003 Assurance Continuity

Issue: 14.0, 2017-Nov-09

Authorisation: Mats Engquist, Quality Manager, CSEC
Table of Contents

1 Preface 3
  1.1 Purpose 3
  1.2 Typography 3

2 Introduction 4
  2.1 Basic concepts 4
  2.2 Characterisation of Changes 4
  2.3 Scheme-specific requirements 4

3 Assurance Continuity Process 5
  3.1 Application 5
  3.2 Application reception and review 5
  3.3 Certificate maintenance 5
  3.4 Re-evaluation 6

4 Impact Analysis Report (IAR) 7
  4.1 Introduction 7
  4.2 Description of the Change(s) 8
  4.3 Affected Developer Evidence 8
  4.4 Description of the Developer Evidence Modifications 8
  4.5 Conclusions 8
  4.6 Annex: Updated Developer Evidence 8
1 Preface

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

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. Complete contact information is provided in the following box.

<table>
<thead>
<tr>
<th>Swedish Certification Body for IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMV / CSEC</td>
</tr>
<tr>
<td>Postal address: SE-115 88 Stockholm, Sweden</td>
</tr>
<tr>
<td>Visiting address: Banérgatan 62</td>
</tr>
<tr>
<td>Telephone: +46-8-782 4000</td>
</tr>
<tr>
<td>E-mail: <a href="mailto:csec@fmv.se">csec@fmv.se</a></td>
</tr>
<tr>
<td>Web: <a href="http://www.csec.se">www.csec.se</a></td>
</tr>
</tbody>
</table>

1.1 Purpose

The purpose of this document is to describe the procedures for assurance continuity within the Scheme and provides detailed information about the assurance continuity procedures and the responsibilities of each party involved.

General information about the Scheme is published in Scheme publication SP-001 Certification and Evaluation Scheme - Scheme Overview.

1.2 Typography

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” indicates “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).
2 Introduction

This document defines an approach to assurance continuity that is in accordance with the procedures agreed for mutual recognition under CCRA. Assurance continuity provides the means to extend the validity of a Common Criteria certificate to an updated version of the certified product (more specifically the certified TOE) without having to perform a fully new certification.

The requirements and procedures for assurance continuity described in this document are based on the CCRA document Assurance Continuity: CCRA Requirements, Version 2.1, June 2012.

Where nothing else is specifically stated the procedures and requirements in the CCRA-documents are applicable to Assurance Continuity also in the Swedish Common Criteria Evaluation and Certification Scheme.

2.1 Basic concepts

Assurance continuity can be performed as certificate maintenance or as a re-evaluation.

Certificate maintenance is applicable when the changes to the certified TOE, its IT environment and/or its development environment can be shown to have minor impact on the assurance baseline.

If the developer cannot, or chooses not to, show that the impact of the changes is minor, a re-evaluation is performed.

2.2 Characterisation of Changes

Characterisation of changes are performed according to the procedures and requirements described in the CCRA document Assurance Continuity: CCRA Requirements, Version 2.1, June 2012.

2.3 Scheme-specific requirements

In addition to the requirements stated in Assurance Continuity: CCRA Requirements, Version 2.1, the following scheme-specific requirements may apply:

- Preparation of the IAR and application for certificate maintenance or re-evaluation SHALL be made by an ITSEF, licensed by the Certification Body, contracted by the developer/sponsor.
- Additional criteria for when changes to the certified TOE are considered to be minor may be issued by the Certification Body. Such criteria may be issued as Scheme Notes and may be changed at any time.
3 Assurance Continuity Process

3.1 Application
The start-up of the assurance continuity process is similar to a normal evaluation and certification process. The ITSEF on behalf of the Sponsor SHALL submit to the Certification Body:

- an application for maintenance or re-evaluation using Scheme publication SP-196 Certification Application with Terms - Form (Or SP-199 Certification Application with Terms (FMV) - Form, for customers within FMV)
- impact analysis report (IAR)
- the certified security target
- the corresponding certification report
- developer test documentation
- if re-evaluation: an evaluation work plan (EWP)
- if there are specific circumstances, an evaluator impartiality and independence justification.

All the documents identified above are referred to as the assurance continuity application deliverables and SHALL be delivered with the application for maintenance or re-evaluation. The application is considered complete when all the documents identified above have been delivered to the Certification Body in a finalised version or in a draft version that meets the requirements of the certification review process.

