ILNAS/ANCC/Pr001
National Supervision Scheme

Modifications: periodic review

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

confiance-numerique@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
NCCA	National Cybersecurity Certification Authority
EA	European cooperation for Accreditation
ANCC	National Cybersecurity Certification Authority (French: Autorité nationale de certification de cybersécurité)
NAB	National Accreditation Body
EA	European cooperation for Accreditation
MRA	Mutual Recognition Arrangements
IAF	International Accreditation Forum
ILAC	International Laboratory Accreditation Cooperation
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 General requirements for the competence of testing and calibration laboratories

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

[5] Avant-projet de loi du XX portant sur certaines modalités d'application et les sanctions du règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité))

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* (hereinafter, CSA - "Cybersecurity Act").

ILNAS has been designated as the NCCA for the Grand Duchy of Luxembourg according to Article 58 of the Cybersecurity Act that is responsible for supervision tasks. The unit *Service de supervision de cybersécurité* of the Digital Trust Department of ILNAS has been created for carrying out these supervision tasks. The unit supervises the activities of certified and self-assessed manufacturers and providers of ICT products, ICT services and ICT processes (hereinafter, "certificate holders" and "issuers of EU statements of conformity"), and of conformity assessment bodies that are established in the Grand Duchy of Luxembourg.

1.2 Purpose and scope

The purpose of this document is to describe the national supervision scheme of certificate holders, issuers of EU statements of conformity and CABs that are involved in certification activities in the context of the CSA. The scope of the supervision includes conformity assessment activities at the assurance levels "basic", "substantial" and "high". The supervision scheme is based upon the rules laid down in the CSA, and it is updated to meet the requirements of European cybersecurity certification schemes (hereinafter, "certification schemes"), associated implementing acts, and the national law, at planned intervals or whenever changes impacting the legal framework require the supervision scheme to be updated.

This document primarily addresses the staff of the NCCA and all the parties involved in the supervision scheme. This document is also intended for anyone that wants to understand the national supervision scheme relating to the CSA.

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 in the CSA apply.

1.4 Entry into force of this document

This document will enter into force after its publication on the website of ILNAS.

2 National supervision scheme

The CSA distinguishes between two following two types of conformity assessments:

1. Assessments performed by an accredited conformity assessment body (CAB) (issuance of certificates)

2. Self-assessments performed by manufacturers and providers themselves (issuance of EU statements of conformity)

Certificates are issued by

- CABs, for the assurance levels “basic”, “substantial” and “high”. At the assurance level “high”, the CABs may issue certificates in case where this task has been delegated to them or upon a prior approval by a national cybersecurity certification authority (NCCA).

