第 1 章　Windows 系统安全概述

从 1983 年 Microsoft 公司宣布 Windows 的诞生到现在 Windows Server 2003 的推出，Windows 已经走过了 20 多年的历史。早期 Windows 之所以取得成功，主要归功于它友好美观、易学易用的面向对象的图形用户界面，降低了用户学习和掌握的门槛。而就从 Windows 系统本身而言，多任务执行、丰富的与设备无关的图形操作、提供大量开发接口和软件等特性，无疑为 Windows 的推广起到了加速作用。

早期的 Windows 系统，如 Windows 3.x、Windows 95 和 Windows 98，由于设计目的等其他因素的限制几乎无安全性可言。而以 Windows NT 为核心的系统开始，Microsoft 便为 Windows 系统引入了越来越多的安全特性。

1.1　Windows NT 基础与安全

Windows NT 是 Microsoft 推出的面向工作站、网络服务器和大型计算机的网络操作系统，也可作为个人计算机的操作系统。它与通信服务紧密集成，提供文件和打印服务，能运行客户机／服务器应用程序，内置了 Internet／Intranet 功能。从操作系统本身来看，Windows NT 主要有以下特点。

- 32 位操作系统，多重引导功能，可与其他操作系统共存。
- 实现了“ 抢先式 ”多任务和多线程操作。
- 采用 SMP（对称多处理）技术，支持多 CPU 系统。
- 支持 CISC（如 Intel 系统）和 RISC（如 Power PC、R4400 等）多种硬件平台。
- 可与各种网络操作系统实现互操作，如：UNIX、Novel Netware、Macintosh 等系统；对客户操作系统提供广泛支持，如 MS-DOS、Windows、Windows NT Workstation、UINX、OS／2、Macintosh 等；支持多种协议：TCP／IP、NetBEUI、DLC、AppleTalk、NWLINK 等。
- 安全性达到美国国防部的 C2 标准。

Windows NT 包含两个版本，分别是 Windows NT Workstation 和 Windows NT Server。Windows NT Workstation 的设计目标是工作站操作系统，适用于交互式桌面环境；而 Windows NT Server 的设计目标是企业级的网络操作系统，提供容易管理、反应迅速的网络环境。两者在系统结构上完全一样，只是为适应不同应用环境在运行效率上做了相应调整。Windows NT Server 具有更多的高级功能，可把 Windows NT Workstation 看作是它的子集。

Windows NT 在系统和网络安全性上引入了以下一些新的概念。

- NTFS（Windows NT File System）：Windows NT 采用的新型文件系统，可提供安全存取控制及容错能力，在大容量磁盘上，它的效率比 FAT 高。
- 共享权限：支持对网络资源设置一定的权限许可，没有得到权限许可，就无法访问网络资源。
- 用户账户（User Account）：要想使用网络资源，就必须有用户账户。Windows NT 对用户和服务程序，都要求提供合法账户。专为应用程序或服务进程创建的账户即服务账户，在系统启动时，服务进程使用服务账户登录以获得在系统中使用资源的权利和权限。普通用户账户由用户登录时提供，用于 Windows NT 控制该用户在系统中的权利和权限，与服务账户本质上没有区别。
- 域（Domain）：域是 Windows NT 中数据安全和集中管理的基本单位。网络由域组

成，域具有惟一的名称。域可以看作由运行 NT 的服务器组成的系统，一组电脑共用相同的账户及安全数据库。

- 工作组（Workgroup）：工作组是一种资源与系统管理都分散的网络结构。在工作组的范围里，每台电脑既可以充当服务器的角色，也可以充当工作站的角色，彼此之间是平等关系。
- 权限（Right）：权限是授权某用户可以在系统上执行某些操作。权限用来保护系统整体。
- 许可（Permission）：许可用来保护特定对象。许可规定可以使用某一对象的用户以及用什么方法使用。
- 安全审核：Windows NT 将记录发生在电脑上各项与安全系统相关的过程。

1.2 Windows 2000 基础与安全

Windows 2000 代表着 Microsoft 公司在其 Windows NT 产品系列的发展中，又向前迈出了重要的一步。Windows 2000 在保留了 Windows NT 部分内核的同时，为了提供业界所需的额外功能又增加了大量的内容，其中大部分新增内容都集中在了安全方面。这其中以活动目录为核心，丰富了安全功能的众多方面。

Windows 2000 操作系统包含有下面四个版本。

- Windows 2000 Professional：作为 Windows NT 4.0 Workstation 的替代产品，Windows 2000 Professional 的设计目标是成为桌面用户和移动用户共同的标准操作系统，提供高层次的安全性、稳定性和系统性能。
- Windows 2000 Server：作为 Windows NT 4.0 Server 的替代产品，Windows 2000 Server 的设计目标为通过支持基础设施服务、文件打印与包括 Web 在内的应用服务以及通信服务来成为主流的工作组和部门商务服务器。它引入了活动目录，通过 MMC 统一管理任务并引入了组策略，从而使管理（尤其是安全管理）得到简化。
- Windows 2000 Advanced Server：作为 Windows NT 4.0 Server Enterprise Edition 的替代产品，Windows 2000 Advanced Server 除了具有 Windows 2000 Server 的所有功能和特性之外，还有一些专为中大型应用范围的服务器所设计的特性。
- Windows 2000 Datacenter Server：这是 Windows 2000 新增的数据中心服务器，它提供了最高等级的性能，在 Windows 2000 Server 标准版的基础上针对企业部署与解决方案进行了必要的优化。

Windows 2000 的安全性很大程度上依赖于它的前身 Windows NT，因为 Windows NT 所有重要的安全特性都被转移到了 Windows 2000 之中，而且 Windows 2000 结构的大多数核心功能和面向对象的设计也都来自于 Windows NT。总的来说，Windows 2000 的某些具体目标是改进 Windows NT 的可扩展性、可靠性和安全性，并将许多附加功能集成到操作系统中。

- 可扩展性：包括更好的内存管理、作业对象管理、内核调整、Windows 驱动程序模型、Microsoft Installer（MSI）、更改和配置管理（Change and Configuration Management, CCM）等。
- 可靠性：包括写保护的驱动程序和内核代码段、驱动程序验证、修复控制台和安全引导等。
- 新的特性和集成特性：包括终端服务、即插即用以及电源管理等。
- 安全性：包括活动目录（Active Directory）、公钥基础结构（PKI）、组策略对象（Group Policy Object）、Kerberos 协议、智能卡支持、IP 安全协议（IPSec）、加密文件系统

（EFS）和安全配置工具集等。

1.2.1 活动目录

活动目录（Active Directory, AD）服务是 Windows 2000 安全模型灵活性与可扩展性的核心，它提供了完全集成于 Windows 2000 的一个安全、分布式、可扩展以及重复的分层目录服务。

活动目录替代了 Windows NT 早期版本中域控制器的注册表数据库内的安全账户管理器（Security Accounts Manager, SAM），从而成为用户账户、工作组和口令等安全信息的主要存储区域。同样地，活动目录形成了本地安全授权（Local Security Authorization, LSA）的一个可信任组件。换句话说，活动目录既为支持验证而存储了用户证书，也为支持授权访问系统资源而存储了访问控制信息。

