Swedish Board for Accreditation and Conformity Assessment's Regulations

SWEDAC

ISSN 1400-4682

Editor: Kari Björkqvist

STAFS 2007:21
Printed
28 November 2007

The Swedish Board for Accreditation and Conformity Assessment's (SWEDAC) Regulations and General Guidelines for Accredited Bodies that Certify IT-security;

ratified on 28 November 2007.

In accordance with 9 § of the Conformity Assessment Ordinance (2005:894), the Swedish Board for Accreditation and Conformity Assessment hereby decides on the following regulations and guidelines.

Scope

1 § These regulations apply to bodies that are accredited or bodies applying for accreditation by SWEDAC to certify IT products, system and protection profiles.

These regulations are a supplement to SWEDAC´s regulations (STAFS 2007:7) and general guidelines for accreditation and SWEDAC´s regulations (STAFS 2007:12) and general guidelines for the accreditation of bodies that certify products.

Definitions

2 § These regulations use the definitions given in:

1. SS-EN 45011:1998 – *General requirements for bodies operating product certification systems (ISO/IEC Guide 65:1996) and,*
2. SIS Handbook 550 – *Terminology for information security.*

Definitions used in these regulations:

Evaluation Facility	Organisation or part of an organisation evaluating products.
Evaluation Technical Report	Detailed technical report presenting evaluation results.
Certification/Validation Report	Report issued by the accredited certification body. The document summarises the results from the evaluation and affirms the total result. It also affirms that the evaluation methods and procedures have been used in an applicable way.

Requirements for Accreditation

3 § According to 4 § in SWEDAC´s regulations (STAFS 2007:12) and general guidelines for the accreditation of bodies that certify products, normative documents used for accredited certification shall be unambiguous, available to the public and accepted by SWEDAC and concerned interested parties.

General Guidelines to 3 §

The normative documents may e.g. be an edition of ISO/IEC 15408 or the international standard Common Criteria (CC). Applicable normative documents are defined in the scope for accreditation.

Approved evaluation facilities (clause 4.4 in SS-EN 45011:1998)
The certification body's policy concerning approval of evaluation facilities defines the procedures for this approval.

Certification body (clause 4.2 and 5 in SS-EN 45011:1998)
To perform an evaluation the team should represent relevant competence and experience in both information security and IT. It shall also have knowledge about the specific sector where the evaluated product is intended to be used.

4 § An accredited certification body shall have taken immediate measures to secure that information security is handled in a satisfactory way. This also includes protection of information that the certification body has received from customers and suppliers.

General guidelines to 4 §

An example of a well-structured way of working to secure the handling of information security is presented in ISO/IEC 27001:2006 - Information security management systems - Requirements. The chosen security level should reflect the results of the risk analyses performed. Risk analyses should be performed on the basis of requirements in current legislation and from a business perspective.

The above is based on the need of protection for handling trade secrets and other information worth protecting (i.e. concerning the evaluation task itself) reflecting the evaluated product/system.

Wording of Certificate

5 § An issued certificate shall contain information according to Appendix 1 in these regulations.

General guidelines to 5 §

Certification reports should contain headings and information concerning certification according to Appendix 2 in these regulations.

Miscellaneous

6 § In individual cases and if special circumstances so require, SWEDAC may grant dispensation from these regulations.

These regulations come into force on 28 November 2007.

On behalf of SWEDAC

HANS-ERIC HOLMQVIST

Roland Jonsson

Appendix 1

Wording of Certificate

Certificate Related to Validation of an IT-product

A certificate, or belonging report, issued by an accredited certification body resulting from the certification/validation of an IT product evaluation is to include the following information:

1. Product Manufacturer,
2. Product Name and Model,
3. Type of Product,
4. Version and Release Numbers,
5. Protection Profile Conformance (if applicable),
6. Evaluation Platform (optional),
7. Name of IT Security Evaluation Facility (optional),
8. Name of Certification Body,
9. Certification Report Identifier,
10. Date Issued, and
11. Assurance Package.

The certificate is also to include the following statements:

"The IT-product identified in this certificate has been evaluated by an accredited evaluation facility using a methodology defined in [reference to specification used] for assessment of conformance. The validation has been conducted in accordance with the requirements in SWEDAC's Regulations and General Guidelines (STAFS 2007:21) for Bodies Certifying IT-security and is based on the conclusions presented in the evaluation technical report. This certificate is not an endorsement of the IT-product by the certification body or by any other organisation that recognises or gives effect to this certificate. The certificate is only applicable to the specific product and version in the configuration that has been evaluated according to the certification report."

Certificates Associated with Protection Profile (PP) Evaluations

A certificate issued by a Participant resulting from the certification/validation of a protection profile evaluation is to include the following information:

1. Protection Profile (PP) Developer,
1. Protection Profile Name/Identifier,
2. Version Number,
3. Name of IT Security Evaluation Facility (optional),
4. Name of Certification/Validation Body,
5. Certification/Validation Report Number,
6. Date Issued, and
7. Assurance Package.

The certificate is also to include the following statements:

"The protection profile identified in this certificate has been evaluated by an accredited evaluation facility using the methodology defined in [reference to specification used] for conformance assessment. The validation has been conducted in accordance with the requirements in SWEDAC's Regulations and General Guidelines (STAFS 2007:21) for bodies certifying IT-security and is based on the conclusions presented in the evaluation technical report. This certificate is not an

endorsement of the protection profile by the certification body or by any other organisation that recognises or gives effect to this certificate. The certificate is only applicable to the specific protection profile and version in the configuration that has been evaluated according to the certification report.

Information above is based on Common Criteria Recognition Arrangement (CCRA) Annex J.

