NAME

openssl-fipsinstall - perform FIPS configuration installation

SYNOPSIS

openssl fipsinstall [**-help**] [**-in** *configfilename*] [**-out** *configfilename*] [**-module** *modulefilename*] [**-provider_name** *providername*] [**-section_name** *sectionname*] [**-verify**] [**-mac_name** *macname*] [**-macopt** *nm*:*v*] [**-noout**] [**-quiet**] [**-no_conditional_errors**] [**-no_security_checks**] [**-self_test_onload**] [**-corrupt_desc** *selftest_description*] [**-corrupt_type** *selftest_type*] [**-config** *parent_config*]

DESCRIPTION

This command is used to generate a FIPS module configuration file. This configuration file can be used each time a FIPS module is loaded in order to pass data to the FIPS module self tests. The FIPS module always verifies its MAC, but optionally only needs to run the KAT's once, at installation.

The generated configuration file consists of:

- A MAC of the FIPS module file.
- A test status indicator.

  This indicates if the Known Answer Self Tests (KAT's) have successfully run.

- A MAC of the status indicator.
- A control for conditional self tests errors.

  By default if a continuous test (e.g a key pair test) fails then the FIPS module will enter an error state, and no services or cryptographic algorithms will be able to be accessed after this point. The default value of '1' will cause the fips module error state to be entered. If the value is '0' then the module error state will not be entered. Regardless of whether the error state is entered or not, the current operation (e.g. key generation) will return an error. The user is responsible for retrying the operation if the module error state is not entered.

- A control to indicate whether run-time security checks are done.

  This indicates if run-time checks related to enforcement of security parameters such as minimum security strength of keys and approved curve names are used. The default value of '1' will perform the checks. If the value is '0' the checks are not performed and FIPS compliance must be done by procedures documented in the relevant Security Policy.

This file is described in **fips_config**(5).

OPTIONS

-help

Print a usage message.

-module *filename*

Filename of the FIPS module to perform an integrity check on. The path provided in the filename is used to load the module when it is activated, and this overrides the environment variable **OPENSSL_MODULES**.

-out *configfilename*

Filename to output the configuration data to; the default is standard output.

-in *configfilename*

Input filename to load configuration data from. Must be used if the **-verify** option is specified.

-verify

Verify that the input configuration file contains the correct information.

-provider_name *providername*

Name of the provider inside the configuration file. The default value is "fips".

-section_name *sectionname*

Name of the section inside the configuration file. The default value is "fips_sect".

-mac_name *name*

Specifies the name of a supported MAC algorithm which will be used. The MAC mechanisms that are available will depend on the options used when building OpenSSL. To see the list of supported MAC's use the command "openssl list -mac-algorithms". The default is **HMAC**.

-macopt *nm*:*v*

Passes options to the MAC algorithm. A comprehensive list of controls can be found in the EVP_MAC implementation documentation. Common control strings used for this command are:

key:*string*

Specifies the MAC key as an alphanumeric string (use if the key contains printable characters only). The string length must conform to any restrictions of the MAC algorithm. A key must be specified for every MAC algorithm. If no key is provided, the default that was specified when OpenSSL was configured is used.

hexkey:*string*

Specifies the MAC key in hexadecimal form (two hex digits per byte). The key length must conform to any restrictions of the MAC algorithm. A key must be specified for every MAC algorithm. If no key is provided, the default that was specified when OpenSSL was configured is used.

digest:*string*

Used by HMAC as an alphanumeric string (use if the key contains printable characters only). The string length must conform to any restrictions of the MAC algorithm. To see the list of supported digests, use the command "openssl list -digest-commands". The default digest is SHA-256.

-noout

Disable logging of the self tests.

-no_conditional_errors

Configure the module to not enter an error state if a conditional self test fails as described above.

-no_security_checks

Configure the module to not perform run-time security checks as described above.

-self_test_onload

Do not write the two fields related to the "test status indicator" and "MAC status indicator" to the output configuration file. Without these fields the self tests KATS will run each time the module is loaded. This option could be used for cross compiling, since the self tests need to run at least once on each target machine. Once the self tests have run on the target machine the user could possibly then add the 2 fields into the configuration using some other mechanism.

-quiet

Do not output pass/fail messages. Implies **-noout**.

-corrupt_desc *selftest_description*, **-corrupt_type** *selftest_type*

The corrupt options can be used to test failure of one or more self tests by name. Either option or both may be used to select the tests to corrupt. Refer to the entries for **st-desc** and **st-type** in **OSSL_PROVIDER-FIPS**(7) for values that can be used.

-config *parent_config*

Test that a FIPS provider can be loaded from the specified configuration file. A previous call to this application needs to generate the extra configuration data that is included by the base "parent_config" configuration file. See **config**(5) for further information on how to set up a provider section. All other options are ignored if '-config' is used.

NOTES

Self tests results are logged by default if the options **-quiet** and **-noout** are not specified, or if either of the options **-corrupt_desc** or **-corrupt_type** are used. If the base configuration file is set up to autoload the fips module, then the fips module will be loaded and self tested BEFORE the fipsinstall application

has a chance to set up its own self test callback. As a result of this the self test output and the options **-corrupt_desc** and **-corrupt_type** will be ignored. For normal usage the base configuration file should use the default provider when generating the fips configuration file.

EXAMPLES

Calculate the mac of a FIPS module *fips.so* and run a FIPS self test for the module, and save the *fips.cnf* configuration file:

```
openssl fipsinstall -module ./fips.so -out fips.cnf -provider_name fips
```

Verify that the configuration file *fips.cnf* contains the correct info:

```
openssl fipsinstall -module ./fips.so -in fips.cnf  -provider_name fips -verify
```

Corrupt any self tests which have the description "SHA1":

```
openssl fipsinstall -module ./fips.so -out fips.cnf -provider_name fips \
    -corrupt_desc 'SHA1'
```

Validate that the fips module can be loaded from a base configuration file:

```
export OPENSSL_CONF_INCLUDE=<path of configuration files>
export OPENSSL_MODULES=<provider-path>
openssl fipsinstall -config' 'default.cnf'
```

SEE ALSO

config(5), **fips_config**(5), **OSSL_PROVIDER-FIPS**(7), **EVP_MAC**(3)

COPYRIGHT