活动目录主要包括两方面：目录和目录相关的服务。目录是存储各种对象的一个物理容器，目录管理的基本对象是用户、计算机、文件以及打印机等资源。而目录服务是使目录中所有信息和资源发挥作用的服务，如用户和资源管理、基于目录的网络服务、基于网络的应用管理。

活动目录是一个分布式的目录服务。一方面，信息可以分散在多台不同的计算机上，保证能够快速访问和容错；另一方面，不管用户从何处访问或信息处在何处，都对用户提供统一的视图。在当今网络计算爆炸性增长的 Internet 时代，活动目录还广泛采用了 Internet 标准，给用户带来了几乎无穷无尽的益处。活动目录集成了众多的关键服务，如域名服务（DNS）、消息队列服务（MSMQ）、事务服务（MTS）等；也集成了众多的关键应用，如电子邮件、网管、ERP 等；同时还集成了当今的关键的数据访问，如 ADSI，OLE DB 等。其中，通过把 Internet 域名系统概念集成到目录服务之中，活动目录可以帮助统一和管理多个现有的名称空间，并提供对所有资源的一个单一管理点。

1. 活动目录的层次结构

与用在 Windows NT 操作系统中的平面文件目录不同，Windows 2000 系统中的活动目录在用以表示业务结构的逻辑层次结构中存储信息，如图 1-1 所示。这种方式允许更大的增长空间及简化的管理。为了创建层次结构，Active Directory 使用域、组织单元（OU）及对象以使能够以更类似于在 Windows 中使用文件夹和文件来组织计算机上信息的方式来组织网络资源。

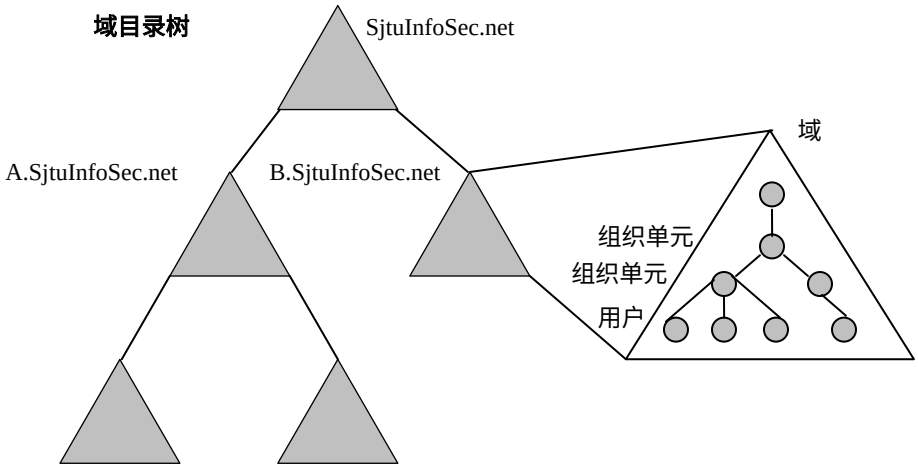

图 1-1 活动目录服务的层次结构

域是网络对象（包括组织单元、用户账户、组和计算机，它们都共享与安全性有关的公用目录数据库）的集合。域形成 Active Directory 内逻辑体系结构的核心单元，因此在安全性中扮演重要角色。如果将对象分组到一个或多个域中，网络就可反映整个公司或单位的组织方式。较大型的组织可以含有多个域，这种情况下的域层次结构就称为域目录树。第一个创建的域是根域，它是在其下创建的域的父域，其下的域称为子域。若要支持非常大型的组织，可将域目录树链接在一起，形成一种称为目录林的排列。在使用多个域控制器的情况下，Active Directory 会按固定时间间隔复制到域中的每个域控制器上，以使数据库永远同步。

域可标识一个安全机构，并使用一致的内部策略及与其他域间的明确安全性关系形成一个安全边界。特定域的管理员只有在本域中有设置策略的权限。这对大型的公司或单位尤其有用，因为不同的管理员可以创建并管理组织中不同的域。

站点则是有关 Active Directory 的另外一个术语。域通常会反映一个组织的商业结构，而站点则通常被用来定义与地理分布有关的 Active Directory 服务器组。这些计算机通常都以高速链接来连接，但它们彼此之间可以有也可以没有逻辑关系。例如，有一个大型办公大厦供一些相对无关的组织活动使用，如生产视频设备、开放软件、文件存储等，那么这栋大厦中的 Active Directory 服务器可以被当作一个站点（即使在该服务器上所完成的处理是不相关的）。

组织单元（OU）是指一个容器，可用它将对象组织成域中的逻辑管理组。OU 可包含对象，如用户账户、组、计算机、打印机、应用程序、文件共享和其他的 OU。对象包含关于个别项目（如特定用户、计算机或硬件等）的信息（称为属性）。例如，用户对象的属性可能包含姓和名、电话号码和管理者名称等；计算机对象可能包含计算机的位置及访问控制列表（ACL），列表中会指定对该计算机拥有访问权限的组和个人。

通过将信息分组到域和 OU 中，可以管理对象集合（如用户组和计算机组）的安全性，而不是逐个管理每个用户和对象。这通过后面所提到的“组策略”来实现。

2. 域间的信任关系

理解“信任关系”对于了解如何使用 Active Directory 来增强安全性极为重要。

为了让用户登录网络一次就可以使用网络上所有资源（通常称为单一登录能力，Single Sign-on），Windows 2000 支持域间的信任关系。所谓信任关系，是指一种逻辑关系，这种逻辑关系在域之间建立，用来支持直接传递身份验证，让用户和计算机可以在目录林的任何域中接受身份验证。这让用户或计算机仅需登录网络一次就可以对任何他们有适当权限的资源进行访问。这种穿越许多域的能力说明了传递信任这个术语，它是指跨越一连串信任关系的身份验证。

基于 Windows NT 的网络使用单向、非传递的信任关系。相反，当基于 Windows 2000 的域被组织成目录树时（如图 1-1 所示），域间会创建隐含的信任关系。这使得在中型和大型组织中建立域间的信任关系更为容易。属于域目录树的域定义与目录树中的父域的双向信任关系，而所有域都隐含地信任目录树中的其他域（如果有不应该有双向信任的特定域，应该定义明确的单向信任关系）。对于具有多个域的组织，使用 Windows 2000 比使用 Windows NT 4.0，明确的单向信任关系总数显著减少，这种改变将大大简化域的管理。传递信任在默认情况下建立于目录树中，这样做之所以有意义是因为通常是由单个管理员来管理一个目录树。但因为目录林不太可能被单个管理员控制，因此目录林的目录树间的传递信任关系必须特别创建。

有关信任关系的工作方式，可回顾一下图 1-1：Windows 2000 自动在根域（SjtuInfosec.net）及其两个子域（A.SjtuInfosec.net 和 B.SjtuInfosec.net）之间建立双向信任关系。此外，因为 SjtuInfosec.net 信任这两个子域，因此信任关系也在 A 和 B 域间传递性地

