

BABEŞ–BOLYAI UNIVERSITY OF CLUJ-NAPOCA
FACULTY OF MATHEMATICS AND INFORMATICS
SPECIALIZATION: COMPUTER SCIENCE

Diploma Thesis

**E-me, the secure document-handling
application**

Abstract

**EZ AZ OLDAL NEM RÉSZÉ A
DOLGOZATNAK!**

Ezt az angol kivonatot külön lapra kell nyomtatni és alá kell írni!

**A DOLGOZATTAL EGYÜTT KELL
BEADNI!**

Kötelező befejezés:

This work is the result of my own activity. I have neither given nor received unauthorized assistance on this work.

2021

BALÁZS MÁRK

ADVISOR:
ASSIST PROF. DR. KOLUMBÁN SÁNDOR

BABEȘ–BOLYAI UNIVERSITY OF CLUJ-NAPOCA
FACULTY OF MATHEMATICS AND INFORMATICS
SPECIALIZATION: COMPUTER SCIENCE

Diploma Thesis

E-me, the secure document-handling application



ADVISOR:

ASSIST PROF. DR. KOLUMBÁN SÁNDOR

STUDENT:

BALÁZS MÁRK

2021

UNIVERSITATEA BABEȘ–BOLYAI, CLUJ-NAPOCA
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
SPECIALIZAREA INFORMATICĂ

Lucrare de licență

E-me, aplicația de gestionare securizată a documentelor



CONDUCĂTOR ȘTIINȚIFIC:
LECTOR DR. KOLUMBÁN SÁNDOR

ABSOLVENT:
BALÁZS MÁRK

2021

BABEŞ–BOLYAI TUDOMÁNYEGYETEM KOLOZSVÁR
MATEMATIKA ÉS INFORMATIKA KAR
INFORMATIKA SZAK

Szakdolgozat

E-me, a biztonságos dokumentum-kezelő alkalmazás



TÉMAVEZETŐ:

DR. KOLUMBÁN SÁNDOR,
EGYETEMI ADJUNKTUS

SZERZŐ:

BALÁZS MÁRK

2021

Contents

1	Introduction	3
1.1	About E-me	3
1.2	Similar applications in the field	3
1.3	Comparison	4
1.3.1	Similarities	4
1.3.2	Differences	4
1.4	Summary	5
2	User documentation	6
2.1	Introductory Pages	6
2.2	My Documents	7
2.3	Requesting a Document	8
2.4	Personal Information	9
2.5	Document Viewer	10
3	Implementation	12
3.1	Technologies	12
3.2	Architecture	13
3.2.1	Application/Backend layer	14
3.3	Security	17
4	Results and evaluation	18
4.1	Metrics	18
4.2	Decisions	18
4.3	Obstacles and difficulties	19
4.4	Possibilities	20
4.5	Retrospective	20

1. Chapter

Introduction

1.1 About E-me

A brief introduction of the application, 1-2 pages.

- general introduction
- why somebody would use this app
- the main features/selling points of the app

1.2 Similar applications in the field

A list of similar applications, their advantages and disadvantages, comparisons, 2-3 pages.

1. Google Docs

- create and edit documents
- sync between multiple devices
- view PDF docs/presentations
- upload and manage files

2. Documents to Go

- edit/view/create word, excel, PowerPoint docs
- supports password protection
- Google Docs support
- bi-directional sync

3. SecureSafe

1. CHAPTER: INTRODUCTION

- secure file and data storage
- double encryption
- secure AES-256 and RSA-2048 encryption
- https
- MFA with SMS
- send files up to 2GB to recipients

4. Quick Office Pro

- create/edit/share Microsoft Office files
- offline file access

1.3 Comparison

1.3.1 Similarities

- Similarly to the **SecureSafe** app, E-me uses AES-256 symmetric encryption standard to securely store and transfer documents.
- E-me allows users to upload their PDF documents.
- Users have quick and secure access to their data and files.

1.3.2 Differences

- E-me only supports PDF documents.
- E-me uses End-to-End Encryption over HTTPS to communicate with the clients.
- Users are able to **generate** their PDF docs using predefined templates filled out with their personal data.
- All PDF documents (**generated or uploaded**) will be verified for authenticity by the system administrators (later government) and will receive a digital signature to mark their authenticity.
- Authorities can request access to users' documents in order to verify their identity or other personal information (this access is temporary).

