A R R A N G E M E N T

on the

Recognition of Common Criteria Certificates

In the field of

Information Technology Security

Final Draft Version 16.5.1

May 14, 2014

The Participants

Defence Signals Directorate
from Australia

and

Secure Information Technology Center – Austria (A-SIT)
from Austria

and

Communications Security Establishment
from Canada

and

National Security Authority
from Czech Republic

and

Centre For Cyber Security
from Denmark

and

Finnish Communications Regulatory Authority
from Finland

and

Agence Nationale de la Sécurité des Systèmes d'Information
from France

and

Bundesamt für Sicherheit in der Informationstechnik
from Germany

and

National INFOSEC Authority (National Intelligence Service)
from Greece

and

[To Be Completed]
from Hungary

and

Ministry of Communications and Information Technology, and Department of Electronics and Information Technology
from India

and

The Standards Institution of Israel
from Israel

and

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
from Italy

and

Ministry of Economy, Trade and Industry, and Information-technology Promotion Agency
from Japan

and

CyberSecurity Malaysia
from Malaysia

and

Ministry of the Interior and Kingdom Relations
from The Netherlands

and

Government Communication Security Bureau
from New Zealand

and

Norwegian National Security Authority
from Norway

and

Ministry of Defence
from Pakistan

and

National Intelligence Service and
National Security Research Institute
from Republic of Korea

and

Infocomm Development Authority
from Singapore

and

Ministerio de Hacienda y Administraciones Públicas and
Centro Criptológico Nacional
from Spain

and

Swedish Defence Materiel Administration (FMV)
from Sweden

and

Turkish Standards Institution
from Turkey

and

CESG
from the United Kingdom

and

National Institute of Standards and Technology and
National Security Agency
from the United States of America

PLAN TO COOPERATE IN THE FOLLOWING MANNER:

Preamble

Purpose of the Arrangement

The *Participants* in this Arrangement share the following objectives:

a) to ensure that *Evaluations* of *Information Technology (IT) Products* and *Protection Profiles* are performed to high and consistent standards, and are seen to contribute significantly to confidence in the security of those products and profiles;

b) to improve the availability of evaluated, security-enhanced *IT Products* and Protection Profiles;

c) to eliminate the burden of duplicating Evaluations of IT Products and Protection Profiles;

d) to continuously improve the efficiency and cost-effectiveness of the Evaluation and *Certification/Validation*[1] process for IT Products and Protection Profiles.

The purpose of this Arrangement is to advance those objectives by bringing about a situation in which IT Products and Protection Profiles which earn a *Common Criteria Certificate*, as per the requirements of the CC standard, can be procured or used without the need for further Evaluation. It seeks to provide grounds for confidence in the reliability of the judgements on which the original certificate was based by requiring that a *Certification/Validation Body (CB)* issuing Common Criteria Certificates should meet high and consistent standards.

It is likely that some sensitive government *IT Systems* will be procured, certified and Recognised according to specific user's requirements for their strategic need or separate bilateral or multilateral agreements. This Arrangement does not constrain such agreements. In particular, the exceptions described in Article 3 do not apply to any such separately negotiated agreements.

The operation of multiple Certification/Validation Bodies (CB) by a Participant or of purely commercial CBs does not comply with the intent of the Arrangement, which requires mutual understanding and trust between governmental organisations in addition to compliance with certain standards. Therefore, the operation of the Arrangement cannot accommodate multiple or purely commercial CBs.

Moreover, as recognising certificates issued in other nations involves decisions and commitments that are specific to government, the functions of issuing and recognising certificates have been distinguished in this Arrangement.

Spirit of the Arrangement

The complexity of information systems is such that even the most carefully written security Evaluation criteria and Evaluation methodology cannot cover every eventuality. In many cases the application of the criteria will call for expert professional judgement, as will the oversight of their application. The Participants in the Arrangement therefore plan to develop and maintain mutual understanding and trust in each other's technical judgement and competence, and to maintain general consistency through open discussion and debate.

[1] Certain Schemes may choose to employ the term validation instead of certification. For the purposes of this Recognition Arrangement, the terms are deemed to be equivalent in their meaning and intended purpose as reflected in the Glossary at Annex A.

The Participants in the Arrangement will endeavour to work actively to improve the Evaluation criteria, Evaluation methodology, and their application, for example, by developing and establishing more cost-effective, consistent, and repeatable assurance packages, and by identifying and discarding those requirements that do not make a significant contribution to assurance. The Participants also plan to advance the economical reuse of Evaluation output, for example, by encouraging sponsors of Evaluations to provide such information to interested parties.

Article 1

Membership

Participants in this Arrangement are government organisations or government agencies, representing their country or countries. Participants may be producers of Evaluation certificates, consumers of Evaluation certificates, or both. *Certificate Consuming Participants*, although they may not maintain an IT security Evaluation capability, nevertheless have an expressed interest in the use of certified/validated IT Products and Protection Profiles. *Certificate Authorising Participants* are the *Sponsors of Compliant Certification/Validation Bodies (CB)* (described in Article 5) operating in their own country and authorise their certificates. Certificate Authorising Participants whose organisations command the resources and expertise of a *Compliant CB* are defined as *Qualified Participants*.

Article 2

Scope

It is mutually understood that, with respect to IT Products and Protection Profiles, the Participants plan to Recognise the Common Criteria Certificates which have been authorised by any other Certificate Authorising Participant in accordance with the terms of this Arrangement and in accordance with the applicable laws and regulations of each Participant. This Arrangement covers certificates with claims of compliance against Common Criteria assurance components of either:

1) a *collaborative Protection Profile (cPP),* developed and maintained in accordance with Annex K, with assurance activities selected from Evaluation Assurance Levels up to and including level 4 and ALC_FLR, developed through an *International Technical Community* endorsed by the *Management Committee*; or
2) Evaluation Assurance Levels 1 through 2 and ALC_FLR[2].

The scope may be modified with the consent of the Participants in this Arrangement at any time, in accordance with the provisions of Article 14, by addition or removal of assurance levels or components.

Article 3

Exceptions

If to Recognise a Common Criteria Certificate would cause a Participant to act in a manner inconsistent with applicable national, international or European Community law or regulation, that

[2] As detailed in Part 3 of the Common Criteria for Information Technology Security Evaluation.

Participant may decline to Recognise such a certificate. In particular, in cases where an IT Product or a Protection Profile is being considered for an application which involves the protection of information attracting a *Security Classification* or *Protective Marking* required or authorised under the provisions of national law, subsidiary legislation, administrative regulation or official obligation, Participants may decline, in respect of that application only, to Recognise a certificate. Annexes F.3 and G.2 of this Arrangement should be followed by Participants who call for exceptions in accordance with this article.

Article 4

Definitions

Terms crucial to the meaning of this Arrangement or which are used in a sense peculiar to this Arrangement are defined in a Glossary at Annex A to this Arrangement. Such terms appear in italic type on their first appearance in the text of this Arrangement.

Article 5

Conditions for Recognition

Except as otherwise provided in this Arrangement, each Participant should Recognise applicable Common Criteria Certificates authorised by any Certificate Authorising Participant. Such *Authorisation* confirms that the Evaluation and Certification/Validation processes have been carried out in a duly professional manner

a) on the basis of accepted *IT Security Evaluation Criteria*;
b) using accepted IT *Security Evaluation Methods* and *Supporting Documents;*
c) in the context of an *Evaluation and Certification/Validation Scheme* managed by a Compliant CB in the Certificate Authorising Participant's country; and
d) the Common Criteria Certificates authorised and *Certification/Validation Reports* issued satisfy the objectives of this Arrangement.

Certificates which meet all these conditions are equivalent for the purposes of this Arrangement.

The IT Security Evaluation Criteria are to be those laid down in the Common Criteria for Information Technology Security Evaluation (CC), the version endorsed by the Management Committee and the Evaluation Methods are to be those laid down in the Common Methodology for Information Technology Security Evaluation (CEM) and CC Supporting Documents, versions endorsed by the Management Committee. The minimum requirements for Certification/Validation Reports are laid down in Annex I to this Arrangement. The minimum requirements for an Evaluation and Certification/Validation Scheme are laid down in Annex B to this Arrangement. An Evaluation and Certification/Validation are deemed to have been carried out in a duly professional manner if, as a minimum:

a) the *Evaluation Facility*

- either has been *Accredited* in its respective country by a Recognised *Accreditation Body* in accordance with ISO/IEC 17025, its successors, or in accordance with an interpretation thereof approved by all Participants, and has been *Licensed* or *Approved* in accordance with Annex B.3,

- or has been established under the laws, statutory instruments, or other official administrative procedures valid in the country concerned and meets the requirements laid down in Annex B.3 to this Arrangement;

and,

b) the CB is accepted as compliant, and

- either has been Accredited in its respective country by a Recognised Accreditation Body either in accordance with ISO/IEC 17065, its successors, or in accordance with a national interpretation thereof, which at minimum satisfies the requirements as specified in Annex C to this Arrangement,

- or has been established under laws, statutory instruments, or other official administrative procedures valid in the country concerned and meets the requirements specified in Annex C to this Arrangement, or the requirements of ISO/IEC 17065, or its successors.

