1 INTRODUCTION 1

2 ABOUT TOKENS, OAUTH 2, AND OPENID CONNECT 3

2.1 Understanding OAuth2 and OpenID Connect 4

2.2 How OpenID Connect Generates Id Token 4

2.3 Types of Clients 5

2.4 OAuth2 and OpenID Connect Endpoints and Flows 6

3 SETTING UP IDENTITYSERVER4 AND UI 8

3.1 Installing UI for the IDP Application 15

4 CREATING A CLIENT APPLICATION 19

4.1 Regarding the API 22

4.2 Testing the Client Application 23

5 SECURING THE WEB APPLICATION 25

5.1 Configuring the IdentityServer to Use the Authorization Code Flow 27

5.2 Securing the Client Application with the Authorization Code Flow 28

5.3 Testing the Functionality 30

5.4 Inspecting Claims 33

5.5 Using PKCE (Proof Key for Code Exchange) 34

5.6 Login, Logout, and Additional User Info 37

5.7 Additional Claims 40

6 WORKING WITH CLAIMS AND AUTHORIZATION 42

6.1 Modifying Claims 42

6.2 Adding Additional Claims 44

6.3 Manually Calling the UserInfo Endpoint 47

6.4 Implementing Role-Based Authorization 49

6.5 Protecting Endpoints with Roles 53

7 SECURING THE WEB API 57

7.1 Implementing Web API Security 57

7.2 Providing an Access Token When Calling an API 61

7.3 Redirecting the Client to the Unauthorized Page 63

7.4 Using Policies to Secure The Application 64

8 HANDLING TOKEN EXPIRATION 69

8.1 Working with Token Lifetime and Expiration 69

8.2 Refreshing the Token 70

9 MIGRATING IDENTITYSERVER4 CONFIGURATION TO THE DATABASE WITH ENTITY FRAMEWORK CORE 76

9.1 Preparing Migrations for the IS4 Configuration 77

9.2 Creating Migrations 78

10 ASP.NET CORE IDENTITY INTEGRATION WITH EXISTING IDENTITYSERVER4 PROJECT 82

10.1 Integrating the ASP.NET Core Identity 83

10.2 Initial Migrations 85

10.3 Seeding the Users 87

10.4 Modifying Login and Logout Logic 90

11 USER REGISTRATION WITH ASP.NET CORE IDENTITY 93

11.1 Actions, View and ViewModel 93

11.2 Implementing Registration Action 96

11.3 Testing User Registration 99

11.4 Working with Identity Options 99

12 RESET PASSWORD WITH ASP.NET CORE IDENTITY 101

12.1 Using Email Service in the IdentityServer4 Project 101

12.2 Implementing Forgot Password Functionality 103

12.3 Implementing Reset Password Functionality 107

12.4 Testing the Solution 110

13 EMAIL CONFIRMATION 113

13.1 Preparing Email Confirmation Implementation 113

13.2 Implementing Email Confirmation 115

13.3 Testing Email Confirmation 117

13.4 Modifying Lifespan of the Email Token 119

14 USER LOCKOUT 121

14.1 Configuration 121

14.2 Lockout Implementation 121

14.3 Testing Lockout 123

15 TWO-STEP VERIFICATION 126

15.1 Enabling Verification Process 126

15.2 Two-Step Implementation 128

15.3 Testing Two-Step Verification 130

16 EXTERNAL PROVIDER WITH IDENTITYSERVER4 AND ASP.NET CORE IDENTITY 132

16.1 Getting ClientId and ClientSecret 132

16.2 Configuring External Identity Provider 135

16.3 External Provider Implementation 136

16.4 Testing 139