1. CHAPTER: INTRODUCTION

1.4 Summary

Describes the structure of the following document, 1 page.

2. Chapter

User documentation

Summary: *In this chapter E-me is described from a user point of view.*

The building blocks of E-me are pages. The primary role of these pages is allowing the user to manage their PDF documents that were created through the application. This management includes the ability to request a new document, view already owned documents, make modifications to them, delete the ones that are obsolete or contain incorrect data, or even share them with other devices using a QR code.

The secondary role is collecting the data from the user that is necessary for generating their documents. This data is then encrypted, processed and later on added to the documents that the user requests.

2.1 Introductory Pages

For an unauthenticated user there are 3 pages available in the application: Greeting, Login and Registration pages. Upon opening the application, the user is confronted with the Greeting page which allows them to navigate to the Login and Registration pages using the dedicated buttons.

The Registration page consists of five text fields. Each of these fields are required in order to create a new user, however only two of them are needed for authentication: Login name and Password. The restrictions for these fields are the following:

- The Email and Login Name fields should be unique.
- The Password and Confirm password fields should be identical.
- The Email field should be a valid email address.

Upon successful registration, the application navigates the user to the Login Page in order for them to authenticate themselves using the Login Name and Password they entered. If the authentication was successful, the main shell appears where three tabs can be seen: My Documents, Request Document and Personal Info.

2. CHAPTER: USER DOCUMENTATION

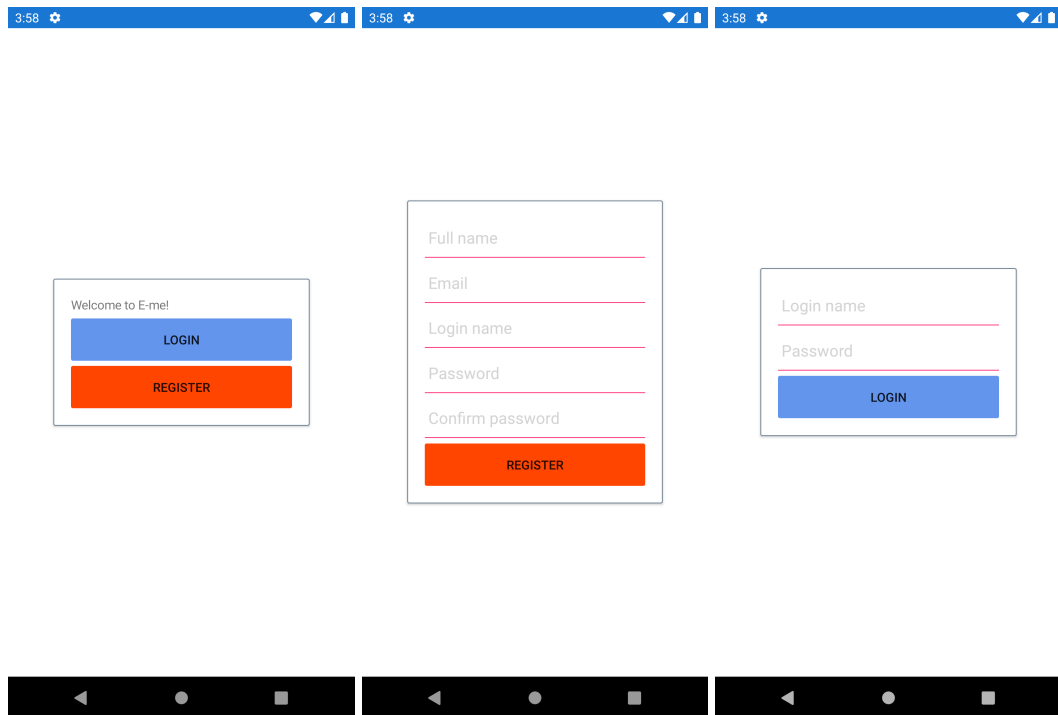


Figure 2.1: Introductory pages (Greeting, Registration, Login)

2.2 My Documents

The My Documents page consists of two main parts: the list of documents and the "Scan QR code" button. The list of documents allows the user to visualize what types of documents they own. On each document two actions can be performed: Share and Remove.