In order to assist the consistent application of the Common Criteria, Common Evaluation Methodology between Evaluation and Certification/Validation Schemes, the Participants plan to work towards a uniform *Interpretation* of the currently applicable Common Criteria and Common Evaluation Methodology through development and harmonised application of Supporting Documents. In pursuit of this goal, the Participants also plan to conduct regular exchanges of information on Interpretations and discussions necessary to resolve differences of Interpretation. In further aid to the goal of consistent, credible and competent application of the Common Criteria, Common Evaluation Methodology and Supporting Documents, the CB should undertake the responsibility for the *Monitoring* of all Evaluations in progress within the Scheme at an appropriate level, and carrying out other procedures to ensure that all IT Security Evaluation Facilities affiliated with the CB:

a) perform Evaluations impartially;
b) apply the Common Criteria, Common Evaluation Methodology and Common Criteria Recognition Arrangement (CCRA) Supporting Documents methods correctly and consistently; and
c) adequately protect the confidentiality of *Protected Information*.

Article 6

Voluntary Periodic Assessments

Assessment of Compliant CBs should take place at intervals of approximately, but no more than five years, for the purpose of assuring that they continue to share the objectives of this Arrangement and will endeavour to advance the objectives of this Arrangement. The form of such assessments is laid down in Annex D to this Arrangement.

Article 7

Publications and the Use of the Service and Certification Mark

Common Criteria Certificates authorised by Certificate Authorising Participants shall bear prominently, in addition to any logo or distinguishing device peculiar to the Participant or its Evaluation and Certification/ Validation Scheme, the mark of the Recognition Arrangement and a

standard form of words. The mark and the form of words are given in Annex E and Annex J to this Arrangement.

Each Certificate Authorising Participant should publish, in a section of its *Certified/Validated Products List* or as otherwise arranged, brief particulars of all IT Products and Protection Profiles having certificates authorised by another Certificate Authorising Participant, unless there is a reason not to do so under this Arrangement including but not limited to the reasons set forth in Article 3 to this Arrangement.

Article 8

Sharing of Information

To the extent disclosure of information is consistent with a Participant's national laws or regulations, each Participant should endeavour to make available to other Participants all information and documentation relevant to the application of this Arrangement.

In meeting this obligation, the commercial secrets or Protected Information of third parties may be disclosed by an *Information Technology Security Evaluation Facility (ITSEF)*, CB, or Participant only if prior agreement has been obtained in writing from the third party concerned.

In particular, each Participant should promptly provide information on prospective changes which might affect its ability to meet the conditions for recognition or which might otherwise frustrate the operation or intention of this Arrangement.

The nature and scope of the information and documentation that Participants are expected to share are more fully described in Annex F to this Arrangement.

Article 9

New Participants

Participants

Participation in this Arrangement is open to representatives from countries that plan to uphold the principles of the Arrangement, subject to the unanimous consent of the existing Participants.

Certification/Validation Bodies

A CB may be determined to be compliant for the purpose of Article 5 of this Arrangement upon unanimous consent of the existing Participants, if the existing Participants are confident that it can fulfil the conditions for recognition laid down in Article 5 of this Arrangement and Annexes cited in Article 5, and that it satisfies the conditions for compliance, according to the procedures laid down in Annex G to this Arrangement, including *Shadow Certification/Validation*.

Article 10

Administration of this Arrangement

A *Management Committee* should administer this Arrangement. The Management Committee should meet as often as required to consider matters affecting the status, terms or application of this Arrangement. All Participants are represented on the Management Committee. The

procedures and principal responsibilities of the Management Committee are set forth in Annex H to this Arrangement.

Article 11

Disagreements

Disagreements between the Participants should be resolved through discussions. Participants should make every effort to resolve disagreements between themselves by negotiation. Failing this, disagreements should in the first instance, be referred to the Management Committee. The Management Committee is expected to document its findings in the disagreement. If the disagreement cannot be resolved by discussion or negotiation, individual Participants may choose not to Recognise affected Common Criteria Certificates and notify the Management Committee of such non-recognition.

Article 12

Use of Contractors

Where Participants propose to involve contractors in the implementation and operation of this Arrangement, particularly the procedures set out in Annexes D, G.3, G.4 or H to this Arrangement, they should ensure that these contractors have appropriate expertise and should notify the other Participants. Protected Information should be passed to contractors only with the agreement of the *Originator*, as laid down in Annex F.4.

Article 13

Costs of this Arrangement

Except as specified otherwise in this Arrangement, each Participant is expected to meet all its own costs arising through its participation in this Arrangement.

Article 14

Revision

Any modification of the terms of this Arrangement will require the unanimous consent of the Participants. Any adopted modification should be recorded in a written document signed by all the Participants.

Article 15

Duration

Cooperation under this Arrangement is expected to continue unless the Participants decide unanimously to end it.

Article 16

Voluntary Termination of Participation

Any Participant may terminate its participation in this Arrangement, or terminate the compliant status of any CB that it represents, by notifying the other Participants in writing.

Article 17

Commencement

This Arrangement or any subsequent modification is to commence on the date on which it has been signed by all its Participants.

In terms of continuation, the qualifying status of all members remains valid for a period of five years from the date of the latest Voluntary Periodic Assessment / Shadow Certification/Validation under the previous version of the Arrangement, unless otherwise approved by the Management Committee.

Certificate Consuming Participants, which have applied to become a Certificate Authorising Participant under the previous version of this Arrangement, and for which the Shadow Certification/Validation has not yet been completed, may choose to complete the Shadow Certification/Validation under the conditions of the previous version of this Arrangement.

Furthermore, all Participants agree:

a) to Recognise conformant certificates issued under the previous version of this Arrangement;
b) to Recognise certificates resulting from products accepted into the certification process prior to approval of this Arrangement according to the previous version of the Arrangement; and
c) for a period of 36 months from the date on which this Arrangement has been signed by all its Participants, to Recognise re-certifications and maintenance addenda issued according to the previous version of this Arrangement. Thereafter, within the scope of this arrangement all Participants shall limit recognition of certifications issued in accordance with Article 2.

Article 18

Effect of this Arrangement

It is recognised and accepted by each of the Participants that this Arrangement does not create any substantive or procedural rights, liabilities or obligations that could be invoked by persons who are not signatories to this Arrangement. Additionally, it is recognised and accepted by each of the Participants that this Arrangement has no binding effect in national, international or European Community law on any or all of them, and that they will not attempt to enforce this Arrangement in any domestic or international court or tribunal. Reports issued by a CB or Common Criteria Certificates authorised by a Participant do not constitute endorsement, warranty or guarantee by that Certification/Validation Body or Participant, respectively, of IT Products or Protection Profiles; nor does *Recognition of Common Criteria Certificates* authorised as a result of Certification/Validation activities constitute the endorsement, warranty, or guarantee in any way of Certification/Validation Reports issued by another CB or resulting certificates authorised by another Participant, respectively.

Annex A

Glossary

This glossary contains definitions of certain terms in the text or Annexes to this Arrangement which are used in a sense specific to this Arrangement or which have a meaning crucial to the interpretation of this Arrangement. It also contains definitions of certain other terms used within this Annex. Where the definitions in this Annex differ from definitions of the same terms given in CC or CEM, the definitions in this Annex are to be used in establishing the intended meaning of this Arrangement. Such definitions are broadly consistent with those given in CC and CEM, which remain generally valid. The differences are in the interest of greater clarity in the specific context of this Arrangement. Terms used in definitions which are themselves defined elsewhere in the Glossary appear in italic type.

Accredited:
Formally confirmed by an *Accreditation Body* as meeting a predetermined standard of impartiality and general technical, methodological and procedural competence.

Accreditation Body:
An independent organisation responsible for assessing the performance of other organisations against a recognised standard, and for formally confirming the status of those that meet the standard.

Achievable Common Level of Security Assurance:
Security assurance requirements defined in *collaborative Protection Profiles* that produce reasonable, comparable, reproducible, and cost-effective results. It is recognised that all *CBs* of *Qualified Participant*s have the potential to certify *Evaluations* against *collaborative Protection Profiles* and related *Supporting Document*s. Schemes may or may not use *cPPs* based on their business need.

Approved:
See *Licensed*.

Approval/Licensing Policy:
A part of the essential documentation of every *Evaluation and Certification/Validation Scheme*, setting out the procedures for making an application to be *Licensed* or *Approved* and for the processing of such applications and of the training and security requirements which an applicant must fulfil in order to qualify.

Assessment of Compliant CBs:
A procedure for establishing that the *Evaluations* and *Certifications/Validations* carried out by a particular *Compliant CB* continue to be as set out in this Arrangement.

Authorisation:
The sanction by a *Participant* of the issuing of a *Common Criteria Certificate* by a *Compliant CB*, permitting the use of the CC Certification Mark.

CC:
Common Criteria for Information Technology Security Evaluation, the title of a document describing a particular set of *IT Security Evaluation Criteria*.

CEM:
Common Methodology for Information Technology Security Evaluation, the title of a technical document describing a particular set of *IT Security Evaluation Methods*.

Certification/Validation:
The process carried out by a *CB* leading to the issuing of a *Common Criteria Certificate*.

Certification/Validation Body (CB):
An organisation responsible for carrying out *Certification/Validation* and for overseeing the day-to-day operation of an *Evaluation and Certification/Validation Scheme*.

Associated CB:
The *Compliant CB* associated with a *Qualified Participant.*

Compliant CB:
A *CB* that is listed as compliant in Annex L.

Certification/Validation Report:
A public document issued by a *CB* which summarises the results of an *Evaluation* and confirms the overall results, i.e. that the *Evaluation* has been properly carried out, that the *Evaluation Criteria*, *Evaluation Methods* and other procedures have been correctly applied and that the conclusions of the *Evaluation Technical Report* are consistent with the evidence adduced.

Certified/Validated Products List:
A public document giving brief particulars of currently valid *Common Criteria Certificates* in accordance with this Arrangement.

Client:
A party in contract with an *ITSEF* for an *Evaluation*.