建立。这些关系在基于 Windows 2000 的域间自动建立。在有基于 Windows 2000 和基于 Windows NT 域的网络中，管理员可以创建用在基于 Windows NT 的网络中明确的单向信任关系。

为了向后兼容性，在 Windows 2000 中，信任关系通过使用 Kerberos v5 协议及 NTLM 身份验证来支持跨域的身份验证。这一点很重要，因为许多组织的基于 Windows NT 的企业域模型非常复杂，具有多个主域和许多资源域，而这些组织发现管理资源域和其主账户域间的信任关系既花费成本又非常复杂。因为基于 Windows 2000 的域目录树支持传递信任目录树，所以简化了较大型组织的网络域集成及管理。传递信任让管理员更容易定义和配置访问权限。

1.2.2 域控制器

与 Windows NT 一样，Windows 2000 的域仍由域控制器（Domain Controller）管理。但在 Windows 2000 系统中，域控制器已不再区分主域控制器（PDC）和备份域控制器（BDC）了。处在域中的服务器只能是域控制器（DC）或者是成员服务器（Member Server），并且可以很方便地互相转换角色，而 Windows NT 则不能。

Windows 2000 的域控制器彼此之间是平等的，各自保存有活动目录的一份复本。管理员可以改变任何一个 DC，并且对活动目录的升级会通过远程过程调用（Remote Procedure Call, RPC）自动复制到域范围内的所有其他 DC 上。这样就可以在域的范围内提供更大的弹性和负载平衡能力。

1.2.3 公钥基础结构

公钥加密技术用于保护开放网络（如 Internet）上活动的安全，它允许对数据进行加密和签名，并通过使用证书来验证客户机和服务器的身份。有两种用于公钥加密技术的密钥类型，一种是公钥，另一种是私钥。公钥在证书中很容易取得，但通过公钥加密后的数据只可以使用私钥来解密。一笔受到保护的交易需要公钥和私钥两种密钥来对包含于交易中的数据进行加密和解密。

这种公钥加密技术（也称作非对称加密）的挑战在于跟踪证书：随着在 Internet 上电子商务开展得越来越蓬勃，非授权用户获取对重要数据（如数字证书）访问权限的潜在机会也在增大。要想通过某种组织安全地分配和管理用户证书，就需要一个设计周密、建设完备的公钥基础结构（Public Key Infrastructure, PKI）。

PKI 是由数字证书、证书颁发机构（CA）和其他检查并验证参与电子交易各方合法身份的注册机构所组成的一个系统，它提供使用、管理及查找公钥证书的能力。

Windows 2000 扩展了以前 Windows 系统中基于公共密钥（PK）的加密服务，引进了全面建立标准的 PKI 所必需的工具。此外，Windows 2000 PKI 与 Active Directory 和操作系统的分布式安全服务完全集成在一起。

Windows 2000 的 PKI 提供了一个服务和相关的管理工具。 其中，证书服务是这一基础结构的核心，它允许部署一个或多个企业级的证书颁发机构（CA）来支持组织的商业需求。证书颁发机构使用公开密钥加密技术对电子商务所涉及的双方进行身份和有效性的验证。通过管理 X.509 公钥证书的颁发和吊销，CA 就能够组织建立和确认证书拥有者的身份。而且，证书服务以用目录服务发布关于证书服务相关信息的方式来集成到活动目录之中，这些信息包括用户证书的位置和证书吊销列表（CRL）。证书服务的一个独立组件是证书 Web 注册页，

它使得需要证书的用户可以方便的通过 Web 浏览器进行申请。而对于证书服务的管理员来说，则可以使用 Windows 2000 的组策略对象（Group Policy Object, GPO）来向计算机自动分配证书、建立证书信任清单和确定普遍受到信任的证书颁发机构。Windows 2000 公钥基础结构的组件构成如图 1-2 所示。

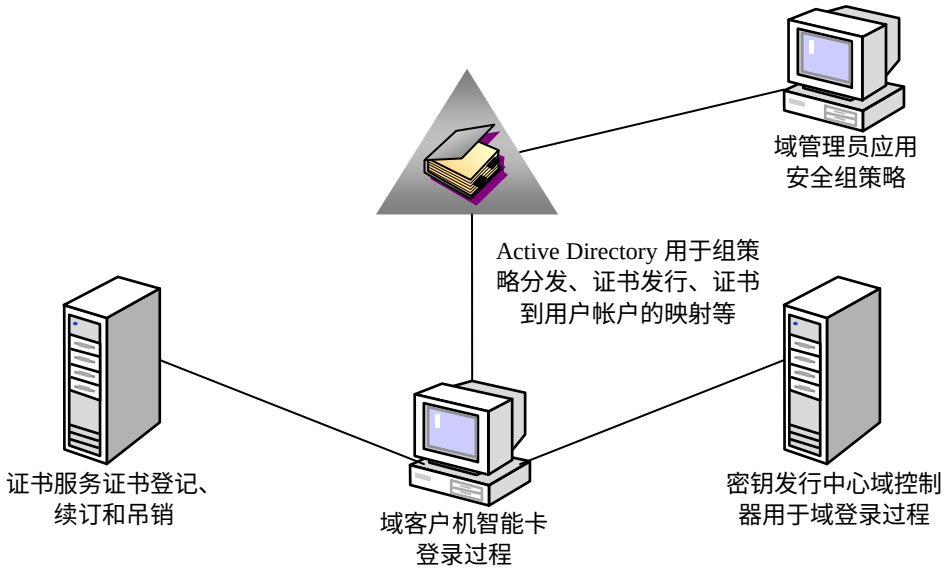

图 1-2　Windows 2000 公钥基础结构组件

一旦建立起管理数字证书的公钥基础结构之后，那么就有一系列增强的安全选项可用来处理下列技术：安全电子邮件、安全 Web 通信、加密文件系统（EFS）、IPSec、智能卡安全和经数字签名的软件。

1. PKI 证书支持

证书是一个由颁发机构签发的数字声明，它基本上可担保私钥持有者的身份。证书将公钥与持有相应私钥的人员、计算机或服务等身份连接到一起。基于 Windows 2000 证书的过程所使用的标准证书格式是 X.509v3。X.509 证书包含关于证书接收方的人或实体的信息、证书的信息以及签发证书的颁发机构的可选信息。

2. 证书服务

为了可以实现 PKI 而无须依靠外部 CA，Windows 2000 包含了一个称为“证书服务”的组件，可以用它来创建并管理 CA。“证书服务”与活动目录（Active Directory）和分布式安全服务紧密的集成在一起，如图 1-2 所示。

CA 负责创建并担保证书持有人的身份。CA 也可以撤消证书（如果证书不再被视为有效）并发布证书撤消列表（CRL）供证书确认方使用。最简单的 PKI 设计仅有一个根 CA。然而，实际上，大多数部署 PKI 的组织会使用许多 CA，这些 CA 组织成信任组（称为证书层次结构）。

