JIL Crisis Policy
Dated: October 2023
Approved: November 2023
Version: 1.0

SOG-IS Recognition Agreement
Management Committee
Policies and Procedures

Document ID: JIL-Crisis Policy
Subject: JIL Temporary crisis operational SOGIS evaluation and certification policy and rules

Introduction

1 The circumstances of the crisis are considered as external events, extraordinary and impossible to prevent, in particular (the list is not exhaustive):

— war, including civil war, riots and acts of terrorism,

— natural disasters, such as strong storms, hurricanes, earthquakes, floods, long-lasting strong precipitation,

— pandemic.

2 A precondition for all evaluation and certification activities is that the maintenance of site-security is continuously ensured.

3 There might be the crises where the precondition is not guaranteed, e.g., a war can cause, among others:

— destruction of necessary infrastructure (energy, communications),

— massive cyber attacks by state-sponsored organisations (beyond the scope of CC),

— lack of availability of key personnel for long time,

— ensuring the secure transport of TOE items is not possible,

— the site is inaccessible.

4 The JIWG crisis policy excludes the crisis in which the maintenance of the site security cannot be considered as ensured.

5 To support continuity of the business the following considerations and temporary rules have been agreed on for the operation of the parties involved. Beside the consideration of certification principles, the rules comply aspects of:

- ALC evaluation,
- reusability of site audit results,
- reusability of ETR-COMP,

as well as some generic considerations for the ITSEF, the Certification Body and the developer organisation.

6 SOGIS-MRA members are aware that the rules defined gain certain lower assurance than in place normally. Nevertheless, SOGIS-MRA members accept this as a temporarily solution to support the parties involved in CC certification during the crisis and to be able to continue business.

Applying members

7 The rules defined are applicable to the Certification Schemes of Certificate Authorizing Participants of SOGIS-MRA as listed at https://www.sogis.eu/uk/status_participant_en.html.

Procedures for entering and exiting the crisis situation

8 Every Authorizing Participant of SOGIS-MRA can initiate the procedure by informing the JIL Working Group Chair on the crisis occurrence; the report describes the type of crisis and possible Authorization Participants or types of operations affected.

9 Upon identification of the crisis occurrence, the JIL Working Group Chair organizes the consultation among the JIL Working Group participants using the way of communications which is appropriate to the case.

10 The JIL Working Group formulates its recommendation to the Management Committee. The recommendation contains justification, specific measures proposed, the original scope of application (i.e., whether all or only specific certification schemes, or specific types of operation, are affected), to be applied to the case.

11 In particular, the JIL Working Group recommendation shall refer to relevant deliverables in the schemes (the list is not exhaustive):

- STAR reports (site certifications),
- ETRs and other applicable documents which result from affected evaluation and certification activities.

12 The JIL Working Group recommendation shall propose the wording to be included in the evidence resulted from affected activities.

13 The Management Committee decides to introduce the state of crisis indicating the rules, the scope of application and measures undertaken.

14 The Management Committee decision can be executed temporarily only and it is limited to 6 months by default.

15 In the case of a longer-lasting state of crisis, the Management Committee decision can be revised and extended, if necessary, based on the JIL Working Group assessment and its further recommendation.

Certification principles

16 The Certification Bodies of the SOGIS-MRA Authorizing Participants will follow common principles for maintaining mutual recognition within SOG-IS MRA during the crisis and its related temporarily restrictions on safety and health care for personnel involved:

17 A certificate issued based on work affected by the crisis should represent a comparable level of quality (i.e., no lower) as before the crisis and acceptable level of assurance (i.e, temporary level) according to a given temporary national policy.

18 Evidence required by CC/CEM and Supporting Documents to be applied under normal conditions shall still be provided (although possibly through adjusted procedures) and evaluated accordingly.

19 Procedures that are adjusted and the application of modified rules due to the crisis should be documented and at all times be kept up to date and communicated to people who are affected (e.g. in the Certification Report, STAR).

20 The following chapters outline aspects of procedures and rules the SOGIS-MRA authorizing members have specifically agreed on for temporarily use.

ALC evaluation aspects

Verification of measures implemented

21 Within the evaluation of the CC ALC assurance class the procedures and practices established and the measures implemented at the related developing and production sites need to be verified by the evaluator.

22 According to e.g. CEM ALC_DVS.2-4 and other related work units as well as CEM Appendix A.4 the evaluator has to assess the related documentation and associated evidences and to verify the implemented measures by a site visit as a well established method.. The following rules applies only in the case that traveling is not possible due to a governmental decree or other statement made by an appropriate authority which is legally binding. Other restrictions such as a quarantine period or company policies are not acceptable as a valid reason for the denial of a regular on-site audit.

23 Therefore, the following rules shall be established:

24 In the first place, a site visit that is planned to be done during a specific evaluation procedure shall if possible be postponed to the latest possible date within the scheduled evaluation procedure assuming that there is a certain chance that travel restriction are being relaxed until this later point in time. This item might be more applicable for on-site audits as part of a product evaluation than an audit for a site certificate.

