atsec information security

 [www.atsec.com](file:///Users/Fiona/Projects/marketing/pre-prepared_material/RFIs/www.atsec.com)

 email contact for FIPS 140-2: cst-info@atsec.com

FIPS 140-2 Request for Information

This form guides you in gathering the basic information that atsec needs in order to provide you with information about FIPS 140-2 .

Please complete this form and submit it via email or fax. 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.

For more information about FIPS 140-2, the CMVP and the terminology used in this form, see the [CMVP website](https://csrc.nist.gov/projects/cryptographic-module-validation-program).

Contact Information

Company name:

Contact name:

Address:

City:

State:

Country:

Zip/Postal code:

Email:

Phone:

Product Information

What is the name of the product you want to have evaluated?

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

General Considerations

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

Why are you considering FIPS 140-2 testing for your product?

[ ]  Government bid

[ ]  Customer requirement

[ ]  Nice to have

[ ]  Improve security

[ ]  Improve quality

How many people are on your development team?

How many people are involved with development of the cryptographic module?

Have you (as a development organization) been involved in FIPS 140-2 testing before?

[ ]  Yes

[ ]  No

If yes, has this product been tested under the CMVP before?

[ ]  Yes

[ ]  No

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

[ ]  Yes

[ ]  No

What is the product type?

[ ]  Hardware

[ ]  Software

[ ]  Firmware

How is the cryptographic module presented?

[ ]  Single Chip

[ ]  Multi-chip embedded (for example, a PCB)

[ ]  Multi-chip standalone (for example, a PC)

If your product is software, on which underlying hardware platforms does it run?

Do you plan to test all of these platforms?

[ ]  Yes

[ ]  No

If your product is software, on which underlying operating systems does it run?

[ ]  AIX [ ]  z/OS [ ]  Solaris [ ]  z/VM

[ ]  HP/UX [ ]  OS/400 [ ]  Linux [ ]  Mac OS X

[ ]  Windows [ ]  Java Card [ ]  Other

If your product runs on other operating systems, please specify them here:

Scope

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

1. Cryptographic Module Specification [ ]  1 [ ]  2 [ ]  3 [ ]  4

2. Ports and Interfaces [ ]  1 [ ]  2 [ ]  3 [ ]  4

3. Roles Services & Authentication [ ]  1 [ ]  2 [ ]  3 [ ]  4

4. Finite State Machine [ ]  1 [ ]  2 [ ]  3 [ ]  4

5. Physical Security [ ]  1 [ ]  2 [ ]  3 [ ]  4 [ ]  N/A

6. Operational Environment [ ]  1 [ ]  2 [ ]  3 [ ]  4 [ ]  N/A

7. Cryptographic Key Management [ ]  1 [ ]  2 [ ]  3 [ ]  4

8. EMI/EMC [ ]  1 [ ]  2 [ ]  3 [ ]  4

9. Self Tests [ ]  1 [ ]  2 [ ]  3 [ ]  4

10. Design Assurance [ ]  1 [ ]  2 [ ]  3 [ ]  4

11. Mitigation of Other Attacks [ ]  1 [ ]  2 [ ]  3 [ ]  4 [ ]  N/A

Overall Security Level [ ]  1 [ ]  2 [ ]  3 [ ]  4

Select the Approved security functions (Refer to FIPS 140-2 Annex A):

[ ]  Block Ciphers: AES: Triple Des, Skipjack

[ ]  Block Cipher Modes: CCM, CMAC, GCM / GMAC / XPN, Key wrap, XTS

[ ]  Digital Signatures: FIPS 186-4: DSA, ECDSA, RSA ; FIPS 186-2: DSA, ECDSA, RSA

[ ]  Symmetric Key: Skipjack FIPS 185 Escrowed Encryption Standard (EES)

[ ]  Key Derivation Functions: KBKDF

[ ]  Key Management: KAS

[ ]  Message Authentication: HMAC (FIPS 198-1)

[ ]  Random Number Generation: DRBG

[ ]  Secure Hashing: SHA-2, SHA-1, SHA-3

[ ]  Component Testing: ECC-CDH (SP 800-56A), ECDSA Signature (FIPS 186-4), KDF (SP800-135), RSA PKCS1-v1.5 RSASP1 (FIPS 186-4), RSA PKCS1-vPSS RSASP1 (FIPS 186-4), RSADP Decryption (SP 800-56B; PKCS#1 v2.1)

Have these functions already been validated by the Cryptographic Algorithm Validation Program?

[ ]  Yes

[ ]  No

When do you want the testing to start?

When do you want the certification process to end?

Do you plan to test later releases of your product?

[ ]  Yes

[ ]  No

Was this product designed/developed with FIPS 140-2 specification as a requirement?

[ ]  Yes

[ ]  No

Name the programming languages used to develop the product:

Design and Documentation

A list of required documentation is given in the [FIPS 140-2 standard in Appendix "A".](https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf) Please review this as you will need to produce all this documentation to the laboratory.

Do you have all the required documentation available to provide to the laboratory?

[ ]  Yes

[ ]  No

Do you have any of these manuals?

[ ]  Administration Guide

[ ]  User Guide

[ ]  Installation Guide

[ ]  Error Reference/Troubleshooting

[ ]  Security Policy compliant with FIPS 140-2 Appendix "A"

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

[ ]  Yes

[ ]  No

In general, what type of design documentation do you develop or maintain for your product?

[ ]  Feature-based documentation only; old design documentation is not updated

[ ]  Updates of old design documentation to reflect the updated implementation in a new release

[ ]  None

[ ]  Other

If you have other type of design documentation, please give a brief description of what type documentation you have:

Processes and Procedures

The scope of the FIPS 140-2 evaluation is not limited to technical aspects. The development environment and its ability to provide for a secure and reliable product are also important.

Which of the following items do you have under configuration management (version control, access control, release management)?

[ ]  Implementation representation (such as source code)

[ ]  Design documentation

[ ]  Test plans, test cases, and results

[ ]  User manuals

[ ]  Security-relevant defects

[ ]  FIPS 140-2 -specific evidence

Specify which tools you use for configuration management?

Do you own the complete source code for your product?

[ ]  Yes

[ ]  No

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

[ ]  Yes

[ ]  No

Where is your product developed and tested?

[ ]  One location

[ ]  Multiple locations

Do all development and manufacturing sites implement measures to physically and logically protect the development of the product (for example, the source code and design documentation)?

[ ]  Yes

[ ]  No

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

[ ]  Yes

[ ]  No

If yes, specify the ECCN:

Comments

Additional comments:

If you have any questions, please contact atsec at cst-lab@atsec.com or by telephone (see <http://www.atsec.com/us/addresses-contact.html> for regional office numbers).