Final Version January 8th, 2010

Mutual Recognition Agreement of Information Technology Security Evaluation Certificates

VERSION 3.0

MANAGEMENT COMMITTEE

January 2010

This document supersedes the document “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates – Version 2.0” dated of April 1999 that superseded the document 017/97 Final approved by Senior Officials Group Information Systems Security (SOG-IS) of the European Commission at their meeting on 26 November 1997 in response to point 3 of Council Recommendation 95/144/EC of 7 April 1995.

Table of contents

The Participants....3
Preamble....5
Purpose of the Agreement....5
Spirit of the Agreement....5
Articles....6
Article 1: Membership....6
Article 2: Scope....6
Article 3: Exceptions....6
Article 4: Definitions....6
Article 5: Conditions for Recognition....7
Article 6: Voluntary Periodic Assessments....8
Article 7: Publications....8
Article 8: Sharing of Information....9
Article 9: New Participants and compliant CBs....9
Article 10: Administration of this Agreement....9
Article 11: Disagreements....10
Article 12: Use of Contractors....10
Article 13: Costs of this Agreement....10
Article 14: Revision....10
Article 15: Duration....10
Article 16: Voluntary Termination of Participation....10
Article 17: Commencement and Continuation....10
Article 18: Effect of this Agreement....11
Annexes....12
Annex A: Glossary....12
Annex B: Evaluation and Certification Scheme....18
Annex C: Requirements for Certification Body....21
Annex D: Voluntary Periodic Assessments....24
Annex E: Certificate and Agreement Marks....26
Annex F: Information to be Provided to Participants....27
Annex G: Compliant Certification Bodies....30
Annex H: Administration of the Agreement....34
Annex I: Contents of Certification Reports....36
Annex J: Common Criteria or ITSEC Certificates....40
Annex K: Compliant CBs....42
Annex L: IT-Technical Domains....44

The Participants

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

and

Bundesamt für Sicherheit in der Informationstechnik - BSI
from Germany

and

CESG
from the United Kingdom

and

Netherlands National Communications Security Agency (NLNCSA), Ministry of the Interior and Kingdom Relations (BZK)
from The Netherlands

and

Swedish Defence Materiel Administration (FMV)
from Sweden

and

Organismo de Certificación de la Seguridad de las Tecnologías de la Información
Centro Criptológico Nacional - CCN
from Spain

and

Finnish Communications Regulatory Authority (FICORA)

from Finland

and

Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security (SERTIT)

from Norway

PLAN TO COOPERATE IN THE FOLLOWING MANNER,

Preamble

Purpose of the Agreement

The Participants in this Agreement share the following objectives:

a) to ensure that *evaluations* of *Information Technology (IT) products* (as defined in Annex A) 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* process for IT products and protection profiles.

The purpose of this Agreement is to advance those objectives by bringing about a situation in which IT products and protection profiles which earn a *certificate* 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 Body (CB)* issuing *Information Technology Security Evaluation Criteria (ITSEC)* or *Common Criteria (CC)* certificates should meet high and consistent standards.

The operation of multiple CBs by a Participant or of purely commercial CBs does not comply with the intent of the Agreement, which requires mutual trust and understanding between governmental organisations in addition to compliance with certain standards. Therefore, the operation of the Agreement 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 Agreement.

Spirit of the Agreement

The complexity of IT-products 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. In exercising such judgement, the Participants will endeavour to use the level of assurance in the IT product under evaluation as their metric. The Participants in the Agreement 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.

The Participants will endeavour to work actively to improve the application of the criteria and methodology, for example by developing and establishing more cost-effective 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.

Articles

Article 1: Membership

Participants in this Agreement are government organisations or government agencies from countries of the European Union or *EFTA*, 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 products and protection profiles. *Certificate authorising Participants are authorizing compliant CBs* (described in Article 5) operating in their own country or countries and *authorise* their certificates. Purely commercial CBs or multiple CBs authorized by a Participant are excluded from being recognized as compliant within this Agreement. 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, in respect of *IT products* (as defined in Annex A) and *protection profiles*, the Participants plan to *recognise the conformant certificates* (as described in Article 5) which have been authorised by any other certificate authorising Participant in accordance with the terms of this Agreement and in accordance with the applicable laws and regulations of each Participant. This Agreement covers claims of compliance against any of the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through E3 with Strength of Mechanisms 'basic'. Recognition of higher assurance levels (including *augmentations*) can be defined for specific *IT technical domains* as agreed by the *Management Committee* and as defined in Annex L. This recognition requires additional proof of competencies as defined in Annex G.

Article 3: Exceptions

If recognition of a *conformant certificate* would cause a Participant to act in a manner inconsistent with applicable national, international or European Community law or regulation, that 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 equivalent *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. Moreover this Agreement does not constrain separate bilateral or multilateral agreements regarding certification and recognition for some sensitive government systems.

Article 4: Definitions

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

Article 5: Conditions for Recognition

Except as otherwise provided in this Agreement, the Participants commit themselves to recognise applicable conformant certificates authorised by any certificate authorising Participant. Such authorisation confirms that the evaluation and certification processes have been carried out in a duly professional manner:

a. on the basis of accepted *IT security evaluation criteria* (hereinafter *criteria*),
b. using accepted IT *security evaluation methods* (hereinafter *method*s),
c. in the context of an *Evaluation and Certification Scheme* managed by a *compliant CB* in the authorising Participant's country,
d. and that the *conformant certificates* authorised and *Certification Reports* issued satisfy the objectives of this Agreement.

Certificates which meet all these conditions are termed conformant certificates for the purposes of this Agreement.

