Microsoft Solutions for Security

Securing Wireless LANs with Certificate Services

Overview

Release 1.6

Microsoft®

Acknowledgments

The Microsoft Solutions for Security (MSS) group would like to acknowledge and thank the team that produced the solution guidance for *Securing Wireless LANs with Certificate Services*. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Authors

Ian Hellen and Stirling Goetz

Additional contributions were made by Mehul Mediwala, Carsten Kinder, and Andrew Hawkins.

Testers

Mehul Mediwala (Test Lead) and Jon Stone

Additional contributions were made by Gaurav Singh Bora.

Editors

Wendy Cleary (Lead Editor), John Cobb, and Steve Wacker

Additional contributions were made by Kelly McMahon and Jon Tobey.

Program Managers

Jeff Coon, Karl Grunwald, and Bomani Siwatu

Release Manager

Flicka Crandell

Other Members of the MSS Team

The following members of the MSS team also contributed to the development of this solution:

Jeff Newfeld, JoAnne Kennedy, Rob Oikawa, and Derick Campbell

Our Thanks

This solution could only have been developed with the collective expertise and assistance of many individuals.

Our deepest thanks to the following people:

- David Cross, Laudon Williams and Darren Canavor of the Windows Certificate Services team for committing significant time and effort reviewing the material and answering countless questions.
- Pat Fetty and Bill Dollar of the Windows Network Infrastructure Team for their speedy review and excellent suggestions.
- Drew Baron and Warren Barkley of the Windows Network Infrastructure Team for their ongoing support and assistance in confirming the solution's operability with WPA.
- Jerry Dyer, Jeff Yuhas and Nigel Cain of the Microsoft Solutions for Management team for their help with the Operations Guide chapters.
- Mark Mortimore and the Technet Team for their help with the publication of the solution.
- Andrew Matthews, Richard Hicks, Paul Thorlby and the rest of the team at Qinetiq for their review, criticism and helpful advice.
- Scott Hogan, Mario Rodriguez, Larry Talbot, Price Oden, Lee Walker, John Biccum, Matthew Lehman, Candy Stark and Olav Opedal from Microsoft OTG for their assistance and review.
- The Windows Server 2003 Security Guide team for their work with us in creating the Certificate Services and IAS server role hardening templates used to lock down the solution.
- MSS sister teams within the Windows Core Infrastructure Solutions group: Microsoft System Architecture (MSA), Microsoft Solutions for Management (MSM) and Microsoft Solutions Framework (MSF) for assisting us with our operations and deployment guidance.

Thanks also to our other content reviewers and contributors, including: Bernard Aboba, Graham Calladine, Gene Ferioli, JP Gorsky (Enterasys), Paresh Gujar, David Hoyle, Holger Luebsen, Ashwin Palekar, Ellis Paul, Keith Proctor, Tony Rice, Jeff Schwartz (Enterasys), Jude Servi (Cisco), Bill Stackpole and Graham Whiteley. Thanks to Ignacio Avellaneda for his help in outlining the solution support requirements, and to Simon Conant for reviewing the supportability of the solution. Thanks also to Michael Stephenson and Ali Jaleel for their support and product management work.

Master Table of Contents

Build Guide

Operations Guide

1

Overview

Introduction

Many organizations have tested the use of wireless LANs (WLANs) but have shied away from large deployments or banned their use altogether. Despite the many productivity and technology benefits of wireless technology, its poor security record has prevented many organizations from deploying WLANs.

Securing Wireless LANs with Certificate Services is aimed at those organizations that want to deploy wireless networks in a secure manner. It was written as a prescriptive guide (it discusses design, deployment, and management) and is based on Microsoft's own secure WLAN deployment.

There are two important characteristics of this solution guide that distinguish it from product documentation and many of the technical white papers available. The first characteristic is the *prescriptive* nature of the guidance: where design choices existed, decisions were made based on the best available knowledge from Microsoft's internal deployment and customer feedback. The solution was then built as described and tested in Microsoft labs to ensure that it works as stated. The second characteristic is that it is an *end–to–end* solution that encompasses design, planning, building, and configuration as well as ongoing monitoring, maintenance, and management of the solution.

