Solution Accelerators –
Security and Compliance
and the
Security Center of Excellence

The Secure Access Using Smart
Cards Planning Guide

Version 1.1

Published: June 2005   Updated: May 2007
For the latest information, please see
microsoft.com/technet/SolutionAccelerators
Table of Contents

Chapter 1: Introduction ............................................................... 1
  Executive Summary ..................................................................... 1
  The Business Challenge ............................................................ 2
  The Business Benefits ............................................................. 2
  Who Should Read This Guide .................................................... 3
  Reader Prerequisites ............................................................... 3
  Planning Guide Overview ......................................................... 3

Chapter 2: Smart Card Technologies ............................................. 5
  Two-Factor Authentication ........................................................ 5
  Hardware Tokens ..................................................................... 5
  Smart Cards ........................................................................... 5
  Implementation Prerequisites .................................................... 6
  Identification of Accounts ........................................................ 6
  Smart Card Infrastructure Support .......................................... 7
  Evaluating Smart Cards .......................................................... 10
  Evaluating Smart Card Readers .............................................. 12
  The Woodgrove National Bank Scenario .................................. 13
  Summary .............................................................................. 14

Chapter 3: Using Smart Cards to Help Secure Administrator Accounts 15
  Approaches to Securing Administrator Accounts with Smart Cards ........................................................................... 15
  Identification of Administrator Accounts and Groups ............... 16
  Require Smart Card for Interactive Logon ................................. 17
  Managing Smart Card Access in Multiple Domains and Forests ......................................................................................... 18
  Securing Servers ..................................................................... 19
  Installing Smart Card Readers on Servers .................................. 20
  Distributing Smart Cards ........................................................ 20
  Activating Smart Cards .......................................................... 20
  Managing Smart Cards ........................................................... 21
  Monitoring Smart Card Use ..................................................... 22
  Issues and Requirements ........................................................ 22
  Background ........................................................................... 23
  Business Issues ...................................................................... 23
  Technical Issues ..................................................................... 23
  Security Issues ..................................................................... 23
  Solution Requirements .......................................................... 24
  Designing the Solution ............................................................ 24
  Solution Concept ................................................................... 25
  Solution Prerequisites ............................................................ 25
  Solution Architecture ............................................................ 26
  How the Solution Works .......................................................... 28
  Extending the Solution ........................................................... 29
  Summary .............................................................................. 29

Chapter 4: Using Smart Cards to Help Secure Remote Access Accounts 31
  Securing Remote Access with Smart Cards .................................. 31
  Client Requirements ............................................................... 31
  Server Requirements ............................................................. 33
  Identify Authentication Server Requirements ............................. 33
  Distribution and the Enrollment of the Smart Cards for Remote Access ................................................................. 34
  Further Considerations ........................................................... 34
  Issues and Requirements ......................................................... 36
Woodgrove National Bank Scenario Background .......................................................... 36
Business Issues ........................................................................................................... 36
Technical Issues ......................................................................................................... 37
Security Issues ........................................................................................................... 37
Solution Requirements .............................................................................................. 38
Designing the Solution ............................................................................................... 39
Solution Concept ...................................................................................................... 39
Solution Prerequisites ............................................................................................... 40
Solution Architecture ............................................................................................... 41
How the Solution Works ............................................................................................ 42
Additional Design Considerations ............................................................................. 43
Monitoring and Management .................................................................................... 47
Summary ..................................................................................................................... 49

Appendix A: Related Links ......................................................................................... 51
Introduction

Executive Summary

Administrators are increasingly aware of the dangers that result if they rely only on user names and passwords to provide authentication to network resources. Attackers can guess user names, or use such publicly available information as an e-mail address on a business card to identify a user name. When an attacker knows a user name, the only security mechanism that remains is a user’s password.

Single secrets such as passwords can be effective security controls. A long password of more than 10 characters that consists of random letters, numbers, and special characters can be very difficult to crack. Unfortunately, users cannot always remember these sorts of passwords, partly due to fundamental human limitations.

Research by George A Miller, published in *The Psychological Review* in 1956, concluded that the human brain has a short-term memory limit of between five and nine random characters, with an average of seven. However, most security guidance recommends at least an eight-character random password. Because most users cannot commit an eight-character random password to memory, many opt to write it down on a piece of paper.

Users rarely show great discretion when they write down passwords, and so provide opportunities for attackers to compromise their credentials. Where there are no restrictions on password complexity, users tend to choose easy to remember passwords such as "password" or other easily guessed words.

Pass phrases are longer passwords that users can remember more easily. Microsoft® Windows® 2000, and later versions of the Windows operating system, supports passwords of up to 127 characters in length. A strong pass phrase such as "I like 5-a-side football!" significantly increases the difficulty for tools that use brute force methods to crack a password and is easier for a user to remember than a random mix of letters and numbers.

Two-factor authentication systems overcome the issues of single secret authentication by the requirement of a second secret. Two-factor authentication uses a combination of the following items:

- Something that the user has, such as a hardware token or a smart card.
- Something the user knows, such as a personal identification number (PIN).

Smart cards and their associated PINs are an increasingly popular, reliable, and cost-effective form of two-factor authentication. With the right controls in place, the user must have the smart card and know the PIN to gain access to network resources. The
two-factor requirement significantly reduces the likelihood of unauthorized access to an organization’s network.

Smart cards provide particularly effective security control in two scenarios: to secure administrator accounts and to secure remote access. This guide concentrates on these two scenarios as the priority areas in which to implement smart cards.

Because administrator-level accounts have a wide range of user rights, compromise of one of these accounts can give an intruder access to all network resources. It is essential to safeguard administrator-level access because the theft of domain administrator-level account credentials jeopardizes the integrity of the domain, and possibly the entire forest, together with any other trusting forests. Two-factor authentication is essential for administrator authentication.

Organizations can provide an important additional layer of security if they implement smart cards for users who require remote connectivity to network resources. Two-factor authentication is particularly important with remote users, because it is not possible to provide any form of physical access control for remote connections. Two-factor authentication with smart cards can increase security on the authentication process for remote users who connect through virtual private network (VPN) links.

The Business Challenge

Compromise of administrator account credentials on domain-joined computers can jeopardize the integrity of the entire domain, the forest in which that domain resides, and other forests and domains that have trust relationships to that forest. The compromise of remote access accounts can result in the access of sensitive information through dial-up or VPN connections by external attackers.

The business challenge to safeguard administrator and remote access connections is to provide a suitable level of security that does not compromise usability. An organization that implements two-factor authentication to improve security cannot run at optimal efficiency if users cannot access the information that they need to do their jobs. It is of critical importance to balance two-factor authentication against usability.

The Business Benefits

The use of smart cards to secure critical accounts can produce the business benefits that follow:

- **Greater protection for sensitive data.** Smart cards reduce the threat of unauthorized access by the use of stolen credentials because the hacker must both steal the smart card and obtain the PIN.
- **Better security for logon credentials.** Smart cards use digital certificates for logon credentials, which are difficult to forge.
- **Higher levels of regulatory compliance.** Being able to identify that the logged-on user is who they say they are provides greater credibility to monitored logs.
- **Lower probability of repudiation.** Smart card authentication reduces the ability of individuals to deny their actions.
- **Better integration with access management systems.** Some smart cards also function as key cards to manage physical access, such as controlled door locks to access a physical site and between sectors within the site. The combination of smart card and key card makes it easy to control the exact level of network and physical access for a user or an administrator, and reduces the fear of security compromise.
Who Should Read This Guide

The intended audience for this guide includes technical decision makers, enterprise architects and enterprise security administrators who will plan, deploy, or operate remote access links and network security. Consultants who will in plan, deploy, or operate Windows-based networks should also find this information useful.

The information in this guide applies to organizations of all sizes that require strong identity protection and data access control.

Reader Prerequisites

To understand the solutions presented in this guide, readers should understand and be familiar with the following areas and technologies in Microsoft Windows Server™ 2003:

- Routing and remote access, which includes VPN components
- Certificate Services and Public Key Infrastructure (PKI)
- The Active Directory® directory service
- Group Policy

This guide covers the Operating and Supporting process model quadrants within the Microsoft Operations Framework (MOF). It also covers the Security Administration and Incident Management service management functions (SMFs) within MOF. For more information about MOF, see the Microsoft Operations Framework Web site at www.microsoft.com/mof.

Planning Guide Overview

This guide includes four chapters that focus on the essential issues and concepts required to plan smart card authentication. These chapters are:

Chapter 1: Introduction

This chapter provides an executive summary, considers the business challenges faced and benefits gained if you implement smart card authentication. The chapter suggests the recommended audience for the guide, lists the reader prerequisites, and provides an overview of the chapters and solution scenarios.

Chapter 2: Smart Card Technologies

This chapter outlines the approaches in the use of smart cards to secure critical accounts. It also discusses the essential elements for the two solution scenarios that chapters 3 and 4 cover. Finally, this chapter introduces Woodgrove Bank, which is the basis of the two solution scenarios.

Chapter 3: Using Smart Cards to Help Secure Administrator Accounts

This chapter describes the design considerations required to secure administrator accounts with smart cards. The chapter goes on to examine the issues and requirements for Woodgrove Bank. It discusses the solution concept, prerequisites, solution architecture, and solution operation for the scenario. Finally, the chapter reviews possible options to extend the solution to incorporate the change management process.
Chapter 4: Using Smart Cards to Help Secure Remote Access Accounts

This chapter describes the design considerations for remote access with smart cards. The chapter goes on to examine the issues and requirements for the implementation of secure remote access for Woodgrove Bank. It discusses the solution concept, prerequisites, solution architecture, and solution operation for the scenario. Finally, the chapter reviews how to extend the solution to incorporate physical access control.
Networked data storage is an essential business requirement for nearly all organizations. Organizations often have to connect networks that contain sensitive and proprietary data to the Internet for communication and to generate revenue. The constant drive for greater connectivity exposes a significant security risk, because the majority of organizations use user names and passwords for authentication and to authorize access to network resources.

Chapter 1, “Introduction,” highlighted the main security issue with user name and password combinations. Because user names are not secret, only the password provides any effective security against an attacker who tries to impersonate a valid user. The realization of the vulnerability of user name and password credentials has resulted in increased interest in two-factor authentication systems.

Two-Factor Authentication

Two-factor authentication goes beyond the simple user name and password combination and requires a user to submit some form of unique token together with a PIN. A number of ways exist to implement two-factor authentication, and doubtless more will appear in the future.

Hardware Tokens

Hardware tokens are a two-factor authentication method whereby users have a physical item such as a key fob or a credit-card authenticator. This hardware provides a simple one-time authentication code, which typically changes every 60 seconds. Users must match the one-time code along with a secret PIN to identify themselves uniquely and gain access.

Hardware tokens provide many of the benefits of smart cards, but can involve a more complex plan and deployment process. Microsoft® Windows Server™ 2003 and Windows® XP do not provide built-in support for hardware tokens.

Smart Cards

Smart cards are credit card–sized plastic items that contain a microcomputer and a small amount of memory, which provide secure, tamper-proof storage for private keys and X.509 security certificates. Smart cards typically have 32 or 64 KB of Electrically Erasable Programmable Read Only Memory (EEPROM) and Read Only Memory (ROM), with just 1 KB of RAM. The ROM contains the smart card operating system, with the EEPROM that contains the file and directory structures, PIN management applet, and
authentication certificate. The RAM provides working memory for card operations, such as encryption and decryption.

To authenticate to a computer or over a remote access connection, the user inserts the smart card into a suitable reader and enters the PIN. The user cannot gain access with just the PIN, or with just the smart card. Brute force attacks on smart card PINs are not possible, because the smart card locks out after several unsuccessful attempts to enter the PIN. Because PINs are usually eight characters or less, they are easier to remember than long random character passwords. Smart cards are the two-factor authentication mechanism that Microsoft prefers.

**Note:** Smart card PINs do not have to be numeric. Smart card vendor development kits enable you to specify how many alphabetic, numeric, upper case, lower case, or non-alphanumeric characters you require.

