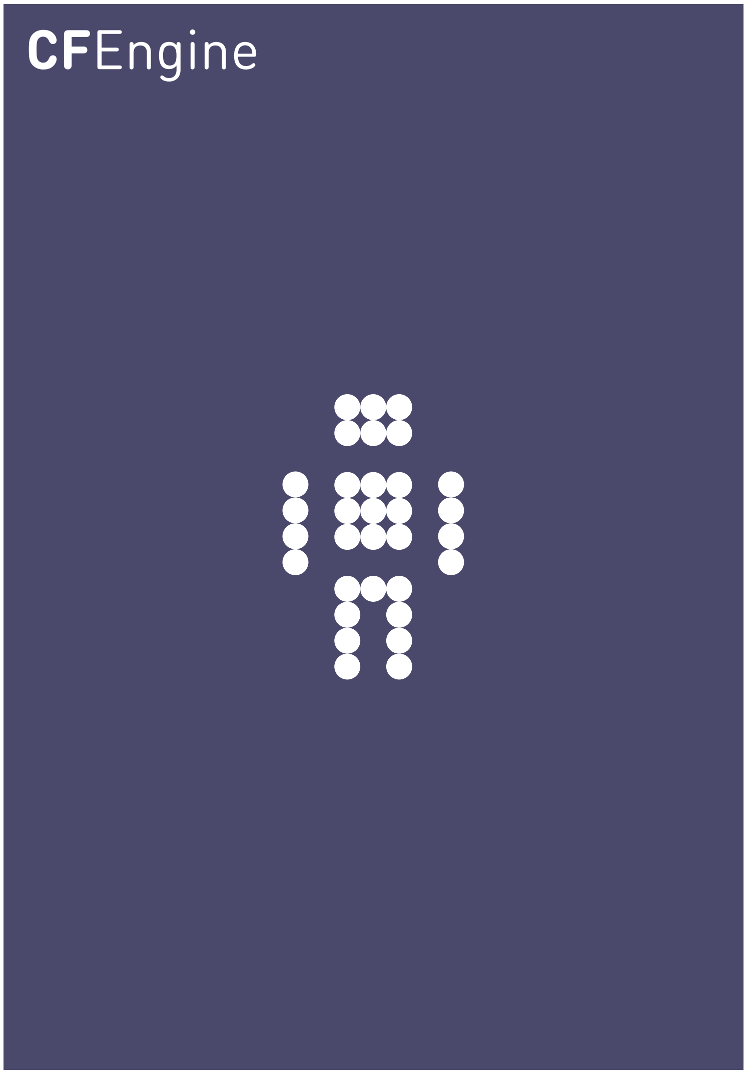

FIPS validated cryptography in CFEngine

A CFEngine Special Topics Handbook

CFEngine AS

The FIPS 140-2 validation for approved cryptographic modules is a current government requirement in the USA. This document explains the use of FIPS 140-2 validated modules in commercial CFEngine versions.

FIPS 140-3 is underway and will supercede FIPS 140-2 at some unknown time in the future.

QA: MB,NP,CR

Table of Contents

What is FIPS 140-2?

FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST)[1]. NIST also established the Cryptographic Module Validation Program (CMVP)[2] that validates cryptographic modules to the FIPS 140-2 standard. Vendors seek validation for their cryptographic modules in order to provide assurance that their encryption solutions are properly implemented to an accepted standard.

A cryptographic module that has already been issued a FIPS 140-2 validation certificate may be incorporated or embedded into another product. [3]

In order to use a validated cryptographic module and attest FIPS 140-2 validation, the new product must:

- Reference the certificate number of the validated module,
- Must not alter the original validated module.
- Must adhere to the documented security policy for the validated module.

What is the certificate number?

CFEngine attests to NIST certificate number 1111.

These validations were not initiated by CFEngine, but any user of this Open Source software module can use them provided we follow the instructions in the security policy.

Declaration from CFEngine

The current FIPS 140-2 Crypto Policy Officer for CFEngine resides at CFEngine AS/Inc headquarters. The security officer attests that packages provided by CFEngine, on the customer download site software.CFEngine.com, whose names contain the term FIPS in upper or lower case have been compiled according to the security policy for certificate 1111 [5]. CFEngine packages, marked FIPS, have been built from source code located at:

`http://www.openssl.org/source/openssl-fips-1.2.tar.gz`

according to the security policy documented in [6]. CFEngine can provide compliant software on all Unix-like platforms, but not currently on Windows.

Algorithms

CFEngine uses OpenSSL encryption code from the libcrypto library. It does not use any SSL or TLS specific modules. CFEngine uses RSA encryption for authentication. Commercial versions of CFEngine use AES-256 symmetric encryption with a random session key for transport.

Future policy

It is CFEngine's policy to obtain a private validation of the OpenSSL crypto module at some time in the next two years for the principal purpose of branding. This is a long process and does not alter the specification of the software in any way.

References

1. Security policy 1111:
2. http://csrc.nist.gov/groups/STM/cmvp/standards.html
3. http://csrc.nist.gov/groups/STM/cmvp/index.html
4. http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf
5. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1111
6. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1111.pdf
7. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1111.pdf