The IT security evaluation criteria are to be those laid down in the Common Criteria for Information Technology Security Evaluation (CC) and in the Information Technology Security Evaluation Criteria (ITSEC), the versions endorsed by the Management Committee and the evaluation methods are to be those laid down in the *Common Evaluation Methodology for Information Technology Security Evaluation (CEM),* in the *Information Technology Security Evaluation Manual (ITSEM)* and *JIWG supporting documents*, the versions endorsed by the Management Committee. The minimum requirements for Certification Reports are laid down in Annex I to this Agreement. The minimum requirements for an Evaluation and Certification Scheme are laid down in Annex B to this Agreement. An evaluation and certification is 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 17025 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 Agreement;

and,

b) the CB is accepted as compliant, and

- either has been accredited in its respective country by a recognised Accreditation Body in accordance with EN 45011 or in accordance with a national interpretation of EN 45011 which at minimum satisfies the requirements as specified in Annex C of this Agreement,

- or has been established under laws, statutory instruments, or other official administrative procedures valid in the country concerned and meets the requirements of EN 45011 or the requirements laid down in Annex C of this Agreement.

In order to assist the consistent application of the criteria and methods between Evaluation and Certification Schemes, the Participants plan to work towards a uniform *interpretation* of the currently applicable criteria and methods and commit to accept the *JIWG supporting documents* that results from this work. 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. The Participants plan also to work on JIWG supporting documents concerning dedicated evaluation techniques like e.g. penetration methods or so-called *Attack Methods*, that shall be implemented by the CB claiming a *Qualifying status* for specific *IT technical domains*.

In further aid to the goal of consistent, credible and competent application of the criteria and methods, the CB shall 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 criteria and methods correctly and consistently;

c) have and maintain the required technical competencies; and

d) adequately protect the confidentiality of *protected information*.

Article 6: Voluntary Periodic Assessments

Assessment of compliant CBs should take place on a regular basis for the purpose of assuring that they continue to share the objectives of this Agreement.

Taking into account the related workload, the Management Committee endeavours to perform such assessments for each compliant CB at periodic intervals not more than five years. The Management Committee selects two or more Qualified Participants to carry out the periodic assessments. In case of suspected non-compliance of a compliant CB, the Management Committee should give priority to the compliance assessment of this CB.

The form of such assessments is set out in Annex D to this Agreement.

Article 7: Publications

Conformant 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 Scheme, the mark of the Recognition Agreement and a standard form of words. The mark and the form of words are given in Annex E and Annex J to this Agreement.

Where either the assurance level of the certificate is higher than the *Recognition level* or, the *IT technical domain* is not covered by the Qualifying status of the compliant CB, then the compliant CB commits itself not to use this mark unless having joined it together with the level of Recognition and the *IT technical domains* of Recognition for which it has Qualifying status as granted by the Management Committee.

Each certificate authorising Participant shall publish a *Certified Products List* that encompasses all valid certificates issued by its Scheme.

Article 8: Sharing of Information

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

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

In particular, each Participant shall 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 Agreement.

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

Article 9: New Participants and compliant CBs

Participants

Participation in this Agreement is open to representatives from countries of the European Union or EFTA that plan to uphold the principles of the Agreement.

Certification Bodies

A CB may be determined to be compliant for the purpose of Article 5 of this Agreement upon unanimous consent of the existing Participants, if the existing Participants are confident that it can fulfil the conditions for recognition set out in Article 5 of this Agreement and Annexes cited in Article 5, and that it satisfies the conditions for compliance, according to the procedures laid down in Annex G of this Agreement, including shadow certification.

Article 10: Administration of this Agreement

A Management Committee shall administer this Agreement, according to written Terms of Reference (ToR). The Management Committee shall meet at least once per year or as often as required to consider matters affecting the status, terms or application of this Agreement. All Participants shall be represented on the Management Committee.

The Management Committee shall adopt the Joint Interpretation Working Group (JIWG) to provide technical advice and recommendations to the Management Committee as laid down in Annex H, and to work on interpretations, on attack methods and to propose and work on *IT technical domains* as mentioned in Article 5.

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

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 conformant 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 Agreement, they shall ensure that these contractors have appropriate expertise. Contractors shall not be responsible to carry out the procedures set out in Annex D, in Annex G or in Annex H of this Agreement. Protected information shall be passed to contractors only with the agreement of the originator, as laid down in Annex F.4.

Article 13: Costs of this Agreement

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

Article 14: Revision

Any modification of the terms of this Agreement will require the unanimous agreement of the Participants. Any adopted modification shall be recorded in a written document signed by all the Participants.

Article 15: Duration

Cooperation under this Agreement 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 Agreement, or terminate the compliant status of any CB that it represents, by notifying the other Participants in writing.

Article 17: Commencement and Continuation

This Agreement or any subsequent modification is to enter into force on the date on which it has been signed by all its Participants.

In terms of continuation, the Qualified Participants under the previous version of this Agreement (Mutual Recognition Agreement of Information Technology Security Evaluation Certificates – VERSION 2.0, April 1999) as listed in Annex K.1 along with their qualifying status are certificate authorising Participants de facto under this new version of the Agreement.

This is valid for a period of five years. A Voluntary Periodic Assessment should take place within five years in accordance with Article 6.

Furthermore,

- all conformant certificates previously issued by these Qualified Participants remain recognised under the new version of this Agreement,

- certificates resulting from products that have been accepted into the certification process before the new Agreement (as notified by the Qualified Participants) comes into force will be recognised under the new version of this Agreement and

- re-certifications and maintenance addenda will be recognised under the new version of this Agreement for a period of two years after the new agreement comes into force.