Common Criteria Certificate:
A public document issued by a *Compliant CB* and authorised by a *Participant* which confirms that a specific *IT Product* or *Protection Profile* has successfully completed *Evaluation* by an *ITSEF*. A *Common Criteria Certificate* always has a *Certification/Validation Report* associated with it.

Evaluation:
The assessment of an *IT Product* or a *Protection Profile* against the *Common Crit*eria using *Common Evaluation Methodology* to determine whether or not the claims made are justified.

Evaluation and Certification/Validation Scheme:
The systematic organisation of the functions of *Evaluation* and *Certification/Validation* under the authority of a *CB* in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.

Evaluation Facility:
An organisation which carries out *Evaluations*, independently of the developers of the *IT Products* or *Protection Profiles* evaluated and usually on a commercial basis.

Evaluation Methods:
See *IT Security Evaluation Methods*.

Evaluation Technical Report:
A report giving details of the findings of an *Evaluation*, submitted by the *Evaluation Facility* to the *CB* as the principal basis for the *Certification/Validation Report*.

International Technical Community (iTC):
A group of technical experts including *Participants*, *Certification/Validation Bodies*, *ITSEFs*, developers and users which are:
a) working in manners that promote fair competition;

b) working in some specific technical area in order to define *cPPs*;
c) endorsed for this purpose by the *Management Committee*; and
d) establishing *Interpretations* of the application of the *CC* and *CEM* necessary for *cPPs* through *Supporting Documents* which are subject to the CCRA approval process.

Interpretation:
Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.

IT Product:
A package of IT software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of *IT Systems*.

IT Security Evaluation Criteria:
A compilation of the information which needs to be provided and of the actions which need to be taken in order to give grounds for confidence that *Evaluations* will be carried out effectively and to a consistent standard throughout an *Evaluation and Certification/Validation Scheme*.

IT Security Evaluation Methods:
A compilation of the methods which need to be used by *Evaluation Facilities* in applying *IT Security Evaluation Criteria* in order to give grounds for confidence that *Evaluations* will be carried out effectively and to a consistent standard throughout an *Evaluation and Certification/Validation Scheme*.

ITSEF:
IT Security *Evaluation Facility*, an *Accredited Evaluation Facility*, *Licensed* or *Approved* to perform *Evaluations* within the context of a particular *IT Security Evaluation and Certification/Validation Scheme*.

IT System:
A specific IT installation, with a particular purpose and operational requirement.

Licensed:
Assessed by a *CB* as technically competent in the specific field of IT security *Evaluation* and formally authorised to carry out *Evaluations* within the context of a particular *Evaluation and Certification/Validation Scheme*.

Management Committee (MC):
The body, on which all *Participants* are represented, which endeavours to ensure the operation of this Arrangement in accordance with its rules.

Monitoring (of Evaluations):
The procedure by which representatives of a *CB* observe *Evaluations* in progress or review completed *Evaluations* in order to satisfy themselves that an *ITSEF* is carrying out its functions in a proper and professional manner.

Originator:
The source, e.g., an *IT Product* or *Protection Profile* developer, *ITSEF*, or *Participant*, producing *Protected Information* associated with an IT security *Evaluation* or *Certification/Validation*.

Participant:
A signatory to this Arrangement.

Certificate Consuming Participant:
A *Participant* with a national interest in recognising *Common Criteria Certificates*.

Certificate Authorising Participant:
A *Participant* representing one or more *Compliant CBs*.

Qualified Participant:
A *Participant* that is also a *Compliant CB* (or that commands the resources and expertise of a *Compliant CB* sufficiently for it to provide technical experts to undertake *Shadow Certification/Validation*). The *CB* is the *Associated CB* of the *Qualified Participant*.

Protected Information:
Information gathered or obtained under the processes or activities in this Arrangement whose unauthorised disclosure could reasonably be expected to cause (i) harm to competitive commercial or proprietary interests, (ii) a clearly unwarranted invasion of personal privacy, (iii) damage to national security, or (iv) otherwise cause harm to an interest protected by national law, subsidiary legislation, administrative regulation or official obligation.

Protection Profile:
A formal document defined in *CC,* expressing an implementation independent set of security requirements for a category of *IT Products* that meet specific consumer needs.

Collaborative Protection Profile (cPP):
A *Protection Profile* collaboratively developed by an *International Technical Community* endorsed by the *Management Committee*. A *cPP* and related *Supporting Documents* define the minimum set of common security functional requirements and the *Achievable Common Level of Security Assurance*. It addresses vulnerability analysis requirements to ensure certified products reach an *Achievable Common Level of Security Assurance*.

Protective Marking:
Marking representing sensitive, critical and/or classified information.

RA in Confidence:
Protective Marking used to distinguish documents with potentially sensitive data to be used only within the context of the CCRA. A procedure of use is explicitly defined within an MC Procedure.

Recognise:
See *Recognition of Common Criteria Certificates*.

Recognition of Common Criteria Certificates:
Acknowledgement by *Participants* that the Evaluation and *Certification/Validation* processes carried out by *Compliant CBs* appear to have been carried out in a duly professional manner and meet all the conditions of this Arrangement, and the intention to give all resulting *CC Certificates* equal weight.

Security Classification:
A marking applied to *Protected Information* in order to indicate minimum standards of protection which need to be applied in the national interest.

Security Target (ST):
An implementation-dependent statement of security needs for a specific identified *Target of Evaluation*.

Shadow Certification/Validation:
Assessment of a *CB* in which representatives of at least one *Qualified Participant* monitor the *Evaluation* and *Certification/Validation* of an *IT Product* in accordance with this Arrangement.

Sponsor (of a CB):

The *Participant* that represents the interests of a *Compliant CB* (or candidate *Compliant CB*) and authorises its *Common Criteria Certificates*.

Supporting Document:
A document that specifies the use of the Common Criteria or *Common Methodology for Information Technology Security Evaluation* in a particular field or domain of technology. Such documents may be either mandatory or guidance and generally specify the *Interpretations* of the *CC* and/or *CEM* when necessary.

Target of Evaluation (TOE):
An *IT Product* and its associated administrator and user guidance documentation that is the subject of an *Evaluation*.

Annex B

Evaluation and Certification/Validation Scheme

B.1 The Purpose and Principal Characteristics of a Scheme

The main purpose of an Evaluation and Certification/Validation Scheme (hereinafter referred to as a Scheme) is to ensure, through the systematic organisation and management of the functions of Evaluation and Certification/Validation, that high standards of competence and impartiality are maintained and that consistency is achieved.

To this end, each Scheme is managed by a single Certification/Validation Body, which is responsible not only for the Certification/Validation of evaluated products and evaluated Protection Profiles, but, equally importantly, for other functions which are listed in section B.2.

The overall policy of a Scheme (including its Licensing or *Approval Policy* - see below) may be set either by the Certification/Validation Body itself or by a management board. In the latter case, the management board has ultimate responsibility for the operation of the Scheme in accordance with its rules and policies and, where appropriate, for the interpretation or amendment of those rules and policies, while the Certification/Validation Body manages the Scheme and applies the rules and policies in accordance with the policy guidance of the management board. In either case, it is very important that mechanisms are in place to ensure that the interests of all parties with a stake in Evaluation and Certification/Validation activities are given an appropriate weight in the running of the Scheme.

The existence of such a Scheme is of crucial importance in the context of recognition. For, in conjunction with the correct and consistent application of common Evaluation criteria and Evaluation Methods, it offers unique grounds for confidence that all ITSEFs are operating to the same high standards and thus in the correctness of results and in their consistency between one ITSEF and another. Such confidence is indispensable in establishing the trust on which any Recognition Arrangement is necessarily based.

B.2 The Role and Principal Characteristics of the CB

An Evaluation Facility which has been Licensed or Approved to carry out Evaluations within a particular Scheme is known as an IT Security Evaluation Facility. The CB is independent of the ITSEFs, and staffed by appropriately qualified personnel.

The CB may be established under the provisions of a law, statutory instruments or other official administrative procedure valid in the country concerned or it may be Accredited by an appropriate Accreditation Body. In both cases, it is to meet the requirements as specified in the Annex C to this Arrangement, or the requirements of ISO/IEC 17065 or its successors.

The principal functions to be performed by the Certification/Validation Body are:

a) to authorise the participation of Evaluation Facilities in the Scheme (see further below);

b) to monitor the performance of participating ITSEFs and, in particular, their adherence to, and application and Interpretation of, the accepted Evaluation criteria and Evaluation Methods;

c) to see to it that procedures are in place within the Scheme to ensure that sensitive information relating to products and Protection Profiles under Evaluation and to the

process of Evaluation itself is appropriately handled and given the security protection it requires and that those procedures are routinely followed (see further below);

d) to issue additional guidance to ITSEFs as required;

e) to monitor all Evaluations in progress within the Scheme at an appropriate level;

f) to review all Evaluation reports (especially including Evaluation Technical Reports) to ensure that the conclusions are consistent with the evidence adduced and that the accepted Evaluation criteria and Evaluation Methods have been correctly applied;

g) to produce a Certification/Validation Report in respect of each Evaluation completed under the auspices of the Scheme;

h) to publish Common Criteria Certificates and their associated Certification/Validation Reports;

i) to regularly publish a document giving brief particulars of all products and Protection Profiles evaluated within the Scheme which hold a currently valid Common Criteria Certificate (Certified/Validated Products List);

j) to document the organisation, policy, rules and procedures of the Scheme, to make that documentation available publicly and to keep it up to date;

k) to ensure that the rules of the Scheme are followed;

l) to establish, and where appropriate, amend, the rules and policies of the Scheme;

m) to ensure that the interests of all parties with a stake in the Scheme's activities are given appropriate weight in the running of the Scheme.