Microsoft deploys smart cards for domain administrators and for remote access to network resources, and is keen to promote this practice as part of the defense-in-depth initiative. Microsoft Consulting Services, Premier Support, Customer Support Services, Microsoft partners, and other solution providers encourage organizations to use smart cards to secure network access.

The following list outlines the steps required to implement a smart card solution for network administrators:

- Enable the target servers to support interactive, secondary, and remote desktop logon with smart card–enabled accounts.
- Identify the administrators who must use a smart card–enabled domain-level administrator account.
- Deploy smart card readers.
- Develop a secure process to distribute the smart cards and enroll the administrators.

The following list outlines the process required to integrate a smart card solution for remote access:

- Upgrade remote access servers to support smart card authentication.
- Identify users who must use smart cards for remote access.
- Deploy smart card readers.
- Distribute smart cards to the appropriate administrators and enroll the remote users.

**Implementation Prerequisites**

Smart card deployment requires a planned approach to ensure that organizations consider all the issues before the start of the implementation phase. This section covers the most common prerequisites, although there might be additional requirements in your environment.

**Identification of Accounts**

The identification of the users and the groups that require smart card access is an important part of a smart card deployment.
Groups and users that require smart cards might include:

- Domain administrators for all domains in the forest
- Schema administrators
- Enterprise administrators
- Database administrators
- Human resource administrators
- Users who have remote access
- Users who have either user or administrative access to sensitive resources, such as accounting and finance information

An organization might also require smart card access for users and groups not in the previous list, such as board-level personnel. The identification of these accounts early in the process helps define the scope of the project and control costs.

To identify critical accounts, you must define when to use smart cards. For example, good security practice recommends that administrators have two user accounts: a standard account for daily tasks such as e-mail, and an administrator-level account for server maintenance and other administrative tasks. Usually, the administrator would log on with the user-level account, and use the Secondary Logon service to perform administrative tasks. Alternatively, the administrator can use the Remote Desktop for Administration component of Windows Server 2003, which supports smart card logon.

For more information about administrator accounts, see the Identification of Administrator Accounts and Groups section in Chapter 3, "Using Smart Cards to Help Secure Administrator Accounts."

**Smart Card Infrastructure Support**

Smart cards require a suitable infrastructure with support from the operating system and network elements. Microsoft provides support for smart card implementations that use the following components:

- Microsoft Certificate Services or external Public Key Infrastructure (PKI)
- Certificate templates
- Windows Server 2003
- The Active Directory® directory service
  - Security Groups
  - Group Policy
  - Enrollment Stations and Enrollment Agents
  - Activation Web Server
- Extensible Authentication Protocol—Transport Layer Security (EAP–TLS)—required for remote access solutions only

Additional components include enrollment stations and enrollment agents.

**Public Key Infrastructure**

Smart cards require a PKI to provide certificates with public key/private key pairs that enable account mapping in Active Directory. You can implement this PKI in one of two
ways: provision the internal certificate infrastructure to an external organization or use Certificate Services in Windows Server 2003. Organizations can outsource all or part of the certificate management process for smart cards.

Financial organizations can benefit if they link their PKI to an external trusted root for e-mail verification and for secure transactions with partner organizations. An alternate approach is to use Certificate Services in Windows Server 2003 to provide the PKI.


The PKI must have a mechanism that deals with certificate revocation. Certificate revocation is necessary when a certificate expires or when an attacker could have compromised a certificate. Each certificate includes the location of its certificate revocation list (CRL). For more information about how to manage certificate revocation, see the Manage Certificate Revocation topic at www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CS_procs_revocation.asp

Certificate Templates

Windows Server 2003 provides specific certificate templates to issue digital certificates for use in smart cards. You can copy and customize these certificates to fit your organization's requirements. The three certificate templates for smart card use are:

- **Enrollment Agent.** Allows an authorized user to request certificates for other users.
- **Smartcard User.** Lets a user log on with a smart card and sign e-mail. Also provides client authentication.
- **Smartcard Logon.** Enables a user to log on with a smart card and provides client authentication but does not enable signed e-mail.

Windows Server 2003, Enterprise Edition, provides version 2 (v2) templates that you can modify and extend to provide multiple capabilities such as logon, signed e-mail messages, and file encryption. You can also extend certificate templates to provide additional information that your organization requires, such as medical details or pension entitlements. Windows Server 2003, Enterprise Edition supports autoenrollment, which makes management of smart cards easier in a large organization. The certificate renewal request can use the current certificate to sign the request.

**Note:** Microsoft strongly recommends that you upgrade a current Windows Server 2003 PKI to a Windows Server 2003 with Service Pack 1 (SP1) PKI to take advantage of enhanced security features.


Windows Server 2003

Microsoft Windows 2000 Server supports smart cards for remote access and administrator authentication for console logon only. To implement smart cards for administrators requires that the managed servers run Windows Server 2003, which supports secondary actions such as smart card logon over remote desktop protocol (RDP) connections. This operating system requirement includes the domain controllers.
For more information about this requirement, see Chapter 3, "Using Smart Cards to Help Secure Administrator Accounts."

**Active Directory**

Active Directory is a key component for the implementation of smart card deployments. Active Directory in Windows Server 2003 contains built-in support to enforce smart card interactive logon and the ability to map accounts to certificates. This capability to map user accounts to certificates ties the private key on the smart card to the certificate held in Active Directory. The presentation of smart card credentials at logon requires Active Directory to match that specific card to a unique user account. For more information about certificate mapping, see the Map Certificates to User Accounts topic at www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssch_pki_cyek.asp.

Active Directory also supports security groups and Group Policy to facilitate management of the smart card logon process and smart card issuance.

**Security Groups**

The smart card deployment and management process is significantly easier if you use security groups within Active Directory to organize users. For example, a typical smart card deployment might require you to create the following security groups:

- **Smart card enrollment agents.** Smart card enrollment agents are responsible for distribution of smart cards to users. The next section covers enrollment agents in detail.
- **Smart card staging.** The smart card staging group contains all users who are authorized to receive smart cards, but for whom an enrollment agent has not yet enrolled and activated their cards.
- **Smart card users.** This group contains all users who have completed the enrollment process and have an activated smart card. The enrollment agent moves the user from the smart card staging group to the smart card users group.

For more information about how to create groups, see the Checklist: Creating a Group topic at www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_adgroups_checklist_create_group.asp.

**Group Policy**

Group Policy enables you to apply configuration settings to multiple computers. You can set up the requirement to use smart cards for interactive logon in a Group Policy object (GPO) and then apply that GPO to organizational units or sites in Active Directory. For more information about how to use Group Policy, see Chapter 3, "Using Smart Cards to Help Secure Administrator Accounts."

**Enrollment Stations and Enrollment Agents**

An organization can use a Web-based interface to issue or enroll users for smart cards, whereby users enter their credentials and obtain their smart card. However, this arrangement effectively downgrades the security for the smart card to the same level as the credentials presented to the Web interface. The preferred solution is to create enrollment stations and designate one or more administrators as enrollment agents.

**Note:** Organizations can use a Microsoft Management Console (MMC) interface or develop their own activation applications.
A typical enrollment station is a computer that has two smart card readers attached. One reader lets the enrollment agent log on and the other reader issues new smart cards to users. Enrollment stations require an enrollment certificate and must have permission to access the certificate templates. The enrollment station has a Group Policy setting that forces logoff as soon as the enrollment agent removes his smart card.

A designated administrator takes on the role of the enrollment agent and uses his smart card to log on to the enrollment station. He then opens the Web page for certificate services, verifies the identity of the user, enrolls the user, and issues the enrolled smart card.

Organizations should carefully consider the required number of enrollment stations, and the location of these stations. The organization might co-locate an enrollment station within its security department offices alongside the facilities that issue facility or site access and other security passes. To expedite the initial deployment in a large organization, teams of enrollment agents can use laptops as mobile enrollment stations in branch offices.

**Note:** To reduce administrative complexity and to control smart card enrollment, it is highly recommended that you restrict the numbers of enrollment agents and enrollment stations to the minimal number required for the deployment.

**Activation Web Server**

An activation Web server is a custom component that enables users to activate their new smart cards by PIN reset. Some vendor software development kits (SDKs) provide tools to assist in the construction of an activation Web server. Microsoft does not provide the activation server component.

To reset the PIN, the user runs a cryptographic service provider (CSP) utility that generates a hexadecimal challenge string from the smart card. The user enters this challenge string into a field on the Web page and the activation Web server generates a response. The user types the response into the response field in the utility, which then allows the user to set the smart card PIN.

The activation Web server can also be part of the management process. Help desk operators can use this process to unblock cards where the user has entered the incorrect PIN too many times. In this case, the user reads the challenge to the help desk operator, who replies with the response.

**EAP-TLS**

Certificate-based security environments use EAP-Transport Level Security (EAP-TLS) to provide the strongest authentication and key determination method. EAP-TLS provides mutual authentication, negotiation of the encryption method, and encrypted key determination between the client and the authenticator. RFC 2284 provides a detailed description of EAP.

**Evaluating Smart Cards**

The primary factor during the evaluation of smart cards is to ensure that the model you choose can support your planned key length. Windows Server 2003 supports certificate key lengths from 384 bits (low security) to 16,384 bits (maximum security).

Certificates that have longer key lengths provide greater security than shorter key lengths, but longer key lengths significantly increase the time to log on with a smart card. Memory limitations in the smart card also restrict the maximum key length you can use.
Chapter 2: Smart Card Technologies

Certificate key lengths of 1,024 bits are suitable to secure administrator accounts or to secure remote access. A certificate with a 1,024-bit key takes approximately 2.5 KB of memory space in the smart card. Other memory requirements include the operating system (16 KB), smart card vendor applications such as the CSP (8 KB), and the smart card file and directory structure (4 KB). Hence, smart cards that have less than 32 KB of memory are unlikely to be suitable for the storage of logon certificates and provide the required functionality to extend a smart card solution.

The second factor to consider is whether the card has built-in support for Windows Server 2003 and Windows XP. Before you purchase smart cards, discuss your requirements with the vendor.

**Note:** You should obtain smart cards directly from their respective vendors. Smart cards are not available from Microsoft.

Although Windows XP and the Windows Server 2003 family include built-in support for some smart cards, additional RSA-based cryptographic smart cards also function well with those operating systems. For those cards whose support is not included natively within Windows, the card vendor must implement a CSP for the card that uses the CryptoAPI.

For more information about the evaluation of smart cards, see the Evaluating Smart Cards and Readers topic at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/0eae38ec-d6e5-4ca7-96a3-42f2fd6c6e74.mspx.

**PIN Management**

A user can change the PIN for a smart card at any time by the use of a utility that enables the CSP to display the private key PIN dialog box. The user then enters the old PIN and the new PIN twice. Because users find it easier to remember PINs that they select, tools should be available to allow them to change their PIN.

**Note:** Users might need to be reminded not to set easily guessed PINs, such as their date of birth, car license plate, or telephone numbers.

The user is responsible for PIN management through the facilities that the CSP provides. Windows XP and the Windows Server 2003 family of operating systems do not manage PINs. For PIN management tools and instructions, contact your smart card vendor.

Most smart card vendors offer smart cards that integrate directly with Windows 2000 or later with no additional customization or development. Manufacturers supply these smart cards with a preset PIN and you can place restrictions on the card such as the card requires a PIN reset on enrollment. However, many enterprises do not find this arrangement acceptable.

To create a more complex and secure PIN, use the PIN management tools to require that users choose a PIN of between five and eight characters in length. Make sure the smart card manufacturer you select supports PINs of up to eight characters.

**Smart Card Software Development Kits**

Microsoft does not provide an off-the-shelf solution for smart card deployment. You might have to provide additional customization if your environment requires it.

Smart card vendors offer SDKs and personalization tools that enable organizations to customize their smart card deployments. For example, developers can use an SDK to
issue smart cards in a pending state. When the enrollment agent issues the card, the user activates the card and changes the PIN. If you want to take advantage of the greater security this method provides, you must budget for additional customization and development.

