Swedish Certification Body for IT Security

191 Cross Frontier Evaluation

Issue: 7.0, 2019-01-16

Authorisation:Dag Ströman, Head of CSEC

Table of Contents

1 Preface

This document is part of the description of the Swedish Common Criteria Evaluation and Certification Scheme ("the Scheme").

The Scheme has been established by the Swedish Certification Body for IT Security (CSEC) to evaluate and certify the trustworthiness of security features in IT products and the suitability of protection profiles (PP) to define implementation-independent sets of IT security requirements.

The objectives of the Scheme are to ensure that all evaluations are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and protection profiles; to improve the availability of evaluated IT products and protection profiles; and to continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles.

This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. This document is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of IT systems for which security is a consideration, as well as those already involved in the Scheme, i.e., Scheme employees, evaluators, current customers, contractors, and security consultants.

The Scheme documents and further information can be obtained from the Swedish Certification Body for IT Security here:

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: SE-115 88 Stockholm, Sweden
Visiting address: Banérgatan 62

Telephone: +46-8-782 4000 E-mail: csec@fmv.se
Web: www.csec.se

1.1 Purpose

This document provides the conditions for an IT Security Evaluation Facility (ITSEF) seeking to perform evaluation activities outside Sweden ("Cross Frontier Evaluation").

1.2 Terminology

Abbreviations commonly used by CSEC are described in SP-001 *Certification and Evaluation - Scheme Overview*

The following terms are used to specify requirements:

SHALL	Within normative text, “SHALL” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).
SHOULD	Within normative text, “SHOULD” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

MAY	Within normative text, “MAY” indicates “a course of action permissible within the limits of the document.” (ISO/IEC).
CAN	Within normative text, “CAN” indicate “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).

2 Scheme Policy - Cross Frontier Evaluations

2.1 Critical Location

Licensed ITSEFs SHALL identify those physical locations, whatever the composition (office, person etc.) or legal relationship (contractor, franchisee etc.) of such location with the ITSEF, where evaluation activities are conducted or controlled that determine or demonstrate the effectiveness of the ITSEFs in accordance with the Scheme, in particular:

- the process for initial qualification, training and ongoing monitoring of evaluators and evaluators personnel records; or
- the decision to perform the evaluation and/or the assignment of evaluators; or
- review of the final evaluation report and the overall evaluation verdict by the lead evaluator; or
- housing the main repository and archiving of any and all records associated with the evaluation.

A physical location where any of the above ITSEF activities are carried out is referred to as “Critical Location”.

Critical Location(s) SHALL be situated within Sweden and be subject to the licensing procedures of the Scheme.

All Critical Locations SHALL be assessed by CSEC at the Swedish Defense Materiel Administration (FMV/CSEC) on site to confirm that the licensed service of the ITSEF may be offered resulting from the work at the Critical Location.

In particular, FMV/CSEC is to assess the effectiveness of the management control, by the licensed ITSEF, over the activities of its Foreign Locations.

2.2 Foreign Location

FMV/CSEC may approve that evaluation activities/processes which are not reserved for Critical Location are performed at a location outside Sweden (referred to as "Foreign Location").

In such case:

- The scope of evaluation activities performed at Foreign Location SHALL be documented in the ITSEF quality management system.
- The ITSEF and associated Foreign Location SHALL fulfill the requirements for evaluation facilities licensed under the Scheme.
- The licensed ITSEF SHALL provide documentation that demonstrate ITSEF and Foreign Location (within claimed scope of operation) requirement fulfillment, including initial requirements, management requirements, staff requirements and security requirements defined in *SP-004 Licensing of Evaluation Facilities*. Such documentation SHALL be up-to-date and subject to configuration management.

Upon request from a licensed ITSEF, FMV/CSEC may assess whether the ITSEF and associated Foreign Location fulfill the Scheme requirements. This assessment will be based on documentation provided by the ITSEF and may include interviews and/or site visits. An assessment fee will be charged in accordance with SP-008 *Charges and Fees*. FMV/CSEC may on request provide a preliminary estimate of the expected total cost once a complete set of documentation has been provided.

If the Scheme requirements have been fulfilled, FMV/CSEC may grant written approval and evaluation activities may then commence in the Foreign Location in accordance with the documented scope.

2.3 Performing Cross Frontier Evaluations

The Evaluation Work Plan (EWP) shall denote all evaluation activities that are performed in Foreign Locations or at the developer site.

The Sponsor and the Developer SHALL approve any evaluation activities to be performed in Foreign Locations.

Unless otherwise has been agreed with FMV/CSEC, evaluator testing activities associated with the assurance class test (ATE) and assurance class vulnerability assessment (AVA) SHALL be performed at a Critical Location or at the developer site.

Unless otherwise has been agreed with FMV/CSEC, the First meeting SHALL be performed at the Certification Body, the Critical Location or at the developer site.

Evaluation activities SHOULD be restricted to Critical Location, Foreign Location and/or developer site.

Any and all records and transmissions associated with the evaluation SHALL be protected in accordance with the rules of the Scheme.

Final Evaluation Report (FER) and Certification Report SHALL identify all locations that have been involved in an evaluation.

2.4 Cross Frontier Assurance Continuity

In addition to the requirements concerning evaluations stated elsewhere in this document, the following requirements apply to Certificate Maintenance and Re-Evaluation activities.

- The Sponsor SHALL have a contract with an ITSEF (Critical Location).
- The description of changes to the certified target of evaluation (TOE) MAY be compiled at the Foreign Location.
- The impact of those changes on the assurance baseline SHALL be determined at the Critical Location.

