

# Glossary

## **addressless ticket**

A Kerberos ticket that is not bound to a particular IP address, which can then be passed through a NAT-created “firewall”.

## **AFS**

A distributed file service (formerly known as the Andrew File System). It is installed on many systems at Fermilab, including FNALU. On strengthened systems, it is integrated with Kerberos.

## **authentication**

The process of verifying the claimed identity of a principal.

## **authentication method**

The method used to verify the claimed identity of a principal, e.g., Kerberos V5, CRYPTOCard.

## **authentication service (AS)**

The portion of the KDC that issues tickets and secret session keys based on a user password or encryption key. The AS can issue ticket-granting tickets (TGTs) and other service tickets.

## **authenticator**

A record containing information that can be shown to have been recently generated using the session key known only by the client and service.

## **authorization**

The process of determining whether a client may use a service, which objects the client is allowed to access, and the type of access allowed for each.

## **challenge**

(used with CRYPTOCard as non-reusable authentication; see *CRYPTO-Card*, also see *response*) Every time you log in from an untrusted machine, the KDC generates an eight-digit string called a *challenge*. The CRYPTO-Card encrypts the challenge with the secret key shared by itself and the KDC in order to generate a non-reusable password, called a *response*.

## **client**

An entity that can obtain a ticket. This entity is usually either a user or a host principal.

## **credential**

A ticket (usually a TGT) plus the secret session key needed to successfully use that ticket in an authentication exchange. Obtaining credentials from the KDC is tantamount to being authenticated on a strengthened machine.

### **credential cache**

Kerberos tickets are stored in a credential cache. The credential cache can be a file with restricted rights, or it can be a persistent memory location.

### **cross-authentication**

This concerns trust relations between two strengthened realms (see *trust relations*). Cross-authentication implies the freedom to access systems in either realm if authentication has been established in one of them and authorization has been established in the other (e.g., via `.k5login`).

### **CRYPTOCard**

An authentication technology that provides tokens via calculator-style one-time-password DES cards. At Fermilab, CRYPTOCards are issued upon demand to users who require access to the FNAL.GOV realm from untrusted machines. The cards are synchronized with the KDC prior to issue. (See *portal mode*; see also *challenge* and *response*)

### **ftp**

`ftp` is a program to transfer files to and from a remote host.

### **host**

A computer that can be accessed over a network.

### **KDC (Key Distribution Center)**

The service which implements Kerberos authentication via the Authentication Service (AS) and the Ticket Granting Service (TGS). The KDC has a copy of every encryption key associated with every principal. Most KDC implementations store the principals in a database, so you may hear the term *Kerberos database* applied to the KDC.

### **kdestroy**

The `kdestroy` utility destroys the user's active Kerberos credentials (tickets) by writing zeros to the specified credentials cache that contains them, and then deleting the cache.

### **Kerberized application**

A software application that requires or performs Kerberos authentication.

### **Kerberized machine**

A machine on which the Kerberos product has been installed and which requires Kerberos V5 authentication for access.

### **Kerberized ssh client**

An ssh client application that requires or performs Kerberos V5 authentication, and which does not implement RSA keys, IP addresses + "privileged ports", or other non-Kerberos authentication.

### **Kerberos**

In Greek mythology, the three-headed dog that guards the entrance to the underworld. In the computing world, Kerberos is a network security package that was developed at MIT.

### **Kerberos client**

Any entity that gets a service ticket for a Kerberos service. A client is typically a user, but any principal can be a client.

### **Kerberos password**

A password used to obtain authentication on a Kerberized system.

### **Kerberos server**

This generally refers to the Key Distribution Center (KDC).

### **key**

A string used to encrypt tickets and other data.

### **keytab file**

A keytab file is used by a service host to store keys.

### **kinit**

**kinit** obtains and caches a ticket (a ticket-granting ticket, by default) for the default principal or for a specified principal.

### **klist**

**klist** lists the Kerberos principal and Kerberos tickets held in a credentials cache (the default), or lists the keys held in a keytab file.

### **kpasswd**

**klist** is used to change your Kerberos password (a second command of the same name, different path, is used to change your AFS password).

### **ksu**

The Kerberos V5 **ksu** program is a Kerberized version of the **su** program that has two missions: one is to securely change the real and effective user ID to that of the target user, the other is to create a new security context.

### **kvno**

The **kvno** command acquires a service ticket for the specified Kerberos principals and prints out the key version numbers of each.

### **Openssh**

OpenSSH is a FREE version of the SSH connectivity tools. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other attacks. Additionally, OpenSSH provides secure tunneling capabilities and several authentication methods, and supports all SSH protocol versions.<sup>1</sup>

### **permanent secret key**

See *secret key*.

