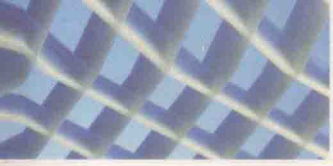
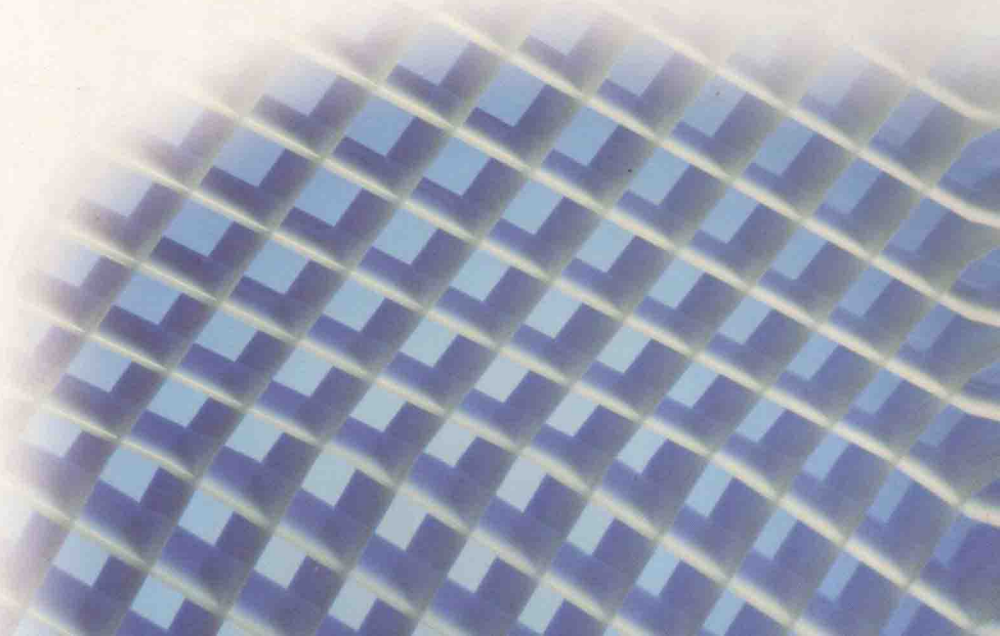
PKI

A Wiley Tech Brief

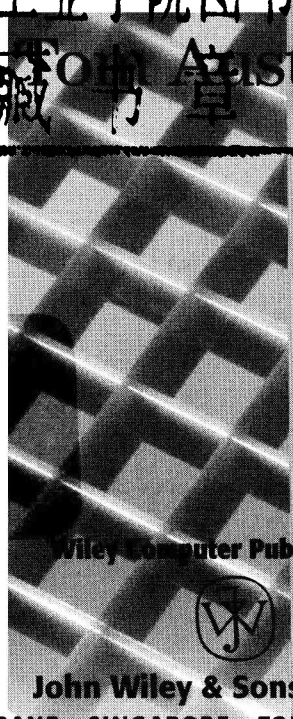




Tom Austin

PKI

A Wiley Tech Brief



Wiley Computer Publishing

John Wiley & Sons, Inc.

NEW YORK • CHICHESTER • WEINHEIM • BRISBANE • SINGAPORE • TORONTO

Publisher: Robert Ipsen
Editor: Margaret Hendrey
Managing Editor: Angela Smith
Text Design & Composition: Benchmark Productions, Inc.

Published by John Wiley & Sons, Inc.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

ISBN 0-471-35380-9

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Advance Praise for *PKI*

" PKI is fast becoming the cornerstone of e-security, and this book provides an excellent perspective on PKI for both technology and business people."

—Fran Rooney, CEO, Baltimore Technologies

" The organization of the book, and the choice and weighting of topics, are excellent. I am not aware of any other books on PKI that emphasize deployment and acquisition concerns like this one. The case studies and example RFP were particularly useful. This book will appeal to those in charge of procuring and operating a PKI."

—Rich Ankney, Vice President, CertCo

" A must read for anyone who will be involved assessing, recommending, approving, buying or implementing digital asset security at any level in a enterprise. Austin brings together an impressive array of authoritative experts, and attains seamless topic integration presenting the right flow of ideas to the reader. Hard to imagine, but he succeeds delivering a PKI treatise with sufficient depth and breadth to please the initiated, yet easy to read from the boardroom to the heart of the IT function."

