```
# time. Be careful however when using both scvs and cvs on the same directory.
# Preferably all cvs traffic should be done with scvs.
#

# TODO:
#
# * Implement better error detection and recovery.
# * Better parsing of the repository (it will not detect strange syntaxes).
# * Better command line option parsing
# * Add more options that are now still environment variables. For example,
#   -S should contain $SSH_DEFAULT_HOST. for example: -S ssh@cvs.n2it.net:22,
#   -S ssh@, -S :22, -S cvs.n2it.net, or -S ssh@:22.
#

#
# Note: there is no way to specify a different port number to cvs. This means
```

```
220 if ($exitcode) { print STDERR "Could not execute CVS command!\n"; }

    # close the tunnel
    #print STDERR "DEBUG: ", ( "$SSH_CMD $ssh_serv -q -x -f"
224 #            . ( ($SSH_PORT) ? " -p $SSH_PORT" : "" )
    #            . " $magicword" );
    # print STDERR "before close\n";
    system ( "$SSH_CMD $ssh_serv -q -x -f"
228             . ( ($SSH_PORT) ? " -p $SSH_PORT" : "" )
                . " $magicword" );

    # print STDERR "right after close\n";
```

C Change Log

D GNU Free Documentation License

References

[1] Anton Berezin, *Chrooted tunnelled read-write CVS server HOWTO*, http://www.prima.eu.org/tobez/cvs-howto.html

[2] Per Cederqvist et al, *The Cederqvist*, http://cvs.home.org/docs/manual/cvs.html

[3] Simson Garfinkel & Gene Spafford, *Practical UNIX & Internel Security*, ISBN 1-56592-148-8