As detailed in later chapters, the solution is based on the Institute of Electrical and Electronic Engineers (IEEE) 802.1X and requires a RADIUS (Remote Authentication Dial-In User Service) infrastructure and a public key infrastructure (PKI). It uses a flexible design and is suited for organizations of several hundred to many thousands of wireless network users. The RADIUS and PKI components were intentionally designed to be reusable in other network applications (for example, remote access VPN) and other security applications (for example, Encrypting File System). The solution was built and tested using Microsoft® Windows® XP clients and Microsoft Windows Server™ 2003 servers (including Active Directory® directory service domain controllers), although it has been designed to work with Windows 2000 domain controllers and Windows 2000 and earlier clients.

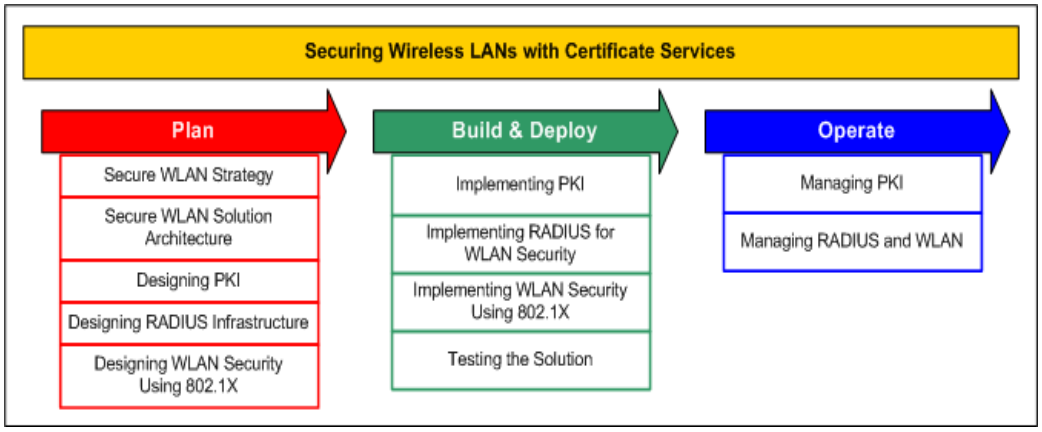

Figure 1.1
Overview of Securing Wireless LANs with Certificate Services

Solution Overview

This *Securing Wireless LANs* solution has four main sections: the Planning Guide, the Build Guide, the Operations Guide, and the Test Guide. A Delivery Guide is also included, as one of the appendixes. Accompanying these documents is a set of tools that includes a sample project plan, script files for automating implementation and operations tasks, and a detailed set of test cases that you can use to verify the functionality of the solution as you build it in your own environment.

The following sections provide brief overviews of the guides, including the purpose and intended audience for each. together with summaries of the each chapter. Much of the guidance can be treated as reference material and does not necessarily need to be read from beginning to end–this is particularly the case with the Operations Guide (chapters 11 and 12). To understand the architecture and design of the solution, though, you should at least read chapters 2 to 6 (the Planning Guide chapters) thoroughly.

Planning Guide — Chapters 2 to 6

This guide is the first in the solution. The Planning Guide has two main purposes: to help you make an informed decision about whether this solution is appropriate for your organization, and to provide a thorough understanding of the technical design of the solution and the reasoning behind the decisions that produced that design.

Conceptually, the guide is divided into three parts, each one a logical progression from the last. The first part (Chapter 2) addresses the business motivations for the adoption of WLANs and weighs them against the security threats that expose serious vulnerabilities

in many WLAN implementations. This discussion is used as the basis to propose a strategy for securely implementing WLANs. The second part (Chapter 3) develops a logical solution design from the proposed WLAN strategy and identifies the major components to be implemented. The third part consists of Chapters 4, 5, and 6, which are the major portion of the guide. These chapters define the detailed design for each of the components identified in Chapter 3. Detailed information about the content of these chapters is provided in the following subsections.

Unlike many planning guides, this one is intentionally prescriptive. The purpose is to produce a single design that can act as a reference for this type of solution. At points in the document where different design options are available, the rationale behind the decision taken is discussed. Where appropriate, optional strategies are indicated and the chapters should provide enough information to diverge from the design if you need to do so. The intent throughout the entire guide, though, is to arrive at a single solution that has actually been implemented and tested to work exactly as described in the solution guides.