2. CHAPTER: USER DOCUMENTATION

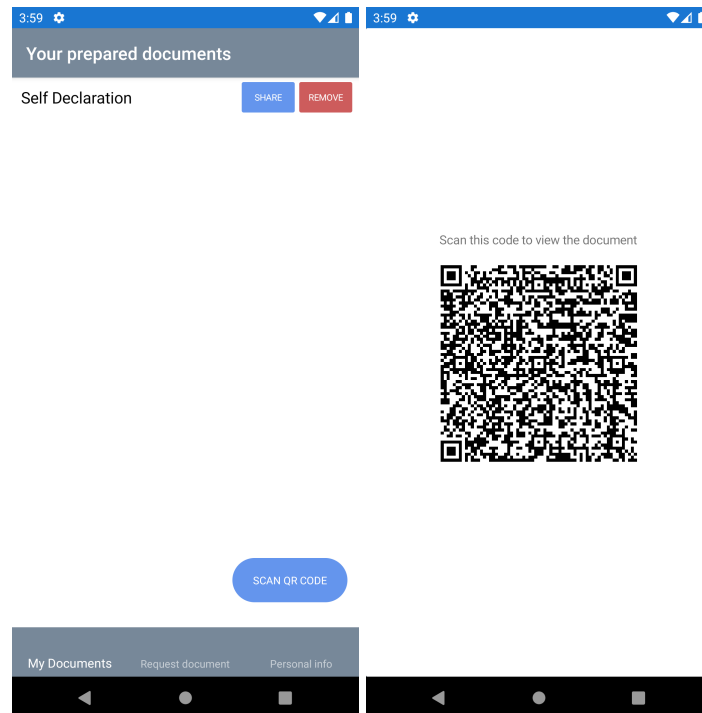


Figure 2.2: Documents and Share Document pages

Tapping the Remove button irreversibly deletes the document from the list. After a successful removal the user is able to request a new document of the same type. If the document template was modified since the previous request or the user modified their personal information, the resulting document may be different than the previously deleted one.

The Share button allows the user to safely transfer their selected document to a different device. Upon tapping the button, the application generates a unique code for the document which is then displayed on the screen via a QR code.

The code can be read using the "Scan QR code" button. Tapping this button will attempt to open the device's main camera in order to scan the code. If this feature is accessed for the first time, a prompt appears asking for the user's permission to use the camera. If the permission is granted, the application will open the camera app. Upon successfully reading a QR code generated by E-me, the selected document will appear on the screen (see [Document Viewer](#)).

2.3 Requesting a Document

The Request Document page consists of a list of document types that can be acquired by the user. The list only contains types that are not yet owned by the corresponding user. If the user acquires one of these document types, it will disappear from the list (it will be listed on the [My Documents](#) page instead).

2. CHAPTER: USER DOCUMENTATION

Combined with the [My Documents](#) page, these two lists contain every document type that can be managed through the application.

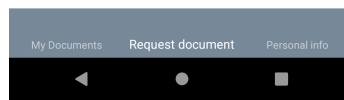
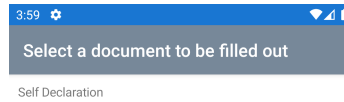


Figure 2.3: Request Document and Personal Information pages

The user can request a document by simply tapping on an item from the list. The requested document will be generated and automatically displayed on the screen (see [Documents Page](#)).

2.4 Personal Information

This page contains several fields containing the personal details of the user. Neither of these fields are required, however if no information is provided about the user, the application will not be able to automatically fill the requested documents. The information provided by the user on this page will be stored in an encrypted form.

2. CHAPTER: USER DOCUMENTATION

3:59

Personal Info

Full Name
Balazs Mark

Email
test2@test2.com

Birthdate
01/January/2000

Personal numeric code
1990702191292

Birth Country
Romania

Birth County
HR

SAVE

My Documents Request document Personal info

Figure 2.4: Request Document and Personal Information pages

Upon requesting a document, E-me attempts to match the fields of the document with the information of the user and fill them out respectively. Fields that require information that is not provided by the user will be left blank and can be filled manually on the **Document Viewer**.

2.5 Document Viewer

On this page a PDF Viewer can be seen which allows the user to inspect or even edit their documents. This viewer supports text searching, bookmarking, zooming, printing and/or saving a PDF to the local storage of the mobile device. The contents of the PDF are generated by the application, however if the document contains fields that could not be matched with any user data, the user is able to fill them out manually. This page can be closed by pressing the Back button.

