Contents

Foreword xi

Introduction 1

Chapter 1: Identity 9

What Are the Components of a Person's Identity? 10

So Where Does Privacy Fit In? 11

Where Do Roles Fit Into the Concept of an Identity? 16

Can I Have Multiple Identities in an Identity Management Environment? 17

Discussion Questions 19

Case Study 19

Chapter 2: Managing Identities andIdentity Stores 21

Identities and User Accounts 22

What Is an Identity Store? 23

Why Multiple Stores Are a Fact of Life 24

Strategies for Multiple-Store Environments 27

Managing Roles 30

Role Modeling 32

Delegated Administration and Self-Service 32

Discussion Questions 33

Case Study 34

Chapter 3: Directories 37

Schemas and Namespace Planning 38

The Power of a DIT 46

Issues to Be Aware Of 46

Authoritative Sources 47

Directory and Database Design 48

Virtual Directory 49

The "M" Word 51
Selecting a Configuration 52
Discussion Questions 55
Case Study 55

Chapter 4: Authentication and Access Control 57
Methods of Authentication 59
Levels of Authentication 64
Authentication Assurance Levels 65
Registration Assurance Levels 66
Access Control 67
Discussion Questions 72
Case Study 73

Chapter 5: Provisioning 75
The Mark of a Robust Process 76
Zero-day Start 78
Business System Issues 78
Workflow 81
The Role of Roles 81
The Benefits of Roles 83
Automating a Provisioning System 84
Sequential and Parallel Authorization 87
Discussion Questions 87
Case Study 88

Chapter 6: Role-Based Access Control 89
So What Is RBAC? 89
Why Is RBAC Important? 92
How Should RBAC Be Implemented? 95
Role Discovery 97
A Word of Caution 98
Discussion Questions 98
Case Study 99

Chapter 7: Single Sign-on andFederated Authentication 101
Single Sign-on for the Enterprise 102
Web SSO 105
Federated Authentication 109
Discussion Questions 114
Case Study 114

Chapter 8: Governance, Risk, and Compliance 115
HR Pattern-based Auditing 117
Pattern Reporting 118
Business Policies (IT Controls and SoD Rules) 120
Best Practices for System Cleansing and Auditing 121
Sample Graphs 123
Federated Authentication Auditing 126
Discussion Questions 127
Case Study 128

Chapter 9: Implementation and Roadmap 129
Getting Started 130
Setting Out 135
Physical Implementation 135
Typical Project Structure 136
Sample Roadmap 138
Navigating the Political Landscape 140
Challenges 141
Discussion Questions 146
Case Study 146

Chapter 10: Public Key Infrastructure 147
Why Do We Need PKI? 149
How Does PKI Work? 150
How Is PKI Used? 152
The Components 153
Key Generation 160

Certificate Management 160
Certificate Issues 161
Implementation Considerations 161
A Final Comment 165
Discussion Questions 166
Case Study 166

Chapter 11: Electronic Identity Smartcards 167
History 167
Interoperability 169
Privacy 170
Deployment Issues 171
An Ideal Platform 176
Discussion Questions 176
Case Study 177

Appendix A: Case Scenario 179
Background 179
The “As-Is” Situation 179
The “To-Be” Requirement 180
Constraints 181
System Descriptions 182
Data Repositories 185
Program of Work 187
Exercise 191

Appendix B: Standards 195
Directory Standards 195
Authentication Standards 196

Appendix C: Glossary 199

Appendix D: Public Key Cryptography Standards 203

Appendix E: X.509 Specification 205

Appendix F: Key Lengths 207