atsec information security

[www.atsec.com](http://www.atsec.com)

email: info@atsec.com

Common Criteria Evaluation Request for Information

This form guides you in gathering the basic information that atsec needs in order to provide you with information about a Common Criteria Evaluation.

Please complete this form and submit it via email. 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.

More information about Common Criteria and the terminology used in this form is available from <http://www.commoncriteriaportal.org>.

Contact Information

Company name:

Contact name:

Address:

City:

State:

Country:

Zip/Postal code:

Email:

Phone:

Product Information

What is the name of the product that you want to be evaluated?

What is the type of the product that you want to be evaluated?

      *(Examples include, operating system, network device, mobile device)*

What is the version of the product that you want to be evaluated?

      *(This is to help us identify the product characteristic. The version to be evaluated will be finalized in a statement of work)*

General Considerations

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

Why are you considering a Common Criteria evaluation of your product?

[ ]  Government bid

[ ]  Customer requirement

[ ]  Nice to have

[ ]  Improve security

Approximately how many people are on your product development team?

Approximately how many people are involved with development of the security features of your product?

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

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

[ ]  Yes

[ ]  No

When do you want the evaluation to start and/or end?

Start date:       End date:

Platforms

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

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

[ ]  AMD [ ]  Snapdragon [ ]  Apple Processor

[ ]  IBM Power [ ]  zSeries

[ ]  Other: Please specify:

Do you plan to certify on 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 [ ]  Android

[ ]  Apple Mac OS [ ]  Apple iOS [ ]  Apple Watch OS [ ]  Apple iPad OS

[ ]  Windows [ ]  VxWorks

[ ]  Other: Please specify:

Evaluation Scope

*Note: NIAP do 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)

[ ]  Other: Please specify:

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

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

[ ]  EAL5 [ ]  EAL6 [ ]  EAL7

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

[ ]  Flaw remediation [ ]  SPM (Security Policy Model) [ ]  ACO (Composition class in 3.1)

[ ]  Other: Please specify:

Should the Security Target comply with a Protection Profile?

[ ]  Yes

[ ]  No

If yes, specify the name and version of the PP-Configuration or any Protection Profile(s),PP-Modules or security functional packages:

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:

Design and Documentation

*Note: Depending on the EAL chosen for your product, the Common Criteria requires you to have several abstraction levels of design documentation for its security functionality, as well as documentation for users and administrators on how to use this functionality.*

*In general, for cPPs and PP-based evaluations a lot of documentation is not required.*

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

[ ]  Mixed

[ ]  None

[ ]  Other:

Are all interfaces that provide access to security functionality specified in a functional specification for the release that is going to be certified?

[ ]  Yes, all are specified

[ ]  Only some are specified

[ ]  Only those that are intended for customer use are specified

[ ]  None are specified

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

For EAL4 only: Do you have low-level designs for the implementation of your product on a module-based level?

[ ]  Yes

[ ]  No

Do you have any of these manuals?

[ ]  Administration Guide

[ ]  User Guide

[ ]  Installation Guide

[ ]  Error Reference/Troubleshooting

[ ]  Secure Configuration and Operation

[ ]  Other user manuals

Processes and Procedures

The Common Criteria does not limit the evaluation scope 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

[ ]  Common Criteria-specific evidence

Which tools do you use for configuration management?

[ ]  CVS [ ]  SVN [ ]  GitHub

[ ]  None

[ ]  Other: Please specify:

Where is your product developed and tested?

*Note: This is important to know when we need to consider site visits.*

[ ]  One location

[ ]  Multiple locations: Please specify:

Are your release management processes and procedures documented?

[ ]  Yes

[ ]  No

Select the development activities for which you have documented processes:

[ ]  Configuration management

[ ]  Delivery and distribution

[ ]  Security flaw reporting

[ ]  Security flaw fix delivery

[ ]  Lifecycle

Have the use and function of your development tools (such as programming languages, compilers, build scripts, test tools) been documented?

[ ]  Yes

[ ]  Partly

[ ]  No

Source Code

*NOTE: The requirement to provide source code to the laboratory is at EAL 4 and above. However, the answers to these questions will guide us in assessing the work needed for vulnerability assessment at any EAL, or in a NIAP evaluation.*

Do you own the complete source code for your product?

[ ]  Yes

[ ]  No

Did any external / 3rd Party organization contribute to developing the security functions of your product?

This includes third party libraries used in your product.

[ ]  Yes

[ ]  No

If yes, please specify which security functions were contributed and in what form those functions were received and integrated into the product:

      [ ]  Source Code [ ]  Binary

      [ ]  Source Code [ ]  Binary

      [ ]  Source Code [ ]  Binary

In the case of Source Code, are these libraries modified in house?

[ ]  Yes

[ ]  No

Does your product contain any open source software?

[ ]  Yes

[ ]  No

If yes, specify the name and version of the technology:

Testing and Vulnerability Analysis

Functional testing of the security functionality that is subject to evaluation is required at externally visible and - depending on the EAL - internal subsystem interfaces. The developer is required to provide a vulnerability analysis as contribution to the vulnerability assessment that will be performed during an evaluation.

Do you perform functional testing of your product?

[ ]  Yes

[ ]  No

If yes, how comprehensive do you consider your test effort?

[ ]  Basic

[ ]  Moderate

[ ]  Extensive

[ ]  Exhaustive

Do you perform regression testing to make sure that security functionality implemented in earlier releases still works as expected?

[ ]  Yes

[ ]  No

Are all aspects of the security functions that are implemented in your product covered by tests?

[ ]  Yes

[ ]  Partly

[ ]  No

Select the parts of your test procedures that are documented:

[ ]  Description of the test cases

[ ]  Coverage of security functionality

[ ]  Testing process

[ ]  Test plan

[ ]  Expected test results

[ ]  Actual test results

Do you perform a vulnerability analysis for the product?

[ ]  Yes

[ ]  No

Do you conduct code reviews before integrating externally developed code into the product?

[ ]  Yes

[ ]  No

Do you have programming guidelines that provide guidance to developers on how to avoid typical programming errors (such as buffer overflows)?

[ ]  Yes

[ ]  No

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

[ ]  Yes

[ ]  No

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

[ ]  Yes

[ ]  No

Does your product implement probabilistic or permutational mechanisms (such as password-based authentication)?

[ ]  Yes

[ ]  No

Do you perform analysis of the user and administration manuals that are delivered with the product to ensure that all security functionality is correctly described?

[ ]  Yes

[ ]  No

Cryptographic functionality

Does your product implement cryptographic mechanisms?

[ ]  Yes

[ ]  No

If yes, has a FIPS 140-2 certification been completed?

[ ]  Yes

[ ]  No

If yes, have algorithm certifications been completed?

[ ]  Yes

[ ]  No

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

This includes third party libraries used in your product.

[ ]  Yes

[ ]  No

If yes, please specify which libraries and their versions are included and in what form those functions were received and integrated into the product:

      [ ]  Source Code [ ]  Binary

      [ ]  Source Code [ ]  Binary

      [ ]  Source Code [ ]  Binary

      [ ]  Source Code [ ]  Binary

      [ ]  Source Code [ ]  Binary

      [ ]  Source Code [ ]  Binary

In the case of Source Code, are these libraries modified in house?

[ ]  Yes

[ ]  No

Entropy Sources

Please explain about the entropy sources that your product uses. For software this is often Platform based.

Comments

Additional comments:

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