What Is Kerberos Authentication?

In this section

- Kerberos Authentication Benefits
- Kerberos V5 Protocol Standards
- Supported Extensions to the Kerberos V5 Protocol
- Technologies Related to Kerberos Authentication
- Kerberos Authentication Dependencies

The Kerberos version 5 authentication protocol provides a mechanism for authentication — and mutual authentication — between a client and a server, or between one server and another server.

Windows Server 2003 implements the Kerberos V5 protocol as a security support provider (SSP), which can be accessed through the Security Support Provider Interface (SSPI). In addition, Windows Server 2003 implements extensions to the protocol that permit initial authentication by using public key certificates on smart cards.

The Kerberos Key Distribution Center (KDC) uses the domain’s Active Directory directory service database as its security account database. Active Directory is required for default NTLM and Kerberos implementations.

The Kerberos V5 protocol assumes that initial transactions between clients and servers take place on an open network in which packets transmitted along the network can be monitored and modified at will. The assumed environment, in other words, is very much like today’s Internet, where an attacker can easily pose as either a client or a server, and can readily eavesdrop on or tamper with communications between legitimate clients and servers.

Microsoft’s implementation of the Kerberos V5 protocol is:


The Kerberos V5 protocol became the default authentication package with Windows 2000. Windows Server 2003 still supports NTLM for non-Kerberos clients such as the Windows NT Server 4.0 operating system.
Based on RFC 1510 and draft revisions.
The Kerberos protocol is a mature, widely used, open standard. Microsoft’s implementation of the Kerberos V5 protocol adheres to the defined RFC standards, and thus provides interoperability with other implementations.

Extensible.
Kerberos architecture allows you to specify additional or alternate security methods. Also, the default shared secret key process can be supplemented with private/public key pairs by using smart cards.

Kerberos Authentication Benefits
The Kerberos V5 protocol is more secure, more flexible, and more efficient than NTLM. The benefits gained by using Kerberos authentication are:

Delegated authentication.
Windows services impersonate a client when accessing resources on the client’s behalf. In many cases, a service can complete its work for the client by accessing resources on the local computer. Both NTLM and the Kerberos V5 protocol provide the information that a service needs to impersonate its client locally. However, some distributed applications are designed so that a front-end service must impersonate clients when connecting to back-end services on other computers. The Kerberos V5 protocol includes a proxy mechanism that enables a service to impersonate its client when connecting to other services. No equivalent is available with NTLM.

Interoperability.
Microsoft’s implementation of the Kerberos V5 protocol is based on standards-track specifications that are recommended to the Internet Engineering Task Force (IETF). As a result, the implementation of the Kerberos V5 protocol in Windows Server 2003 lays a foundation for interoperability with other networks in which the Kerberos V5 protocol is used for authentication.

More efficient authentication to servers.
With NTLM authentication, an application server must connect to a domain controller in order to authenticate each client. With the Kerberos V5 authentication protocol, on the other hand, the server is not required to go to a domain controller. Instead, the server can authenticate the client by examining credentials presented by the client. Clients can obtain credentials for a particular server once and then reuse those credentials throughout a network logon session. Renewable session tickets replace pass-through authentication. For more information about what renewable session tickets are and how they work, please see “How the Kerberos Version 5 Authentication Protocol Works.”

Mutual authentication.

By using the Kerberos protocol, a party at either end of a network connection can verify that the party on the other end is the entity it claims to be. Although NTLM enables servers to verify the identities of their clients, NTLM does not enable clients to verify a server’s identity, nor does NTLM enable one server to verify the identity of another. NTLM authentication was designed for a network environment in which servers were assumed to be genuine. The Kerberos V5 protocol makes no such assumption.

Kerberos V5 Protocol Standards

The Kerberos authentication protocol originated at MIT more than a decade ago, where it was developed by engineers working on Project Athena. The first public release was the Kerberos version 4 authentication protocol. After extensive industry review of that protocol, the protocol’s authors developed and released the Kerberos version 5 authentication protocol.

The Kerberos V5 protocol is now on a standards track with the IETF. The implementation of the protocol in Windows Server 2003 closely follows the specification defined in Internet RFC 1510. In addition, the mechanism and format for passing security tokens in Kerberos messages follows the specification defined in Internet RFC 1964.

The Kerberos V5 protocol specifies mechanisms to:

• Authenticate user identity. When a user wants to gain access to a server, the server needs to verify the user’s identity. Consider a situation in which the user claims to be, for example, Alice@tailspintoys.com. Because access to resources are based on identity and associated permissions, the server must be sure the user really has the identity it claims.
• **Securely package the user’s name.** The user’s name — that is, the User Principal Name (UPN): Alice@tailspintoys.com, for example — and the user’s credentials are packaged in a data structure called a ticket.

• **Securely deliver user credentials.** After the ticket is encrypted, messages are used to transport user credentials along the network.

**Note**

• Although the Kerberos protocol authenticates the user's identity, it does not authorize access. This is an important distinction. Tickets in other contexts, such as drivers' licenses, often both prove identity and authorize actions or access. A Kerberos ticket only proves that the user is who the user claims to be. After the user’s identity is verified, the Local Security Authority will authorize or deny resource access.

**Keys: Privacy Through Encryption**

Kerberos messages are encrypted with various encryption keys to ensure that no one can tamper with the client’s ticket or with other data in a Kerberos message.

Possible Kerberos keys include:

**Long-term key.**

A key — known only to the target server and the KDC — with which the client’s ticket is encrypted.

