

Kerberos Explained

By Mark Walla

Article from the May 2000 issue of *Windows 2000 Advantage Magazine*

Although this article is billed as a primer to Kerberos authentication, it is a high technical review. Kerberos is an integral part of Windows 2000 Active Directory implementations, and anyone planning to deploy and maintain a Windows 2000 enterprise must have a working knowledge of the principals and administrative issues involved in this front-line security technology.

Since many other operating system vendors are also adopting this MIT-developed authentication protocol, Kerberos Version 5 will increasingly become a centerpiece of enterprise-level interoperability. Kerberos provides secure user authentication with an industry standard that permits interoperability. The Active Directory domain controller maintains user account and log-in information to support the Kerberos service.

The process of authenticating the identity of users during log-in is the first step in gaining system access. For local machines that aren't actively participating in a domain, Windows NT LAN Manager protocol is still utilized to verify a user's name and password before granting system access. However, in domain environments, Microsoft has coupled Active Directory closely with Kerberos. Once access is granted, tickets that permit specific access to other system resources within the domain are exchanged.

Kerberos 101

Underlying Windows 2000 security is the concept of user authentication. The centralized account management supported by Active Directory Services requires a corresponding authentication protocol for network log-on. Based on RFC 1510, the Kerberos Version 5 protocol provides enhanced authentication for the distributed computing environment and standardization to interoperate with other operating systems.

Defaulting to Kerberos

NT LAN Manager is the authentication protocol used in Windows NT and in Windows 2000 work group environments. It is also employed in mixed Windows 2000 Active Directory domain environments that must authenticate Windows NT systems. At the stage Windows 2000 is converted to native mode where no down-level Windows NT domain controllers exist, NT LAN Manager is disabled. Kerberos then becomes the default authentication technology for the enterprise.

Understanding Kerberos concepts

Kerberos Version 5 is standard on all versions of Windows 2000 and ensures the highest level of security to network resources. The Kerberos protocol name is based on the three-headed dog figure from Greek mythology known as Kerberos. The three heads of Kerberos comprise the Key Distribution Center (KDC), the client user and the server with the desired service to access. The KDC is installed as part of the domain controller and performs two service functions: the Authentication Service (AS) and the Ticket-Granting Service (TGS). As exemplified in Figure 1, three exchanges are involved when the client initially accesses a server resource:

1. AS Exchange
2. TGS Exchange
3. Client/Server (CS) Exchange

Kerberos Explained

By Mark Walla

Article from the May 2000 issue of Windows 2000 Advantage Magazine

Error! Bookmark not defined.

