

**NAME**

**keyserv** - server for storing private encryption keys

**SYNOPSIS**

**keyserv** [-d] [-D] [-n] [-p *path*] [-v]

**DEPRECATION NOTICE**

**keyserv** is deprecated and is not available as of FreeBSD 15.0.

**DESCRIPTION**

The **keyserv** utility is a daemon that is used for storing the private encryption keys of each user logged into the system. These encryption keys are used for accessing secure network services such as secure NFS.

Normally, root's key is read from the file */etc/.rootkey* when the daemon is started. This is useful during power-fail reboots when no one is around to type a password.

If a client with no secret key calls **keyserv**, then the key of user *nobody* is used instead as the default key.

The following options are available:

- d**     Disable the use of default keys for *nobody*.
- D**     Run in debugging mode and log all requests to **keyserv**.
- n**     Root's secret key is not read from */etc/.rootkey*. Instead, **keyserv** prompts the user for the password to decrypt root's key stored in the */etc/publickey* database and then stores the decrypted key in */etc/.rootkey* for future use. This option is useful if the */etc/.rootkey* file ever gets out of date or corrupted.
- p path**  
Specify where to search for *libdes.so.3*. Default is */usr/lib*.
- v**     Display status of DES support (enabled/disabled).

**FILES**

*/etc/.rootkey*

*/usr/lib/libdes.so.3*

**SEE ALSO**

keylogin(1), keylogout(1), publickey(5)