Unmasking Identity Management Architecture (IMA)

Digital Identity

O'REILLY®

Phillip J. Windley

O'REILLY®

Digital Identity

The rise of network-based, automated services in the past decade has changed the way businesses operate, and not always for the better. Offering services, conducting transactions, and moving data on the Web opens new opportunities, but many CTOs and CIOs are more concerned about the risks. Like the rulers of medieval cities, they adopt a siege mentality, building walls to keep the bad guys out. This need for a secure perimeter often hampers the flow of commerce.

Fortunately, some corporations are beginning to rethink how they provide security, so that interactions with customers, employees, partners, and suppliers will be richer and more flexible. *Digital Identity* explains how to go about it. This book details an important concept known as "identity management architecture" (IMA): a method to provide ample protection while giving good guys access to vital information and systems. IMA is a coherent, enterprise-wide set of standards, policies, certifications, and management activities that enable companies like yours to manage digital identity effectively—not just as a security check, but as a way to extend services and pinpoint the needs of customers.

How does digital identity increase business opportunity? Author Phillip J. Windley's favorite example is the ATM. With ATMs, banks can now offer around-the-clock service, serve more customers simultaneously, and do it in a variety of new locations. *Digital Identity* shows CIOs, other IT professionals, product managers, and programmers how security planning can support business goals and opportunities, rather than holding them at bay.

Drawing on his experience as CTO of iMall, Inc., VP of product development for Excite@Home and CIO in Governor Michael Leavitt's administration in Utah, Windley provides a rich, real-world view of the concepts, issues, and technologies behind identity management architecture.

www.oreilly.com

US $34.95 **CAN $48.95**

ISBN: 978-0-596-00878-9

9 780596 008789 53495

Digital Identity

Phillip J. Windley

O'REILLY®
Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

Digital Identity
by Phillip J. Windley

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*safari.oreilly.com*). For more information, contact our corporate/institutional sales department: (800) 998-9938 or *corporate@oreilly.com*.

Editors:	Allison Randal and Tatiana Apandi
Production Editor:	Sarah Sherman
Cover Designer:	Ellie Volckhausen
Interior Designer:	David Futato

Printing History:

August 2005: First Edition.

This book uses RepKover™, a durable and flexible lay-flat binding.

ISBN: 978-0-596-00878-9
[M]

To my parents, Rolla and Ranae Windley, for giving me the freedom to explore.

Table of Contents

Foreword

The migration of sociability, business, entertainment, and other activities from the physical world to the virtual world of the Internet has dramatic implications on many fronts. The societal mores, legal structures, and commonly accepted business practices that govern everyday life in the physical world have evolved over thousands of years, and that evolution continues every day. But now we're in the process of translating those structures to the Internet, creating a new place where people can interact. That "place" is radically different from the physical world, one where networked applications combine with ubiquitous connectivity to free transactions, communications, and other activities from physical constraints, thus, creating an entirely new set of requirements.

When it comes to enabling a truly virtual world that can accommodate the breadth and depth of human endeavor, nothing is more important than identity. On the Internet, movement is instantaneous. People, applications, transactions, and data can cross many types of borders via many different paths. At the same time, the security issues associated with a very public and virtual space have become painfully clear as spam, phishing attacks, fraud, and identity theft have become all too common.

Digital identity is the keystone that will ensure that the Internet infrastructure is strong enough to meet basic expectations for not just service and functionality, but security, privacy, and reliability. That fact is becoming more and more obvious to more and more people every day. But as the Zen master once said, knowing the path and walking the path are two very different things.

How we create, use, store, and verify identity in the Internet context is a complex question, one that transcends both the public and private sectors, and every conceivable business. It raises a large number of thorny issues for society and individuals (not the least of which is privacy), corporations (including the regulation of core operations), and governments (laws, regulations, international treaties). The manner in which these issues are resolved will have a long-term impact on all segments of society and will determine what forms of digital identity will first augment, and then (at least potentially) replace the "official" and "trusted" manifestations of identity on

which the physical world relies today. That change will take years, extending past the end of the current decade, involving societal, cultural, business, and political efforts.