“证书服务”有一个独立的组件是 CA Web 注册页。默认情况下，这些 Web 页在设置 CA 并允许证书请求者具有用 Web 浏览器提交证书请求的能力时就安装好了。此外，CA Web 页可以安装在未安装证书颁发机构的基于 Windows 2000 的服务器上。这种情况下，Web 页用于将证书请求定向到 CA，因为无论出于什么原因，都不会希望请求者直接进行访问。

为了部署公钥基础结构简单化，在 Windows 2000 内实现了计算机所用证书注册步骤的自动化。因为使用了 Active Directory，服务器会知道他们可以取得证书，而且会在需要时自动取得。这表示服务器管理员不需要到每一个服务器上手动执行所有步骤来注册服务器证

书。

3. 公钥策略

使用 Windows 2000 中的“组策略”不仅可以自动将证书分发给计算机，建立证书信任列表及信任证书颁发机构的列表，而且可以管理加密文件系统的恢复策略。

4. CryptoAPI

除“证书服务”外，Windows 2000 PKI 还依靠 Microsoft CryptoAPI v2 来进行安全的密码操作及私钥管理。CryptoAPI 是 Windows 2000 应用程序编程接口（API），为 Windows 和 Windows 应用程序提供密码服务。它提供一组功能，以允许应用程序加密数据或以数字方式灵活地签发数据，而同时又提供对私钥的保护。实际的密码功能由被称为密码服务提供程序（CSP）的独立模块实现。

5. 使用证书来验证外部用户的身份

在某些情况下，可能希望为外部用户提供一些对某 Web 站点上发布的特定数据的安全访问权（通常公众无法访问该站点）。典型的情况有：合作伙伴需要 Extranet 访问权；某一部门需要访问另一部门的 Intranet 网页；或者希望对部分公众提供选择性访问权。为此，Windows 2000 提供了一种可安全地为用户授予访问权限的方法，也就是使用 PKI 和 Active Directory 来验证用户的身份。可以将其运作方式简单地概述为：通过在 Active Directory 中创建用户账户并指派给外部用户来提供访问权；此账户对外部用户可在被访问的网络上使用的资源具有访问权；每个外部用户都需要有证书来验证其身份，该证书必须由证书颁发机构签发，这些机构列在 Active Directory 站点、域或组织单元（已在其中创建了用户账户的）的证书信任列表中；当用户登录时，系统会将用户的证书映射到账户，然后决定用户可以使用内部 Web 站点的哪些部分；而身份验证过程对外部用户来说是透明的。

6. PKI 用于 Windows 2000 的情况

除了上述的供外部用户验证其身份的方法外，还有其他一些情况也需要依靠 PKI。使用公钥技术的常规安全功能有：

- 使用安全/多重目的 Internet 邮件扩展（S/MIME）来保护电子邮件通信的安全。
- 为进行安全交易而创建数字签名。
- 使用 Secure Sockets Layer（SSL）或 Transport Layer Security（TLS）来保护 Web 上的通信安全。
- 签署可执行代码以便在公用网络上传递。
- 支持本地网络登录或远程网络登录。
- 为不使用 Kerberos 协议的客户端，或为 IPSec 通信的共享机密密码提供 Internet 协议安全性（IPSec）身份验证。
- 使用 Windows 2000 EFS 对文件进行加密。
- 使用智能卡保护登录凭据的安全。

1.2.4 组策略对象

Windows 2000 中的组策略对象（GPO）代替了 Windows NT 4.0 中的系统策略编辑器（System Policy Editor，用来配置存储在 Windows NT 注册表数据库中的用户和计算机设置）。“组策略”是 Active Directory 一项显著的功能，它允许以相同的方式将所有类型的策

略应用到众多计算机上。组策略设置是配置设置，管理者可用此设置来控制 Active Directory 中对象的各种行为。例如，可以使用组策略来配置安全性选项，管理应用程序，管理桌面外观，指派脚本，以及将文件夹从本地计算机重新定向到网络位置。

组策略是为用户和计算机组集中定义系统设置和应用程序而设置的，主要分为针对计算机的设置和针对用户的设置。系统将组策略设置在计算机激活时应用于计算机，在用户登录时应用于用户。

组策略可以设置以下内容。

- 软件策略：可设置那些影响操作系统的组件与应用软件的内容。
- 脚本：可添加、更改、删除牵涉到计算机启动、关闭、登录、注销等的脚本。
- 用户文档与设置：可向用户桌面的特定文件夹（位于 Documents And Settings 里的用户配置文件下）中增加文件、文件夹和快捷方式。
- 软件管理选项：可控制系统中哪些应用程序对哪些用户是可用的，系统管理员可通过这些选项为用户与计算机组安装、分配、发行、升级、维护和删除软件。
- 安全策略：可从一个安全模板中导入安全策略设置并自动采用；反之，可通过使用一个安全模板来分析系统当前的安全策略配置状况。

组策略被活动目录管理工具定义为域或组织单元（OU）的一个属性，所以可以将“组策略”配置设置与三个 Active Directory 容器相关联：组织单元（OU）、域或站点。与特定容器相关的“组策略”设置不是影响该容器中所有的用户或计算机，就是影响该容器中特定的对象集合。

可以使用“组策略”来定义广泛的安全性策略。域级策略应用于域中的所有用户并包含如账户策略等信息。例如，最短密码长度或用户多久该更改密码一次；可以指定在较低级别是否可改写这些设置。

在使用“组策略”功能来应用广泛的策略后，可以进一步细化个别计算机上的安全性设置。本地计算机安全性设置控制想要授予特定用户或计算机的权限和特权。

特定计算机的设置是从域到 OU 所有策略设置的组合。例如，在图 1-1 中，B.SjtuInfosec.net 域中用户的设置是 SjtuInfosec.net 域、B.SjtuInfosec.net 域及域中所有 OU 上设置的所有策略的集合。

1.2.5 Kerberos 协议

Windows 2000 使用 Internet 标准 Kerberos V5 协议（RFC 1510）作为验证用户身份的主要方法。Kerberos 协议提供在客户机和服务器之间的网络连接打开前交互身份验证的机制。此方法对包含开放通信（如那些已经在 Internet 上实现的）的网络来说是非常理想的。

Kerberos 验证协议定义了客户、资源和网络验证服务（密钥分配中心、KDC）之间的安全交互。在 Windows 2000 中，KDC 是作为每个域控制器上的验证服务来实现的。通过把活动目录当作用户（主体）和工作组的账户数据库，Windows 2000 域变成了 Kerberos 域的一个等价物。Windows 2000 将 Kerberos 协议完全集成到了 Winlogon 单一登录体系结构之中，提供了身份验证和访问控制功能。

Kerberos 协议是基于“票据”的思想。票据是由密钥分发中心（KDC）的可信颁发机构颁发的加密数据包。票据可以证明用户的身份，同时还携带了其他信息。KDC 为其颁发机构范围或“领域”内的所有用户提供票据，它提供身份验证服务和票据授予服务这两项服务。在 Windows 2000 中，每个域控制器就是一个 KDC，而域控制器的领域与其所在的域对应。

