

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 | Similarities in the field | 3 |
| 1.3 | Contrast | 4 |
| 1.3.1 | Similarities | 4 |
| 1.3.2 | Differences | 4 |
| 1.4 | Summary | 5 |
| 2 | User documentation | 6 |
| 2.1 | Greeting Page | 6 |
| 2.2 | Registration Page | 7 |
| 2.3 | Login Page | 7 |
| 2.4 | Documents Page | 8 |
| 2.5 | Request Document Page | 9 |
| 2.6 | Personal Information Page | 10 |
| 2.7 | Share Document Page | 11 |
| 2.8 | Document Page | 12 |
| 3 | Implementation | 14 |
| 3.1 | Technologies | 14 |
| 3.2 | Architecture | 15 |
| 3.3 | Security | 15 |
| 4 | Results and evaluation | 17 |
| 4.1 | Metrics | 17 |
| 4.2 | Decisions | 17 |
| 4.3 | Obstacles and difficulties | 18 |
| 4.4 | Possibilities | 19 |
| 4.5 | Retrospective | 19 |

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 Similarities 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 Contrast

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 I describe the application from a user point of view.*

Here I describe the visuals of the application with images, 2-3 pages.

2.1 Greeting Page

The Greeting Page of the application consists of a frame containing a greeting message followed by two buttons: Login and Register.

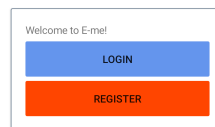


Figure 2.1: Greeting Page

These buttons allow the user to navigate to the Login Page and Registration Page respectively in order to authenticate themselves or create a new profile.

2. CHAPTER: USER DOCUMENTATION

2.2 Registration Page

The Registration Page consists of a frame containing the registration form and a submit button (Register). The form contains five text fields which can be filled out by the user:

1. Full name
2. Email
3. Login name
4. Password
5. Confirm password

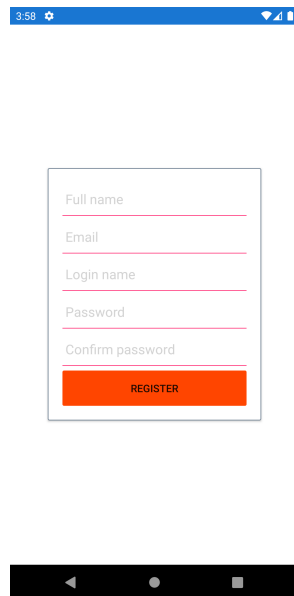


Figure 2.2: Registration Page

Every field is required in order to create a new user. Upon successful registration, the application navigates the user to the Login Page in order for them to authenticate themselves.

2.3 Login Page

The Login Page consists of a frame containing the login form and a submit button (Login). The form contains two text fields which can be filled out by the user:

1. Login name

2. CHAPTER: USER DOCUMENTATION

2. Password

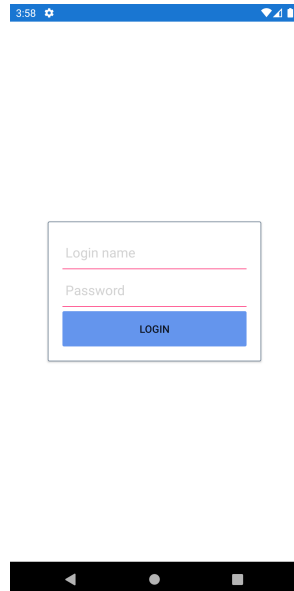


Figure 2.3: Login Page

Both fields are required in order to successfully authenticate a user. Upon successful login, the application navigates the user to the main tab menu where three tabs can be seen: My Documents, Request Document and Personal Info.

2.4 Documents Page

The 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. For each type the list contains the name of the document on the left and two buttons on the right: "Share" and "Remove".

The "Scan QR code" button is a rounded floating element on the bottom right of the page which is always visible.

2. CHAPTER: USER DOCUMENTATION



Figure 2.4: Documents Page

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, however 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 (see [Share Document Page](#)).

The code mentioned above can be read using the "Scan QR code" button. Tapping the 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 Page](#)).

2.5 Request Document Page

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 user. If the user acquires one of these document types, it will not be shown on this page anymore (it will be listed on the [Documents Page](#)).

Together with the [Documents Page](#), these two pages contain every document type that can be managed through the application.

2. CHAPTER: USER DOCUMENTATION

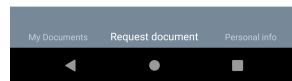
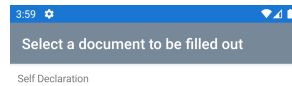


Figure 2.5: Request Document Page

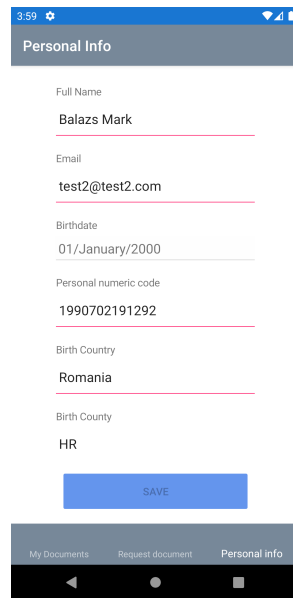
The user can request a document by simply tapping on an item from the list (this action removes the selected item from this list). The requested document will be generated and automatically displayed on the screen (see Documents Page).

2.6 Personal Information Page

The Personal Information Page consists of a form and a submit button (Save). The form contains multiple text fields, date pickers, masked textboxes that can be filled out by the user.

The submit button is located at the bottom of the page and is disabled until the user modifies at least one of the form fields.

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 2.6: Personal Information Page

The information provided by the user on this page will be encrypted and stored by the application. 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 Page.

2.7 Share Document Page

The Share Document Page contains a short hint followed by a QR code in the middle of the screen. The code contains information about the document which was selected to be shared.

2. CHAPTER: USER DOCUMENTATION



Figure 2.7: Share Document Page

The user can return to the **Documents Page** by pressing the Back button.

2.8 Document Page

The Document Page is a PDF Viewer that consists of three parts: header menu, content and footer menu. The header menu contains four icons for saving, searching, printing and bookmark browsing in the opened PDF document. The content part of the viewer is the PDF itself which was generated and filled out by the application. The footer menu contains information about the number of pages that the document has, but also a drawer menu with actions for editing the opened document.

2. CHAPTER: USER DOCUMENTATION

The screenshot shows a mobile application interface with a document page. At the top, there is a status bar with the time 6:55 and various icons. Below the status bar, there is a navigation bar with a back button, a search icon, and a page number 1. The document itself is titled 'DECLARAȚIE PE PROPRIE RĂSPUNDERE' and contains the following fields:

- Schimbare de loc:** A dropdown menu with the selected value 'Intermed 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000.

Figure 2.8: Document Page

If the document contains form fields that were not filled automatically by the application, the user is able to fill them out manually. The document can be closed by pressing the Back button.

3. Chapter

Implementation

Summary: *This is the summary of the chapter where I describe the general form-factors of the application 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

In this section I describe the architecture with multiple diagrams, 4-5 pages.

- 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
 - * 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

3. CHAPTER: IMPLEMENTATION

- * 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