Unidad 6

SEGURIDAD EN SISTEMAS DE MULTIPLES USUARIOS- CONTROL DE ACCESO

Todo sistema debería tener algún tipo de seguridad. Como mínimo, debería utilizar seguridad de las contraseñas de forma que puede controlar y auditar el acceso a su sistema.

Además de esto, puede adoptar uno de los siguientes enfoques básicos de seguridad.

Restrictivo: Algunas personas llaman a esto esquema de seguridad necesario-saber. En un entorno de seguridad restrictivo, se da a las personas únicamente acceso a la Información y las funciones que necesitan para hacer su trabajo. Todo lo demás queda excluido. Muchos auditores recomiendan este enfoque.

No restrictivo: En un entorno de seguridad no restrictiva, los usuarios del sistema autorizados tienen permitido el acceso libre a la mayoría de los recursos del sistema. El acceso queda restringido en el caso de recursos específicamente críticos o confidenciales.

Este enfoque es común en los sistemas utilizados por un único departamento o una pequeña compañía.

Se debe decidir qué tipo de seguridad pretende utilizar. El enfoque de seguridad de un sistema debería estar de acuerdo con la política general para acceder a la información de toda la organización.

Niveles de Seguridad

El nivel de seguridad del sistema le permite controlar "cuánta" seguridad espera para su sistema. Para comprender cómo trabajan los cinco diferentes niveles de seguridad, imagine que su sistema es un edificio. Donde la gente trata de entrar:

Nivel 0: Sin seguridad alguna o con seguridad de acceso físico sobre los recursos (*Seguridad Física*). Se utilizan puertas, llaves, rejas, etc., para impedir que un usuario no autorizado acceda al sistema. La gente que posea llave del edificio ingresa en el mismo.

Nivel 10: *Seguridad en Inicio de Sesión*: Con el nivel 10, no tiene realmente seguridad. Tiene un guardia en la puerta pidiendo a la gente que firme, pero el guardia no pide ninguna identificación. La gente puede utilizar nombres diferentes cada día, si lo desean. Usted no tiene idea de quién esta en el edificio ni qué están haciendo.

Nivel 20: *Seguridad de la Contraseña*: Si selecciona el nivel 20, tiene alguna protección de seguridad. El guardia de la puerta del edificio pide la identificación y la contraseña secreta. Sólo quien tenga ambas es admitido en el edificio. Pero una vez dentro, pueden hacer lo que quieran, si alguien oye una contraseña secreta y la utiliza para pasar ante el guardia de la puerta, usted no tiene protección.

Nivel 30: *Seguridad de la Contraseña y de los Recursos*: El nivel 30 le da todo lo que tenía en el nivel 20, y además puede controlar quién va a ciertas partes del edificio y qué hacen cuando están allí. Puede definir algunas zonas del edificio como públicas, mientras que otras quedan restringidas con guardias en las puertas.

Puede de permitir a aquellos que tienen acceso a las secciones restringidas que hagan lo que quieran, o puede pedir que hagan sus solicitudes de información a los empleados autorizados (programas). Un intruso que entre utilizando la contraseña de algún otro, podría todavía tener que obtener el pase del guardia del interior para acceder a las secciones protegidas.

Niveles 40 y 50: *Protección de la Integridad*: En los niveles 40 y 50, los guardias de las puertas dentro del edificio utilizan un estricto juego de reglas. En el nivel 30, una persona con conocimientos especiales (un programador experimentado) podría ser capaz de pasar las puertas restringidas. El guardia escribe una nota para el responsable de seguridad pero deja entrar a la persona. En los niveles 40 y 50, el guardia anota una entrada en el libro de seguridad y rehúsa la admisión.

El nivel de seguridad 50 se define para sistemas con requisitos de seguridad muy estrictos. En el nivel 50, dispone de un conjunto de reglas aún más estricto para evitar que una persona con conocimientos especiales pueda pasar las puertas restringidas.

