

# Preface

---

In the past few years, identity has finally been receiving the attention it deserves.

With rampaging phishing and widespread cybercrime as the forcing functions, the industry as a whole is reacting with a concerted effort to understand what the best practices are and is getting there fast. We had the privilege of being among the first people concretely working on one of the key efforts of the identity renaissance: Windows CardSpace.

Windows CardSpace is an expression of the new user-centered approach to identity management. The new approach is poised to solve many different problems of diverse natures: There are technological considerations, such as offering better authentication mechanisms than passwords; usability considerations, such as guaranteeing that the user has a clear understanding of what is going on; and even social-science considerations about how we can effectively leverage trust relationships and make obvious to the common user the identity of the website being visited.

That is the reason why explaining Windows CardSpace in just a few words is so challenging. Depending on your background

and your role, you will be interested in a different angle of the story. We experienced this fact countless times in the past two years: with customers and partners, at conferences, with the press, with colleagues from other groups, and even with spouses, trying to explain what was that super important thing that kept us late at the office.

We believe that user-centered identity management has the potential to change for the better how everybody uses the Internet. We also believe that the best way of reaping its benefits is to develop a deep understanding of the approach, complemented by hands-on knowledge of supporting technologies such as Windows CardSpace. The book you are holding in your hands has the goal of helping you to gain such insights.

We live in exciting times. The entire industry is moving toward a common solution, with a true spirit of collaboration and a strong will to do the right thing. The discussion is open to anybody who wants to participate. We hope that you will join us!

## **Book Structure, Content, and Audiences**

---

Windows CardSpace is part of a comprehensive solution, the Identity Metasystem, which tries to provide a solution to many security-related bad practices and widespread problems. CardSpace is also a very flexible technology that can be successfully leveraged to address a wide range of different scenarios and business needs. Finally, Windows CardSpace enables new scenarios and radically new ways of dealing with known problems. Given the sheer breadth of the areas it touches, it comes as no surprise that people of all positions and backgrounds are interested in knowing more about it.

To address so many different aspects and such a diverse audience, we divided the book into three parts.

## Part I: Setting the Context

---

The first part of this book introduces you to user-centered identity management, the model on which Windows CardSpace is based. This part lays the foundation for understanding the context in which CardSpace is meant to operate and the problems it has been designed to overcome. Architects, analysts, and even strictly nontechnical folks will get the most from this part. There are practically no assumptions of prior knowledge; the text introduces the necessary concepts and technologies as needed. Note that in the first part CardSpace is barely mentioned because the focus is on the underlying models and considerations that are purely platform-agnostic.

Chapter 1, “The Problem,” explores the problems with identity management today. It explores how authentication technologies evolved into the current practices, showing the historical reasons for current widespread problems. The chapter introduces basic concepts such as Internet protocols, types of attacks, introductory cryptography, authentication technologies, and so on.

Chapter 2, “Hints Toward a Solution,” presents the current thinking about what the ideal authentication system would look like. The seven laws of identity are described in great depth. The Identity Metasystem is introduced, and its compliance with the identity laws is explained in detail. This chapter also provides a basic introduction to advanced web services and highlights how the abstract concepts in the Identity Metasystem map to concrete features in the web services set of specifications.

By the end of Part I, you will have a comprehensive view of the situation: what the problems are we are wrestling with, why they are here, and how the Identity Metasystem can solve them. You will also understand the role of Windows CardSpace in the big picture.

## **Part II: The Technology**

---

Part II focuses on Windows CardSpace from a technological standpoint. It describes the technology, the elements and artifacts it entails, the operations and development practices, and the most common usage scenarios. This part is for the developer or whoever wants to have hands-on experience with Windows CardSpace.

Chapter 3, “Windows CardSpace,” introduces the technology. This includes the user experience, Information Cards and the different card types, the private desktop, and the canonical usage scenario.

Chapter 4, “CardSpace Implementation,” describes the usage of CardSpace in the most common scenarios. From the HTML integration syntax to token manipulation, going through federation, integration with web services and CardSpace invocation via native APIs, this chapter covers all the basic development tasks.

Chapter 5, “Guidance for a Relying Party,” presents a detailed example of a common scenario: enabling Personal Cards on an ASP.NET website.

## **Part III: Practical Considerations**

---

The last part of this book is devoted to design and business considerations that come in handy when architecting a solution based on Windows CardSpace (or on user-centered identity management technologies in general). The chapters in this part will prove useful for architects and project managers. Business decision makers and IT managers will probably be interested in some of these considerations, too. Hints for developers are spread throughout the text.

Chapter 6, “Identity Consumers,” presents some thoughts about deciding to be or to use an identity provider. It also looks at things from the viewpoint of being a relying party: for example, the main effects on your business and operations of accepting identities in form of tokens and from third parties, and the opportunities you want to take advantage of and the caveats you want to avoid.

Chapter 7, “Identity Providers,” lists some considerations to keep in mind when becoming an identity provider.

## **Conventions**

---

This book follows the conventions of the Independent Technology Guides series. Analysis sections appear in boxed sidebars and give you added perspective on the issues and technologies being discussed. Also, margin notes are included throughout the chapters summarizing or pointing out the most important points.

Code-continuation characters are occasionally used in lines of code when we’ve broken lines to fit the printed page. Lines broken by code-continuation arrows should be entered as one line when programming.