CHAPTER 1

Introduction

Over the past year, I've spent a significant amount of time working with enterprise customers interested in leveraging the .NET Framework 3.0 in their businesses. Specifically, I've worked with them on architecting systems that leverage Windows Workflow Foundation (WF), Windows Communication Foundation (WCF), and Windows CardSpace.

My focus has been global in scope, with multiple visits throughout the United States and Western Europe. As you might have guessed, I traveled by air for all of these trips, and as I traveled to Boston, New York, Tulsa, London, Paris, and Munich, I encountered many differences—airlines, countries, food, and languages. But there was one commonality on every trip—the need for me to prove my identity.

If you've traveled by plane before, you're familiar with the check-in process. You approach the ticket counter for your airline, and you provide a paper ticket (if you have one) or identify that you have an e-ticket. At that point, the clerk asks you for identification.

If I were to respond with "My name is Marc Mercuri. I live in Washington state in the United States." The response from the clerk would surely be "That's very nice, Mr. Mercuri. Now can you provide some identification?" In this particular situation, my self-assertion of who I am is not acceptable to both the airline and the government of the country I'm in. This particular scenario, like many others we encounter in the real world, requires that we provide some form of documentation that was supplied by someone who the recipient knows, who has an established reputation, and with whom the recipient has an established level of *trust*.

The same is true for a number of scenarios, such as attempting to purchase liquor, obtaining entry to a secured building, or obtaining credit from a financial institution. These types of interactions are of high value and/or of considerable risk. In scenarios where there is risk, value, or a combination of the two associated with a transaction, my identity is less about how I identify myself and really more about what others say about me.

Now, this is not true of all scenarios. If, at a cocktail party, I were to meet you and you asked me who I was, I could respond with "My name is Marc Mercuri. I live in Washington state in the United States." Your reaction would be considerably different from that of the airline employee. You'd likely think I was awkwardly formal for a cocktail party, but aside from that, you would likely accept my self-asserted identity. No risk or value is attached to the introduction. If you think about it, self-asserted identity is valid in a number of everyday scenarios. For example, you're not asked for a government-issued ID when identifying yourself at a dry cleaners or when making a reservation at a restaurant.

If you look at the online world, unless money is involved, websites are primarily based on self-asserted identity. Whether it's your free online email account, your account for your favorite sports website, or comments you make on a blog, your statements of identity are accepted at face value.

This chapter will cover some fundamental topics around identity, such as authentication, authorization, and federation. In addition, you will be introduced to topics such as personalization, the Laws of Identity, the identity metasystem, and Windows CardSpace, all of which are covered in depth in later chapters.

Authentication

Going back to the air travel scenario, why does the clerk at the airline counter trust what someone else says about me more than what I tell her? Well, when I provide certain types of ID, the airline is confident that my claims are authentic because they are made by an authority the airline trusts.

With regard to identity, *authentication* is the process by which an individual or entity is deemed to be who he/she/it is.

One of the acceptable forms of identification for an airline is typically a driver's license. If one looks at the driver's license, it contains several key *claims* about its owner, including name, address, date of birth, gender, height, weight, and eye color. The driver's license also typically contains a photograph.

Now you might think that the authentication occurs when the picture is examined and then compared to the person presenting it. But the claims are not believed just because a picture is present; the claims are considered authentic because they were issued by the state's Department of Motor Vehicles. The license was issued by an organization that the airline has chosen to *trust*.

There is a level of confidence at the airline that the Department of Motor Vehicles has processes in place that authenticate the individual. As you apply for the license in person, the clerks at the Department of Motor Vehicles can validate certain physical claims as authentic—height, gender, approximate age, and so on. For the claims beyond those that can't be seen with the naked eye, the agency depends on the authentication done by other entities that *the Department of Motor Vehicles trusts*.

To authenticate your claims, the Department of Motor Vehicles typically requests up to two types of other forms of identity, such as a birth certificate issued by a hospital or city where you were born that confirms your age, a utility bill that has an address that matches the one on your driver's license application, and so on.