Kerberos 协议的操作过程其实比较简单，如图 1-3 所示。登录时，用户向 KDC 验证自

己的身份，KDC 为用户提供一个初始票据，称为 TGT（Ticket Granting Ticket, 票据授予票据）。此后，当用户需要使用网络资源时，其用户会话将 TGT 提交给域控制器，并请求特定的资源票据，即 ST（Service Ticket, 服务票据）。然后，用户将 ST 提交给资源，由资源授权访问。

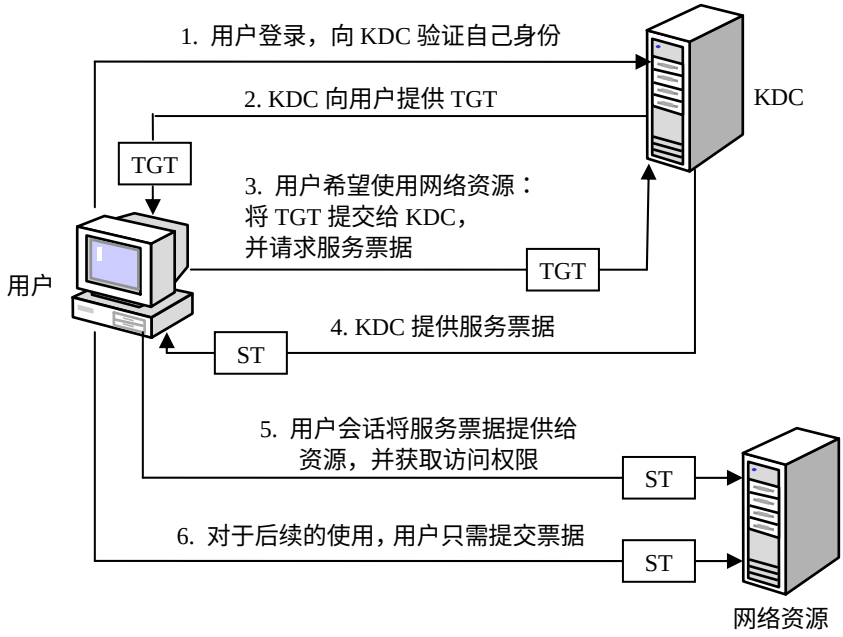

图 1-3 Kerberos v5 协议的验证流程

基于 Kerberos 协议的身份验证方法是对 Windows NT 4.0 身份验证过程（NTLM）的一种改进，后者则需要对用户所访问的每个网络资源进行单独的客户端身份验证。Kerberos 替换 NTLM 成为访问基于 Windows 2000 Server 的域内或域间的资源的主要安全协议（为确保向后兼容性，仍支持 NTLM）。完整的 Kerberos 协议支持对基于 Windows 2000 Server 的资源以及支持此协议的其他环境进行快速、单一的登录。

1.2.6 IPSec 协议

对于基于 Internet 协议（IP）网络安全的需求已经非常巨大，并且日益增长。今天在 Internet、企业内部网、分支办公室和远程访问的整体互连的商业世界中，敏感信息经常通过网络传输。由于 Internet 协议本身的问题，这些敏感信息容易遭受到篡改、监听、未授权访问等威胁。为了解决此问题，Windows 2000 合并了 Internet 协议安全措施（IPSec）。

IPSec 是一套 Internet 标准协议，允许两台计算机在不安全的网络上进行安全的、加密的通信。加密应用于 IP 网络层，亦即它对大部分使用特定网络协议的应用程序都是透明的。此外，IPSec 提供端对端的安全性，意味着 IP 包由发送计算机加密，在途中不可读取，只能由收件计算机解密。为了更加安全，此过程使用加密算法来产生用于连接两端的单一加密密钥，因此密钥无须通过网络发送。

可以配置 IPSec 以使其执行下列安全功能中的一个或多个。

- 根据 Kerberos 身份验证、数字证书或共享机密密钥（密码）来验证 IP 数据包发送者身份。
- 确保在网络上传送的 IP 数据包的完整性。
- 按照绝密等级对所有在网络上传送的数据进行加密。
- 在数据传输过程中，隐藏 IP 源地址。

这些功能可以确保网络上的数据传输是安全的，数据在途中不会被修改也不会被未经授权的一方截取、查看或复制。

Windows 2000 则对 IPSec 协议进行了实现，并与之相结合来保护网络通信数据。Windows 2000 的 IPSec 策略可通过 IP 安全策略这一 MMC 内嵌组件（工具）进行配置。使用这个工具就可以集中地设计 IPSec 策略，然后就可用活动目录中的组织单元把这些策略分配给单一计算机或者计算机组。IPSec 策略是围绕着 IP 筛选器列表和筛选器操作的概念而建立起来的。IP 筛选器列表决定了进行操作的对象范围，是基于单个还是某个范围内的源与目标 IP 地址、协议类型，甚至包括单个 IP 数据包的 TCP/UDP 端口；而筛选器操作等同于协商的策略，决定了你所要求的安全服务，如要求机密性还是不要求机密性等。结合这两者，就可以制定一个 IPSec 策略来为一个数据包提供 IPSec 服务，可以允许它未经加密地完整通过，或者经过协商加密后通过，还是将其丢弃。

1.2.7 加密文件系统

Windows 2000 中的加密文件系统（Encrypt File System, EFS）通过采用公开密钥加密技术来对磁盘上保存的数据进行加密，就可以保护用户系统中的文件和文件夹免遭非授权的访问。这里的非授权的访问包括如下两种情况：

- 未使用 Windows 2000 标准的访问控制列表（ACL）进行权限控制。
- 能够以物理途径访问系统的人可以使用特殊的工具软件来读取 Windows 的 NTFS 磁盘分区，来绕过 Windows 2000 操作系统文件访问控制的内置安全特性。

Windows 2000 的 EFS 设计得非常好用，对用户来说几乎是透明的。EFS 紧密集成到了 NTFS 中，提供了一个用户感觉不到读取加/解密文件时与原来有何不同的高性能系统。EFS 既支持对存储在本地磁盘中的文件进行加/解密，也支持对存储在远程主机磁盘中的文件进行加/解密。但因为加密是在读写操作期间自动发生的，所以一个已加密的文件在发送给远程主机之前从磁盘读出的时候就被解密，然后再写入远程主机操作系统的磁盘时又被重新加密。因此，EFS 只对本地存储的文件提供了保护，而未对传输中的数据提供保护。而要想保护传输中的数据就必须使用 IPSec 等其他网络安全协议。

此外，数据加密就带来了数据恢复的问题。若加密密钥丢失的话（如重装系统、人员离职等），则数据就无法再次访问，会带来很严重的损失。所以，Windows 2000 提供了在活动目录默认域策略中定制整个组织的 EFS 恢复策略，并把策略委托给域中的所有计算机。当然，Windows 2000 也提供了其他可选择方案。默认情况下，由域管理员控制 EFS 恢复策略，他可以把控制权授予他所指派的安全管理员，这就具有了高级控制和灵活性。EFS 还支持使用多个恢复代理，允许在实现恢复过程时可以有一定的冗余度和灵活性。

1.2.8 安全配置工具集

安全配置工具集（Security Configuration Tool Set）允许对 Windows 2000 操作系统安全属性进行配置，然后进行周期性的系统分析以保证配置的完整性，或者过后再进行必要的更改。换言之，该工具集允许管理员：

