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

Fiona Pattinson, Ken Hake,
Gerald Krummeck, Staffan Persson

October 29th, 2013

Table of Contents:

Introduction

The intended audience for this document is any organization interested in pursuing Common Criteria (CC) certification using atsec as the certification laboratory that has not yet selected a national scheme to perform validation and certification.

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 three validation schemes with which atsec is accredited in order to perform Common Criteria evaluations, which are the following:

- the United States **Common Criteria Evaluation and Validation Scheme** (CCEVS) operated by the National Information Assurance Partnership (NIAP),
- the Swedish **Sveriges Certifieringsorgan för IT-Säkerhet**, (CSEC) and
- the **German Bundesamt für Sicherheit in der Informationstechnik** (BSI).

Although in this document we restrict ourselves to these three schemes, the points documented in this paper can be researched for other schemes and used comparatively should you wish to pursue CC evaluation with another validation scheme. We do not attempt to detail every difference between the schemes, but restrict the points discussed in this document to those commonly used as selection criteria by vendors or sponsors of evaluation projects.

Although all three schemes are harmonized through the CCRA so that evaluation and validation work meet a common minimum level, the various operating policies, processes and procedures often differ and so some variations between the validation schemes emerge.

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

General Considerations

Web sites:

CCEVS: https://www.niap-ccevs.org/

CSEC: http://www.fmv.se/csec

BSI: https://www.bsi.bund.de/EN/Topics/Certification/certific.html

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 this agreement, CC evaluation results (up to and including 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/ccra/

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 if it is augmented above EAL 4 (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 to determine if this is acceptable or not.

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

Current politics are also often considered. For example, one validation scheme may have a travel ban imposed on 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 Security Target (ST) and public documents are also 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.

Specific Considerations

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, although if the amount of effort varies because of national policies, this may be a factor.

The cost of validation is levied by the validation scheme.

CCEVS: The U.S. scheme currently does not charge a fee for validation. This was discussed by NIAP in 2007, but to date has not been implemented.

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 published a document detailing their costs at:
http://fmv.se/Global/Dokument/Verksamhet/CSEC/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 published a document detailing their costs at:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/exparte_costs_pdf.pdf?__blob=publicationFile

Scheme Travel Expenses

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

CSEC: CSEC charges 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 Defense 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 charges for expenses for attending the site visits. Their travel policy includes first class travel.

Tax

CCEVS: Not applicable.

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.)

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 of the schemes will find products destined for their national markets more “interesting” than other products.

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

In order to reduce costs, NIAP has implemented a variety of policies over the last few years. Currently, NIAP will only accept evaluations which claim compliance to a NIAP-approved protection profile (Policy Letters 10 and 12); if no protection profile exists, the vendor should contact the CCEVS office for guidance.

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

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

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

Prerequisites for Evaluation

CCEVS: The formal application process now consists of a new “Check In” process which includes an ST review and multiple Sync sessions (Initial, Guidance, and Final). This new process is being introduced in parallel as the current VOR evaluations are completed.

In addition, atsec must have already performed a review of the product for compliance to policy letters #10 and #12, and filled out an evaluation application.

For CCEVS, the Security Target (ST) must be complete and successfully evaluated using the CEM (ASE).

Note that, where applicable, the CCEVS also requires an entropy assessment report.

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

Project Progress

CCEVS: NIAP has a policy about inactive evaluations. Policy Letter #4 (http://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-4-update3.pdf) 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.

NIAP also imposes time limits on CCEVS evaluations (http://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-18-update1.pdf):

- All evaluations will be required to be completed within 12 months
- If an EAL4 exception exists, that time limit is extended to 24 months

The time clock for evaluations begins on the kick-off date.

CSEC: Nothing is established yet – they are currently working on 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.

Initial Kickoff Meeting

CCEVS: A check-in meeting will be scheduled two weeks after the required check-in package is submitted.

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.

Validation Oversight

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, though the VOR process is being phased out in favor of the Check In process. (See https://www.niap-ccevs.org/Documents_and_Guidance/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) or Sync Sessions. VOR timeslots/Sync Sessions are limited and must be scheduled in advance.

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.

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.