How much control individuals will be able to take—or will want to take—over their digital identity is the subject of intense debate, for example. Pessimists predict that the intersection of government and commerce will create a surveillance state, one that will make privacy an artifact of the past. Optimists predict the liberation of the individual from both corporate and government control through the use of identity technologies that will put the individual in charge, inverting the traditional relationship between "consumers" and "service providers." That debate will continue for the foreseeable future as unfolding events pull us in both directions.

Today, much of the activity around digital identity is business-focused. The pressure to compete in a networked world while simultaneously reducing costs is driving companies to integrate business processes and information technology on an increasing scale. Many enterprises are creating inward- and outward-facing systems that tie employees, customers, partners, suppliers, contractors, and other constituents into their business processes, for example. Instead of thinking about individual applications, enterprise IT architects must consider end-to-end business processes that span many boundaries, and how they can integrate the components of IT to support them. These trends are causing wholesale change in IT architectures, moving them to what we at Burton Group call "the virtual enterprise."

The move to the virtual enterprise brings with it new security risks. These risks, along with the rapidly increasing number of regulations, both in North America and the European Union, are driving the need for new security models. Simply put, the traditional exclusionary security model—perimeter-based systems focused on keeping bad people out of the network—are not sufficient to protect the virtual enterprise. Today, businesses must augment exclusionary security with an inclusionary security model, one capable of explicitly determining, through policy, who can access the applications and data that support core business processes.

Such inclusionary models are unattainable without identity management. Identity must become persistent through the continuum of any given business process, spanning not just multiple applications, but also multiple organizations. Only then can identity provide the predicates for corporate governance, security, regulatory compliance, risk and liability management, and other core business functions.

For most enterprises, identity management is not easy. In fact, most enterprises' identity management processes are poor, a fact that internal and external audits make painfully clear. Historically, enterprises have treated the symptoms of the identity management problem with point solutions. But Internet-scale identity management requires an integrated set of infrastructure services that enable a holistic approach to defining and managing identity. This sophisticated array of tools includes directory services, rules-based user provisioning, delegated administration, and self-service administration for passwords or other attributes. General-purpose, strong authentication

systems, along with good credential management, are also core components of better identity management. Beyond authentication, enterprises must link applications to access management systems across a variety of operating systems, applications, and web-based single sign-on (SSO) products, making policy management yet another important part of the system.

Effective identity management also requires a new approach to systems integration and interoperability. Previous efforts to solve the identity problem (such as X.509-based, public-key infrastructure) attempted to achieve interoperability through symmetry and homogeneity. But federation has recently emerged as a new and more effective approach to enabling interoperability between security domains. Emerging federation standards rely heavily on the loosely coupled web services architecture, which in turn relies heavily on the eXtensible Markup Language (XML). Both the web services framework and interoperable identity are evolving along similar architectural lines for obvious reasons. While the web services framework enables the virtual enterprise, identity management secures it. So it's quite necessary for them to share architectural underpinnings.

The web services framework has, in essence, begun to create a standard software "communications bus" in support of service-oriented architecture. Applications and services can "plug in" to the bus and begin communicating using standard tools. The emergence of this "bus" has profound implications for identity exchange. Just as application and transactional data will flow across that bus, identity data will flow over that bus. And within service-oriented architectures, identity will become a core service.

The combination of web services and federated identity management has enormous potential; however, we have only just begun a long but inevitable transition to such a full-scale identity management infrastructure. And technology alone will not enable it. Regulations, laws, policies, and other mechanisms must evolve—both nationally and internationally—to create the context and boundaries for the acceptable use and management of identity. Likewise, business models for federating identity—including liability, risk management, and workable governance models—must evolve.