**Evaluating Smart Card Readers**

The principal factor when you select a suitable smart card reader is to choose one that is best suited to its purpose. For example, a modern workstation that sits underneath an administrator's desk has two or more USB connections, so a USB smart card reader is probably the most appropriate choice. The user can attach the smart card reader to the side of his monitor or place the reader in another convenient location. Users that make remote access connections from laptops usually prefer a smart card reader in the PC card format.

Keyboards can include smart card readers that also work through a USB interface. These keyboards are suitable for use with a single computer, and might work with multiple computers in server racks through USB-equipped Keyboard Video Mouse (KVM) switches. Check with your chosen KVM switch manufacturer to see whether their KVM switches support smart card authentication to multiple servers.

Windows XP and the Windows Server 2003 family support the smart card readers listed in the following table. Windows installs the correct drivers upon detection of the Plug and Play smart card reader hardware.

**Note:** Microsoft strongly recommends that you use smart card readers that have obtained the Windows-compatible logo.

<table>
<thead>
<tr>
<th>Brand</th>
<th>Model</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express</td>
<td>GCR435</td>
<td>USB</td>
</tr>
<tr>
<td>Bull</td>
<td>SmarTLP3</td>
<td>Serial</td>
</tr>
<tr>
<td>Compaq</td>
<td>Serial reader</td>
<td>Serial</td>
</tr>
<tr>
<td>Gemplus</td>
<td>GCR410P</td>
<td>Serial</td>
</tr>
<tr>
<td>Gemplus</td>
<td>GPR400</td>
<td>PCMCIA</td>
</tr>
<tr>
<td>Gemplus</td>
<td>GemPC430</td>
<td>USB</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>ProtectTools</td>
<td>Serial</td>
</tr>
<tr>
<td>Litronic</td>
<td>220P</td>
<td>Serial</td>
</tr>
<tr>
<td>Schlumberger</td>
<td>Reflex 20</td>
<td>PCMCIA</td>
</tr>
<tr>
<td>Schlumberger</td>
<td>Reflex 72</td>
<td>Serial</td>
</tr>
<tr>
<td>Schlumberger</td>
<td>Reflex Lite</td>
<td>Serial</td>
</tr>
<tr>
<td>SConnection Manager Microsystems</td>
<td>SCR111</td>
<td>Serial</td>
</tr>
<tr>
<td>SConnection Manager Microsystems</td>
<td>SCR200</td>
<td>Serial</td>
</tr>
<tr>
<td>SConnection Manager Microsystems</td>
<td>SCR120</td>
<td>PCMCIA</td>
</tr>
<tr>
<td>SConnection Manager Microsystems</td>
<td>SCR300</td>
<td>USB</td>
</tr>
<tr>
<td>Brand</td>
<td>Model</td>
<td>Interface</td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
<td>-----------</td>
</tr>
<tr>
<td>Systemneeds</td>
<td>External</td>
<td>Serial</td>
</tr>
<tr>
<td>Omnikey AG</td>
<td>2010</td>
<td>Serial</td>
</tr>
<tr>
<td>Omnikey AG</td>
<td>2020</td>
<td>USB</td>
</tr>
<tr>
<td>Omnikey AG</td>
<td>4000</td>
<td>PCMCIA</td>
</tr>
</tbody>
</table>

1. **Note:** Smart card readers that use a serial interface require a computer restart after installation. This requirement might not be acceptable for server implementations.

Microsoft neither supports nor recommends the use of smart card readers that are not Plug and Play. If you use such a reader, you must obtain installation instructions (this includes associated device driver software) directly from the manufacturer of the smart card reader.

### The Woodgrove National Bank Scenario

The chapters that remain of this guide use the Woodgrove National Bank scenario. Woodgrove National Bank is a fictional global investment bank that serves institutional, corporate, government, and individual clients in its role as a financial intermediary. Its business includes securities, sales and trading, financial advisory services, investment research, venture capital, and brokerage services for financial institutions.

Woodgrove National Bank employs more than 15,000 people in more than 60 offices worldwide. They have corporate headquarters (hub locations) that have large numbers of employees in New York (5,000 employees), London (5,200 employees), and Tokyo (500 employees). Each hub location supports several offices.

Although Woodgrove National Bank has a mixed server environment with Windows Server and UNIX, their infrastructure runs on a Windows Server backbone. They have 1,712 Windows servers, most of which run Windows Server 2003. About 100 of these servers are Internet-facing. There are also 18,000 workstations within the organization, and 2,000 laptops. The organization is in the process of setting a baseline that standardizes on Windows XP Professional with SP2 and a server standard of Windows Server 2003 with SP1.

The majority of servers are located in three corporate headquarters locations. The organization has distributed the workstations and laptops throughout all locations. The laptops often move between countries or regions. Woodgrove National Bank uses Microsoft Systems Management Server 2003 to manage desktop and laptop computers and Microsoft Operations Manager (MOM) 2005 to manage servers.

Woodgrove National Bank must operate within the requirements of the relevant financial regulatory frameworks for each country/region in which it operates. It must also comply with all applicable data protection legislation and demonstrate effective operational security.

The remainder of this document describes the design choices available to Woodgrove National Bank as they planned their smart card deployment.
Summary

This chapter described common considerations needed to plan smart card authentication solutions. This includes the prerequisites, such as a PKI and Active Directory. It outlined the need to evaluate smart cards and smart card readers, covered the issues of smart card memory, key length, and PIN management. The chapters that follow concentrate on the unique aspects of using smart cards to help secure administrator accounts and to help secure remote access to networks.
Microsoft® Windows Server™ 2003 enables organizations to help secure administrative accounts through a set of specific account security features. In addition to the requirement that administrators log on with smart cards, Windows Server 2003 supports smart card authentication with the listed secondary actions:

- Create a mapped drive with the `net use` command.
- Use the Secondary Logon service by typing `runas` at the command prompt.
- Install the Active Directory® directory service by using the Active Directory Installation Wizard (which you can access if you type `dcpromo` at the command prompt).
- Log on through Windows Server 2003 Remote Desktop sessions
- Log on through Windows Server 2003 Terminal Server sessions

**Note:** Although Microsoft Windows® 2000 supports smart card access for authentication, it does not support these additional features, which are available in Windows Server 2003 only.

**Approaches to Securing Administrator Accounts with Smart Cards**

Windows Server 2003 support for smart card authentication of secondary actions enables better segregation of user and administrator accounts. For everyday actions, administrators can log on to workstations with non-administrative accounts. If they must perform an administrative task, administrators can use their smart cards to authenticate the action by use of a secondary action. This is a more secure and convenient arrangement than if the administrator is required to enter a user name and a password or required to log off and log on again with an administrator account.
Identification of Administrator Accounts and Groups

The implementation of smart cards for administrators requires that an organization identify the administrator accounts that require two-factor authentication. To perform this step correctly, you must understand the characteristics of the various administrator accounts and groups within Windows XP and Windows Server 2003.

Groups allow administrators to manage several user accounts together. Microsoft Windows NT® and later operating systems include security groups with built-in administrative rights.

These security groups can be local groups (on domain-joined computers such as workstations and member servers) or default groups (on domain controllers). Administrator accounts receive their privileges through membership of one or more of these security groups.

Local Groups

The local groups on domain-joined computers have varying levels of administrative rights. These include:

- **Administrators.** Members of this group have complete control of the local computer. The Administrator user account is a member of this group by default. If the computer is a member of a domain, the Domain Admins group for that domain is also a member of this group.

- **Backup Operators (all computer types).** Members of this group can bypass NTFS file system permissions to back up files and folders. Backup Operators can also shut down member servers.

- **Power Users.** Members of this group have limited administrative rights over resources on a local workstation or member server. They can also shut down a member server.

- **Print Operators.** Members of this group can manage print servers, printers, and print jobs. They can also shut down a member server.


Your organizational security policies should define which members of the Administrators, Server Operators, and Power Users groups require smart cards for logon and administration.

Default Groups

Each domain has a number of default groups that provide administrative functions on domain controllers. These groups include:

- **Administrators.** Members of this group have complete administrative control over domain controllers. The Administrator account and the Domain Admins group are members of this group by default.

- **Backup Operators.** Members of this group can bypass NTFS file system permissions to back up files and folders. Backup Operators can also log on locally and shut down domain controllers.

- **Server Operators.** This group has limited administrative rights on domain controllers, similar to Power Users on workstations. Server operators can log on locally and shut down domain controllers.
● **Print Operators.** Members of this group manage print servers, printers, and print jobs. They can also log on locally and shut down domain controllers.

● **Account Operators.** Members of this group have limited rights to manage user accounts and groups. They can log on interactively but cannot shut down domain controllers.

For more information about default groups, see the Default groups topic at http://go.microsoft.com/fwlink/?linkid=81737.

Your organization policies should specify that all members of these groups require smart cards for administration.

### Domain and Forest Default Groups

In addition to the default groups, creation of an Active Directory forest sets up the following security groups:

● **Domain Admins.** Members of this group have complete control over all objects in the domain. Each subsequent domain in the forest also has a Domain Admins group.

● **Enterprise Admins (forest root domain only).** Members of this group have complete control of all objects in the forest.

● **Schema Admins (forest root domain only).** Members of this group can create classes and attributes in the schema, as well as manage the schema operations master.

**Note:** To increase security, keep membership of these three groups to a minimum.

All members of these groups should require smart cards for administration.

### Require Smart Card for Interactive Logon

There are two ways to require a smart card for interactive logon. You can configure:

● User account properties in Active Directory Users and Computers.

● Group Policy for specific computers or for groups of specific computers.

In most environments, the most manageable approach is to use Group Policy.

### User Account Properties

You can configure any user account to require a smart card for interactive logon. To do this, in Active Directory Users and Computers, double-click the user, click the Account tab, under **Account Options**, select the **Smart card is required for interactive logon under Account Options** check box. The selection of this option changes the user's password to a random complex value and sets the property **Password never expires**. If you then turn off the smart card requirement, you must also reset the user's password.

Because setting the smart card requirement resets the user's password to an unknown value, the user can no longer use a user name and password combination to log on to the domain. Hence, the user cannot log on to programs such as Microsoft Outlook® Web Access for Microsoft Exchange Server 2003 with a user name and password.

You could use a script to enable this setting during enrollment. However, this method requires you to develop suitable scripts that can enable and disable the smart card requirement for selected individuals.
With the user account smart card requirement selected, the administrator must use a smart card to log on interactively to any computer in the domain, not just the protected servers. This could be inconvenient if not all computers have smart card readers.

If you enforce smart card use through the user account properties, administrators cannot remotely administer computers that run Windows 2000 Server. Windows 2000 Server Terminal Services sessions don't support smart card redirection, so the administrator must log on locally to manage any computers that run Windows 2000. This requirement could be very inconvenient if the administrator is at a different location from the server.

**Group Policy**

A more manageable approach is to use Group Policy settings to specify that certain computers require smart cards for interactive logon, and to control what happens when a user removes a smart card. You can create Group Policy objects (GPOs) with these settings configured and link the GPOs to the organizational unit (OU) that contains the computer for which you require smart card logon. The path to the smart cards options in Group Policy is Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options. The settings are **Interactive logon: Require smart card** and **Interactive Logon: Smart card removal behavior**.

**Note:** This setting requires either Windows XP with Service Pack 2 or an update for this setting. For more information, see the Update for the "interactive logon: require smart card" security setting in Windows XP Knowledge Base article at [http://support.microsoft.com/?id=834875](http://support.microsoft.com/?id=834875).

For greatest security, you should require smart cards for interactive logon and then set the smart card removal policy to lock the workstation or log off the user. These Group Policy settings should become part of a customized GPO that applies to administrators. GPOs can apply to the site, domain, or OU level. In most cases, GPOs that apply smart card settings apply to an OU.

**Note:** Microsoft recommends that you not modify the Default Domain Controllers Policy or the Default Domain Policy to include smart card settings or any other policy changes. Always create a new GPO or use a GPO that exists to set Group Policy settings for smart card logon.

The Group Policy settings for smart cards control interactive logon and do not affect access to a server across the network. Interactive logon includes logging on with Remote Desktop or Terminal Services.