Article 18: Effect of this Agreement

It is recognised and accepted by each of the Participants that this Agreement does not create any substantive or procedural rights, liabilities or obligations that could be invoked by persons who are not signatories to this Agreement. Additionally, it is recognised and accepted by each of the Participants that this Agreement 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 Agreement in any domestic or international court or tribunal. Reports issued by a CB or conformant certificates authorised by a Participant do not constitute endorsement, warranty or guarantee by that Certification Body or Participant, respectively, of IT products or protection profiles; nor does recognition of conformant certificates authorised as a result of certification activities constitute the endorsement, warranty, or guarantee in any way of Certification Reports issued by another CB or resulting certificates authorised by another Participant, respectively.

Annexes

Annex A: Glossary

This glossary contains definitions of certain terms in the text or Annexes of this Agreement which are used in a sense peculiar to this Agreement or which have a meaning crucial to the interpretation of this Agreement. It also contains definitions of certain other terms used in this Annex. Where the definitions in this Annex differ from definitions of the same terms given in CC, ITSEC, CEM or ITSEM, the definitions in this Annex are to be used in establishing the intended meaning of this Agreement. Such definitions are broadly consistent with those given in CC, ITSEC, CEM and ITSEM, which remain generally valid. The differences are in the interest of greater clarity in the specific context of this Agreement. 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.

Approved:

See *licensed*.

Approval Policy:

See *licensing policy*.

Assessment of compliant CBs:

A procedure for establishing that the *evaluations* and *certifications* carried out by a particular *compliant CB* continue to be as set out in this Agreement.

Attack Methods:

A set of documents describing technical penetration methods that shall be known and implemented by the CB claiming a *Qualifying status*. These documents are applicable to specific *IT technical domains* and are produced under the auspices of the *Management Committee*.

Augmentation:
The addition of one or more requirement(s) to a package

Authorisation:

The sanction by a Participant of the issuing of a *conformant certificate* by a *compliant CB*, permitting the use of the recognition mark.

CB:

Certification Body.

Compliant CB:

A CB that fulfils the conditions for recognition set out in article 5 of this Agreement and Annexes cited in article 5 and that satisfies the conditions for compliance according to the procedures laid down in Annex G of this Agreement."

CC:

Common Criteria for Information Technology Security Evaluation, a document describing a particular set of *IT security evaluation criteria*. The CC have been the subject of the standard ISO 15408.

CEM:

Common Evaluation Methodology for Information Technology Security Evaluation, a document which describes a particular set of *IT security evaluation methods*. The CEM has been the subject of the standard ISO 18045.

Certificate:
A brief publicly available document in which is confirmed by a *Certification Body* that a given *IT product* or *protection profile* has been awarded a certain assurance level, following evaluation by an *ITSEF*. A Certificate always has associated with it a *Certification Report*.

Certification:

The process carried out by a *CB* leading to the issuing of a *certificate*.

Certification Body:

An organisation responsible for carrying out *certification* and for overseeing the day-to-day operation of an *Evaluation and Certification Scheme*.

Certification 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 Products List:

A publication giving brief particulars of currently valid *conformant certificates* in accordance with this Agreement.

Client:

A party in contract with an *ITSEF* for an evaluation.

Conformant 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 *conformant certificate* always has associated with it a *Certification Report*.

EFTA:

European Free Trade Association.

Evaluation:

The assessment of an *IT product* or a *protection profile* against the *IT security evaluation criteria* and *IT security evaluation methods* to determine whether or not the claims made are justified.

Evaluation and Certification Scheme:

The systematic organisation of the functions of *evaluation* and *certification* 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.

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 Report*.

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 or hardware, providing functionality designed for use or incorporation within a multiplicity of *systems or within a specifically defined operational environment and with a particular purpose*.

ITSEC:

Information Technology Security Evaluation Criteria, a document published by the European Commission, describing a particular set of *IT security evaluation criteria*.

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 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 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 Scheme*.

ITSEM:

Information Technology Security Evaluation Manual, a document published by the European Commission, which describes a particular set of *IT security evaluation methods*.

IT System:

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

IT technical domain:
A family of IT products that require common technical competencies, especially with regard to the vulnerability analysis, for performing the evaluation. These IT technical domains shall be defined by the Management Committee.

JIWG:
Joint Interpretation Working Group: Executive working group working on behalf of the *Management Committee* as defined in Annex H.

JIWG supporting documents:

A set of documents that describe how the criteria and evaluation methods are applied when certifying specific technologies and that shall be accepted by the Participants as laid down in Article 5.

Licensed:

Assessed by a *CB* as technically competent in the specific *IT technical domain* and field of IT security *evaluation* and formally *authorised* to carry out *evaluations* within the context of a particular *Evaluation and Certification Scheme*.

Licensing policy:

A part of the essential documentation of every *Evaluation and Certification 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.

Management Committee:

The body, on which all *Participants* are represented, which endeavours to ensure the operation of this Agreement 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.

Originating party:

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*.

Participant:

A signatory to this Agreement.

Certificate Consuming Participant:

A Participant with a national interest in recognising *conformant certificates*.

Certificate Authorising Participant:

A Participant representing a *compliant CB*.

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*).

Protected information:

Information gathered or obtained under the processes or activities in this Agreement 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 the 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.

Protective marking:

A marking, as the *security classification*, used under the provisions of national law, subsidiary legislation, administrative regulation or official obligation where information has to be protected.

Qualifying Status:

The status granted to a *CB* where recognised by the *Management Committee* as compliant under this Agreement.

Recognition level:

Level of recognition for *conformant certificates* issued by a *compliant CB*.

Recognition of conformant certificates:

Acknowledgement by Participants that the evaluation and certification processes carried out by *compliant CBs* appear to have been carried out in a duly professional manner and meet all the conditions of this Agreement, and the intention to give all resulting *conformant certificates* equal weight. This acknowledgement may be restricted to specific *IT technical domains* and to some assurance levels depending on the *recognition level* of the *compliant CB*.

