FIPS 140-3 Request for Information

This form will guide you in gathering basic information that atsec uses to provide guidance about potential FIPS 140-3 projects.

Thank you for completing as much of the form as you can.

If you have concerns about sharing proprietary information, please contact us to set up an NDA and appropriate transaction security before submitting the form to us.

FIPS 140-3 testing is comprehensive module testing that typically includes Cryptographic Algorithm Validation testing (CAVP), as well as Entropy Source Validation testing (ESV). For more information about FIPS 140-3 and the terminology used in this form see: <https://www.nist.gov/programs-projects/cryptographic-module-validation-program-cmvp>.

Table of Contents

[Contact Information 2](#_Toc169687176)

[General Considerations 3](#_Toc169687177)

[Module Information & Scope of FIPS 140-3 Testing 4](#_Toc169687178)

[Design, Development, and Documentation 7](#_Toc169687179)

[Entropy Source Validation Information 9](#_Toc169687180)

[Comments and Questions 10](#_Toc169687181)

# Contact Information

Legal Company Name:

State of Incorporation:

Contact Name:

Address:

City:

State:

Zip/Postal Code:

Country:

Email:

Phone:

Date of Submission:

# General Considerations

The following questions are intended to make you aware of factors that influence the complexity and duration of a module evaluation.

Do you own or have full access to the complete source code for your module?

Yes  No

Did any external organization contribute to developing the security functions of your module?

Yes  No

Has the module been tested under the CMVP before?

Yes  No

If “Yes”, specify the last certificate number:

Do you plan to test later releases of your module?

Yes  No

Is the module classified?

Yes  No

Is the module restricted under ITAR regulations?

Yes  No

Is the module classified for export control by BIS (<http://www.bis.doc.gov/>)?

Yes  No

If “Yes”, specify the ECCN:

Are there any other export/import requirements applicable?

Yes  No

If “Yes”, please explain:

# Module Information & Scope of FIPS 140-3 Testing

What is the name of the cryptographic module you want to have evaluated?

What is the version number of the cryptographic module you want to have evaluated?

What is the module type?

Hardware

Software or  Firmware

Firmware/Hardware Hybrid OR  Software/Hardware Hybrid

Please outline the components of your hybrid module:

How is the cryptographic module presented?

Single Chip

Multi-chip embedded (e.g., a PCB)

Multi-chip standalone (e.g., a PC, table or mobile phone)

What is your operational environment?

|  |  |  |
| --- | --- | --- |
| **Platform** | **Operating System**  **(incl. version number)** | **CPU** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Do you plan to test on all of the above platforms?

Yes  No

If “No”, specify which platforms will be tested:

At which Security Levels do you plan to test your module?

1. General  1  2  3  4
2. Cryptographic Module Specification  1  2  3  4
3. Cryptographic Module Interfaces  1  2  3  4
4. Roles, Services & Authentication  1  2  3  4
5. Software/Firmware Security  1  2  3  4
6. Operational Environment  1  2  3  4  N/A
7. Physical Security  1  2  3  4  N/A
8. Non-Invasive Security  1  2  3  4  N/A
9. SSP Management  1  2  3  4
10. Self-Tests  1  2  3  4
11. Life-Cycle Assurance  1  2  3  4
12. Mitigation of Other Attacks  1  2  3  4  N/A

Overall Security Level  1  2  3  4  
*Note*: Overall Security Level is equal to the lowest of the individual levels.

Does the module have any non-Approved services?

Yes  No

Does the module have any non-Approved algorithms?

Yes  No

**Does your module contain an entropy source?**

Yes  No

Which approved security functions (algorithms and RNGs) will need to be tested?