Microsoft recommends that you implement smart cards for administrators with other control mechanisms such as IPsec or Group Policy settings to prevent the management of a server with remote administration tools such as Microsoft Management Console (MMC) tools.

**Managing Smart Card Access in Multiple Domains and Forests**

The implementation of smart cards for administrators requires that you understand the issues involved with multiple domains and forests. For example, administrators who are members of the Domain Admins group in more than one forest might need one smart card for each forest in which they have administrative rights. This requirement can result in these administrators having to carry several smart cards.
Although smart cards can contain more than one certificate, Windows Server 2003 currently can only accept one smart card logon certificate (the certificate held in slot 0 on the smart card) for each certification authority (CA) certificate root. This constraint might require some network administrators to carry multiple smart cards unless the organization has trust relationships between forests.

Securing Servers
Computers that run services, such as file and print, databases, e-mail, and directories, require higher levels of security than workstations. In particular, you should consider the use of smart card authentication for all accounts that administer computers that have the following roles:

- Domain controllers
- Database servers
- Certificate servers
- File and print servers

Securing Domain Controllers
Domain controllers are the most important computers for the use of two-factor authentication, because these computers contain and control all of the domain account information and apply security rules to each account. If an attacker compromises a domain controller, the attacker could then create a new account, escalate privileges, or access all domain controllers as an administrator.

Securing Database Servers
A database server stores information that is critical to the operation of an organization. This stored information might be subject to strict check-in and check-out processes, with audit tracking of data access requests. Examples of database servers include servers that store the source code for a software company, the secret recipes of a beverage manufacturer, or customer account information. Smart card authentication should secure access to all database servers.

An organization should identify high security servers, and work with their owners to change the type of account on which the service or scheduled task runs, or place the accounts and servers into special security groups that have greater access and user restrictions.

Securing Certificate Servers
The servers that host certification authorities and Certificate Services must have a high level of security. The compromise of the certification authority voids the integrity of the organization, rendering all issued certificates as insecure. Servers that host Certificate Services must have the highest security priority both from the network and for physical access.

Securing File and Print Servers
A file server can host important company documents and confidential information. The compromise of this information could harm future revenues or incur penalties from regulatory organizations. Smart card authentication must definitely secure print servers that print invoices or bank checks.

Installing Smart Card Readers on Servers

You must attach a smart card reader to every server on which Group Policy requires smart cards for interactive logon. Most rack-mounted computers have USB ports at the back that are suitable for use with smart card readers. You can then place the smart card reader at the front of the rack for user access. It is important to label the smart card readers clearly, so that administrators know which reader belongs to which server.

If an administrator has to log on to another server, he must remove his smart card from the first reader and insert it into the reader attached to the other computer. This inconvenience makes the administration of servers with Remote Desktop significantly more attractive.

Distributing Smart Cards

To plan the process for the distribution of smart cards for administrators includes the following activities:

- Create suitable groups for smart cards distribution.
- Appoint security officers who can act as enrollment agents.
- Select a suitable method for the transportation of the cards.
- Carry out rigorous identification checks.

You should create a staging security group that contains the selected administrator accounts. You also require a security group to contain the activated accounts. Part of the enrollment process involves that the administrator accounts move from the staging group to the activated group.

The distribution process requires appointment of security officers. These security officers can then:

- Deliver the smart cards to the enrollment station.
- Act as enrollment agents.
- Carry out identification checks.

The identification checks must be rigorous. Administrators should be personally verified by the security officer against a suitable identity document such as a passport or driver's license, and their identity confirmed by their line manager.

Organizations should also do background checks on their administrators. These checks are particularly important in the financial sectors, or for any organization that is subject to regulatory requirements. For more information about background security checks on administrators, see The Security Monitoring and Attack Detection Planning Guide at http://go.microsoft.com/fwlink/?LinkId=41309.

Activating Smart Cards

Smart card activation should take place in a secure location, such as the office used to issue passes that allow access to premises. The security officer sets up an enrollment station with two smart card readers and logs on with his smart card.

After the security officer confirms the administrator's identity, he makes a certificate request for that user account. He opens a new smart card and installs the requested certificate. The security officer then moves the administrator account from the pending group to the activated group. Finally, he writes down the serial number of the card before he hands over the card to the administrator.
The administrator then uses the PIN reset tool to reset the default PIN or uses the PIN unblock tool in conjunction with the Activation Web server to set a new PIN. The administrator's smart card is now ready for use.

Managing Smart Cards
The implementation of smart cards is not a one-time action, because the security certificates embedded on the cards require management and you must cope with situations in which administrators forget their smart cards, lose them, or have them stolen. You should establish applicable procedures and an appropriate budget for smart card management.

Exceptions Management
Your organization needs to develop a plan that focuses on how to manage situations in which administrator smart cards are forgotten, lost, or stolen. How your organization implements the plan depends on how smart card logon requirements are enforced in your organization.

If your organization has chosen to enforce a smart card logon requirement through user accounts in Active Directory, you can easily grant an exception to the affected user in such a situation. The method for granting the exception would be to remove the requirement for smart card logon for the account, and then reset the password after ensuring that the User must change password at next logon setting is enabled. You could then provide the password to the account owner, and after a reasonable period, re-enable the requirement. To apply this method, in Active Directory Users and Computers, double-click the user name, click the Account tab, and then under Account Options, clear the check box for Smart card is required for interactive logon and select the check box for User must change password at next logon. Click OK, and then from the context menu, right-click the user name and select Reset Password to set the password and enforce these requirements for the administrator.

If your organization uses Group Policy to enforce the smart card logon requirement, there is no way to create an exception for a user at this time. In this case, you will have to determine a policy appropriate for your organization that administrators can follow in the event that they forget or lose their smart cards.

In the case of forgotten smart cards, you can implement a number of responses. For example, a policy might require administrators to return home to retrieve misplaced smart cards.

If your organization outsources its smart card infrastructure, you could implement a policy that requires an administrator to maintain a few generic smart cards with certificates tied to specific user accounts on site. If a user loses a smart card, an administrator could temporarily issue one of these generic smart cards to the user with the understanding that the user is responsible for any actions taken to access resources with the generic account. In such a policy, it is recommended that the administrator who maintains the generic smart cards reset the password PIN on the smart card each time prior to issuing it to a user.

If your organization maintains its own smart card infrastructure, you could issue a new certificate with a short lifespan to a generic user account. Under this exceptions management method, the administrator would again be accountable for using the generic account to access resources.

Finally, when an administrator loses a smart card, your organization should institute a policy to issue a new smart card to the administrator, and revoke the administrator's old certificate.
Certificate Revocation
You might have to revoke a certificate under a number of circumstances, for example, on compromise of the private key, if the smart card user changes assignments, or when the user leaves the organization. When you revoke a certificate, this action publishes details about the certificate to the certificate revocation list (CRL) location. This location is typically a URL or a network UNC path.

An issued certificate includes a list of distribution points where an authentication server can verify the status of the certificate against the CRL. For more information about certificate revocation, see the Revoking certificates and publishing CRLs topic at www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CS_SrvAdCRL.asp.

Certificate Renewal
The expiration date of the digital certificate on a smart card depends on the settings in the certificate template that creates the smart card certificate. Certificates for smart card use have typical lifetimes from six months to two years.

When a certificate comes towards the end of its lifetime, it requires renewal to ensure that the owner can continue to use the certificate or replace it. In certificate renewal, the renewal requester already owns a certificate. The renewal takes the information of the current certificate into account when the renewal request is submitted. You can then renew a certificate with a new key or use the current key.

Certificate Autoenrollment
Certificate autoenrollment is feature of Windows Server 2003, Enterprise Edition Certificate Services that automatically signs a renewal request using the existing certificate to obtain a new certificate. This feature helps in the management of large numbers of certificates. For more information about certificate autoenrollment, see Certificate Autoenrollment in Windows Server 2003, at http://go.microsoft.com/fwlink/?linkid=69027.

Monitoring Smart Card Use
Administrators use smart card–enabled accounts when they perform highly privileged operations, such as server restarts, the management of user accounts, and the configuration of file permissions. Malicious or poorly trained administrators have significant potential to damage your network infrastructure. Hence, you should monitor your security logs to record when administrators log on and log off with their smart cards.

Enterprise management tools such as Microsoft Operations Manager (MOM) 2005 that can monitor and evaluate security event logs are suitable for monitoring smart card use. For more information about how to monitor security event logs, see The Security Monitoring and Attack Detection Planning Guide at http://go.microsoft.com/fwlink/?LinkId=41309.

Issues and Requirements
This section describes the specific issues and requirements Woodgrove National Bank encountered during the design of their solution to secure administrator accounts with smart cards.
Background

Woodgrove National Bank possesses a number of critical servers that require tight administrative control and secure access. Administrators currently authenticate to these critical servers by using a user name and password combination. Unauthorized users have attempted to access critical servers with stolen credentials.

Business Issues

Woodgrove National Bank has identified the following three business continuity and administrator accountability issues:

- **Accountability.** The IT department cannot verify critical changes to servers by administrators who use user name and password authentication because administrators often share credentials.

- **Protection of credentials.** Malicious or rogue users who steal administrators' credentials can seriously affect the reputation of the organization and generate financial costs through downtime. Smart card authentication would significantly reduce the possibility of theft of administrator credentials.

- **Business continuity.** Because Woodgrove National Bank cannot allow changes to network configuration to disrupt business services, a carefully planned approach is essential during the implementation phase of the smart card solution.

Technical Issues

The Woodgrove National Bank IT department has identified the following technical issues that must be overcome to implement a smart card solution:

- **Support for smart card readers.** Every server that administrators need to access with a smart card must provide hardware support for a smart card reader.

- **Implement operational best practices.** The integrity of a smart card deployment is dependent upon effective long-term management and maintenance. Woodgrove National Bank IT should implement the operational best practices outlined by the Microsoft Operations Framework (MOF).

- **Scheduled tasks that run with administrator rights on a smart card-restricted server.** Woodgrove National Bank runs scheduled tasks that use accounts with administrator-level privileges. Woodgrove National Bank needs to review these accounts and, where possible, use accounts that do not require administrative privileges. Woodgrove National Bank must also implement a permanent exclusion group that includes any accounts that run scheduled tasks so that these accounts are exempt from the requirement for smart card logon.

- **Integration with UNIX.** Woodgrove National Bank operates a heterogeneous environment, so smart card integration with computers that run UNIX is a concern. Woodgrove National Bank plans to investigate products such as TrustBroker from CyberSafe Limited that provide integrated smart card authentication for both Windows and UNIX.

Security Issues

The goal of using smart cards to help secure administrator accounts is to improve security and accountability. The Woodgrove National Bank IT department has identified the following security issues that the bank must address before they can deploy the solution:

- **Distribution and activation.** The distribution and activation of the smart cards is important to maintain the integrity of the entire solution. Because Woodgrove
National Bank has sites throughout the world, Woodgrove IT cannot distribute smart cards from a single source location. Verification of smart card recipients is a key factor to maintain the integrity of the project. Woodgrove National Bank plans to deploy security teams that use Human Resources identification data to ensure that they issue each smart card to the correct person.

- **Least-privilege approach to administrative rights.** Woodgrove National Bank should examine its current network administration model and reduce the number of user and service accounts that run with full administrative privileges. The bank should assign only those privileges that administrators require to do their jobs. The analysis and reduction in the number of administrator accounts can help in the deployment, monitoring, and continued management of the smart card solution.

- **Management of service accounts.** Woodgrove IT reviewed program service accounts and has ensured that as few services as possible require administrator security context. Many programs are marked for either upgrades or replacement.

- **One smart card for each forest in a full trust relationship.** Woodgrove National Bank has two forests linked by a two-way trust relationship. Although a smart card can hold multiple certificates, Windows Server 2003 only uses the certificate located in slot 0 of the smart card for interactive logon. This design requires network administrators who work across multiple unlinked forests to have multiple smart cards. However, an administrator with a smart card has access to resources in all forests with which the forest that authenticates the administrator has a full trust relationship, unless a security restriction in the trusting forest overrides this access.