Therefore, for every trip you take on an airline, the airline authenticates your identity based on claims authenticated by a trusted third party, but it actually goes much deeper than that. In reality, a successful interaction is really based upon a *chain of trust*.

As someone who travels quite a bit, I need to withdraw funds from my bank account while away from home. To withdraw funds from this bank account at a physical location from a bank teller, I am required to provide a form of government-issued identification, such as a driver's license. But I rarely have the opportunity to perform a withdrawal from a physical bank location. Instead, I withdraw funds primarily with the assistance of automated teller machines (ATMs).

To utilize these machines, my bank has provided me with a card that has a magnetic stripe. This card contains information about me, typically the information that is visible on the printed card such as my name and account number. When I want to withdraw funds, I insert my card

into an ATM, where I am then challenged to present my personal identification number (PIN). In this case, the combination of the presence of the physical card (and the information contained within it) and my knowledge of the PIN is used to authenticate me. This is referred to as *two-factor authentication*.

Authorization

Authentication is typically a prerequisite to authorization. Authentication establishes my identity; *authorization* establishes what resources that identity can access and what actions that identity is allowed to perform.

In the case of air travel, your identity is authenticated with a government-issued ID, it is compared against the information on your plane ticket, and you are then authorized to board the plane and access the seat specified on your ticket.

On most planes, seats are available in what is called the *exit row*. This is a row on the plane located next to the emergency exit. Children are not allowed to sit in this row. If my seat assignment on the plane were for a seat within the exit row, the airline representative would check the claim of age on my driver's license or passport. Because I am older than 18, I would be authorized to sit in this row.

In the exit row scenario, this is an example of authorization based on age. There are many examples of this type of authorization. For example, if I attempt to purchase liquor or cigars in the state of Washington in the United States, the salespeople in each store I visit would request identification and validate I was at least 21 or 18 years of age, respectively.

As I mentioned earlier, I spent a good portion of the past year traveling. As a result, many times I was not home when a shipping company attempted to deliver an order from an online store. As a result, I needed to go to the company's facility to retrieve the package. Now because I was picking up the package at the shipping company's facility, the company needed to guarantee that the package was being delivered to the right party. To validate this, a representative inspected the claims on my driver's license. The combination of name, address, and picture authenticated me, and I was then authorized to receive this specific package.

Thus far, you've learned about authorization based on a form of identification provided by a government agency. There are a number of scenarios where you're given a token by a third party to identify yourself that authorizes you to access a resource from that party.

Let's look at an example of this. If you go to a restaurant or a nightclub, you'll often see a coat check, which provides patrons the opportunity to drop off their coat and retrieve it later in the evening. When you leave your coat, you're typically given a small plastic or other type of token. Although your government-issued identification has a robust number of personalized claims about who you are, this plastic token contains a single claim—a number. A corresponding token with that number is attached to your coat in the coat check closet. At the end of the evening, you present your token to the individual working in the coat check, and that token authorizes you to access the coat that has the same number.

In the preceding examples, the authorization rules have been fairly straightforward, but many times, authorization requires processing a set of business rules. These rules utilize the claims provided on the ID presented. For instance, if I attempt to enter a building at Microsoft, I must present my employee ID. The employee ID is then cross-referenced to determine whether I have access to that particular building on that particular day at that particular time. I might be authorized to access a building from 8 a.m. to 5 p.m. from Monday to Friday, but not at 10 p.m. or on Saturdays.

Authenticating Others

So far, you've seen scenarios where I have been proving my identity to others. But what about others proving their identity to me? In the real world, this is simple enough. If I were to interact with a bank, it would have a physical location, and that location would have a number of physical factors used to validate its authenticity. From signage to ATM machines to branded deposit slips and product literature to employees with name tags to the drive-through teller window—an abundant number of elements can help validate that the entity is indeed what it claims to be. Those physical representations are not, unfortunately, available when engaging with an entity online.

On average, I receive several emails a day from a large online payment company. The email states that there is an issue with my account and that I must go to the website to resolve an issue; for my convenience, a link is provided to the site. Figure 1-1 shows a sample email.