In the context of involvement in this Arrangement, the Certification/Validation Body associated with a Qualified Participant is also responsible for providing technical support to activities relating to this Arrangement in accordance with the provisions of this Arrangement.

B.3 Accreditation and Licensing of Evaluation Facilities

Unless an Evaluation Facility has been established under a law or statutory instrument, if it is to participate in a Scheme, it needs to fulfil two conditions:

a) be Accredited by an Accreditation Body officially Recognised in the country concerned; and

b) be Licensed or otherwise Approved by the CB responsible for the management of the Scheme.

Accreditation entails the Evaluation Facility demonstrating its impartiality and its general technical, methodological and procedural competence and in particular that it meets the requirements of ISO/IEC 17025 or its successors in so far as these requirements are consistent with the peculiarities of the domain of IT security.

The Evaluation Facility also has to demonstrate to the satisfaction of the CB that it is technically competent in the specific field of IT security Evaluation and that it is in a position to comply in full with the rules of the Scheme concerned. This includes demonstrating that it has the ability to apply the applicable Evaluation criteria and Evaluation Methods correctly and consistently and that it meets stringent security requirements necessary for the protection of sensitive or Protected

Information relating to IT Products or Protection Profiles under Evaluation and to the process of Evaluation itself.

The Licensing or Approval Policy for each Scheme includes details of security and training requirements and of the procedures for making an application to be Licensed or Approved and for the processing of such applications.

Annex C

Requirements for Certification/Validation Body

C.1 General Requirements

The services of the CB are to be available without undue financial or other conditions. The procedures under which the CB operates are to be administered in a non-discriminatory manner.

C.2 Administrative Structure

The CB is to be impartial. In particular, it should have permanent staff responsible to a senior executive enabling day-to-day operations to be carried out free from undue influence or control by anyone having a commercial or financial interest in the Certification/Validation.

C.3 Organisational Structure

The CB is to have and make available on request:

a) a chart showing clearly the responsibility and reporting structure of the organisation;

b) a description of the means by which the organisation obtains financial support;

c) documentation describing its Evaluation and Certification/Validation Scheme; and

d) documentation clearly identifying its legal status.

C.4 Certification/Validation Personnel

The personnel of the CB are to be competent for the functions they undertake. Information on the relevant qualifications, training and experience of each member of staff is to be maintained by the CB and kept up-to-date.

Personnel are to have available to them clear, up to date, documented instructions pertaining to their duties and responsibilities.

If work is contracted to an outside body, the CB is to ensure that the personnel carrying out the contracted work meet the applicable requirements of this Annex.

C.5 Documentation and Change Control

The CB is to maintain a system for the control of all documentation relating to its Evaluation and Certification/Validation Scheme and ensure that:

a) current issues of the appropriate documentation are available at all relevant locations;

b) documents are not amended or superseded without proper authorisation;

c) changes are promulgated in such way that those who need to know are promptly informed and are in a position to take prompt and effective action;

d) superseded documents are removed from use throughout the organisation and its agencies; and

e) those with a direct interest in the Scheme are informed of changes.

C.6 Records

The CB is to maintain a record system to suit its particular circumstances and to comply with relevant regulations applied in the jurisdiction to which the Participant is subject. The system is to include all records and other papers produced in connection with each Certification/Validation; it is to be sufficiently complete to enable the course of each Certification/Validation to be traced. All records are to be securely and accessibly stored for a period of at least five years.

C.7 Certification/Validation Procedures

The CB is to have the required facilities and documented procedures to enable the IT Product or Protection Profile Certification/Validation to be correctly carried out in accordance with the Common Criteria and related Evaluation Methods (i.e. CEM, CC Supporting Documents).

C.8 Requirements of Evaluation Facilities

The CB is to ensure that IT Security Evaluation Facilities conform to requirements specified in this Arrangement.

The CB is to draw up for each IT Security Evaluation Facility a properly documented agreement covering all relevant procedures including arrangements for ensuring confidentiality of Protected Information and the Evaluation and Certification/Validation processes.

C.9 Quality Manual

The CB is to have a Quality Manual and documentation setting out the procedures by which it complies with the requirements of this Annex. These are to include at least:

a) a policy statement on the maintenance of quality;

b) a brief description of the legal status of the CB;

c) the names, qualifications and duties of the senior executive and other Certification/Validation personnel;

d) details of training arrangements for Certification/Validation personnel;

e) an organisation chart showing lines of authority, responsibility and allocation of functions stemming from the senior executive;

f) details of procedures for Monitoring IT Product or Protection Profile Evaluations;

g) details of procedures for preventing the abuse of Common Criteria Certificates;

h) the identities of any contractors and details of the documented procedures for assessing and Monitoring their competence; and

i) details of any procedures for appeals or conciliation.

C.10 Confidentiality

To the extent permitted by the national laws, statutes, executive orders, or regulations of the Participants, the CB should have adequate arrangements to ensure confidentiality of the

information obtained in the course of its Certification/Validation activities at all levels of its organisation and is not to make an unauthorised disclosure of Protected Information obtained in the course of its Certification/Validation activities under this Arrangement.

C.11 Publications

The CB is to produce and update as necessary a Certified/Validated Products List. Each IT Product or Protection Profile mentioned in the list is to be clearly identified. The list is to be available to the public.

A description of the Evaluation and Certification/Validation Scheme is to be available in published form.

C.12 Appeals or Conciliation

The CB is to have procedures to deal with disagreements among itself, its associated ITSEFs, and their *Clients*.

C.13 Management Review

The CB is to undertake management reviews of its scheme operations to ensure that it continues to share the objectives of this Arrangement.

C.14 Misuse of Common Criteria Certificates

The CB is to exercise proper control over the use of its Common Criteria Certificates.

It is incumbent upon the CB to take appropriate administrative, procedural or legal steps to prevent or counter the misuse of certificates and to correct false, misleading or improper statements about certificates or about the Evaluation and Certification/Validation Scheme.

C.15 Withdrawal of Common Criteria Certificates

The CB is to have documented procedures for withdrawal of Common Criteria Certificates and is to advertise the withdrawal in the next issue of its Certified/Validated Products List.

Annex D

Voluntary Periodic Assessments

The Management Committee may select two or more Qualified Participants (excluding the CB's Sponsor) to carry out a periodic assessment of a Compliant CB. Assessments may not be conducted except pursuant to the written consent or request of the Sponsor, and such consent may be withdrawn or revoked prior to or during an assessment. The Sponsor is expected to represent to the Management Committee any concerns the CB may have about the choice of the assessment team. Assessments should be performed as described below, and in accordance with guidance issued by the Management Committee that will ensure that assessments are performed to a uniform standard and involve a predictable commitment of resources.

The Participants performing the assessment may make nominations for a primary assessment team to consist of two experts acceptable to the Management Committee. Any Participant may provide an additional expert at its own expense. The costs of providing primary assessment teams for *Associated CBs* should be distributed among the Qualified Participants in an equitable manner, to be agreed by the Executive Subcommittee. If the CB under assessment is not an Associated CB, it should meet all the costs of the primary assessment team arising out of the assessment (including the travel, accommodation, subsistence costs, and salaries)[3].

The CB undergoing the periodic assessment should within one month provide the complete scheme documentation applicable at the time. The experts review the documentation to assure that the CBs continue to share the objectives of this Arrangement, and report their findings to the Management Committee.

A Voluntary Periodic Assessment should be performed on at least two IT Products that are within the scope of this Arrangement as decided by the Participants directly involved. A non-disclosure agreement should be signed or some other appropriate information sharing mechanism be established between them.

The experts should satisfy themselves that the CB undergoing the periodic assessment is acting consistently in respect of all aspects of the Evaluation and Certification/Validation processes. In carrying out this responsibility, the experts may wish to take part in some aspects of the Certification/Validation process. The CB undergoing the assessment should facilitate this.

The experts are also to check the application of the procedures to ensure the confidentiality of Protected Information described in this Arrangement, particularly in Annexes B and C to this Arrangement.

At appropriate stages of the Evaluation and Certification/Validation, the following documentation should be provided for checking by experts:

a) the *Security Target*;

b) the Evaluation Technical Report;

c) any written comments on the above documents made by the Certification/ Validation Body; and

d) the Certification/Validation Report.

[3] This may be waived if the Qualified Participant carrying out the assessment is prohibited by national law or regulation from receiving such payment.

Other Evaluation reports should be provided on request in accordance with guidance issued by the Management Committee.

All documentation referred to above should be made available in English or in another language acceptable to the experts. Evaluation reports should be translated only if necessary. Participants who have consented to an assessment should find and implement a solution to any problem of language which is acceptable to the experts.

The experts report their findings to the Management Committee, and make a recommendation on the assessment. The Management Committee reviews the report of the assessment team. Once the Management Committee is satisfied that the report is internally consistent and that the conclusion follows from the evidence, the result is delivered to the Certification/Validation Body undergoing the assessment. The CB being assessed should demonstrate that it has rectified any shortcomings identified in the assessment within a maximum of six months.

Annex E

Certificate and Service Marks

E.1 Common Criteria Certification Mark

Every Common Criteria Certificate issued under the terms of this Arrangement is to bear the mark shown in Figure 1 to Figure 4.

