ILNAS/PSCQ/Pr001

Supervision of Qualified Trust Service Providers (*QTSPs*)

Modifications: Simplifications & minor corrections

1, avenue du Swing
L-4367 Belvaux
Tél.: (+352) 247 743 50
Fax: (+352) 247 943 50

confiance-numerique@ilnas.etat.lu
https://portail-qualite.public.lu

1 Introduction

The Luxembourg Institute for standardisation, accreditation, safety, and quality of goods and services (ILNAS, “Institut Luxembourgeois de la Normalisation, de l’Accréditation, de la Sécurité et qualité des produits et services”) is placed under the administrative supervision of the Minister of the Economy of the Grand Duchy of Luxembourg. The legal missions of ILNAS – Digital Trust Department are defined in [1].

ILNAS, via the “Digital Trust Department”, is notably charged with the supervision of QTSPs (Qualified Trust Service Providers) that are established in the Grand Duchy of Luxembourg and offer qualified trust services.

This document describes the scheme, requirements and process applied by the ILNAS – Digital Trust Department for the supervision of QTSPs. The supervision scheme is based upon Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation) [2].

2 Purpose of the procedure

The purpose of this procedure is to describe the process of supervising QTSPs. The procedure addresses primarily the clients and the staff of ILNAS – Digital Trust Department.

3 Definitions

For the requirements of this document, the definitions given in the eIDAS Regulation [2] apply. Furthermore, we denote by (Q)TSP a TSP that is either qualified or not, and by QTSP a TSP that holds the qualified status.

4 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[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) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ;

[3] European Union Agency for Network and Information Security (ENISA), Conformity Assessment of Trust Service Providers, Technical Guidelines on Trust Services, April 2017, available electronically at https://www.enisa.europa.eu/topics/trust-services/guidelines/auditing_framework

[4] ETSI TS 119 612 v2.1.1. (2015-07) Electronic Signatures and Infrastructures (ESI); Trusted Lists.

[5] ETSI EN 319 403 - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[6] CEN/TS 419 261 Security requirements for trustworthy systems managing certificates and time-stamps

[7] ISO/IEC 17 065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services

5 Supervision scheme for QTSPs

Figure 1 *National supervision scheme* illustrates the model for QTSP supervision. This scheme relies on the following elements:

1. The national accreditation body 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 conformity assessment bodies to carry out conformity assessment of a QTSP and the qualified trust services it provides;
2. **Conformity assessment bodies** (CABs), independent bodies of assessors, accredited by the national accreditation body of a Member state in accordance with Article 3 (18) of the eIDAS Regulation, carry out conformity assessments of QTSPs and the qualified trust services they provide against the requirements of the eIDAS Regulation [2]. The CAB should also be accredited according to the requirements in ISO/IEC 17065:2012 as well as those in ETSI EN 319403.
3. **ILNAS – Digital Trust Department**, the national supervisory body is responsible for the supervision of QTSPs and for establishing, maintaining and publishing the national trusted list (see [1]);
4. The national **trusted list** is a list which includes information on the QTSPs established in Luxembourg and supervised by ILNAS as well as information on the qualified trust services they provide.