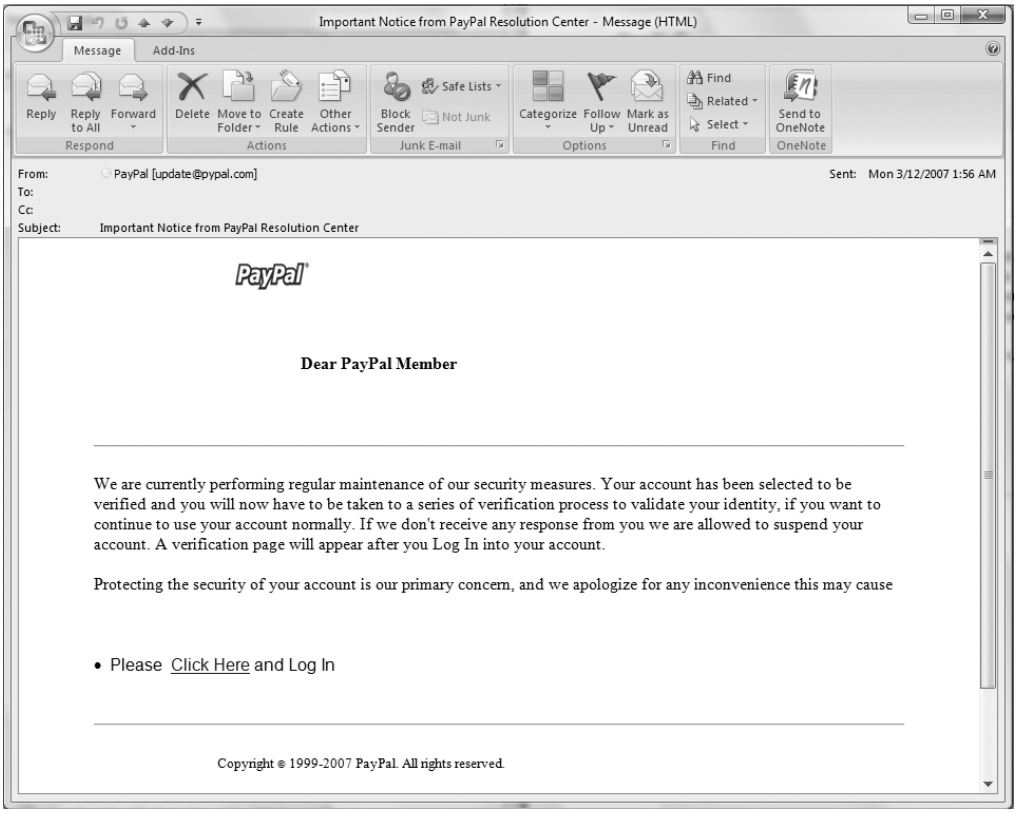

Figure 1-1. *Email from an "online payment site"*

I click the link and am taken to a site that looks identical to the website for the real payment provider, as shown in Figure 1-2. But as you might have guessed, it isn't.

