

Chapter 2: Fermilab Computing Policy Issues

The full text of the Fermilab Policy on Computing is maintained at <http://computing.fnal.gov/cd/policy/cpolicy.pdf>. In this chapter we summarize the important points as regards Strong Authentication.

2.1 The Strong Authentication Policy in a Nutshell

Computers at Fermilab must be configured such that they require Kerberos V5 authentication for login over the network. Our working definition of *computer*, as regards strong authentication, is: “any machine to which you can log in, and on which you can run arbitrary code”.

Kerberos authentication is currently **not** required for:

- uses which involve only reading public information (e.g., via the web)
- anonymous FTP
- email
- entering information into a web or database form, in most cases

All other network accesses to computers on the Fermilab site must be preceded by Kerberos V5 authentication if the access is comparable to shell or FTP service.

Compliance can be achieved in different ways:

- Run Kerberos authentication locally
- Remain unKerberized, but remove incoming network services
- (not for desktops) Remain unKerberized, but require users to gain access through a computer that either:
 - requires Kerberos authentication, or
 - is isolated from the general network and physically accessible only to individuals carrying a valid Fermilab ID card.

Furthermore, an on-site system may not be configured to accept a reusable login password over the network.

Telnet, ssh, and other connection program daemons must not prompt for or accept a Kerberos password. To log in over the network:

- Authenticate on local desktop machine prior to remote login (and forward tickets if possible)
- From nonKerberized node, authenticate using your CRYPTOCard

Off-site computers participating in Fermilab's strengthened realm must enforce comparably secure access mechanisms, but they are not required to use Kerberos V5.

2.2 Authentication Guidelines for On-site vs. Off-site Machines

First let us distinguish between an authentication method and a transport mechanism as they pertain to on-site versus off-site machines:

- *Authentication methods* serve to identify the user; examples include: Kerberos credentials, CRYPTOCards, passwords, RSA keys, and IP addresses + "privileged ports". For on-site machines, only Kerberos credentials and CRYPTOCards are allowed as authentication methods. For off-site machines, any secure method is acceptable.
- Ssh, telnet, FTP, and so on are the network connection programs, or the *transports*, and none is forbidden per se. The restriction is imposed on the authentication methods, and the transport is restricted only in that it must support an acceptable authentication method.

The following table summarizes Fermilab's policy regarding how strong authentication may be achieved on UNIX machines in the Fermilab strengthened realm depending on whether the machine is on- or off-site:

Authentication Method	Allowed for ON-site System?	Allowed for OFF-site System?
Kerberos V5 strong authentication via kerberos product (Fermi kerberos or from other source)	yes	yes
Kerberos-based authentication via software other than Kerberos (e.g., Kerberos-based ssh)	yes	yes
CRYPTOCard challenge/response authentication	yes	yes
Clear-text reusable passwords entered at system console	yes	yes
Other non-reusable and/or non-clear-text password authentication over the network	no	yes

Authentication Method	Allowed for ON-site System?	Allowed for OFF-site System?
Non-Kerberos strong authentication (e.g., RSA or equivalent authentication) followed by obtaining Kerberos credentials via kinit over encrypted connection	no	no
Standard UNIX security (e.g., rhosts-based authentication)	no	no
Cleartext passwords (Kerberos or otherwise) transmitted over network	no	no

2.3 Transient Machines

Laptop machines brought in by visitors for short periods of time (e.g., a week) do not need to be registered or Kerberized. Visitors may use their host's accounts (with host's permission) at the host's responsibility, although sharing Kerberos passwords is not allowed. Local accounts that allow access only at the console will be permitted for visitors (no NIS accounts). Facilities created primarily for visitors may be granted exemptions from the requirement for Kerberos-validated users.

2.4 Obtaining an Exemption from the Policy

Exemptions from the strong authentication policy are granted on a case-by-case basis. Exemptions will be considered only for cases which involve a large effort for compliance *and* a small risk for noncompliance. If this applies to your situation, see your experiment's or your division's GCSC (General Computer Security Coordinator)¹ to request an exemption; he or she will forward your request to the Fermilab Computer Security Coordinator (FCSC). The duration of any exemption granted is determined on a case-by-case basis.

1. The GCSCs are listed on the CD Security web page <http://computing.fnal.gov/security/>.

2.5 Compliance with Policy

First, a few notes regarding good user practices:

- Fermilab's policy seeks to limit the transmission of users' Kerberos passwords over the network, even over encrypted connections. We therefore urge you to install software on your machine that allows you to authenticate to Kerberos locally, and to forward Kerberos tickets automatically to remote hosts. You are allowed to type your Kerberos password over an **encrypted** link on an emergency basis with the **kinit** or **kpasswd** commands (e.g., when initially changing your password), however as a regular practice, please authenticate locally and forward your credentials.
- Do not disclose your Kerberos password to anybody, and do not ever type it over an unencrypted connection. Try to minimize the number of times per day or per week that you need to type it for any reason.
- In short, following the usage recommendations and installation instructions provided throughout this manual will keep you in compliance with Fermilab's Computing Policy as regards Strong Authentication.

Regarding penalties for noncompliance, we quote from section 1 of the Fermilab Policy on Computing (at <http://www.fnal.gov/cd/main/cpolicy.html>):

“Hosts found to be noncompliant may be barred from obtaining Kerberos tickets from our realm. If the noncompliance is deliberate or extremely careless it may be deemed to constitute blatant disregard for computer security.”