The evolution will be painful at times, occurring in fits and starts. Today, we're several years and many breakthroughs away from the combination of standards, technologies, legal frameworks, and business models necessary to create a fully interoperable identity framework. While we're in the early days, however, it's clear that the era of digital identity management has arrived, and tools and techniques are emerging that will help companies address the issue. There are clear and strong links between identity management and enterprise business objectives in many industries. The market forces that will drive us inexorably forward to resolve these complex problems are active, causing real and significant movement.

Given these realities, today's IT managers must start creating an identity management infrastructure that meets their business objectives. And that makes books such as this one all the more important. Through his work in both the public and private

sectors, Phil Windley has a perspective on the issues of IT architecture and identity management that can come only through experience. Phil has lived the problem and is dedicated to finding a solution: one that works not just for one company, but for all companies. Phil has poured much of his experience into this book, which provides a great starting point for anyone needing to understand both the issues and technologies behind effective identity management.

It's that starting point that is often the most important in any attempt to drive significant change, either in an organization or a technical architecture. The people and companies who take what Phil has to offer in this book, learn from it, and use it to start the process of change will be better prepared for the future. This book can be the first step toward a general-purpose identity management infrastructure that will enable new applications, services, or business models while reducing costs.

As an increasing number of enterprises take that path, digital identity management will emerge as a pervasive infrastructure, within, between, and across organizational structures. The technologies and standards, as well as the law and policy that evolve to regulate corporate use of identity information will both influence and be influenced by the larger personal identity infrastructure to come. Enterprise identity management and the larger societal move toward digital identity for customer, governmental, and other activities will inevitably intersect, changing the way we live and work in the process. I look forward to working with Phil and a host of other participants in the creation of that infrastructure.

—Jamie Lewis
CEO and Research Chair
Burton Group
February 2005

Preface

In late 2000, Governor Michael Leavitt of Utah asked me to serve as his CIO and a member of his cabinet. Governor Leavitt had a strong belief in the power of e-government to transform government operations and thought that my private-sector experience as CTO for an early e-commerce start-up, iMall.com, and then as vice president of product development at Excite@Home was just what was needed to help build e-government in Utah.

I spent almost two years working on that vision and building an infrastructure to support it. While I was CIO, I struggled to learn how to build flexible, interoperable infrastructure in a large, loosely coupled organization. Many of the issues we faced, such as privacy, naming, directories, authentication, and digital signatures, were identity issues. Many more of them were about how to execute an enterprise strategy in a decentralized organization. State governments are not alone in those challenges.

I have a deep respect for the power of digital identity, and I am convinced by my experiences in e-commerce and as CIO that digital identity was a foundational element in modern IT systems. I can't imagine an agile, business-responsive IT infrastructure that doesn't have at its core a flexible, interoperable identity infrastructure.

Not long ago, Doug Kaye sent an email to a group of folks that said, essentially: "The world needs a book on digital identity. Would any of you like to write it?" I thought that sounded fun, and this book is a direct result of Doug's question.

Throughout this book, you'll find stories from my experiences as a CTO and CIO that illustrate identity concepts. Interestingly, when I had those experiences, I wasn't usually thinking about digital identity. Consequently, I was surprised to find that many of my past experiences were directly related to the subject of this book. In relating these experiences, I don't want to take undue credit for what happened. Literally hundreds of people participated in the experiences I relate, and I'm grateful that they did. I learned a lot.

Who Should Read This Book

This book is designed to familiarize CIOs, IT managers, and other IT professionals with the language, concepts, and technology of digital identity. As I said, I believe that managing digital identity is one of the most fundamental activities in IT and that a good identity management strategy is the key to not only protecting the enterprise from attack, but, more important, providing flexible access for partners, customers, and employees to needed information and systems.

The concepts in this book apply equally well to a wide variety of organizations. While this book primarily talks about digital identity in the context of business, the concepts are as applicable, and opportunities as great, for non-profit groups and government agencies. As I mentioned, my experiences cover the public and private sectors as well as large and small organizations. When I use the word "enterprise" in this book, I mean any business or organization—for-profit or not. The term can even apply to business units, provided their decisions about identity are relatively independent from other business units in the larger organization.