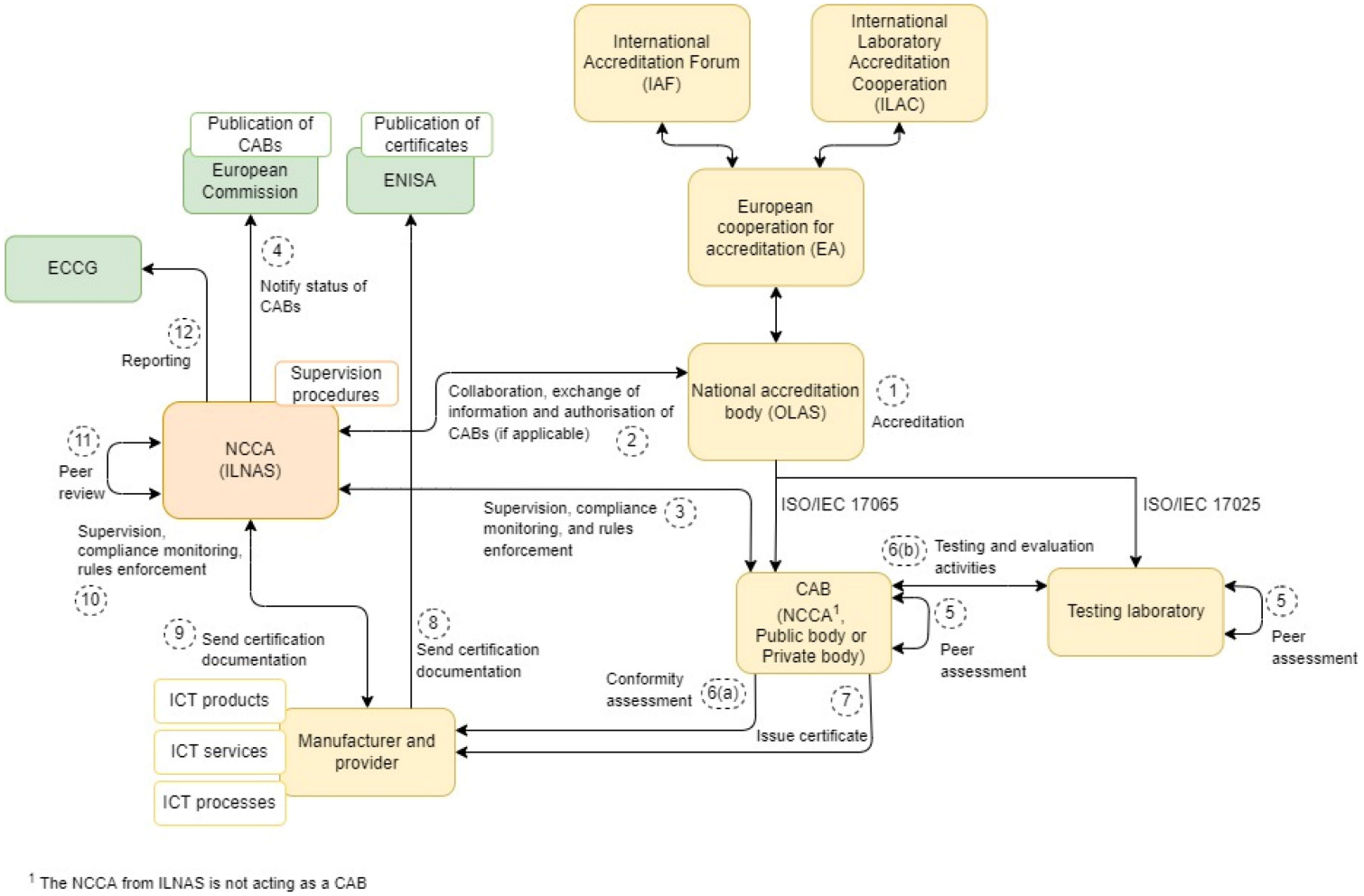
- NCCAs, for the assurance level “high” or, in special cases, for the assurance levels “basic” and “substantial” as well.

To simplify the description of the supervision scheme, we will use the term CAB to refer to the certification activities of the NCCA in the following sections.

EU statements of conformity are issued by the manufacturers or providers themselves (issuers of EU statement of conformity) by means of a self-assessment. Here, the issuers of EU statements of conformity perform their own assessments against the requirements of the CSA and the targeted certification schemes. A self-assessment is only permitted for the assurance level “basic” for certification schemes that explicitly allow self-assessments. In this scenario, the issuers of EU statements of conformity are solely responsible for the conformity assessments.

2.1 Supervision scheme - Certificates

This section aims to describe the national supervision scheme in relation to certification activities in the context of the CSA. The national supervision scheme shown in *Figure* 1 below covers all the parties involved in accreditation, certification and supervision activities.



[1] The NCCA from ILNAS is not acting as a CAB

Figure 1: National supervision scheme - Certifications

2.1.1 Description of the different steps

1. CABs shall be accredited by the "Office Luxembourgeois de l'Accréditation et da la Surveillance (OLAS)" or any national accreditation body recognized by OLAS as equivalent, pursuant to points 1 and 2 of paragraph 1 of article 5 of the ILNAS law. The accreditation shall cover the respective conformity assessment activities of the CABs. The CABs shall be accredited against the requirements of the CSA, in particular the requirements stated in its annex and article 54 (1) f).
   The relevant standard for certification of products, services and processes for CABs, mentioned in paragraph 19 of the annex, is ISO/IEC 17065. Testing laboratories, mentioned in paragraph 20 of the annex, used by CABs shall be accredited according to ISO/IEC 17025.

   Note:
   A CAB can have the role as a certificate issuer and also perform testing activities as a testing laboratory, in which case both activities shall be appropriately separated. An accreditation against ISO/IEC 17025 [3] for the laboratory and against ISO/IEC 17065 [4] for the issuance of certificates is required.