KERBEROS TICKET EXCHANGE

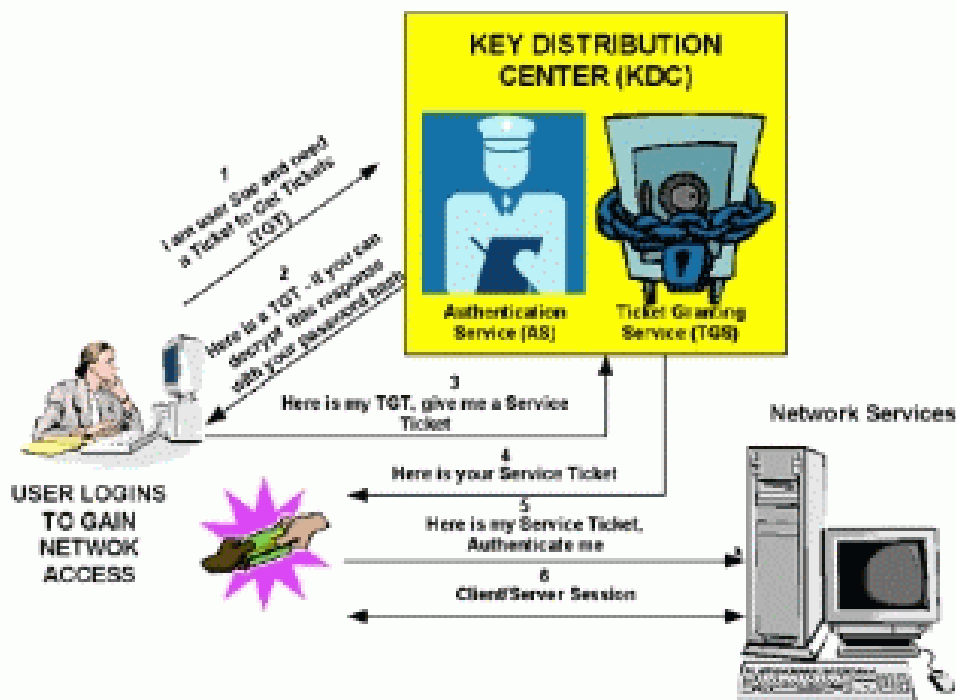


Figure 1:

Let's take a closer look at this exchange process and its component parts.

AS Exchange

When initially logging on to a network, users must negotiate access by providing a log-in name and password in order to be verified by the AS portion of a KDC within their domain. The KDC has access to Active Directory user account information. Once successfully authenticated, the user is granted a Ticket to Get Tickets (TGT) that is valid for the local domain. The TGT has a default lifetime of 10 hours and may be renewed throughout the user's log-on session without requiring the user to re-enter his password. The TGT is cached on the local machine in volatile memory space and used to request sessions with services throughout the network. The following is a discussion of the TGT retrieval process.

Example AS Administration

The AS request identifies the client to the KDC in plain text. If preauthentication is enabled, a time stamp will be encrypted using the user's password hash as an encryption key. If the KDC reads a valid time when using the user's password hash (stored in the Active Directory) to decrypt the time stamp, the KDC knows that request isn't a replay of a previous request. The preauthentication feature may be disabled for specific users in order to support some applications that don't support the security

Kerberos Explained

By Mark Walla

Article from the May 2000 issue of *Windows 2000 Advantage Magazine*

feature. Access the user account from the Active Directory users and the computers will snap-in and select the account tab. From the account options: slide window, check mark the "Do not require Kerberos" preauthentication option (Figure 2).