Figure 1: Common Criteria Certification Mark

Note: The two symbols associated with trademarks ™ (the trademark symbol) and ® (the registered trademark symbol) represent the status of a mark and accordingly its level of protection. While ™ can be used with any common law usage of a mark, ® may only be used by the owner of a mark following registration with the relevant national authority and should conform to the requirements of local trademark law. In general, the requirements and consequences of using or not using symbols or indications that denote trademark marking must be ascertained on a per country basis and consulting with local counsel is always advisable.

This mark confirms that the Common Criteria Certificate has been authorised by a Participant to this Arrangement and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Arrangement.

It is incumbent upon the CB to take appropriate administrative, procedural or legal steps to prevent or counter the misuse of certificates and to correct false, misleading or improper statements about certificates or about the Evaluation and Certification/Validation Scheme.

Upon receipt of a Common Criteria Certificate, the Common Criteria Certification Mark may be used by vendors in conjunction with advertising, marketing, and sales for which the certificate is issued. The Certificate Authorising Participants shall make necessary legal arrangements with their ITSEFs and their Client vendors, to the effect that the vendors are also required to:

a) use the issued certificate in documentation or marketing material by reproducing the entire certificate in an accurate and readable form;

b) conform to the requirements of this Arrangement and its Participants (or Compliant CBs) when making reference to its certification status in communication media such as the internet, brochures or advertising, or other documents;

c) not make or permit any misleading statement regarding its certification;

d) not use or permit the use of a certification document or any part thereof in a misleading manner;

e) upon withdrawal of its certification, discontinues its use of all advertising matter that contains a reference to certification, as directed by the Participants (or Compliant CBs) of this Arrangement;

f) not allow reference to its product certification to be used in such a way as to either express or imply that the Participants of this Arrangement, or other organisation that Recognises or gives effect to this certificate, endorse or give warranty to the certified product;

g) not imply that the certification applies to activities that are outside the scope of certification; and

h) not use its certification in such a manner that would bring the Arrangement into disrepute and lose public trust.

The Common Criteria Certification Mark as shown in Figure 1 shall be reproduced and shall be reprinted according to the following specifications;

a) in colours coded as shown in Figure 2 and Figure 3; or

b) in black and white as shown in Figure 4 and Figure 5; and

c) in any size, uniformly enlarged or reduced (and preserving all proportions).

When used on paper, it may also be embossed or stamped.

Vendors shall follow the specification as specified in Figure 2, Figure 3, Figure 4, or Figure 5 below.

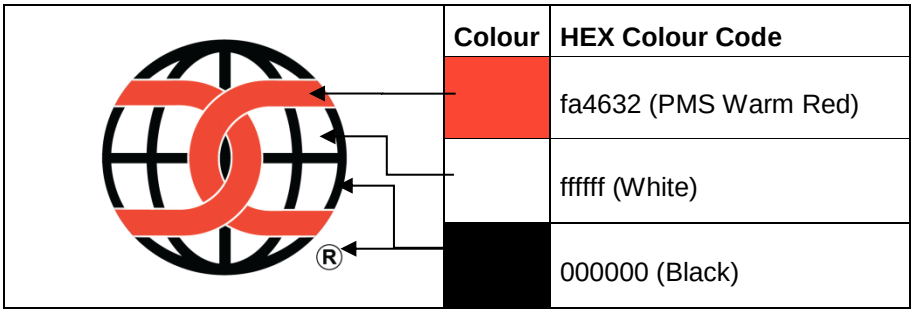

Figure 2: Common Criteria Certification Mark in colour with registered trademark symbol

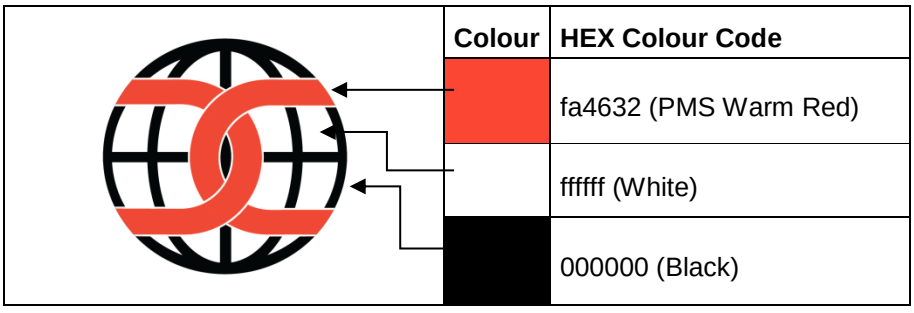

Figure 3: Common Criteria Certification Mark in colour without registered trademark symbol

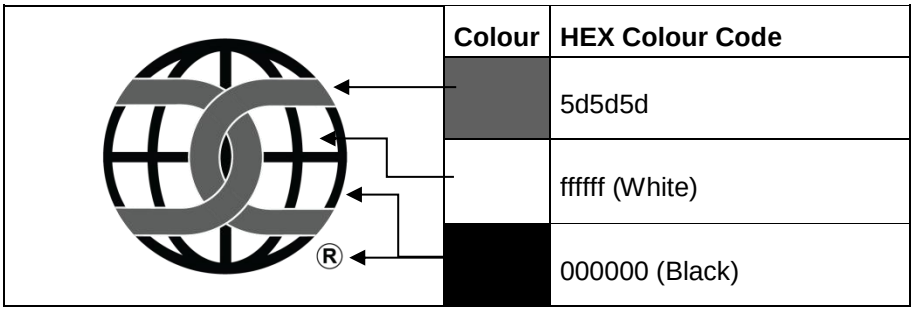

Figure 4: Common Criteria Certification Mark in black-and-white with registered symbol

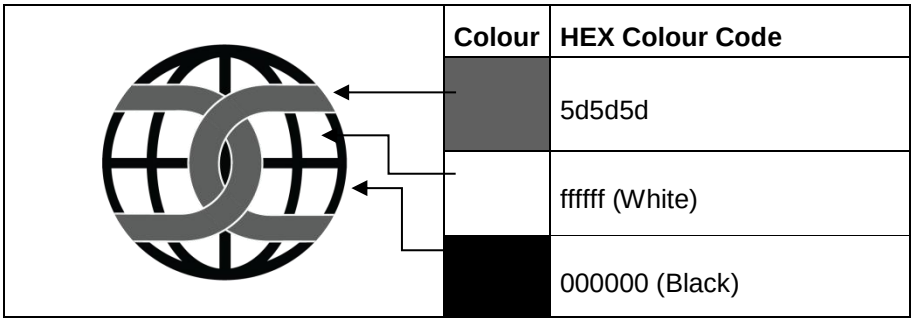

Figure 5: Common Criteria Certification Mark in black-and-white without registered symbol

E.2 Recognition Arrangement Service Mark

The service mark of this Recognition Arrangement, which is shown in Figure 6 below, is to be used to identify, advertise and market services which are performed by a Participant (or Compliant CBs) in conjunction with this Arrangement.

Figure 6: Recognition Arrangement Service Mark

Note: The two symbols associated with trademarks ™ (the trademark symbol) and ® (the registered trademark symbol) represent the status of a mark and accordingly its level of protection. While ™ can be used with any common law usage of a mark, ® may only be used by the owner of a mark following registration with the relevant national authority and should conform to the requirements of local trademark law. In general, the requirements and consequences of using or not using symbols or indications that denote trademark marking must be ascertained on a per country basis and consulting with local counsel is always advisable.

After termination of participation in this Arrangement, the terminating Participant shall immediately cease to use the Service Mark and distribute any certificates bearing the Certification Mark of

making reference to this Arrangement. The Participant shall provide its customer the information on the termination of its participation and on its consequences.

The Recognition Arrangement Service Mark as shown in Figure 6 shall be reproduced and shall be reprinted according to the following specifications;

a) in colours coded as shown in Figure 7 and Figure 8; or

b) in black and white as shown in Figure 9 and Figure 10; and

c) in any size, uniformly enlarged or reduced, which makes all the words clearly distinguishable.

When used on paper, it may also be embossed or stamped.

Participants (or Compliant CBs) shall follow the specification as specified in Figure 7, Figure 8, Figure 9, or Figure 10 below.