Recomendaciones: El nivel 40 de seguridad es la mejor elección para la mayoría de las instalaciones, tanto si su política de seguridad es restrictiva o no. Si su enfoque no es restrictivo, puede establecer acceso público a la mayoría de los recursos de su sistema. Utilizando el nivel 40 de seguridad desde el principio, tiene la flexibilidad de hacer su sistema más seguro en el futuro sin hacer muchos cambios.

Debería comprobar con cada desarrollador de software, para estar seguro, de que los programas han sido probados al nivel 40. Algunas aplicaciones utilizan operaciones que causan error en un nivel de seguridad alto (40 ó 50).

El nivel de seguridad 50 se diseña para evitar sucesos que no ocurren normalmente en la mayoría de sistemas. El sistema hace comprobaciones adicionales siempre que los programas se ejecutan en el sistema. Esta comprobación adicional puede tener un efecto negativo sobre el rendimiento.

Microsoft proyecto la arquitectura de Win 9x sacrificando la seguridad a favor de la facilidad de uso. Esto constituye un riesgo doble, por un lado para los administradores y por otro para los usuarios finales que no se toman en serio el tema de la seguridad.

Además un usuario final podría estar proporcionando una puerta trasera en la LAN de su empresa y con la creciente adopción del cable y del ADSL de alta velocidad, que permiten una conexión total a Internet este problema empeora.

Afortunadamente la simplicidad de win 9x favorece los temas de seguridad, debido a que no fue diseñado para ser un sistema multiusuario, posee funciones de administración remota muy limitadas.

Hay que tener en cuenta que existen dos niveles de seguridad:

User-level: a nivel de usuario

Share-level: a nivel de compartición.

Share-level es el comportamiento predeterminado de Win 9x, es decir que este no puede funcionar como un servidor de autenticación a nivel de usuario.

Un atacante solo tiene dos formas de adueñarse de un sistema win 9x:

Engañar al operador del sistema ejecutando un código de su elección.
Conseguir acceso físico a la consola del sistema.

Las técnicas de explotación remota para win 9x se pueden dividir en cuatro categorías.

Conexión compartida a recursos compartidos.
Instalación de demonios de puerta trasera.
Explotación de las vulnerabilidades conocidas de las aplicaciones del servidor.
Negación de servicio.

Conexión directa a recursos compartidos.

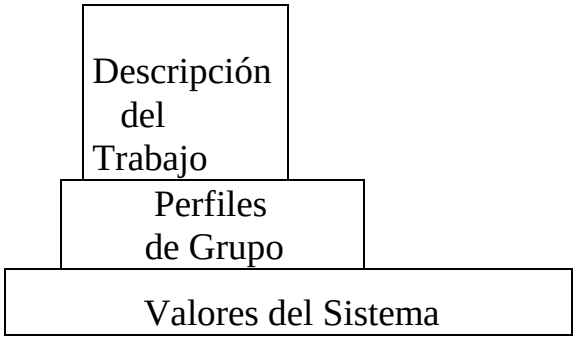
Win 9x proporciona tres mecanismos para el acceso directo al sistema:

Compartición de archivos e impresoras.
El servidor de acceso telefónico a redes.
Manipulación remota del registro.

Contramedida : se debe desactivar la compartición de archivos e impresoras. Si se tiene un gran número de sistemas, es conveniente usar ***POLEDIT.EXE*** que viene con Windows 9x. Si se necesita compartir archivos e impresoras asignar una contraseña compleja de ocho caracteres alfanuméricos y también meta caracteres. También es aconsejable añadir el símbolo $ para evitar que aparezca en el entorno de red.

Planificación de los grupos de Usuarios

El primer paso del proceso de planificación, el decidir su enfoque global, es como establecer la política de la compañía. Ahora está preparado para planificar los grupos de usuarios que es como decidir la política de departamento.



