

# Medicarium, securitatea și intimitatea datelor în contextul aplicațiilor mobile

Ghimpu Lucian Eduard

March 23, 2019

CONDUCĂTOR ȘTIINȚIFIC  
DR. CZIBULA ISTVAN, PROFESOR UNIVERSITAR

# Contents

<b>I</b>	<b>Partea teoretică</b>	<b>3</b>
<b>1</b>	<b>Introducere</b>	<b>4</b>
1.1	Introducere . . . . .	4
1.2	Ecosistemul aplicațiilor mobile . . . . .	4
1.3	GDPR . . . . .	4
<b>2</b>	<b>Autentificarea si înregistrarea</b>	<b>4</b>
2.1	Ceva introducere * . . . . .	4
2.2	Autentificare prin senzori biometrici . . . . .	4
2.3	JWT si OAuth2 . . . . .	4
2.4	Autentificare prin factori multipli . . . . .	4
<b>3</b>	<b>Comunicarea cu serverul si servicii (networking) *</b>	<b>4</b>
3.1	HTTP și HTTPS . . . . .	4
3.2	Alte canale de comunicare (SMS) . . . . .	4
<b>4</b>	<b>Persistența datelor</b>	<b>4</b>
4.1	Metode de persistare a datelor . . . . .	4
4.2	Criptografie . . . . .	4
4.3	Gestionarea datelor sensibile . . . . .	4
<b>5</b>	<b>Alți factori</b>	<b>4</b>
5.1	Permisuni . . . . .	4
5.2	Webviews . . . . .	4
5.3	Distribuirea aplicației . . . . .	4
5.4	Probleme specifice pe anumite platforme . . . . .	4
<b>II</b>	<b>Partea practică</b>	<b>4</b>
<b>6</b>	<b>Descrierea aplicației</b>	<b>4</b>
6.1	Problematica . . . . .	4
6.2	Funcționalități . . . . .	4
6.3	Arhitectura aplicației . . . . .	4
<b>7</b>	<b>Serverul si serviciile</b>	<b>4</b>
7.1	Tehnologii folosite . . . . .	4
7.1.1	Server REST . . . . .	4
7.1.2	Node.js . . . . .	4
7.1.3	MongoDB . . . . .	4
7.2	Rute disponibile . . . . .	4
7.3	Autentificare in doi pași . . . . .	4

<b>8</b>	<b>Clientul Mobil</b>	<b>4</b>
8.1	Tehnologii folosite . . . . .	4
8.1.1	Android Jetpack . . . . .	4
8.1.2	Kotlin . . . . .	4
8.2	Autentificarea . . . . .	4
8.3	Securitatea aplicației . . . . .	4
8.3.1	Gestionarea permisiunilor . . . . .	4
8.3.2	Gestionarea fișierelor . . . . .	4
<b>9</b>	<b>Manual de utilizare</b>	<b>4</b>
<b>10</b>	<b>Concluzii</b>	<b>4</b>
	<b>References</b>	<b>5</b>

## Part I

# Partea teoretică

## 1 Introducere

### 1.1 Introducere

### 1.2 Ecosistemul aplicațiilor mobile

### 1.3 GDPR

## 2 Autentificarea si înregistrarea

### 2.1 Ceva introducere \*

### 2.2 Autentificare prin senzori biometrici

### 2.3 JWT si OAuth2

### 2.4 Autentificare prin factori multipli

## 3 Comunicarea cu serverul si servicii (networking) \*

### 3.1 HTTP și HTTPS

### 3.2 Alte canale de comunicare (SMS)

## 4 Persistența datelor

### 4.1 Metode de persistare a datelor

### 4.2 Criptografie

### 4.3 Gestionarea datelor sensibile

## 5 Alți factori

### 5.1 Permisuni

### 5.2 Webviews

### 5.3 Distribuirea aplicației

### 5.4 Probleme specifice pe anumite platforme

## Part II

# Partea practică

## 6 Descrierea aplicației

4

### 6.1 Problematika

### 6.2 Funcționalități

### 6.3 Arhitectura aplicației

## 7 Serverul si serviciile

## References

- [1] ENISA, Privacy and data protection in mobile applications, 29.01.2019  
<https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applicat>
- [2] ENISA, Smartphone Secure Development Guidelines, 27.02.2017  
<https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016>
- [3] OWASP Mobile Application Security Verification Standard  
<https://github.com/OWASP/owasp-masvs>