionist for identity vetting, Customer brings his CNIC Card with him
    - If the patient has submitted the right information ,the asset transition is:
      PatientIdentity → VETTED
    - If the patient has submitted the right information ,the asset transition is:
      PatientIdentity → FAKE

Participants : Patient - Receptionist

Asset: DocumentRequest , Document

1. Patient visits the Document Request Forum ,selects the health centre, enters the MRN and the Date,**DocumentRequest** is created and a state is assigned to that asset:

   DocumentRequest → FORWARDED_TO_RECEPTIONIST

2. Receptionist gets a notification and sees a **DocumentRequest**, he/she checks the availability of the requested Document

   a. if the document is available and relevant . The Receptionist creates a document and the following state transitions takes place :
      - **DocumentRequest → FORWARDED_TO_DOCTOR**
      - **Document → SIGNED_BY_RECEPTIONIST**

   b. if the document is not available, the following state transition takes place:
      - **DocumentRequest→CANCELED_BY_RECEPTIONIST_UNAVAILABLE_DOCUMENT**

   c. if the document is available but not relevant, the following state transition takes place:
      - **DocumentRequest→CANCELED_BY_RECEPTIONIST_IRRELEVANT_DOCUMENT**

Participants : Doctor

Asset: DocumentRequest , Document

1. The doctor gets a notification for the request.

    a. If he/she finds the document to be Right according to his/her information,then the following state transitions takes place:

    DocumentRequest→FORWARDED_TO_PATIENT

    Document→SIGNED_BY_RECEPTIONIST_AND_DOCTOR

    b. If he/she finds the document to be Wrong according to his/her information,then the following state transitions takes place:

    DocumentRequest→CANCELED_BY_DOCTOR

Participants : Patient

Asset: DocumentRequest , Document,Provider(Hospital Organization)

1. If all goes well, then the Patient receives a notification,validates with his copy and a copy of that document is forwarded to the Provided organization.
    a. If he receives the relevant document then the following state transitions take place:
        - **DocumentRequest → COMPLETED**
        - **Document→SIGNED_BY_PATIENT_RECEPTIONIST_AND_DOCTOR**

    b. If he receives the irrelevant or wrong document then the following state transitions takes place:
        - **Document→CANCELED_BY_PATIENT_IRRELEVANT_DOCUMENT**

9. Iteration 3:

Iteration 3 of SecureMed is majorly focused on the creation of GUI, rest API and connection between them. GUI is basically a web application for our users.

9.1. Expanded Use Cases:

UC01: Register Organization

Scope: SecureMed

Level: User Goal

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Organization registrar is registered

Main Success Scenario:

Actor Action	System Response
13. The admin of SecureMed logs into SecureMed	
	14. SecureMed opens the main page
15. The admin registers organization	
	16. SecureMed asks about the organization
17. The admin issues the certificate to the organization	
	18. The system identifies the organization

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be user friendly.

Technology and Data Variation List: Web page.

UC02: Register Owner

Scope: SecureMed

Level: Business requirement

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Owner of organization is registered

Main Success Scenario:

Actor Action	System Response
13. The admin of SecureMed logs into SecureMed	
	14. SecureMed opens the main page
15. The admin registers owner of the organization	
	16. SecureMed asks about the Owner
17. The admin enters owner's information	
	18. The system stores information in system of records

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be clear and user friendly.

Technology and Data Variation List: Web page.

UC03: Register Registrar

Scope: SecureMed

Level: Business requirement

Primary Actor: Admin

Pre-Conditions: Admin must login

Success Guarantee: Default registrar of the organization is registered

Main Success Scenario:

Actor Action	System Response
13. The admin of SecureMed logs into SecureMed	
	14. SecureMed opens the main page
15. The admin registers default registrar of the organization	
	16. SecureMed asks about the registrar and the privileges
17. The admin enters the required information	
	18. The system maintains the record for the information

Extensions: May be something not present on menu that admin wants.

Special Requirements: Menu should be clear and user friendly.

Technology and Data Variation List: Web page

UC04: Login

Scope: SecureMed Goal

Level: Security Goal

Primary Actor: Admin, Registrar, Manager, Patient, Third Party Officer, Receptionist, Doctor

Pre-Conditions: System must be on

Success Guarantee: Login to the system

Main Success Scenario:

Actor Action	System Response
13. The user opens the SecureMed	
	14. SecureMed show the main page having different roles
15. The user selects his role and enter	
	16. The system asks for the credentials.
17. The admin enters the required information	
	18. The system logs in

Extensions: May be the credentials entered by the user are not correct.

Special Requirements: Log in box should be clear and visible.

Technology and Data Variation List: Login Web Page

UC05: Register User

Scope: SecureMed

Level: Business requirement

Primary Actor: Registrar

Pre-Conditions: Registrar must login and registrar should be registered

Success Guarantee: Registrar registers defined users of the organization.

Main Success Scenario:

Actor Action	System Response
13. The registrar of organization logs into SecureMed	
	14. SecureMed opens the main page
15. The registrar selects register user option and select the user	
	16. System confirms the user
17. The registrar enters the required information of user.	
	18. The system stores the information of users and create a user account

Extensions: May be something not present on menu that registrar wants.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC06: Issue Certificate

Scope: SecureMed

Level: Business requirement

Primary Actor: Registrar

Pre-Conditions: Registrar must login and registrar should be registered

Success Guarantee: Registrar issues certificates to the registered users of the organization

Main Success Scenario:

Actor Action	System Response
13. The registrar of organization logs into SecureMed	
	14. SecureMed opens the main page
15. The registrar selects registered user option and select the user	
	16. System confirms the user
17. The registrar enters the required information of user.	
	18. The system issues the certificate to the requested user.

Extensions: May be some users don't have the privilege of certificate

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen.

Technology and Data Variation List: Web page

UC07: Track Request

Scope: SecureMed

Level: Business requirement

Primary Actor: Manager

Pre-Conditions: Manager must login

Success Guarantee: Manager of the organization can track the request of patient and other users as well

Main Success Scenario:

Actor Action	System Response
11. The Manager of organization logs into SecureMed	
	12. SecureMed opens the main page
13. The Manager opens the requests	
14. The Manager track the requested request	
	15. The system shows the information of the request

Extensions: May be some requests cannot be tracked.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC08: Register Patient

Scope: SecureMed

Level: Business requirement

Primary Actor: Patient, Receptionist

Pre-Conditions: Patient, Receptionist must login, Receptionist should be registered by the registrar.

Success Guarantee: Receptionist registers the patient.

Main Success Scenario:

Actor Action	System Response
11. The receptionist of organization logs into SecureMed	
	12. SecureMed opens the main page
13. The receptionist checks the request log of the patients.	
14. The receptionist confirms the request.	
	15. The system accepts the request and update the system of records.

Extensions: May be some patient cannot be registered due to some limitations

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC9: Request Report

Scope: SecureMed

Level: Business requirement

Primary Actor: Patient

Pre-Conditions: Patient must login and Patient should have been vetted by the receptionist of the hospital(organization)

Success Guarantee: Patient requests for medical report.

Main Success Scenario:

Actor Action	System Response
13. The patient logs into SecureMed	
	14. SecureMed opens the main page
15. The patient selects the report request option.	
	16. The system opens the MRN page
17. The patient enters his/her MRN	
	18. System send the MRN to the receptionist of the hospital

Extensions: MRN may not be exist.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen

Technology and Data Variation List: Web page

UC10: Authenticate Report

Scope: SecureMed

Level: Security Goal

Primary Actor: Patient

Pre-Conditions: Patient must login and receptionist should send the report to the patient for cross check

Success Guarantee: Patient signs the report sent by the receptionist.

Main Success Scenario:

Actor Action	System Response
13. The patient logs into SecureMed	
	14. SecureMed opens the main page
15. The patient checks the report by clicking requested reports	
	16. System shows the report
17. The patient confirms the report	
	18. The system sends the confirmation message and hash of the report to the receptionist.

Extensions: May be the report is not that, that was expected by the patient

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen.

Technology and Data Variation List: UML model may be produced

UC11: Share Report

Scope: SecureMed

Level: User Goal

Primary Actor: Patient

Pre-Conditions: Patient must login and Patient should be registered having some medical reports.

Success Guarantee: Patient shares the report with the third party (visa officer)

Main Success Scenario:

Actor Action	System Response
11. The patient logs into SecureMed	
	12. SecureMed opens the main page having third party list
13. The patient selects the desired party and enters	
	14. System confirms the third party
	15. The system accepts the request and update the system of records.

Extensions: May be some patients cannot share the report due to the privilege issues.

Special Requirements: Menu should be clear and user friendly. User should be defined on the screen. Up to 98% accuracy

Technology and Data Variation List: Web page

UC12: Cross-check Report

Scope: Security goal

Level: User Goal

Primary Actor: Third Party Officer

Pre-Conditions: Third Party Officer must login and Third-party officer should be registered

Success Guarantee: Third-party officer cross checks the shared medical document by the patient.