Descripción de las aplicaciones
Seguridad Física

¿Qué es un Grupo de Usuarios?

Un grupo de usuarios es exactamente lo que su nombre indica: un grupo de personas que necesitan utilizar las mismas aplicaciones de la misma forma. Típicamente, un grupo de usuarios se compone de personas que trabajan en el mismo departamento y tienen responsabilidades de trabajo similares. Se define un grupo de usuarios creando un perfil de grupo.

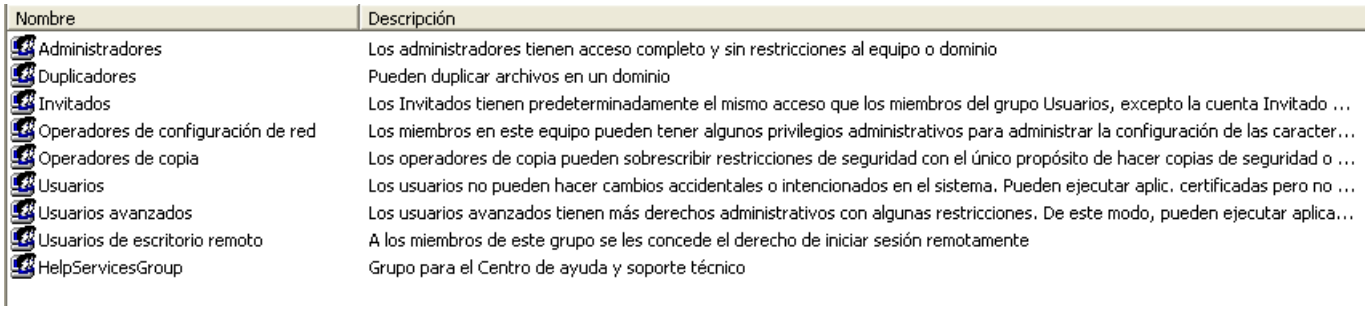
¿Qué Hace un Perfil de Grupo?: Un perfil de grupo es un tipo especial de perfil de usuario. Tiene dos propósitos en el sistema:

Un perfil de usuario proporciona un camino fácil para organizar quién puede utilizar ciertos recursos en su sistema (autorización de objetos). Usted puede definir autorización de objetos para un grupo completo mejor que para algún miembro individual del grupo.

Se puede utilizar un perfil de grupo como patrón para crear los perfiles de usuario individuales. La mayoría de personas que forman parte del mismo grupo tienen las mismas necesidades de adaptación, como el menú inicial y la impresora por omisión. Puede definirlos en el perfil de grupo y copiarlos en los perfiles individuales de usuario..

Los perfiles de grupo le facilitan el mantenimiento de un esquema simple y consistente tanto para la seguridad como para la adaptación.

Ejm. Grupos de Usuarios en Windows XP Profesional SP2



Nombre	Descripción
Administradores	Los administradores tienen acceso completo y sin restricciones al equipo o dominio
Duplicadores	Pueden duplicar archivos en un dominio
Invitados	Los Invitados tienen predeterminadamente el mismo acceso que los miembros del grupo Usuarios, excepto la cuenta Invitado ...
Operadores de configuración de red	Los miembros en este equipo pueden tener algunos privilegios administrativos para administrar la configuración de las caracter...
Operadores de copia	Los operadores de copia pueden sobrescribir restricciones de seguridad con el único propósito de hacer copias de seguridad o ...
Usuarios	Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema. Pueden ejecutar aplic. certificadas pero no ...
Usuarios avanzados	Los usuarios avanzados tienen más derechos administrativos con algunas restricciones. De este modo, pueden ejecutar aplica...
Usuarios de escritorio remoto	A los miembros de este grupo se les concede el derecho de iniciar sesión remotamente
HelpServicesGroup	Grupo para el Centro de ayuda y soporte técnico

Ejemplo Clases de Usuarios en OS400

Hay cinco clases de usuario que son jerárquicos en autorización:

QSECOFR Oficial de seguridad
SECADM Administrador de seguridad
PGMR Programador
SYSQPR Operador del sistema
USER Usuario final

AUTORIZACIONES ESPECIALES

Hay privilegios de usuario especiales para determinadas funciones de seguridad y de administración del sistema. Hay seis:

ALLOBJ Permite accesos ilimitados a todo

SECADM Permite la administración de perfiles de usuario

SAVSYS Salvar y restaurar tareas del sistema

JOBCTL Permite manipular colas de trabajo y subsistemas

SPLCTL Permite controlar las funciones de spool

SERVICE Un caso especial que permite funciones de servicio

ACCESO A ARCHIVOS FÍSICOS

Las autorizaciones sobre los archivos físicos se otorgan con el comando GRTOBJAUT y puede dar los siguientes derechos:

USE Puede leer, pero no escribir, vaciar o borrar.

CHANGE Puede leer y escribir, pero no vaciar ni borrar.

ALL Puede leer, escribir, vaciar y borrar.

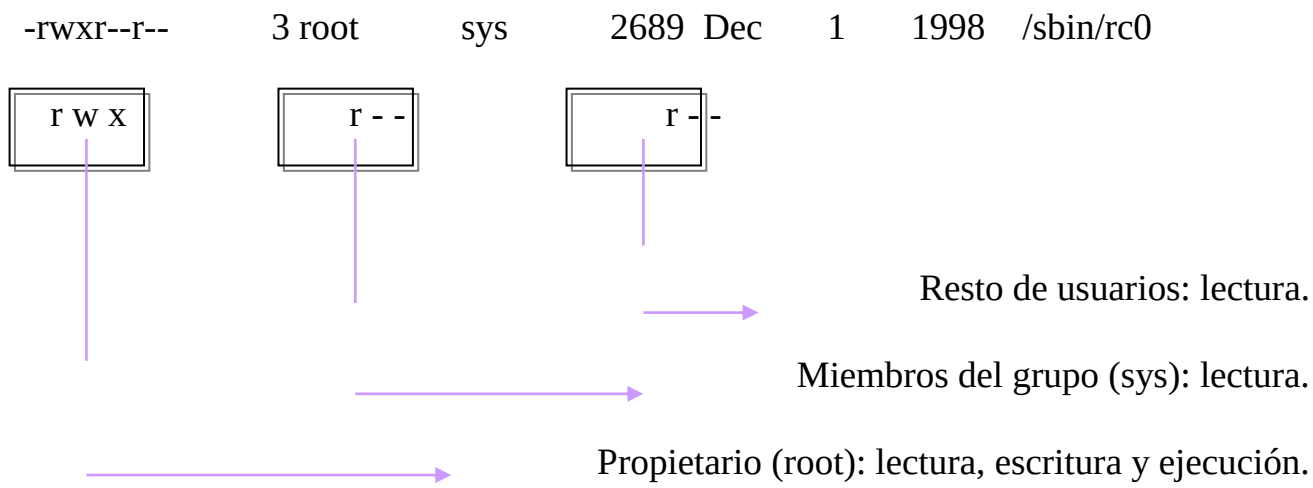
AUTORIZACIONES DE OBJETOS

El propietario de un objeto es el usuario que lo crea y las autorizaciones sobre él debe darlas el usuario o el oficial de seguridad explícitamente a aquellos que lo necesiten.

LISTAS DE AUTORIZACIONES

Un objeto sólo puede tener una lista de autorizaciones asociada, pero una lista puede englobar a varios objetos y un usuario puede aparcar en muchas listas distintas.

