NAME

fips_config - OpenSSL FIPS configuration

DESCRIPTION

A separate configuration file, using the OpenSSL **config**(5) syntax, is used to hold information about the FIPS module. This includes a digest of the shared library file, and status about the self-testing. This data is used automatically by the module itself for two purposes:

- Run the startup FIPS self-test known answer tests (KATS).
  This is normally done once, at installation time, but may also be set up to run each time the module is used.

- Verify the module's checksum.
  This is done each time the module is used.

This file is generated by the **openssl-fipsinstall**(1) program, and used internally by the FIPS module during its initialization.

The following options are supported. They should all appear in a section whose name is identified by the **fips** option in the **providers** section, as described in "Provider Configuration Module" in **config**(5).

activate

If present, the module is activated. The value assigned to this name is not significant.

install-version

A version number for the fips install process. Should be 1.

conditional-errors

The FIPS module normally enters an internal error mode if any self test fails. Once this error mode is active, no services or cryptographic algorithms are accessible from this point on. Continuous tests are a subset of the self tests (e.g., a key pair test during key generation, or the CRNG output test). Setting this value to 0 allows the error mode to not be triggered if any continuous test fails. The default value of 1 will trigger the error mode. Regardless of the value, the operation (e.g., key generation) that called the continuous test will return an error code if its continuous test fails. The operation may then be retried if the error mode has not been triggered.

security-checks

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. A value of '1' will perform the checks, otherwise if the value is '0' the checks are not performed and FIPS compliance must be

done by procedures documented in the relevant Security Policy.

module-mac
The calculated MAC of the FIPS provider file.

install-status
An indicator that the self-tests were successfully run. This should only be written after the module has successfully passed its self tests during installation. If this field is not present, then the self tests will run when the module loads.

install-mac
A MAC of the value of the **install-status** option, to prevent accidental changes to that value. It is written-to at the same time as **install-status** is updated.

For example:

```
[fips_sect]
activate = 1
install-version = 1
conditional-errors = 1
security-checks = 1
module-mac = 41:D0:FA:C2:5D:41:75:CD:7D:C3:90:55:6F:A4:DC
install-mac = FE:10:13:5A:D3:B4:C7:82:1B:1E:17:4C:AC:84:0C
install-status = INSTALL_SELF_TEST_KATS_RUN
```

NOTES

When using the FIPS provider, it is recommended that the **config_diagnostics** option is enabled to prevent accidental use of non-FIPS validated algorithms via broken or mistaken configuration. See **config**(5).

SEE ALSO

config(5) **openssl-fipsinstall**(1)

HISTORY

This functionality was added in OpenSSL 3.0.

COPYRIGHT