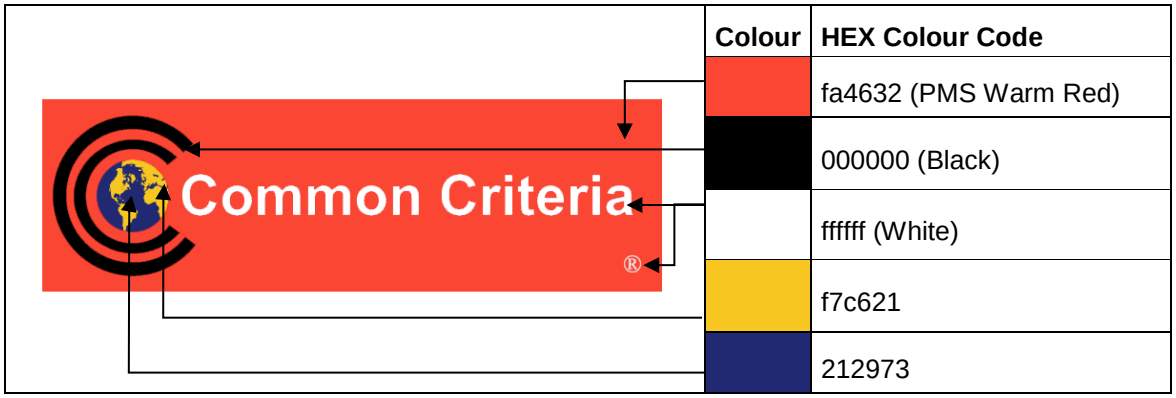

Figure 7: Recognition Arrangement Service Mark in colour with registered symbol

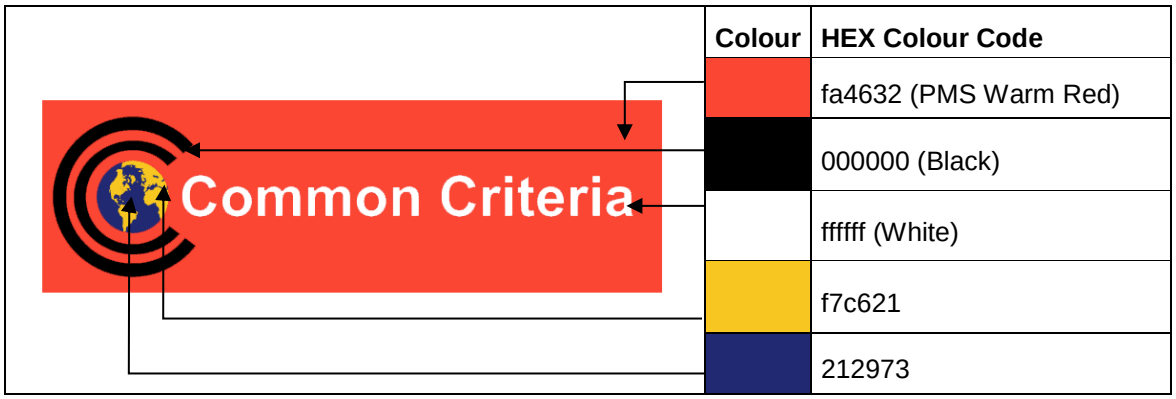

Figure 8: Recognition Arrangement Service Mark in colour without registered symbol

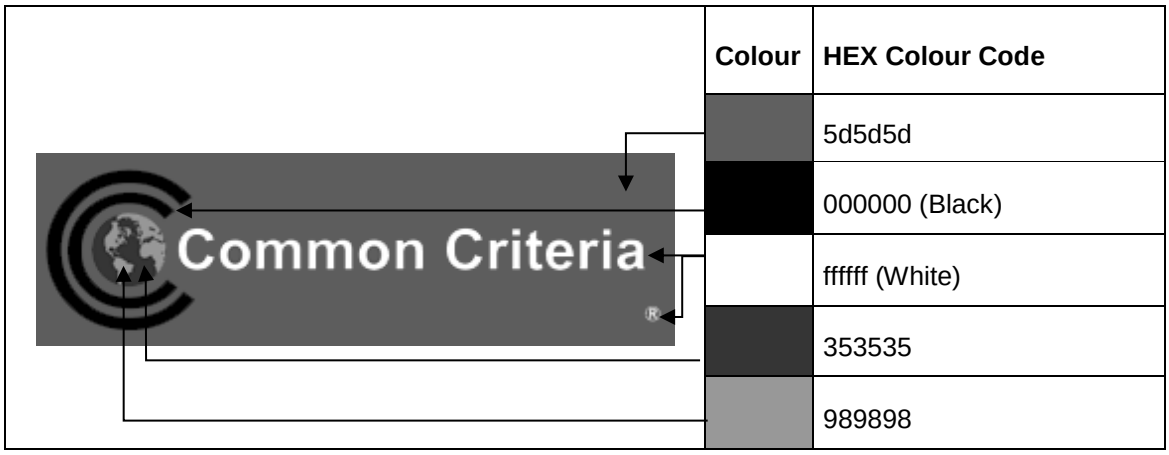

Figure 9: Recognition Arrangement Service Mark in black-and-white with registered symbol

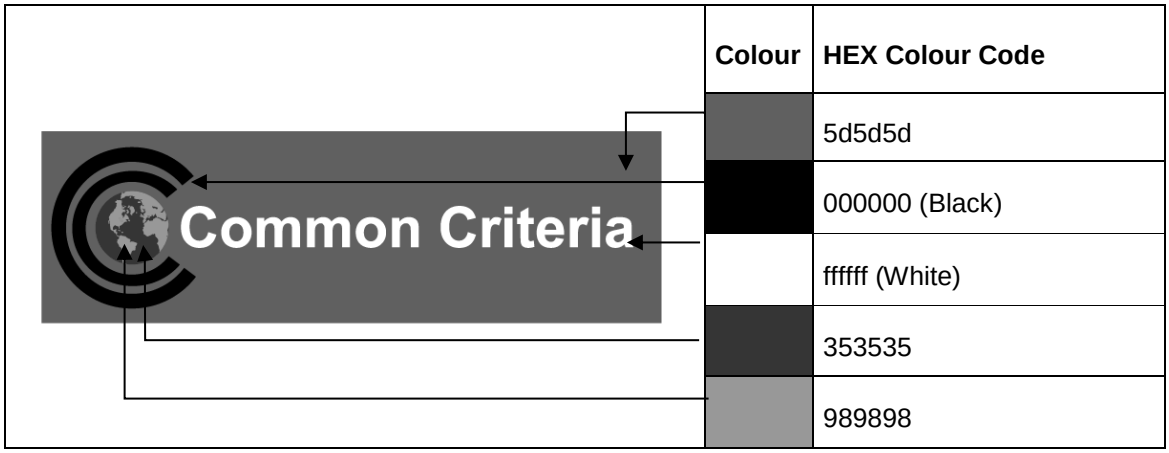

Figure 10: Recognition Arrangement Service Mark in black-and-white without registered symbol

Annex F

Information to be Provided to Participants

F.1 Scheme Documentation

Each Compliant CB is to make available to the Participants copies of the documents covering the following aspects of the Evaluation and Certification/Validation Scheme for which it is responsible:

a) the national set of rules and regulations for Evaluation and Certification/Validation in accordance with mutually agreed IT Security Evaluation Criteria and methods;

b) the organisational structure of the Scheme;

c) the Certification/Validation Body Quality Manual;

d) the policy for ITSEF accreditation or licensing/approval;

e) the titles and addresses of the ITSEFs associated with the Scheme and their status (e.g., governmental or commercial); and

f) if applicable, the national interpretation of ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories (or its successors).

On each occasion that changes are made to these documents, or new versions issued, copies of the modifications or the new version are promptly to be made available to all Participants.

F.2 Common Criteria Certificates and Certification/Validation Reports

Each Participant is to make available to each of the other Participants a copy of each Common Criteria Certificate, Certification/Validation Report and Certified/Validated Products List it authorises. Whenever a Compliant CB omits or removes an IT Product or Protection Profile from its Certified/Validated Products List, such CB should promptly notify the Participants.

F.3 General Information Affecting the Terms of this Arrangement

Each Participant is to provide a statement about the effects of all national laws, subsidiary legislation, administrative regulations and official obligations applying in the country concerned and directly affecting the Recognition of Common Criteria Certificates.

Each Participant should promptly draw to the attention of the Management Committee any changes or prospective changes to:

a) national laws, administrative regulations or official obligations; or

b) the operation or procedures of its Evaluation and Certification/Validation Scheme(s)

which may affect the ability of that Participant to act consistently with the terms of this Arrangement.

F.4 Information Protection Principles

Some of the procedures under this Arrangement may on occasion require the exchange of Protected Information, the unauthorised disclosure of which would cause actual damage to the

Participants, parties associated with the Participants, or parties involved in this Arrangement, including but not limited to IT Product manufacturers. It is important that this information is appropriately handled and that procedures are defined to ensure that such protection is achieved. To this end, each Participant will endeavour to establish a system that applies such procedures. Recognising that the continual advancement of technology has a profound influence on the manner in which information is stored, processed and transmitted, such procedures will require periodic review and update in order to remain relevant to the current state of the art. As a result, the overall principles for information protection are presented here, whereas the specific details of the associated protective procedures are conveyed in Management Committee standard operating procedures.

F.4.1 Creation and Management of Protected Information

Documents and media that contain Protected Information are to be appropriately protected and bear the words "*RA in Confidence*" and a unique identifier from the time that they are created; until such time as the document is either destroyed or where it has been determined that the information content no longer requires protection.

F.4.2 Storage and Transmission of Protected Information

Appropriate access controls should be in place to protect documents during storage and transmission. This will likely include physical controls to address transmission of paper copies of documents, and may also be relevant in cases where documents are shared using transferrable media. In the case of electronic transmission of Protected Information, transmission should be done using secure electronic means.

F.4.3 Access to Protected Information

Unless otherwise agreed with the Originator, and to the extent permitted by law, access to Protected Information received by a Participant is to be restricted to staff who are directly employed by the Participant or, at the discretion of the head of the Participant's organisation, to government officials with a need to know. The duty to keep Protected Information confidential is expected to survive this Arrangement.

Annex G

New Compliant Certification/Validation Bodies

G.1 Formal Request

If a CB wishes to achieve the status of Compliant CB under this Arrangement and believes that it fulfils the conditions laid down in Article 5, the Annexes cited in Article 5 and Interpretations thereof issued by the Management Committee, it should submit an application in writing through the Participant in its country. (Note, the CB and the Participant may be one and the same organisation.) If the Participant supports the application, it becomes the Sponsor of the CB, and it should forward the application to the Management Committee. The forwarded application will not be considered a formal endorsement by the Sponsor of the capability of the applicant to meet the conditions laid down in this Arrangement.

The application is to include a written statement that the applicant wishes to be determined as compliant under this Arrangement and plans:

a) to meet all costs of the primary assessment team (See G.3 below) arising out of the application or out of considering and processing that application (including the travel, accommodation and subsistence costs, and - if and only if the applicant is not applying to become the Associated CB of its Sponsor - also including the salary costs of the primary assessment team[4]) whether or not the application is successful;

b) to provide the documentation detailed below; and

c) to submit for Shadow Certification/Validation a suitable product which is to be evaluated and certified/validated under the applicant's oversight.