This book is not a book with code examples and recipes for building digital identity management systems. Even so, it is a technical book that explains the technology of digital identity in some detail. More importantly, the book puts the technology in context and shows how it can all be put to the task of managing digital identities inside your organization.

The book is divided into three sections. The first section is about the core concepts in digital identity, including privacy and trust. The second section discusses the technology of digital identity. The third section portrays in some detail a process, called an *identity management architecture* (*IMA*), that you can use to build a digital identity infrastructure in your organization, regardless of its size or organization. The information in the last section is prescriptive in nature. Because of my experiences, I have a clear philosophy on how to build an IMA. I present a rather a detailed series of steps that show how to create an IMA and how to use it.

Conventions Used in This Book

The following typographic conventions are used in this book:

Italic
: Used for file and directory names, email addresses, Unix commands, and URLs, as well as for new terms where they are defined.

`Constant Width`
: Used for code listings and for keywords, variables, tags, functions, command options, and strings where they appear in the text.

`Constant Width Bold`
: Used to mark lines of output in examples.

Constant Width Italic
: Used as a general placeholder to indicate items that should be replaced by actual values.

Comments and Questions

Please address comments and questions concerning this book to the publisher:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
(800) 998-9938 (in the United States or Canada)
(707) 829-0515 (international or local)
(707) 829-0104 (fax)

We have a web page for this book, where we list errata, examples, and any additional information. You can access this page at:

http://www.oreilly.com/catalog/digidentity

To comment or ask technical questions about this book, send email to:

bookquestions@oreilly.com

For more information about our books, conferences, Resource Centers, and the O'Reilly Network, see our web site at:

http://www.oreilly.com

Safari Enabled

When you see a Safari® enabled icon on the cover of your favorite technology book, that means the book is available online through the O'Reilly Network Safari Bookshelf.

Safari offers a solution that's better than e-books. It's a virtual library that lets you easily search thousands of top tech books, cut and paste code samples, download chapters, and find quick answers when you need the most accurate, current information. Try it for free at *http://safari.oreilly.com*.

Acknowledgments

This book would have never happened without the encouragement, help, and advice of Doug Kaye. I've mentioned his original question that motivated the book. He also provided valuable coaching and mentoring, as well as served as the book's first editor. I'm grateful for his guidance and friendship.

Bradford Windley drew the picture of the trebuchet in Chapter 1.

Some portions of Chapter 12, on federating identity, are adapted with permission from *Scenarios for Identity Federation & Drivers of the Identity Network* by Linda Elliott and Eric Nolin of Ping Identity Corporation, Tom McKenna of SRI Consulting Business Intelligence, and Kevin Werbach of the Supernova Group LLC.

I'm grateful for the help of Gary Daemer of Booz Allen Hamilton who provided valuable information and advice about the maturity model for identity discussed in Chapter 15.

Burton Group and Jamie Lewis, in particular, were very generous in letting me use their ideas in writing Chapter 19 on reference architectures. I'm also grateful to Jamie for agreeing to write the Foreword to this book and for his insights into the state of the art in digital identity systems and technology.

The technical reviewers offered many thoughtful suggestions that greatly improved the final result. I'm thankful for their efforts.

Lastly, I'm grateful to my wife, Lynne, and my children, Bradford, Alexandra, Jacob, Joseph, and Samantha, for their support, help, love, and mostly for their understanding at the many times I had to say "Sorry, I can't—I've got to work on the book."

CHAPTER 1
Introduction

In medieval times, strong walls and moats surrounded great cities. Guards were posted at the gates of the city, and everyone coming or going was inspected and questioned about their purpose for entering or leaving the city. At the same time, cities were where the markets were held. You can imagine the crush at the gates on market day with peasants bringing their goods into the city from outside and visitors clamoring to get to market. After market was over, the process was reversed. With our modern eyes, we can see what an impediment to commerce the walls were, yet at the time, city residents were thankful for their security.