The content requirements for the IAR are described in chapter 4 Impact Analysis Report (IAR).

If the application is for certificate maintenance, the description of the changes to the certified TOE should list all changes made to the TOE and show that the resulting impact on the assurance baseline is minor.

If the application is for a re-evaluation, the description of the changes to the certified TOE should focus on the changes in developer evidence and the consequent scope of the re-evaluation.

3.2 Application reception and review
An application fee will be charged upon reception of the application, see SP-008 Charges and fees.

The certification body will review the application and may require additional or changed documents to be delivered.

Based on the results of the application review, the certification body will determine

- Whether the reported changes to the certified TOE are to be considered minor or major, i.e. whether certification maintenance or re-evaluation will be performed
- The proposed fee for the certification maintenance or re-evaluation, which will be charged after completion of the assurance continuity project
- When the project can be started

3.3 Certificate maintenance
If the development environment has been changed, the evaluator will perform a subset evaluation and submit a report.
The certifier will review the IAR and other submitted documents to confirm that the changes made to the certified TOE and/or the development environment have not adversely affected the assurance baseline.

The certifier will then publish a maintenance addendum and a Maintenance Report in the list of certificates issued by CSEC on www.csec.se.

The maintenance addendum serves to include the changed version of the TOE in the original certificate.

The Maintenance report is based on the IAR and is considered an addendum to the original Certification Report.

Maintenance may, in general, continue for up to 2 years beyond the certification date.

The certificate body may, as circumstances warrant, either lengthen or shorten this maintenance period, based on the IT product type and the needs of the consumer.

3.4 Re-evaluation

Re-evaluation is performed in the same way as a complete evaluation taking into consideration only those components determined to be affected by the changes.

The evaluator submits one or several evaluation reports. The certifier will review these and prepare a technical oversight report (TOR).

After concluded evaluation, the Certification Body will issue a new certificate and Certification Report for the changed TOE.

This changed TOE becomes the updated basis for any future charges that might be made.
4 Impact Analysis Report (IAR)

This chapter describes the minimum content of the Impact Analysis Report. The contents are portrayed in Figure 2; this figure may be used as a guide when constructing the structural outline of the document. The Impact Analysis Report is a required input for the assurance continuity process.

Throughout the following description, for "the developer" read "the developer or the ITSEF on behalf of the developer".

![Impact Analysis Report Diagram]

### 4.1 Introduction

The developer shall report the Impact Analysis Report configuration control identifiers. The Impact Analysis Report configuration control identifiers contain information that identifies the Impact Analysis Report (e.g. name, date and version number).

The developer shall report the current TOE configuration control identifiers. The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the certified TOE.

The developer shall report the configuration control identifiers for the FER, CR, and the certified TOE. These configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.
The developer shall report the configuration control identifiers for the version of the ST related to the certified TOE.

The developer shall report the identity of the developer. The identity of the TOE developer is required to identify the party responsible for producing the TOE, performing the impact analysis and updating the evidence.

The developer may include information in relation to legal or statutory aspects, for example related to the confidentiality of the document.

4.2 Description of the Change(s)

The developer shall report the changes to the product. The identified changes are with regard to the product associated with the certified TOE.

The developer shall report the changes to the development environment. The identified changes are with regard to the development environment of the certified TOE.

4.3 Affected Developer Evidence

For each change, the developer shall report the list of affected items of the developer evidence. For each change to the product associated with the certified TOE or to the development environment of the certified TOE, any item of the developer evidence that need to be modified in order to address the developer action elements shall be identified.

4.4 Description of the Developer Evidence Modifications

The developer shall describe briefly the required modifications to the affected items of the developer evidence. For each affected item of the developer evidence, the modifications required to address the corresponding content and presentation of evidence elements shall be briefly described.

4.5 Conclusions

For each change the evaluator shall report if the impact on assurance is considered minor or major.

For each change the evaluator should provide a supporting rationale for the reported impact. In the event that the change is to the development environment, the rationale will show that there is no follow-on impact on other assurance measures.

The evaluator shall report if the overall impact is considered minor or major. The evaluator should include a supporting rationale, taking the accumulation of changes into consideration.

4.6 Annex: Updated Developer Evidence

The developer shall report for each updated item of developer evidence the following information:

- the title;
- the unique reference (e.g. issue date and version number).

Only those items of evidence that are notably changed need to be listed; if the only update to an item of evidence is to reflect the new identification of the TOE, then it does not need to be included.