Main Success Scenario:

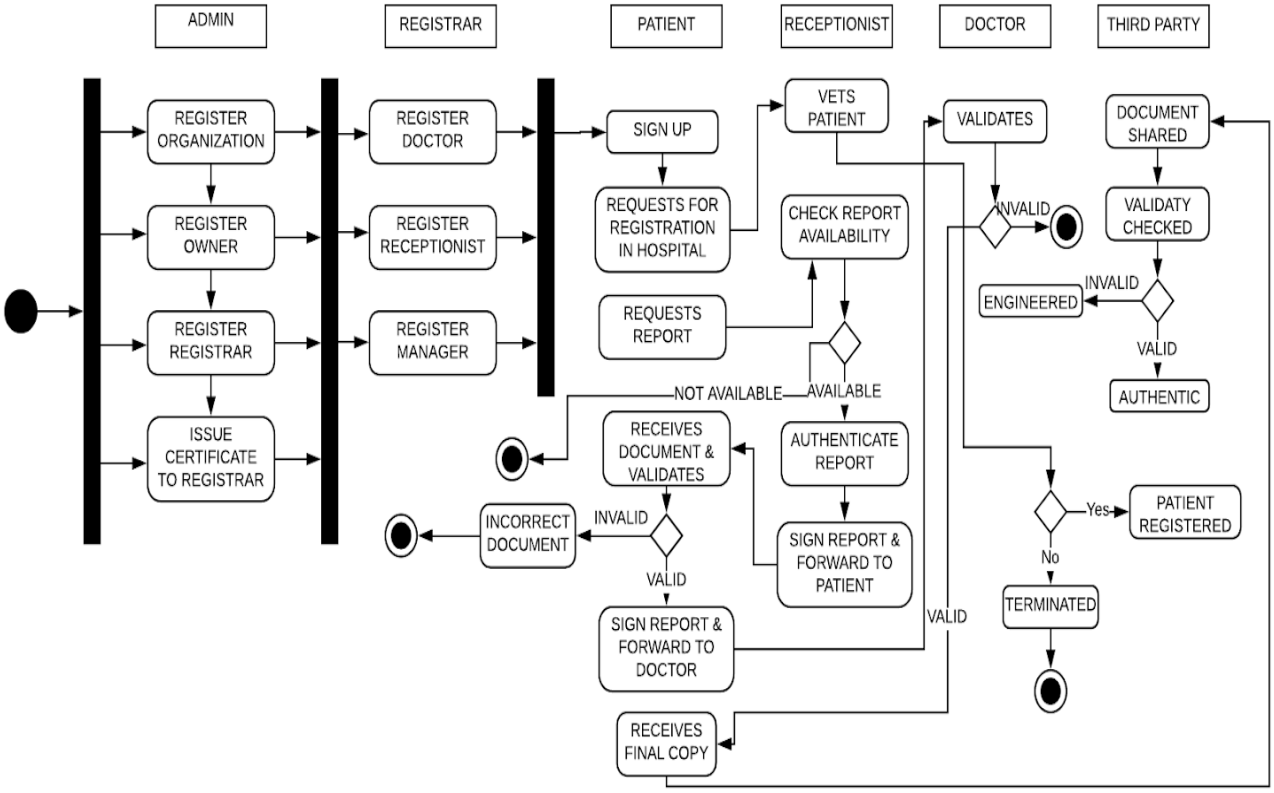
Actor Action	System Response
13. The officer logs into SecureMed	
	14. SecureMed opens the main page.
15. The officer checks the shared reports and select the desired one.	
	16. System opens the document
17. The officer hashes the document and check it on the ledger (Blockchain)	
	18. The system checks the report on the ledger and confirms the report

Extensions: Shared report may not be original or not on blockchain. So, can't be cross check by the visa officer.

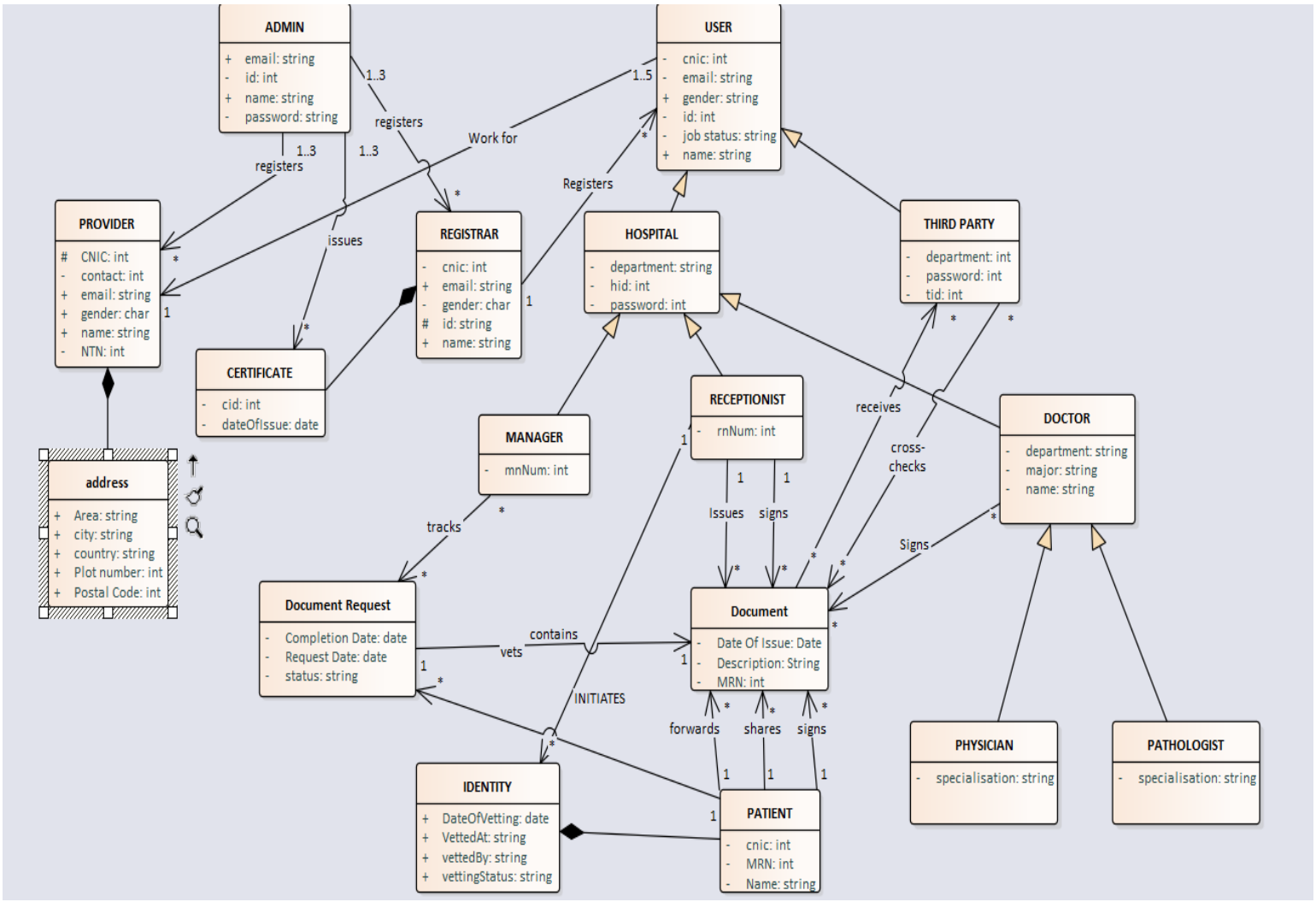
Special Requirements: Menu should be clear and user friendly. User should be defined on the screen. Up to 98% accuracy.