—Juan Rodriguez-Torrent, PKI Forum founder, President & CEO Aposematic Corporation

"...grounded in the real world of the business benefits PKI provides. Case studies show how PKI has been implemented by a variety of companies today, allowing readers to learn from the experiences of others without vendor hype or bias. Austin's conversational style that explains the nuts and bolts of PKI along with substantive, practical case studies make this book a must-have resource for anyone considering PKI deployment."

—Debra Cameron, President, Cameron Consulting

"This thorough look at PKI will help to enrich understanding in the industry and help to move efforts in e-business forward."

—Laura Rime, Global Marketing Manager, Identrus

Wiley Tech Brief Series

Other titles in the series:

Steve Mann and Scott Sbihli, *The Wireless Application Protocol (WAP).* 0471-39992-2

Ray Rischpater, *Palm Enterprise Applications.* 0471-39379-7

Chetan Sharma, *Wireless Internet Enterprise Applications*. 0471-38382-7

William A. Ruh, Francis X. Maginnis, and William J. Brown, *Enterprise Application Integration.* 0471-37641-8

Jon Graff, *Cryptography and E-Commerce*. 0471-40574-4

Acknowledgments

In the nearly two years it took to complete this book, I've had the opportunity to meet with some great people that contributed to this book, offered their assistance in one way or another, or simply shared their thoughts and ideas.

The idea for this book became reality as a result of the fine people at Wiley. I'm especially grateful to Marjorie Spencer and Margaret Hendrey. Marjorie, who believed in me, the concept for this book, and made it happen. Margaret, from start to finish, was always available to see this project through. Her expert direction, patience, and prompt response to my many questions and requests is the mark of a true professional. Equally, thanks go to Carol Long for her ongoing support, encouragement, and objectivity as well as Angela Smith and Kerstin Nasdeo for their painstaking efforts in taking this draft to production.

The case studies presented in this book would not have been possible without the efforts of many people, especially Wayne Austad, Gavin Grounds, Richard Karon, Art Purcell, John Taylor, and Ron Szoc who made a tremendous effort in responding to my numerous list of questions. The essence of what you'll learn from these case studies are a direct result of these people willing to share their experience and wisdom with you.

Special thanks go to Tracy Shouldice, Susan Hannah, and Roger Sabourin of Entrust Technologies. This book would not have been what it is without them. Their untiring and ceaseless efforts on my behalf helped make this book what it is. They are truly the best!

With topics ranging from biometrics to cryptography, from legacy systems to time stamping, few people, if any, can be an expert in all areas of PKI. The knowledge and depth of experience of the people that contributed to this book are more than one writer alone could ever match. I'd especially like to thank Jeff Stapleton, Roseanne Day, and Steve McIntosh. In addition to contributing chapters to this book, they've all helped to make it that much better. Jeff, for agreeing to contribute to this effort and for putting me in touch with other experts that also contributed to this book. Roseann, for always sharing her thoughts, insights, and valued friendship. Steve, for his many offers of help, and for also improving my writing.

Of course, no book would be complete without illustrations. The outstanding visuals you see in this book are the masterful work of Richard Eberly. Richard has the unique skill of taking a simple sketch and creating artwork that contributes immensely to helping us understand beyond just the written word.

I'd like to recognize Laura Rime of Identrus, and Richard Guida of the Federal PKI Steering Committee, for their guidance and responsiveness as well as Brian Iverson of Novell, Gary Miller of EXOCOM, Carl Norell of CeloCom, and Michael Thieme of International Biometric Group.

For reviewing and critiquing this book, I sincerely appreciate the time and efforts of Rich Ankney of Certco, Dr. Burt Kaliski of RSA Laboratories, Juan Rodriguez-Torrent of Aposematic Corporation, Roger Sabourin of Entrust Technologies, and Dr. Richard Y. Yen of The Chase Manhattan Bank.

Most of all, I'd like to thank my wife Bonnie, for all the support she provides me. Not only has she freely and unconditionally supported all of my endeavors, but she also read and provided me with her feedback, even after many a long day at work, on all that I wrote for this book. I couldn't ask for more.

