Common Criteria Recognition Arrangement

Management Committee

Policies and Procedures

Document Number: 2006-04-004

Date: [April, 2006]

Subject: ST sanitising for publication

1 Rationale

The CCRA requires the Security Target to be included with the Certification Report. However Appendix I.13 allows it to be sanitised by the removal or paraphrasing of proprietary technical information. This procedure defines the rules for sanitising a Security Target and describes the minimum content of the resulting document which is named ST-lite.

2 Introduction

The Certification 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 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. The Security Target must be included with the Certification Report. However, it may be sanitised by the removal or paraphrasing of proprietary technical information. This document is named ST-lite.

The ST-lite must be a real representation of the complete ST. This means that the ST-lite can not omit information which is necessary to understand the security properties of the TOE and the scope of the evaluation.

3 Minimum content

Based on the structural outline of the common criteria (CC Part 1, Annex C) the following describes the minimum content of the ST-lite:

- The ST introduction includes in general no proprietary information. Therefore, the introduction need not be sanitized further. The ST-lite needs a unique identifier to be distinct from the complete ST.
- The TOE description might be reduced. It may include proprietary and detailed information about the TOE design which should not be published.

- The TOE security environment description (assumptions, threats, organisational security policies) cannot be reduced. All this information is necessary to understand the scope of the evaluation.
- The security objectives cannot be reduced, all information has to be made public to understand the intention of the ST and TOE evaluation.
- All security requirements have to be made public. Application notes might give information on how CC Part 2 components were used to understand the ST. However, refinements and application notes might be sanitized to remove proprietary information (e.g. about design).
- The TOE summary specification might be sanitized to remove proprietary information (e.g. about design). As a minimum, all TOE Security Functions have to be included.
- The PP claims shall be included.
- The rationale may be sanitized to remove proprietary information.

4 Evaluation

The TOE evaluation has to be based on a complete Security Target as stated by the criteria.

The ST-lite will not be formally evaluated according to the criteria. The check for the compliance of the ST-lite with the complete Security Target can be performed by the evaluator or the certification body. The Certification Report shall reference both, the complete ST as well as the ST-lite. The CB has to approve the ST-lite for publication.