atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: 512-615-7300
Fax: 512-615-7301
www.atsec.com

Common Criteria:
National Validation Scheme Differences:
CCEVS, CSEC and BSI

Fiona Pattinson, Ken Hake, Gerald Krummeck, Staffan Persson

April 29th, 2009

Table of Contents:

1 Introduction

The intended audience for this document is any organization interested in pursuing CC certification using atsec as the certification lab that has not yet selected which scheme to certify against.

There are three Evaluation Authorities (also referred to as Validation Schemes or Certification Bodies) for which atsec is accredited to perform Common Criteria evaluations.

This document will describe the validation schemes with which atsec is accredited in order to perform Common Criteria evaluation: the United States Common Criteria Evaluation and Validation Scheme (CCEVS) operated by the National Information Assurance Partnership (NIAP), the German Bundesamt für Sicherheit in der Informationstechnik (BSI), and the Swedish Sveriges Certifieringsorgan för IT-Säkerhet. Although we restrict ourselves to these three schemes many of the comparison points can be researched for other schemes and used comparatively should you wish to pursue CC with another validation scheme. We do not attempt to detail every difference, but rather restrict the document to those commonly used as selection criteria by vendors or sponsors.

Although all three schemes are harmonized through the CCRA so that evaluation and validation work is the same, the various operating policies, processes and procedures often differ and so some variations appear.

Policies can change quickly. We have included links to the source documents so that the reader has an opportunity to verify the current policies.

2 The US scheme new policy notice

How this will effect vendors wishing to certify in the US is currently not clear. However the old policies discussed in this document remain in place until October 2009.

> ***March 16, 2009*** *- Based on the results of evaluations against the Basic and Medium Robustness Protection Profiles and comments from vendors and our customers, NIAP has determined that the current U.S. Protection Profile Robustness model needs to be revised. The model assumed that the same assurance levels could be achieved for every technology. Also, the implementation did not create the necessary test plans and documentation needed to achieve consistent results across different products evaluated in different labs.*
>
> *The security requirements for many technologies are the same for many sectors of Government and industry. For each technology, NSA is creating a Standard Protection Profile, which will replace any corresponding U.S. Government Protection Profile. We will work with industry, our customers, and the Common Criteria community to create these Protection Profiles. The first generation of these Protection Profiles will take into account the current assurance that is achievable for a technology and the Evaluated Assurance Level (EAL) will be set based on the availability of the documentation, test plans, and tools needed to obtain consistent and comparable results.*
>
> *Future increases in the Evaluated Assurance Level (EAL) of each Protection Profile will require more refinement of the assurance criteria, more detailed test plans, and greater disclosure of evaluator evidence, testing performed, and vulnerabilities found. NIAP will work with the Common Criteria community to ensure that Common Criteria 4.0 supports these requirements.*
>
> *All evaluated products will maintain their certification and remain on the NIAP CCEVS Validated Products List (VPL). All on-going evaluations will continue to completion and receive their certification and VPL listing based on their original entry criteria. Over the next few months, the existing U.S. Government Basic Robustness Protection Profiles will be updated to reflect more current functional requirements. Beginning 1 October 2009, NIAP will only accept products into evaluation that comply with either the updated U.S. Government Basic Robustness Protection Profile or with the corresponding new Standard Protection Profile. As each new Standard Protection Profile is published, the old corresponding U.S. Government Protection Profile will be given a 1-year expiration date.*
>
> *When no validated U.S. Government Protection Profile exists and FIPS validation is not appropriate, NSTISSP #11 currently requires that COTS IA and IA enabled IT products be Common Criteria evaluated. Consequently, many products are evaluated against a vendor provided Security Target without any reference to government needs in a validated Protection Profile. NSA and NIAP will pursue revisions to existing U.S. Government policies to only require a Common Criteria evaluated product if a validated U.S. Government Protection Profile exists for that technology.*
>
> *CCEVS will continue to provide updates on the status of the program via the NIAP CCEVS website. Please direct questions to us at scheme-comments@niap-ccevs.org or (410) 854-4458.*