Recognise:

See *Recognition of conformant certificates*.

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:

implementation-dependent statement of security needs for a specific identified Target of Evaluation

Shadow certification:

Assessment of a CB in which representatives of at least two *Qualified Participants* monitor the evaluation and certification of an *IT product* in accordance with this Agreement.

Target of Evaluation:

An *IT product* and its associated administrator and user guidance documentation that is the subject of an *evaluation*.

Annex B: Evaluation and Certification Scheme

B.1 The Purpose and Principal Characteristics of a Scheme

The main purpose of an Evaluation and Certification Scheme (hereinafter referred to as a Scheme) is to ensure, through the systematic organisation and management of the functions of evaluation and certification, 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 Body, which is responsible not only for the certification 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 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 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 to ensure that mechanisms are in place to ensure that the interests of all parties with a stake in evaluation and certification 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 Agreement is necessarily based.

B.2 The Role and Principal Characteristics of the CB

The CB is independent of the ITSEFs, and staffed by appropriately qualified personnel.

It may be established under the provisions of a law, subsidiary legislation 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 of EN 45011 or the requirements as specified in the Annex C of this Agreement.

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

a) to authorise the participation of Evaluation Facilities in the Scheme (see further below) and to avoid that an Evaluation Facility is licensed by more than one Compliant CB of this Agreement. The licensing by more than one Compliant CB could only be done in special cases where there is a specific agreement between the *Participants* involved. The Management Committee should be notified.

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 ensure that ITSEFs have appropriate competencies in the field of IT security and vulnerability analysis;

d) to ensure that sensitive information relating to products and protection profiles under evaluation and to the process of evaluation itself is given the security protection it requires by establishing and routinely following appropriate handling procedures within the Scheme.

e) to issue additional guidance to ITSEFs as required;

f) to monitor all evaluations in progress within the Scheme at an appropriate level and to ensure that the technical monitoring required by the agreement is performed by technical personnel of the governmental body as part of the CB.

g) to review all evaluation reports (including especially 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;

h) to produce a Certification Report in respect of each evaluation completed under the auspices of the Scheme;

i) to publish conformant certificates and their associated Certification Reports;

j) to publish regularly a document giving brief particulars of all products and protection profiles evaluated within the Scheme which hold a currently valid conformant certificate (Certified Products List);

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

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

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

n) 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 Agreement, the Certification Body associated with a Qualified Participant is also responsible for providing technical support to activities relating to this Agreement in accordance with the provisions of this Agreement.

B.3 Accreditation and Licensing of Evaluation Facilities

Unless an Evaluation Facility has been established under a law or statutory instrument or other official administrative procedure, 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's demonstrating its impartiality and its general technical, methodological and procedural competence and in particular that it meets the requirements of ISO 17025 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. Therefore, the CB performs an assessment of the skills, the equipment and the technical competence of the ITSEF, specifically in those *IT-technical domains* the ITSEF is working on, by auditing the ITSEF on an a regular basis (two years minimum).

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 (ITSEF).

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 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.

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 Scheme;

d) documentation clearly identifying its legal status.

C.4 Certification 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 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;

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; it is to be sufficiently complete to enable the course of each certification to be traced. All records are to be securely and accessibly stored for a period of at least five years.

C.7 Certification Procedures

The CB is to have the required facilities and documented procedures to enable the IT product or protection profile certification to be carried out in accordance with the applicable IT security evaluation criteria and methods.

C.8 Requirements of Evaluation Facilities

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

The CB is to draw up for each IT Security Evaluation Facility a properly documented agreement covering all relevant procedures including agreements for ensuring confidentiality of protected information and the evaluation and certification 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 personnel;

d) details of training arrangements for certification 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 monitoring that ITSEFs have competencies in the domain of IT security and in particular of vulnerability analysis;

h) details of procedures for preventing the abuse of conformant certificates;

i) the identities of any contractors and details of the documented procedures for assessing and monitoring their competence;

j) 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 shall have adequate arrangements to ensure confidentiality of the information obtained in the course of its certification 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 activities under this Agreement.

C.11 Publications

The CB is to produce and update as necessary a Certified 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 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 Periodic Review

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

C.14 Misuse of conformant Certificates

The CB is to exercise proper control over the use of its conformant 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 Scheme.

C.15 Withdrawal of conformant Certificates

The CB is to have documented procedures for withdrawal of conformant certificates and is to advertise the withdrawal in the next issue of its Certified Products List.

Annex D: Voluntary Periodic Assessments

The Management Committee may select two or more Qualified Participants (excluding the CB's Authorizing Participant) 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 Authorizing Participant, and such consent may be withdrawn or revoked prior to or during an assessment. The Authorizing Participant 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 qualified 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 *compliant CBs* should be distributed among the Qualified Participants in an equitable manner, to be agreed by the Management Committee (including the travel, accommodation and subsistence costs).

Where the CB undergoing the periodic assessment has already undergone in the five last years an assessment through an equivalent procedure within the framework of another international Mutual Recognition Agreement (MRA), the Management Committee may decide to exempt partly the compliant CB from the procedures laid down here. For that purpose, all necessary information on that other MRA, its procedures and the results of that assessment shall be provided by the compliant CB. If recognition for IT technical domains is concerned, the partial exemption will not mean to avoid a visit to the CB during the assessment, it should be only a reduction in the duration of it.

The CB undergoing the periodic assessment should within one month provide the complete scheme documentation as described in Annex G.2 and applicable at the time. The experts review the documentation to assure that the CB continues to share the objectives of this Agreement, and report their findings to the Management Committee.