Technology and Data Variation List: Web page

9.2. Activity Diagram

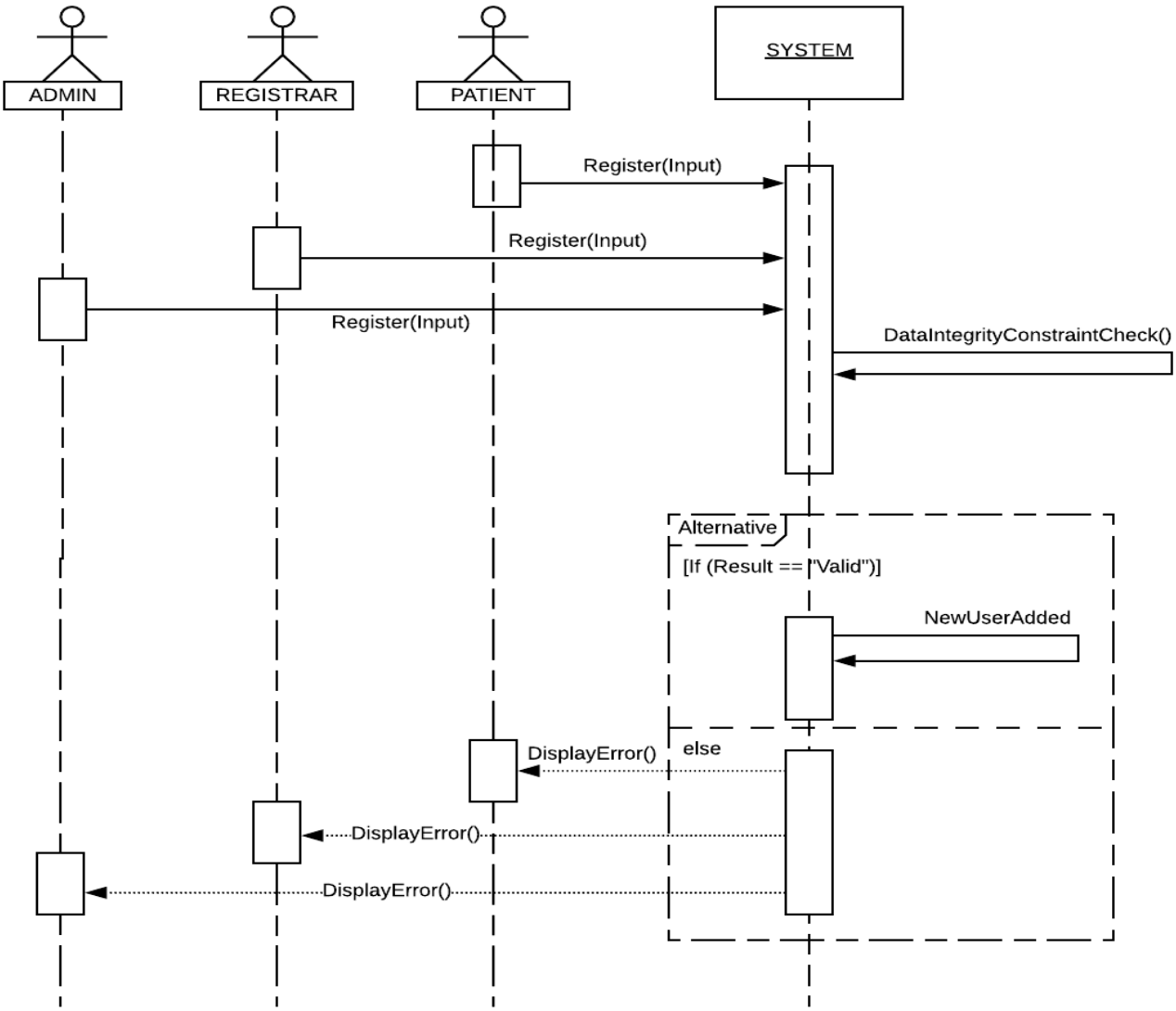


9.3. Domain Model

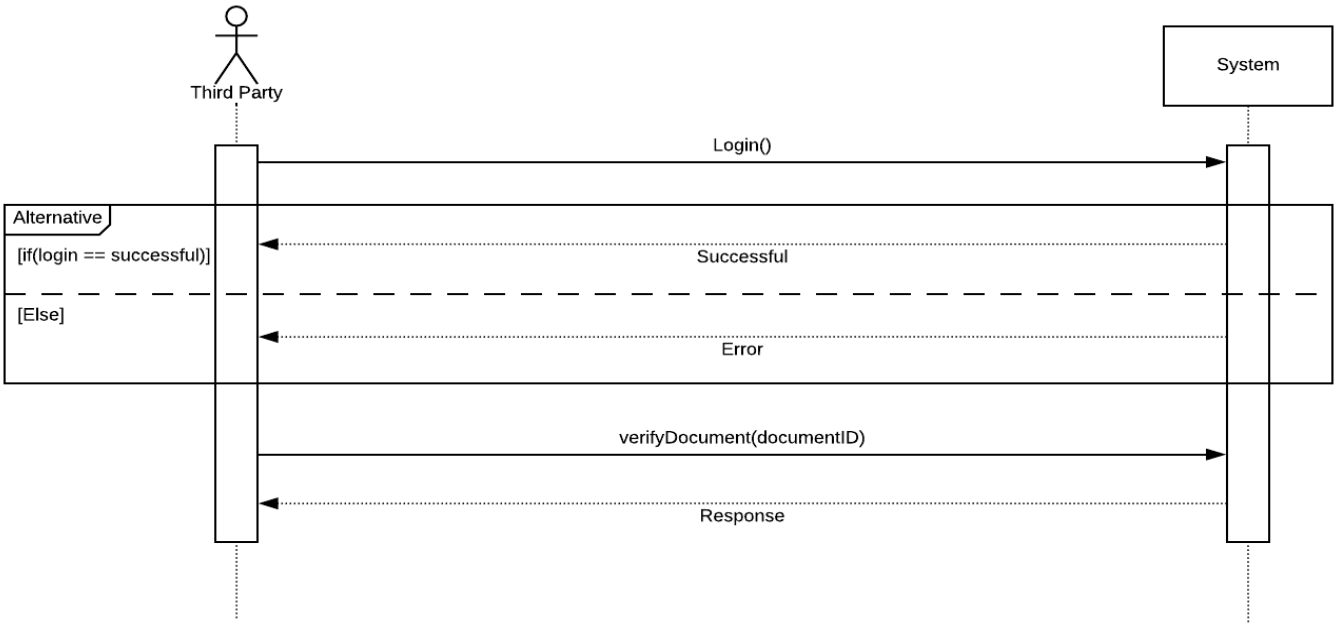


9.4. System Sequence Diagram

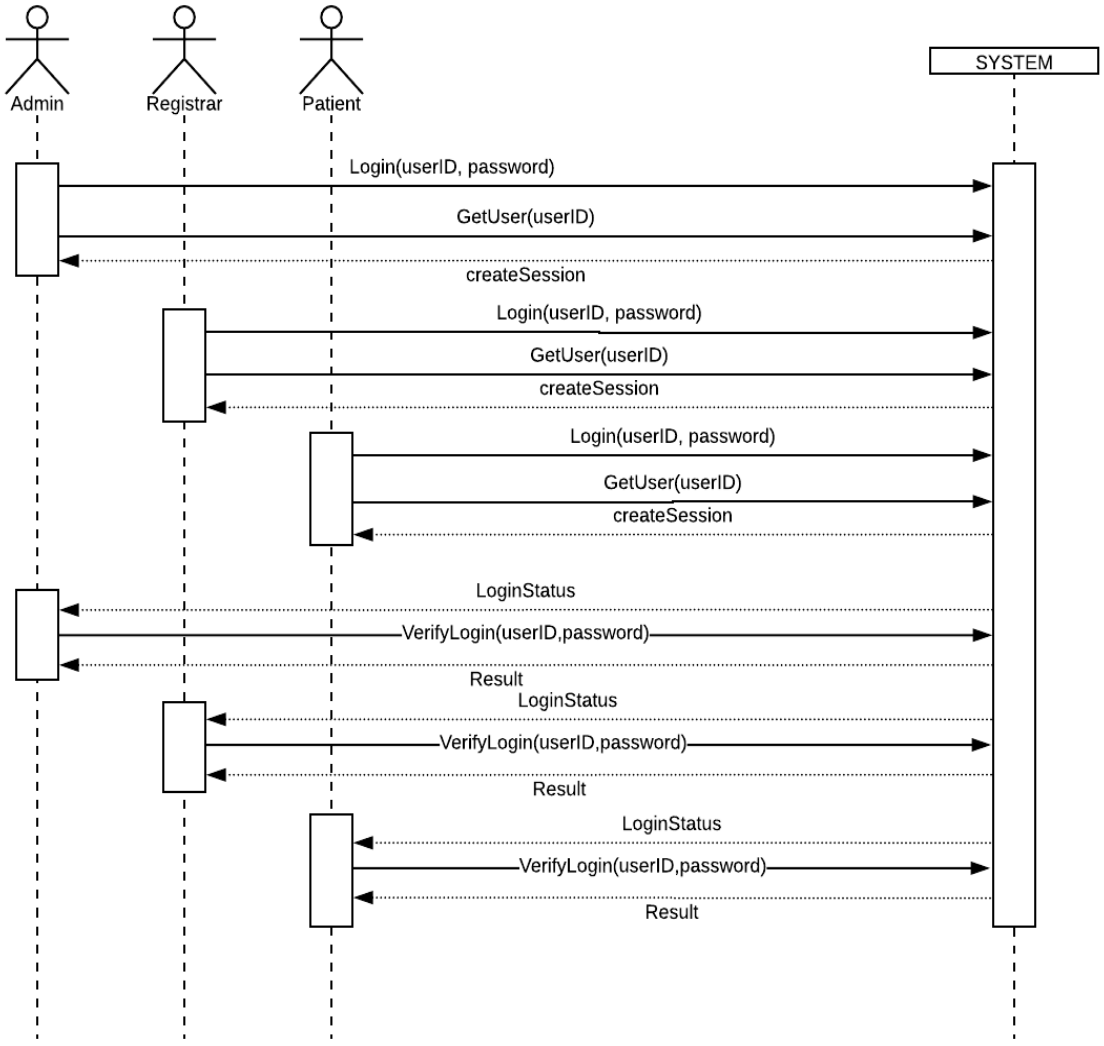
REGISTRATION:



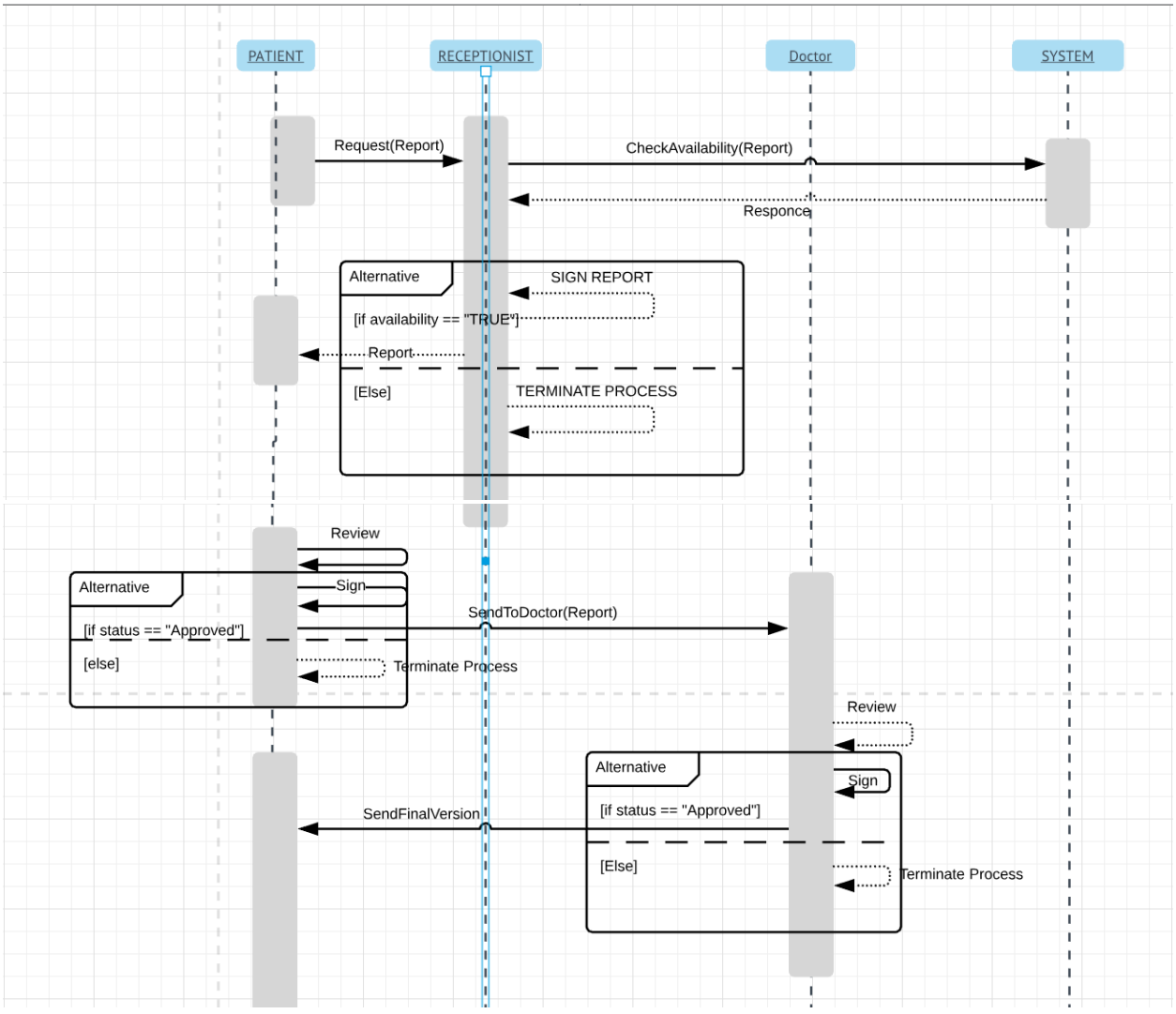
Third Party Authentication



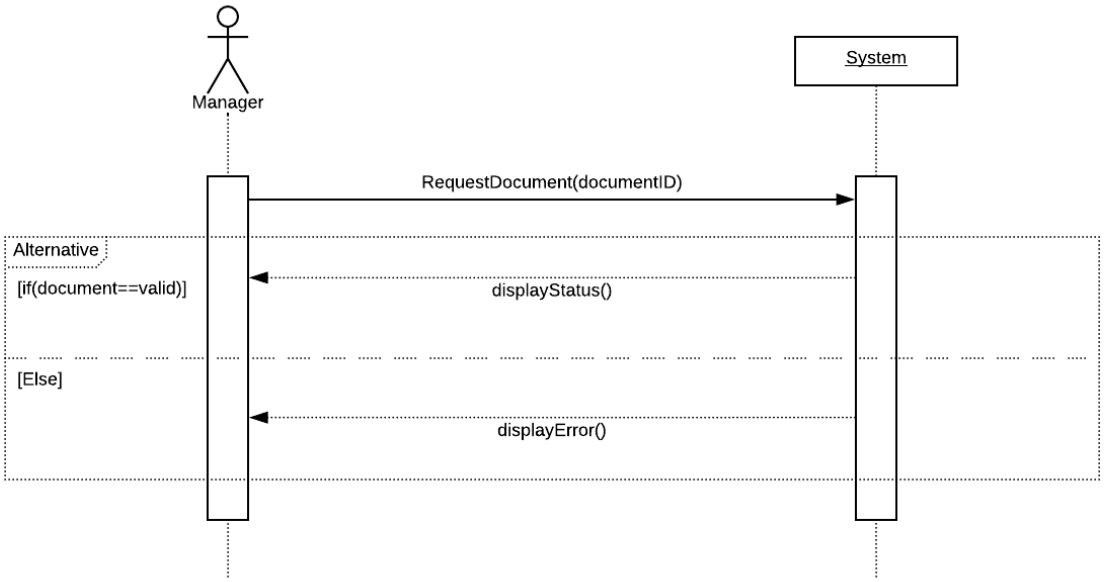
Login


Admin
Registrar
Patient
SYSTEM
Login(userID, password)
GetUser(userID)
createSession
Login(userID, password)
GetUser(userID)
createSession
Login(userID, password)
GetUser(userID)
createSession
LoginStatus
VerifyLogin(userID,password)
Result
LoginStatus
VerifyLogin(userID,password)
Result
LoginStatus
VerifyLogin(userID,password)
Result

Authentication, signing, request & validity (patient, receptionist):



CHECKING STATUS:



9.5. Operation contracts

Name:	Register(input)
Responsibility:	Register users of the system
Type:	System.
Cross Reference:	Register User
Pre-Conditions:	User must be stakeholder of the system
Post-Conditions:	New instance was instantiated of user User. Status was updated by registrar or admin User was saved to the database

Name:	dataIntegrityConstraintCheck ()
Responsibility:	Check the credential of the user
Type:	System.
Cross Reference:	Register User
Pre-Conditions:	This is a registration process underway
Post-Conditions:	New instance was instantiated of user User. Status was updated by registrar or admin User was saved to the database

Name:	DisplayError()
Responsibility:	Customer places order.
Type:	System.
Cross Reference:	Register User, register organization, Register Owner
Pre-Conditions:	This is a registration process underway
Post-Conditions:	New instance was not instantiated of user User. Status was not updated by registrar or admin User was not saved to the database Error message was displayed

Name:	GetUser (UserID)
Responsibility:	Check the user status
Type:	System.
Cross Reference:	Track request
Pre-Conditions:	User must be registered
Post-Conditions:	New instance of user was instantiated of user User. Status was updated by registrar or admin UserID was got by the manager object

Name:	verifyLogin (UserID, password)
Responsibility:	System verify user
Type:	System.
Cross Reference:	Login
Pre-Conditions:	User must be registered. User ID must be present in the system
Post-Conditions:	New instance of user was instantiated of user User. Status was updated User was associated with the current scenario.

Name:	Request (Report)
Responsibility:	User wants to share the report with the officer of third party
Type:	System.
Cross Reference:	Cross-check Report
Pre-Conditions:	Officer and patient are the part of the system
Post-Conditions:	Patient instance was created Officer instance was created Patient was associated with the officer and receptionist

Name:	CheckAvailability(Report)
Responsibility:	User wants to share the report with the officer of third party
Type:	System.
Cross Reference:	Authentication + signing + request & validity(patient + receptionist):
Pre-Conditions:	Instance of report is instantiated. Patient have MRN
Post-Conditions:	A report was made by system Report was instantiated.

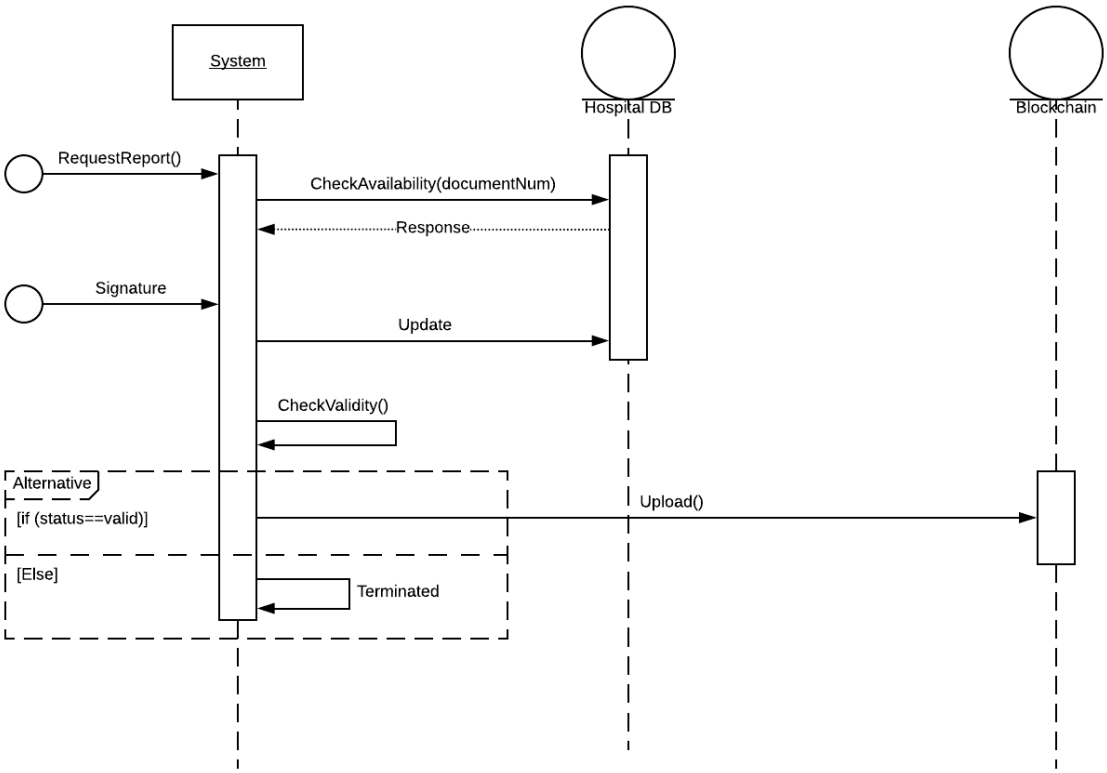
Name:	sentToDoctor(Report)
Responsibility:	Report send to the doctor
Type:	System.
Cross Reference:	Authentication + signing + request & validity(patient + receptionist):
Pre-Conditions:	New request made by the patient
Post-Conditions:	Instance of doctor was created Report instance was associated with the doctor.

