Beginning Information Cards and Cardspace

From Novice to Professional

■ ■ ■

Marc Mercuri

Apress®

Beginning Information Cards and CardSpace: From Novice to Professional

Copyright © 2007 by Marc Mercuri

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN-13 (pbk): 978-1-59059-807-8

ISBN-10 (pbk): 1-59059-807-5

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Jonathan Hassell
Technical Reviewer: Steven Woodward
Editorial Board: Steve Anglin, Ewan Buckingham, Gary Cornell, Jonathan Gennick, Jason Gilmore, Jonathan Hassell, Chris Mills, Matthew Moodie, Jeffrey Pepper, Ben Renow-Clarke, Dominic Shakeshaft, Matt Wade, Tom Welsh
Project Manager: Beth Christmas
Copy Edit Manager: Nicole Flores
Copy Editor: Kim Wimpsett
Assistant Production Director: Kari Brooks-Copony
Production Editor: Katie Stence
Compositor: Susan Glinert
Proofreader: Elizabeth Berry
Indexer: Becky Hornyak
Artist: April Milne
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail orders-ny@springer-sbm.com, or visit http://www.springeronline.com.

For information on translations, please contact Apress directly at 2855 Telegraph Avenue, Suite 600, Berkeley, CA 94705. Phone 510-549-5930, fax 510-549-5939, e-mail info@apress.com, or visit http://www.apress.com.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

The source code for this book is available to readers at http://www.apress.com in the Source Code/Download section. You will need to answer questions pertaining to this book in order to successfully download the code.

Contents at a Glance

Foreword xiii

About the Author xv

About the Technical Reviewer xvi

Acknowledgments xvii

Introduction xix

Before You Begin xxiii

CHAPTER 1 Introduction 1

CHAPTER 2. A Lap Around CardSpace 13

CHAPTER 3. The Laws of Identity and the Identity Metasystem 35

CHAPTER 4. The Identity Metasystem Beyond CardSpace:
A Look at Third-Party and Open Source Solutions 51

CHAPTER 5. Introduction to Adding CardSpace to Your Web Applications 69

CHAPTER 6. CardSpace with ASP.NET 2.0 Forms Authentication
and Membership 89

CHAPTER 7. Software + Services with CardSpace and the Windows
Communication Foundation 129

CHAPTER 8. Consuming Multiple Information Card–Secured Services
in Smart Client Applications 163

CHAPTER 9. Using CardSpace with RSS and OPML 185

CHAPTER 10. Security Token Services 217

CHAPTER 11. Managed Cards 243

CHAPTER 12. Automating Card Issuance with WF 299

CHAPTER 13. Resources for Supporting Information Cards in PHP,
Java, Ruby, and Perl-Based Relying Parties 345

CHAPTER 14. Personalization 365

CHAPTER 15. Information Cards and Personalization 381

INDEX 413

Contents

Foreword xiii
About the Author xv
About the Technical Reviewer xvi
Acknowledgments xvii
Introduction xix
Before You Begin xxiii

CHAPTER 1 **Introduction** 1

Authentication 2
Authorization 3
Authenticating Others 4
Personalization 7
Federation 8
The Seven Laws of Identity 9
The Identity Metasystem 10
Windows CardSpace 10
Summary 11

CHAPTER 2 **A Lap Around CardSpace** 13

Getting Started with CardSpace 13
    Making Sure You Have CardSpace Installed 13
    Creating and Using CardSpace and Information Cards 16
    Using Your Newly Created Card at Another Site 23
    Understanding That Personal Cards
        Are Not Accepted Everywhere 27
What Is Going on Behind the Scenes in These Interactions? 29
    Revisiting the Airline Counter Scenario 29
    Understanding Identity Providers and Relying Parties 30
    Looking at Identity Providers and Relying Parties in a
        Real-World Scenario 30

A Closer Look at Some of the Benefits of CardSpace 32
Passwords 32
Entering Basic Demographic Data at Each Site. 32
Separate Desktop 33
Visual Representation of *Your* Cards 33
Only the Names of the Claims Live on Your PC. 33
Summary 34

CHAPTER 3 The Laws of Identity and the Identity Metasystem 35

The Laws of Identity 36
Law #1: User Control and Consent. 37
Law #2: Minimal Disclosure for a Constrained Use 37
Law #3: Justifiable Parties 40
Law #4: Directed Identity. 40
Law #5: Pluralism of Operators and Technologies 41
Law #6: Human Integration 42
Law #7: Consistent Experience Across Contexts 42
The Identity Metasystem 43
Roles in the Identity Metasystem 43
Claims-Based Identities 44
The Microsoft Road Map for the Identity Metasystem 46
CardSpace on the Client 46
Information Cards on the Server. 48
Information Card Support in the Development Tools 48
Browser Support. 49
Summary 50

CHAPTER 4 The Identity Metasystem Beyond CardSpace: A Look at Third-Party and Open Source Solutions 51

Identity Commons 52
The Open Source Identity System (OSIS) 52
Eclipse Higgins 53
Bandit 53
Pamela Project 54

User-Centric Identity Without Information Cards 54
Shibboleth 54
Liberty Alliance 55
LID 55
OpenID 56
Yadis. 58
OpenID and Information Card Integration. 58
VeriSign PIP 61
PingTrust 61
Identity Selectors and Browser Support 62
Mozilla Firefox. 62
Apple Safari. 67
Summary 68