About the Contributors

Santosh Chokhani is the founder, President and CEO of CygnaCom Solutions Inc., an Entrust Technologies company specializing in PKI.

Roseann Day is a security consultant who works with a wide range of systems and software vendors on their marketing and product development strategies. Her professional career spans over 25 years which includes positions at Digital and IBM.

Todd Glassey is the creator of Certifiable Time Data and its use models in modern eBusiness systems. His 20+ years of experience include strategic and industry specific technology assessment, network, project operations, and security consulting, as well as hardware and software development.

Sven Hammar is CEO, Celo Communications Ltd. and President, Celo Communications Inc. He has 15 years experience as a consultant in the security field and has been president and vice president of various Swedish consulting companies.

Diana Kelley is the General Manager for Jawbreaker, a security software development effort, at Symantec Research Labs. Ms. Kelley has ten years of experience creating secure network architectures and eBusiness solutions.

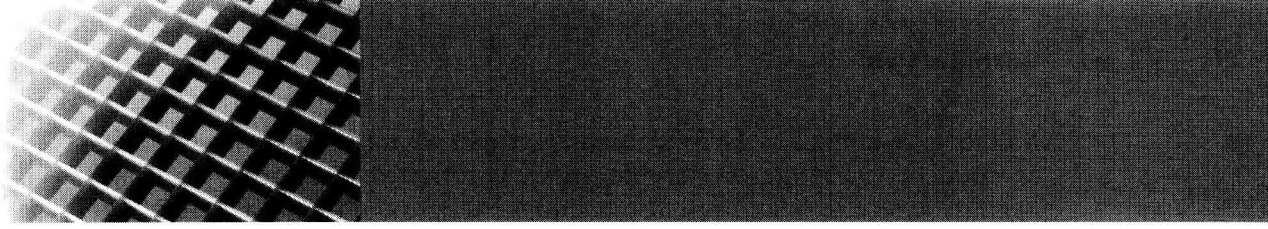
Sathvik Krishnamurthy is vice president, marketing and business development at ValiCert. Prior to ValiCert, he held various positions at Worldtalk Corporation, Deming Internet Security and Retix.

Steve McIntosh. Focusing primarily on PKI, network security, and UNIX in his 20 years with technology vendors, Steve McIntosh has held product management positions at nCipher, CertCo, and Digital.

Samir Nanavati is a partner at International Biometric Group, LLC, a biometric consulting and integration firm he co-founded in 1996 to help companies investigate, design, and implement biometric solutions.

Ruven Schwartz is an attorney with over 15 years experience in the technical and legal communities and is currently Vice President of Trust Practices at CertifiedTime. He also serves as vice chair of the American Bar Association Information Security Committee.

Jeff Stapleton is a manager with KPMG, LLP in the Information Risk Management practice focusing on Secure Electronic Commerce and PKI services. He is the chair of the ANSI/ASC X9F4 working group and has participated in developing Financial Industries security standards with ISO TC68 and ANSI/ASC X9.



Introduction

Whether it's to build market share, develop new business, increase productivity or profitability, there's no doubt your organization needs to take advantage of the Internet to stay competitive. However, with stories today about Internet security problems about as frequent as weather reports, doing business online clearly represents risks as well as benefits. When conducting crucial business over the public Internet, we need to have certain assurances. The question is, just what are those assurances?

Those assurances are a set of security services that are provided through a technology we refer to as Public Key Infrastructure, or simply PKI. The essential services that PKI can provide are confidentiality, authentication, integrity, and non-repudiation. These services are important because:

- Confidentiality *assures you* that your information is protected.
- Authentication *assures you* that you know with whom you're doing business.
- Integrity *assures you* that information is not being modified or substituted.
- Non-repudiation *assures you* that the originator cannot deny originating a message or business transaction.

Of course, these services do come at a cost—but just how much? What impact will PKI have on your organization and your customers? How complex is it to implement, and just how long will it take? While it's easy to learn the benefits from vendors, it can be much harder to get answers about the costs. You'll find many of the answers in this book.

Moreover, you'll learn the fundamentals of just what makes up the various components of PKI, such as cryptography, certificates, directories, key management, and time stamps. It also includes background information on government and industry initiatives, ongoing efforts for industry standards, and legislation that affects how you conduct business online.