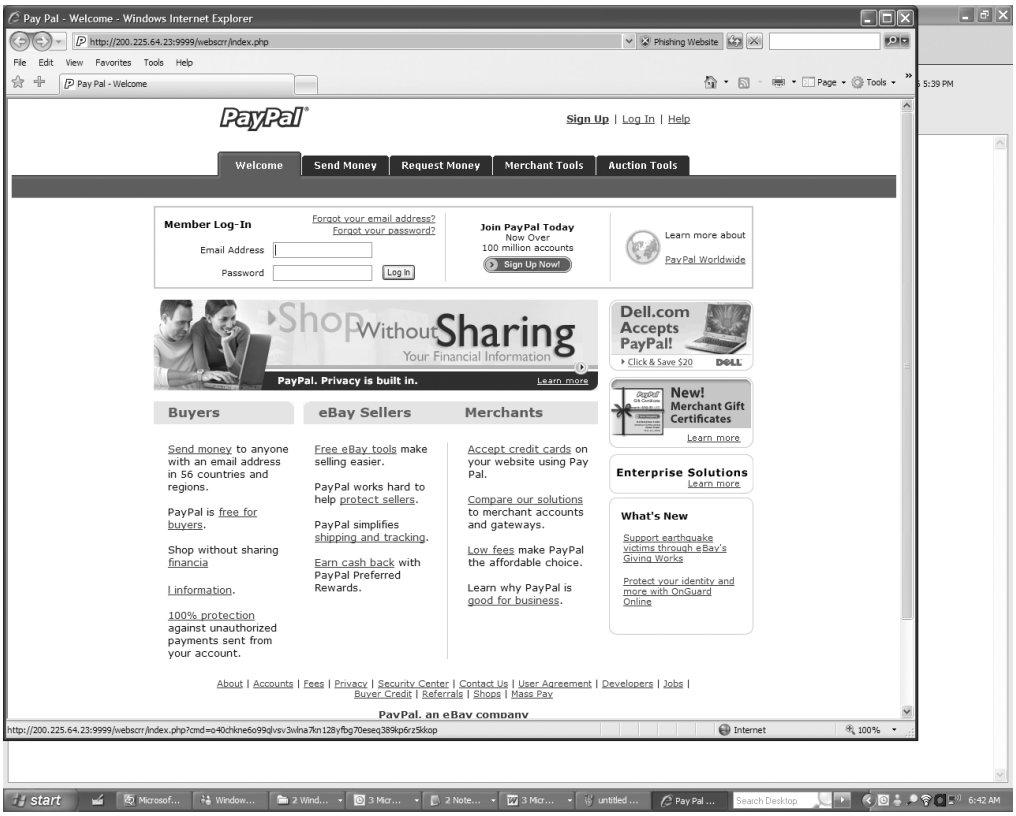

Figure 1-2. *The site at the other end of the link*

The email and site are part of a malicious attempt to gain the information to authenticate to my account on that site. If they managed to steal my identity with their fake site, they could then use my identity on the real one. With this identity, the thief could authenticate to the real site and be authorized to any funds I have in the account.

■ **Note** The payment provider the attacker is targeting here is just an example. I also get emails about "my" accounts at many large, well-known banks.

There's an old adage that states, "He who has the gold makes the rules." When it comes to usernames and passwords, the user is attempting to access a resource. That resource is analogous to gold; it's something we desire to access. The site or service, therefore, sets a rule that you must provide both a username and a password to access it. These two data elements are a shared secret with the site.

To prove my identity, I must share these with the site to prove who I am. Unfortunately, the site does not necessarily do the same. As discussed earlier, in the real world if I were to go to a bank, I could discern whether it was indeed a bank by a number of physical factors. This is not the case in an online scenario, and it is fairly trivial to duplicate the look and feel of a third

party's website. Because most people use the web page similarities in graphics and layout to verify a site, it increases the likelihood of inadvertently sharing your secret—your username and password combination—with someone other than the real site.

Because of the potential of leveraging this type of attack for financial gain, it has moved beyond hackers to criminal syndicates who steal significant sums from the unsuspecting. This type of attack is called *phishing*, and according to Gartner, these types of attacks are growing at a rate of 1,000 percent per year.

What's worse is that the people perpetrating these attacks know that end users have password fatigue. It's unrealistic that an individual will remember unique usernames and passwords for every site on the Web they visit, and a number of patterns have emerged on how people manage their usernames and passwords.

My colleague Steven Woodward has identified four categories of users:

- Individuals who use a single username and password across all sites
- Individuals who use a pool of several usernames and passwords across all sites
- Individuals who use an attribute of a site to hash a username and password from a standard key
- Individuals who maintain a password-encrypted Microsoft Excel spreadsheet with 100+ usernames and passwords and where they use them

Hackers have recognized the first two patterns and have evolved their attacks such that the fake version of a site will respond that the username/password entered is not valid. In most cases, users of the site will enter another of their username/password pairs. The fake site will continue to collect the username/password pairs until the user enters the same username/password—at which point it redirects the user to the real site. At that point, the criminals behind the fake site have quite possibly stolen all your identities for multiple sites.