G.2 Documentation to be Provided

All documentation and information acquired during the compliance process is to be treated in accordance with the provisions of Annex F.4. These confidentiality rules may be supplemented by means of non-disclosure agreement(s).

The following documentation is to be provided:

a) a full description of the scope, organisation and operation of the applicant's Evaluation and Certification/Validation Scheme, including:

   - the title, address and principal point of contact of the CB;
   - the CB Quality Manual;
   - the subordination of the CB and the statutory or other basis of its authority;
   - the system for overseeing the general management of the Scheme, for deciding questions of policy and for settling disagreements;
   - the procedures for Certification/Validation;

[4] This may be waived if the Qualified Participant carrying out the assessment is prohibited by national law or regulation from receiving such payment.

- the titles and addresses of the ITSEF(s) participating in the Scheme and their status (commercial or governmental);

- the Licensing/Approval Policy and the procedures for accrediting Evaluation Facilities;

- the rules applying within the Scheme to the protection of commercial secrets and other sensitive information;

- the procedures by which the CB ensures that ITSEFs:

    - perform Evaluations impartially;

    - apply the IT criteria Evaluation Methods correctly (i.e. CEM, CC Supporting Documents,.); and

    - protect the confidentiality of sensitive information involved.

b) the latest issue of the Scheme's Certified/Validated Products List;

c) two or more Common Criteria Certificates and Certification/Validation Reports issued under the oversight of the applicant;

d) a statement about the effects of all national laws, subsidiary legislation, administrative regulations and official obligations applying in the country of the applicant and directly affecting the conduct of Evaluations and certifications/validations or the Recognition of Common Criteria Certificates; and

e) a statement that the applicant is not bound by or about to be bound by any law, subsidiary legislation or official administrative order which would give it or the IT Products and Protection Profiles to which it awards Common Criteria Certificates an unfair advantage under this Arrangement or which would otherwise frustrate the operation or intention of this Arrangement.

G.3 Management Committee's Response

The Management Committee is to acknowledge the application within three weeks of its receipt and make a preliminary response to it within a target of three months. The preliminary response should indicate the acceptability of the application assuming that technical examination of the documentation and the Shadow Certification/Validation are successful.

When the Management Committee concurs that the information supplied by the applicant is satisfactory and that no clarification or supplementary information is required, the applicant will be asked to nominate as candidates for Shadow Certification/Validation at least two products evaluated against a collaborative Protection Profile, or a Security Target claiming at least Evaluation Assurance Level 2 and, if appropriate, ALC_FLR where no cPP is used.

The applicant should supply an outline summary of each product and details of the arrangements for its Evaluation and Certification/Validation. The Management Committee is, within a target of one month of receipt of the nomination, to select one of the products for Shadow Certification/Validation and to notify the applicant accordingly.

The Management Committee is to select two or more Qualified Participants (other than the Sponsor) to carry out the Shadow Certification/Validation. The Participants selected are to make nominations for a primary assessment team to consist of two experts. Any Participant (including

the Sponsor) may provide an additional expert at its own expense. The Management Committee is to inform the applicant of the names and parent organisations of the experts.

G.4 Shadow Certification/Validation Procedure

It is for the experts to decide, based on guidance issued by the Management Committee (that will ensure that assessments are performed to a uniform standard) and in the light of all the information available to them, how much of the Evaluation and Certification/Validation process they need to shadow. The Management Committee guidance will be made available to the applicant CB to permit an estimate of the resources required by the assessment.

The experts are to report their findings in writing to the Executive Subcommittee for review prior to submission to the Management Committee within one month of the completion of their investigation and no later than one month from the completion of the Evaluation and Certification/Validation process on the selected product, together with a recommendation on whether the candidate's application should be accepted or rejected. The Management Committee is to convey its decision to the applicant in writing within a target of two months following receipt of the experts' report. In the case of rejection, the Committee should provide a summary of the reasons for the decision and of the principal evidence on which it is based. In the case of acceptance, the Committee should record the decision by updating Annex L accordingly.

Annex H

Administration of the Arrangement

H.1 Responsibilities and Competence

The Management Committee acts in any matters of policy relating to the status, terms and operation of this Arrangement. It decides on the admittance of new Participants, the compliance of CBs, and changes to the scope of the Arrangement.

H.2 Composition

All Participants are to be represented on the Management Committee. The Chairman of the Management Committee is to be appointed annually by the Management Committee from among the Participants. The current chair should provide for administrative support to the Management Committee.

H.3 Decisions

Each country represented on the Management Committee is to have one vote. The Management Committee should always attempt to achieve a unanimous vote, but decisions are to be reached by simple majority, except in those cases where a specific requirement is laid down elsewhere in this Arrangement for unanimity.

H.4 Attendance

The Management Committee may invite experts or technical advisers to attend meetings of the Management Committee to advise on specific issues.

H.5 Use of Experts

The Management Committee may establish ad-hoc groups of experts to provide support and advice as required.

H.6 Frequency of Meetings

The Management Committee will meet in plenary yearly, or as it deems fit. Where practical, it will take decisions by e-mail.

H.7 Executive Subcommittee

The Management Committee should establish an Executive Subcommittee to manage the day-to-day business of the Arrangement and provide advice and recommendations to the Management Committee.

All Participants may be represented on the Executive Subcommittee.

The business of the Executive Subcommittee includes:

a) developing and recommending procedures for the conduct of the business of the Arrangement;

b) assessing the technical compliance of CBs;

c) recommending revisions of this Arrangement;

d) managing the continuous Monitoring activities;

e) managing the promotion of the Common Criteria.

H.8 Development Board

The Management Committee should establish a Development Board to manage the technical aspects of the Arrangement, foster and oversee the development and maintenance of the criteria, associated methodology and the development of collaborative Protection Profiles by suitable International Technical Communities, and to provide technical advice and recommendations to the Management Committee.

All Participants may be represented on the Development Board. .

The business of the Development Board includes:

a) resolving technical disagreements about the terms and application of this Arrangement;

b) managing the development of IT Security Evaluation Criteria and IT Security Evaluation Methods;

c) managing the maintenance of historical databases as to the background to Interpretations and any resultant decisions that could affect future versions of either the criteria or methodology;

d) technical approval of updated criteria, methodology and CC Supporting Documents, to ensure technical consistency;

e) ensuring the effective development of collaborative Protection Profiles by means of suitable technical communities.

Annex I

Contents of Certification/Validation Reports

I.1 Certification/Validation Report and Its Use

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[5] contain Protected Information since, like the Security Target, it contains information for the consumer necessary to securely deploy the evaluated IT Product.

The Certification/Validation Body must ensure that users (risk owners, system integrators, developers and end-users, etc.) have access to relevant information. Some of this information may be provided in other publically available documentation in which case it need not be repeated within the Certification/Validation Report but clear and accurate references must be provided.

Where an International Technical Community has specified the information that must be provided (for example in the cPP or Supporting Documents) this should be contained within or readily available and clearly referenced by the Certification/Validation Report.

I.2 Expected Contents

It is expected that the report (directly or via its references) will contain the following information. This may be expanded in those cases where Supporting Documents requires additional information.

I.2.1 Executive Summary

The executive summary is a brief summary of the entire report. The information contained within this section should provide the reader 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 readers, (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:

a) Name of the evaluated IT Product, enumeration of the components of the product that are part of the Evaluation, developer's name, and product version;

b) Name of IT Security Evaluation Facility;

c) Certification/Validation Identification[6];

d) Completion date of Evaluation;

e) Expiry date (optional); and

[5] Products where all or part of a certification report is considered ‘protected’ and not made public fall outside of this arrangement.

[6] The Certification/Validation Identification is the unique identifier of the certificate (including a number and abbreviation of the schemes name) defined by the Certification/Validation Body.

f) Brief description of the report results:

1) PP to which the product complies or assurance package for ST only Evaluations;

2) functionality;

3) summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT Product;

4) special configuration requirements;

5) assumptions about the operating environment;

6) disclaimers.

I.3 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 labeling 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.

I.4 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.

I.5 Assumptions and Clarification of Scope

The security aspects of the environment/configuration in which the IT Product is expected to be used 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.

I.5.1 Usage Assumptions

In order to provide a baseline for the IT Product during the Evaluation effort certain assumptions about the usage of the 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.

I.5.2 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 have to be made. This section documents any environmental assumptions made about the IT Product during the Evaluation.

I.5.3 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 be the case 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 uncountered threats should be listed for clarification. It would however, be impractical to list all possible threats that cannot be countered by an individual product.

I.6 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-TOE Design (ADV_TDS). The intent of the section is to characterise the degree of architectural separation of the major components.

I.7 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.

I.8 IT Product Testing

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

I.9 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.

I.10 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.

I.11 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 mention of features which are particularly useful.

I.12 Annexes (Optional)

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. complete description of security policy).

I.13 Security Target

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

I.14 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.

I.15 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 their release dates and version numbers.

Annex J

Common Criteria Certificates

The following information is provided for inclusion on all Common Criteria Certificates issued on behalf of Participants to this Arrangement.