Who Should Read This Book

This book is intended to help technology, business, and sales professionals understand PKI technology and how it can be applied to meet business requirements. Its goal is to help readers quickly get a grasp on what's involved, whether your role is selling, buying, planning, or implementing a PKI. The book also illustrates key business and competitive reasons for PKI through a set of case studies that underscore what others have found to be critical success factors, their lessons learned, and what they would do differently.

You may or may not already be familiar with PKI. For those just starting out, this book will provide a great starting point to learn what PKI is all about. You'll gain a sound understanding of basic concepts and principles, realize what others are doing, and learn about the security services and solutions that PKI can address. In short, you'll have the background information you'll need to be able to ask serious questions about PKI, and be able to begin planning one.

For those who are more advanced in their knowledge of PKI, the case studies will help you with your business justification for PKI, and should also provide added insight in what others have accomplished and the process they followed to really implement their PKI. Additionally, if there's a need to understand more about auditing, biometrics, hardware mechanisms, time stamps, and creating a Certificate Policy and Certification Practice Statement, you'll find the right information in this book to help you get the job done.

What You Will Find in This Book

This book covers the fundamental technology and business topics that are critical when considering and deploying a PKI. Furthermore, it delves into the experiences of others who have implemented PKI, the outside influences that affected them, and more importantly, the impact it has had on their business.

Part One: Security Basics

Part One introduces you to the underlying mechanisms present in a PKI, and the essential security concepts and standards required to maintain an appro-

priate working environment. In addition to the various technology disciplines within a PKI, basic business requirements and issues are discussed.

Chapter 1, "PKI Explained," looks at the need for PKI, factors to consider in authentication, how cryptography works and enables digital signatures and certificates, and the environmental security that's necessary before a PKI can be implemented.

Part Two, "PKI Technologies," delves into the heart of a PKI. The life cycle and necessary supporting disciplines that ensures the security and continued operation of a PKI are presented, along with the roles that certificate and validation authorities perform. Considerations are also offered about directories, time stamps, and hardware mechanisms and the business value they bring to a PKI.

Part Three, "PKI and Business Issues," takes an in-depth look at Certificate Policies and Certification Practice Statements and issues around auditing a PKI. Besides factors to consider about qualifying vendors, and at the looking the costs involved, you'll learn how to obtain your own digital certificate to help familiarize yourself with its basic features and functions.

Part Four, "Case Studies" offers you insight into how PKI is being used in the real world. Comprehensive case studies include government, financial, and service sectors that feature how these organizations proceeded to build their PKI and what they've accomplished. Moreover, it captures internal migration issues and the external forces that are at work that could have a direct effect on how you might proceed with your PKI.

It also reveals the details behind the usual technology planning and implementation by looking at concrete business requirements that necessitated PKI, the investment they made, the impact it's had on their business, and how they're measuring results. Discover what they would do differently and what they found to be the most helpful in getting their PKI up and running.

Part Five, "PKI Efforts," gives you an overview as to what government and industry consortia efforts are underway, as well as a synopsis of related standards, laws, and regulations. Which biometric technologies are best for PKI, and what potential approaches can be taken are also discussed, in addition to listing and describing the technical issues you'll face when integrating existing enterprise applications.

In Appendix A, "Request for Proposal for Public Key Infrastructure," you'll receive some help in getting started with a sample, generic Request for Proposal (RFP) that you can use that includes general guidelines and descriptions, and specific questions you can tailor to your needs.

Looking Forward

Getting your arms around PKI isn't easy. Yet, more organizations than ever are planning or actually deploying PKI, because it's the technology that effectively provides the necessary foundation for electronic commerce.

Lastly, the interest and activity surrounding PKI has never been greater. When I attended the first Entrust PKI conference in 1998, the level of interest of 700-plus attendees in a vendor's first conference amazed me. The next year, attendance at the Entrust event more than doubled. And it's not just the Entrust Conference. Both the conferences for Baltimore Technologies and RSA are also experiencing record attendance. It's a strong signal of where business is headed.

While you can learn a lot from going to these conferences, this book will provide you with perspective to the point you'll be prepared to implement a PKI in your own environment.

Contents