Mutual Recognition Agreement

of

Cybersecurity Evaluation Certificates

issued under an

Fixed-time Certification Process

March 23rd, 2022

Version 1.0

Table of contents

The Participants

Agence Nationale de la

Sécurité des Systèmes d'Information - ANSSI

representing France

and

Bundesamt für Sicherheit in der Informationstechnik - BSI

representing Germany

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 cybersecurity evaluations of products containing Information Technology (IT) and certification processes done by means of an fixed-time certification process as addressed by this Agreement are performed to reasonable and consistent standards, and are seen to contribute significantly to the confidence put in them;
b) to improve the availability of evaluated, security-enhanced products containing IT;
c) to eliminate the burden of duplicating evaluations of products containing IT within the applicant;
d) to continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for products containing IT.

The purpose of this Agreement is to advance those objectives by bringing about a situation in which products containing IT, which earn a certificate issued under a fixed time certification process can be 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 certificates under a fixed-time certification process should meet 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 Participants will endeavour to guarantee a consistent and comparable level of assurance in their respective fixed-time certification processes to ensure mutual trust in the certificates issued by each Participant. 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 their national criteria and methodology based on a common approach described in Annex C.

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 and operating as a *Certification Body* (CB).

Article 2: Definitions

Terms crucial to the meaning of this Agreement or which are used in a sense particular 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 3: Scope of Recognition

Except as provided otherwise in this Agreement, the Participants commit themselves to recognise certificates as comparable with each other if issued according to a *fixed-time certification process* defined in Annex B of this Agreement and authorised by any Participant.

Article 4: Technical Meetings

Biannual technical meetings shall be held between the Participants in order to:

- share difficulties raised during evaluation;
- share national specific methodologies applied for some particular products or market sectors that have been formalised or are under creation;
- develop common specific methodologies on topics interesting all Participants;
- approve common specific methodologies in the context of this agreement;
- identify possible improvements in the certification processes with the goal of having the best balance between the time of evaluation and the efficiency of its contribution to assurance.

If needed, additional meetings may be requested by either member of this agreement.

Article 5: Exceptions

A Participant may decline to recognise a certificate if there is evidence that this certificate was not obtained through a process that meets the requirements of Annex C of this Agreement or if a national specific methodology is required for the particular product by either of the Participants.

If recognition of a conformant certificate (as described in Article 3) would cause a Participant to act in a manner inconsistent with applicable national, international or European Community law or regulation, a Participant may decline to recognise such a certificate.

Article 6: Publications

Each participating CB shall publish a *Certified Products List* that encompasses all *valid certificates* issued by its certification process as described in Annex B. This list also indicates the exceptions resulting from the application of article 5.

Each participating CB shall further publish a list of national specific methodologies that may result in the application of article 5.

Article 7: 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 *IT Security Evaluation Facility*, CB, or Participant only if prior agreement has been obtained in writing from the third party concerned. Every *IT Security Evaluation Facility*, CB, or Participant shall use its reasonable best effort to obtain the permission of the third party concerned.

In particular, each Participant shall *promptly* provide information on prospective changes, which might affect its ability to perform a process that meets the requirements of Annex C of this Agreement or which might otherwise frustrate the operation or intention of this Agreement.

Article 8: New Participants and Certification Processes

a) Participants

Participation is limited to representatives of Germany and France. A future revision (see Article 12) may open the Agreement to any representatives correspondent to Article 1 from countries of the European Union or EFTA that plan to uphold the principles of the Agreement.

b) Certification processes

A certification process may be determined to be added to Annex B of this Agreement upon unanimous consent of the existing Participants, if the existing Participants are confident that this certification process meets the requirements of Annex C of this Agreement and is therefore comparable to the existing certification processes in Annex B.

Article 9: Disagreements

Participants should make every effort to resolve disagreements between themselves by negotiation. Failing this, disagreements should in the first instance, be referred to the Certification body managers. If the disagreement cannot be resolved by discussion or negotiation, individual Participants may choose not to recognise affected conformant certificates.

Article 11: 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 12: Revision

Any modification of the terms of this Agreement or its annexes will require the unanimous agreement of the Participants. Any adopted modification must be recorded in a written document signed by all the Participants prior to their coming into effect.

A revision of this agreement is planned two years after its first signature in order to consider setting up a peer review process between Participants and consider opening the agreement to new members.

Article 13: Duration

Cooperation under this Agreement continues for a duration of two years unless the Participants decide unanimously to end it prior to this date. The Participants acknowledge that the Agreement is intended for conversion into a permanent Agreement after its termination if the cooperation has proven fruitful.