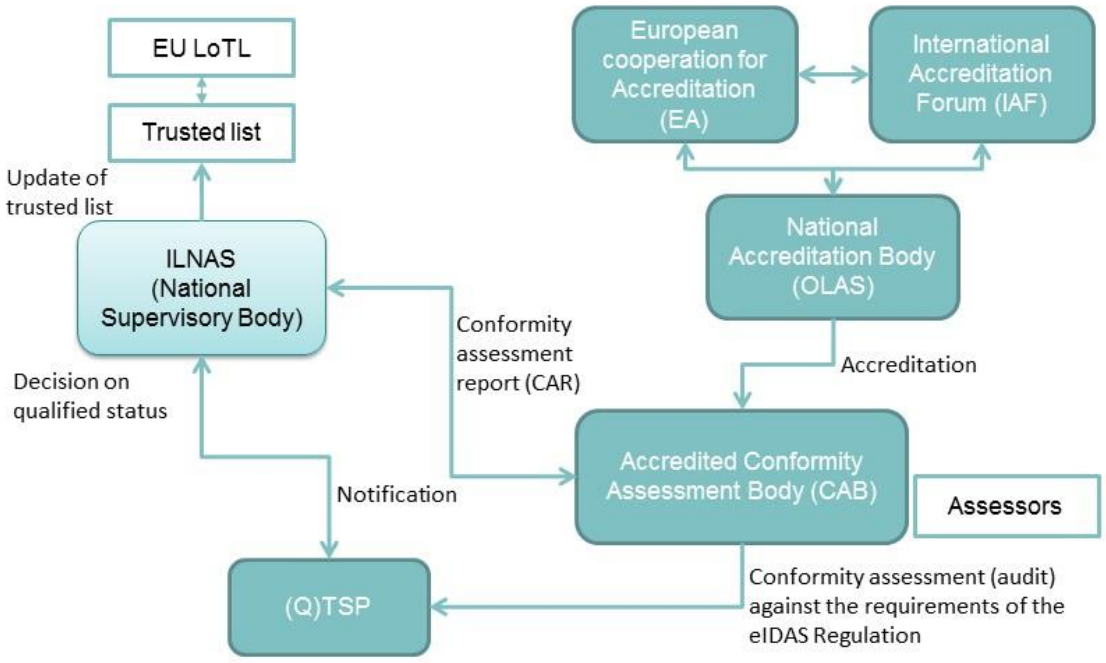

Figure 1 National supervision scheme

5.1 Requirements for qualified trust service providers issuing qualified certificates for electronic signature or for electronic seal in the case where the electronic signature creation data resp. electronic seal creation data are managed by the qualified trust service provider on behalf of the signatory resp. creator of seal:

1. The Qualified Trust Service Provider (QTSP) complies with the applicable requirements of the eIDAS Regulation.
2. The conformity of the qualified electronic signature (resp. seal) creation device shall be certified in accordance with Article 30 (resp. Article 39 (2)) of the eIDAS Regulation.
3. The Qualified Trust Service Provider implements the qualified electronic signature (resp. seal) creation device in accordance with the conditions of use specified in the Certificate of Conformity of the qualified signature (resp. seal) creation device and in the related certification report.
4. The Qualified Trust Service Provider has an up-to-date risk analysis that covers the risks associated with the use of the qualified electronic signature (resp. seal) creation device.

The conformity assessment body (CAB) has to check whether all of the above requirements are fulfilled.

Remark: Neither the certificate of conformity with respect to the applicable requirements of the eIDAS Regulation nor the certification report shall refer to opinion reports.

Criteria relating to the authentication of the legal person to the remote signature server for the creation of « remote qualified electronic seal creation »:

- The confidentiality and integrity of the data exchanged between the user and the remote signing server shall be guaranteed.
- Strong authentication of the user and the QTSP shall be put in place.
- The transmission of data between the user and the QTSP's environment shall be protected by appropriate cryptographic means.[1]
- If secret authentication information of the user (e.g., passwords, authentication codes, cryptographic keys) are stored on the "server" side (QTSP environment), then this secret authentication information shall be stored securely.
- Organizational measures shall be put in place that clarify the responsibilities of the legal person in the context of the usage of the qualified trust service (in particular, regarding the management of secret authentication information).
- The binding between "authentication" and "data to seal" shall be guaranteed.
- The elements mentioned above shall be treated in the risk analysis; mitigating measures shall be taken accordingly.

General recommendations:

- A policy on the use of cryptographic measures (e.g., algorithms, security protocols, hash functions, key management, key sizes) to protect the confidentiality, integrity, and authenticity of data should be developed and implemented.
- A policy on password management should be developed and implemented.
- The qualified trust service provider should monitor the authentication means that a user is allowed to use to authenticate himself to the qualified trust service provider's environment and should take appropriate measures in case of compromise of one of these authentication means.

[1] To meet this requirement, state-of-the-art security protocols (e.g., TLS) shall be used to secure the transmission of data between the user and the qualified trust service provider's environment.

