ILNAS/SANCC/Pr001
National supervision scheme

Modification : Corrections mineures

1, avenue du Swing
L-4367 Belvaux
Tél. : (+352) 247 743 55

supervision-cybersecurite@ilnas.etat.lu
https://portail-qualite.public.lu

Contents

I Abbreviations

ILNAS	Luxembourg Institute for standardisation, accreditation, safety, and quality of goods and services (FR: Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services)
CSA	Cybersecurity Act
OLAS	Office Luxembourgeois d'Accréditation et de Surveillance
ENISA	The European Union Agency for Cybersecurity
ICT	Information and communication technologies
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Commission
CAB	Conformity Assessment Body
CB	Certification Body
ECCG	European Cybersecurity Certification Group
NAB	National Accreditation Body
NCCA	National Cybersecurity Certification Authority
EA	European cooperation for Accreditation
IAF	International Accreditation Forum
SANCC	National Cybersecurity Certification Authority Service (FR: Service de l'autorité national de certification de cybersécurité)
NAB	National Accreditation Body
EA	European cooperation for Accreditation
MRA	Mutual Recognition Arrangements
IAF	International Accreditation Forum
ECCG	European Cybersecurity Certification Group

II References

[1] Loi du 4 juillet 2014 portant réorganisation de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services et portant organisation du cadre général pour la surveillance du marché dans le contexte de la commercialisation des produits ;

[2] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013;

[3] ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories

[4] ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services

1 Introduction

1.1 Overview

ILNAS is placed under the administrative supervision of the Ministry of the Economy of the Grand Duchy of Luxembourg. The legal missions of ILNAS are defined in [1]. In this context, ILNAS is in charge of carrying out supervision activities related to the *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013* (hereafter, CSA - “Cybersecurity Act”).

ILNAS, via the national cybersecurity certification authority Service (SANCC), is responsible to supervise activities of certified and self-attested manufacturers and providers of ICT products, ICT services and ICT processes (hereafter, “certificate holders” and “issuers of EU statement of conformity”) and conformity assessment bodies, that are established in the Grand Duchy of Luxembourg.

1.2 Purpose and scope

This document has been drafted with the purpose to describe the procedure of the national supervision scheme that includes certification and self-assessment activities in the context of the CSA. The scope of supervision includes the assurance levels ’basic’, ’substantial’ and ’high’. The supervision scheme is based upon the rules laid down in the CSA, but is regularly updated to meet the requirements of European cybersecurity certification schemes (hereafter, “schemes”), related implementing acts, the national law, other normative documents or when new and pertinent information is available.

This document addresses the staff of the SANCC and all the parties involved in the supervision scheme. This document also targets further actors that may have an interest to understand on how the national supervision scheme works.

Moreover, this procedure will be subject to a peer review, according to article 59 of the CSA.

1.3 Terms and definitions

For the requirements of this document, the terms and definitions provided by the CSA apply.

1.4 Entry into force

This document will enter into force after the start of operational activities related to the CSA.

2 National supervision scheme

The CSA allows the following two types of conformity assessments:

1. Assessments performed by accredited third parties, which might be
   - Conformity Assessment Bodies – CAB, including testing laboratories;
   - National Cybersecurity Certification Authorities – NCCA; and
   - Other public bodies.

   A successful conformity assessment by a third party results in the issuance of a certificate.

2. Self-assessments performed by manufacturers and providers on their own responsibility. At the end of a self-assessment, the manufacturers or providers will issue an EU statement of conformity.

Certificates might be issued by

- Private CABs or public bodies acting as CAB for assurance level ’basic’ and ’substantial’.

- NCCAs for assurance level ‘high’. Private or public CABs may also issue certificates for assurance level ‘high’ in the following cases:
  - Upon prior approval by an NCCA for each certificate (Art. 56-6 (a))
  - On the basis of a general delegation of the task of issuing certificates by the NCCA (Art. 56-6 (b))

- In duly justified cases, by NCCAs for assurance level ‘basic’ and ‘substantial’.

EU statements of conformity are issued by manufacturers or providers on their own responsibility by the means of a self-assessment. A self-assessment is only permitted for assurance level “basic” and if it has been allowed by a particular scheme.

2.1 Supervision scheme - Certificates

This section aims to describe the national supervision scheme. The national supervision scheme on *Figure 1* below covers all the actors involved in accreditation, certification and supervision activities. It must be emphasised that the SANCC only intervenes ex-post the issuance of certificates.