2. The NCCA collaborates and exchanges information with the NABs in order to supervise the activities of the CABs. An additional task of the NCCA is to authorise CABs, notably in terms of competencies. According to Article 58 (7) e), the NCCA shall, where applicable, authorise CABs and restrict, suspend or withdraw existing authorisations where CABs infringe the requirements of the CSA. The task of authorising CABs will depend on the requirements of the specific certification schemes.

3. The NCCA ensures the direct supervision, monitoring of compliance and the enforcement of rules in relation to accredited CABs based on the information and documents exchanged between the CAB and the NCCA. Further details on the supervision activities will be specified in the certification schemes.

4. The NCCA notifies the status of CABs that have been accredited and, where applicable, authorised by the NCCA (cf. Article 61) to the European Commission. The NCCA also notifies restrictions, suspensions, and withdrawals of such authorisations. The European Commission will subsequently update the Official Journal of the European Union.

5. Peer assessment has the aim of evaluating the quality, efficiency and effectiveness of testing laboratories associated to CABs and CABs that issue certificates for the assurance level "high" in order to assess whether these bodies carry out their activities in a harmonised way. The requirements and mechanisms of peer assessment, if any, will be determined in the certification schemes.

6. CABs and testing laboratories' activity:

   a. An accredited CAB will perform a conformity assessment
   b. The testing laboratories perform the functionality testing and evaluation of ICT products of manufacturers. After finalising the evaluation and assessment activities, the testing laboratories transmit reports to the CAB. The CAB reviews

these reports in order to decide whether a certificate can be issued to the manufacturer.

7. The CAB issues the certificate after reviewing the report prepared either by the testing laboratories or by their own auditors.

   The manufacturer or provider that is being evaluated, audited and assessed has to provide all the necessary information so that the aforementioned assessment activities can be performed as accurately as possible.

8. After the manufacturer or provider becomes certified, a copy of the certificate and any associated information must be made available to ENISA, who will publish the certificate and the associated information on a dedicated website. The certificate may also be published by the NCCA in accordance with the requirements of the certification schemes.

9. At the same time, the manufacturer or provider sends a copy of his certificate, associated information and supporting documents to the NCCA. In this step, the supervision process of the manufacturer or provider by the NCCA will start.

10. The NCCA will apply its supervision procedures to certificate holders and issuers of EU statements of conformity in order to supervise, monitor the compliance and enforce the obligations regarding the CSA, the certification schemes and other applicable requirements. These supervision activities start from the registration process and continue through the whole certificate life cycle, until the end of the validity of the certificate or the EU statement of conformity.

11. A peer review (cf. Article 59 of the CSA) is the process of evaluating the procedures, practices and competencies of NCCAs among themselves. Similarly to peer assessment, the main objective of a peer review is to ensure that the NCCAs apply equivalent practices in terms of certification and supervision.

12. The NCCA reports to and collaborates with the European Cybersecurity Certification Group (ECCG), whose tasks are, among others (cf. Article 62 of the CSA), to

    - advise and assist the European Commission in its work to ensure the consistent implementation and application of the CSA;
    - to assist, advise and cooperate with ENISA; and
    - support the implementation of peer assessment mechanisms.

2.2 Supervision scheme - EU statement of conformity

The aim of this section is to describe the national supervision scheme relating to EU statements of conformity. An EU statement of conformity is issued by manufacturers or providers themselves after performing a self-assessment of a specific ICT product, ICT service or ICT process (cf. Article 53 of the CSA). The objective of an EU statement of conformity is to demonstrate that the requirements of a certification 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 below illustrates the applicable supervision scheme.