- The transmission of data inside the qualified trust service provider's environment should be protected by appropriate cryptographic means. State-of-the-art security protocols (TLS, IPSEC, …) should be used to secure the transmission of data between technical assets in the qualified trust service provider's environment.

6 Supervision process

Figure 2 *Supervision process* illustrates the different steps to obtain the "qualified" status:

1. Notification;
2. Registration of the QTSP;
3. Assessment & supervision conclusions.

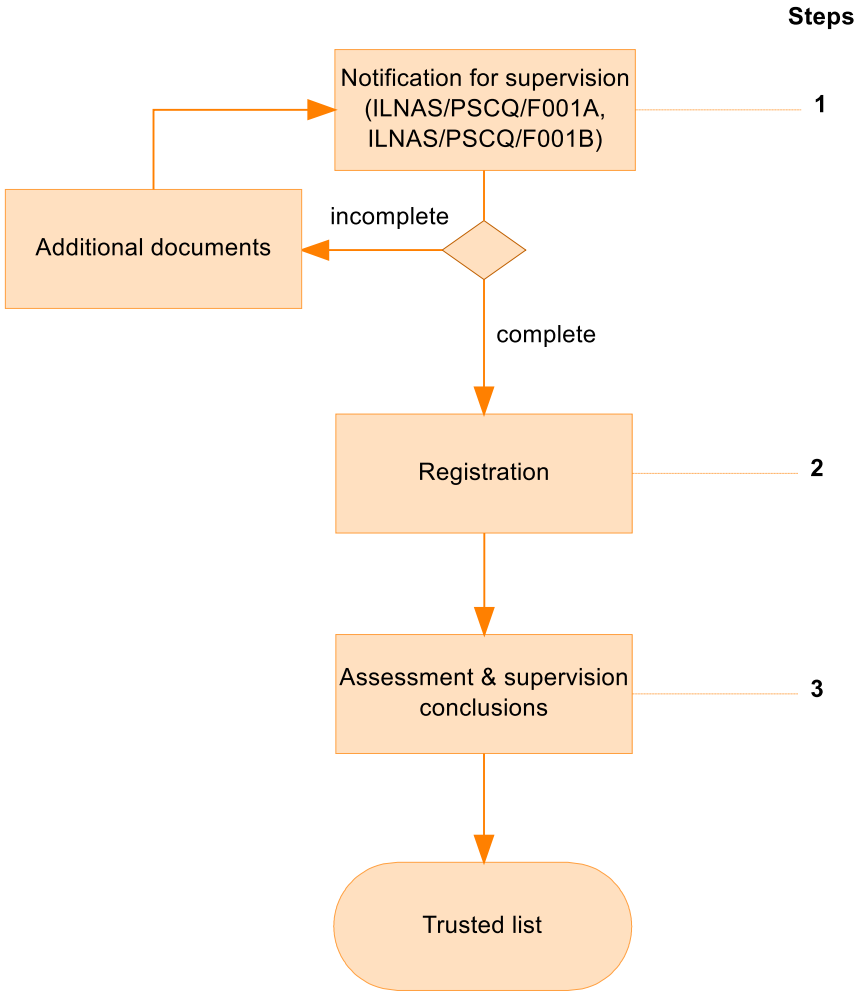

Figure 2 Supervision process

Step 1: Notification

A notification of a (Q)TSP who intends to provide qualified trust services is made by means of application form ILNAS/PSCQ/F001A - *Notification form to provide qualified trust services*.

The form includes, in addition to general information of the (Q)TSP, the scope of supervision. The form has to be dated and signed by a representative authorized to commit the (Q)TSP.

The (Q)TSP must also provide all the supporting documents listed in the notification form.

A (Q)TSP who intends to issue qualified certificates for electronic signature and/or for electronic seal, where the electronic signature creation data resp. electronic seal creation data are managed by the (Q)TSP on behalf of the signatory resp. creator of seal, is requested to also provide a description and/or diagram of the protocol between the user and the remote signing server to sign (resp. seal) data, in addition to the documents above.