Ejemplos. Permisos en archivos UNIX (LINUX)



En este caso vemos que el archivo listado es un fichero plano (el primer carácter es un `-') y sus permisos son `rwxr--r--'. ¿Cómo interpretar estos caracteres? Los permisos se dividen en tres ternas en función de a qué usuarios afectan; cada una de ellas indica la existencia o la ausencia de permiso para leer, escribir o ejecutar el fichero: una r indica un permiso de lectura, una w de escritura, una x de ejecución y un `-' indica que el permiso correspondiente no está activado. Así, si en una de las ternas tenemos los caracteres rwx, el usuario o usuarios afectados por esa terna tiene o tienen permisos para realizar cualquier operación sobre el fichero. ¿De qué usuarios se trata en cada caso? La primera terna afecta al propietario del fichero (root –administrador de UNIX), la segunda al grupo del propietario cuando lo creó

(sys) (recordemos un mismo usuario puede pertenecer a varios grupos) y la tercera al resto de usuarios.

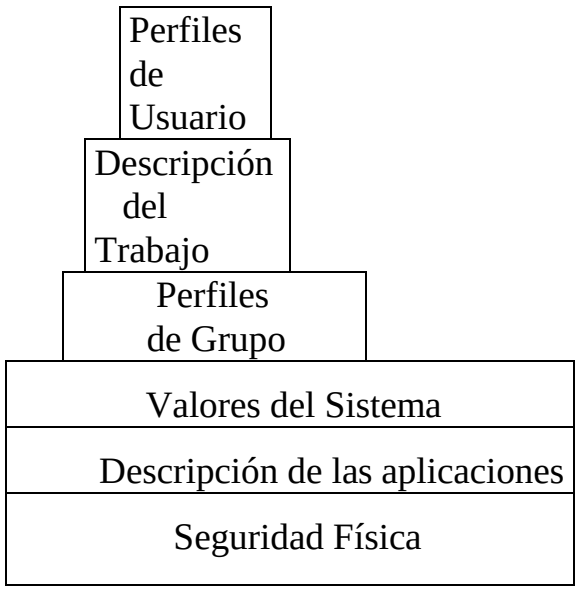
PERFILES DE GRUPO

Un perfil de usuario puede enlazarse a un perfil de grupo. Un usuario puede pertenecer a un único grupo o puede ser parte de ninguno. Los perfiles de grupo se utilizan para organizar a los usuarios según sus funciones de trabajo y para simplificar la asignación y administración de autorizaciones de objetos.

Planificación de los Perfiles individuales de Usuario

Ahora que ha decidido su enfoque global y ha diseñado los perfiles de grupo, ya está listo para planificar los perfiles individuales de usuario.

El perfil de usuario es uno de los más potentes y versátiles objetos del sistema. Contiene cosas como la contraseña del usuario y el menú que ve el usuario después de conectarse. El perfil de usuario define qué puede o no hacer una persona en el sistema. Determina una sola visión del sistema por el usuario. La planificación de los perfiles de usuario es uno de los trabajos más importantes del responsable de seguridad



La seguridad en la conexión evita que una persona no identificada se conecte al sistema. Para conectarse, el individuo debe entrar una combinación válida de ID del usuario y contraseña.
La seguridad de conexión se activa cuando el nivel de seguridad del sistema es 20, o mayor.

Podemos utilizar tanto los valores del sistema como los perfiles individuales del usuario para asegurarnos que la seguridad de conexión no se viola. Por ejemplo, podemos solicitar que se cambien las contraseñas regularmente. También podemos evitar que se utilicen contraseñas fáciles de adivinar.

Un papel importante de la seguridad, y de la adaptación del sistema, es definir qué es lo que pueden hacer los usuarios. Desde la perspectiva de la seguridad, esto es a menudo una

función de limitación, tal como evitar que cualquier persona vea cierta información. Desde la perspectiva de la adaptación del sistema, ésta es una función de autorización. Un sistema personalizado adecuadamente hace posible que la gente haga bien su trabajo, eliminando tareas e información innecesarias. Algunos métodos para definir qué pueden hacer los usuarios son propios del responsable de seguridad, mientras otros son responsabilidad de los programadores.

