OpenSSL FIPS support

This release of OpenSSL includes a cryptographic module that is intended to be FIPS 140-2 validated. The module is implemented as an OpenSSL provider. A provider is essentially a dynamically loadable module which implements cryptographic algorithms, see the README-PROVIDERS file for further details.

The OpenSSL FIPS provider comes as shared library called `fips.so` (on Unix) resp. `fips.dll` (on Windows). The FIPS provider does not get built and installed automatically. To enable it, you need to configure OpenSSL using the `enable-fips` option.

Installing the FIPS module

If the FIPS provider is enabled, it gets installed automatically during the normal installation process. Simply follow the normal procedure (configure, make, make test, make install) as described in the INSTALL file.

For example, on Unix the final command

```
$ make install
```

effectively executes the following install targets

```
$ make install_sw
$ make install_ssldirs
$ make install_docs
$ make install_fips     # for `enable-fips` only
```

The `install_fips` make target can also be invoked explicitly to install the FIPS provider independently, without installing the rest of OpenSSL.

The Installation of the FIPS provider consists of two steps. In the first step, the shared library is copied to its installed location, which by default is

```
/usr/local/lib/ossl-modules/fips.so                  on Unix, and
C:\Program Files\OpenSSL\lib\ossl-modules\fips.dll   on Windows.
```

In the second step, the `openssl fipsinstall` command is executed, which completes the installation by doing the following two things:

- Runs the FIPS module self tests
- Generates the so-called FIPS module configuration file containing information about the module such as the self test status, and the module checksum.

The FIPS module must have the self tests run, and the FIPS module config file output generated on every machine that it is to be used on. You must not copy the FIPS module config file output data from one machine to another.

On Unix the `openssl fipsinstall` command will be invoked as follows by default:

```
$ openssl fipsinstall -out /usr/local/ssl/fipsmodule.cnf -module /usr/local/lib/ossl-modules
```

If you configured OpenSSL to be installed to a different location, the paths will vary accordingly. In the rare case that you need to install the fipsmodule.cnf to non-standard location, you can execute the `openssl fipsinstall` command manually.

Using the FIPS Module in applications

Documentation about using the FIPS module is available on the fips_module(7) manual page.