J.1 Common Criteria Certificates Associated with IT Product Evaluations with a cPP claimed

A Common Criteria Certificate authorised by a Certificate Authorising Participant resulting from the Certification/Validation of an IT Product Evaluation with a cPP claimed is to include the following information:

Identification of what has been certified (to be printed as a structured text block on the certificate):

a) Certification/Validation Identification;

b) Type of Product;

c) Product Name;

d) Version and Release Numbers;

e) Evaluation Platform of *Target of Evaluation* (optional);

f) Product Manufacturer;

g) Name of Evaluation Sponsor (optional);

Identification of certification result (to be printed as a structured text block on the certificate):

h) Collaborative Protection Profile Conformance (including name, version and Certification ID);

Other items to be placed on the certificate:

i) Name of IT Security Evaluation Facility (optional);

j) Name of Certification/Validation Body and name of Certificate Authorising Participant;

k) Certification/Validation Report Identifier[7];

l) Date Issued;

m) Expiry Date (optional); and

n) Signature of issuing Certification/Validation Body;

[7] The Certification/Validation Report identifier should uniquely identify the document. It should include, as a minimum, the Certification/Validation Body name, the evaluation criteria used, the report number, and year of issue.

The certificate is also to include the following statements:

"The IT Product identified in this certificate has been evaluated [insert "at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of [insert name of Participant's country]"] using the Common Methodology for IT Security Evaluation, [insert version number], [insert if applicable: "and CC Supporting Documents as listed in the Certification/Validation Report"] for conformance to the Common Criteria for IT Security Evaluation, [insert version number]. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the [insert formal name of Scheme] and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the [insert name of Certificate Authorising Participant] [and (if different) name of Certification/Validation Body] or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by [insert name of Certificate Authorising Participant] [or by (if different) name of Certification/Validation Body] or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied."

In addition to the information listed, the Common Criteria Certification Mark referenced in Annex E and a logo of the Scheme shall be placed on each IT Product-related Common Criteria Certificate authorised by the Participant. The Recognition Arrangement Service Mark may also be printed on the certificate.

J.2 Common Criteria Certificates Associated with IT Product Evaluations without a cPP claimed

A Common Criteria Certificate authorised by a Certificate Authorising Participant resulting from the Certification/Validation of an IT Product Evaluation without a cPP claimed is to include the following information:

Identification of what has been certified (to be printed as a structured text block on the certificate):

a) Certification/Validation Identification;

b) Type of Product;

c) Product Name;

d) Version and Release Numbers;

e) Evaluation Platform of *Target of Evaluation* (optional);

f) Product Manufacturer;

g) Name of Evaluation Sponsor (optional);

Identification of certification result (to be printed as a structured text block on the certificate):

h) (if applicable) Protection Profile Conformance (including name, version and Certification ID);

i) Conformance of Functionality[8];

j) Assurance Package (optional) [9];

Other items to be placed on the certificate:

k) Name of IT Security Evaluation Facility (optional);

l) Name of Certification/Validation Body and name of Certificate Authorising Participant;

m) Certification/Validation Report Identifier;

n) Date Issued;

o) Expiry Date (optional); and

p) Signature of issuing Certification/Validation Body;

The certificate is also to include the following statements:

"The IT Product identified in this certificate has been evaluated [insert "at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of [insert name of Participant's country]"] using the Common Methodology for IT Security Evaluation, [insert version number], [insert if applicable: "and CC Supporting Documents as listed in the Certification/Validation Report"] for conformance to the Common Criteria for IT Security Evaluation, [insert version number]. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the [insert formal name of scheme] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the [insert name of Certificate Authorising Participant] [and by (if different) name of Certification/Validation Body] or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by [insert name of Certificate Authorising Participant] [or by (if different) name of Certification/Validation Body] or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied."

In addition to the information listed, the Common Criteria Certification Mark referenced in Annex E and a logo of the Scheme shall be placed on each IT Product-related Common Criteria Certificate authorised by the Participant. In case the assurance package confirmed includes CC Part 3 components above CC Part 3 EAL 2 and, if appropriate, ALC_FLR, the following wording amends the logo: "CCRA recognition for components up to EAL 2 and ALC_FLR only". The Recognition Arrangement Service Mark may also be printed on the certificate.

J.3 Common Criteria Certificates Associated with Protection Profile Evaluations

[8] The conformance statement on functionality should indicate: "PP conformant functionality" or "Product specific Security Target," and "CC Part 2 conformant" or "CC Part 2 extended."

[9] The assurance package confirmed should say "Common Criteria Part 3 conformant", [name of the assurance package (e.g. EAL 2)] and if applicable "augmented by [name of augmented CC Part 3 components]"; or state the conformant Protection Profile Assurance Package.

A Common Criteria Certificate authorised by a Participant resulting from the Certification/Validation of a Protection Profile Evaluation is to include the following information:

Identification of what has been certified (to be printed as a structured text block on the certificate):

a) Certification/Validation Identification;

b) Protection Profile Name/Identifier;

c) Protection Profile Version Number;

d) Protection Profile Developer;

e) Protection Profile Sponsor (optional);

f) Assurance Conformance[10];

Other items to be placed on the certificate:

g) Name of IT Security Evaluation Facility (optional);

h) Name of Certification/Validation Body and name of Certificate Authorising Participant;

i) Certification/Validation Report Identifier;

j) Date Issued;

k) Expiry Date (optional); and

l) Signature of issuing Certification/Validation Body;

The certificate is also to include the following statements:

"The Protection Profile identified in this certificate has been evaluated [insert "at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of [insert name of Participant's country]"] using the Common Methodology for IT Security Evaluation [insert version number], [insert if applicable: "and CC Supporting Documents as listed in the Certification/Validation Report"] for conformance to the Common Criteria for IT Security Evaluation [insert version number]. This certificate applies only to the specific version of the Protection Profile listed in this certificate and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the [insert formal name of Scheme] and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the Protection Profile by the [insert name of Certificate Authorising Participant] [and by (if different) name of Certification/Validation Body] or by any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by [insert name of Certificate Authorising Participant] [or by (if different) name of Certification/Validation Body] or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied."

[10] The conformance claim for the certified product shall list the selected assurance components or if applicable the EAL (e.g. EAL2 or EAL2 augmented by [list of components augmented]).

In addition to the information listed, the Common Criteria Certification Mark referenced in Annex E and a logo of the Scheme shall be placed on each Protection Profile-related Common Criteria Certificate authorised by the Participant. The Recognition Arrangement Service Mark may also be printed on the certificate.

Annex K

Collaborative Protection Profiles

A collaborative Protection Profile (cPP) and related Supporting Documents define the minimum set of common security functional requirements and the Achievable Common Level of Security Assurance. It includes vulnerability analysis requirements to ensure certified products achieve an expected level of security.

K.1 Composition of a cPP

cPPs shall not contain requirements that have a dependency on national conformity assessment schemes.

cPPs may explicitly specify examples of international standards for cryptographic primitives/protocols defined by appropriate international standards bodies. cPPs should also allow use of other national approved primitives/protocols so nations can provide their own refinements.

cPPs shall only include assurance components to a maximum of EAL2, except where the International Technical Community can demonstrate a rationale that activities up to and including EAL4 can be reproduced between schemes. The use of extended assurance components should be avoided unless such a rationale can be provided and is subject to the CCRA approval process.

K.2 CC and CEM

cPPs shall be compliant with the generic framework of the CC and CEM in order to support mutual recognition. Supporting Documents supplementing the cPPs are expected to be created to give Interpretations to the CEM as needed. When a rationale demonstrates that the cPP and/or Supporting Documents cannot express the security needs, the CC and/or CEM may be modified, subject to the CCRA approval process.

K.3 Mutual recognition

CCRA certificates that claim conformance to a cPP shall only cover the assurance requirements defined in the said cPP and related Supporting Documents.

CCRA certificates that claim conformance to a cPP shall only cover the security functionality defined in the said cPP.

Annex L

Compliant CBs

Australasian Certification Authority - Australasian Information Security Evaluation Program
sponsored by
Defence Signals Directorate and Government Communication Security Bureau,
from Australia and New Zealand

Canadian Common Criteria Evaluation and Certification Scheme
sponsored by
Communications Security Establishment,
from Canada

Schema d'Evaluation et Certification Francais
sponsored by
Agence nationale de la sécurité des systèmes d'information,
from France

Bundesamt für Sicherheit in der Informationstechnik (Zertifizierungsstelle)
sponsored by
Bundesamt für Sicherheit in der Informationstechnik,
from Germany

Organismo di Certificazione della Sicurezza Informatica (OCSI)
sponsored by
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione,
from Italy

Japan Information Technology Security Evaluation and Certification Scheme
sponsored by
Ministry of Economy, Trade and Industry, and Information-technology Promotion Agency,
from Japan

Malaysian Common Criteria Evaluation and Certification Scheme
sponsored by
CyberSecurity Malaysia,
from Malaysia

Netherlands Scheme for Certification in the Area of IT Security (NSCIB)
sponsored by
Netherlands National Communications Security Agency (NLNCSA) and operated by TÜV Rheinland Nederland B.V.,
from The Netherlands

Norwegian Certification Authority for IT Security (SERTIT)
sponsored by
Norwegian National Security Authority (NSM),
from Norway

IT Security Certification Center
sponsored by
National Intelligence Service and National Security Research Institute,
from Republic of Korea

Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
sponsored by
Ministerio de Hacienda y Administraciones Públicas and Centro Criptológico Nacional,
from Spain

Swedish Certification Body for IT-Security
sponsored by
Swedish Defence Materiel Administration (FMV),
from Sweden

Ministry of Communications and Information Technology
sponsored by
Department of Electronics and Information Technology,
from Turkey

UK IT Security Evaluation and Certification Scheme
sponsored by
CESG,
from the United Kingdom

National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme
sponsored by
National Institute of Standards and Technology, and National Security Agency,
from the United States of America