In credit card fraud, the consumer has little to no liability for fraudulent purchases made with a stolen credit card. Unfortunately, that is not the case when a criminal logs into your bank account after having authenticated to the site using your username and password. There are numerous cases where individuals have lost tens of thousands of dollars as a result. These cases are becoming well publicized and lowering consumer confidence.

Some application vendors have taken it upon themselves to add protections for customers against these types of attacks. For example, I'm using Microsoft Outlook 2003 and Internet Explorer 7, and these two applications have a number of antiphishing mechanisms that help me identify the site shown in Figure 1-2 as a fake. Outlook initially sent the email to my Junk Mail folder. Within the Junk Mail folder, it turned the link off, and I explicitly had to turn it back on to click it. Internet Explorer 7 identified the site as a phishing site and strongly suggested I not continue. Even after continuing, it turned the address bar in the browser to red indicating a concern about the site. In Outlook 2007, this functionality is extended, such that the URLs are expanded to provide further opportunity to determine whether a link is an attempted phishing attack.

But some people might not be using Outlook; they might be using Lotus Notes. Others might not be using Internet Explorer 7 but instead either an earlier version or another browser such as Opera or Firefox. Although Outlook and Internet Explorer 7 made it difficult to get to this site, this might not be the case in these other scenarios.

So in those cases, someone might make it through to the site unwarned. For the untrained eye, these emails and sites look genuine, and as a result people enter their usernames and passwords.

Although a trained eye can pick up on the signs such as that the email was sent via blind carbon copy (BCC) and that the website is located at an IP address vs. a domain, even the best-trained eyes can be vulnerable. I know of at least one senior person in the identity space who was checking his email late one night, was a bit tired, and fell prey to a phishing attack.

Personalization

Identity can provide more value than just authentication and authorization; it can also provide the means by which to deliver a rich, personalized experience. By allowing an application or website to know certain characteristics of who I am, the site can provide a more one-to-one engagement with me.

Amazon is a recognized leader in the personalization space. Once you've been authenticated and are logged into its website, Amazon utilizes the demographics in your account and combines them with your purchase history to provide a customized experience.

As you can see in Figure 1-3, Amazon has a Marc's Store tab based on what Amazon knows about me—a combination of my expressed and implied identity. Essentially, Amazon has provided me with a personalized store. Because I've purchased several books about identity as research for this book, you can see that the Marc's Store tab consists of a number of books about identity and privacy.