The notification form enables the (Q)TSP to officially notify its intent to provide qualified trust services and constitutes "the triggering factor" for the supervision process. The form is also used to provide the ILNAS – Digital Trust Department - with any updated information about supervised QTSPs, which have undergone major changes to their structure, their organization or in their resources required to carry out the activities covered by the notification.

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

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

Alternatively, the notification can be sent electronically, in a secure way, to ILNAS (Digital Trust Department). The Digital Trust Department (confiance-numerique@ilnas.etat.lu) has to be contacted prior to sending the form and the supporting documents to discuss the transmission modalities.

On receipt of a notification form, the **administrative assistant** reviews the application and resources on the basis of *ILNAS/PSCQ/F004A – Check-list: Revue de la notification pour surveillance*. The scope of supervision is validated by the **supervision manager**.

Multi-Site organisations: For the supervision of a multi-site (Q)TSP organisation, the administration of the notification is described in Appendix ILNAS/PSCQ/A013 – *Supervision of multi-site QTSPs*.

If necessary, the Digital Trust Department can request additional documents not indicated in the notification form from the (Q)TSP before to recording the file.

Application to reduce, to voluntarily suspend or cancel supervision

A QTSP may apply at any time for a reduction, a suspension or cancelling of its qualified status by a letter sent to the ILNAS – Digital Trust Department - and signed by a representative authorized to commit the QTSP. The Trusted list or the scope of supervision is then updated and the changes notified to the QTSP.

The suspension leads to the prohibition for the TSP to refer to its status of supervised QTSP. Each voluntary suspension on which the QTSP hasn't done any follow-up within 18 months following the date of reception of the mail results in a change of status on the trusted list.

Step 2: Registration

ILNAS – Digital Trust Department - allocates an identification number to each notification for supervision. This number is valid for the whole supervision and can be used in all correspondence. The Digital Trust Department will transmit the number to the (Q)TSP making the notification for supervision. The notification for supervision is validated by the **head of the Digital Trust Department (Fr.: "chef du Département de la confiance numérique")**.

The case manager opens Form ILNAS/PSCQ/F018 *–Historique du Prestataire de Services de Confiance Qualifiés (PSCQ)* internally, which enables him to ensure traceability of key events during supervision (e.g., audits, supervision meetings). This record is reviewed by the supervision manager.

Step 3: Assessment & supervision conclusions

The supervision shall ensure that the QTSP and its qualified trust services meet the applicable requirements laid down in the eIDAS Regulation [2]. In this regard the certification shall be renewed every 2 years (via a reassessment audit) and a surveillance audit shall be conducted yearly. Furthermore, the EDP audit shall be renewed every 2 years.

The following elements are notably reviewed during supervision:

- Accreditation and scope of the conformity assessment body;
- Certification and scope of the conformity assessment of the QTSP;
- Coverage of the applicable requirements in [2] in the conformity assessment report;
- The provided documentation;
- If applicable, the resolution of nonconformities (including corrective actions)detected during conformity assessment.

The ILNAS – Digital Trust Department may request a CV of the auditors who performed the conformity assessment, if deemed necessary.

The management of the national Trusted List is under the authority of the ILNAS – Digital Trust Department *(see also,* ILNAS/PSCQ/Pr002 – *Gestion de la Liste de confiance ("Trusted list")*).

Decision by ILNAS

According to Article 21, paragraph 2, of the eIDAS-Regulation:

> "The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.
>
> If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists.."

Consequently, the final decision on granting the qualified status to a service provider and on inserting the trust services of the service provider into the national Trusted List is taken by ILNAS as supervisory body of qualified trust service providers.

After validation by the Director of ILNAS, the Digital Trust Department notifies the (Q)TSP of its decision.

Note 1:

In case of an ongoing supervision, if the applicable requirements in the eIDAS Regulation are met by the (Q)TSP and its (qualified) trust services, then the qualified status is either granted to the TSP and its trust services (in case of an initial conformity assessment) or retained by the QTSP and its qualified trust services.

If the applicable requirements in the eIDAS Regulation are not met by the QTSP or the qualified trust services it provides and if the QTSP fails to resolve non-conformities as requested by ILNAS – Digital Trust Department, then ILNAS – Digital Trust Department-may withdraw the qualified status of the QTSP or the qualified status of the concerned trust service(s). The status in the trusted list is then set to "withdrawn".