- **PIN management.** The security and integrity of the smart card solution increases if users can easily change their PINs. Hence, Woodgrove National Bank IT department acquired suitable PIN management tools from the selected smart card vendor.

## Solution Requirements

After the review of the initial pilot, Woodgrove IT developed specific solution requirements. The solution employed by Woodgrove National Bank to help secure administrator accounts that have smart cards must:

- Ensure that secured servers require a valid smart card for an interactive, secondary, or Remote Desktop logon.
- Distribute and activate smart cards in a secure and timely manner.
- Provide an audit of the access to secure servers, and collect the resultant security data in a central repository.
- Enable management and monitoring of smart card use.
- Ensure rapid revocation of compromised certificates, such as on lost or stolen smart cards.
- Provide a structure for ongoing management.

Woodgrove National Bank has identified several key business, technical, and security issues that emerged from the initial plan. Woodgrove IT performed a review to address these issues and conducted tests of workarounds and fixes. Woodgrove National Bank has created detailed plans for the deployment phase of the solution.

## Designing the Solution

After you understand the business, technical, and security issues that the smart card solution must address, you can design a solution that suits your environment. The design
process identifies the essential elements and logically analyzes the requirements to plan the solution.

Woodgrove National Bank has carried out this appraisal. This section describes the issues from the initial plan that Woodgrove National Bank system architects considered, the conclusions they reached, and the design decisions that they made.

This section outlines the design choices made by Woodgrove National Bank IT to help secure administrator accounts by the use of smart cards. It details the solution concept and its prerequisites and describes the architecture that Woodgrove National Bank planned.

**Solution Concept**

In the proposed solution, all server administration activity requires authentication of the administrator's identity by the presentation of a certificate stored on a smart card and its corresponding PIN. The solution uses a combination of Group Policy settings, X.509 version 3 (v3) user certificates, smart cards, and smart card readers. The solution requires the installation of an X.509 v3 certificate onto the smart card.

To log on to a server, the administrator inserts the smart card into a smart card reader installed on the computer. The insertion of the card causes the operating system to display a prompt for the PIN. The administrator then enters the PIN for the smart card. If the PIN is correct, the administrator can access the server with administrative rights.

**Solution Prerequisites**

When you engage in a project of this nature, it is necessary to meet a number of prerequisites. These prerequisites include the recruitment of the project team, consultation with the user base, the implementation of tests or pilots, and the need to upgrade the hardware and software to meet the solution requirements.

**Consulting Administrative Teams**

A key consideration when a changing a user service is to consult the users and groups involved. In return, the users must understand what they can expect and not expect from the service. Mutual consultation and the management of user expectations is often the key to user acceptance. Measurable objectives must be set to judge the ultimate success of the project in a rational manner. These objectives might include the reduction of security-related incidents associated with stolen credentials.

Woodgrove National Bank operates in several countries/regions throughout the world, and uses regional support centers. The initial design team extensively canvassed administrative teams in all locations to identify candidate servers for the smart card solution. The team also identified any servers that they would not be able to upgrade to meet the solution prerequisites within an acceptable timescale.

**Recruitment of the Project Team**

Ensure that you have the right personnel and skills to implement a project of this nature. The project team is likely to require input from the following representative occupations:

- Program manager
- Information systems architect
- Systems analyst or integrator
- Systems engineers
- Product release manager
● Product testing manager
● Support or help desk manager
● User support specialists
● Security officers


If you do not have certain skills available in-house, you must recruit additional personnel. Because the project typically does not require all personnel at all stages, you must determine individual availability throughout the duration of the project.

**Solution Architecture**

The implementation of a smart card solution to help secure administrator accounts requires:

● Active Directory
● Group Policy
● That servers that run Windows Server 2003 have smart card readers
● Enrollment stations
● Personalization of smart cards
● PIN management tools

Before implementing the solution, Woodgrove National Bank completed the following:

● Upgraded certificate services to Windows Server 2003, Enterprise Edition or later.
● Upgraded all managed servers to Windows Server 2003 to support interactive logon that uses Terminal Services. This requirement depends upon application compatibility.
● Customized smart card certificate user templates and set appropriate permissions.
● Created and tested Group Policy objects (GPOs) for smart card enforcement, temporary exclusions, and permanent exclusions.

Woodgrove National Bank IT also implemented solutions to the following challenges:

● Distribution of smart cards
● Activation of smart cards
● Management and support of smart cards
● Management of exceptions

**Smart Cards Distribution**

Prior to smart card distribution, Woodgrove National Bank IT department placed its administrators in an Active Directory staging security group. A team of security officers was required to verify the identities of the administrators and to distribute the smart cards. After an administrator received his card, the IT department moved that person from the staging group to the smart card user group. The administrator then has access to the activation Web server to activate his smart card and change the PIN.
Smart Cards Activation
Because administrators received their smart cards in a pending state, the cards require activation prior to use. The administrator activates his smart card when he inserts the card into a smart card reader, enters a challenge, and then changes the PIN.

Smart Cards Management and Support
Although the administrators at Woodgrove National Bank are a technically astute group, the smart card deployment team needed to work closely with help desk. Help desk personnel required suitable instruction so that they could handle any queries that arose.

Exception Management
Woodgrove National Bank instituted a corporate policy to cope with lost, stolen, or forgotten cards. For lost or stolen cards, the IT department revokes all assigned certificates and issues new cards within 24 hours. The IT department deals with administrators who forget to bring their smart cards to work by issuing them temporary smart cards. Although a certificate might be revoked, it does not mean the smart card is deactivated during that same time. Woodgrove must review the CRL policies to match the security policies.

Certificate Revocation
The smart card logon certificates for Woodgrove National Bank administrators use intranet URLs to locate the CRL and check for revoked certificates. The IT department implemented Windows Network Load Balancing (NLB) to ensure high availability for the Web site that hosts the CRL.

Certificate Renewal
The Woodgrove National Bank IT department developed a certificate renewal process that requires the administrator's manager to approve the smart card renewal request. After the manager approves a request, the current certificate signs the certificate request and the smart card certificate is renewed.

Monitoring the Solution
Woodgrove National Bank uses Microsoft Operations Manager (MOM) 2005 to collect and analyze security event logs and to monitor the solution availability and performance. The smart card solution integrates with MOM, monitors security event logs, and provides alerts and produces usage reports. Woodgrove National Bank plans to review the service on a quarterly basis and to generate reports from the MOM data.
How the Solution Works

This section describes the detailed processes that occur during authentication of a smart card logon.

1. An administrator inserts a smart card into the smart card reader attached to a computer and the Microsoft Graphical Identification and Authentication DLL (MSGINA) and the computer prompts the user to enter a PIN.

2. MSGINA passes the PIN to the Local Security Authority (LSA) and the computer uses the PIN to access the smart card.

3. The client-side Kerberos package reads the X.509 v3 certificate and private key from the administrator's smart card.

4. The Kerberos package sends an authentication service request to the Key Distribution Center (KDC) service that runs on a domain controller, to request authentication and a Ticket Granting Ticket (TGT). The authentication service request consists of a Privilege Attribute Certificate (PAC), which lists the user's security identifier (SID), the SIDs of any group of which the user is a member, and a request for the Ticket Granting Service (TGS) together with pre-authentication data.

5. The KDC verifies the certification path of the user’s certificate to ensure that the certificate is from a trusted source. The KDC uses CryptoAPI to build a certification path from the administrator's certificate to a root CA certificate that resides in the root store on the domain controller. The KDC then uses CryptoAPI to verify the digital signature on the authenticator that was included as signed data in the pre-authentication data fields. The domain controller verifies the signature and uses the public key from the administrator's certificate to prove that the request originated from the owner of the public key. The KDC also verifies that the issuer is trusted and appears in the NTAUTH certificate store.

6. The KDC service retrieves user account information from Active Directory based on the user principal name (UPN) specified in the Subject Alternative Name field in the administrator's certificate. The KDC constructs a TGT from the user account information that it retrieves from Active Directory. The TGT includes the administrator's security identifier (SID), the SIDs for any domain groups to which the administrator belongs, and (in a multidomain environment), the SIDs for any universal groups of which the user is a member. The TGT’s authorization data fields include the list of SIDs.

   **Note:** A SID is a security identifier that is created for each user or group, at the time a user account or a group account is created within either the local security accounts database on Windows NT or higher computers, or within Active Directory. The SID never alters even if the user or group account is renamed.

7. The domain controller returns the TGT to the client. Either the client or the card decrypts the TGT and uses its private key to obtain the KDC secret key. This depends on the type of card or certificate used.

8. The client validates the reply from the KDC. It first verifies the KDC’s signature by the construction of a certification path from the KDC’s certificate to a trusted root CA and then uses the KDC’s public key to verify the reply signature.
The following figure illustrates this process.

![Diagram](image.png)

**Figure 3.1**
*Smart card logon authentication process*

Woodgrove National Bank IT linked a GPO to the organizational units that contain the servers that require smart card authentication. This GPO applies the changes to the following computer configuration settings:

- Interactive logon requires a smart card
- Removal of the smart card forces the account to log off

These settings help prevent administrators from sharing smart cards or leaving a server unattended while logged on.

**Extending the Solution**

Woodgrove National Bank envisions integration of the smart card solution into the server and application change management process. The plan is to authenticate each stage of the change management process, and integrate this process into the workflow. For example, changes to the Woodgrove Web server would require verification from two or more Web administrators.

**Summary**

Using smart cards to authenticate administrator user accounts reduces fraudulent access to critical computers and increases the integrity and accountability of server administration. The implementation of smart cards for administrators will benefit your organization by the reduction of security incidents and the increased quality of administrative procedures.
Most organizations must provide remote access to network resources over dial-up or virtual private network (VPN) connections. Ongoing changes to business practices, such as the provision of support for remote users or field sales staff, will only accelerate this trend. Although remote access provides numerous advantages to an organization, any external access significantly exposes the organization’s network to potential security threats. Two-factor authentication is an increased requirement for networks that support remote access.

Securing Remote Access with Smart Cards

Remote access should enable all authorized employees to access an organization’s intranet resources. To facilitate remote access through VPN, you must open up ports on your external firewalls. This increase in accessibility creates a route through which attackers can possibly penetrate the network.

Chapter 1, "Introduction," of this guide points out that the authentication of accounts that rely on user names and passwords concentrates all the access control security on the password. Passwords are vulnerable to compromise, and the credentials for a compromised account that has remote access to a corporate network could be of interest to criminal organizations.

Although you can configure a domain password lockout policy for user accounts, the account lockout policy provides an opportunity for denial of service (DoS) attacks by constantly locking out the remote user account. Although this attack does not compromise any information on the network, it is a source of frustration for the locked out user.

Strong user authentication that uses digital certificates embedded in a smart card provides a robust and flexible approach to secure remote access connections.

Client Requirements

The use of smart cards to control remote access depends on the components that run on the remote client. You must have a good level of knowledge of these components, and in particular, Connection Manager and the Connection Manager Administration Kit (CMAK).
Connection Manager centralizes and automates the establishment and management of network connections. Connection Manager supports the following key areas for the configuration of smart card access:

- Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) for VPN and remote access connections
- Application-level security checks to manage client computer configurations automatically
- Computer security checks and validations that are part of the logon process

For more information about Connection Manager and CMAK, see Connection Manager Administration Kit at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/be5c1c37-109e-49bc-943e-6595832d5761.mspx.

**Connection Manager for the Client**

To implement a manageable remote access solution, you must create and deploy Connection Manager settings to multiple clients. To deploy Connection Manager to multiple clients, you create Connection Manager profiles.

Connection Manager profiles are customized Connection Manager client dialer packages that you create with CMAK and deploy to client computers in a self-extractable executable file. You can use any software distribution mechanisms to distribute profiles, such as Group Policy, Microsoft® Systems Management Server 2003, CDs, or USB keys.

When you run the executable, it installs the profile onto the local computer, together with the appropriate telephone numbers or host addresses to connect to the remote access servers. When a user initiates a connection through their Connection Manager profile, Connection Manager automatically checks for the presence of a smart card and prompts the user for the PIN. If the user supplies the correct PIN, Connection Manager establishes the appropriate dial-up and VPN connections and authenticates the user's credentials.

