Entropy Source Validation Testing

Request for Information

This form will guide you in gathering basic information that atsec uses to provide guidance about potential Entropy Source Validation (ESV) testing 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.

ESV testing focuses on verifying the design, operation, and documentation of the noise source for the entropy source, as well as verifying the compliance of the cryptographic module using the entropy source with SP 800-90B by analyzing raw noise data. For more information about ESV or the terminology used in this form see: <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations>.

Table of Contents

[Contact Information 2](#_Toc169687711)

[General Considerations 3](#_Toc169687712)

[Entropy Source Information & Scope of ESV Testing 4](#_Toc169687713)

[Design, Development, and Documentation 5](#_Toc169687714)

[Comments and Questions 5](#_Toc169687715)

# 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 ESV testing.

Are you planning to pursue FIPS 140-3 certification after ESV certification?

☐ Yes ☐ No

If “Yes”, do you also need Cryptographic Algorithm Testing Protocol (CAVP) testing performed?

☐ Yes ☐ No

Do you own or have full access to the complete design documentation for your entropy source?

[ ]  Yes [ ]  No

Has the entropy source been tested before?

[ ]  Yes [ ]  No

If “Yes”, specify the last certificate number:

Is the entropy source restricted under ITAR regulations?

[ ]  Yes [ ]  No

Is the entropy source 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:

# Entropy Source Information & Scope of ESV Testing

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

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

What is the evaluated version type?

[ ]  Physical

[ ]  Non-physical

What are your operational environments?

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

# Design, Development, and Documentation

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

Of ypur entropy source includes a non-vetted conditioning component, have you already collected the conditioned entropy data at the output of this conditioning component?

[ ]  Yes [ ]  No

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

[ ]  Yes [ ]  No

Name the programming languages used to develop the entropy source:

Has the development organization been involved in entropy source testing before?

[ ]  Yes [ ]  No

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

[ ]  Yes [ ]  No

Where is your entropy source developed and tested?

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?