3 General Considerations

Web sites:

CSEC: http://www.fmv.se/WmTemplates/Page.aspx?id=824

BSI: http://www.bsi.de/english/index.htm

CCEVS: http://www.niap-ccevs.org/cc-scheme/

Acceptance of the certificates: all three validation schemes are certificate authorizing signatories to the Common Criteria Recognition Arrangement (CCRA), which is signed by 24 countries. Through the agreement CC evaluation results (up to an evaluation assurance level of EAL4) will be mutually accepted in all countries that have signed the arrangement. For the current list of CCRA participating nations (both certificate producers and consumers), see http://www.commoncriteriaportal.org/theccra.html

In practice this means that most certificates produced by one of the three schemes under discussion will be accepted by any of the member nations. However if you propose an EAL 5 or above project, or it is augmented above EAL4 (A common example of this is vulnerability analysis) then it may be the case that the recognition is not conferred by the CCRA. The organization responsible for sponsoring the CC evaluation may have to make further negotiations with their customer's to determine if this is acceptable or not.

Sponsor factors: In addition to the tangible differences to be considered when selecting a scheme that are listed below, our customers also consider their own internal policies, market requirements,

Current politics: are also often considered. For example one validation scheme may have a travel ban imposed to the country in which product development occurs, and another may not have such a restriction.

Language: The evaluation reports are always written in English. The ST and public documents are always written in English, although translations may be available. Evidence may be in English or another language, but the evaluation team has to be able to understand it and the scheme may ask for translations of key evidence.

4 Specific Considerations

4.1 Validation Costs

The costs of evaluation are levied by the laboratory. atsec's prices for our services do not vary because of the national scheme chosen.

The cost of validation is levied by the validation scheme

CSEC: The certification and licensing services provided by the Certification Body according to the Scheme are mostly provided at a fixed price rate. One exception is re-evaluations, which are charged on an hourly basis when the expected work effort is less than the corresponding fixed price rate.

CSEC publish a document detailing their costs at

http://www.fmv.se/upload/Bilder%20och%20dokument/Verksamhet/CSEC/schemadok/SP-008.pdf

BSI: The cost of evaluation is specified by BSI for the German scheme. Costs are levied at the end of the project, after the certificate has been produced.

BSI publish a document detailing their costs at

http://www.bsi.de/english/experte_costs.pdf

CCEVS: The US scheme currently does not charge a fee for validation, however their holding organization, NIAP, have begun the process (July 2007) in order to start to levy a “fee for service: Information on this is presented on their web site.

4.2 Scheme travel expenses

CSEC: CSEC charge for expenses when travel is required outside of Stockholm. Charging of expenses must be agreed to by the customer and will be conducted in accordance with FMV (Swedish Defence Materiel Administration) travel regulations.

Expenses include actual costs and a per diem compensation. The per diem compensation is in accordance with Swedish tax authority regulations.

BSI: BSI also charge for expenses for attending the site visits. Their travel policy includes first class travel.

CCEVS: CCEVS staff rarely travel. It is not known if travel expenses are levied by the NIAP.

4.3 Tax

CSEC: The applicable VAT (MOMS) will be added to all charges.

BSI: The applicable VAT will be added to all charges. (In most cases atsec can reclaim this tax)

CCEVS: Not applicable.

4.4 Product Restrictions

Each scheme is operated with a degree of influence from their national government. Accordingly various policies about product acceptance can be made on a national basis. Efforts are made to maintain consistency between the national schemes, but this is not always possible. All the schemes will find products destined for their national markets more “interesting” than other products.

CSEC: CSEC prioritize acceptance of products based on their national use.

BSI: BSI prioritize acceptance of products based on their national use.

CCEVS: CCEVS prioritize acceptance of products based on their national use and the inclusion of useful functionality.