Connection Manager also simplifies the connection process for the user. It limits the number of configuration options that a user can change, and helps to ensure that the user can always connect successfully. Organizations can customize Connection Manager to define:

- **Available phone numbers.** A list of phone numbers available to the user based on their physical location.
- **Customized content.** The dialer can include customized graphics, icons, messages, and Help content.
- **Pre-tunnel connections.** A dial-up connection to the Internet that automatically occurs before the VPN connection attempt.
- **Pre-connection and post-connection actions.** Examples include the ability to reset the dialer profile or the configuration of the Windows Firewall to ignore exceptions to packet filter rules.

**Operating System Requirements**

The smart cards for remote access solution only works with Microsoft Windows® XP Professional. Microsoft recommends Windows XP Professional with SP2 or later. Client computers should have all current security updates installed.
Server Requirements

Server requirements for smart card access are relatively straightforward. The remote access servers must run Windows 2000 Server or later and must support EAP-TLS.

Note: Unlike the smart cards for the administrators scenario, the smart cards for the remote access scenario do not require Microsoft Windows Server™ 2003, although it is highly recommended that you upgrade your PKI to Windows Server 2003 with Service Pack 1 (SP1) or later.

Dial-up and VPN Considerations

The solution uses smart cards to secure remote access supports dial-up access through Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) connections, but users might experience extended logon times.

Remote connections that use VPN connections place an additional processor load on the remote access server. Smart card secured logon does not add noticeably to that load but can increase logon times. VPN remote access servers that service a high volume of inbound connections require fast processors, preferably in a multiprocessor configuration. Organizations that use IPsec–secured VPNs can implement network cards that offload the IPsec encryption process onto a separate processor on the network card.

Support for Extensible Authentication Protocol

EAP-TLS is a mutual authentication mechanism developed for use with authentication methods in conjunction with security devices, such as smart cards and hardware tokens. EAP-TLS supports Point-to-Point Protocol (PPP) and VPN connections, and enables exchange of shared secret keys for Microsoft Point-to-Point Encryption (MPPE).

The main benefits of EAP-TLS are its resistance to brute force attacks and its support for mutual authentication. With mutual authentication, both client and server must prove their identities to the other. If either client or server does not send a certificate to validate its identity, the connection terminates.

Windows Server 2003 supports EAP-TLS for dial-up and VPN connections, which enables the use of smart cards for remote users. For more information about EAP-TLS, see the Extensible Authentication Protocol topic at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/auth_eap.mspx

For more information about EAP certificate requirements, see Certificate Requirements when you use EAP-TLS and PEAP with EAP-TLS at http://support.microsoft.com/default.aspx?scid=kb;en-us;814394

Identify Authentication Server Requirements

To log on, remote users must present their credentials to an authentication service. Windows provides two authentication services for remote users:

● Internet Authentication Service (IAS) servers
● The Active Directory® directory service

If your organization decides to use the Remote Authentication Dial-In User Service (RADIUS) authentication provider, you must include IAS servers in your configuration. IAS is the Microsoft implementation of RADIUS, and runs as a service on Windows 2000 Server or later.
Organizations can gain benefits from the implementation of IAS for RADIUS authentication with smart cards, which include:

- Centralized user authorization and authentication
- Separate management and accounting mechanisms
- Wide range of authorization and authentication options

The IAS server manages the authentication process. IAS delivers the user’s authentication request and logon certificate information to Active Directory, which compares the logon certificate to the stored certificate information for that remote user. If the certificate information matches, Active Directory authenticates the user.

For more information about a design solution that uses IAS, see the "Designing the Solution" section later in this chapter.

**Distribution and the Enrollment of the Smart Cards for Remote Access**

The distribution and enrollment of smart cards for remote access follows a process similar to that for the administrator account solution as described in Chapter 3, "Using Smart Cards to Help Secure Administrator Accounts." The main differences are the higher number of users and that the process might take place in multiple countries/regions.

The verification of the remote user’s identity is still an important part of the process. However, because remote users do not have the same rights as administrators, the use of photo identification such as a passport or driver’s license should be adequate for identification purposes. A manager must provide justification before the administrator grants the user remote access.

Enrollment stations should still be in suitable locations, such as the personnel department or security department, and users can report there to collect their smart cards. If a user cannot travel to an enrollment station, you can use remote tools to unblock and to enroll the user and activate the smart card.

The enrollment procedure requires an enrollment agent to generate the certificate request on behalf of the user and install the resultant certificate on the smart card. The enrollment agent sends the blocked smart card to the user by a secure delivery method. The user then contacts the help desk, establishes his identity, and unblocks the smart card, as described in the section on Activation Web Server in Chapter 2, "Smart Card Technologies."

**Further Considerations**

The introduction of secure remote access within an organization often results in an increase in the number of users who want to use the service. Organizations must review their current network infrastructure and, where necessary, provide additional resources. Areas to consider are:

- Certificate revocation lists
- High availability and bandwidth
- Software update distribution

**Certificate Revocation Lists**

The implementation of certificates for remote users involves changes to how clients can locate a certificate revocation list (CRL) to check that a certificate is still valid. The default
Uniform Resource Locator (URL) CRL for Windows Server 2003 points to an intranet location, for example URL=http://Certification_Root_Server_DNS_Name/CertEnroll/Certification_Authority_Name.crl.

For remote users, this URL must point to a location that is accessible from the Internet. This requirement involves all issued certificates and includes both the intranet and the extranet URLs for the CRL. For more information about the customization of CRLs, see the Specify certificate revocation list distribution points in issued certificates topic at www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CSprocs_CDP.asp.

Note: Remote computers might experience time-out problems if they download the CRL through a slow connection.

Software Update Distribution

The implementation of a mechanism for the distribution of software updates is an important step in the provision of smart cards for user access. Software updates include updated Connection Manager profiles and new releases of smart card tools.

You can distribute software updates by:

- Externally accessible Web servers that contain the updates.
- CDs or USB keys.
- Software management solutions such as Systems Management Server (SMS) 2003.
- E-mail messages that contain code-signed updates.

If you implement VPN quarantine, you can distribute Connection Manager profile updates by the use of the same method that you use to provide security updates and antivirus software. For more information about VPN quarantine, see Implementing Quarantine Services with Microsoft Virtual Private Network Planning Guide at http://go.microsoft.com/fwlink/?LinkId=41307.

The provision of Connection Manager and smart card updates through externally accessible Web servers enables users to download the updates before connection to an organization's network. The downside to this solution is that it might not be possible to use the smart card to authenticate to the external Web server. In this case, users must rely on user name and password combinations to log on and download updates. Although this appears to defeat the purpose of two-factor authentication, because this Web server only provides update resources, you might consider this risk acceptable.

The use of CDs to distribute updates is a useful method for large initial rollouts, because the cost for each CD drops when produced in high volumes. USB keys are more appropriate for the distribution of updates on an individual basis.

The use of software management systems such as Systems Management Server 2003 to distribute software updates requires the computers to connect to the network. This mechanism can be suitable for mobile and remote users who connect to the LAN on a regular basis, and who use computers that are members of the organization's domain. However, software update mechanisms such as Systems Management Server are not appropriate for remote users who use their own computers from home.

You can e-mail updates in certain situations. To implement this method of software distribution, you must provide code-signed updates and train the users to check the veracity of the code-signing certificate.
This section covered the components that can provide smart card authentication for remote access accounts. The next section on Issues and Requirements looks at the issues that Woodgrove National Bank faces during the implementation of smart cards.

Issues and Requirements

During the plan and design phase of the smart card remote access solution, Woodgrove IT found several business, technical, and security issues. The section that follows identifies those issues.

Woodgrove National Bank Scenario Background

Woodgrove National Bank provides remote access to its corporate network for sales staff, IT support workers, and executives. The current remote access solution employs dial-up networking through private circuits to dedicated remote access servers equipped with modems or Integrated Services Digital Network (ISDN) adapters. These connections are slow and expensive when compared to broadband, particularly for remote users who travel across the globe.

The increased availability of broadband Internet access allows organizations to use VPN for remote access. This approach reduces costs by the elimination of dial-up access and provides a better user experience, although it also increases the bank's vulnerability to malicious attack.

Complying with Legal Requirements

As a financial institution, Woodgrove National Bank must comply with strict legal requirements in various countries/regions. The bank must maintain customer confidence by the protection of corporate and customer assets. Woodgrove National Bank implemented a secure computer initiative and set strict security policies on all computers that access the company network, whether these computers connect to the local area network (LAN) or remotely.

Verifying Users

Woodgrove National Bank's current remote access solution does not adequately cope with impersonation attacks (in which an attacker tries to guess the user name and password combination). Impersonation attacks cause remote access accounts to lock out, which prevents the legitimate user from being able to connect. This vulnerability increases the risk to the corporate network and has forced Woodgrove National Bank to limit the connectivity options it provides to its employees.

Business Issues

Many executives use remote access. Although security is paramount during the deployment of a smart card solution, maintenance of remote worker productivity is also important. The deployed solution must properly balance these needs.
Maintaining Productivity
Employees often lose confidence in security-based solutions that affect productivity. Users are frequently frustrated if they are unable to access network resources during and directly after a solution deployment. Woodgrove IT must provide alternative access methods to help overcome these frustrations. The following list of tools provides alternative methods of network access:

- **Outlook Web Access.** Provides the user with secure access to e-mail through a Web browser.
- **Remote Desktop and Terminal Services.** Employees can use Remote Desktop and Terminal Services to access line-of-business applications and desktop files.

Help Desk Support
User acceptance and the integrity of a remote access solution often depend on the level of support available. Executives become frustrated if they spend time in support queues. Organizations must budget for training both the end user and support personnel.

Technical Issues
Woodgrove National Bank has identified several key technical issues that require attention prior to the smart card for remote access deployment. These issues include distribution of smart cards and smart card readers, the integration of the solution into the current network with minimal disruption, and integration into the current IT management infrastructure.

- **Supported smart card readers.** Remote users might work from home on a range of computers that have various operating systems. The Woodgrove IT department decided that the only supported configuration would be Windows XP Professional with SP2 or later. Remote users who run Windows 2000 Professional had no assurances that the smart card readers would work with their computers.
- **Network latency.** The time that packets take to travel from client to remote access server and back can cause VPN-secured connections to fail. This is particularly problematic on satellite broadband connections. Woodgrove National Bank decided not to support remote connections that exhibit average latency times of more than 300 milliseconds.
- **Smart cards distribution.** Because Woodgrove National Bank operates in several countries/regions around the world, distribution of smart cards is both a technical issue and a security issue. The enrollment agents must be able to contact the activation Web server regardless of which country/region they are in. Alternatively, users might have to unblock smart cards through a challenge/response system. The challenge/response system might require development effort to create with the smart card vendor's software development kit (SDK).

Security Issues
The following issues affect the security strategy for the Woodgrove National Bank implementation of secure remote access using smart cards:

- **Remote access user identification.** The Woodgrove National Bank IT department must validate the identity of remote access users during the smart card distribution and activation process.
- **Connection exceptions for the Woodgrove solution.** Because smart cards can become lost, stolen, or simply forgotten, the Woodgrove IT department must ensure that its smart card deployment solution includes a fast method to securely distribute replacement smart cards and a method to handle exceptions while replacement cards are in transit.

**Solution Requirements**

The solution requirement for using smart cards to secure remote access accounts includes the following components:

- **Internet Authentication Service (IAS).** The current IAS servers require upgrades to Windows Server 2003 with Service Pack 1 or later to facilitate the improved IP filters and acceptance of vendor-specific attributes. In addition, Woodgrove IT must enable support for EAP-TLS on the remote access servers.

- **Smart card user templates.** Woodgrove National Bank must carry out customization of certificate templates and set the correct permissions on the templates. The certificate enrollment agent and smart card logon templates require suitable permissions.

  **Note:** You can restrict remote access to smart card certificates by setting remote access policy to accept only a certificate with a specific object identifier. For more information about certificate templates and object identifiers, see the Implementing and Administering Certificate Templates in Windows Server 2003 white paper at [www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspx](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspx).