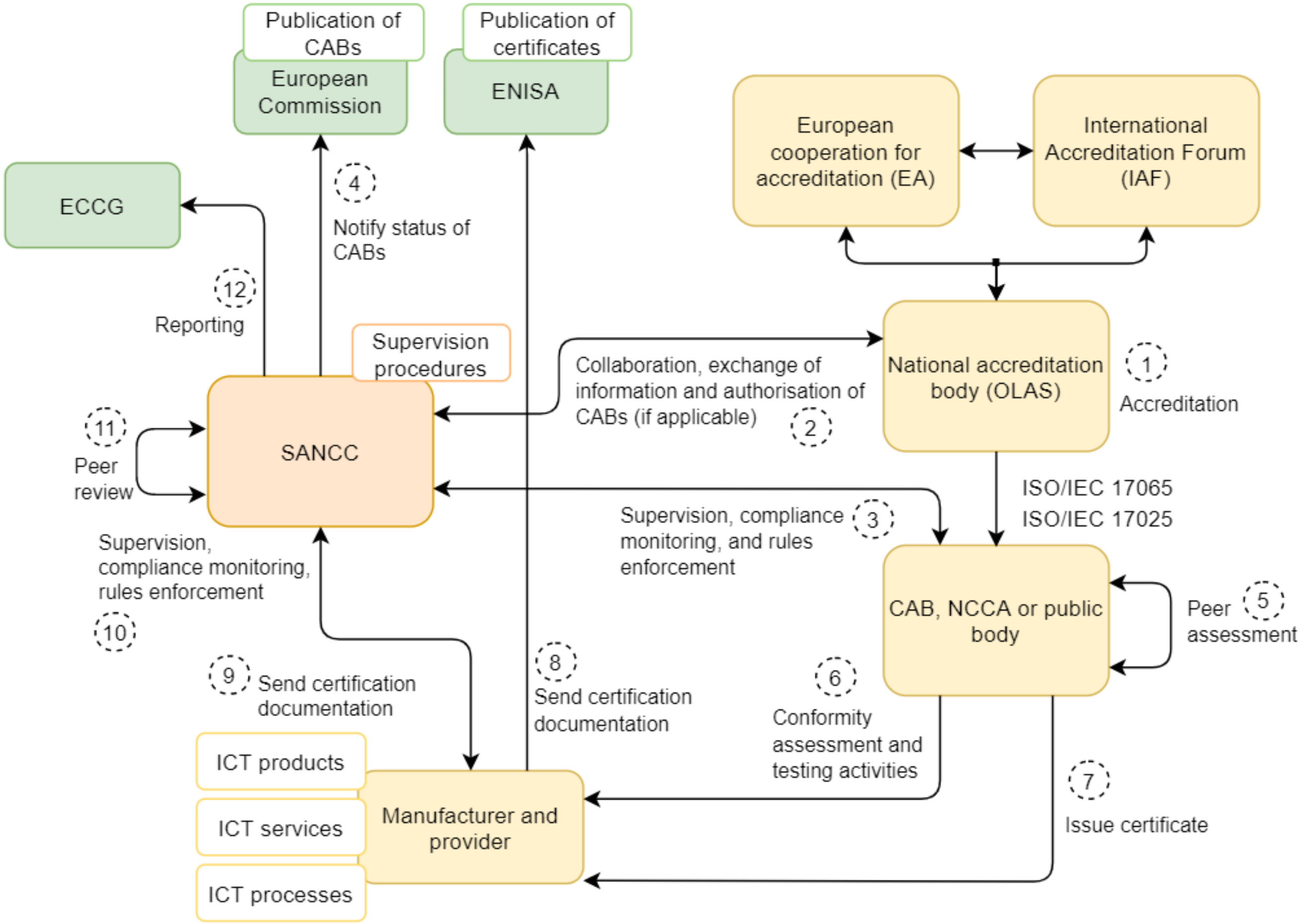
Publication of CABs
European Commission
Publication of certificates
ENISA
European cooperation for accreditation (EA)
International Accreditation Forum (IAF)
ECCG
4
Notify status of CABs
12
Reporting
Supervision procedures
National accreditation body (OLAS)
1
Accreditation
Collaboration, exchange of information and authorisation of CABs (if applicable)
2
11
Peer review
SANCC
ISO/IEC 17065
ISO/IEC 17025
Supervision, compliance monitoring, and rules enforcement
3
Supervision, compliance monitoring, rules enforcement
10
CAB, NCCA or public body
Peer assessment
5
9
Send certification documentation
8
Send certification documentation
6
Conformity assessment and testing activities
7
Issue certificate
ICT products
ICT services
ICT processes
Manufacturer and provider

Figure 1: National supervision scheme - Certifications

2.1.1 Description of the different steps

1. The national accreditation body (NAB) of a Member state (e.g., OLAS in Luxembourg) that has signed the European cooperation for Accreditation (EA) multilateral agreement (EA MLA), accredits the competence of CABs, NCCAs and other public bodies that carry out conformity assessment activities.

