**Cryptographic Algorithm Validation Program**

**Request for Information**

This form will guide you in gathering basic information that atsec uses to provide guidance about potential Cryptographic Algorithm Validation Program (CAVP) projects. The questions on this form are not mandatory, but they help us make the first call more productive. As such, we appreciate you 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.

CAVP testing focuses on validating approved cryptographic algorithms by using NIST-provided test vectors and analyzing the response files generated by the cryptographic module using the tested algorithm. For more information about CAVP or the terminology used in this form see: <https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program>.

Table of Contents

[Contact Information 2](#_Toc169687503)

[General Considerations 3](#_Toc169687504)

[Algorithm Information and Scope of CAVP Testing 4](#_Toc169687505)

[Design, Development, and Documentation 6](#_Toc169687506)

[Comments and Questions 6](#_Toc169687507)

**Contact Information**

Legal Company Name:

State of Incorporation:

Contact Name:

Address:

City:

State:

Zip/Postal Code:

Country:

Email:

Phone:

**General Considerations**

The following questions are intended to make you aware of factors that influence the complexity and duration of algorithm validation.

**Have you confirmed your algorithm is a CAVP Supported Algorithm (**<https://pages.nist.gov/ACVP/#supported>**)?**

☐ Yes ☐ No

**Are you planning to pursue FIPS 140-3 certification after CAVP validation?**

☐ Yes ☐ No

If “Yes”, does your product also implement a true random number generator which needs to be validated?

☐ Yes ☐ No

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

☐ Yes ☐ No

**Has the algorithm been validated by the CAVP before?**

☐ Yes ☐ No

If “Yes”, specify the last validation number:

**Is the algorithm restricted under ITAR regulations?**

☐ Yes ☐ No

**Is the algorithm 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:

**Algorithm Information and Scope of CAVP Testing**

**What is the algorithm implemented on?**

☐ Hardware

☐ Software

☐ Firmware

**What is your operational environment you would like to test your algorithm on?**

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

**Which approved security functions (algorithms and RNGs) will need to be tested? Select all that apply.**

Block Ciphers

☐ AES ☐ TDES (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**

**Name the programming languages used to develop the algorithm(s):**

**Has the development organization been involved in CAVP validation before?**

☐ Yes ☐ No

**Do you have a test harness to support algorithm testing (import the test vectors into your implementation and collect the results in the correct format)?**

☐ Yes ☐ No

**Is the development of the algorithm(s) that you want to test already completed?**

☐ Yes ☐ No

**Are there any restrictions on access to the product?**

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

**Comments and Questions**

**Do you have any additional comments or questions for us?**