- **PIN management tools.** Users need a software utility to manage their own PINs. Most smart card vendors provide basic PIN management tools. Woodgrove IT decided to provide additional customization to integrate the PIN management tool with a remote PIN unblocking utility.

- **Group Policy objects (GPOs).** Woodgrove IT must create the appropriate GPO for their organizational unit structure. These GPOs must include settings to support exceptions, such as a user who loses or forgets his or her smart card or PIN.

- **Connection Manager profiles.** Woodgrove IT must create specially configured Connection Manager profiles that contain the appropriate dial-up or VPN server connection settings for the Woodgrove remote access servers. Woodgrove IT also needs to customize the text in the Connection Manager profile user interface to help users understand the connection process, and to tell the user what to do if problems arise. Woodgrove IT created different Connection Manager profiles for different users, such as executives, regular users, and one for administrative staff. Each profile had different priorities during connection setup. Administrators can connect remotely irrespective of network traffic levels.

- **Windows XP Professional with Service Pack 2.** Woodgrove National Bank must upgrade all remote access computers to Windows XP Professional with SP2 or later. Windows XP Professional with SP2 offers improved security features such as Windows Firewall and better support for automatic updates that increase the integrity of the remote access solution. Windows XP Home with SP2 provides these security advantages, but cannot join a domain and make use of Group Policy. Windows 2000 Professional with SP4 does not have the security enhancements of Windows XP Professional with SP2.
• **Smart card and smart card reader procurement.** Although Woodgrove National Bank has a mature PKI in place, the bank would gain little benefit from the installation of the Windows for Smart Cards operating system onto blank smart cards. Most vendors offer smart cards with the operating system already installed on the card. The choice of smart cards and smart card readers from a single vendor provides the benefit of a single point of contact for any support issues.

• **USB or PC card smart card readers.** Creation of a standard baseline for deployment minimizes the cost of the installation of a smart card solution. Woodgrove National Bank implemented a corporate policy that requires all new portable computers to have built-in smart card readers. Woodgrove National Bank has also set a common standard for the supply of USB smart card readers. The bank supplies USB card readers to employees who use their own computers to work from home. Woodgrove has ensured continuity through a contract with the card reader supplier to supply the same model of card readers for two years.

• **Trust relationships.** The Woodgrove National Bank smart card deployment used the current trust relationships between separate forests and any one-way trusts such as those between smaller, development team forests and the main corporate forest. This arrangement did not require any changes to the certificate templates.

• **Windows Server 2003 Public Key Infrastructure (PKI).** Windows Server 2003 Certificate Services provides the ability to assign permissions to elements of a default smart card certificate template and to customize templates. The improved flexibility of template permissions is a key element that enables Woodgrove IT to delegate the defined certificate issuance model in a secure manner. The Woodgrove IT department uses the enhanced PKI features of Windows Server 2003 to set rules for certificate autorenewal. The IT department uses the certificate template permission features to require that Woodgrove National Bank security officers manually create all new smart card certificate enrollments. However, the user can automatically renew all current smart card certificates.

Woodgrove National Bank already had a Windows 2000 Server PKI in place when the organization made the decision to implement smart cards. For the initial pilot, the Woodgrove National Bank IT department decided to use its current Windows 2000–based security infrastructure to create and manage certificates for smart cards, instead of third-party services. However, the Woodgrove smart card security solution requires that certificates expire in one year. This requirement would incur large support costs from the manual renewal of tens of thousands of user certificates each year. Due to this increased administrative workload, the Woodgrove National Bank IT team decided to upgrade its PKI to Windows Server 2003.

If Woodgrove National Bank had used the Windows 2000 Server PKI for certificate autorenewal, their certificate renewal options would be limited to either setting all certificate renewals as autorenewal, or the manual renewal of all certificates. The autorenewal for all certificates would eliminate any flexibility for renewal options.

**Designing the Solution**

This section outlines the design choices that the Woodgrove National Bank IT department made to use smart cards to help secure remote access. This section includes the solution concept, solution prerequisites, and describes the solution architecture.

**Solution Concept**

The solution uses a combination of Group Policy settings, remote access policies, Connection Manager profiles, X.509 v3 user certificates installed onto smart cards, and
smart card readers. The outline of the concept is that a remote access user launches a customized Connection Manager profile, which prompts the user to insert a smart card into the attached smart card reader. The operating system then prompts the user to enter a PIN. If the PIN is correct, the reader extracts the smart card certificate and account information. Connection Manager then makes a connection to the corporate remote access server and presents the credentials from the smart card. Active Directory authenticates these credentials and the remote access server grants the user access to the corporate network.

Solution Prerequisites
The prerequisites for the use of smart cards to secure remote access accounts are similar to those for the smart card solution to secure administrator accounts. You need to:

- Consult users and groups
- Recruit the project team
- Set user expectations
- Upgrade the hardware and software
- Distribute and activate smart cards securely

Consult Users and Groups
Within the planned cycle, you should evaluate any current remote access solutions and consult those who use them. Woodgrove National Bank operates in several countries/regions that all have remote access users. The initial team canvassed feedback from the current remote access users and support teams to identify and engage potential users, groups, and support staff to include in the pilots.

Recruit the Project Team
You must ensure that you have the right personnel and skills to implement a project of this nature. The project team is likely to require input from the following representative occupations:

- Program manager
- Information systems architect
- Systems analyst or integrator
- Systems engineers
- Product release manager
- Product testing manager
- Support or help desk manager
- User support specialists
- Security officers


If you do not have certain skills available in-house, you must recruit additional personnel. Because the project typically does not require all personnel at all stages, you must determine individual availability throughout the duration of the project.
Set User Expectations
The main issue for user expectations with smart card and remote access is that of the increased logon times. Users must expect logon times to increase by several seconds with smart card authentication.

Upgrade the Hardware and Software
The smart card for remote access solution requires the latest Microsoft operating systems and service packs. This requirement enables the remote access solution to take advantage of the latest advances and security facilities in Windows XP Professional with SP2 and Windows Server 2003 with SP1, such as Windows Firewall, Data Execution Prevention (DEP), Security Configuration Wizard, and VPN Quarantine. The software upgrades might require upgrades to client or server hardware. A pilot program can establish whether older equipment can run the newer operating systems. To check whether equipment is certified for Windows XP or Windows Server 2003, see the Products Designed for Microsoft Windows – Windows Catalog and HCL topic at www.microsoft.com/whdc/hcl/default.mspx?gssnb=1.

Distribute and Activate Smart Cards Securely
Implementation of smart cards for remote access requires a secure method for smart card distribution and activation. Typically, this distribution process would require remote users to report to their local administrative office so that the enrollment agent can verify their identity, issue the smart card, and carry out the activation procedure. The Delegated Issuance Model section later in this chapter describes how Woodgrove National Bank distributed and activated smart cards for remote users.

Solution Architecture
The implementation of the Woodgrove National Bank smart card solution for remote access requires the following components:

- Active Directory
- IAS installed on a Windows Server 2003 server
- Windows Server 2003 with SP1 with routing and remote access
- Group Policy
- Client computers that run Windows XP Professional with SP2 or later
- Smart card readers
- Smart cards with at least 32 KB memory
- Connection Manager profiles created with CMAK
- Client-side scripts for the Connection Manager profile

The Woodgrove IT department initially considered the provision of support for all currently deployed versions of Windows. However, the increased awareness of the threat to computers connected to the Internet led them to standardize on Windows XP Professional with SP2 or later.

User accounts and group memberships stored in Active Directory regulate remote connectivity and access to corporate resources at Woodgrove National Bank. Woodgrove IT also uses GPOs for the configuration of client computers to meet corporate network security policies.
How the Solution Works

This section provides technical details of the Woodgrove National Bank solution. It explains how Active Directory authenticates the user and traces the authentication path for the smart card credentials.

The following procedure enables remote access with smart cards:

1. A remote user logs onto a computer that has Internet access and a smart card reader attached. The user initiates the customized Connection Manager profile by double-clicking on the connection labeled **Woodgrove IT Connection Manager for smart cards**.

2. The Connection Manager profile checks for a smart card in the smart card reader. A dialog box appears that prompts the user to enter the PIN. Connection Manager uses the PIN to perform key operations on the card as a system service because it cannot prompt and show the user interface (UI) on the desktop. If the user enters the correct PIN, the card unlocks and allows the remainder of the remote access logon process to continue.

3. The Local Security Authority (LSA) is the trusted operating system component that performs all authentications. SChannel, the code that implements SSL, runs partly in the LSA and initiates the mapping sequence.

4. The Connection Manager profile initiates a link to the IAS servers at Woodgrove National Bank using a dial-up or VPN connection. The IAS server performs a revocation check on the client certificate. With the certificate mapping to the user principal name (UPN), the issuing CA must be in the NTAUTH store. Explicit mapping can also be set on the Active Directory user account.

5. The LSA presents the user information to the IAS server. The SChannel code that runs on the IAS server sends a message to the SChannel code that resides on the domain controller and passes it the UPN information from the certificate.

6. The SChannel code that runs on the IAS server validates the certificate and then does a user lookup against the Active Directory on the domain controller. The domain controller generates a Privilege Access Certificate (PAC) that contains the user’s 128-bit identifier and the group membership of the user. Future communications from this point uses the Kerberos v5 protocol.

7. The domain controller transmits a randomly generated session key that includes the Kerberos Ticket Granting Ticket (TGT) to the client computer. Receipt of this key authenticates the remote access server to the client. Both computers have now mutually authenticated.

8. The client computer decrypts the logon session key and presents the Kerberos v5 TGT to the ticket granting service. After this process completes, all other Kerberos v5 protocol communication uses symmetric encryption.

9. If the user connected through a dial-up connection, a user name and password prompt appears. The user enters the credentials and can now access all network resources at Woodgrove Bank. Users who connect through VPN do not have to complete this step.
Chapter 4: Using Smart Cards to Help Secure Remote Access Accounts

43

The following figure illustrates the steps to use a smart card for remote access authentication.

Figure 4.1
Remote access logon and authentication process that uses a smart card

The additional processor cycles required to process the smart card information adds approximately 20 to 25 seconds to the initial authentication process. After authentication is complete, performance is not affected.

Additional Design Considerations

The next section details additional considerations for smart card deployment, and includes the smart card distribution mechanism that Woodgrove National Bank used.

Delegated Issuance Model

The Woodgrove National Bank IT department developed a delegated issuance model for smart cards. This model offers responsive support that helps to ensure the highest level of security for the distribution of smart cards to employees around the world.

Woodgrove National Bank IT used a delegated issuance model to deploy smart cards outside the main Woodgrove National Bank IT center in London. The Woodgrove National Bank IT department sent technicians to offices around the world to train the delegated issuance officers (DIOs). The technicians trained the DIOs on how to distribute smart cards and how to use the smart card tools. After the initial visit, the DIOs participated in weekly conference calls with the Woodgrove National Bank central IT team to discuss issues that emerge.
The following figure illustrates the steps that make up the delegated issuance model for certificate request approval.

The steps performed in accordance with this flowchart are:

1. User requests a smart card from the DIO.
2. The DIO validates the user’s identity against an acceptable form of identification, such as a passport or a driver’s license and checks the user’s identity with the head of department. After the DIO confirms the user’s identity, the DIO submits a certificate request to the security officer in London.
3. To validate the request, the security officer checks for any prior certificates issued in that user’s name. The security officer also determines if the user has made any other smart card requests. If there is no objection to issue the smart card, the security officer gives approval. If the security officer uncovers a problem, the process must be subject to an audit, as described in step five.
4. The DIO receives the approval and uses the enrollment agent account to issue the certificate. This certificate attaches to a new smart card, which the DIO issues to the user in person. The delegated issuance process then completes.
5. If there are concerns over the validity of the request, the security officer initiates an audit of the request to determine whether to grant approval for that user. After the audit concludes, the user must make a new request.
6. The delegated issuance process completes.