   Accreditation of such bodies will be founded on reliable accreditation infrastructure, that includes harmonised accreditation criteria, guidelines, competence and mutual recognition arrangements (MRA) established by EA and the International Accreditation Forum (IAF). In general, such bodies shall be accredited against the requirements of the CSA. More specifically, accreditation against the following standards is required, depending on the conformity assessment activities that the body plans to perform:

   a. *ISO/IEC 17025* [3]
      This relates to testing laboratories that evaluate and assess the security and functionality of ICT products. These testing laboratories shall be accredited against the ISO/IEC 17025 standard [3] (laboratories of informatics);

   b. *ISO/IEC 17065* [4]
      Bodies that issue certificates shall be accredited against the ISO/IEC 17065 standard. The ISO 17065 standard lays down conformity assessment requirements for bodies that issue certificates for ICT products, ICT services and ICT processes.

   c. *Additional requirements laid down in specific schemes*
      When accrediting bodies, the NAB shall consider additional requirements laid down in in the schemes. Those schemes will enter into force by the means of implementing acts.

   In addition to the accreditation aspects, the schemes might define further authorisation rules for the CABs, in particular regarding assurance level “high”. This authorisation aims to complement the accreditation by assessing the technical competence of the personnel of CABs that aim to perform, for instance, evaluation activities in penetration testing.

2. The SANCC collaborates and exchanges information with the NABs in order to supervise the activities of accredited CABs more efficiently.

3. The SANCC ensures the supervision, compliance monitoring and rules enforcement of accredited bodies. These activities are, among others, achieved based on the information and documents exchanged between the accredited body and the SANCC. Supervision of accredited bodies also takes place by assisting, supporting and collaborating with the NABs.

4. The SANCC notifies to the European Commission on the status of bodies that have been accredited and, where applicable, authorised by the SANCC (cf. article 61). The SANCC also notifies restrictions, suspension, and withdraws of such authorisations.

The European Commission will consequently update the Official Journal of the European Union.

5. Peer assessment has the objective to evaluate the quality, efficiency and effectiveness of accredited bodies, that are involved in evaluation and certification activities that relate to assurance level “high”. The requirements and mechanisms of peer assessment, if any, will be specified in the schemes.

6. Conformity assessment and testing activities verify the conformance of ICT products, ICT services or ICT processes of manufacturers or providers against the applicable requirements. A report is drafted at the end of these activities.

7. Based on the conformity assessment report, the certification body (CB) of the CAB, the NCCA or the public body acting as CAB takes the decision to issue a certificate.

8. The manufacturer or provider makes his certificate and related documentation available to ENISA. ENISA will publish the certificate on a dedicated website.

9. In parallel to point 8, the manufacturer or provider sends a copy of his certificate, associated information and supporting documents to the SANCC. At this step, the supervision process will start.

10. The SANCC will apply its supervision procedures to supervise, monitor compliance and enforce the obligations with regards to the CSA, the schemes and other applicable requirements.

11. Peer review (cf. article 59 of the CSA) is the process of evaluating the procedures, practices and competencies of NCCAs. As for the peer assessment, the main objective of peer review is to make sure the NCCAs apply equivalent standards in their activities and practices in terms of certification and supervision.

12. The SANCC reports its activities to the ECCG. In addition, the SANCC cooperates with other NCCAs or other public bodies by sharing information on possible non-compliances.

2.2 Supervision scheme - EU statement of conformity

This chapter aims to describe the national supervision scheme that relate to the EU statement of conformity. An EU statement of conformity is issued by manufacturers or providers on their own responsibility after performing a self-assessment of a specific ICT product, ICT service or ICT process (cf. article 53). The objective of an EU statement of conformity is to demonstrate that the requirements of a scheme have been fulfilled (if self-assessment is permitted). According to recital 79 of the CSA, self-assessment “should be considered to be appropriate for low complexity ICT products, ICT services or ICT processes that present a low risk to the public, such as simple design and production mechanisms”.

Figure 2 hereunder illustrates the applicable supervision scheme.

