

What's the difference between a Kerberos principal and a Kerberos account, and why is this important?

Q: What's the difference between a Kerberos principal and a Kerberos account, and why is this important?

Answer:

A **Kerberos principal** is a named human user or other participant in the Kerberos protocol. "**Kerberos account**" is the MIT-specific term for a Moira (Athena) account or, more generally, a user's access to the large collection of MIT services that uses Kerberos for authentication (either directly, or indirectly through services like Touchstone). A user might also have multiple Kerberos principals, e.g., a root instance principal is a Kerberos principal that isn't the name of a Moira account.

Why is this important?

Much of the externally-facing documentation about Kerberos describes the core Kerberos protocol and authentication service. An MIT user seeking information related to Moira accounts could become confused by reading externally facing documentation about Kerberos. Similarly, external users seeking information about Kerberos could encounter documentation intended for an internal MIT audience and become confused, or contact the Service Desk.

MIT IT support providers should be aware that external users with no MIT affiliation might ask for support about Kerberos that MIT support providers aren't usually obligated to give. Support providers should direct such external users to resources such as the kerberos@mit.edu mailing list, setting the expectation that those are community help resources with no formal support commitment.

Similarly, users at MIT should be aware that externally-facing resources about Kerberos (even if they're hosted at MIT) won't cover MIT-specific services such as Moira or Touchstone. Externally facing mailing lists like kerberos@mit.edu have hundreds or thousands of subscribers world wide and are usually not appropriate destinations for queries about issues specific to MIT.