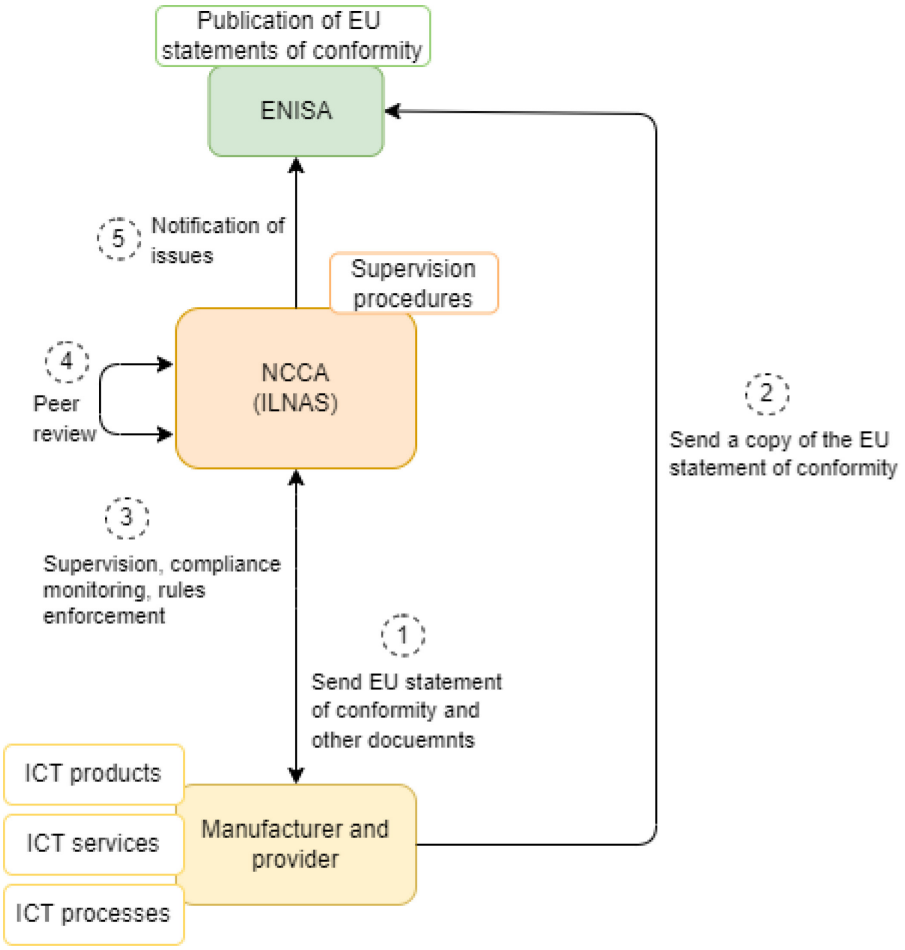


Figure 2: National supervision scheme - EU statement of conformity

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 NCCA, including supporting documents.

2. The manufacturers or providers must also send a copy of the EU statement of conformity to ENISA. The copy of the EU statement of conformity may also be sent to ENISA by the NCCA in accordance with the requirements of the certification schemes. ENISA will publish the EU statement of conformity on their web site.

3. The NCCA verifies the compliance of the EU statement of conformity and the relevant documentation against the applicable requirements. In addition, the NCCA applies its

supervision procedures in order to supervise the manufacturers and providers, monitor their compliance and enforce the obligations of the CSA.

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

5. If necessary, the NCCA notifies any issues concerning the EU statements of conformity to ENISA.

3 Supervision activities

3.1 Introduction

The aim of this section is to describe the supervision activities related to the activities of issuance of certificates and EU statements of conformity. The supervision shall ensure that the certificate holders, issuers of EU statements of conformity and CABs meet the applicable requirements laid down in the following documents:

- the CSA,
- the requirements defined in related certification schemes,
- the national law [5], and
- other relevant documents.

CABs have the obligation to assess the conformity of manufacturers and providers against all the requirements defined in the documents above.

The evaluation methodologies, competencies and procedures of CABs shall meet the requirements defined in the documents above.

All of these aspects are supervised and monitored by the NCCA.

Regarding the supervision activities, we differentiate between the following two phases:

- the registration process for the supervision, and
- continuous supervision activities.

The **registration process for the supervision** is the process used to register manufacturers or providers that have been certified by a CAB or that have issued an EU statement of conformity with the NCCA. The registration process also includes the notification of changes regarding the scope of the certification or the EU statement of conformity.

Continuous supervision activities relate to supervision activities carried out after manufacturers and providers have already been registered with the NCCA. The supervision activities are executed through the life cycle of the supervision and as long as a manufacturer or provider is registered with the NCCA as a certificate holder or an issuer of an EU statement of conformity.