7 Standard's for assessing (Q)TSPs

7.1 Tools to support compliance

The conformity assessments shall be against the requirements of the eIDAS Regulation [2]. However, the following standards and technical specifications can be used as a tool to support the demonstration of compliance to eIDAS requirements (non-exhaustive list):

Scope of (Q)TSP activities or systems	Standard
General policy requirements for trust service providers supporting electronic signatures	ETSI EN 319 401
Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	ETSI EN 319 411-1
Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for Trust service providers issuing EU qualified certificates ;	ETSI EN 319 411-2
Certificate Profiles	ETSI EN 319 412
Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	ETSI EN 319 421
Time-stamping protocol and time-stamp token profiles	ETSI EN 319 422
Cryptographic Suites	ETSI TS 119 312
Security Requirements for Trustworthy Systems Supporting Server Signing	CEN/TS 419 241:2014
Security requirements for trustworthy systems managing certificates and time-stamps	CEN/TS 419 261:2015
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	IETF RFC 3647
Internet X.509 Public Key Infrastructure Time-Stamp Protocol	IETF RFC 3161
Cryptographic Message Syntax	IETF RFC 2630

7.2 Criteria Trusted Lists

The table below contains an extract from ETSI TS 119 612 V2.1.1 (2015-07) - D.5 EU specific Trusted Lists URIs [4] (pages 62-63):

Under Supervision "The service identified in "Service digital identity" (see clause 5.5.3) provided by the trust service provider identified in "TSP name" (see clause 5.4.1) is currently under supervision, for compliance with the provisions laid down in the applicable European legislation, by the Member State identified in the "Scheme territory" (see clause 5.3.10) in which the trust service provider is established." URI: http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision
Supervision of Service in Cessation "The service identified in "Service digital identity" (see clause 5.5.3) provided by the trust service provider identified in "TSP name" (see clause 5.4.1) is currently in a cessation phase but still supervised until supervision is ceased or revoked. In the event a different person than the one identified in "TSP name" has taken over the responsibility of ensuring this cessation phase, the identification of this new or fallback person (fallback trust service provider) shall be provided in "Scheme service definition URI" (clause 5.5.6) and in the "TakenOverBy" extension (clause 5.5.9.3) of the service entry. "Supervision of Service in Cessation" status shall be used when a TSP directly ceases its related services under supervision; it shall not be used when supervision has been revoked." URI: http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation
Supervision Ceased "The validity of the supervision assessment has lapsed without the service identified in "Service digital identity" (see clause 5.5.3) being re-assessed. The service is currently not under supervision any more from the date of the current status as the service is understood to have ceased operations. "Supervision Ceased" status shall be used when a TSP directly ceases its related services under supervision; it shall not be used when supervision has been revoked." URI: http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased
Supervision Revoked "Having been previously supervised, the trust service provider's service and potentially the trust service provider itself has failed to continue to comply with the provisions laid down in the applicable European legislation, as determined by the Member State identified in the "Scheme territory" (see clause 5.3.10) in which the trust service provider is established. Accordingly the service has been required to cease its operations and shall be considered by relying parties as ceased for the above reason. The status value "Supervision Revoked" may be a definitive status, even if the trust service provider then completely ceases its activity; it shall not be migrated (without any intermediate status) to either "Supervision of Service in Cessation" or to "Supervision Ceased" status in this case. The only way to change the "Supervision Revoked" status is to recover from non-compliance to compliance with the provisions laid down in the applicable European legislation according the appropriate supervision system in force in the Member State owing the trusted list, and regaining "Under Supervision" status. "Supervision of Service in Cessation" status, or "Supervision Ceased" status shall be used when a TSP directly ceases its related services under supervision; they shall not be used when supervision has been revoked." URI: http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionrevoked
Granted