In order to reduce costs, the NIAP have implemented a variety of policies over the last few years. Currently, the NIAP will only accept level EAL4 (and above) evaluations for products which must also have a letter of interest (LOI) identifying the Department of Defense (DoD), Intelligence Community (IC) or Department of Homeland Security (DHS) customer who has expressed interest in purchasing the product to be evaluated.

Additionally, the NIAP has specified that Audit Generation functionality is mandatory for a product (see policy letter 13, policy letter 13 (addendum 1) and policy letter 15).

For more information on these NIAP policies, see the policy letters listed at: http://www.niap-ccevs.org/cc-scheme/policy/ccevs/.

4.5 Prerequisites for Evaluation

CSEC: For CSEC, a draft version of the Security Target (ST), an evaluation work plan, an evaluator impartiality and independence justification and an evaluation application (filled out by the developer) is necessary to accept a product into evaluation.

BSI: For BSI, a draft version of the Security Target (ST), and an evaluation application (filled out by the developer) is necessary to request that BSI formally accept a product into evaluation. BSI also ask for a project schedule showing the major milestones to be submitted.

CCEVS: For the CCEVS, the ST must be complete and successfully evaluated against the CEM. The ST must be accompanied by a LOI (see Product Restrictions) and the Sponsor's approval to list products in evaluation (form F8001, see http://www.niap-ccevs.org/cc-scheme/forms/).

In addition, atsec must have already performed a review of the product for compliance to policy letter #10 and #13, and filled out an evaluation application. In order to enter the initial VOR all the product documentation available must be supplied.

In order to be formally accepted as a CCEVS project and issued an ID number the Initial VOR must be performed and passed. CCEVS also expect a project schedule to be submitted.

4.6 Project Progress

CSEC: Nothing established yet – they are currently working on a establishing a policy.

BSI: the procedure to abort evaluations in the German scheme is described in BSI7125, section 2.3.5 and AIS28:

When entering an evaluation, the sponsor/manufacturer accepts the obligation to deliver the product and all required evidence in a timely manner, as agreed in the milestone plan.

If the sponsor/manufacturer is inactive for more than 3 months, the certification body will notify the sponsor/manufacturer in writing that the certification will be aborted within four weeks if they continue to be inactive. The ITSEF will be informed about this decision. The sponsor/manufacturer will be charged the certification cost accumulated up to this point.

CCEVS: The NIAP have a policy about inactive evaluations in policy letter 4 which describes the 30 day notification period to the vendor should the lab notify NIAP that they believe the project is inactive or the final VORs are not scheduled within a reasonable timeframe.

http://www.niap-ccevs.org/cc-scheme/policy/ccevs/policy-ltr-4-update2.pdf

The NIAP also impose time limits on CCEVS Evaluations:

1. EAL 2s will be required to complete evaluation within a 12-month period.
2. EAL 3s and Basic Robustness PP compliant products will be required to complete evaluation within an 18-month period.
3. EAL 4s, augmented EAL 4s and the CCTL evaluation requirements of Medium Robustness PP compliant products will be required to complete evaluation within a 24-month period.
4. Time limits for EAL 5 and above evaluations will be negotiated with the CCTL and the NSA evaluation team prior to the commencement of the evaluation.

The time clock for evaluations begins on the kick-off date
http://www.niap-ccevs.org/cc-scheme/policy/ccevs/policy-ltr-18.pdf

4.7 Initial Kickoff Meeting

CSEC: During the pre-evaluation phase after the certification application is submitted to the Certification Body, all participants (Developer, Sponsor, ITSEF and Certification Body) meet.
The Certification Body uses the certification application deliverables and the initial meeting to decide whether to accept or reject the certification. The Certification Body will request the initial meeting.

BSI: An initial meeting between BSI and the sponsor/developer may be held, as determined by BSI and depending on the size of the TOE.