2. CHAPTER: USER DOCUMENTATION

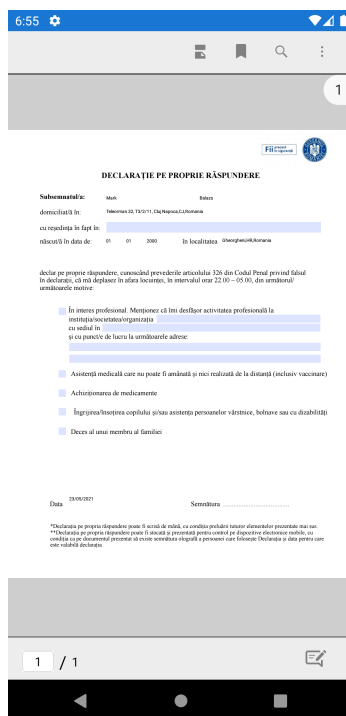


Figure 2.5: Document Viewer

3. Chapter

Implementation

Summary: In this chapter E-me is described from a technological standpoint.

3.1 Technologies

Here I list the technologies used for building the application with logos, descriptions for each, 6-7 pages.

– Backend

- * .NET 5
- * Entity Framework Core 5
 - Code-first
 - Microsoft SQL Server
 - additional Data Encryption layer
- * NSwag
- * Serilog
- * AutoMapper
- * Newtonsoft Json
- * Windows CNG (Cryptographic Next Generation) API

– Frontend

- * Xamarin Forms
- * Telerik UI for Xamarin
- * Telerik Document Processing Core
- * Syncfusion Xamarin PDF viewer
- * GoogleVision API - BarcodeScanner XF implementation

3. CHAPTER: IMPLEMENTATION

3.2 Architecture

E-me follows a commonly used N-tier architecture with three main parts: data, application (backend) and presentation (frontend) layers. Each of these tiers can be broken down into layers that are defined by their responsibilities within the application. This tier-based architectural approach adds modularity to the application which results in a low cost of change when compared to a single-tier structure.

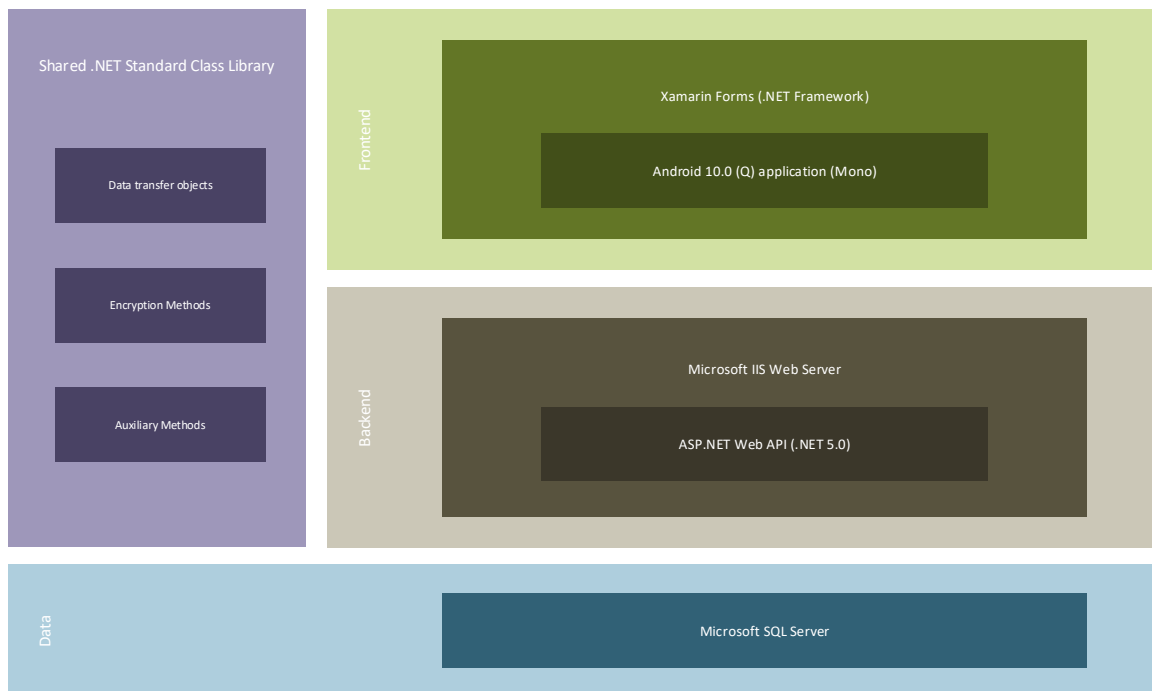


Figure 3.1: General architecture

Along with the low cost of change, the independence of the layers allows for future expansion of the application by means of multiple frontend platforms (ex. web applications, desktop applications), cloud storage/services and additional Web API's that can easily be integrated into the existing application. This, combined with the high compatibility of the .NET 5.0, provides a high level of scalability and maintainability for the application.