25 In case an on-site visit is not possible within the timeframe of a product or site evaluation scheduled the evaluator shall do, after consultation with the responsible certification body, a document based ALC evaluation as defined by the CC/CEM/JIL requirements. To gain some assurance that measures are implemented on site so far, the evaluator shall request “alternative evidence” or remote controls supported and provided by the responsible operator of the site. Such “alternative evidence” could be, but are not limited to: process evidences confirming that a process step defined has been performed, photo and video material generated by a responsible person on site possibly with date/time/location attached, interviews of the evaluator by phone or video conference with specific persons on-site responsible for certain aspects, etc. Confidentiality requirements have to be fulfilled adequately when using online interaction with audio and or video means.

In beforehand the evaluator and certifier agree on the kind and amount of “alternative evidence” sensible and applicable to be considered.

Such audit is called a “virtual audit”. The evaluation report, the related certification report and if provided the STAR (Site Technical Audit Report according to related

JIL requirements) shall state if such specific audit has been performed and the date of the “virtual audit”, typically the date of delivery of the “alternative evidence”.

A document-based site evaluation with “virtual audit” can be performed for a ALC site re-evaluation as well as for a new site to be considered.

For a re-evaluation an IAR outlines the changes at the site and updated documentation needs to be provided as usual. It is recommended that, if possible, the evaluator is the same person as for the initial site audit assuming that he remembers the site and the persons on-site involved and thus he can more easily judge on the measures implemented.

For an initial site evaluation, the related documentation needs to be provided and evaluated in detail. The “virtual audit” part shall comprise a more intense interaction between evaluator and site personnel than for a re-evaluation.

Validity and reuse

26 A document-based site evaluation with “virtual audit” performed as defined above provides less assurance than the on-site audit of the evaluator. Therefore, the “virtual audit” can be reused within a product evaluation for a maximum of 18 months counted from the date of the “virtual audit” as stated in the certification report or STAR to the approval date of the product evaluation ETR. The reduced reuse time frame from 30 months for a regular audit to 18 months gathered by a “virtual audit” reflects the lower warranty on assurance causing an increased risk for the reusing party. A virtual audit can be reused up to 24 months in the case that it is a re-audit of a physical audit by the same ITSEF and with no or minor change of the scope of the physical audit and of the implemented processes.

Despite from the 18 / 24 months mentioned, a “virtual audit” should be replaced by a regular on-site audit as soon as the restrictions of the crisis and scheduling of the parties involved allows for. The maximum validity of all virtual audits in total is 72 months after the last regular on-site audit (or 42 months after the first virtual audit if no regular on-site audit ever took place).

27 To decide whether the audit results can be reused for 18 months of for 24 months the STAR report shall include the following information:

- Type of the audit performed: virtual or physical.
- Type of the previous audit: virtual or physical.
- Description of major changes at the site since the previous audit.

Reuse of ETR-for-Composition

28 The reuse time frame for an ETR-for-Composition is defined in the SOGIS JIL Document “Composite product evaluation for Smart Cards and similar devices”. Chapter 6, [R42] with “not more than one and a half year”. Based on previous pandemic crises experience, it is expected that ITSEFs have reorganised their business adequately in order to start and to perform the AVA assessment and penetration testing required for an ETR-for-Composition early enough to fulfil the composite evaluation project needs.

29 In exceptional cases, e.g. when testing personnel is ad hoc not available due to the crisis situation, a delay in providing an ETR-for-Composition document expected to be used in a composite evaluation may occur. With confirmation of this delay by the Platform Certification Body, the Composite Certification Body can extend the acceptance of the existing old version of the ETR-for-Composition from 18 up to 24 months. A composite Certification Body making use of such extension may ask the platform Certification Body for a partial update of the ETR-for-Composition, if already available.

ITSEF organisation

30 The security measures in the working environment of an evaluator are established in order to protect the developers and ITSEF IP and to not-jeopardize the AVA rating. The accreditation and licensing requirements of the scheme apply according to the MRA.

31 In case the national regulations caused by the crisis are in place they need to be followed. Therefore, the Certification Body may allow the ITSEF to temporary deviate from the standard rules such as if working from a non audited environment is needed. The allowance is accompanied by adequate technical and organisational measures for physical and logical security to be followed as defined by the responsible Certification Body having the confidentiality claims on evidences and evaluation results in mind. The sponsor of an evaluation should be informed and agree as e.g. a NDA in place could be affected.

Certification Body organisation

32 The security measures in the working environment of a certifier are established to protect the developers and ITSEF IP and to not-jeopardize the AVA rating. The requirements of the MRA apply.

33 In case the national regulations caused by the crisis are in place they need to be followed. Therefore, the Certification Body may temporarily deviate from its standard rules but applying adequate technical and organisational measures for physical and logical security having the confidentiality claims on evidences and evaluation results in mind.

Developer organisation

34 The developers' concept for protecting the development and production environment and the claims on confidentiality and integrity are essential for the rating of AVA aspects in an evaluation. Such concept is part of the evaluation in ALC class. A document like the JIL MSSR document as published on the SOGIS website includes a lot of aspects to be considered.

35 In case the national regulations caused by the crisis are in place they need to be followed. Related modifications in developers' security procedures and measures have to be taken into account by the evaluation.