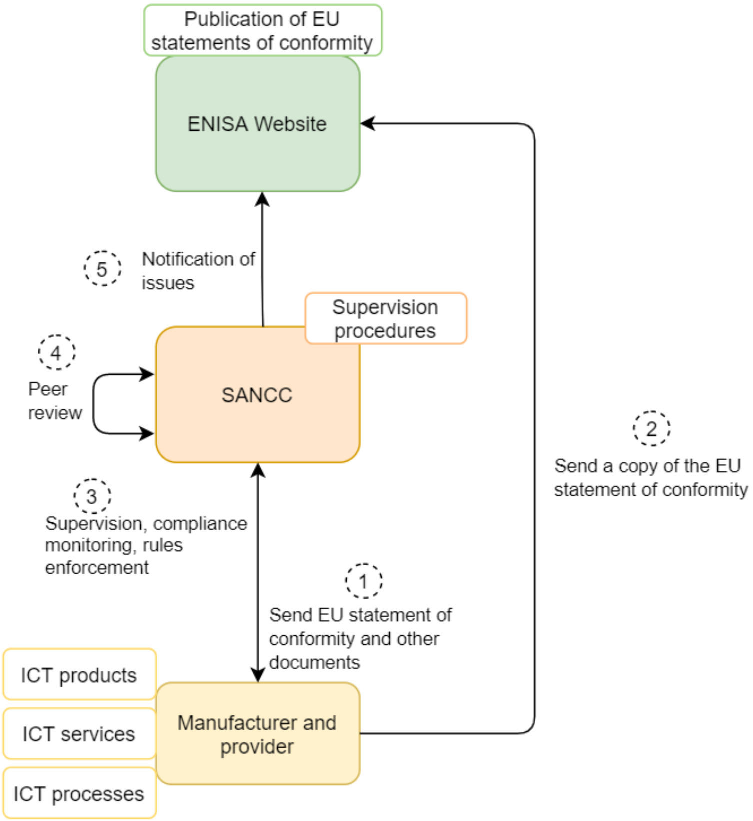
Publication of EU statements of conformity
ENISA Website
5
Notification of issues
Supervision procedures
4
Peer review
SANCC
2
Send a copy of the EU statement of conformity
3
Supervision, compliance monitoring, rules enforcement
1
Send EU statement of conformity and other documents
ICT products
ICT services
ICT processes
Manufacturer and provider

Figure 2: National supervision scheme - EU statement of conformity

2.2.1 Description of different steps

After performing a self-assessment, the manufacturer or provider will issue an EU statement of conformity.

1. At first, the manufacturer or provider will send a copy of the EU statement of conformity to the SANCC, including supporting documents.

2. The manufacturers or providers send a copy of the EU statement of conformity to ENISA. This activity might be taken over by the SANCC in accordance with the requirements of the schemes. ENISA will publish the EU statement of conformity on their web site.

3. The SANCC verifies the compliance of the EU statement of conformity and the relevant documentation against the applicable requirements by using its supervision procedures.

4. The peer review system has been briefly explained in *chapter 2.1*.

5. The SANCC notifies any issues that are present in EU statements of conformity to ENISA.

3 Supervision activities

3.1 Introduction

This chapter aims to describe the supervision activities with regards to the issuance of certificates and EU statements of conformity. The supervision shall ensure that the certificate holders, issuers of EU statement of conformity and accredited bodies meet the applicable requirements laid down in the following documents:

- The CSA;
- The requirements defined in schemes;
- The national law (when published in the "Journal officiel du Grand-Duché du Luxembourg"); and
- Other relevant documents.

The role of accredited bodies is to assess the conformity of manufacturers and providers against all the requirements defined in these documents.

Regarding the supervision activities, we differentiate between the following two aspects of supervision:

- The registration process for supervision
- Continuous supervision activities

The registration **process for supervision** is the process used to register manufacturers or providers, that have been certified by an accredited body or that have issued an EU statement of conformity. This registration process also relates to notification of changes in the scope of certification or EU statement of conformity.

On the other hand, **continuous supervision activities** relate to ex post supervision activities that are carried out after the registration process. The supervision activities are executed through the life cycle of the supervision and as long as a manufacturer or provider is registered by the SANCC as certificate holders or issuers of EU statement of conformity.

3.2 Registration process for supervision

The registration process for supervision is achieved through the following steps:

1) Notification for supervision
2) Validation and registration
3) Review of documentation
4) Registration conclusions

3.2.1 Notification for supervision

Certificate holders or issuers of EU statement of conformity fills the form ILNAS/SANCC/F001 to notify their certification or self-assessment conclusions. This form shall be sent to the SANCC jointly with the following supporting documents:

- A copy of the certificate or the EU statement of conformity;
- The technical documentation that covers the design, manufacture and operation of the ICT product, ICT service or ICT process;
- Audit reports from accredited bodies (only for certification purposes); and
- All other information that are relevant to demonstrate conformity of ICT products, ICT services and ICT processes against the applicable requirements.