The walls were not broken down by enlightened thinking about of how markets should work, but rather a weapon for which the walls were no match: the trebuchet (see Figure 1-1). A trebuchet is a gravity-powered catapult that is vastly superior to its torsion-powered cousins. The trebuchet revolutionized medieval siege warfare and eventually spelled the end for city walls. The result not only forced an alternative strategy for security, but also had the pleasant side effect of increasing commerce.

I recently had the opportunity to sit with a group of CIOs and discuss digital identity. What struck me was how much of the conversation was about security and liability rather than identity and opportunity. They had a siege mentality and their security planning showed it.

Modern corporations are the walled cities of our time—sitting behind firewalls and defending themselves from attack. What these CIOs and others can't see is that their security implementations are restricting their company's opportunities in the same way that ancient walls restricted commerce in their day. Fortunately, commercial enlightenment, rather than a weapon that cannot be withstood, is awakening a desire in corporations to rethink how we provide security so that our interactions with customers, employees, partners, and suppliers are richer and more flexible.

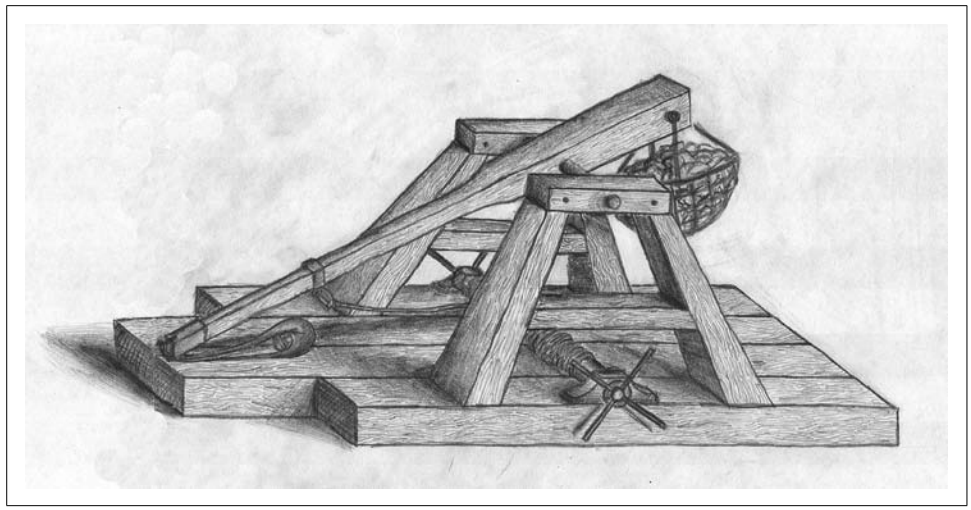

Figure 1-1. Trebuchet

Business Opportunity

The economic shifts that have occurred over the last decade have changed how businesses operate and the expectations of customers. One of the most dramatic shifts has been the rise of network-based, automated services. In many cases, we're "spending more and owning less," in the words of Jeremy Rifkin. When I fly, I almost always purchase tickets online, but more than that, almost all of my needs as a customer of the airline are self-serviced, using online web applications. I can check flight schedules, be notified by SMS if my plane is running late, check my frequent flyer account balance, and even redeem upgrade points and change my seat online. The changes underlying these trends have profound implications for businesses and customers alike.

For businesses, a service-oriented economy means that they must adjust to entirely new ways of relating to their customers. The World Wide Web changed the way companies market their products. But more importantly, the products themselves have changed. Perhaps the most significant change is that there is no longer a human in the loop to create a trust relationship with the customer, make up for process deficiencies, and represent the company. When two businesses merge, they often find that they have very different approaches to knowing their customer and that this makes leveraging the combined operation almost impossible.