- 在一台或多台基于 Windows 2000 的计算机上配置安全设置
- 在一台或多台基于 Windows 2000 的计算机上执行安全分析
- 把安全配置当作组策略的一部分来使用

安全配置工具集可允许管理员定义包括下列几方面内容（也可称之为安全区域）的安全

模板。

- 账户策略：包括密码策略、账户锁定策略和 Kerberos 策略的安全设置（只和 Windows 2000 域控制器有关）。
- 本地策略：包括审核策略、用户权限分配与计算机安全选项的配置。
- 事件日志：包括对事件日志的配置设置。
- 受限制的组：包括对所选组的组成员身份管理的安全设置，所选组可能是被视为敏感的，如本地管理员和备份操作员。
- 系统服务：包括对所有的本地和网络系统服务的安全启动设置。这一部分的设计让独立软件供应商（ISV）能够为特定系统服务的配置和分析创建安全配置工具集附件。此外，Microsoft 将为随系统发行的一些服务创建附件。
- 注册表：包括对本地注册表键的访问控制设置和取值。
- 文件系统：包括对本地文件系统的访问控制设置。

为使组织的网络的安全性设置的管理及设置更容易一些，Windows 2000 Server 中包含了“安全模板”工具。Microsoft Management Console（MMC）管理单元允许管理员定义标准模板并将它以同样的方式应用于多个计算机或用户。安全模板是安全配置的实际体现。换句话说，它是一个可以存储一组安全设置的文件。Windows 2000 包含一组标准安全模板，每个模板分别适合一台计算机的角色：模板适用的范围从低安全性域客户端的安全性设置到高安全性域控制器的安全性设置皆可。这些模板可以用于提供、修改，也可以被当作创建自定义安全模板的基础。“安全配置和分析”工具是“安全模板”管理单元所附带的。它用于将定义在安全模板中的限制应用到实际系统中。它还可用于分析系统的安全性并与计算机上已经部署好的设置进行比较以确保它们符合标准。

1.2.9 智能卡

若要使未经授权的人更难取得访问网络的权限，智能卡是相对简单的一种方法。因此，Windows 2000 中包含对智能卡安全性的内置支持。

智能卡通常和信用卡大小一样，它所提供的抗篡改存储能够保护用户的证书和私钥。因此，智能卡提供了一种十分安全的用于用户身份验证、交互式登录、代码签名以及安全电子邮件的方法。智能卡包含一个芯片，用于存储用户私钥、登录信息和具有多种用途（如数字签名和数据加密）的公钥证书。

由于以下几种原因，智能卡要比密码安全一些。

- 验证用户身份时需要实体对象，即智能卡。
- 智能卡必须与个人标识号码（PIN）一起使用，以确保专人用专卡。
- 攻击者使用偷来的凭据这一风险被有效地排除了，因为要从卡中抽取密钥实际上是不可能的。
- 没有此卡，入侵者就无法访问智能卡所保护的资源。
- 没有任何密码形式或任何可重复使用的信息是通过网络传送的。

智能卡增强了仅针对软件的身份验证，方法是：在让用户访问资源前先要求用户提供实际对象（智能卡）并需要知道卡片的 PIN 码。这种既要展示卡片又要展示 PIN 的需求称为两项因素身份验证。用户不是输入密码，而是将卡片插入附于计算机上的智能卡读取器，然后输入卡的 PIN。Windows 2000 使用私钥和存储在卡片上的证书对在 Windows 2000 域控制器上的 KDC 验证用户身份。验证用户身份后，KDC 会返回授予票据的票据。自此，用户在此会话期间所进行的其他连接也都会使用上述的 Kerberos 身份验证。

1.2.10 其他安全性

还有一些更多是增强可靠性的方面，无疑也会增强安全性，因为这些方面直接影响到 Windows 2000 实施其安全模式的能力。

1. 核心模式写保护

为了保护操作系统中的每一部分不会受其他部分的错误的影响，Windows 2000 在内核部分和设备驱动程序中添加了写保护和只读部分，正像 Windows NT 总是有用户模式应用程序和动态链接库一样。为了提供这种保护，物理内存映射标志出包含代码的内存页面，保证它们不能够被覆盖，即使是操作系统也不能。这样就阻止了核心模式软件破坏其他核心模式软件。

2. Windows 文件保护

在 Windows 2000 以前的 Windows 版本中，安装软件可能覆盖系统文件。如果系统文件被覆盖，系统性能就会变得不可靠，程序的行为就会混乱，操作系统可能会失败。

Windows 文件保护系统在安装之前检查原来的系统文件的版本，这样就保证像.sys, .dll, .ocx, .ttf, .fon, .exe 等系统文件不会被替代。Windows 文件保护在后台运行，保护所有由 Windows 2000 安装程序所安装的文件。它检测其他程序要替换或删除一个被保护的系统文件的企图。Windows 文件保护检查文件的数字签名来确定新文件是否为正确的版本，如果这个文件的版本不正确，Windows 文件保护就从 dllcache 目录，网络安装路径或者 Windows 2000 光盘中替换这个文件。如果 Windows 文件保护找不到合适的文件，它就会提示用户输入正确的路径。Windows 文件保护还会将替换文件的企图写入事件日志。

默认情况下，Windows 文件保护是被激活的。Windows 2000 系统只允许在安装下面的软件时替换被保护的系统文件：

- 安装 Windows 2000 Service Packs
- 安装 Hotfix.exe
- 升级操作系统
- Windows 2000 Device Manager/Class Installer

3. 驱动程序签名

大多数的 Windows 2000 崩溃错误往往是由于驱动程序的问题所引起的。驱动程序签名是指将一个加密的数字签名附加在通过了 Windows Hardware Quality Labs（WHQL）测试的代码文件上。驱动程序签名有助于提高驱动程序的质量，因为它允许 Windows 2000 和 Windows 98 通知用户它们安装的驱动程序是否通过了微软的认证。

如果驱动程序运行在 Windows 2000 和 Windows 98 操作系统中，那么给驱动程序签名则是 WHQL 测试的一部分。数字签名与独立的驱动程序包结合在一起，Windows 2000 可以识别它。该数字签名确保文件已经执行并通过了一个水平测试，而且这些文件没有被篡改。如果用户试图安装未签名的驱动程序，Windows 2000 就会通知用户。 驱动程序允许用户采取三种反应：警告（Warn）、阻止（Block）和忽略（Ignore）。

- Warn：在被安装的驱动程序没有数字签名的情况下，让用户了解，并且让用户决定是否安装。Warn 还使用户可以选择安装一个被保护的驱动程序文件的未签名版本。
- Block：禁止安装所有未签名的驱动程序。
- Ignore：允许安装所有文件，而不管这些程序有无数字签名。