The notification form has to be dated and signed by a representative authorised to commit the manufacturer or provider.

3.2.2 Validation and registration

The SANCC validates the completeness of the information and documentation by the means of an internal validation check-list F004 (“ILNAS/SANCC/F004 – Checklist pour la revue de la notification F001”). The SANCC allocates an identification number to each notification for supervision. This number is valid for the whole supervision period and can be used in all correspondence. The SANCC transmits the identification number to the certificate holders and issuers of EU statement of conformity, which have proceeded to the notification for supervision. The notification for supervision is validated by the SANCC.

The SANCC may request further information, in case the required documentation or information are incomplete.

The SANCC opens a form F020 (“ILNAS/SANCC/F020 – History of manufacturers and providers”) internally, which enables traceability of key events during supervision (e.g., audits, supervision meetings, etc.).

3.2.3 Review of documentation

The SANCC will review all the documents and information required and received. Those documents are referred in the form ILNAS/SANCC/F001.

The SANCC may request a detailed CV of the auditors who performed the conformity assessment, if deemed necessary. The SANCC may ask questions to certificate holders and issuers of EU statement of conformity to verify the accuracy and to get more details of the information provided.

3.2.4 Confirmation of registration

The registration process is concluded and confirmed if step 3 “Review of documentation” is considered as satisfactory by the SANCC.

Here, the SANCC sends a formal, written confirmation letter to inform the certificate holders and issuers of EU statement of conformity that the registration process has been successful completed. From this moment, the continuous operational supervision activities will take place.

Practical information

The notification form ILNAS/SANCC/F001 and documentation enable manufacturers and providers to officially notify their intent to provide certified ICT products, ICT services or ICT processes and constitutes "the triggering factor" for the registration process for supervision. The form is also used in order to provide the SANCC with any updated information about supervised manufacturers and providers, which have undergone major changes to their structure, their organisation or in their resources required to carry out the activities covered by the notification.

The duly completed, dated and signed notification form, together with the requested supporting documents, must be mailed or brought in an envelope marked "confidential" to:

ILNAS
SANCC
1, avenue du Swing
L-4367 Belvaux

Alternatively, the notification can be sent electronically, in a secure way, to the SANCC. The SANCC (*supervision-cybersecurite@ilnas.etat.lu*) has to be contacted prior to sending the form and related supporting documents to discuss the transmission modalities.

3.3 Continuous supervision activities

The objective of continuous supervision activities is to ensure that certificate holders, issuers of EU statement of conformity and accredited bodies continuously demonstrate compliance against applicable requirements. Continuous supervision also intends to analyse, evaluate and assess occurred events and their impact on certified or self-assessed ICT product, ICT service or ICT process.

For this purpose, the following activities with respect to the requirements of certification schemes shall take place:

- Supervision meetings together with the certificate holders, issuers of EU statement of conformity and CABs at planned intervals or if needed;

- The SANCC proceeds to additional assessments in order to verify potential non-compliance aspects of ICT products, ICT services and ICT products. In that case, the certificate holders and issuers of EU statement of conformity shall make available all needed resources (human, technology, etc.) to the SANCC. If needed, the SANCC might subcontract external experts for those kinds of verifications.

- In case of non-compliance, the sanctions of the national law apply (when published in the “Journal officiel du Grand-Duché du Luxembourg”).

- The SANCC and the other actors in the national supervision scheme should communicate regularly to proactively address issues or to discuss on elements that are not clear or ambiguous.

4 Collaboration and cooperation

The SANCC is responsible to supervise compliance and enforce the obligations with regards to the implementation of the applicable requirements of Certificate holders and issuers of EU statement of conformity and accredited bodies established in the Grand-Duchy of Luxembourg.

The SANCC also supports and assists other Member states in their supervision and certification activities. For this purpose, the SANCC closely cooperates with the NABs, other NCCAs, market surveillance authorities (e.g. the “Département de la surveillance du marché” from ILNAS), other public bodies, ENISA and the European Commission, including sharing of information on potential non-compliance of ICT products, ICT services and ICT processes with the requirements of the CSA and the related schemes. The SANCC also shares expertise and good practices with other NCCAs.

The SANCC supports and assists all actors within the supervision scheme, notably by providing them with expertise and relevant information.

The SANCC handles complaints lodged by natural and legal persons. The SANCC should proceed to investigations and should inform the complainants on the progress and the outcome of the complaints.

The supervision procedures applied by the SANCC will be assessed by other NCCAs, the European Commission, the European Cybersecurity Certification Group (ECCG) and ENISA through a peer review system.