For customers, the changes are equally dramatic. Where they used to purchase things from people at physical locations, they now purchase or use services delivered to them electronically on their computer, PDA, and even their phone. The usual trust marks that customers have relied on in the past are either missing or easily forged. As the number and breadth of services that people use grows, they find that they are inundated with requests to identify themselves and to divulge information they consider private.

In addition to their customers, businesses have relationships with partners, suppliers, and employees. Networks have changed those relationships as well. Just as with the business-customer relationship, these relationships are increasingly moving to the electronic world and being mediated by automated processes rather than people.

Digital Identity Matters

At the heart of this service-oriented economy are network-based, automated transactions. Automated transactions are fundamentally different than the transactions that occur in the physical world. When I stop by the convenience store to buy a snack, I can exchange cash for peanuts. Unless the clerk happens to know me, the transaction is anonymous. In contrast, in the service-oriented economy, anonymous transactions are rare, because delivering service automatically almost always implies that you have to know something about who's receiving the service—if not their names, then at least their preferences or other attributes. This identifying information is usually transferred digitally, across the network. In a service-oriented economy, digital identity matters.

Of course when we talk about the service-oriented economy, we're not just talking about e-commerce. Note that my example with the convenience store involved a small cash purchase. But imagine the same scenario, except this time I use a debit card, credit card, or check. In any of those cases, I've invoked a network-based financial service as part of the overall transaction. Network-based services are as pervasive in transactions that occur in the physical world as they are in online interactions.

In an automated, network-based service, I have to know who you are in order to sell you access to my service. Since these services are increasingly delivered over digital networks, businesses need reliable, secure, and private means for creating, storing, transferring, and using digital identities. Network-based, automated services are not just delivered to customers—employees, partners, and suppliers also interact with the enterprise via services. In many cases, anonymous service is impossible or undesirable, and as a consequence, digital identities must be assigned and managed.

In addition to identifying customers to sell them services, business have an increasing need to identify employees, systems, resources, and services in a systematic way to create business agility and ensure the security of business assets.

Using Digital Identity

Digital identity is the lynch pin in each of the activities we have just discussed, along with a wide variety of other activities important to business. Consequently, how your organization manages digital identities will have a great impact on whether you are constantly fighting problems brought on by a lack of attention to managing identity, or whether you are exploiting opportunity enabled by a flexible and rational digital identity infrastructure.

The common ATM machine is a great example of how digital identity enables new business opportunities. Before ATMs were invented, a bank's customers took care of their banking needs by presenting pieces of paper to a human teller. The papers included instructions to the bank (e.g., deposit slips), cash, checks, and other financial instruments. Unless the teller personally knew the customer, the customer usually also presented some kind of identity credential, such as a driver's license. The teller was able to verify the identity of the customer and the validity of the various pieces of paper.

The ATM was possible only because banks created a means of identifying their customers digitally. We're all familiar by now with the debit card and PIN that ATMs require from us before service. The card carries identity information and the PIN tells the bank that the person presenting the identity is entitled to use it. With the advent of a digital identity infrastructure, banks no longer needed a human in the loop to verify the customer's identity.

From the bank's perspective, the most obvious benefit from an ATM is to reduce the cost of employing the teller, but there are other benefits as well. I lived in Japan for two years during the 1970s and experienced ATM machines there for the first time. I'd never even heard of ATM machines before that. I had a chance to visit Japan again in 1996 and found something strange. There were still plenty of ATM machines, but they operated only when the bank was open. You you could only receive during banking hours.

Japanese banks, at least in 1996, still viewed ATMs as simply "teller replacements." But in the U.S., something more interesting had happened: ATMs were used to extend service in ways that went beyond merely replacing the teller in the branch. ATM machines extended service in three fundamental ways:

- ATM machines were open 24 hours per day, seven days a week. In fact, the first time I ever saw the phrase "24/7" was as part of a branding campaign for a small credit union in California. 24/7 was a catch phrase in the banking industry before the Internet made it popular.
- ATM machines increased the number of customers a bank could service simultaneously, with multiple ATM machines being installed in many bank branches.
- Because they are relatively inexpensive, ATM machines were installed outside of bank branches in convenience stores, shopping malls, theaters, and so on. These businesses usually shared in the profit from the ATM transactions.