CCEVS: An initial meeting between the NIAP and the sponsor/developer will be held after the initial VOR (note, the ST must already be evaluated prior to this meeting).

4.8 Validation Oversight

CSEC: Validation is ongoing throughout the project, and evaluation reports are submitted as single evaluation reports. Feedback on these may be obtained before the final Evaluation Technical report is validated.

The result of the examination of an evaluation report is documented in a technical oversight report produced by the certifier and sent to the evaluator. The evaluator SHALL produce the final evaluation report, which SHALL be based on the full set of accepted single evaluation reports, by compiling relevant information.
.

BSI: Validation is ongoing throughout the project, and evaluation reports are submitted as single evaluation reports. Feedback on these may be obtained before the final Evaluation Technical report is validated.

CCEVS: Three Validation Oversight Reviews (VORs) are held during the course of evaluation between the validators and atsec. These three VORs are: initial, test, and final (see http://www.niap-ccevs.org/cc-scheme/policy/ccevs/Final%20VOR%20Guide_2.0_18%20Mar%2008.pdf).

Additional delays might be imposed through additional oversight from the Scheme because of dependencies on Validation Oversight Reviews (VORs). VOR timeslots are limited and must be scheduled in advance.

The developer/sponsor can attend the initial VOR meeting if so desired, but cannot participate. NIAP discourage attendance at the meeting by the developer.

4.9 CC Interpretations

Scheme interpretations may be made on a national level before being harmonized internationally. Therefore some differences may prevail at a given time period. Note that not ALL international interpretations are made public.

CSEC: At the time of publishing there are no Swedish national interpretations of the CC.

If any are published they will be available at http://www.fmv.se/WmTemplates/Page.aspx?id=2270

BSI: BSI have published several interpretations at a national level.

http://www.bsi.bund.de/zertifiz/zert/interpr/ais_cc.htm

CCEVS: US national level public interpretations are found at:

http://www.niap-ccevs.org/cc-scheme/PUBLIC/

4.10 Crypto Policies

Each national scheme has its own policies regarding cryptography in CC

CSEC: The Swedish policy is found at:

http://www.fmv.se/upload/Bilder%20och%20dokument/Verksamhet/CSEC/Scheme%20note%205%20-%20Scheme%20Crypto%20Policy.pdf

BSI:

CCEVS: The US policy is found at:

http://www.niap-ccevs.org/cc-scheme/policy/ccevs/policy-ltr-9-update1.pdf

4.11 Site Visits

CSEC: The evaluator SHALL invite the certifier to attend the site visit well in advance of the scheduled date.
The certifier reserves the right to attend site visits performed by the evaluator.
The certifier shall assess and approve the evaluator's site visit plan before the evaluator conducts the site visit.

BSI: A BSI interpretation (AIS 1) requires that certifiers participate in site visits, and they expect that physical site visits be conducted. In addition, the 31.07.2007 revision of AIS 1 (version 12) specifies: "The audit shall be performed by evaluators who have worked on the evaluation of the relevant developer evidence and the site visit checklist. Exceptions must be justified and agreed with the CB on a case-by-case basis."

CCEVS: CCEVS does not normally participate in site visit, and a national interpretation allows employing alternative site visit means if agreed to by the validation team.

4.12 Certification Phase and Issuance of Certificate

The timing of the certification phase depends on the availability of personnel from the certification body and cannot be influenced or guaranteed by atsec.

CSEC: as soon as possible – no certain common time frame

BSI: Several months after completion of the project a physical certificate is sent my mail. One copy is sent to the sponsor and to atsec.

CCEVS: Certificates are signed after about 6 weeks. The customer then has a choice of having the certificate formally presented at a conference or sent by mail. Two or three events are selected for publicly handing over the certificate each year. These usually include the International Common Criteria Conference, RSA conference in the U.S., and FIAC the Federal Information Assurance Conference. If certificates are requested by mail they are framed and mailed to the sponsor.