The primary audience for this guide is IT architects and business decision makers (although only Chapter 2 is particularly relevant to the latter). Architects will want to focus on chapters 2 and 3 and at least the high–level points of the remaining chapters. IT professionals engaged in building, deployment, and management of this solution will also want to familiarize themselves with the overall architecture and design of the solution presented in these chapters.

IT security professionals will want to read through the chapters in this guide—particularly the latter chapters. It is essential that those responsible for IT security in your organization read and approve the design, build, and operational instructions prior to any deployment and before the system enters into production.

Chapter 2: Deciding on a Secure Wireless Networking Strategy

This chapter focuses on the selection of a technical solution for secure wireless networking. The chapter looks at the business reasons driving the adoption of WLAN technology and the security hurdles that must be overcome to make it safely adoptable. It then discusses the options for addressing these security problems and proposes a solution based on strong authentication and data protection that uses public key certificates. The decision is based on the assessed security needs of medium to large organizations, and balances immediate needs for robust security with a longer-term view of how well the solution protects the organization's investment.

Chapter 3: Secure Wireless LAN Solution Architecture

This chapter focuses on the architectural design of the secure wireless solution. The starting point is an overview of how a WLAN solution based on 802.1X and EAP–TLS (Extensible Authentication Protocol–Transport Layer Security protocol) works and the following key components of this solution:

- A WLAN infrastructure that supports robust authentication and data protection standards.
- A RADIUS authentication infrastructure.
- A PKI.

The security requirements from the previous chapter are brought together with a profile of the target organization to create a set of design criteria for the solution. A logical design based on these criteria is then described showing the options for scaling the design to suit organizations of different sizes.

Finally, the chapter illustrates some of the ways in which the proposed design can be used as a basis for building other network access solutions, such as virtual private networking (VPN) and wired network access control solutions. There is also a brief discussion of how the PKI component of the design can support a broad variety of security services and applications.

Chapter 4: Designing the Public Key Infrastructure

This chapter explains the design of a PKI based on Microsoft Certificate Services. In addition to WLAN security, it is likely that many organizations will want to use their PKIs for other applications, such as secure e–mail, file encryption, and smart card logon. The design is therefore a balance between a relatively simple and low-cost certificate solution for secure WLANs and one that provides enough flexibility and security to be extended to support many different applications.

The documentation of your certificate needs is followed by the design of an appropriate certification authority (CA) hierarchy. Integrating the CAs with Active Directory, Internet Information Services (IIS), and other PKIs is also discussed. Finally, the development of a certificate management plan and creating certificate templates is discussed.

Chapter 5: Designing a RADIUS Infrastructure for Wireless LAN Security

This chapter provides a detailed design of the RADIUS infrastructure. This infrastructure provides strong authentication and secure key management services to the WLAN. The chapter explains how RADIUS, implemented using Microsoft Internet Authentication Service (IAS), can provide a broad network access management solution and how it works with WLANs in particular. It enumerates the environmental prerequisites for the solution and discusses in detail the design decisions involved in architecting a RADIUS infrastructure for an 802.1X WLAN. Also discussed are the management strategies for maintaining the IAS server infrastructure over an extended period of time.

Chapter 6: Designing Wireless LAN Security Using 802.1X

Chapter 6 describes the architecture and design of the security aspects of wireless networking. (Wireless network design issues not related to security are not discussed.) Topics include how an 802.1X–based solution addresses the security flaws in basic Wired Equivalent Privacy (WEP) WLANs, the decision to use certificates rather than passwords, and identifying the prerequisites for a successful deployment. Subsequent sections deal with selection of WLAN security options and the configuration of those options into RADIUS access policy, wireless access points (APs), and clients (using Group Policy). Finally, the chapter discusses some key deployment issues such as dealing with roaming profiles and bootstrapping the configuration of wireless-only clients.