Qué están Autorizados a Hacer los Usuarios

Técnicas disponibles:

Limitación de los Usuarios a Unas Pocas Funciones: El perfil del usuario, puede limitar a éste a un programa específico, a un menú específico o a un conjunto de menús, y a unos pocos mandatos del sistema.

Restricción de las Funciones del Sistema: Las funciones del sistema son actividades como salvar y restaurar la información, manejar la salida de impresora, y la preparación de nuevos usuarios del sistema. El perfil de cada usuario especifica qué funciones más comunes del sistema puede realizar el usuario.

Decisión de Quién Puede Utilizar los Archivos y Programas: La seguridad de los recursos facilita la posibilidad de controlar la utilización de cada objeto del sistema. Para cualquier objeto, se puede especificar quién puede utilizarlo y cómo. Por ejemplo, se puede especificar que un usuario pueda ver sólo la información de un archivo; otro usuario pueda cambiar datos de ese archivo; un tercer usuario pueda cambiar el archivo o suprimirlo por completo.

Evitar el Abuso de los Recursos del Sistema: La capacidad de proceso del sistema puede ser tan importante para la empresa como los datos almacenados en él. El responsable de seguridad ayuda a asegurar que los usuarios no hagan un mal uso de los recursos del sistema, ejecutando sus trabajos con más prioridad, imprimiendo sus informes de forma preferente, o utilizando demasiado almacenamiento en disco.

Hay parámetros disponibles en los perfiles individuales del usuario, en las descripciones de trabajo, y en las clases, para controlar la utilización de los recursos del sistema.

KERBEROS

Uno de los principales problemas de seguridad en las redes actuales es que cuando un usuario intenta entrar en uno de los nodos de la red, la información de contraseña se envía sin cifrar. Las aplicaciones que se utilizan normalmente, como telnet o ftp, no cifran la contraseña cuando la envían desde el nodo cliente al sistema servidor para su verificación.

Kerberos es el sisterna de verificación desarrollado como parte del Proyecto Athena del MIT. Kerberos exige una contraseña para cada transacción que se realiza utilizando un servicio de red. Cada usuario y cada servicio de red tienen su propia contraseña, y la única entidad que conoce todas las contraseñas es el Servidor de Verificación de Kerberos (KAS). Las contraseñas siempre se envían por la red en forma cifrada. El servidor de verificación debe ser una máquina físicamente segura)A continuación presentamos un resumen de la terminología

asociada al sistema Kerberos.

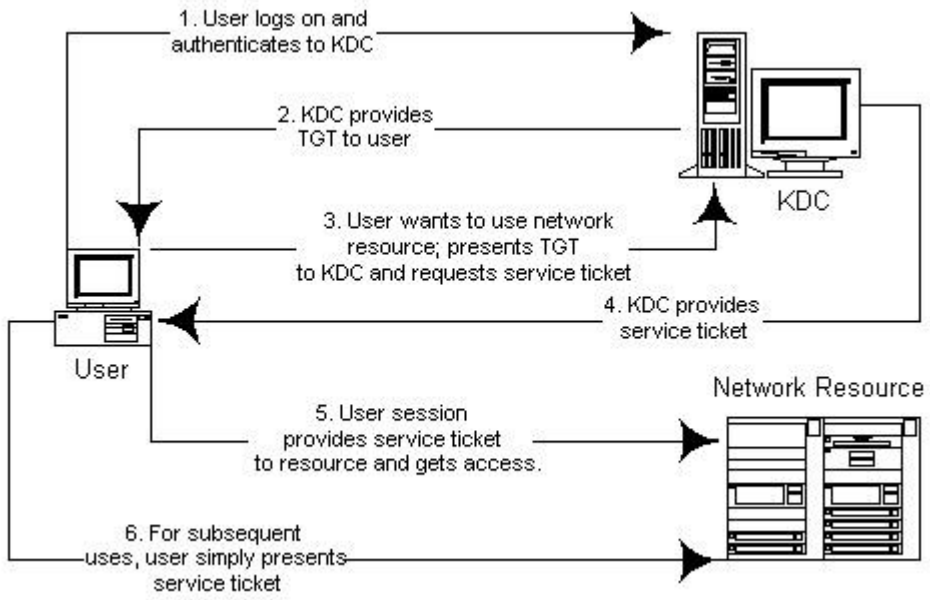
Kerberos Sistema de verificación de usuarios y servicios
TGS El servidor de billetes de permiso es el responsable de conceder billetes a los clientes de la red (usuarios y servicios).
Billete Utilizado por los usuarios para proporcionar sus credenciales. En el entorno Kerberos se utiliza para obtener una clave de sesión. El billete contiene el nombre del servidor, del cliente, la dirección de Internet del sistema cliente, una marca temporal, duración de la sesión y una clave de sesión aleatoria.