A Shadow Certification as described in Annex G should be performed on at least two EAL3 or EAL4 (CC level) resp. E2 or E3 (ITSEC level) candidate evaluations as agreed upon by the Participants directly involved. At least one of these must be an EAL4 (CC) resp. E3 (ITSEC) evaluation. However, if the compliant CB has a Qualifying status for specific IT technical domains including an assurance level (including augmentations) higher than ”E3” (ITSEC) or ”EAL4” (CC), the compliant CB shall be assessed in addition on its competencies in monitoring vulnerability analysis in the *IT technical domains* (for which it has Qualifying status). This assessment shall be conducted as described in Annex G.5. In the latter case, the Management Committee may also decide to carry out audits ”on site” of the compliant CB and associated ITSEFs as described in Annex G.5.

The experts shall satisfy themselves that the CB undergoing the periodic assessment is acting consistently in respect of all aspects of the evaluation and certification processes. In carrying out this responsibility, the experts may wish to take part in some aspects of the certification 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 Agreement, particularly in Annexes B and C to this Agreement.

At appropriate stages of the evaluation and certification, 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 body;

d) the certification report.

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

The experts report their findings to the Management Committee, and make a recommendation on the assessment. The Management Committee reviews the report on the shadow procedures, the audits and the vulnerability analysis assessments. 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 Body undergoing the assessment.

Where shortcomings have been identified, the Management Committee shall decide whether they affect the reliability of the certificates issued by that Certification Body and could possibly withdraw provisionally the Qualifying status or restrict the recognition level or the *IT technical domains* covered by the Qualifying status. In any case, the CB being assessed should demonstrate that it has rectified any shortcomings within a maximum of six months, otherwise the Management Committee may decide to withdraw definitively the Qualifying status.

Annex E: Certificate and Agreement Marks

Every conformant certificate issued under the terms of this Agreement is to bear the mark shown below:

Figure 1: SOGIS-Logo

Where either the assurance level of the certificate is higher than the Recognition level or, the IT technical domain is not covered by the Qualifying status of the compliant CB tho logo has to be joined with a statement as follows:

1. The Assurance level of the certificate is higher than the recognition level or the IT technical domain so that is not covered by the Qualifying status of the compliant CB: “for components up to EAL 4” or “for components up to E3 basic”
2. The Assurance level of the certificate exceeds an upper bound of an IT technical domain: “for components applicable for the IT technical domain concerned”. The IT technical domain shall either be referred to in the certificate or the certification report.

This mark confirms that the conformant certificate has been authorised by a Participant to this Agreement and it is the Participant’s statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments contained in the certificate and the Certification Report are those of the compliant Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

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 Scheme for which it is responsible:

a) the national set of rules and regulations for evaluation and certification in accordance with mutually agreed IT security evaluation criteria and methods;

b) the organisational structure of the Scheme;

c) the Certification Body Quality Manual;

d) accreditation or licensing/approval policy;

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

f) (if applicable) the national interpretation of ISO 17025.

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

F.2 Common Criteria or ITSEC Certificates and Certification Reports

Each Participant is to provide to each of the other Participants a copy of each Common Criteria or ITSEC certificate, Certification Report and Certified Products List it authorises. The Certification Report or certificate copy could be provided in the manner of a link in the certified product list of the CB official website. Whenever a compliant CB omits or removes an IT product or protection profile from its Certified Products List, such CB should promptly notify the Participants.

F.3 General Information Affecting the Terms of this Agreement

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 or ITSEC 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 Scheme

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

F.4 Confidentiality Rules

Some of the procedures under this Agreement 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 Agreement, 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.

A document may be in paper (hard copy) or in electronic form.

Documents which contain protected information are to be identified by a special marking "RA in Confidence". The originating party should apply this special marking.

Each Participant will endeavour to enforce the protection rules which follow and to establish a system to apply them.

F.4.1 Creation and management of protected information

Every document which contains protected information is to bear a brief, but clear indication of the identity of the originator and the date of issue. It is also to have an identifier to make it unique (e.g. a one-up serial number). If the document is modified, then its identifier is also to be modified, at least to the extent of a version number and the date of issue.

A document remains protected either for the period stated on the document or, in the absence of a specific statement, until the originating party no longer claims protection for the protected document.

F.4.2 Procedures for handling protected information

Marking of protected information

Paper copies of documents which contain protected information are to bear on each page the words "RA in Confidence" and the unique identifier. The period of protectability may be shown on the first page.

Removable magnetic media for computers which contain protected information, are at a minimum, to have a label bearing the words "RA in Confidence" and a unique identifier. A listing on paper of the content should be attached to the magnetic medium whenever it is transported from one Participant to another.

Storage and rules for safeguarding protected information

Storage and safeguarding rules are applicable to documents containing protected information, including draft versions.

When protected information is processed or stored on a computer, it should be appropriately safeguarded. Any removable magnetic medium on which protected information is stored should be safeguarded as though it were a document containing the same information.

Transmission of protected information

Documents containing protected information which are to be sent through the mail, are to be enclosed in an inner and outer envelope system. The outer envelope should bear the address of the person nominated by the receiving Participant as a point of contact for RA correspondence. The inner envelope(s) should contain the protected information, and bear the words "RA in Confidence" together with the name of the intended recipient.

In case of electronic transmission of protected information, transmission should be done using secure

electronic means.

Copying of protected information

Protected information may be copied by a recipient only when this can be clearly justified on operational grounds.

Disposal of removable magnetic media and protected information

When no longer required, removable magnetic media containing protected information should be disposed of in a secure manner, and this action recorded in an appropriate register.

Protected information should be thoroughly erased from magnetic media prior to disposal.