Block Ciphers

AES  TDES (decryption only)  Skipjack (decryption only)

Block Cipher Modes

ECB  CBC  CFB  OFB  CTR

CCM  GCM  XTS  KW  KWP

Secure Hashing

SHA-1  SHA-2  SHA-3

SHA2-224  SHA2-256  SHA2-384  SHA2-512

SHA2-512/224  SHA2-512/256

SHA3-224  SHA3-256  SHA3-384  SHA3-512

SHAKE128  SHAKE256

cSHAKE128  cSHAKE256

Message Authentication

CMAC  GMAC  HMAC  KMAC128  KMAC256

Key Derivation Functions

KBKDF  PBKDF2  HKDF  OneStep KDF

TwoStep KDF  Protocol-Specific KDFs

Random Number Generation

Hash\_DRBG  CTR\_DRBG  HMAC\_DRBG

Key Agreement/Transport

*Diffie-Hellman*

KAS FFC  KAS-FFC-SSC

*EC Diffie-Hellman*

KAS-ECC  KAS-ECC-SSC

*RSA KEM*

KAS-IFC  KAS-IFC-SSC

*RSA OAEP*

KTS-IFC

Digital Signatures

RSA  ECDSA  EdDSA  DSA (verification only)

LMS

Component Testing

☐ RSASP1 Signature Generation Component (FIPS 186-4)

☐ ECDSA Signature Generation Component (FIPS 186-4)

☐ RSA Decryption Primitive (7.1.2.1 of SP 800-56Brev2)

# Design, Development, and Documentation

A list of required documentation is given in ISO/IEC 19790:2012 Appendix A and NIST SP 800-140A “CMVP Documentation Requirements”. Please review this, as you will need to provide all the required documentation to the laboratory.

Was this module designed/developed with FIPS 140-3 specification as a requirement?

Yes  No

Which of these documents do you already have?

Administration Guide  User Guide  Installation Guide

Error Reference/Troubleshooting

Finite State Model

Do you have a high-level design document that describes the major structural units (subsystems) of the module and the implementation of its security functionality for the release that is going to be certified?

Yes  No

Name the programming languages used to develop the module:

Has the development organization been involved in FIPS 140-3 testing before?

Yes  No

Is the development of the module that you want to test already completed?

Yes  No

Where is your module developed and tested?

Do you perform any functional testing on the module?

Yes  No

If “Yes”, please specify what testing is done:

Do you perform any low-level testing (e.g. unit tests) on the module?

Yes  No

If “Yes”, please specify what testing is done:

Do you run automated security diagnostic tools (e.g. Valgrind, SonarQube, Coverity, etc.) on the module?

Yes  No

If “Yes”, please list the tools:

**Is your module open source?**

Yes  No

If “Yes”, please provide a link:

Will you be able to share source code with our lab, so we have it at our facility?

Do you have any CAVP certificates and/or ESV candidates?

Are there any restrictions on access to the product?

Are there any restrictions on who can work on this product (e.g. citizenship)?

# Entropy Source Validation Information

What is the noise source category of the entropy source you want to have evaluated?

What is the size of the noise source sample (prior to conditioning, if present)?

Do you already have an estimate of the entropy in the noise source sample (i.e. the H\_submitter)?

Yes  No

If “Yes”, please specify the H\_submitter:

Do you already have a theoretical model that describes why the noise source can produce entropy and support the H\_submitter entropy rate?

Yes  No

Does your entropy source implement the health tests described in SP800-90B, Section 4.4 (Repetition Count Test and Adaptive Proportion Test)?

Yes  No

Does your entropy source implement any additional (vendor-defined) health tests that are not described in the SP800-90B?

Yes  No

If “Yes”, please describe them:

Does your entropy source include one or more conditioning components (such as SHA, HMAC, AES, etc. functions)?

Yes  No

Does your entropy source seed only approve SP800-90Ar1 DRBGs?

Yes  No

Does your entropy source seed a chain of DRBGs (e.g. one parent DRBG which itself seeds multiple child DRBGs)?

Yes  No

Have you already collected the raw noise data (consecutive and restart) at the output of the noise source?

Yes  No

If “No”, are you familiar with the process of collecting raw data?

Yes  No

# Comments and Questions

Do you have any additional comments or questions for us?