Article 14: Voluntary Termination of Participation

Any Participant may terminate its participation in this Agreement by notifying all other Participants four weeks prior in writing.

Article 15: 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.

All conformant certificates previously issued by the Participants in the last 36 months before the signature date remain recognised under this Agreement even if some certificates are not fully conformant with Annex C.

Article 16: 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 products containing IT; 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 particular 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.

CB:

Certification Body

Certificate:

A brief publicly available document in which is confirmed by a *Certification Body* that a given product containing IT has successfully fulfilled the requirements of the certification scheme, following evaluation by an *ITSEF*. A Certificate always has associated with it a Certification Report.

Conformant Certificate:

Certificates that meet the conditions of Article 3 of this Agreement.

Valid Certificate:

A certificate that has been obtained in a process defined in Annex B and is currently valid according to the national law of a Participant of this Agreement.

Certification Body:

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

Certification:

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

Certified Products List:

A publication giving brief particulars of currently valid *conformant certificates* in accordance with this Agreement including the certification report and the security target.

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.

Product containing IT:

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.

ITSEF:

IT Security Evaluation Facility, an Evaluation Facility according to national law, licensed or approved to perform evaluations within the context of a particular IT Security Evaluation and Certification Scheme.

Participant:

A signatory to this Agreement**.**

Annex B: List of Comparable Certification Processes

This agreement covers certificates issued under the following fixed time certification processes:

1. CSPN (Certification de sécurité de premier niveau) by ANSSI

2. BSZ (Beschleunigte Sicherheitszertifizierung) by BSI

Annex C: Requirements on Certification Scheme

This Annex describes the certification scheme covered by this Agreement.

General framework of certification

The certification scheme contains a time-constrained certification process focused on the analysis, through penetration tests made by an ITSEF licensed or approved for its technical skills, of a product's strength/robustness to a level of attacker equivalent to AVA_VAN.3 of Common Criteria.

Actors

CB skills

The CB shall have sufficient technical skills to supervise and, if need be, to challenge evaluation results.

ITSEF skills

Licensed ITSEF must have sufficient technical skills to lead vulnerability analysis comparable to AVA_VAN.3 level of Common Criteria.

The ITSEF shall be able to perform state of the art penetration testing and shall be capable to perform cryptographic analysis for products that include evaluated cryptographic features, when such analysis is required.

The CB shall ensure that ITSEFs are able to protect sensitive information managed as part of their activities.

A license is delivered by the CB to confirm these abilities.

The CB is responsible for the harmonization of evaluations' results among the different ITSEFs it has granted a license.

Evaluation

Security Target (ST)

At least, the ST shall define the scope of the evaluation, i.e. the perimeter, version of the product, security problem and functionality to evaluate.

The ST shall follow a structure, predefined for each scheme; harmonization of the ST structures might be sought later on.

The ST shall be validated by the CB at the beginning of the certification project. Validation here means that the scope and TOE perimeter are sound and meaningful and that the ST is not misleading. Yet errors or inconsistencies may be exposed by the ITSEF during the evaluation.

Unicity

One product version shall equal one evaluation: no change of the product is allowed during an evaluation, especially to correct a bug. Only minor changes of the documentation – ST, guides – to clarify or specify the intended use cases or to adjust security recommendations are allowed.

The handling of product series within one evaluation is scheme dependent, and should be designed to allow the mutual recognition of individual product certificates within the series. A detailed common approach will be harmonized.

Evaluation workload

The evaluation workload shall be estimated by the ITSEF and validated by the CB.

The default workload is set to 25m*d, plus 10m*d when cryptographic mechanisms are implemented in essential security functions of the product.

Unless national or common specific methodologies require otherwise, the workload in an initial certification shall not be less than 15 m*d or more than 50 m*d, plus 10m*d when cryptographic mechanisms are implemented in essential security functions of the product.

National or common specific methodologies may be defined that can legitimate the increase or reduction of the evaluation workload[1].

If the TOE perimeter is too large to fit into the maximum workload for an evaluation:

- if relevant, the project shall be split into several sub-projects, each one being evaluated separately;
- otherwise, no certification under this agreement shall be performed and an alternative evaluation strategy shall be sought.

Evaluation deliverables

They shall contain, at least:

- The product itself, in a testable condition (provided with a test environment if required),
- The ST as validated by the CB,
- User and/or security Guidance,
- Detailed specifications and source code for cryptographic analysis, when applicable.