Name:	verifyDocument(documentID)
Responsibility:	Third party authentication
Type:	System.
Cross Reference:	Third party authentication
Pre-Conditions:	Patient make a request
Post-Conditions:	Officer was instantiated. Officer was associated with the patient

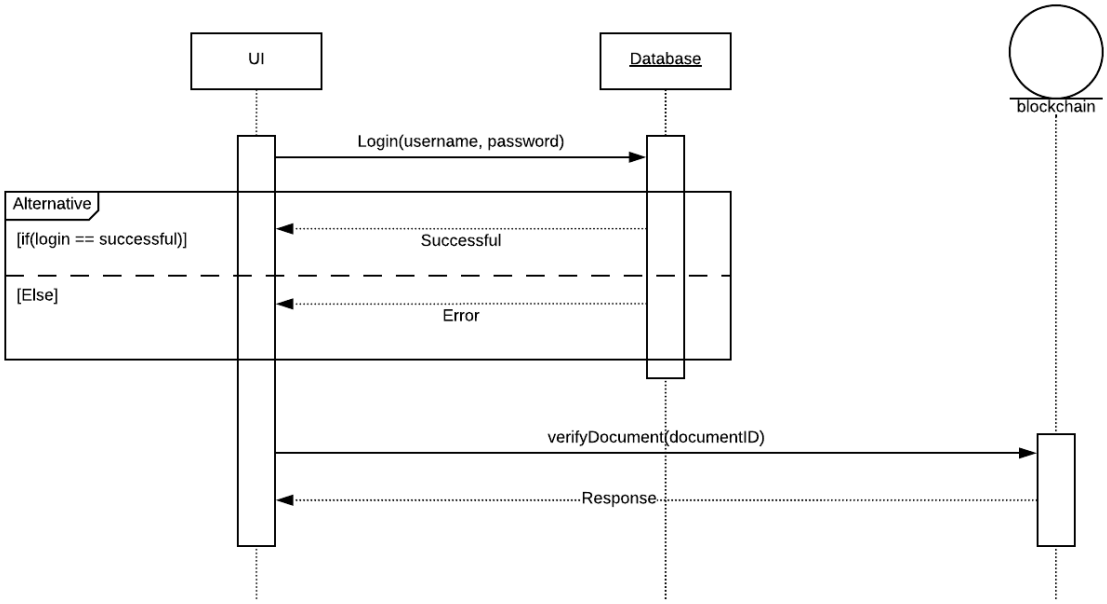
Name:	IssueCertificate(registrarID, organizationID)
Responsibility:	Customer places order.
Type:	System.
Cross Reference:	Issue certificate
Pre-Conditions:	Organizations is registered
Post-Conditions:	Hospital was instantiated. Hospital was associated with the Admin of the system. Organization. Certificate was called

9.6. Sequence Diagrams

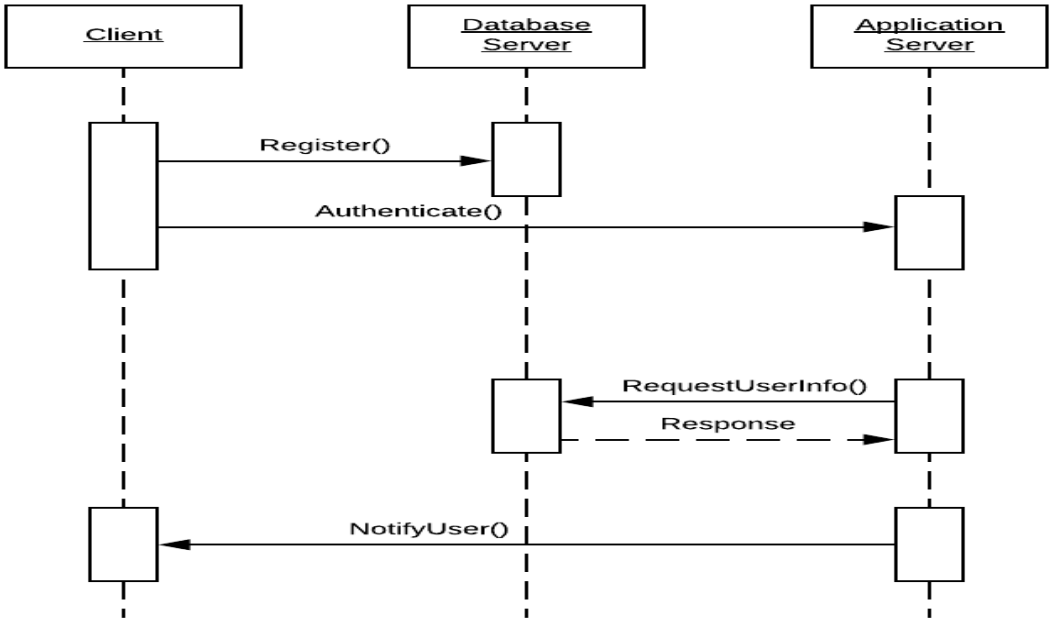
Authentication, signing, request & validity (patient, receptionist):



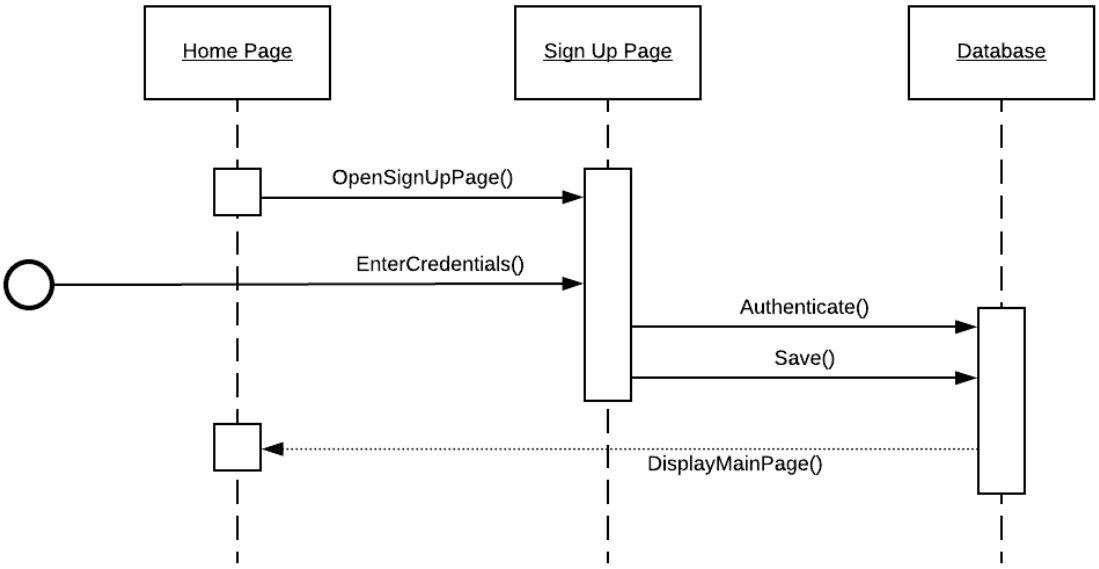
THIRD-PARTY VERIFICATION:



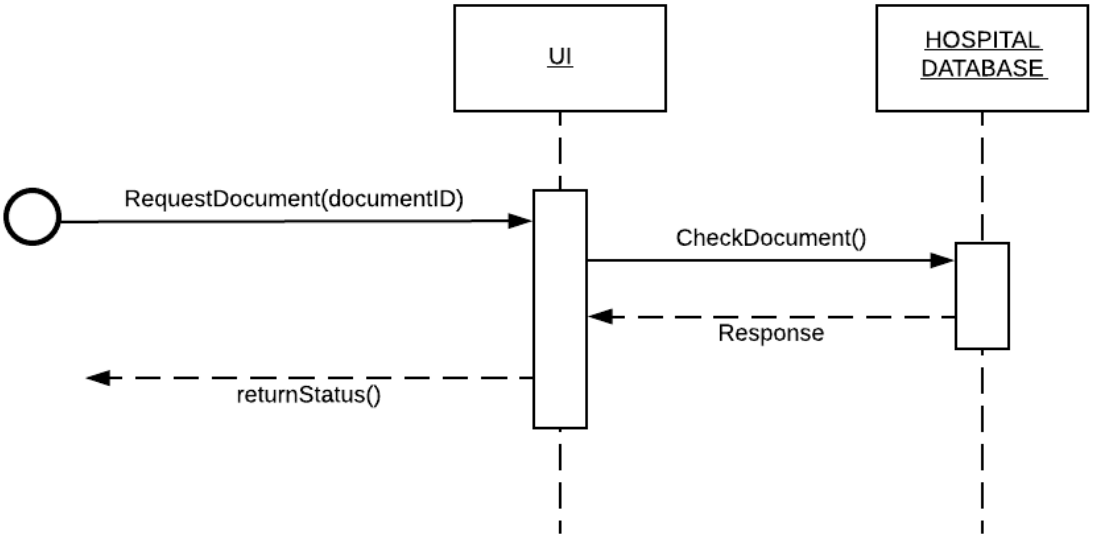
LOGIN:



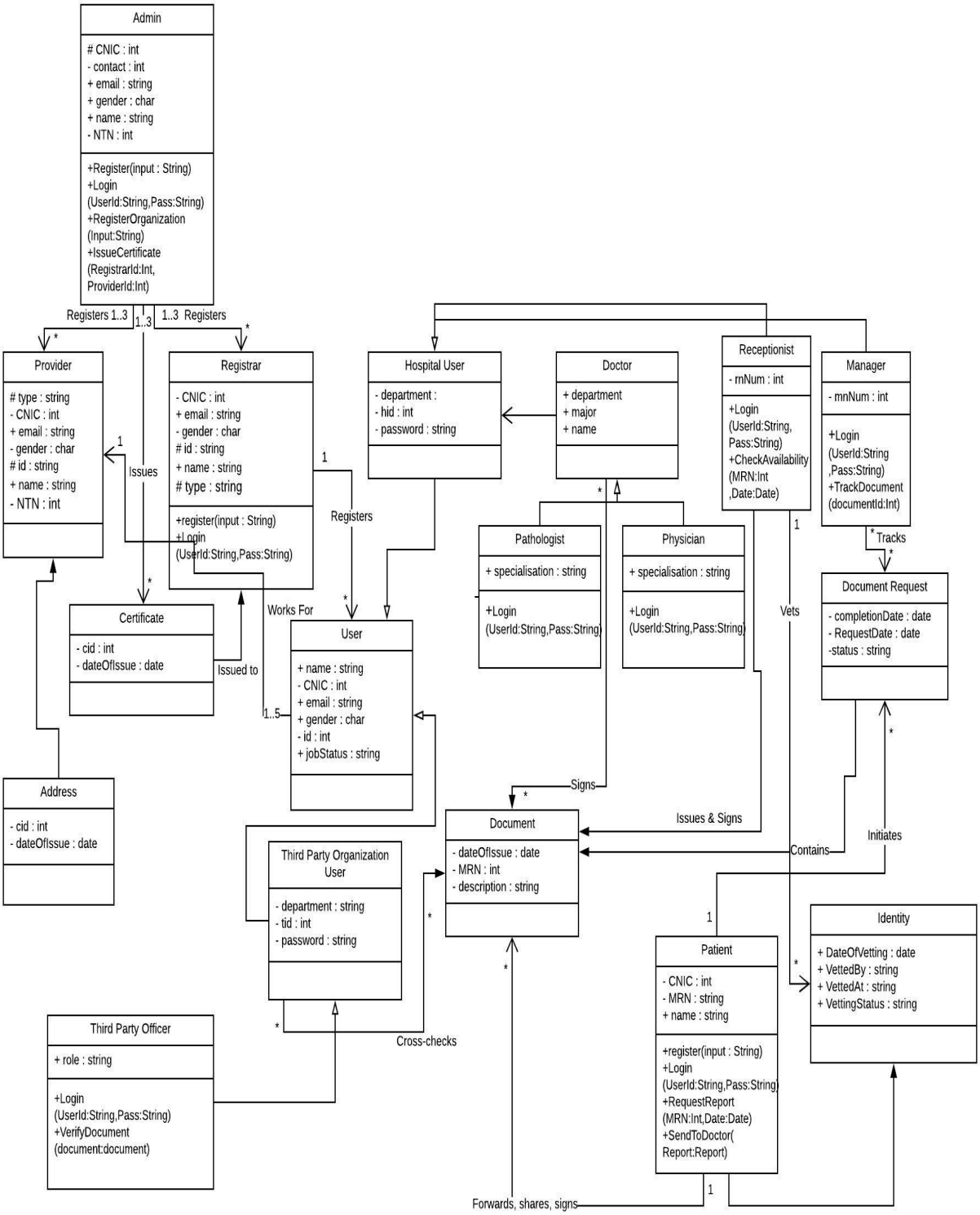
REGISTRATION:



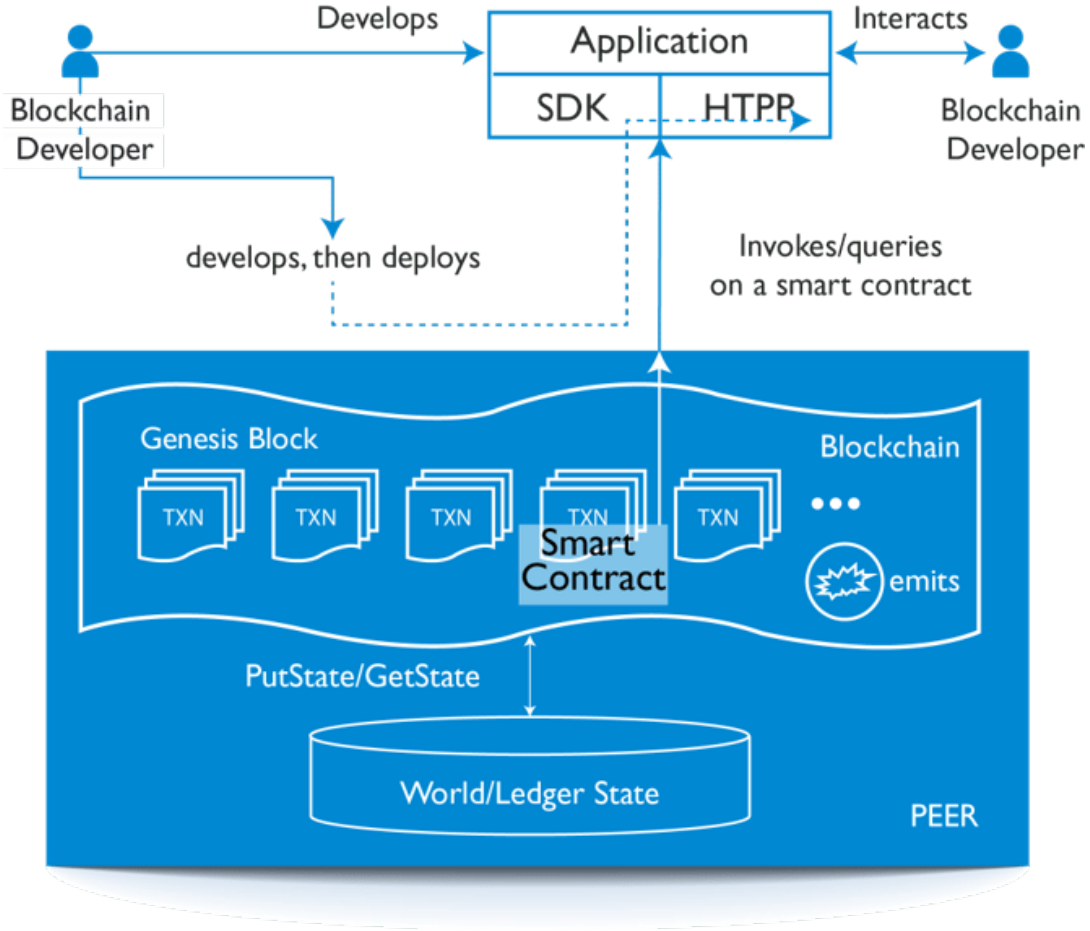
DOCUMENT TRACKING:

