NAME

tor-gencert − Generate certs and keys for Tor directory authorities

SYNOPSIS

tor−gencert [−h|−−help] [−v] [−r|−−reuse] [−−create−identity−key] [−i *id_file*] [−c *cert_file*] [−m *num*] [−a *address*:*port*]

DESCRIPTION

tor−gencert generates certificates and private keys for use by Tor directory authorities running the v3 Tor directory protocol, as used by Tor 0.2.0 and later. If you are not running a directory authority, you don’t need to use tor−gencert.

Every directory authority has a long term authority *identity key* (which is distinct from the identity key it uses as a Tor server); this key should be kept offline in a secure location. It is used to certify shorter−lived *signing keys,* which are kept online and used by the directory authority to sign votes and consensus documents.

After you use this program to generate a signing key and a certificate, copy those files to the keys subdirectory of your Tor process, and send Tor a SIGHUP signal. DO NOT COPY THE IDENTITY KEY.

OPTIONS

−v
Display verbose output.

−h or **−−help**
Display help text and exit.

−r or **−−reuse**
Generate a new certificate, but not a new signing key. This can be used to change the address or lifetime associated with a given key.

−−create−identity−key
Generate a new identity key. You should only use this option the first time you run tor−gencert; in the future, you should use the identity key that’s already there.

−i *FILENAME*
Read the identity key from the specified file. If the file is not present and −−create−identity−key is provided, create the identity key in the specified file. Default: "./authority_identity_key"

−s *FILENAME*
Write the signing key to the specified file. Default: "./authority_signing_key"

−c *FILENAME*
Write the certificate to the specified file. Default: "./authority_certificate"

−m *NUM*
Number of months that the certificate should be valid. Default: 12.

−−passphrase−fd *FILEDES*
Filedescriptor to read the passphrase from. Ends at the first NUL or newline. Default: read from the terminal.

−a *address*:*port*
If provided, advertise the address:port combination as this authority’s preferred directory port in its certificate. If the address is a hostname, the hostname is resolved to an IP before it’s published.

BUGS

This probably doesn’t run on Windows. That’s not a big issue, since we don’t really want authorities to be running on Windows anyway.

SEE ALSO

tor(1)

See also the "dir−spec.txt" file, distributed with Tor.