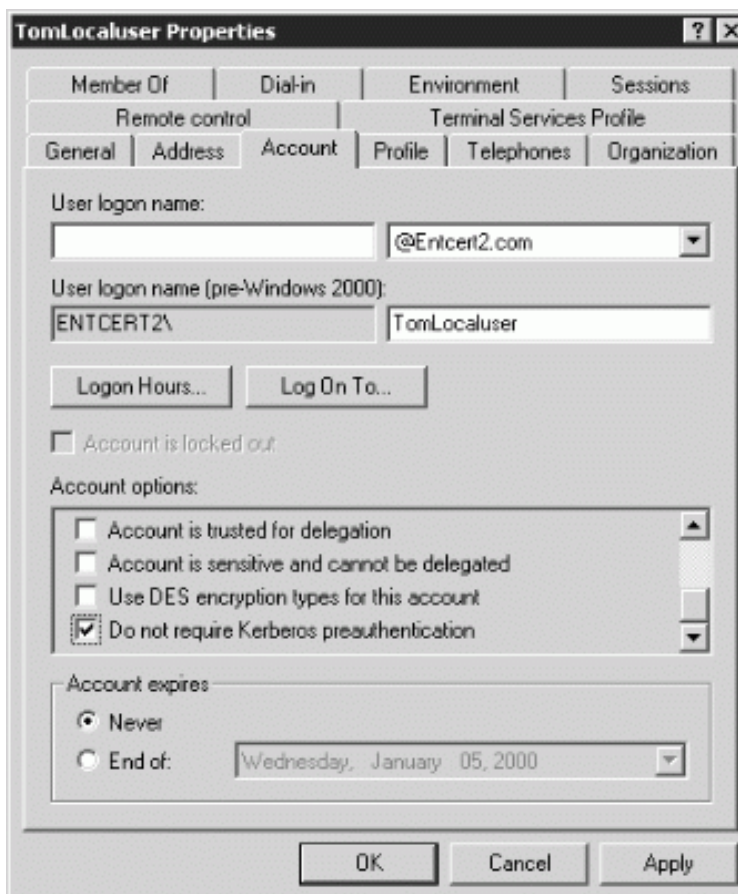


Figure 2: Disable Kerberos Preauthentication

If the KDC approves the client's request for a TGT, the reply (referred to as the AS reply) will include two sections: a TGT encrypted with a key that only the KDC (TGS) can decrypt and a session key encrypted with the user's password hash to handle future communications with the KDC. Because the client system cannot read the TGT contents, it must blindly present the ticket to the TGS for service tickets. The TGT includes time to live parameters, authorization data, a session key to use when communicating with the client and the client's name.

TGS Exchange

The user presents the TGT to the TGS portion of the KDC when desiring access to a server service. The TGS on the KDC authenticates the user's TGT and creates a ticket and session key for both the client and the remote server. This information, known as the service ticket, is then cached locally on the client machine.

Kerberos Explained

By Mark Walla

Article from the May 2000 issue of *Windows 2000 Advantage Magazine*

The TGS receives the client's TGT and reads it using its own key. If the TGS approves of the client's request, a service ticket is generated for both the client and the target server. The client reads its portion using the TGS session key retrieved earlier from the AS reply. The client presents the server portion of the TGS reply to the target server in the client/server exchange coming next.

Client/Server Exchange

Once the client user has the client/server service ticket, he can establish the session with the server service. The server can decrypt the information coming indirectly from the TGS using its own long-term key with the KDC. The service ticket is then used to authenticate the client user and establish a service session between the server and client. After the ticket's lifetime is exceeded, the service ticket must be renewed to use the service.

Client/Server Exchange Detail

The client blindly passes the server portion of the service ticket to the server in the client/server request to establish a client/server session. If mutual authentication is enabled, the target server returns a time stamp encrypted using the service ticket session key. If the time stamp decrypts correctly, not only has the client authenticated himself to the server, but the server also has authenticated itself to the client. The target server never has to directly communicate with the KDC. This reduces downtime and pressure on the KDC.

Further Clarification of the Log-in Process

A TGT and a service ticket are needed to access services on remote computers, but they are also required to successfully log on to a local system. When the log-on window appears, password encryption using a one-way hash algorithm occurs immediately and negotiations commence with the KDC for a valid TGT and service ticket. The process is the same as accessing a remote service. An access token is created for the user containing all security groups to which they belong. This access token is attached to the user's log-on session and is subsequently inherited by any process or application the user starts.

Referral Tickets

The AS and TGS functions are separate within the KDC. This permits the user to use the TGT obtained from an AS in his domain to obtain service tickets from a TGS in other domains. This is accomplished through referral tickets.

Once a trust has been established between two domains, referral tickets can be granted to clients requesting authorization for services in other domains. When there is a trust established between the two domains, an interdomain key based on the trust password becomes available for authenticating KDC functions. This can best be explained by example of a user/client seeking services in another domain. As illustrated in Figure 3, a user client in Entcert1.com requests authority for a server in Entcert2.com. He utilizes referral tickets. The numbers in Figure 3 correspond to the following numbered explanations:

Kerberos Explained

By Mark Walla

Article from the May 2000 issue of Windows 2000 Advantage Magazine

1. The client contacts its domain KDC TGS using a TGT. The KDC recognizes a request for a session with a foreign domain server and responds by returning a referral ticket for the KDC in the foreign domain.
2. The client contacts the KDC of the foreign domain with the referral ticket. This ticket is encrypted with the interdomain key. Given that the decryption works, the TGS service for the foreign domain returns a service ticket for the server service in Entcert2.com.
3. The client performs the client/server exchange with the server and begins the user session with the service.