Appendix 2

Contents of Certification/Validation Reports

Certification/Validation Report and Its Use

The Evaluation Technical Report (ETR) is written by the Evaluation Facility for the Certification/Validation Body and serves as the principal basis for the Certification/Validation Report. The objective of the ETR is to present all verdicts, their justifications and any findings derived from the work performed during the evaluation, including errors found during the development of the IT product or protection profile and any exploitable vulnerabilities discovered during the evaluation. The ETR may contain protected information as necessary to justify evaluation results.

The Certification/Validation Report is the source of detailed security information about the IT product or protection profile for any interested parties. Its objective is to provide practical information about the IT product or protection profile to consumers. The Certification/Validation Report need not, nor should contain protected information since, like the Security Target, it contains information for the consumer necessary to securely deploy the evaluated IT product.

Executive Summary

The executive summary is a brief summary of the entire report. The information contained within this section should provide the audience with a clear and concise overview of the evaluation results. The audience for this section could include developers, consumers and evaluators of secure IT systems and products. It may be that the reader will be able to gain a basic familiarity with the IT product or the protection profile and the report results through the executive summary. Some clients, (e.g. accreditors, management) may only read this section of the report; therefore it is important that all key evaluation findings be included in this section. An executive summary should contain, but is not limited to the following items:

1. Name of the evaluated IT product, enumeration of the components of the product that are part of the evaluation, developer's name, and version;
2. Name of IT security evaluation facility;
3. Completion date of evaluation; and
4. Brief description of the report results:
    a) assurance package;
    b) functionality;
    c) summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product;
    d) special configuration requirements;
    e) assumptions about the operating environment;
    f) disclaimers.

Identification

The evaluated IT product has to be clearly identified. The software version number, any applicable software patches, hardware version number and peripheral devices (e.g. tape drives, printers, etc.) must be identified and recorded. This provides the labelling and descriptive information necessary to completely identify the evaluated IT product. Complete identification of the evaluated IT product will ensure that a

whole and accurate representation of the IT product can be recreated for use or for future evaluation efforts.

Security Policy

The security policy section should contain the description of the IT product's security policy. The security policy describes the IT product as a collection of security services. The security policy description contains the policies or rules that the evaluated IT product must comply with and/or enforce.

Assumptions and Clarification of Scope

The security aspects of the environment/configuration in which the IT product is expected to be used in should be included in this section. The section provides a means to articulate the clarification of the scope of the evaluation with respect to threats that are not countered. Users can make informed decisions about the risks associated with using the IT product. Usage, environmental assumptions, and clarification of the scope of the evaluation with respect to threats that are not countered should be stated in this section.

Usage Assumptions

In order to provide a baseline for the product during the evaluation effort certain assumptions about the usage of the IT product have to be made. Items such as proper installation and configuration, minimum hardware requirements being satisfied, etc., all have to be assumed. This section documents any usage assumptions made about the IT product during the evaluation.

Environmental Assumptions

In order to provide a baseline for the IT product during the evaluation effort certain assumptions about the environment the product is to be used in has to be made. This section documents any environmental assumptions made about the IT product during the evaluation.

Clarification of Scope

This section lists and describes threats to the IT product that are not countered by the evaluated security functions of the product. It may occur that some clients will assume that some threats are being met by the IT product but in fact they are not. It is for these reasons that these threats not countered should be listed for clarification. It would however, be impractical to list all possible threats that cannot be countered by an individual product.

Architectural Information

This section provides a high level description of the IT product and its major components based on the deliverables described in the Common Criteria assurance family entitled Development-High Level Design (ADV_HLD). The intent of the section is to characterise the degree of architectural separation of the major components.

Documentation

A complete listing of the IT product documentation provided with the product by the developer to the consumer is listed in this section. It is important that all relevant documentation be noted with the version numbers. The documentation at a minimum describes the user, administration and installation guides. It may occur that the administration and installation guide information is contained in a single document.

IT product testing

This section describes both the developer and evaluator testing effort, outlining the testing approach, configuration, depth, and results.

Evaluated Configuration

This section documents the configuration of the IT product during the evaluation. Typically, the administrator or installation guide will provide the necessary details for the correct configuration of the IT product. The IT product may be configurable in a number of different ways depending on the environment it is used in or the security policies of the organisation that it enforces.

The precise settings and configuration details with accompanying rationale for these choices are outlined in this section. Any additional operational notes and observations can also be included. This section is of particular importance, as it provides a baseline for the evaluated product installation.

Results of the Evaluation

This section documents the assurance requirements that the IT product satisfies. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the Security Target.

Evaluator Comments/Recommendations

This section is used to impart additional information about the evaluation results. These comments/recommendations can take the form of shortcomings of the IT product discovered during the evaluation or the mentioning of features which are particularly useful.

Annexes

The Annexes are used to outline any additional information that may be useful to the audience of the report, but does not logically fit within the prescribed headings of the report (e.g. a complete description of the security policy).

Security Target (ST)

The Security Target must be included in the Certification/Validation Report. However, it should be sanitised by the removal or paraphrase of proprietary technical information.

Glossary

The Glossary is used to increase the readability of the report by providing definitions of acronyms or terms of which the meanings may not be readily apparent.

Bibliography

The Bibliography section lists all referenced documentation used as source material in the compilation of the report. This information can include but is not limited to:
a) criteria, methodology, program scheme documentation;
b) technical reference documentation; and
c) developer documentation used in the evaluation effort.

It is critical for the sake of reproducibility that all developer documentation is uniquely identified with the proper release date, and proper version numbers.

The above is the text given in Common Criteria Recognition Arrangement (CCRA) Annex I.