The ITSEF shall be able to perform all relevant tests, even those that may put the product out of use.

Mandatory evaluation tasks

The ITSEF shall perform at least the following tasks:

- A compliance analysis: check that the claimed security functionalities are actually implemented, and in conformance with their description and the security objective to be fulfilled,
- A vulnerability analysis: attempt to compromise the assets described in the ST by searching potential vulnerabilities in the TOE, and analysing their applicability:
    - *product-specific* vulnerabilities (e.g. bypassing, weakening or deactivating security functions through penetration testing);
    - generic vulnerabilities (e.g. vulnerabilities affecting the class of products to which the TOE belongs, or vulnerabilities affecting, by design, standard protocols used by the TOE);
    - known vulnerabilities (e.g. public vulnerabilities of the TOE of its components, but also non-public vulnerabilities of proprietary components of the TOE).

  It should include, whenever it is relevant, an expert opinion on vulnerabilities introduced by the TOE on its environment (e.g. a TOE requires unnecessary privileges to run on its host OS, a TOE allows an attacker to bounce back to another network device in this environment …).
- A review of the guides: ensure that relevant security recommendations are provided to users,
- A cryptographic analysis.

It is considered that unjustified deviations from best practices can lead to a FAIL verdict.

Theoretical cryptographic analysis shall be made in compliance of the SOG-IS ACM (agreed Cryptographic Mechanisms).

---

[1] E.g.: great number of security functions to be evaluated, implementation of proprietary protocols, product series, parts of the security functionalities being implemented in external components etc. may lead to an increase of the workload.
On the contrary, instrumented or rooted product, provision of the source code, delivery of an unciphered firmware or reevaluation may lead to a reduction of the workload.

For protocols that are not in the scope of the SOG-IS ACM, the CB shall endorse the analysis provided by the lab or perform it itself.

If the cryptographic analysis cannot be performed in its entirety due to missing evidence (which the applicant cannot provide) this fact shall be clearly mentioned in the certification report. A detailed common approach for these cases will be harmonized.

Presentation of evaluation work

The ITSEF provides an Evaluation Technical Report (ETR) detailing:

- The ToE and its version,
- The test environment, with OS, equipment and software components of the platform on which tests were performed,
- The list of evaluated functions,
- The reference of analysed documents (security target, guides),
- The evaluation workload used (if different from what had been agreed upon prior to the evaluation),
- A summary of evaluation tasks, including any non-conformity and potential vulnerabilities identified,
- An analysis of results, attack paths and vulnerabilities; for the rating of attacks, the Common Criteria table is used. The Attack Potential considered corresponds to AVA_VAN.3 level.
- An expert advice and the resulting ITSEF verdict on the evaluation results,
- Recommendations if need be:
    - To operate the product in a secure state,

The ETR is established according to a national template.

It is first to be submitted to the CB, in order to confirm the ITSEF verdict before it is given to the developer.

Certification

Verdict

The verdict shall be based on the results of the evaluation, especially the conformity and vulnerability analysis performed by the ITSEF.

The CB shall approve the ETR and confirm or disprove the ITSEF verdict.

The validation of the ETR requires the CB to challenge the ITSEF during a presentation of the evaluation results.

The presentation meeting can lead to an update of the ETR by the ITSEF. If need be, additional tests may be requested to the ITSEF.

The developer's opinion can only be taken into account later in a confrontation with the CB and optionally the involved ITSEF.

If the final verdict is PASS, the CB shall establish a certification report.

The certification report shall describe at least:

- The ToE and its evaluated version,
- The test environment, including OS, hardware and software components of the platform on which test were performed,
- The list of evaluated functions,

- The reference of the analysed documents (security target, guides)
- The workload dedicated to the evaluation,
- A Summary of the evaluation work,
- The final verdict,
- If need be, recommendations to operate the product in a secure state.

Surveillance/reassessment and maintenance

Surveillance/reassessment and certificate maintenance are recognized in the same way as initial certifications.

Information on vulnerabilities after certification

The developer shall provide an e-mail address for third parties to report (potential) security issues that shall be included in the certification report.

The developer informs the CB about any vulnerability discovered after certification affecting the certified version.

The management of declared vulnerabilities will be aligned on procedures defined within the SOG-IS.

Language

National languages and English can be used indifferently. An English version of implemented procedures for each scheme must be available.

Recognition mark

A common logo is affixed on the certificate list to identify the recognition framework applicable to each certificate.