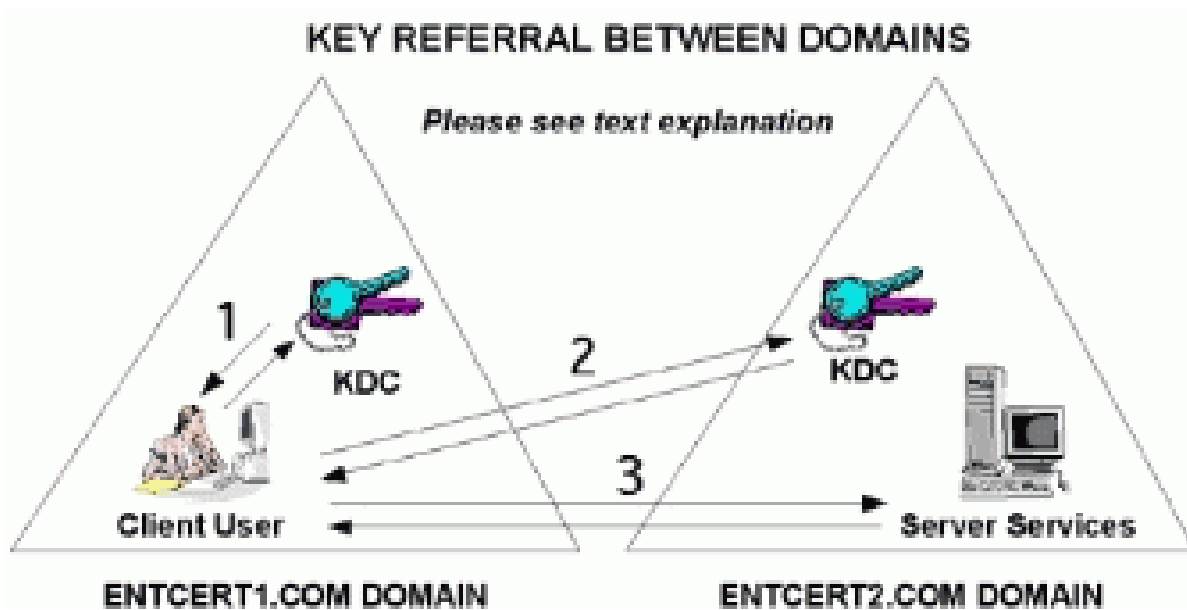


Figure 3: Domain Referrals

When more domains are involved, the referral process extends and involves the transitive properties between Windows 2000 domains. Maintaining individual two-way trusts between all domains creates a complex administrative nightmare. The use of Kerberos transitive domains cuts down on interdomain administration. This can best be explained by example of a user/client seeking services in another domain. As illustrated in Figure 11-4, Entcert1.com has a trust relationship with Entcert2.com. Entcert2.com has a trust relationship with Entcert3.com. There is no trust between Entcert1.com and Entcert3.com. A client from Entcert1.com accessing a service on a server in Entcert3.com would obtain a service ticket through the following steps (the numbers appearing in Figure 4 correspond to the following numbered explanations):

1. Use the TGS service in Entcert1.com to obtain a referral ticket for a KDC in Entcert2.com.
2. Use the referral ticket with the TGS service on the KDC in Entcert2.com and obtain a referral for Entcert3.com.

Kerberos Explained

By Mark Walla

Article from the May 2000 issue of *Windows 2000 Advantage Magazine*

3. Use the second referral ticket with the TGS service on the KDC for Entcert3.com and obtain a service ticket for the server in Entcert3.com.
4. Use the Client/Server Exchange to open a session with the service in Entcert3.com.