This example shows clearly the three primary ways that information technology can extend a business. Tom Parenty* describes them as extensions of time, scale, and locale.

* Parenty, Thomas J. *Digital Defense: What You Should Know About Protecting Your Company's Assets*. Cambridge. Harvard Business School Press, 2003.

Each of these extensions is built on a foundation of digital identity. Without a digital identity infrastructure to give bank executives the ability to trust that people using the ATMs are allowed to take authorized actions, ATMs would have never been deployed.

The other side of this relationship is equally instructive. Customers feel good about participating in transactions with the bank because of trust marks that they encounter before and during the experience: the big building, the brand of the bank, the FDIC sticker, and last but not least, the teller are all part of this. The first ATMs were installed in bank lobbies to keep much of that intact. Humans frequently helped customers through their initial fear of dealing with a machine, effectively transferring the trust that customers placed in the human teller to the digital identity infrastructure and computer systems that made up the ATM system. Nowadays, of course, ATMs appear in all kinds of settings, and most people trust the debit card and PIN to adequately protect their assets.

Just as ATMs changed the way banks do business, information technology, and especially the growth of the Internet, has fueled a multitude of opportunity for business to throw off the old restrictions of time, scale, and locale. Doing so, however, requires a better understanding of digital identity than ever before.

The Business Context of Identity

Like medieval city planners, IT professionals and others have traditionally thought of security as an edge game. Given a firewall and access control to the network, we can do a reasonable job securing a business. However, the economic shifts spoken of previously have driven the need to integrate systems not only internally, but with trading partners and customers as well. This trend is fueled by XML and the creation of standards for exchanging data and the increasing trend to decentralized computing that is embodied in service-oriented architectures (SOAs) and web services. But this trend has ramifications for business security: we can no longer treat the edges of the network as a secure perimeter.

When integration is driven by business, rather than IT needs, security policies need to talk about documents, data, actions, people, and corporations instead of machines and networks. This new security model is infinitely more complex than the old "secure perimeter" model. But even if you can define your identity strategy, how do you ensure that it is properly implemented across dozens or even hundreds of systems, and, at the same time, control access to fields of a database or paragraphs of a document?

Foundational Technologies for Digital Identity

Understanding how your organization can make use of digital identity requires understanding concepts such as trust and privacy. Moreover, digital identity is built on a set of technologies that includes cryptography, authentication, authorization, identity provisioning, directories, digital rights management, identity federation, and interoperability standards. Later chapters in this book will discuss these concepts and technologies in detail, and show how they fit into an overall identity management strategy.

Identity Management Architectures

The most difficult part of getting identity management right isn't technical. Management, policy, and even political issues are more likely to be the things that stand in the way of success. To that end, the final section of this book will describe a methodology for creating what I call an identity management architecture (IMA) that can help you overcome these challenges.

An IMA is unique to each organization. Creating an IMA for your organization requires a firm framework for governance and understanding the business context within which it will operate. To that end, the methodology in this book includes detailed ideas about how you can document, analyze and understand the business context that your identity infrastructure will have to support.

An IMA has three primary components:

Process Architecture
: The process architecture is a methodology for determining how your business accomplishes identity related tasks now and how they should be accomplished in the future. The architecture is based on an identity infrastructure maturity model that lays out how processes can be changed to make them more effective in supporting the identity needs of the business.

Data Architecture
: The data architecture is a model of the identity data in your organization. Recently, a number of news stories have highlighted organizations that lost control of identity data and were publicly embarrassed over the resulting privacy concerns. Getting a handle on where your identity data is and what processes affect it will help you avoid these problems and help you build an infrastructure that is responsive to business needs.