3. CHAPTER: IMPLEMENTATION

3.2.1 Application/Backend layer

The architecture of the application layer has a similar design approach to the general architecture. Consisting of 4 layers, the backend of the application follows the single-responsibility principle in its core. Because of its vertical structure, each layer is dependent on one single layer that is directly below it, providing a high level of maintainability.

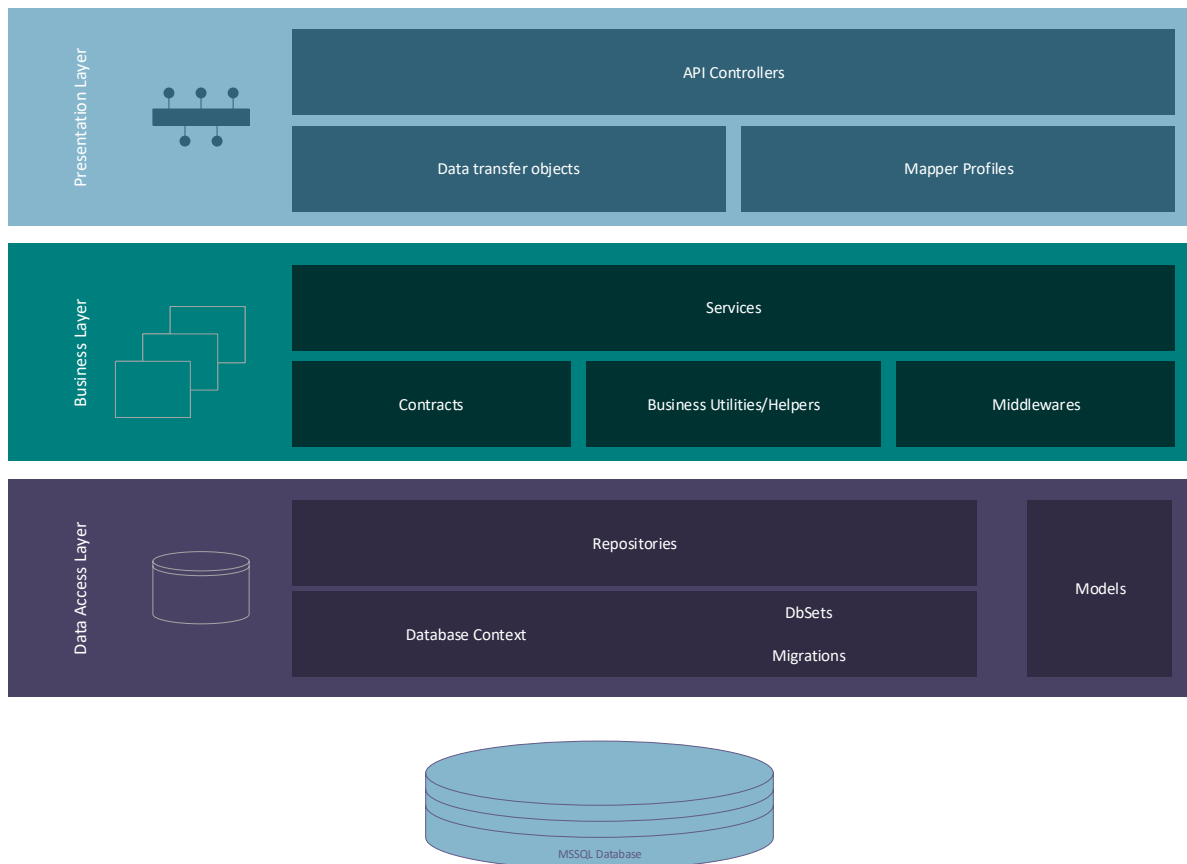


Figure 3.2: Backend architecture

3. CHAPTER: IMPLEMENTATION

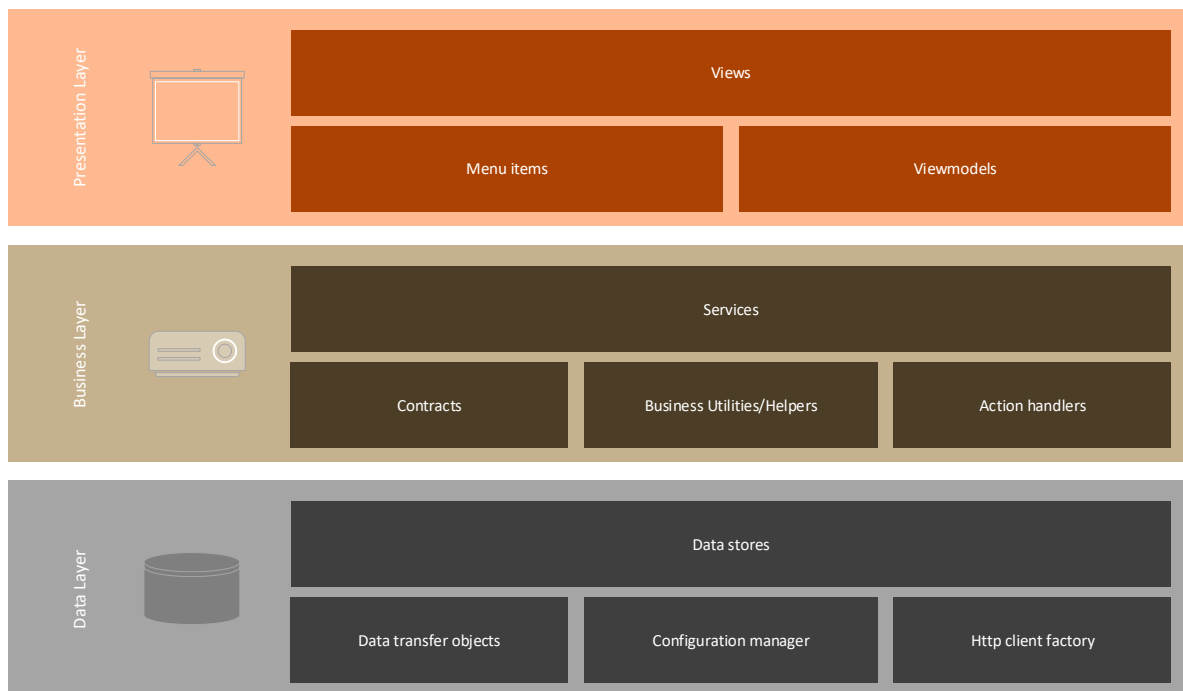


Figure 3.3: Frontend architecture

3. CHAPTER: IMPLEMENTATION

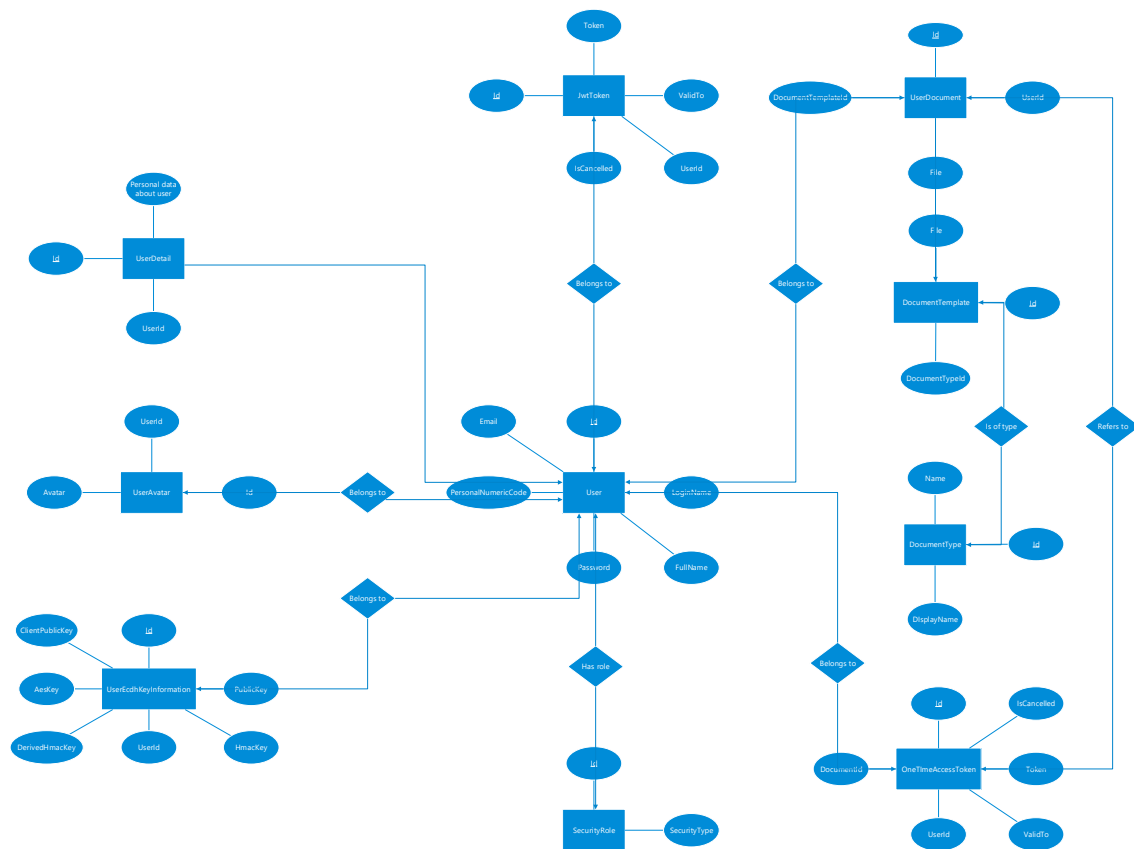


Figure 3.4: Model UML

- General 3-tier architecture
 - * diagram
 - * general description
- Backend multi-tier architecture
 - * diagram
 - * general description
- Model UML diagram
 - * diagram
 - * general description
- Frontend multi-tier architecture
 - * diagram

3. CHAPTER: IMPLEMENTATION

- * general description

3.3 Security

Here I describe the Diffie-Hellman key exchange and the used encryption techniques in more detail, 3-4 pages.

- data-layer security
 - * using built-in EF Data Encryption with AES256