1.3 Windows Server 2003 基础与安全

Windows Server 2003 包含有以下几个版本。

- Windows Server 2003 标准版：标准版是一个可靠的网络操作系统，可迅速方便地提供企业解决方案。这种灵活的服务器是小型企业和部门应用的理想选择。
  - 支持文件和打印机共享
  - 提供安全的 Internet 连接
  - 允许集中化的桌面应用程序部署
- Windows Server 2003 企业版：企业版是为满足各种规模的企业的一般用途而设计的。它是各种应用程序、Web 服务和基础结构的理想平台，它提供高度可靠性、高性能和出色的商业价值。
  - 一种全功能的服务器操作系统，支持 8 个处理器
  - 提供企业级功能，如 8 节点群集、支持高达 32 GB 内存等
  - 可用于基于 Intel Itanium 系列的计算机
  - 可用于能够支持 8 个处理器和 64 GB 内存的 64 位计算平台
- Windows Server 2003 Datacenter 版：数据中心版是为运行企业和任务所依靠的应用程序而设计的，这些应用程序需要最高的可伸缩性和可用性。
  - 是 Microsoft 迄今为止开发的功能最强大的服务器操系统
  - 支持高达 32 路的 SMP 和 64 GB 的内存
  - 提供 8 节点群集和负载平衡服务是它的标准功能
  - 可用于能够支持 64 位处理器和 512 GB 内存的 64 位计算平台
- Windows Server 2003 Web 版：这是 Windows 操作系统系列中的新产品，Windows Server 2003 Web 版用于 Web 服务和托管。
  - 用于生成和承载 Web 应用程序、Web 页面以及 XML Web 服务
  - 其主要目的是作为 IIS 6.0 Web 服务器使用
  - 提供一个快速开发和部署 XML Web 服务和应用程序的平台，这些服务和应用程序使用 ASP.NET 技术，该技术是.NET 框架的关键部分
  - 便于部署和管理

Windows Server 2003 提供了一些新的安全特性和功能，来为企业组织在保护它们的信息资产时，能够满足其需求。Windows Server 2003 在 Windows 2000 的基础上，提供了以下一些新的安全特性。

1.3.1 身份验证

在一个大型网络环境中要安全地与各种关系的用户（如客户、合作伙伴和员工）进行合作，就需要对用户的身份进行验证来避免未授权的公共信息资产访问。Windows Server 2003 通过 Kerberos 协议延续了 Microsoft 许诺的基于标准的安全。此外，Windows Server 2003 还为身份验证引入了新的特性。

1. 森林信任

Windows Server 2003 支持跨森林的信任，这将允许明确地信任某个或者全部域，或者是另一个森林的用户或者组。还能为其他森林的用户或者用户组设置权限。跨森林信任关系

将使得企业能够很方便地与其他使用 Active Directory 服务的单位进行业务交流。

新增的这一安全特性将使得管理多森林信任关系和跨域信任关系变得更加简单。凭证管理器提供一个安全放置用户凭证的位置，包括用户凭证以及 X.509 证书。此外，森林间信任关系将提供一个新的 Windows 信任类型用于管理两个森林之间信任关系的安全问题，跨森林安全管理和验证都变得非常简单。

该特性允许用户在不牺牲单一登录机制的前提下，通过使用 Kerberos 或者 NTLM 来安全地访问另一个森林中的资源。而且，由于只存在一个需要维护的用户 ID 和口令，管理也被大大简化了。

2. 信任关系管理

该安全特性提供了用户名和密码的一个安全存储，并且也存储了证书和密钥的链接。这使得能够为用户（包括漫游用户）提供一致的单一登录。单一登录特性使得用户无须重复提供它们的凭证，就能够通过网络访问资源。

3. 改进的委派模式

委派是一种允许服务模拟用户或计算机的账户来通过网络访问资源的行为。委派模式的改进包括允许任意客户端和 Web 服务器之间使用任意 Internet 协议进行连接并允许 Kerberos 用于 Web 服务器和后台数据服务器之间的验证。该特性还包括一个基于 Kerberos 的委派新模式，这一新模式不需要可传递的 Ticket Granting Tickets（TGT）以及设置强制约束委派，允许某个账号委派控制域级策略中的某一个服务。

4. 协议转换

现在 Intranet 的用户普遍使用基于 Kerberos 协议的标准认证机制来进行身份验证，但是在 Internet 中，用户应用得却没有那么普遍。正因如此，一个需要访问 Internet 的应用必须放弃委派的好处，或者获取用户的密码并亲自对其进行验证。在 Windows Server 2003 中，新的 Kerberos 协议转换机制允许一个服务转换为用户的一个基于 Kerberos 的标识，而无须知道用户的密码，也无须用户使用 Kerberos 进行验证。这样，一个基于 Internet 的用户能够使用传统的验证机制进行身份验证，然后获取一个 Windows 标识。

1.3.2 访问控制

健壮的权限授予能够帮助企业更有效地控制用户、计算机和服务对公共信息资产的访问。Windows Server 2003 提供了新的特性，使得能够以更细的粒度，通过使用基于角色的授权、基于 URL 的授权以及软件限制策略来管理和控制访问。

1. 基于角色的访问控制

Windows NT 和 Windows 2000 提供的是以对象为中心的授权模型。而与之相比，在 Windows Server 2003 中基于角色的访问控制则是以用户为中心的授权模型。该模型允许管理员根据单位的组织结构来设置访问控制，而不必为每个用户枚举系统中的对象和指定权限。基于角色的访问控制提供了一个核心对象——角色，也就是被指定执行特定工作的用户。角色本身暗含了对某些已定义资源集的授权权限。

2. 基于 URL 的访问控制

这种访问控制机制允许通过限制用户对 URL 的访问，来对暴露在 Web 上应用的访问进

行控制。举个例子，一个匿名用户只能够执行某些特定的应用程序，而一个授权用户则允许执行其他应用程序。

3. 软件限制策略

访问控制策略限制对资源的访问，而 Windows Server 2003 中的软件限制策略（Software Restriction Policy, SRP）则控制在系统上应用程序的运行。这将允许系统管理员使用策略或强行阻止在某台计算机上运行可执行程序。例如，明确为企业内部范围的应用程序可被限制运行，除非它们在特殊路径上运行。软件限制策略也可通过设置来防止运行时遭到病毒感染或恶意攻击。

1.3.3 审计

在 Windows Server 2003 系统中使用了增强的审计特性来提供更高效、实时的入侵检测系统来监控和帮助识别可疑行为（可能就是攻击行为）。

1. 基于操作的审计

在 Windows Server 2003 中，通过在服务器或工作站的安全日志中选择记录特定的事件类型，能够提供更细粒度的用户行为跟踪能力。比如，新的审计特性不但能够跟踪到用户访问了一个文件，而且能够跟踪到用户对文件的具体操作，比方说用户如何修改文件等。

2. 每用户选择的审计

使用 Windows Server 2003 中的新功能，除了系统级别的审计策略之外，还能够为单独的一个用户设置审计策略。

3. 增强的登录和注销账户管理的审计

Windows Server 2003 增强了登录和注销账户管理的审计。举例来说，登录和注销事件中还包括了 IP 地址和登录/注销请求者的信息。此外，账户管理审计还能够精确提供账户更改前后的属性变化情况。