CCEVS: U.S. national level public interpretations are found at: http://www.niap-ccevs.org/Useful_Links/PUBLIC/

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

If any are published in the future, they will be available at http://www.fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/Documents/Interpretations/

BSI: BSI has published several interpretations at a national level: https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/AISCC/ais_cc.html

Crypto Policies

Each national scheme has its own policies regarding cryptography in CC.

CCEVS: The crypto requirements are established in the individual Protection Profiles.

CSEC: The Swedish policy is found at: http://www.fmv.se/Global/Dokument/Verksamhet/CSEC/SP-188.pdf

BSI: BSI does not have a general crypto policy, but the Bundesnetzagentur publishes a list of approved algorithms in regards to digital signatures: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile

Site Visits

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

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."

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.

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, the RSA conference in the U.S., and the Federal Information Assurance Conference (FIAC). If certificates are requested by mail, they are framed and mailed to the sponsor.

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

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

The U.S. Scheme Policies Changes

The U.S. is currently updating its policies surrounding information assurance and IT product certification.

Committee on National Security Systems Policy 11

The CNSSP-11 is the NATIONAL POLICY GOVERNING THE ACQUISITION OF INFORMATION ASSURANCE (IA) AND IA-ENABLED INFORMATION TECHNOLOGY PRODUCTS. This policy governs acquisition of Information Assurance and IT products. It replaces the former NSTISSP - 11 policy. The CNSSP-11 policy states that COTS products must comply with NIAP program requirements and with FIPS cryptographic validation. U.S. government agencies are required to select products first from Commercial Off the Shelf products and then Government Off the Shelf products.

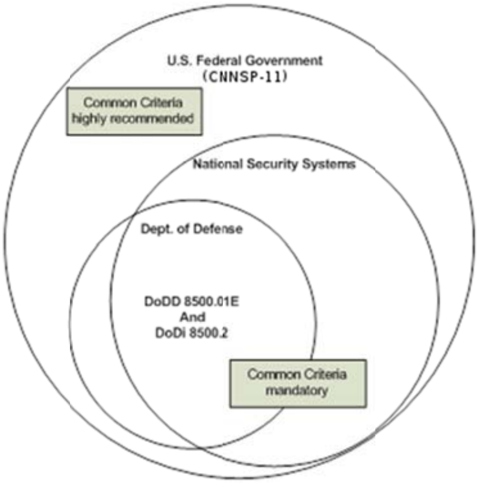
Agencies are also required to participate in developing protection profiles.

The policy also outlines specifics that NSA, NIAP, agency heads are responsible to do. The policy is listed here: https://www.cnss.gov/Assets/pdf/CNSSP-11.pdf.

DoDD 8500.01E, and **DoDI 8500.2** give the National Security Agency (NSA) the responsibility for establishing criteria and processes for evaluating and validating all IA and IA-enabled IT products used in DoD information systems.

Pending the planned updates to these policies, the DoD has provided a memorandum, dated September 14th, 2010, that gives interim guidance for IA acquisition. This document is a key policy which shows that NIAP can supervise product evaluation under the following circumstances:

- For products claiming compliance against a U.S. government approved protection profile and,
- When a U.S. approved Protection Profile does not exist and a government agency requests a Common Criteria evaluation, NIAP will consider accepting a product into evaluation at EAL2 only. Validator resource availability and customer need (as specified in a "Letter of Intent" (LOI)) will serve as the basis for acceptance.


U.S. Federal Government
(CNNSP-11)
Common Criteria highly recommended
National Security Systems
Dept. of Defense
DoDD 8500.01E And DoDi 8500.2
Common Criteria mandatory

The net effect of these U.S. policies and the restricted resource available to enable them is to make initiating evaluation projects under the CCEVS somewhat problematic. Until a full range of U.S. approved Protection Profiles are deployed, it will remain difficult to get a product accepted into evaluation by the CCEVS. For the population of federal end-user systems that are not designated as national security systems, providing the security assurance highly recommended by CNNSP-11, to address the risks of specifying COTS can only be achieved by performing evaluation projects under non U.S. schemes

- A current list of approved PPs is given on the NIAP web site at http://www.niap-ccevs.org/pp/