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 Agreement.

F.4.3 Additional degree of protection

Occasionally, the information may require an even higher degree of protection. This is to be determined on a case-by-case basis.

Annex G: Compliant Certification Bodies

G.1 Formal Request for achieving status of new compliant CB

If a CB wishes to achieve the status of new compliant CB under this Agreement against any of the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through E3 and believes that it fulfils the conditions laid down in Article 5 and the Annexes cited in Article 5, 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 should forward the application to the Management Committee. The forwarded application will not be considered a formal endorsement of the capability of the applicant to meet the conditions laid down in this Agreement.

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

a) If requested by the shadowing nations, 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) whether or not the application is successful

b) to provide the documentation detailed below (See G.2); and

c) to submit for shadow certification (See G.4) by representatives of two or more of the Participants, suitable products which are to be evaluated and certified 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 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;
- the titles and addresses of the ITSEF 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 mutually agreed IT criteria and methods correctly and consistently; and
    - protect the confidentiality of sensitive information involved.

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

c) two or more Common Criteria or ITSEC certificates and Certification 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 or the recognition of Common Criteria or ITSEC certificates;

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 or ITSEC certificates an unfair advantage under this Agreement or which would otherwise frustrate the operation or intention of this Agreement; and

f) where the CB has already been granted a Qualifying status through a similar procedure within the framework of another international Mutual Recognition Agreement (MRA), all necessary information on this Qualifying status and on this MRA.

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 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 at least two products for which a EAL3 or EAL4 (CC level) resp. E2 or E3 (ITSEC level) evaluation level as a minimum is claimed. At least one of these must be an EAL4 (CC) resp. E3 (ITSEC) evaluation.

The applicant shall supply an outline summary of each product and details of the arrangements for its evaluation and certification. The Management Committee will, within a target of one month of receipt of the nomination, select two of the products for shadow certification and notify the applicant accordingly.

The Management Committee is to select two or more Qualified Participants (other than the CB's Authorizing Participant) to carry out the shadow certification. The Participants selected are to make nominations for a primary assessment team to consist of two experts. Any Participant (including the Authorizing Participant) may provide an additional expert at its own expense. Other Participants (qualified or not) can propose to attend as observers to the assessment. The Management Committee could define a limit in the number of them, but a minimum of two observers should be allowed. The Management Committee is to inform the applicant of the names and parent organisations of the experts.

Where the CB applicant has already been granted a Qualifying status through a similar procedure within the framework of another international Mutual Recognition Agreement, the Management Committee may decide to exempt partly the applicant from the procedures there laid down.

G.4 Shadow Certification 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 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 Management Committee within one month of the completion of their investigation and no later than one month from the completion of the shadow procedure on the selected products, together with a recommendation on whether the candidate's application should be accepted or rejected. The Management Committee is to make its decision based on the experts' report and recommendation. The Management Committee is then 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 shall record the decision by updating Annex K accordingly.

G.5 Achieving the status of compliant CB for higher recognition level

G.5.1 Formal request and prerequisites

If a CB wishes to achieve the status of compliant CB under this Agreement for *IT technical domains* including higher assurance levels (including augmentations) than the Common Criteria Evaluation Assurance Level 4 or ITSEC Assurance Level E3, it should submit an application in writing through the Participant in its country to the Management Committee. The *IT technical domains* amongst those defined by the Management Committee and its assurance levels for which recognition is requested shall be included in the application.

The application is to include a written statement that the applicant plans:

a) If requested by the shadowing nations, to meet all costs of the primary assessment team arising out of the application or out of considering and processing that application (including the travel, accommodation and subsistence costs) whether or not the application is successful;

b) to provide the documentation necessary for the instruction of the application as requested by the Management Committee;

c) to submit for shadow certification by representatives of two or more of the Participants, suitable products where required by the Management Committee;

d) to perform, when required by the Management Committee, specific vulnerability analysis, assessed by two or more of the Participants, on IT products selected by the Management Committee.

e) to accept an audit "on site" of the CB and of the associated ITSEFs, when required by the Management Committee, carried out by the Participants designated by the Management Committee for this task.

The prerequisites for the CB applicant to be fulfilled are:

a) to have the status of compliant CB for the EAL4 (CC) or E3 (ITSEC) level under this Agreement for more than one year; and
b) to have issued at least three conformant certificates recognized under this Agreement.

Where the CB applicant has already been granted a Qualifying status through a similar procedure within

the framework of another international Mutual Recognition Agreement, the Management Committee may decide to exempt partly the applicant from the procedures there laid down.

G.5.2 high level Recognition procedure

The Management Committee is to acknowledge the application within two months of its receipt and make a preliminary response on the procedure to be followed by the applicant and on the documentation to be provided.

Generally, the applicant shall be asked to undergo a Shadow Certification in the same way as described in section G.3 and section G.4 for each *IT technical domain* including its higher assurance levels resp. augmentations than the Common Criteria Evaluation Assurance Level 4 or ITSEC Assurance Level E3 as requested by the applicant.

Additionally, the technical competencies of the CB and of the ITSEFs with regard to the vulnerability analysis in the requested *IT technical domains* shall be assessed by the Management Committee. For that purpose, the Management Committee may require:

- to carry out an audit ”on site” of the Scheme in order to assess the technical competencies of the ITSEFs through discussion with the staff and visit of the premises ;

- to ask the applicant to perform vulnerability analysis against the Attacks methods on the products selected by the Management Committee.

The audits and the assessments of vulnerability analysis shall be conducted by a team of experts designated by the Management Committee amongst the Qualified Participants in the requested *IT technical domains* by default or, failing that, by Qualified Participants in another *IT technical domain*s. In the latter case, the management committee may decide to apply a cross shadow procedure.