"Following ex ante and active approval activities, in compliance with the provisions laid down in the applicable national legislation and Regulation (EU) No 910/2014 [i.10], it indicates that the Supervisory Body identified in the "Scheme operator name" (see clause 5.3.4) on behalf of the Member State identified in the "Scheme territory" (see clause 5.3.10) has granted a qualified status: to the corresponding trust service being of a service type specified in clause 5.5.1.1 and identified in "Service digital identity" (see clause 5.5.3), and to the trust service provider identified in "TSP name" (see clause 5.4.1) for the provision of that service." URI: http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
Withdrawn "In compliance with the provisions laid down in the applicable national legislation and Regulation (EU)No 910/2014 [i.10], it indicates that the qualified status has not been initially granted or has been withdrawn by the Supervisory Body on behalf of the Member State identified in the "Scheme territory" (see clause 5.3.10): from the trust service being of a service type specified in clause 5.5.1.1 and identified in "Service digital identity" (see clause 5.5.3), and from its trust service provider identified in "TSP name" (see clause 5.4.1) for the provision of that service." URI: http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

..... Source: ETSI TS 119 612 V2.1.1 (2015-07), pages 62-63.

Note 2 (Ad hoc conformity assessments):

Besides the yearly surveillance audit and the 2-yearly re-assessment audit, the supervisory body may, according to Article 20 (2) of the eIDAS Regulation, at any time audit or request a conformity assessment body to perform a conformity assessment of a qualified trust service provider at the expense of the trust service provider. The aim of this audit is to confirm that the qualified trust service provider and its qualified trust services fulfil the requirements laid down in this eIDAS Regulation. These ad hoc audits are triggered by the occurrence of certain events, for example:

- Events detected by the ILNAS, or
- Events notified by the QTSP to the ILNAS, e.g.:
  - Termination of one or more qualified trust services,
  - Changes of policies or procedures of the QTSP,
  - Major changes in the documentation of the QTSP,
  - Change in the provision of one or more qualified trust services,
  - Provision of a new trust service of the same type as trust services already provided by under significantly different policies,
  - Security breaches,
  - Personal data breaches,
  - Complaints.

Depending on the outcome of the ad hoc conformity assessment, the ILNAS may update the status of the QTSP or its qualified trust service(s) in the national trusted list.

Note 3 (Supervision meetings):

There shall be no larger period than six months for periodic surveillance of the QTSP by ILNAS – Digital Trust Department. The periodic supervision meetings are recorded in the form ILNAS/PSCQ/F018 *Historique du Prestataire de Services de Confiance Qualifié (PSCQ).*The minutes of the periodic supervision meetings are recorded using the form ILNAS/PSCQ/F016 - *Compte rendu des réunions dans le cadre de la surveillance des QTSP*. A periodic supervision meeting may be replaced by members of the Digital Trust Department being present during an audit of the QTSP, in which way case it is not necessary to prepare meeting minutes using the form ILNAS/PSCQ/F018.

8 Conformity assessment – Audit time

Conformity assessment bodies must give auditors enough time to perform initial audits, surveillance audits and reassessment audits.

Members of the ILNAS – Digital Trust Department - may be present during conformity assessments.

“Audit time” includes the time spent by an auditor or audit team in stage 1 audit (documentation review), stage 2 audit (on-site audit) and planning, interfacing with organization, personnel, records, documentation and process; and report writing. Usually, about 25% of the total audit time is spent on the stage 1 audit. Where additional time is required for planning or report writing, this will not be justification for reducing on-site auditor time. Auditor travel time is not included in the audit time.

The conformity assessment body and the (Q)TSP shall, in particular, take into account the following factors when determining audit time:

- The complexity of the trust service and of the IT infrastructure,
- The number of sites to audit,
- Third party arrangements used within the scope of the concerned trust service(s),
- The standards and regulatory requirements with respect to which the trust service(s) is (are) to be certified,
- Existing certifications and previous audits.

The (Q)TSP has to inform the ILNAS – Digital Trust Department- of the planned audit time prior to the audit. The audit time has to be agreed upon with the ILNAS – Digital Trust Department- for initial audits, surveillance audits, and reassessment audits, prior to the audit.

The conformity assessment body shall indicate the stage 2 (on-site) audit time in the conformity assessment report.