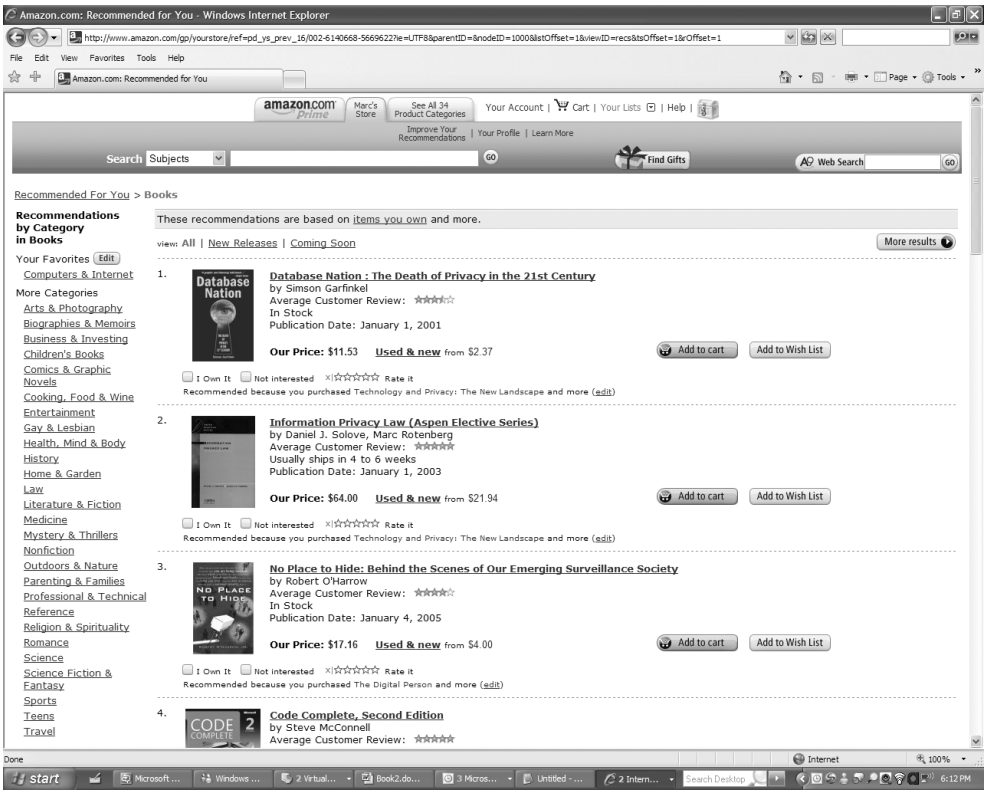

Figure 1-3. *Amazon's "my" store*

Rather than have me peruse a huge online warehouse of books, Amazon has presented just a subset of those it thinks I might be interested in. Historically, this has worked well for both Amazon and me. I've made numerous purchases based on recommendations—and have been happy with the recommended products.

Personalized experiences are most obvious in retail, but they truly span all vertical markets. Regardless of whether you're looking to sell more or make your site "stickier," the ability to personalize a site based on user information can help you get there.

In this book, you'll look at how individuals are doing personalization today and how Windows CardSpace can enable personalization in several scenarios. Also, the book includes a stand-alone project that shows a robust sample that includes personalization as a key piece.

Federation

One of the definitions of the word *federation* is "an organization formed by merging several groups or parties." In reference to identity, federation translates to an ability to share a single identity across multiple sites.

Imagine a business scenario involving a bank and a corporation. If the bank has a partnership with the corporation, there will undoubtedly be an interest in sharing resources between the two companies.

To access these resources, one must be authenticated and authorized. In this particular case, each company maintains identities for its own employees. One option to facilitate access would be to copy the accounts from the bank that needed access to resources at the corporation and place them in the corporation's identity store.

The problem with this scenario is that it requires close communication between the two corporations when an employee event occurs. This scenario works fine, *until* there is a change—a new employee, a change in role for an existing employee, or the termination of an employee.

If there is a change in the bank that occurs and the corporation is not notified—particularly with employee terminations—the corporation is subjected to a level of exposure. A terminated employee with malicious intent could continue to utilize resources at the corporation until such time that the corporation receives a notification from the bank that the employee should no longer have access to the system.

In addition to the challenges of additional risks, this approach also requires a fair amount of time dedicated to setting up and maintaining the identity in two locations by two staffs.

This is not just an issue across businesses but also across applications in a business. For my blog, I use a third-party web hosting company. For my hosting plan, I have one username and password for my administration page, another for the blog itself, a third to access the website statistics, another for my email, and yet another for access to the FTP server. For my one site, I am forced to use five different ID and password pairs. A better solution would be to have a single federated identity that worked across all these different applications.

In the consumer space, I've already established that there's password fatigue. There are distinct benefits to being able to share a single identity across multiple sites.

This book will discuss several approaches to handling federation of identity, including examples using CardSpace.

The Seven Laws of Identity

When looking at a federated identity for consumers, you might be familiar with a service Microsoft began offering a number of years ago, called Passport. Passport was intended to provide the same type of functionality that you saw in the airline travel scenario earlier in the chapter. Specifically, this was to provide a single, trusted identity for an individual that could be used across multiple sites.

Passport was a very successful solution for Microsoft's web properties; however, it was not a runaway success with third parties.

Microsoft has actually spent a fair amount of time looking into what some of the challenges were with the adoption of Passport. Kim Cameron, Microsoft's lead identity architect, looked long and hard at not only this but also why in general people either will accept and use an identity system or will reject it out of hand. He then published his thoughts on his Identity Blog (`http://www.identityblog.com`), where he discusses identity not just with individuals from Microsoft but with individuals from across the industry, from academics to enterprises and many representatives from the open source community. The distillation of these ideas has come to be known as the Laws of Identity, of which there are seven.