Verificador Sistema responsable de la asignación de billetes.

Entre los objetivos de Kerberos están:

- No enviar por la red contraseñas sin cifrar.
- No almacenar en las estaciones de trabajo contraseñas sin cifrar.
- Definir la duración de una sesión verificada. Si la sesión se prolonga más allá de ese intervalo de tiempo definido, el usuario deberá identificarse de nuevo.

La figura describe los pasos involucrados en la verificación que realiza Kerberos.



En un entorno de Kerberos, el usuario introduce su nombre de usuario en respuesta al mensaje login: Antes de que se muestre el mensaje de petición de contraseña, se envía por la red un mensaje al servidor de verificación de Kerberos. El mensaje incluye el nombre de usuario y el nombre de un servidor de Kerberos en particular, conocido como el servidor de billetes de permiso de Kerberos (TGS) [3].

mensaje = {nombreusuario, nombre-TGS}

Este mensaje no se envía cifrado. El KAS busca el nombre del usuario y el del servidor de TGS en la base de datos de Kerberos y obtiene una clave de cifrado unidireccional para cada uno. KAS construye seguidamente una respuesta que envía al programa de entrada al sistema en la estación de trabajo. La respuesta contiene un billete que permite al usuario acceder al TGS solicitado. Los billetes siempre estpan cifrados, y constan de

billete = (nombreusuario, nombre-TGS, dir-lP-WS, clave-sesión-TGS)

La clave de la sesión TGS es un número aleatorio generado por el KAS. El billete contiene también una marca temporal y una fecha de caducidad. El tiempo de v'ida de un billete es generalmente de ocho horas, transcurrido el cual el usuario se deberá identificar de nuevo ante Kerberos, proporcionando de nuevo el nombre de usuario y la contraseña. KAS cifra el billete empleando la clave de cifrado del servidor TGS, produciendo lo que se denomina un billete sellado. Se construye entonces un mensaje, compuesto por el billete sellado y la clave de la sesión de TGS, como sigue:

mensaje = (clave-sesión-TGS, billete sellado)

El mensaje se cifra empleando la contraseña de usuario almacenada en la base de datos de Kerberos. El programa login recibe el mensaje cifrado y después pregunta por la contraseña. La contraseña sin cifrar que se introduce se procesa mediante el algoritmo estándar unidireccional de UNIX y el resultado, denominado clave de cifrado de usuario, se utiliza para descifrar el mensaje recibido (con al sesión de TGS y el billete sellado). La contraseña sin cifrar se borra entonces de la memoria. El software de la estación de trabajo guarda una copia del billete sellado y de la clave de sesión de TGS [3].

Si se solicita posteriormente un servicio de red, como el acceso a un archivo de un servidor de archivos o la impresión de un archivo en una impresora, el sistema que solicita el servicio debe obtener un billete para ese servicio en particular. El sistema que solicita el servicio se denomina servidor final, y para obtener el billete el software de la estación de trabajo contacta con Kerberos.