---

1. Adapted from description at <http://www.openssh.com/>.

## **portal**

A secure gateway between the untrusted and strengthened realms that requires non-reusable passwords. At Fermilab, any Kerberized host may be configured to respond in *portal mode* to requests for access from untrusted machines (see *portal mode*).

## **portal mode**

(See *portal*.) When a request for access comes from an untrusted machine, Kerberized hosts at Fermilab respond in *portal mode* and thus require entry of a non-reusable password for authentication.

## **preauthentication**

This is the stage of authentication in which you prove to the KDC that you know the shared secret key (which is a function of your password) before the KDC delivers a ticket to decrypt with the key.

## **principal**

A uniquely named client or server instance that participates in a network communication. It is essentially a string that names a specific entity to which a set of credentials may be assigned. For a user, it can be thought of as a realm userid. It has three parts and is of the form `primary/instance@REALM`. For a user, the instance portion is generally null, and the principal is of the form `primary@REALM`. The parts are defined as:

### **primary**

The first part of a Kerberos principal. In the case of a user, it is the userid. In the case of a service, it is the name of the service.

### **instance**

The second part of a Kerberos principal, preceded by a slash (/). It gives information that qualifies the primary. The instance may be null. In the case of a user, the instance is often used to describe the intended use of the corresponding credentials. In the case of a host, the instance is the fully qualified hostname.

### **realm**

The logical network served by a single Kerberos database and a set of Key Distribution Centers. By convention, realm names are generally all upper-case letters, to differentiate the realm from the internet domain.

## **rcp**

**rcp** copies files between machines.

## **response**

(used with CRYPTOCard as non-reusable authentication; see *CRYPTOCard*, also see *challenge*) A response is a single-use eight-digit hex password generated by a CRYPTOCard as a result of encrypting a challenge.

## **rlogin**

**rlogin** connects your terminal on the current local host system to the remote host system, as specified.

### **rsh**

**rsh** connects to the specified host, and executes the specified command.

### **scp**

**scp** copies files between hosts on a network. It uses **ssh** for data transfer, and uses the same authentication and provides the same security as **ssh**.

### **secret key**

A long-term (permanent) encryption key shared by a principal and the KDC, used to encrypt/decrypt the session key included with the TGT on the initial authentication. In the case of a human user's principal, the secret key is derived from the user's Kerberos password.

### **server**

A particular principal which provides a resource to network clients.

### **service**

Any program or computer you access over a network.

### **session key**

A temporary encryption key used between two principals, with a lifetime limited to the duration of an accompanying ticket.

### **slogin**

**slogin** is the "login" part of **ssh**; if the <command> argument is left off, **ssh** runs **slogin**.

### **ssh**

**ssh** (SSH client) is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to replace **rlogin** and **rsh**, and provide secure encrypted communications between two untrusted hosts over an insecure network. Also see Openssh.

### **strengthened application**

A software application that requires Kerberos authentication for use.

### **strengthened machine**

A machine on which the Kerberos (or other authentication service) product has been installed and which requires strong authentication.

### **strengthened realm**

The set of all systems (whether on- or off-site) that require strong authentication for access from the network.

### **strong authentication**

A system of verifying workstation user and network server identities on an unprotected network that eliminates the transmission of reusable passwords over the network and their storage on local systems. Typically the authentication is done via a trusted third-party authentication service using conventional cryptography.

**telnet**

A program used to communicate with another host using the TELNET protocol.

**ticket**

A set of electronic credentials that verifies the identity of a client for a particular service.

**TGS (Ticket-Granting Service)**

The portion of the KDC that issues tickets to clients for specific services. The user process communicates with the TGS via a ticket-granting ticket (TGT).

**TGT (Ticket-Granting Ticket)**

A special Kerberos ticket that permits the client to obtain additional Kerberos tickets transparently.

**transport**

The program/protocol used to make a network connection and transport commands, data, etc. across the network. A transport program must implement an authentication method.

**trusted realm**

Sites which implement strong authentication, and which meet certain criteria, may be recognized as “trusted” realms. Trusted realms provide levels of security and authentication equivalent to our own.

**trust relations**

This refers to relations between two strengthened realms. Trust relations imply the freedom to access systems in either realm if authentication has been established in one of them (see *cross-authentication*).

**untrusted realm**

The set of all systems that do not require strong authentication, but which permit traditional means of access.

**XDMCP**

(X Display Manager Control Protocol) provides a mechanism for an X terminal to request a session from a remote host.