I'll detail the laws in Chapter 3, but here's a complete list:

Law #1: User Control and Consent

Law #2: Minimal Disclosure for a Constrained Use

Law #3: Justifiable Parties

Law #4: Directed Identity

Law #5: Pluralism of Operators and Technologies

Law #6: Human Integration

Law #7: Consistent Experience Across Contexts

One could suggest that Passport did not gain broad adoption amongst third-party sites because it is in conflict with several of the laws. One such conflict is with Law #3, "Justifiable Parties." While looking at Passport adoption, one can see that Microsoft's involvement in a transaction connected to a Microsoft-owned site was considered justified by end users, and Passport, in that instance, was acceptable. Microsoft's involvement (via Passport) in other scenarios on third-party sites, such as in a banking transaction, was not. Another conflict is with Law #5 because there was no pluralism; it was a closed system run by a single entity, Microsoft. One of the benefits of the laws is that they provide a common language to use in identity discussions. One can now say, "This was done to comply with Law #2" or "We can't do that; it violates Law #3."

■ **Note** Chapter 3 is dedicated to the Laws of Identity, where I will discuss each of them in more detail.

The Identity Metasystem

Law #5 is "Pluralism of Operators and Technologies." This was one of the challenges that Passport faced. Its implementation was provided by a single operator, Microsoft.

To satisfy Law #5—in other words, to provide a pluralism of operators and technologies—one needs to provide a level of interoperability across platforms, languages, and corporations. In essence, this takes us back to something done in the real world that I discussed earlier—let's revisit the airline scenario.

Specifically, when I check in for a flight, I provide a government-issued ID. This could be a driver's license. In the United States, this allows me to present an identity token provided by more than 50 different identity providers (all the U.S. states, territories, and so on). If I were not a U.S. citizen, I could provide a passport from a host of recognized nations. Although each of the tokens provided by the states or governments might have its own nuances, it complies with standards—whether defined or assumed—that make these tokens readily interoperable.

In the online world, as in the offline world, it is unlikely that there will be a single provider of identity. Instead, there will be a multitude of solutions and operators, as stated in "Microsoft's Vision for an Identity Metasystem":

> *This metasystem, or system of systems, would leverage the strengths of its constituent identity systems, provide interoperability between them, and enable creation of a consistent and straightforward user interface to them all. The resulting improvements in cyberspace would benefit everyone, making the Internet a safer place with the potential to boost e-commerce, combat phishing, and solve other digital identity challenges.*
>
> —"Microsoft's Vision for an Identity Metasystem"

Chapter 3 delves deeper into the identity metasystem, including covering the roles and components contained within it.

Windows CardSpace

If the Laws of Identity provide the guidance and the identity metasystem provides the infrastructure, the next logical piece is an implementation on top of the metasystem.

CardSpace is Microsoft's implementation of a client application for the identity metasystem. It provides a secure, consistent experience for end users that supports the interoperability of the underlying identity metasystem. In essence it acts as an identity selector simplifying the process by which a user selects which identity to use for a specific interaction.

CardSpace ships as part of the .NET Framework 3.0 and can be used in both web applications and with services. In this book, Chapters 5 and 6 are dedicated to utilizing CardSpace in a web application, as well as in services built with WCF.

CardSpace is preinstalled with .NET Framework 3.0 on Windows Vista. It is also available for use on Windows XP Service Pack 2 and Windows Server 2003.

This book focuses on looking at what CardSpace is and where you can use it. In the remainder of the book, I'll explore each of the topics discussed earlier in the chapter and show how the identity metasystem and CardSpace will fundamentally change how identity is handled on the Web.

Summary

As the name of this book implies, the focus is on understanding CardSpace. But to understand CardSpace, it is important to have an understanding of the challenges and opportunities tied to identity.

In this chapter, you learned about the various concepts that are important. You gained an understanding of authorization and authentication and now understand both the challenges (in other words, federation) and the opportunity (in other words, personalization) that are present in the identity space.

In the next chapter, I'll take you on a quick lap around Windows CardSpace. You'll get to see what it is and how it works from hands-on usage.