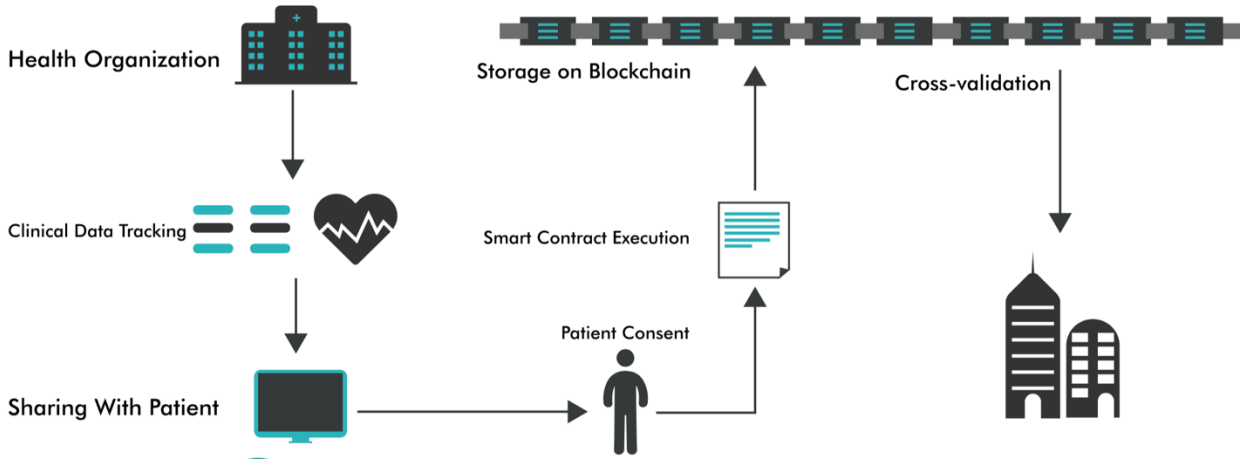


9.7. Class Diagram

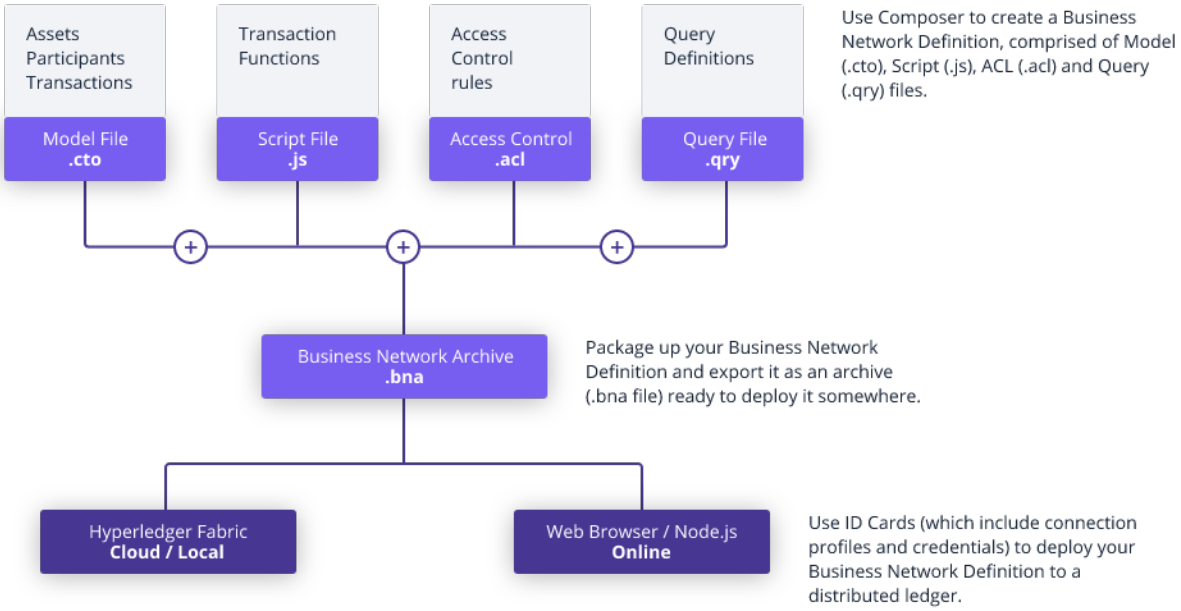


9.8. Architecture Diagram





9.9. Package and Deployment Diagram



9.10. Design Description

Assets:

- Patient Identity
- Document Request
- Document

Participants:

- Admin
- Provider
- Owner Of Organization
- Registrar
- Doctor
- Manager
- Receptionist
- Patient
- Third Party Officer

Transactions:

- CreatePatientIdentity
- ForwardPatientIdentityToHospital
- VetPatientIdentity
- RejectPatientIdentity
- DocumentRequestForwarding
- DocumentRequestNotAvailable
- DocumentRequestIrrelevant
- DocumentRequestForwardingToDoctor

- DocumentRequestCompletion
- DocumentRequestCanceledByDoctor
- DocumentCanceledByPatient
- DocumentAcceptance
- OurSetupDemo

Asset States:

Patient Identity :

- SIGNED_UP_IDENTIY
- FORWARDED_TO_HOSPITAL
- VETTED

Document Request Status:

- FORWARDED_TO_RECEPTIONIST
- FORWARDED_TO_PATIENT
- FORWARDED_TO_DOCTOR
- CANCELED_BY_RECEPTIONIST_UNAVAILABLE_DOCUMENT
- CANCELED_BY_RECEPTIONIST_IRRELEVANT_DOCUMENT
- CANCELED_BY_DOCTOR
- COMPLETED

Document:

- SIGNED_BY_RECEPTIONIST
- SIGNED_BY_RECEPTIONIST_AND_DOCTOR
- SIGNED_BY_PATIENT_RECEPTIONIST_AND_DOCTOR
- RECORD_CONFLICT
- CANCELED_BY_PATIENT_IRRELEVANT_DOCUMENT

Participants : Patient - Receptionist

Asset: PatientIdentity

4. Patient Signups by filling all the fields and the asset **PatientIdentity** is created and given the state
    - As soon as the patient creates the identity , it is assigned the state:
        - **PatientIdentity → SIGNED_UP_IDENTIY**

5. Patient selects a health centre from a list of specified Health Centres and forwards a request for identity vetting to the Health Center
    - **PatientIdentity → FORWARDED_TO_RECEPTIONIST**

6. Patient visits the Health centre and reaches the counter and asks the receptionist for identity vetting, Customer brings his CNIC Card with him
    - If the patient has submitted the right information ,the asset transition is:
      PatientIdentity → VETTED
    - If the patient has submitted the right information ,the asset transition is:
      PatientIdentity → FAKE

Participants : Patient - Receptionist

Asset: DocumentRequest , Document

3. Patient visits the Document Request Forum ,selects the health centre, enters the MRN and the Date,**DocumentRequest** is created and a state is assigned to that asset:

   DocumentRequest → FORWARDED_TO_RECEPTIONIST

4. Receptionist gets a notification and sees a **DocumentRequest**, he/she checks the availability of the requested Document

   a. if the document is available and relevant . The Receptionist creates a document and the following state transitions takes place :
      - **DocumentRequest → FORWARDED_TO_DOCTOR**
      - **Document → SIGNED_BY_RECEPTIONIST**

   b. if the document is not available, the following state transition takes place:
      - **DocumentRequest→CANCELED_BY_RECEPTIONIST_UNAVAILABLE_DOCUMENT**

   c. if the document is available but not relevant, the following state transition takes place:
      - **DocumentRequest→CANCELED_BY_RECEPTIONIST_IRRELEVANT_DOCUMENT**

Participants : Doctor

Asset: DocumentRequest , Document

2. The doctor gets a notification for the request.

    a. If he/she finds the document to be Right according to his/her information,then the following state transitions takes place:

        DocumentRequest→FORWARDED_TO_PATIENT

        Document→SIGNED_BY_RECEPTIONIST_AND_DOCTOR

    b. If he/she finds the document to be Wrong according to his/her information,then the following state transitions takes place:

        DocumentRequest→CANCELED_BY_DOCTOR

Participants : Patient

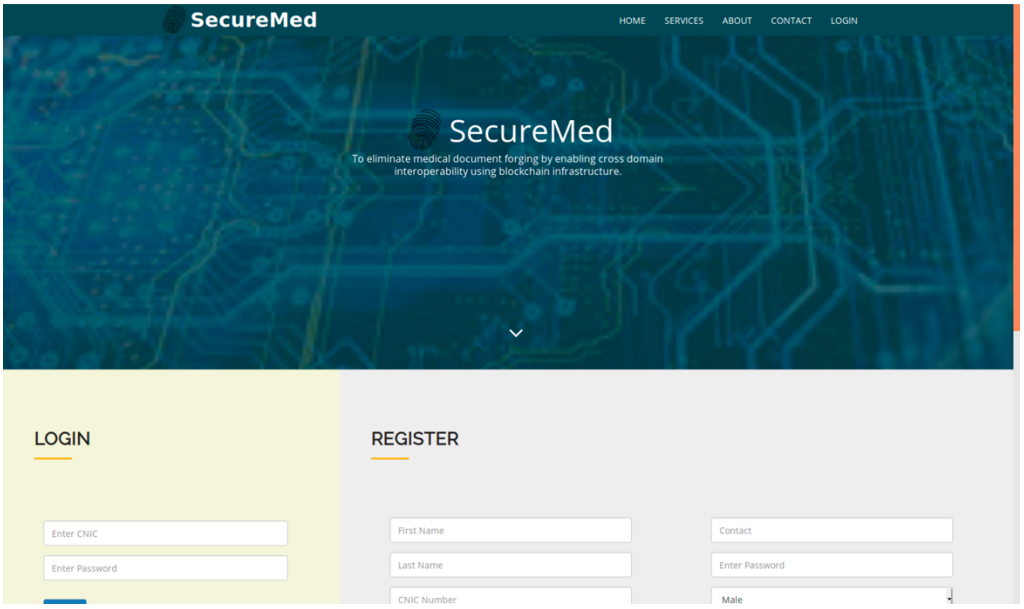
Asset: DocumentRequest , Document,Provider(Hospital Organization)

