ILNAS/ANCC/Pr004
Management of CAB authorisation

Modifications: initial version

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

ANCC	National Cybersecurity Certification Authority (French: Autorité nationale de certification de cybersécurité)
CAB	Conformity Assessment Body
CB	Certification Body
Commission	European Commission
CSA	CyberSecurity Act
ENISA	The European Union Agency for Cybersecurity
ICT	Information and communication technologies
ILNAS	Luxembourg Institute for standardisation, accreditation, safety, and quality of goods and services (French: Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services)
ITSEF	IT Security Evaluation Facility
NCCA	National Cybersecurity Certification Authority
OLCN	Luxembourg Digital Trust Body (French : Organisme Luxembourgeois de la Confiance Numérique)

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 (hereinafter 'ILNAS law')

[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 (hereinafter 'Cybersecurity act')

[3] Loi du 20 décembre 2024 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) et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS (hereinafter 'National CyberSecurity law')

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 the ILNAS law [1]. In this context, ILNAS is in charge of carrying out supervision tasks within the meaning of Article 58 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on cybersecurity certification of information and communications technologies, and repealing Regulation (EU) No 526/2013 (Cybersecurity Regulation) and responsible for certification tasks within the meaning of Article 56(6) of the aforementioned Regulation (EU) No 2019/881.

ILNAS has been designated as the NCCA for the Grand Duchy of Luxembourg according to Article 58 of the Cybersecurity Act **Error! Reference source not found.** that is responsible for supervision tasks and certification tasks as defined in the National Cybersecurity law [3][3]. The OLCN has been created for carrying out these supervision and certification tasks. The unit supervises the compliance of manufacturers and providers of ICT products, ICT services, ICT processes, and managed security services and of conformity assessment bodies that are established in the Grand Duchy of Luxembourg.

In the following, we use the acronym NCCA to refer to the OLCN.

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.

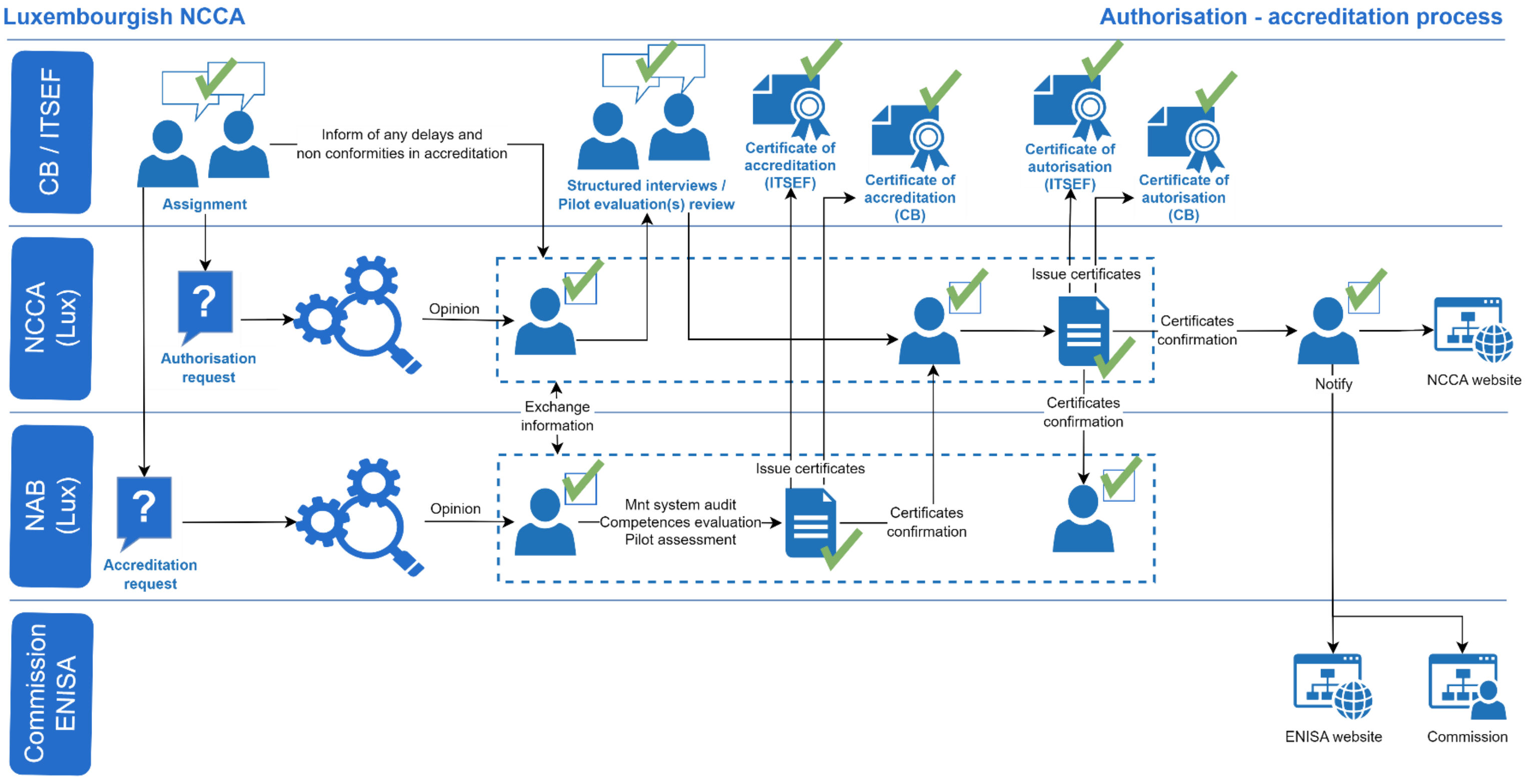
This procedure will be subject to a peer review, according to Article 59 of the CSA.