3.2 Registration process for supervision

The registration process for supervision contains the following steps:

1) notification for supervision
2) validation of notified information and registration
3) review of the documentation
4) confirmation of the registration

3.2.1 Notification for supervision

Certificate holders or issuers of EU statements of conformity fill in the form ILNAS/ANCC/F001 to notify their successful certification or self-assessment to the NCCA. The form ILNAS/ANCC/F001 shall be sent to the NCCA accompanied by the following supporting documents:

- a copy of the certificate or the EU statement of conformity
- the technical documentation that covers the design, manufacturing and operation of the ICT product, ICT service or ICT process;
- audit reports from the CABs (only for certificate holders); and
- all other information that is relevant for demonstrating the 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 of notified information and registration

The NCCA validates the completeness of the information and documentation that has been provided through the check-list F004 (“ILNAS/ANCC/F004 – Checklist pour la revue de la notification F001”). The NCCA allocates an identification number to each notification for supervision. The identification number is valid for the whole supervision period and can be used in all correspondence. The NCCA transmits the identification number to the certificate holders and issuers of EU statements of conformity that submitted a notification for supervision. The notification for supervision is validated by the head of the Digital Trust Department of ILNAS.

The NCCA may request further information if necessary.

The NCCA fills in the internal form F018 (“ILNAS/ANCC/F018 – History of manufacturers and providers”) to record key events that have occurred during the supervision (e.g., audits, supervision meetings, etc.). The form is updated at planned intervals or whenever an update is needed.

3.2.3 Review of documentation

The NCCA will review the received documents. In addition to the notification form and the supporting documents mentioned in step 1 (notification for supervision), the NCCA will review the following elements in case of a certification by a CAB:

- accreditation and scope of the CAB;

- authorisation of the CAB (if applicable);
- the certification of the manufacturer or provider and its scope;
- coverage of the applicable requirements in the conformity assessment report;
- if applicable, the resolution of the nonconformities (including corrective actions) detected during the conformity assessment.

The NCCA may request detailed CVs of the auditors who performed the conformity assessment, if deemed necessary. The NCCA may pose additional questions to certificate holders and issuers of EU statements of conformity, e.g., to verify the accuracy of the provided information or to obtain more details.

3.2.4 Confirmation of registration

The registration process is concluded and confirmed if step 3 “Review of documentation” has been completed by the NCCA.

The NCCA will send a formal confirmation letter to inform the certificate holder or the issuer of an EU statement of conformity that the registration process has been completed successfully. From this moment on, the continuous operational supervision activities will take place.

Practical information

The notification form ILNAS/ANCC/F001 enables manufacturers and providers to officially notify their intent of providing certified ICT products, ICT services or ICT processes and it constitutes the trigger of the registration process for the supervision. The form is also used to inform the NCCA of updates concerning the supervised manufacturers and providers, such as, e.g., major changes relating to their structure, their organisation or their resources used to carry out the activities covered by the notification.

The duly completed, dated and signed notification form ILNAS/ANCC/F001, together with the requested supporting documents, must be mailed or brought in an envelope marked "confidential" to:

ILNAS
Digital Trust Department / NCCA
1, avenue du Swing
L-4367 Belvaux

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

3.3 Continuous supervision

The objective of the continuous supervision is to ensure that certificate holders and issuers of EU statements of conformity are continuously meeting the applicable requirements.

Continuous supervision also intends to evaluate and assess events that have occurred relating to ICT products, ICT services or ICT processes and their impact.

The continuous supervision is based on the following aspects:

- Supervision meetings together with the certificate holders or issuers of EU statements of conformity and CABs take place at planned intervals or whenever they are needed.

- The NCCA may conduct additional conformity assessments in order to assess potential non-compliance aspects of ICT products, ICT services and ICT products. Certificate holders and issuers of EU statements of conformity shall make available the needed resources (access to employees, documentation, etc.) to allow the NCCA to conduct its investigations. The NCCA might subcontract external experts for those kinds of verifications.

- In case of non-compliance, the sanctions laid down in the national law [5] apply.

- The NCCA and the other actors involved in the national supervision scheme communicate regularly to proactively address issues and to exchange information.

4 Collaboration and cooperation

The NCCA is responsible for ensuring the compliance of certificate holders and issuers of EU statements of conformity and CABs established in the Grand Duchy of Luxembourg with the applicable requirements from certification schemes and the CSA.

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

The NCCA supports and assists all actors involved in the supervision scheme, notably by providing them with expertise and relevant information.

The NCCA handles complaints lodged by natural and legal persons. In response to a complaint, the NCCA will carry out investigations and inform the complainants about the progress of its investigations and their outcome.

If necessary, the NCCA will submit formal requests to the European Commission to withdraw the authorization of a CAB to perform certifications with respect to a certification scheme.

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

The activities of the NCCA are supervised by the head of the Digital Trust Department of ILNAS.