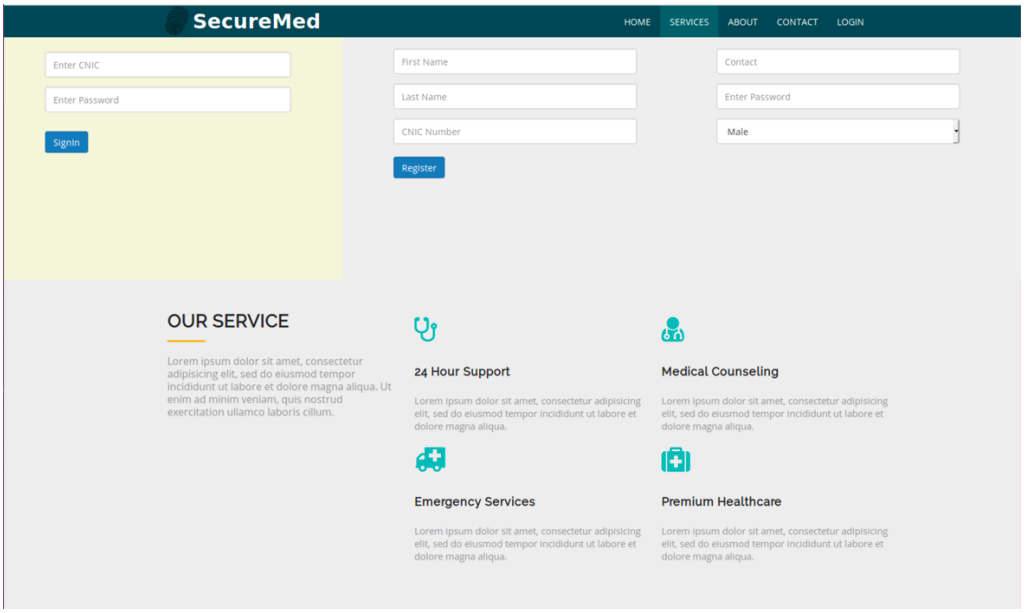
2. If all goes well, then the Patient receives a notification,validates with his copy and a copy of that document is forwarded to the Provided organization.
    a. If he receives the relevant document then the following state transitions take place:
        - **DocumentRequest → COMPLETED**
        - **Document→SIGNED_BY_PATIENT_RECEPTIONIST_AND_DOCTOR**

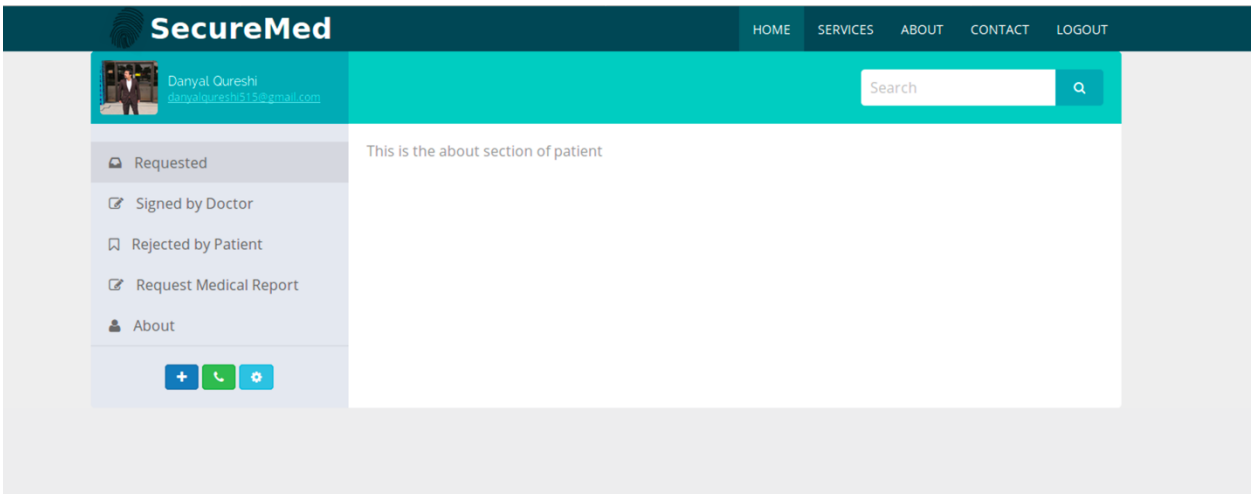
    b. If he receives the irrelevant or wrong document then the following state transitions takes place:
        - **Document→CANCELED_BY_PATIENT_IRRELEVANT_DOCUMENT**

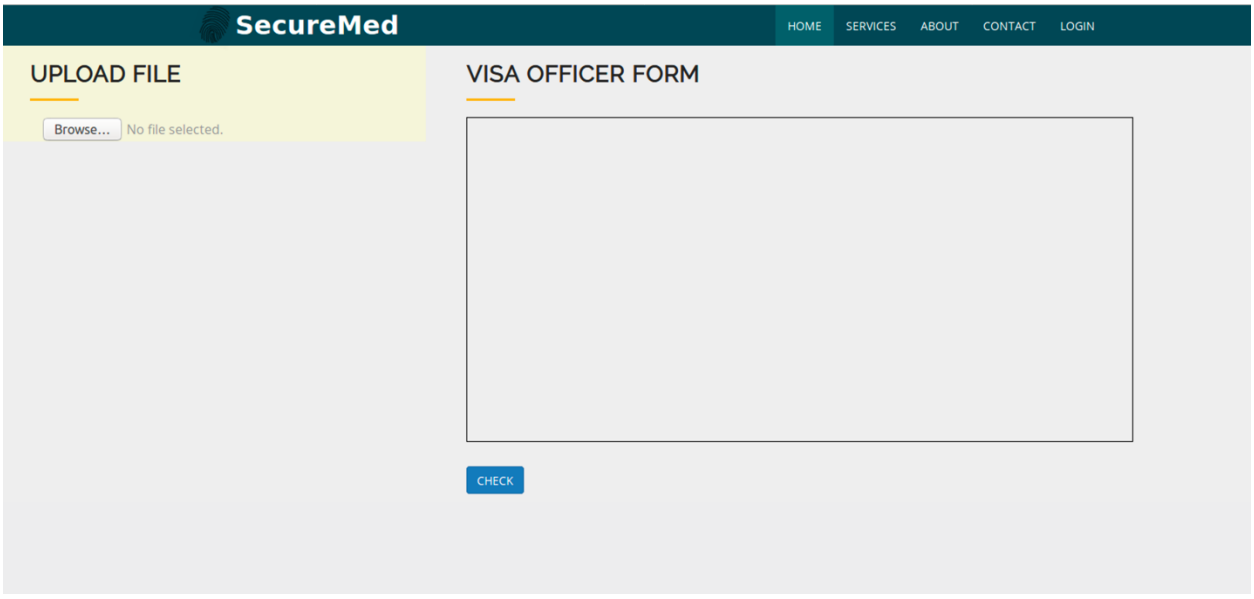
9.11. Graphical User Interface

Some screen shorts of our web application are following:

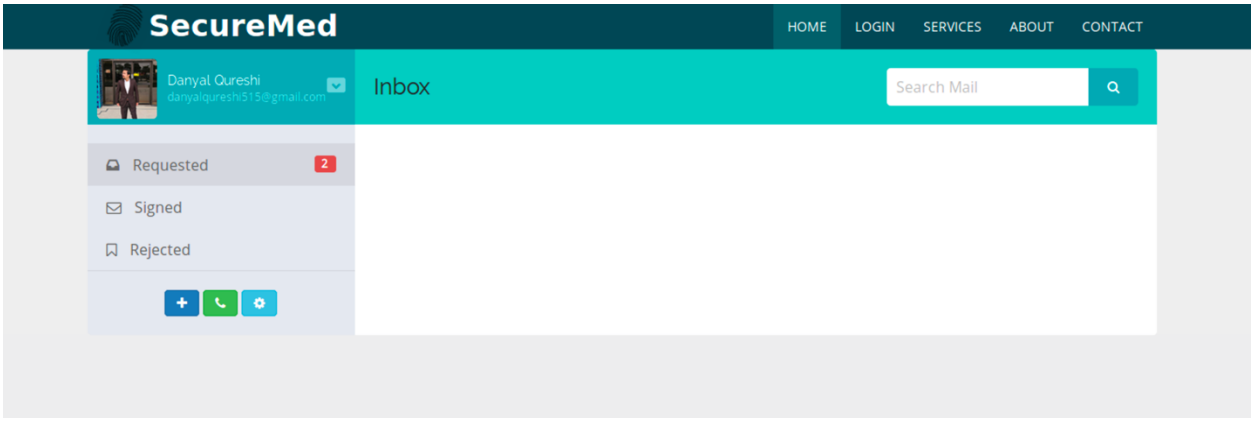





SecureMed
HOME
SERVICES
ABOUT
CONTACT
LOGOUT
Danyal Qureshi
danyalqureshi515@gmail.com
Search
Requested
Signed by Doctor
Rejected by Patient
Request Medical Report
About
This is the about section of patient


SecureMed
HOME
SERVICES
ABOUT
CONTACT
LOGIN
UPLOAD FILE
Browse...
No file selected.
VISA OFFICER FORM
CHECK


REPORTS
Report 1 - Signed
Report 2 - Declined
Report 3 - Pending
SIGN REPORT
SIGN
DECLINE


SecureMed
HOME
LOGIN
SERVICES
ABOUT
CONTACT
Danyal Qureshi
danyalqureshi515@gmail.com
Inbox
Search Mail
Requested
2
Signed
Rejected

SecureMed Blockchain Based Medical Document Sharing

ORIGINALITY REPORT

12%	3%	0%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Higher Education Commission Pakistan Student Paper	10%
2	legalbeagle.com Internet Source	1%
3	legaldictionary.net Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		