1.3 Terms and definitions

In this document, the terms and definitions provided in the Cybersecurity Act, its implementing regulations (in particular European cybersecurity certification schemes) and other documentation publicly available on the website of ILNAS apply.

2 Management of CAB authorisation

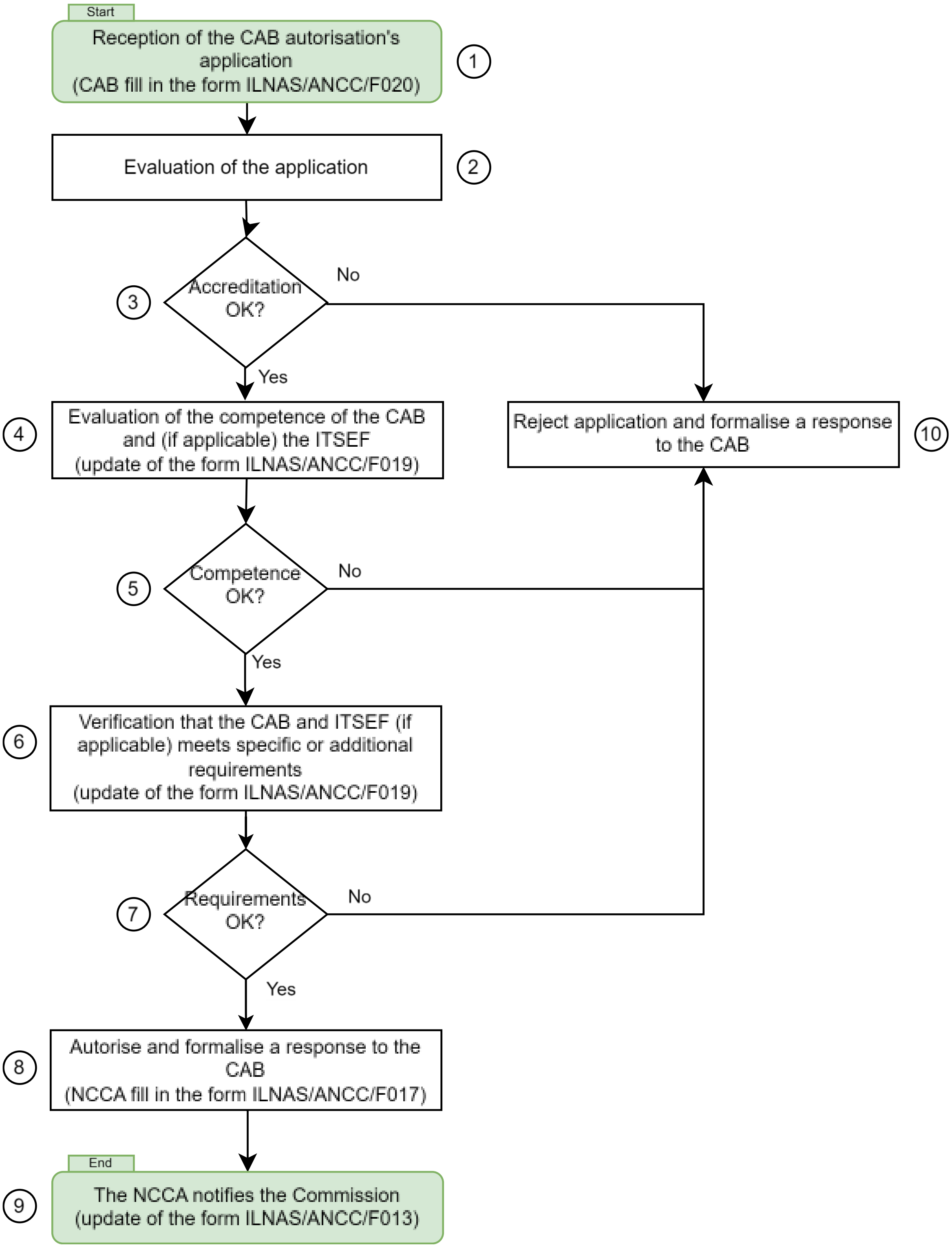
The CAB authorisation procedure can be started in parallel with CB / ITSEF accreditation. It may concern an initial CAB authorisation or a renewal request. The Figure 1 below shows the close relationship between authorisation and accreditation:



Luxembourgish NCCA
Authorisation - accreditation process
CB / ITSEF
NCCA (Lux)
NAB (Lux)
Commission ENISA
Assignment
Inform of any delays and non conformities in accreditation
Structured interviews / Pilot evaluation(s) review
Certificate of accreditation (ITSEF)
Certificate of accreditation (CB)
Certificate of autorisation (ITSEF)
Certificate of autorisation (CB)
Authorisation request
Opinion
Issue certificates
Certificates confirmation
Notify
NCCA website
Exchange information
Certificates confirmation
Accreditation request
Opinion
Issue certificates
Mnt system audit
Competences evaluation
Pilot assessment
Certificates confirmation
ENISA website
Commission

Figure 1: Management of CAB authorisation / accreditation

The procedure in Figure 2 focuses on the management of CAB authorisation.



Start
Reception of the CAB autorisation's application (CAB fill in the form ILNAS/ANCC/F020)
1
Evaluation of the application
2
3
Accreditation OK?
No
Yes
4
Evaluation of the competence of the CAB and (if applicable) the ITSEF (update of the form ILNAS/ANCC/F019)
Reject application and formalise a response to the CAB
10
5
Competence OK?
No
Yes
6
Verification that the CAB and ITSEF (if applicable) meets specific or additional requirements (update of the form ILNAS/ANCC/F019)
7
Requirements OK?
No
Yes
8
Autorise and formalise a response to the CAB (NCCA fill in the form ILNAS/ANCC/F017)
End
9
The NCCA notifies the Commission (update of the form ILNAS/ANCC/F013)

Figure 2: Management of CAB authorisation

1) **Receipt of the CAB's authorisation's application**
The CAB applies for a CAB authorisation by filling in the ILNAS/ANCC/F020 form and sending it, along with all applicable evidence to the NCCA (ILNAS).

2) **Evaluation of the application**
The NCCA (ILNAS) reviews, verifies and analyses the received information. The NCCA (ILNAS) shall enforce the applicable requirements.

3) **Accredited or not yet accredited?**
The NCCA (ILNAS) verifies if the CB and its associated ITSEF are accredited, or are in the process of being accredited by a National Accreditation Body. The NCCA (ILNAS) rejects the application if it is not the case.

4) **Specific or additional requirements**
The NCCA (ILNAS) verifies if the CB and its associated ITSEF meet the specific or additional requirements as referenced in the Cybersecurity Act and the applicable European Cybersecurity schemes by using the internal ILNAS/ANCC/F019 form.
The NCCA (ILNAS) may request additional evidence if required. At minimum, one on-site visit shall be organised for the CB itself and each of its ITSEFs.