3 Questions and Answers

What is the purpose of this policy?

FMV/CSEC has been asked whether foreign evaluation facilities are accepted within the Swedish Scheme. We have found that the cost of overseeing a foreign ITSEF is likely to create significant overhead cost compared to our oversight of ITSEF established in Sweden. The spirit of this policy is that FMV/CSEC may allow evaluation activities to be performed in a well-managed and controlled Foreign Location under the supervision and ultimate responsibility of an ITSEF being established within Sweden. The intent is that significant parts of the evaluation activities can be done in Foreign Location, while FMV/CSEC oversight would be concentrated to the licensed ITSEF Critical Location in Sweden and the developer site.

Is it necessary to perform a trial evaluation at the Foreign Location?

No, this is not necessary. A licensed ITSEF has demonstrated that it is competent to perform CC evaluations in accordance with the Scheme. Under the license, the ITSEF is responsible for continuing to adhere to the Scheme and for assuring that evaluation activities performed in Foreign Location are carried out using appropriate documented procedures by staff that has the necessary competence and training.

What are the requirements for how inclusion of a Foreign Location in an ITSEF needs to be documented?

The ITSEF, its personnel and activities performed within the scope of the license shall demonstrate that it complies with the Scheme requirements, in particular SP-004 *Licensing of Evaluation Facilities*. The ITSEF documentation must demonstrate how the general requirements, quality requirements, security requirements, competence requirements and requirements on management of subcontractors are fulfilled at both Critical and Foreign Location. The ITSEF documentation must demonstrate how it ensures that activities, responsibilities and decisions that are reserved for Critical Locations only are performed there.

Does a Foreign Location need to be 17025 accredited?

Not necessarily. All evaluation activities performed at a Foreign Location, within the Scheme, SHALL be covered by the accreditation of the licensed ITSEF of which the Foreign Location is a part.

The Foreign Location itself need not be accredited but if the Foreign Location is not accredited, it is the ITSEF's responsibility to ensure that the evaluation work performed at the Foreign Location meets the standards set up by the accreditation.

If the Foreign Location is not accredited, FMV/CSEC may choose to extend the license assessment, and license surveillance, to cover more aspects of the ISO/IEC 17025.

Does the actual training activities of evaluators and other staff need to be carried out in Critical Location?

No, not necessarily. The policy mandates that management of qualification and training of evaluators is carried out at Critical Location, but the actual training activities may be carried out elsewhere, e.g., courses could be held at other places than Critical Location.

Does the evaluator qualification testing (interview and written test) have to be performed in Sweden?

We prefer that arrangements are made in such order that the evaluator qualification is done either at FMV/CSEC office or at other locations in Sweden. However, we are open to discussion of other options, including that interviews are performed via video conference or phone. We can also accept that the written exam is made in other locations (including the Foreign Location) under the supervision of a trusted person whom CSEC has agreed to oversee the test. The Head of a licensed ITSEF is one such trusted person, as well as senior managers of Foreign Locations having appropriate agreement with the licensed ITSEF.

What more precisely is meant by "measures of effectiveness" of the management control ... over ... Foreign Locations'" that FMV/CSEC would be looking for?

The Critical Location is by and large responsible for ensuring that the evaluation is being performed by competent evaluators, following appropriate processes and delivering sound and reasonable verdicts. The overall evaluation verdict based on the review of the final evaluation report is the sole responsibility of staff associated with the Critical Location. FMV/CSEC will monitor that the licensed ITSEF fulfills this responsibility and that processes are applied with well-defined responsibilities in Foreign Location. This in order to ensure that there will be no difference in quality or conclusions in evaluations, regardless of if evaluation activities are being performed at Critical Location or at the Foreign Location.

Can the First Meeting be held via tele-conference or video-conference?

In principle - Yes. However, performing evaluations is always a complex task, in particular when stake holders are being separated geographically. FMV/CSEC therefore believe that face-to-face meetings are a valuable instrument to make people achieve mutual respect and reach common understanding. FMV/CSEC will in good faith be reasonably flexible, but will ask that there are opportunities where evaluators, developers, certifiers and other stake holders in an evaluation meet at the same physical location. This will be of particular importance when a new Foreign Location is being established.

Do Scheme rules allow the use of PGP, SSL/TLS/HTTPS to provide protection?

Communications between the ITSEF and its stakeholders may rely on well established and accepted security protocols and tools, provided that the ITSEF has informed the stakeholders that such tools will be used, and that the stakeholders accept their use. FMV/CSEC will oversee that the ITSEF and Foreign Location apply good management and best practice to secure information, and may comment when we find weaknesses or generally unacceptable risks.

Communication between FMV/CSEC and other stakeholders of the Scheme can only be based on use of crypto solutions that has been approved for such use by FMV/CSEC.

Information which is attracting a national or international security classification or equivalent protective marking may be subject to other more specific security regulations. It is the responsibility of the ITSEF to know and adhere to such regulations in these cases.

Can the Foreign Location keep local copies of confidential information after the completion of an evaluation?

The licensed ITSEF is responsible for keeping all confidential information protected during and after the evaluation in accordance with the Scheme and as agreed with the evaluation stake holders. The ITSEF is responsible for that appropriate legal arrangements are in place to ensure that individuals and/or organisations involved in an evaluation fulfill the Scheme requirements. Only staff associated with the ITSEF (Critical and/or Foreign Location) or otherwise having relevant authorization should have access to such information. It should be noted that a complete repository of the evaluation is to be physically located in Critical Location.