- transport-layer security (TLS)
 - * https
 - * JWT auth and auth verification
 - * protected and unprotected endpoints
- End-To-End encryption
 - * Elliptic Curve Diffie-Hellman key derivation - open-source implementation
 - * encryption of documents
 - * hash-based message authentication (HMAC)

4. Chapter

Results and evaluation

***Summary:** In this chapter I describe decisions I made, difficulties I faced during development and the quality of my code.*

4.1 Metrics

In this section I will evaluate some of the algorithms used in the application, test coverage, code analysis. 4 pages

- chart about the duration of the encryption (time versus file size)
- service-level test coverage
- code metrics
 - * maintainability
 - * cyclomatic complexity
 - * average depth of inheritance
 - * average class coupling
- system requirements
 - * server
 - * mobile

4.2 Decisions

Here I describe decisions I made about what technologies to use, what I considered using and how they can be replaced with other ones. 3-4 pages

- backend

4. CHAPTER: RESULTS AND EVALUATION

- * Java
- * Python
- frontend
 - * Kotlin
 - * Java
 - * React Native
- why I chose C# and .NET instead of native languages
- Data storage
 - * MySQL
 - * MongoDB
 - * Oracle
 - * Firebase
- Auth technologies
 - * Cookie-based auth
 - * Multi-factor auth
 - * Biometric auth

4.3 Obstacles and difficulties

In this section I contemplate about different parts of the applications that were problematic to develop. 3 pages

- HTTPS on Android
 - * difficulties connecting to the server on HTTPS
 - * certificate issues
- Windows CNG not being implemented in Mono
 - * switching to the open-source ECDH implementation
- accessing resources within the Android secure storage (icons, config files etc.)

4. CHAPTER: RESULTS AND EVALUATION

4.4 Possibilities

Here I describe possible features, future upgrades for the app. 1-2 pages

- Adding biometric authentication
 - * fingerprint
 - * face recognition
- ML based form categorization
 - * categorize unknown fields based on user inputs
- Requirement-tree for documents
- digital signatures
- notifications (expired/soon-to-be expired documents)
- Administration application
 - * validating data
 - * granting permission for document release
 - * preparing templates
- IOS release

4.5 Retrospective

In this section I review the development process and describe what would I do differently and why. 1-2 pages