5) **Does CAB meet specific or additional requirements?**
The NCCA (ILNAS) rejects the application if the CB or its associated ITSEF do not meet those specific or additional requirements.

6) **Accredited or not accredited?**
The NCCA (ILNAS) verifies if the CB and its associated ITSEF are accredited by a National Accreditation Body. The NCCA (ILNAS) rejects the application if it is not the case.

7) **Deliver authorisation**
The NCCA (ILNAS) delivers an authorisation report (ILNAS/ANCC/A002) to the CB and its associated ITSEF. The CB and its associated ITSEF authorisations are formalised by using the internal ILNAS/ANCC/F017 form.

8) **Inform the Commission and update annual summary report**
The NCCA updates its annual summary report (internal ILNAS/ANCC/F013 form) with a summary of the CB and its associated ITSEF authorisation. The annual summary report is submitted once a year to the European Commission.

Application rejection

9) **Reject application and formalisation**
When the NCCA (ILNAS) rejects the application of the CB or its associated ITSEF, a formalised response is provided to the applicant.

3 Complaint handling

Electronic communication with the NCCA regarding complaints should always take place via the email inbox supervision-cybersecurite@ilnas.etat.lu and can be carried out encrypted. The corresponding key can be found on the contact page of the NCCA website[1].
Confirmation of receipt of a complaint will be issued. The complainants will be kept informed of the progress and results of the assessment of the complaint, as far as possible, within an appropriate deadline.

4 Subcontracting

Both the CB and the ITSEF may decide to subcontract a third party to perform some of its conformity assessment activities. In that case, it has to be performed according to points 34 to point 38 of the ENISA authorisation of CBs and ITSEFs guidelines version 0.7.

5 Pilot evaluation

The pilot evaluation shall be performed according to points 55 to 58 of the ENISA authorisation of CBs and ITSEFs guidelines version 0.7.

6 Compliance audit

The NCCA performs at least 2 compliance audits during the duration of the authorisation to monitor the CABs in their compliance. The first compliance audit occurs not later than 1,5 years after the start of the authorisation.
The compliance audits are performed by the NCCA according to point 72 of the ENISA authorisation of CBs and ITSEFs guidelines version 0.7.

7 Re-authorisation audit

To uphold the authorisation once issued, the CAB must comply with the specifications of this document, the scheme in question and any ancillary provisions potentially contained in the notice of authorisation. Any changes involving a modification of the information provided in ILNAS/ANCC/F020 form during the initial CAB authorisation request or an authorisation renewal request shall be notified to the NCCA to avoid any restriction or temporary suspension of the authorisation. A re-authorisation report will be provided to the CAB if the compliance with the specifications mentioned above is maintained.
The changes mentioned in points 64 a) to 64 g) of the ENISA authorisation of CBs and ITSEFs guidelines version 0.7 shall be notified by the authorised CAB to the NCCA.
The re-authorisation procedure is described in points 65 to 68 of the ENISA authorisation of CBs and ITSEFs guidelines version 0.7

[1] https://portail-qualite.public.lu/fr/cybersecurity-act/ncca/contact-ncca.html

8 Renewal audit

For the renewal of an authorisation, it is recommended to fill the ILNAS/ANCC/F020 form and submit it not later than 6 months before the expiration of the current authorisation. The procedure is the same as for an initial authorisation request, excepted that no pilot certification is required. The Articles 21(2) - authorisation for CBs, and 22 (3) - authorisation for ITSEFs, of Commission Implementing Regulation (EU) 2024/482 provide the sources of re-use of documentation.

9 Notification

The notification of the authorised CAB to the Commission is transmitted by the NCCA through the NANDO[2] system.

10 Timeline

The entire authorisation procedure should be completed within a maximum of 12 months.

11 Costs

The cost related to the authorisation of a CAB (accreditation excluded) are fully supported by the CAB and cover the external auditors mandated by the OLCN to cover the CAB competences review and the pilot evaluation review. The cost will be initially invoiced to ILNAS according to the invoicing of auditors' services form (ILNAS/ANCC/A003) and re-invoiced to the CAB.

[2] New Approach Notified and Designated Organisations (NANDO)