First meeting

Swedish Certification body for IT Security

Introduction

Who we are

- Angelica Lundin - Account Manager and Administrator
- Mats Engquist - Chief Operating Officer

What we do

- We are CSEC, the Swedish Certification body for IT-security
- CSEC oversees evaluations and issues certificates, if all goes well
- The Certification body is described in document SP-001 which can be found on our website

Who are you?

The certification approach

- The **Sponsor** pays for the certification and is our customer
- The **Developer** develops the product
- The Sponsor is responsible for meeting the requirements for certification, but the Developer does the actual job
- The **Evaluator** performs the evaluation by review and testing
- The **Certifier** oversees the evaluation
- The Evaluator reports to the Certifier at the Certification body
- After successful evaluations/certifications, the **Certification body** may issue certificates
- The evaluation and certification is described in the document SP-002

Project timeline

The effect of a certification

A certification can take anywhere from a few months to a few years, from start to finish.

Most customers expect a certification to result in a certificate.

However, to succeed with a certification, the Developer will most certainly need to update the product/Target of Evaluation and/or the documentation to meet the requirements of Common Criteria and any claimed Protection Profile!

Key factors for CSEC

- Incoming and complete applications are handled in the order they arrive
- Incoming reports are handled according to the plan agreed with the Evaluator
  - Our goal is to review, and reply to, any incoming reports within 10 working days
  - If this is not possible, or if the evaluations is planned in another way, we keep the evaluator informed about when we expect to reply
- In case of delays:
  - Reports are handled in the order they arrive
- Queues may appear in case of high workload and are handled according to our Policy for Certification Queues, SP-184.
- Since most of the work is performed by the Developer and the Evaluator, time for completion of a certification mostly depends on the Developer and the Evaluator.
- The Certification body is impartial and is not allowed to act on requests to prioritize.

The impact of Iterations

Incomplete reports increase the number of iterations…

… and iterations will slow the project down. It is therefore crucial that evaluation reports delivered to the Certification body are correct and complete, every time.

We recommend the evaluator, and the internal quality assurance within the ITSEF, to “think like a certifier” prior to sending reports to the certification body.

Roles within the Certification body

- The **Lead Certifier** is responsible for the certification and usually performs the majority of the certification work.
- For every certification we assign a **Certifier team** who will cooperate during the certification.
- The team consists of a Lead Certifier and one another Certifier. The team member may, at any time, take over as lead.
- Peer review is normally carried out by the **Certifier** in the team.
- The **Account Manager** is responsible for the communication between the Certification body and the Sponsor and the Developer.
- The **Administrator** acts as a Project Administrator.
- The **Chief Operating Officer** is responsible for coordinating resources in certifications.

Estimating effort

- It is difficult to estimate the effort for an evaluation and certification.
- The planned certification effort is based on the evaluation assurance level and the complexity of the product.
- The actual effort rather tends to be based on the experience of the customer.
- The Evaluator and Certifier can never guarantee that an evaluation project will result in a successful certification, since they are required to maintain strict independence.
- The quality objective of the Certification body is to deliver reports within 10 working days after receiving the material to be reviewed, or within the time frame communicated from the Certifier to the Evaluator.
- Requests on speeding up this process will not make the reviewing go any faster.

Updated documentation

- Updates in our SP-documents are valid immediately after we make them public at http://fmv.se/csec and send the information about the changes to the Evaluators.
- We obviously want the Evaluator to work according to the valid versions of the documents and the routines, immediately after they have been published. It is however rare that the changes affect the certification projects retroactively.
- An exception would be changes regarding our prices, these are always published long before the changes are actually valid. This gives potential Sponsors and developers time to adjust to the upcoming price change.

Confidentiality

Documents received or written by the Certification body are official documents. These may be kept secret by the Certification body only when it is required to protect the interests covered by articles in The Swedish Law on Publicity and Secrecy regarding the following:

- The security of the realm or its relationships with another state or international organisation
- Inspection, control, or other supervisory activities of a public authority
- The prevention or prosecution of crime
- The economic interests of the public institutions
- The protection of the personal or economic circumstances of private subjects

Information handled during certifications will be classified according to this!

Managing information

The arrangements below only cover how CSEC manages information. The sponsor and the evaluation facility should agree on appropriate arrangements for their own information handling.

The following documents are unclassified by default, i.e. no particular protection will be applied

- The Certification application form
- The Tender
- The administrative information exchange between CSEC, the evaluation facility, and the sponsor/developer
- The final version of the Security Target (approved for publication by the sponsor)
- The Certification Report and the certificates

Encryption

- Classified information on paper as well as in electronic form on a computer will be kept in a safe when not in use.
- Digital files will always be encrypted using equipment approved for government use, when stored or transmitted in environments accessible to people outside the certification body.
- Classified information should always be transmitted through crypto approved for government use. The evaluators have access to such programs.
- The drafts of the certification report and the certificates will be sent by e-mail to the sponsor and the evaluator for review. These will be considered OPEN documents.

Scheme Notes

These Scheme Notes are always mandatory:

- *Scheme Note 15*, which is a CC interpretation regarding minimal test coverage and will affect the ATE part of the evaluation.
- *Scheme Note 18*, which is an interpretation of the content requirements on ST's and will affect the ASE part.

Other Scheme Notes and/or technical documents might be applicable for specific certifications. The developer will be informed about this.

All relevant documents can be found at http://fmv.se/csec.

Laws and regulations

The operations of the Certification body is governed by:

- ISO/IEC 17065
- Act concerning Technical Conformity Assessment
- The Secrecy Act
- The Freedom of the Press Act

When Site visits and testing oversight is relevant

CSEC as a part of a Swedish authority will not sign any NDA (Non Disclosure Agreement).

Fees

The fees for the certification consists of:

- The application fee, which is always the same
- The certification fee, which is calculated from the EAL and the complexity of the product
- Travel expenses, if any

The fees are invoiced in the following way:

- Application fee: Immediately after receiving the application
- Certification fee and travel expenses: After concluding the certification

Invoicing

Invoices from FMV are sent through physical mail and not electronically. If you wish to receive an invoice in PDF – let us know. Always provide us with the correct invoicing address!

It is common for sponsors to choose to handle the invoicing through the evaluator.

This often simplifies the administration for foreign sponsors – receiving an invoice from a private company is often less complicated than an invoice from a government. In this case, the invoice is sent to the evaluation facility, who then pays the specified fee and sends a new invoice to the sponsor. Both the certification body and the evaluators has to be informed by the sponsor that this is how the invoicing should be handled.

During the summer

The Swedish summer vacation takes place around late June to early August each year.

During this time

- Reports will not be reviewed when the Certifier is on vacation
  - Since the review requires the presence of the Lead Certifier
- Certification decisions may be delayed until after the vacation period
  - Since most of CSEC has to be present to make such a decision
- Ambitions to speed up the certification process before vacations often slows the process down
  - Because stressing typically results in lower quality

During the winter

In Sweden we go for vacation also during Christmas and New years.

The impact is the same as for the summer but for a shorter period, approx. December 23rd to January 8th.