G.5.3 Management Committee's Response

The experts are to report their findings on the Shadow procedures, the audits and the vulnerability analysis assessments in writing to the Management Committee within one month of the completion of their work, together with a recommendation on whether the candidate's application should be accepted or rejected. The Management Committee is to make its decision based on these reports and recommendations. This decision may be either to reject the application, or to accept it possibly with limitations regarding the level of Recognition or regarding the *IT technical domains* covered.

The Management Committee is then to convey its decision to the applicant in writing within a target of two months following receipt of the experts’ reports. 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 shall record the decision by updating Annex K accordingly.

Annex H: Administration of the Agreement

H.1 Responsibilities and Competence

The Management Committee acts in any matters of policy relating to the status, terms, and operation of this Agreement. It decides upon the compliance of CBs and defines the procedures to address the application of CBs and, in particular, defines IT technical domains for recognition at levels beyond EAL4 / E3 based on propositions by the Management Committee working group (JIWG) in accordance with H.7. The detailed operation of the Management Committee shall be governed by a 'Terms of Reference' Document approved by the Management Committee and reviewed on a regular basis.

H.2 Composition

All Participants are to be represented on the Management Committee. The Chairman of the Management Committee is to be appointed by the Management Committee from among the Participants to serve for a period of not more than two years on a voluntary basis. The current chair should provide for administrative support to the Management Committee including the maintenance of documents and correspondence.

H.3 Decisions

Each country represented on the Management Committee is to have one vote. For those cases where a specific requirement is laid down elsewhere in this Agreement for unanimity (such as voting on compliance of CBs) then voting is obligatory and, if there are any abstentions, then it shall not be considered unanimous approval. In all other cases the aim should always be to achieve a unanimous vote but, where this proves impossible in the first ballot, then a second ballot shall be held and positive votes from at least 2/3rd of the whole membership shall be required in order for the motion to pass.

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. These will generally be operated and report via the JIWG.

H.6 Frequency of Meetings

The Management Committee will meet in plenary as it deems fit, at least once a year. Where practical, it will take decisions by e-mail.

H.7 Management Committee Working Group

The Management Committee shall adopt the Joint Interpretation Working Group (JIWG) to provide technical advice and recommendations to the Management Committee, and to work on interpretations, on attack methods and to propose and work on IT technical domains. The JIWG shall consist of Qualified Participants and additional discretionary Participants (on a voluntary basis) up to a numerical limit determined by the Management Committee. The business of that Working Group includes:

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

b) recommending revisions of this Agreement;

c) advising on the technical disagreements about the terms and application of this Agreement;

d) contributing to the development of IT security evaluation criteria and IT security evaluation methods;

e) developing and managing the JIWG supporting documents as to the background to interpretations and advising on any resultant decisions that could affect the application of either the criteria or methodology;

f) developing Attack methods for *IT technical domains* and proposing the *IT technical domains* and its assurance level and augmentations for which recognition can be claimed by the CBs.

The detailed operation of the JIWG shall be governed by a 'Terms of Reference' Document approved by the JIWG, reviewed by the JIWG on a regular basis, and endorsed by the Management Committee.

Annex I: Contents of Certification Reports

I.1 Certification Report and Its Use

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

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

I.2 Executive Summary

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

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

b) Name of IT security evaluation facility;

c) Completion date of evaluation; and

d) Brief description of the report results:
   - assurance package;
   - functionality;
   - summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product;
   - special configuration requirements;
   - assumptions about the operating environment;
   - 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 in should be included in this section. The section provides a means to articulate the clarification of the scope of the evaluation with respect to threats that are not countered. Users can make informed decisions about the risks associated with using the IT product. Usage, environmental assumptions, and clarification of the scope of the evaluation with respect to threats that are not countered should be stated in this section.

I.5.1 Usage assumptions

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

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 has 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 occur that some clients will assume that some threats are being met by the IT product but in fact they are not. It is for these reasons that these 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 for instance on the deliverables described in the Common Criteria assurance family entitled Development-High Level Design (ADV_HLD). The intent of the section is to characterise the degree of architectural separation of the major components.

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 is 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

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 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 the proper release date, and proper version numbers.

Annex J: Common Criteria or ITSEC Certificates

The following information is provided for inclusion on all certificates issued on behalf of Participants to this Recognition Agreement.

J.1 Certificates Associated with IT Product Evaluations

A certificate authorised by a Participant resulting from the certification of an IT product evaluation is to include the following information:

a) Product Manufacturer;

b) Product Name;

c) Type of Product;

d) Version and Release Numbers;

e) Protection Profile Conformance (if applicable);

f) Evaluation Platform (optional);

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

h) Name of Certification Body;

i) Certification Report Identifier[1];

j) Date Issued; and

k) IT security evaluation criteria and methodology used and their version

l) Assurance Level or Package confirmed[2].

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 methodology for IT Security Evaluation *[insert name of the methodology and version number],* for conformance to the criteria for IT Security Evaluation *[insert name of the criteria and 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 report. The evaluation has been conducted in accordance with the provisions of the *[insert formal name of the scheme]* and the conclusions of the evaluation facility

1 The Certification report identifier should uniquely identify the document. It should include, as a minimum, the Certification Body name, the evaluation criteria used, the report number, and year of issue.

2 For Common Criteria certificates, the assurance package confirmed should distinguish between Common Criteria Evaluation Assurance Level Part 3 conformant and Common Criteria Evaluation Assurance Level Part 3 augmented. Augmentation should be designated by a plus, (e.g., EAL 3 +) or by listing the augmented components names. Augmentations shall be outlined in detail in the certification report.