4. Microsoft 审计采集系统

Microsoft 审计采集系统（Microsoft Audit Collection System, MACS）是一个基于客户端/服务器的应用程序。该应用程序利用了审计特性上的改进，实时地收集安全事件并且存储在 SQL 数据库中以备分析。MACS 允许用户在一个中心点上收集数据，而不受管理员的干预。这样就将管理员的角色和审计员的角色分开。

1.3.4 公钥基础结构

PKI 是数字证书的一个系统，认证授权机构（CA）以及其他的注册授权机构（RA）核实和验证通过公钥加密技术进行电子交易的每一方。Windows Server 2003 在 PKI 上的改进使得 PKI 及与其相关的技术（如智能卡）能够更易管理，更方便进行开发和操作。

1. 交叉认证

交叉认证允许在分隔的层次结构之间建立信任，增强了管理 PKI 的效率。交叉认证采

用交叉证书，所谓的交叉证书是 CA 之间互相签发的证明对方身份的证书。交叉证书是由一个 CA（如 CA1）向另一 CA（如 CA2）提出请求，由后者签发的。所以这张证书的主体是 CA1，证书的签发者是 CA2。由于 CA2 信任 CA1，于是 CA2 安全域中的用户也将信任 CA1，也将信任 CA1 安全域中的用户，这样 CA1 安全域中的用户就可以进行跨域访问。交叉证书一般是互相签发的。

2. Delta 证书吊销列表

Windows Sever 2003 支持 Delta 证书吊销列表（CRL），这使得发布吊销 x.509 证书更加有效。在 Windows 2000 中，证书发行机构将通过发布完整的 CRL 而负责提供证书状态信息。CRL 可按预先定义的间隔进行手动或自动发布。而 Delta CRL 列表中仅包含自上一个完整的（基本）CRL 以来状态已发生变化的证书。相对于标准 CRL 发布而言，Delta CRL 有以下几点主要优势：

- 对象大小远小于完整的 CRL。
- 可经常发布，对客户机或网络体系结构有很小的影响或无影响。
- 非常小的吊销状态延迟。
- 对体系结构或网络的影响最低。

3. 密钥归档

在对数据进行恢复之前，常常必须进行密钥恢复。在 Windows Server 2003 中，认证授权机构（CA）习惯于归档和恢复与单独的一个证书请求关联的私钥。所以，在为已用加密文件系统（EFS）加密的文件和 S/MIME 加密的邮件进行解密时，它比使用 Windows 2000 Server 的数据恢复代理提供了更大的弹性。

4. 自动注册和更新

在 Windows Server 2003 中，证书的自动注册和自动更新显著降低了管理 x 509 加密证书所需的资源数量。这些特性也使得开发智能卡更方便、更快速；且通过自动注销和更新证书也能够改善无线（IEEE 802.1x）连接的安全性。

1.3.5 网络安全

Windows Server 2003 既提供有线通信的安全，也提供无线通信的安全。为了增强无线通信的安全，Windows Server 2003 支持 802.1x 协议，提供对 PEAP（保护扩展认证）的支持。为了改进有线通信，Windows Server 2003 增强了 IPSec 协议。

1. Internet 连接防火墙

在 Windows XP 和 Windows Server 2003 中使用基于软件的防火墙以提供 Internet 安全，即 Internet 连接防火墙（ICF）。ICF 可为直接连到 Internet 上的计算机和位于 Internet 连接共享主机（ICS）后面的计算机提供保护。

2. 隔离

网络访问隔离控制是 Windows Server 2003 家族的一个新特性。这一特性延迟了正常的对虚拟网络的远程访问，直到远程访问计算机的配置被管理员所提供的脚本检查并验证过。网络访问隔离控制被设计成阻止具有不安全配置的计算机连接私有网络，而不是阻止拥有一系列合法凭证的不怀好意者访问私有网络。

3. 无线和以太局域网安全

Windows Server 2003 内置对 IEEE 802.1x（Wi-Fi）认证协议的支持，使得能够对计算机和用户进行身份识别，动态创建密钥和集中式鉴别。对扩展验证协议（EAP）的 Wi-Fi 支持使得开发安全的无线访问（包括智能卡）更加容易。因为带有可扩展认证协议—传输层安全协议（EAP-TLS）的 IEEE 802.1x 提供动态密钥检测，通过对与 IEEE802.11 定义认证和有线等效保密性（WEP）相关的一些熟知文件的定位，IEEE802.11 无线网络的安全得到了极大的提高。

作为 IETF 因特网“保护式 EAP”草案的共同认证者，Microsoft 使用保护式可扩展认证协议（PEAP）。当预留对任何 IEEE 802.11 和 802.1X 无线访问点的互操作性时，组织的观点是使用 Windows 域的口令而不是部署证书架构来认证和加密无线连接。

通过使用 Internet 认证服务器（IAS），企业同样可以在一个验证网络中使用 802.1X 验证或自引导系统配置来授予 Guest 用户 Internet 访问权。管理员可能拒绝那些不能提供有效的验证凭证的连接请求，例如互联网和用于自引导配置的网段地址，从而把一些特定地址范围或一些虚拟局域网（VLAN）隔离保护起来。

4. 增强的 IP 安全（IPSec）

Windows Server 2003 的 IPSec 支持使用 2048 位的 Diffil-Hellman 密钥交换，使得密钥变得更强壮。此外，在 Windows XP 和 Windows Server 2003 系统家族中，IP 安全监视器已经被实现为 MMC（Microsoft 管理控制台）的一部分，即成为其中的一个管理单元了。IP 安全监视器还作了改进，允许查看本地计算机和远程计算机的信息。此外，在本地 IPSec 策略或者一个基于 Active Directory 的 IPSec 策略不能被应用的时候，还可能创建并指派一个固定的 IPSec 策略来保护计算机。

1.3.6 数据加密

1. 多用户支持

Windows Server 2003 支持一个单独的加密数据文件在多用户之间共享。加密文件的共享为在用户之间不共享私钥的前提下进行协作提供了有用和方便的途径。

2. WebDAV 支持

加密文件系统（EFS）与 WebDAV（Web Distributed Versioning and Authoring, Web 分布式创作与版本控制）目录组合在一起，能够跨网络提供简单和安全共享敏感数据的途径，而无须配置复杂的架构或者应用高深的技术。WebDAV 是一种使用 XML 描述的文件协议。

3. 加密脱机文件和文件夹

脱机文件，即客户端缓存，是在 Windows 2000 中被引入的，它允许一个移动用户在断开网络的情况下查看文件。当用户以后连接网络的时候，系统将与服务器上的旧版本文件保持一致。Windows 2000 不允许对隐藏文件加密，所以不支持加密脱机文件和文件夹。而 Windows Server 2003 则允许使用 EFS 加密脱机文件和文件夹。

4. 增强的加密

Windows Server 2003 对于 EFS 支持比默认数据加密标准算法（DESX）更强壮的算法，这是可选的。默认情况下，加密文件系统使用高级加密标准（AES-256）来对所有的文件进

行加密。客户端也须使用一种联邦信息处理标准（FIPS）140-1 适应算法，比如包含在 Windows XP 系统中的 3DES 算法。