**Client/server session key.**

A short-term, single-session key that is created by the KDC and used to encrypt the client-to-server and server-to-client messages after identity and authorization have been confirmed.

**KDC/user session key.**

The KDC and the user share a secret encryption key as well, which is used, for example, to encrypt the message to the client containing a session key.

**The Kerberos V5 protocol can use both symmetric and asymmetric encryption**

Because most Kerberos encryption methods are based on keys that can be created only by the KDC and the client, or by the KDC and a network service, the Kerberos V5
protocol is said to use symmetric encryption. That is, the same key is used to encrypt and decrypt messages.

Microsoft’s implementation of the Kerberos protocol can also make limited use of asymmetric encryption. A private/public key pair can be used to encrypt or decrypt initial authentication messages from a network client or a network service.

**Kerberos Authenticator Prevents Packet Replay**

The Kerberos authentication mechanism creates and securely delivers an authenticator — usually based on unique timestamps — along with the client’s ticket. The authenticator is unique and valid for only one use. This limited use minimizes the possibility of someone obtaining and re-using (replaying) the client ticket, perhaps in an attempt to steal and use the client’s identity.

**Supported Extensions to the Kerberos V5 Protocol**

Windows Server 2003 implements extensions to the Kerberos V5 protocol. The extensions enable initial authentication by using public key certificates instead of conventional shared secret keys. This enhancement enables the protocol to support interactive logon with a smart card. The extensions for public key authentication are based on a draft specification being worked on by the IETF working group.

**Technologies Related to Kerberos Authentication**

The following diagram shows how Kerberos authentication fits with other technologies in Windows Server 2003. Depending on whether the client or server applications are user-mode or kernel-mode applications, they use either Secur32.dll or Ksecdd.sys, respectively, by means of SSPI calls to communicate with the Local Security Authority Subsystem (LSASS).

**Kerberos Architecture**

The following table is a description of the components that participate in Kerberos Authentication.

**Security Subsystem Components Used in Digest Authentication**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>

5
<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos.dll</td>
<td>The SSP that implements an industry-standard protocol that is used with either a password or a smart card for interactive logon. It is also the preferred authentication method for services in Windows 2000 and Windows Server 2003.</td>
</tr>
<tr>
<td>Kdcsvc.dll</td>
<td>The Kerberos Key Distribution Center (KDC) service, which is responsible for providing ticket-granting tickets to clients.</td>
</tr>
<tr>
<td>Ksecdd.sys</td>
<td>The Kernel Security Device Driver is used to communicate with LSASS in user mode.</td>
</tr>
<tr>
<td>Lsasrv.dll</td>
<td>The LSA Server service, which both enforces security policies and acts as the security package manager for the LSA.</td>
</tr>
<tr>
<td>Secur32.dll</td>
<td>The Secur32.dll component is the multiple authentication provider that implements SSPI for user mode applications.</td>
</tr>
</tbody>
</table>

Windows Server 2003 implements the Kerberos V5 authentication protocol as an SSP, which is a dynamic-link library (DLL) supplied with the operating system. The system uses the Kerberos SSP, Kerberos.dll, as its first choice for authentication. After the LSA establishes a security context for an interactive user, another instance of the Kerberos SSP can be loaded by a process running in the user’s security context in order to support the signing and sealing of messages.

Because the Kerberos protocol is the preferred authentication protocol for Windows Server 2003, all domain services support the Kerberos SSP, including:

- Remote server or workstation management using RPC calls.
- Print services.
- Client-server authentication.
- Remote file access that uses Common Internet File System/server message block (CIFS/SMB).
- Distributed file system management and referrals.
- Intranet authentication to Internet Information Services (IIS).
- Security authority authentication for Internet Protocol security (IPSec).
- Certificate requests to Certificate Services for domain users and computers.

**Kerberos Authentication Dependencies**

This section reviews dependencies and summarizes how each dependency relates to Kerberos authentication.
Operating System
Kerberos authentication relies on client functionality that is built into the Windows Server 2003 operating system, the Microsoft Windows XP operating system, and the Windows 2000 operating system. If a client, domain controller, or target server is running an earlier operating system, it cannot natively use Kerberos authentication.

TCP/IP Network Connectivity
For Kerberos authentication to occur, TCP/IP network connectivity must exist between the client, the domain controller, and the target server. For more information about TCP/IP, see “TCP/IP Technical Reference.”

Domain Name System
The client uses the fully qualified domain name (FQDN) to access the domain controller. DNS must be functioning for the client to obtain the FQDN.

For best results, do not use Hosts files with DNS. For more information about DNS, see “DNS Technical Reference.”

Active Directory Domain
Kerberos authentication is not supported in earlier operating systems, such as the Microsoft Windows NT 4.0 operating system. You must be using user and computer accounts in the Active Directory directory service to use Kerberos authentication. Local accounts and Windows NT domain accounts cannot be used for Kerberos authentication.

Time Service
For Kerberos authentication to function correctly, all domains and forests in a network should use the same time source so that the time on all network computers is synchronized. An Active Directory domain controller acts as an authoritative source of time for its domain, which guarantees that an entire domain has the same time. For more information, see “Windows Time Service Technical Reference.”

Service Principal Names
Service principal names (SPNs) are unique identifiers for services running on servers. Every service that uses Kerberos authentication needs to have an SPN set for it so that clients can identify the service on the network. If an SPN is not set for a service, clients have no way of locating that service. Without correctly set SPNs, Kerberos
authentication is not possible. For more information about user-to-user authentication, see “How the Kerberos Version 5 Authentication Protocol Works,” and search for “The User-to-User Authentication Process.”