Woodgrove National Bank could only implement the delegated issuance model after Woodgrove IT migrated the corporate certificate authorities to Windows Server 2003. The Windows Server 2003 PKI provides the ability to apply detailed permissions to sections of the certificate templates, which enables the role of DIOs within the delegated issuance
model. Within the issuance model, Woodgrove developed procedures to securely reissue lost or stolen smart cards.

**Configure RADIUS Accounting**

Although the maintenance of logs is not a requirement for the implementation of a remote access solution that uses smart cards, Microsoft strongly recommends it. If you use IAS, one benefit is the built-in support for the RADIUS accounting provider, which logs client connection requests and sessions. Woodgrove National Bank wants to monitor which users log on, when they log on, and for how long they connect to the corporate network. RADIUS gives Woodgrove the capability to analyze connection trends, with the aim to review and improve the service.

Each IAS server collects user session data, which it stores in Microsoft SQL Server™ Desktop Engine (Windows) (WMSDE) on Windows Server 2003 or on SQL Server 2000 Desktop Engine (MSDE 2000) on Windows 2000 Server and earlier. IAS transfers the accounting information from WMSDE or MSDE to a central SQL Server 2000 database in near real time. This arrangement ensures cost-effective use of SQL Server licensing and does not inhibit the server’s performance.

Woodgrove National Bank deployed regional SQL Server–based data collection servers to collect IAS remote access session data.

**Deploy Pilots**

Woodgrove National Bank IT tests any solution in both a lab environment and more than one pilot before deployment to the production network. Woodgrove IT developed two pilots for the remote access smart card deployment: one involved a small but experienced group of users and the other included a more diverse group of users in several countries/regions with a wide range of remote access experience.

The pilot with the more experienced users enabled Woodgrove National Bank to identify the major problems with the smart card deployment. The more experienced users were able to cope with minor disruptions and unexpected dialog boxes. After the Woodgrove IT department completed the first pilot, they knew that the smart card solution would work but that some refinement was necessary.

The second pilot with the diverse range of users enabled the Woodgrove IT department to experience the sort of support calls expected from the full deployment. This pilot enabled the help desk to resolve technical issues and indicated any further development that might be required before the deployment of smart cards to all remote users.

**Ensuring High Availability**

The solution scenario must be highly reliable because maintained productivity is a key requirement to the remote access solution. Woodgrove National Bank must consider provisions for high availability. These include:

- Load-balanced remote access servers
- Load-balanced IAS servers
- Redundant network paths

---

**Note:** Woodgrove Bank has geographically located Routing and Remote Access/IAS entry points because of the physical layout of the network.
Ensuring Adequate Network Bandwidth

System architects must consider current network paths, expected connection times, and the type and extent of the expected remote access traffic. The additional bandwidth that remote access users require should not be underestimated. The pilot deployments should help in the analysis of the remote access traffic patterns and the effect this traffic can have on the current network infrastructure. It is important that trials include nontechnical users and typical usage patterns to simulate the issues that are likely to appear in the full deployment. Hardware switches that incorporate bandwidth control and virtual local area networks (VLANs) can reduce the effects of remote access traffic on other users.

Woodgrove National Bank uses multiple Internet service providers to achieve good Internet connectivity. Much of the current bandwidth provides access to the Internet for Web research and e-mail. Woodgrove IT must reassess the current arrangements to allow for the additional traffic from remote access connections.

Exceptions

The system architects at Woodgrove National Bank understand that any solution must cope with situations in which business needs require temporary exemption for a device or devices from usual security requirements. For example, remote access for executives during a critical meeting might be exempt from the requirement for smart card authentication. If the smart card solution cannot provide exemptions for individual devices, the IT department would have to disable all secure remote access requirements simply to grant a single exemption. Hence, the smart card solution for remote access must support exceptions.

Note: The Woodgrove IT security group should be the sole authority that determines when the business need for an exemption justifies the security risk.

To deal with exceptions, Woodgrove IT created a new security group called RemoteSmartCardUsersTempException for temporary exceptions to the remote access smart card requirement. They then configured the remote access policies for the inbound remote access server as set out in the following table.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Policy Conditions</th>
<th>Authentication type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require smart card authentication for members of the remote access users group</td>
<td>Windows-Groups matches &quot;WOODGROVE\RemoteSmartCardUsers&quot;</td>
<td>EAP - Smart Card or other Certificate only.</td>
</tr>
<tr>
<td>Do not require smart card authentication for members of the temporary exclusions group</td>
<td>Windows-Groups matches &quot;WOODGROVE\RemoteSmartCardUsersTempException&quot;</td>
<td>MSCHAP v2</td>
</tr>
</tbody>
</table>

This arrangement enforces the smart card requirement on the members of RemoteSmartCardUsers group but not on the members of RemoteSmartCardUsersTempException. For more information about how to require smart card authentication for remote users, see the Configure smart card remote access topic at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/863638a6-f9e0-48d7-9db5-0b54af3cf135.mspx.
Apply Best Practices

Woodgrove National Bank IT department established the following list of best practice recommendations:

- **Involve the help desk.** A well-prepared help desk should be part of all smart card projects. After deployment, the help desk involvement changes to a maintenance role. It is essential to keep help desk personnel current about any changes in the internal system and any technological developments that affect usage.

- **Provide PIN management.** Because the primary goal for the use of smart cards is to improve network security, the security of the data that the smart card stores is vital. Forgotten PINs are a challenge both during and after smart card deployment. You should check with your smart card vendor about the supply of PIN management tools and implement a PIN reset processes for users who are unable to reset their PIN at a corporate location (for example, when they travel).

- **Implement anti-tamper measures.** Smart cards require anti-tamper protection, so that the card locks up if a user enters the incorrect PIN five times in sequence.

- **Retain a post-deployment team.** A post-deployment team can be much smaller than the initial deployment team, but is necessary to monitor system integrity regularly and to test and coordinate any upgrades to the smart card infrastructure.

Monitoring and Management

A solution that uses smart cards to secure remote access must include the ability to monitor the operational health of the solution. This process should provide the ability to monitor the entire network, a single asset, or list of assets in real time. The monitor tools must show the necessary information that an organization needs to provide operation support. If the solution does not meet this requirement, security personnel cannot determine if the solution maintains secure remote access connections effectively.

Identify Operational Considerations

Woodgrove IT identified the following operational considerations during the deployment of the solution:

- **Test authentication to internal applications.** A smart card should affect initial logon only. The pilot program should test and verify successful authentication to internal applications.

- **Troubleshoot remote-client issues.** To troubleshoot successfully, client issues can require close cooperation of multiple teams spread across different time zones. Rigorous tests and a proper pilot deployment help reduce support calls.

- **Understand organizational remote access scenarios and threats.** You must understand your organization’s remote access scenarios, security threats, and the balance between them. You must prioritize the assets that need the most protection and determine the appropriate balance between cost and risk are strategic decisions that senior management must take.

- **Anticipate technical challenges.** You should anticipate technical challenges, such as installation routines and distribution of smart card management tools. You might need to integrate the smart card solution into your existing enterprise management tools.
- **Monitoring and manage performance issues.** You must monitor and manage performance issues and set user expectations in advance of the deployment. For example, remote users who log on for the first time can experience a lengthy logon time if they select the **Log on using dial-up connection** check box on the **Log On to Windows** dialog box. You should ensure that remote users are aware of this delay.

- **Keep up to date.** If you plan to upgrade to the latest technology, do so early in the project implementation process. This strategy provides a baseline client and server platform and removes many of the variables that you might otherwise encounter during deployment. Service stability should also increase and user support costs decrease.

- **Implement project phases.** You should plan to implement the project in phases, and allow adequate time between phases for user adoption and for system and process stabilization. Phases that overlap can adversely affect the service, and will prevent the identification of service problems.

- **Consider personal assets.** Remember that employees’ home computers are their personal property and are not managed by corporate IT. If an employee does not want to or is unable to install the hardware and software to support smart card–secured remote access, other options are available. For example, Microsoft Outlook® Web Access provides employees with secure access to their Microsoft Exchange Server mailbox.

- **Manage changes to the solution.** You must manage any changes and enhancements to the solution through similar processes to those required for the initial deployment.

- **Optimize the solution.** All aspects of the smart card solution require periodic review and optimization. On a regular basis, Woodgrove IT needs to review the processes for enrollment and the need for account exceptions with the goal to improve security and integrity.

### How to Extend the Solution

Smart cards offer considerable potential for application development. For example, programmers can adapt the smart card extensible open platform and secure memory for uses such as a cashless payment system for the cafeteria.

Although the use of smart cards to secure remote access reduces attacks by unauthorized users, the solution does not ensure that remote access computers comply with network security policies. Network Access Quarantine Control, a feature of Windows Server 2003 with SP1, can confirm that remote computers run the latest antivirus updates and security updates. Quarantine control can perform other checks, for example a check that the Windows Firewall on Windows XP with SP2 is enabled. For more information about quarantine control, see [Implementing Quarantine Services with Microsoft Virtual Private Network Planning Guide](http://go.microsoft.com/fwlink/?LinkId=41307).
Summary

The implementation of smart cards to authenticate remote access connections provides greater security than simple user name and password combinations. Smart cards implement two-factor authentication through a combination of the smart card and a PIN. Two-factor authentication is significantly more difficult to compromise and the PIN is easier for a user to remember than a strong password.

The provision of smart card authentication for remote access users is a reliable and cost effective method that increases network security. This guide has taken you through the steps required to plan and implement this solution.
Appendix A: Related Links

The following resources contain further information about items that this guide discusses:

For more information about the new PKI enhancements found in Windows XP and Windows Server 2003, see [PKI Enhancements in Windows XP Professional and Windows Server 2003](www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.mspx)

For more information about smart card deployments, see [Planning a Smart Card Deployment](www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/DSSCG_SMC_OVERVIEW.asp)


For more information about deploying smart cards, see [The Smart Card Deployment Cookbook](http://www.microsoft.com/technet/security/guidance/identitymanagement/smrtcdcb/default.mspx).


To purchase smart card readers for evaluation purposes, see the [Windows Marketplace](at www.windowsmarketplace.com/results.aspx?text=smartcard).

For more information about Windows Server System reference architecture, see [Windows Server System Reference Architecture](www.microsoft.com/technet/itsolutions/wssra/default.mspx)

For more information about cross certification and qualified subordination, see [Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003](www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx)

Acknowledgements

The Solution Accelerators – Security and Compliance (SA-SC) team and the Security Center of Excellence (SCoE) would like to acknowledge and thank the team that produced The Secure Access Using Smart Cards Planning Guide. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

**Authors**
- Anthony Steven, **Content Master**
- Terry Tull, **Content Master**
- Lee Walker

**Reviewers**
- Mert Biyikly
- Chase Carpenter
- David Cross
- Kurt Dillard
- John Howie
- Greg Lenti
- Jose Maldonado
- John Morello
- Dave Mowers
- Steve Patrick

**Program Managers**
- Neil Bufton, **Content Master**
- Chase Carpenter
- Tom Cloward
- Alison Woolford, **Content Master**

**Editors**
- John Cobb, **Wadeware, LLC**
- Deborah Jay, **Content Master**
- Jennifer Kerns, **Content Master**
- Frank Manning, **Volt**

**Testers**
- Ashish Java, **Infosys Technologies**
- Mehul Mediwalla, **Infosys Technologies**
- Gaurav Singh Bora, **Infosys Technologies**

**Release Manager**
- Flicka Enloe
- Karina Larson

**Contributors**
- Tony Bailey
- Krishna Bhardwaj, **Vidyatech Solutions**
- Prabish Chandran, **Vidyatech Solutions**
- Charles Denny
- Christine Duell, **Valente Solutions**
- Amy Frampton
- Michael Glass, **Volt**
- Karl Grunwald
- Joanne Kennedy
- Karina Larson, **Volt**
- Chrissy Lewis, **Siemens**
- Don McGowan
- Tessa Porterfield
- Bivin Pachatt, **Vidyatech Solutions**
- Vivek Manohar Prabhu, **Vidyatech Solutions**
- Stacey Tsurusaki, **Volt**
- David Visintainer, **Volt**
- Vikas Walia, **Vidyatech Solutions**