Build Guide — Chapters 7 to 9

The Build Guide provides step–by–step instructions for implementing all of the components of the solution: a PKI based on Windows Server 2003 Certificate Services, a RADIUS infrastructure based on IAS, and the configuration of wireless access points (APs) and clients. Each chapter contains detailed procedures for installing and securing the operating system, configuring software components, and integrating them into the solution. Each major step is linked with verification procedures to help minimize errors.

The primary audience for this guide is IT professionals engaged in the design, build, and deployment of the PKI, RADIUS, and WLAN components. Included in this audience description are IT engineering professionals engaged in the design and specification of IT

infrastructures and IT delivery professionals engaged in the deployment of solutions in production environments.

IT architects will want to read through the build steps to ensure that the solution conforms to their organization's standards and practices. However, much of the detail contained in these chapters will not be relevant to them. IT security professionals will want to read through this guide after having read the Planning Guide. As stated previously, it is important that those responsible for IT security in your organization read and approve the design, build, and operational instructions prior to any deployment.

IT support and operations managers responsible for the components of this solution will want to skim through these chapters to understand the interdependencies between the solution components and the rest of the IT infrastructure. Technical support professionals will need to use this guide and the Planning Guide chapters as a reference.

Chapter 7: Implementing the Public Key Infrastructure

This chapter gives detailed instructions for building the solution's PKI, including preparing the hardware and operating system for the CA servers, applying security policies to the servers, and preparing the supporting infrastructure for the PKI (Active Directory and IIS). Next, Certificate Services is installed and configured to build an offline root and issuing CAs. The configuration of client PKI settings using Active Directory and Group Policy is also explained, as well as the delegation of configuration and management tasks. This provides the certificate infrastructure used by later chapters of this guide to build the complete solution.

Chapter 8: Implementing the RADIUS Infrastructure

This chapter describes implementing the solution's RADIUS infrastructure, including preparing and building the servers, applying security policies, preparing Active Directory security groups, and configuring IAS on each server. The result is a resilient RADIUS infrastructure that provides the solution's authentication and authorization components.

Chapter 9: Implementing Wireless LAN Security

This chapter explains how to configure the WLAN security solution with the PKI and RADIUS components built in the earlier chapters. Topics include preparing the network infrastructure (DHCP and Active Directory), creating and issuing the correct certificate types, creating the remote access policies on the IAS servers, and configuring the wireless APs to use on the new RADIUS infrastructure. This chapter completes the installation of the solution.

Operations Guide — Chapters 10 to 12

The Operations Guide outlines procedures for long-term maintenance of the solution components. Based on Microsoft Solutions for Management (MSM), the guide provides a complete set of tasks and instructions to operate, monitor, change, and support the Certificate Services and IAS components. Included are setup tasks to implement the management system (including regular daily and weekly health-checking and monitoring scripts), backup and recovery procedures, and troubleshooting resources.

Unlike other guides in this solution, these chapters do not need to be read from beginning to end. Each of the main chapters has two parts. The first part is relatively short and is intended to provide all of the necessary information to plan and set up your operational processes and operational technical infrastructure. You should read this first part completely. The second part is primarily reference material documenting all of the operations and support tasks needed to maintain the solution components.

The primary audience for this guide is IT professionals engaged in managing the PKI, RADIUS, and WLAN components of this solution. In many organizations, different people or even different parts of the organization may be responsible for the maintenance of different components of the solution–so not all of the chapters may be of interest to these different groups.

IT architects will want to familiarize themselves with the content of these chapters to understand the overall impact that the operational requirements the solution has on the IT infrastructure as a whole. However, much of the detail contained in these chapters will not be relevant to them. If the architects make any changes to the design described in the Planning Guide, they must communicate these changes to IT service management so that relevant changes to the operational guide can be made.

IT professionals engaged in building and deploying IT infrastructure for your organization will need to be broadly familiar with the contents so that they can effectively communicate relevant information about the build and deployment of the solution to IT service management staff.

IT security professionals will want to read through this guide after having read the Planning and Build guides to ensure that the operational practices are in line with corporate security standards.

Chapter 10: Introduction to the Operations Guide

This chapter provides background information on the Microsoft Operations Framework (MOF) and is important for a proper understanding of the following two chapters. If you are not familiar with MOF concepts, you should read some of the background information referenced in the "More Information" section at the end of this chapter.

