What is a principal name?

A Kerberos *principal* is a unique identity to which Kerberos can assign tickets. Principals can have an arbitrary number of components. Each component is separated by a component separator, generally `/'. The last component is the realm, separated from the rest of the principal by the realm separator, generally `@'. If there is no realm component in the principal, then it will be assumed that the principal is in the default realm for the context in which it is being used.
Traditionally, a principal is divided into three parts: the *primary*, the *instance*, and the *realm*. The format of a typical Kerberos V5 principal is `primary/instance@REALM`.

- The *primary* is the first part of the principal. In the case of a user, it's the same as your username. For a host, the primary is the word `host`.
- The *instance* is an optional string that qualifies the primary. The instance is separated from the primary by a slash (`/`). In the case of a user, the instance is usually null, but a user might also have an additional principal, with an instance called admin, which he/she uses to administrate a database. The principal `jennifer@ATHENA.MIT.EDU` is completely separate from the principal `jennifer/admin@ATHENA.MIT.EDU`, with a separate password, and separate permissions. In the case of a host, the instance is the fully qualified hostname, e.g., `daffodil.mit.edu`.

The *realm* is your Kerberos realm. In most cases, your Kerberos realm is your domain name, in upper-case letters. For example, the machine `daffodil.example.com` would be in the realm `EXAMPLE.COM`.

What is a Kerberos ticket?

Your Kerberos *credentials*, or "*tickets*", are a set of electronic information that can be used to verify your identity. Your Kerberos tickets may be stored in a file, or they may exist only in memory.
The first ticket you obtain is a *ticket-granting ticket*, which permits you

to obtain additional tickets. These additional tickets give you permission for specific services. The requesting and granting of these additional tickets happens transparently.

A good analogy for the ticket-granting ticket is a three-day ski pass that is good at four different resorts. You show the pass at whichever resort you decide to go to (until it expires), and you receive a lift ticket for that resort. Once you have the lift ticket, you can ski all you want at that resort. If you go to another resort the next day, you once again show your pass, and you get an additional lift ticket for the new resort. The difference is that the Kerberos V5 programs notice that you have the weekend ski pass, and get the lift ticket for you, so you don't have to perform the transactions yourself.