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 Qualified Participant]* or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by *[insert name of Qualified Participant]* 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 mark referenced in Annex E shall be placed on each IT product-related certificate authorised by the Participants.

J.2 Common Criteria Certificates Associated with Protection Profile Evaluations

A Common Criteria certificate authorised by a Participant resulting from the certification of a protection profile evaluation is to include the following information:

a) Protection Profile Developer;

b) Protection Profile Name/Identifier;

c) Version Number;

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

e) Name of Certification Body;

f) Certification Report Number;

g) Date Issued; and

h) Assurance Package required for a product conformat to the Protection Profile[3].

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]* 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 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 Qualified Participant]* or by any other organisation that recognises or gives effect to this certificate, and no warranty of the profile by *[insert name of Qualified Participant]* 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 mark referenced in Annex E shall be placed on each protection profile-related Common Criteria certificate authorised by the Participants.

3 The assurance package confirmed should distinguish between Common Criteria Evaluation Assurance Level Part 3 conformant and Common Criteria Evaluation Assurance Level Part 3 augmented. Augmentation should be designated by a plus, (e.g., EAL 3 +) or by listing the augmented components names. Augmentations shall be outlined in detail in the certification report.

Annex K: Compliant CBs

K.1 CBs with a Qualifying status when the agreement comes into force

This chapter lists the Compliant CBs and their qualifying status when the agreement comes into force.

Centre de Certification National de la Direction
Centrale de la Sécurité des Systèmes d'Information
authorized by
Agence Nationale de la Sécurité des Systèmes d'Information
from France
Qualifying status:

- including the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through Level E3 with Strength of Mechanisms 'basic' and
- the IT technical domain "Smart card and similar devices" as defined in annex L

Bundesamt für Sicherheit in der Informationstechnik (Zertifizierungsstelle)
authorized by
Bundesamt für Sicherheit in der Informationstechnik,
from Germany
Qualifying status:

- including the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through Level E3 with Strength of Mechanisms 'basic' and
- the *IT technical domain* "Smart card and similar devices" as defined in annex L

UK IT Security Evaluation and Certification Scheme
authorized by
CESG
from the United Kingdom
Qualifying status:

- including the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through Level E3 with Strength of Mechanisms 'basic' and
- the *IT technical domain* "Smart card and similar devices" as defined in annex L

Netherlands Scheme for Certification in the Area of IT Security (NSCIB)
authorized by
Netherlands National Communications Security Agency (NLNCSA), Ministry of the Interior and Kingdom Relations (BZK)
from the Netherlands
Qualifying status:

- including the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through Level E3 with Strength of Mechanisms 'basic' and
- the *IT technical domain* "Smart card and similar devices" as defined in annex L

Organismo de Certificacion del Esquema Nacional de Evaluation y certificacion de la Securidad de las Tecnologias de la Informacion
authorized by
Centro Criptologico Nacional
from Spain

Qualifying status:

- including the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through E3 with Strength of Mechanisms 'basic'.

K.2 CB candidates for a qualifying status before the agreement comes into force

This chapter lists the CBs that have applied for the qualifying status.

Organismo de Certificacion del Esquema Nacional de Evaluation y certificacion de la Securidad de las Tecnologias de la Informacion
authorized by
Centro Criptologico Nacional
from Spain
Candidate for Qualifying status: according to annex L.1

K.3 Compliant CBs with a qualifying status after the agreement comes into force

This annex will list the Compliant CBs and their qualifying status accepted by the Management Committee after the agreement comes into force in addition to annex K1. This list will be kept in a separate document to be updated by the Management Committee as required.

Annex L: IT-Technical Domains

This annex will list the technical domains accepted by the Management Committee after the agreement comes into force. This list will be kept in a separate document to be updated by the Management Committee as required.

L.1 Smart card and similar devices

L.1.1 Definition

This section provides the scope and rationale for the *IT-Technical Domain* with Smart card and similar devices.

The *IT-Technical Domain* is related to smart cards and similar devices where significant proportions of the required security functionality depend upon hardware (for example smart card hardware, smart card composite products , TPMs used in Trusted Computing, digital tachographs, Host Security Modules, etc.).

Rationale
In the technologies covered by the scope above an attacker will often be able to obtain ready physical access to the device (or a set of devices), the device may well contain critical information such as security credentials/keys and part of the security functionality required of the device will relate to self protection either by active (tamper detection) or passive means (such as tamper resistant coatings). This contrasts with standard multipurpose hardware as used in a general processing equipment such as a PC. The evaluation approach needs to consider all hardware specific aspects of vulnerability analysis including those that require significant additional equipment and resources. Such devices are frequently composed from elements produced by different developers (for example hardware, smart card operating system, and application) and may involve production across a range of development sites (e.g. IC design, mask production, fabrication, characterisation, etc). These factors must also be consistently taken into account during evaluation and certification.

L.1.2 List of approved JIWG supporting documents for the IT-Technical Domain ”Smart card and similar devices”

The JIWG supporting documents listed in the following are related to the IT-Technical Domain ”Smart card and similar devices” and are approved with the version indicated at the time when this agreement comes into force. The documents listed below support the evaluation up to EAL 7. They are monitored and updated by the JIWG as defined in Annex H.7

Document Title	Version	Type
Guidance for Smartcard evaluation	1.2	Guidance
The Application of Attack Potential to Smart Cards	2.7	Mandatory
The Application of CC to Integrated Circuits	3.0	Mandatory
Composite product evaluation for Smartcards and similar devices and ETR-template lite for composition	1.0 1.0	Mandatory Guidance
Requirements to perform IC evaluations including Annex A	1.0	Mandatory
Attack Methods for Smartcards and Similar Devices	1.5	Mandatory