Chapter 11: Managing the Public Key Infrastructure

This chapter is designed to enable you to implement a full management system for your PKI. Topics include all of the set up tasks needed to begin monitoring and maintaining the system, the regular operational tasks needed to keep it working properly, and procedures to help you deal with support incidents, manage changes to the environment, and optimize the performance of the system.

Chapter 12: Managing the RADIUS and Wireless LAN Security Infrastructure

This chapter is designed to enable you to implement a full management system for your Remote Authentication Dial–In Server (RADIUS) and wireless LAN (WLAN) security infrastructure. Like the previous chapter, it includes all of the setup tasks needed to begin monitoring and maintaining the system, the regular operational tasks needed to keep it working properly, and procedures to help you deal with support incidents, manage changes to the environment, and optimize the performance of the system.

Test Guide — Chapter 13

The Test Guide consists of one chapter—Chapter 13—and explains the overall test strategy that Microsoft used to validate this solution. It also describes the primary test cases that you can use to validate the solution in your own labs. The chapter was developed from the test processes and test cases that Microsoft used to validate the solution in its own labs; the complete set of test cases are included. This solution was also penetration tested by a third party.

Appendixes and Supplementary Files

The following appendixes are included with the solution guides.

Appendix A: Platform Support Matrix

This appendix is a table that details which operating system versions are supported for the wireless clients and for the various server roles in the solution.

Appendix B: Scripts and Support Files

The procedures in the Build Guide and Operations Guide chapters use a number of scripts and other support files. This appendix describes them, as well as the separate Readme.txt file included with the scripts.

Appendix C: Delivery Guide

This appendix outlines a framework based on Microsoft Solutions Framework (MSF) and MSM, which can be used to help implement the solution.

Appendix D: WPA Support

This appendix contains information about the status of the solution's support for WiFi Protected Access (WPA) security. The solution was designed to support WPA, and WPA is referred to throughout much of the guidance. Support for WPA in Windows XP and in WLAN adapters and access points, however, was in the early stages of shipping as the solution was being developed.

Style Conventions

The following table describes style conventions used in this book.

Table 1.1 Style Conventions

Element	Meaning
Bold font	Characters that are typed exactly as shown, including commands and switches. User interface elements in text that is prescriptive are also bold.
Italic font	Italic font is used in two contexts: –Where italics are used within the main body of the text, they indicate the title of another document. –Where italics are used within commands or code (or text referring to a command or code), they indicate a placeholder for variables where specific values need to be supplied. For example, *Filename.ext* indicates that you should replace the italicized *Filename.ext* with the file name of your choice
Screen Text	For text displayed on the screen (for example, the output from a command line tool) and for commands that need to typed in at the command line. Some commands do not fit within the page margins. Where this occurs, the command text is wrapped onto multiple lines with subsequent lines indented (this is indicated by a note following the command).
`Monospace font`	Code samples and contents of configuration files.
%SystemRoot%	The folder in which the Windows operating system is installed.
Note	Alerts the reader to supplementary information.
Important	Alerts the reader to supplementary information that is essential to the completion of the task.
Caution	Alerts the reader that failure to take or avoid a specific action could result in the loss of data.
Warning	Alerts the reader that failure to take or avoid a specific action could result in physical harm to the user or hardware.

Support and Feedback

For additional support with implementing the technologies discussed in this solution, you may want to contact your local Microsoft office or a Microsoft Services partner.

- To find your local Microsoft office, visit the Microsoft Worldwide Web site at www.microsoft.com/worldwide/ and select the appropriate country/region.
- To find a Microsoft partner in your region, search in the **Solutions and Services** section of the Microsoft Resource Directory at http://directory.microsoft.com/ResourceDirectory/Solutions.aspx
- For more information about how the Windows Server 2003 components used in this solution are supported, including escalation paths, support offerings, resources and support levels, see the Microsoft Help and Support Web site at http://support.microsoft.com

Microsoft would like your feedback on this material. In particular, please try to answer the following questions:

- How useful was the information provided?
- Were the step-by-step procedures accurate?
- Were the chapters readable and interesting?
- Overall, how would you rate the solution?

Send your feedback to the following e-mail address: SecWish@Microsoft.com