Common Criteria Evaluation

Request for Information

This form will guide you in gathering basic information that atsec uses to provide guidance about potential Common Criteria evaluation projects. The questions in this document 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.

Common Criteria evaluations focus on testing a product against specific security requirements to demonstrate assurance the security functions work as stated. For more information about the Common Criteria or the terminology used in this form see: <https://www.commoncriteriaportal.org/>.

Table of Contents

[Contact Information 2](#_Toc170372280)

[Evaluation Scope 3](#_Toc170372281)

[General Considerations 4](#_Toc170372282)

[Platforms 4](#_Toc170372283)

[Vulnerability Analysis 5](#_Toc170372284)

[Cryptographic Functionality 5](#_Toc170372285)

[Entropy Source 5](#_Toc170372286)

[Comments and Questions 5](#_Toc170372287)

# Contact Information

Legal Company Name:

State of Incorporation:

Contact Name:

Address:

City:

State:

Zip/Postal Code:

Country:

Email:

Phone:

# Evaluation Scope

*Note: NIAP does not allow EAL evaluations, but it may be possible to run an evaluation in a scheme that can produce a certificate able to be recognized by NIAP as well as a certificate specifying an EAL for the European market.*

Which CC Scheme(s) would you prefer to use?

[ ]  U.S. (NIAP’s CCEVS)

[ ]  Germany (BSI)

[ ]  Sweden (CSEC)

[ ]  Italy (OCSI)

[ ]  Singapore (CSA)

[ ]  Other

Please specify:

If pursuing an evaluation using NIAP’S CCEVS or using Protection Profiles:

Which Protection Profile(s) do you plan to claim conformance with for your product?

Note: Specify the name and version of the PP-Configuration or any Protection Profile(s) (e.g., PP for Application Software), PP-Modules (e.g., PP-Module for VPN Clients), or security Functional Packages (Functional Package for TLS):

If pursuing an evaluation with BSI, CSEC, OSCI, or CSA:

At which Evaluation Assurance Level do you plan to certify your product?

[ ]  EAL1 [ ]  EAL2 [ ]  EAL3 [ ]  EAL4

[ ]  EAL5 [ ]  EAL6 [ ]  EAL7

Will the EAL be augmented with an additional assurance requirement
(EAL ”+”)?

[ ]  Flaw remediation

[ ]  Other

Please specify:

If pursing an EAL, select the major security functions of your product:

[ ]  Security Audit [ ]  Communication

[ ]  Identification and Authentication [ ]  User Data Protection

[ ]  Cryptographic Support [ ]  Security Management

[ ]  Protection of Security Functionality [ ]  Privacy

[ ]  Trusted Path/Channels [ ]  Resource Utilization

[ ]  TOE Access

[ ]  Other

Please specify:

# General Considerations

Have you (as a development organization) been involved in a security evaluation before?

[ ]  Yes [ ]  No

If “Yes”, has this product been evaluated before?

[ ]  Yes [ ]  No

If “Yes”, which standard?

[ ]  Common Criteria

[ ]  FIPS 140-3

[ ]  Others

For Common Criteria, which national scheme?

[ ]  U.S. (NIAP’s CCEVS)

[ ]  Germany (BSI)

[ ]  Sweden (CSEC)

[ ]  Italy (OCSI)

[ ]  Singapore (CSA)

[ ]  Other

For CCEVS-NIAP (US), please specify the Protection Profile(s) in which the product was compliant, e.g., Protection Profile for General Purpose Operating System, version 4.3:

Where is your product developed and tested?

Note: For EAL 3 and above, this is important to know when we need to consider site visits.

Is the development of the release that you want to certify already completed?

[ ]  Yes [ ]  No

# Platforms

If your product is software, on which underlying hardware platform(s) does it run?

[ ]  Intel Xeon [ ]  Intel Atom [ ]  Intel Core [ ]  Itanium

[ ]  AMD [ ]  Snapdragon [ ]  Apple Processor

[ ]  IBM Power [ ]  zSeries

[ ]  Other

Please specify:

If your product is non-operating system software, on which underlying operating system(s) does it run?

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

[ ]  HP/UX [ ]  OS/400 [ ]  Linux [ ]  Android

[ ]  Apple macOS [ ]  Apple iOS [ ]  Apple Watch OS [ ]  Apple iPadOS

[ ]  Windows [ ]  VxWorks

[ ]  Other

Please specify:

# Vulnerability Analysis

Do you perform vulnerability analyses for the product?

[ ]  Yes [ ]  No

Do you monitor public sources that publish product-related flaws and exploits to ensure that your product is not affected?

[ ]  Yes [ ]  No

If “Yes”, specify which National Vulnerability Database you monitor:

Do you have procedures in place to ensure the timely fix of each security vulnerability that is identified in the product?

[ ]  Yes [ ]  No

# Cryptographic Functionality

Please specify all the cryptographic modules and their versions in your products, e.g., OpenSSL 3.0.

Do any of the modules specified above have Cryptographic Algorithm Verification Program (CAVP) certificates?

[ ]  Yes [ ]  No

If “Yes”, please provide the certificate number:

# Entropy Source

Please provide details about the entropy sources that your product uses (for software, this is often platform-based):

Does your product provide its own entropy sources?

[ ]  Yes [ ]  No

If “Yes”, is the entropy source software-based or hardware-based? Please list the entropy source:

Does your product use any platform-provided entropy sources?

[ ]  Yes [ ]  No

If “Yes”, is the entropy source software-based or hardware-based? Please list the entropy source:

Do any of the entropy sources specified above have an Entropy Source Validation (ESV) certificate?

[ ]  Yes [ ]  No

If “Yes”, please provide the certificate number:

# Comments and Questions

Do you have any additional comments or questions for us?