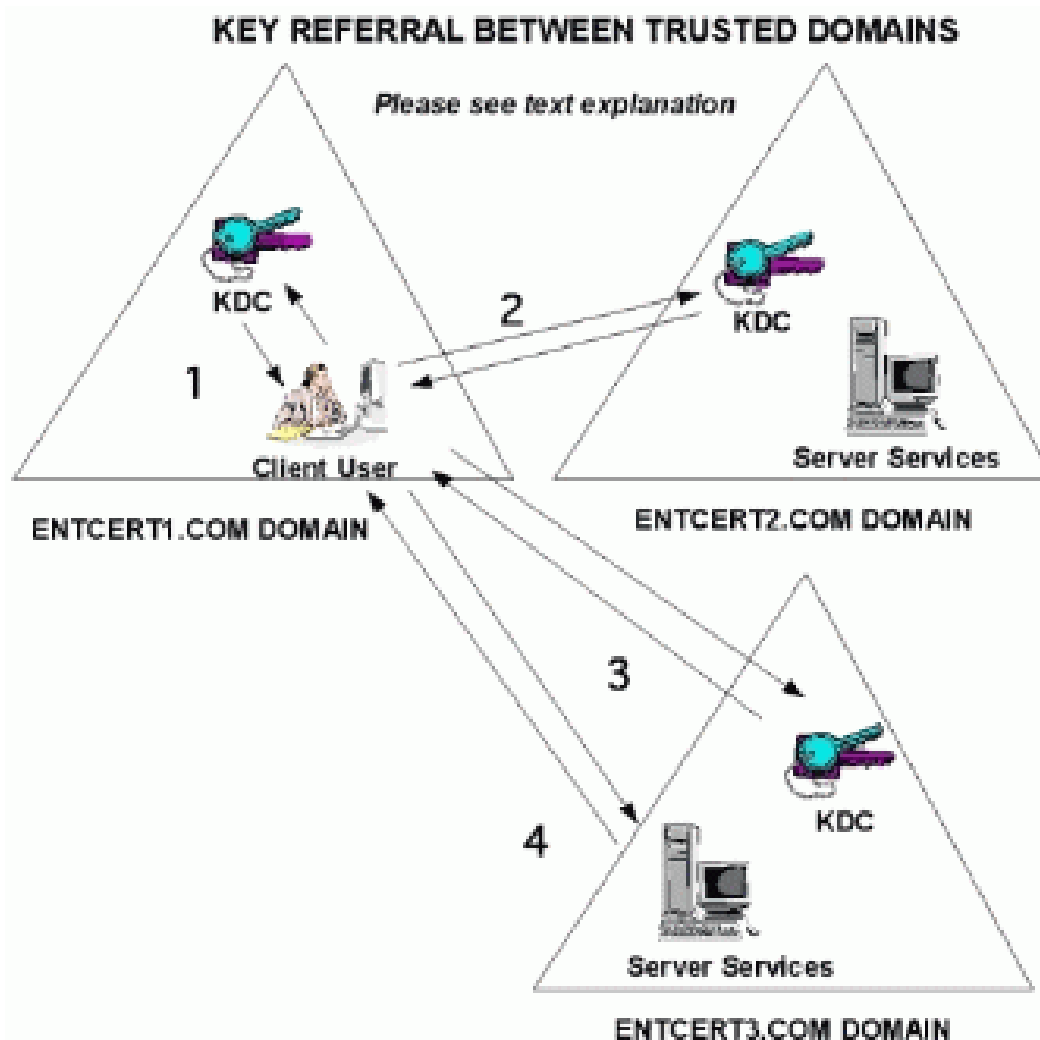


Figure 4: Transitive Domain Trusts

Delegation with Forwarding and Proxy

Some server services require access to a second server, such as a back-end database. In order to establish a session with the second server, the primary server must be authenticated on behalf of the client's user account and authority level. This is common in a three-tier client/server model. This activity is commonly accomplished with proxy or forwarding authentication.

Kerberos Explained

By Mark Walla

Article from the May 2000 issue of *Windows 2000 Advantage Magazine*

Postscript

The authentication process implemented by Kerberos is highly effective, but a few hundred words cannot do the subject justice. That is why I recommend that this article be used as a primer and that you seek more in-depth technical white papers, books or consulting services prior to actual implementation. Once you understand Kerberos and how it can serve both a pure Windows 2000 and mixed operating environment then your investment should pay high dividends.