CHAPTER 5 Introduction to Adding CardSpace to Your Web Applications 69

Challenges Associated with Username and Passwords 69
Too Many Passwords 70
Phishing 70
Configuring the Server 71
Configuring the IIS 6 Environment 71
Configuring the IIS 7 Environment 71
Triggering the Identity Selector via ActiveX. 72
Triggering the Identity Selector via Binary. 75
Retrieving the Token 76
Retrieving Claims from the Token. 77
Taking a Closer Look at TokenHelper. 80
Confirming That CardSpace Is Installed 83
Summary 87

CHAPTER 6 CardSpace with ASP.NET 2.0 Forms Authentication and Membership 89

Installing the Database 90
Configuring Forms Authentication 92
The FormsAuthentication Class. 93
The Membership Class. 94

Configuring Standard Forms Authentication 95
Testing the Solution 97
Adding Support for Information Cards 99
Summary 127

CHAPTER 7 **Software + Services with CardSpace and the Windows Communication Foundation** 129

Windows Communication Foundation 129
Introduction to WCF 130
The ABCs of WCF 131
Service Hosting 131
Building an Application with WCF 131
Using CardSpace with WCF 144
Summary 161

CHAPTER 8 **Consuming Multiple Information Card–Secured Services in Smart Client Applications** 163

Enabling Token Caching 165
Setting Up the New Project 166
Creating the PolicyInfo Class 166
Creating a New ClientCredentials Class 171
Creating a New TokenManager 174
Creating the Custom Behavior Configuration Handler 175
Modifying app.config on the Client 176
Adding the Custom Behavior Extension 176
Adding the Actual Custom Behavior 177
Applying the Custom Behavior to the Endpoint 177
Testing the Solution with One Service 178
Testing the Solution with Two Services: Part 1 178
Testing the Solution with Two Services: Part 2 181
Summary 183

CHAPTER 9 **Using CardSpace with RSS and OPML** 185

Introducing the Formats 186
RSS 186
OPML 190
Atom 191

Building the RSS Service 192
Getting the Data Contracts. 192
Creating the Service Contracts 192
Creating the Services 194
Creating the Service Host 197
Populating the Configuration File 199
Building the RSS Reader 202
Creating Proxies for Your Services 202
Modifying the Configuration 202
Creating the User Interface 208
Testing the Solution 215
Summary 216

CHAPTER 10 Security Token Services 217

To Issue or Not to Issue 217
Exploring the Role of the STS 218
Taking a Closer Look at Microsoft's Simple-STS Sample 220
Getting the Bits 220
Exploring the Simple-STS Code 220
Looking More Closely at the Simple-STS Sample. 221
Extending the Simple-STS Sample 232
Authorizing Issuance of a Token. 239
Auditing the Relying Party 241
Summary 241

CHAPTER 11 Managed Cards 243

Thinking About Cards 243
Branding and Federation 244
To Issue or Not to Issue 245
Looking Inside an Information Card 246
Starting with Information Card Templates 250
Building a Card Template Creator. 250
Creating an Information Card Template 293
Creating a Managed Card 296
Summary 297

CHAPTER 12 **Automating Card Issuance with WF** 299

Introducing Workflow 299
Types of Workflow 300
Long-Running Workflows 300
Introducing Windows Workflow Foundation 300
Activities 301
Custom Code and Activities. 301
Workflow and Web Services 301
Workflow Types in Windows Workflow Foundation 301
Workflow Hosting 303
Runtime Services 304
Creating a Simple Workflow 305
Creating a Basic Custom Activity 307
Creating Properties for the Activity. 309
Creating Events. 310
Creating the Actual Activity Code 311
Creating Custom Activities for Information Card Issuance 314
Creating the CreateAndSignInformationCard Activity 315
Creating the LoadManagedCardTemplate Activity 318
Creating the RetrieveX509CertificateFromStore Activity 321
Creating the SaveInformationCardToFile Activity 325
Creating the SaveManagedCardTemplate Activity 327
Creating the SendEmail Activity 330
Creating a Sequential Workflow to Issue Information Cards 335
Summary 344

CHAPTER 13 **Resources for Supporting Information Cards in PHP, Java, Ruby, and Perl-Based Relying Parties** 345

The Sequence of an Information Card Exchange 345
Creating a Login Page 347
Java Relying Party Spotlight: xmldap.org’s Java-Based Relying Party 351
Getting the Bits 352
Creating the Java Servlet. 352
Reviewing the Servlet Code. 354

PHP Relying Party Spotlight: Kim Cameron’s Simple Information Card Demo for PHP 356
Getting the Bits 356
Requesting a Card 357
Processing the Token at the Relying Party 357
Additional Relying Parties 360
Java-Based Relying Parties 361
PHP-Based Relying Parties 362
Ruby on Rails-Based Relying Party 362
Summary 363

CHAPTER 14 Personalization 365

Introduction to Personalization 365
Personalization and the Long Tail 367
Personalization with CardSpace 369
Basic Personalization with a Self-Issued or Third-Party Card 369
Personalization with a Card and Purchase History 373
Personalization with a Card and Opt-in Profile Information 375
Summary 380

CHAPTER 15 Information Cards and Personalization 381

Registering for the StrikeIron Data Services 382
Creating the Website 383
Referencing the Services in the Personal Government Website 383
Adding a Reference to the ZipCodeInformation Service 383
Adding a Reference to the StateInformation Service 384
Adding a Reference to the SenatorInformation Service 385
Adding a Reference to the CountyWebSites Service 386
Adding a Reference to the CityWebSites Service 387
Adding a Reference to the CensusInformationForZipCode Service 388
Creating a Page to Collect the ZIP Code 389
Creating a Page to Display the Personalized Content 390
Testing the Solution 401
Adding Information Card Support 403
Summary 411

INDEX 413