ILNAS

WHITE PAPER

DIGITAL TRUST

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Version 4.0 · December 2023
ISSN 2354-4996


COLLABORATION
PARTNER
OFFICE
SERVICE
EXCELLENCE
INDUSTRIAL
COLLABORATION

DIGITAL TRUST

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Version 4.0 · December 2023

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

Foreword

Contracts agreed upon online;

Meetings or vacations booked from smartphones;

Real-time video calls with our families or co-workers;

The list of examples of digitally-supported services that society benefits from nowadays goes on with many more items. Therefore, it is only natural that we require our communications to remain private, signatories of electronic contracts to be held to account, and online merchants to be authentic. In short, we need digital trust; and, the more digital services are offered, the more critical it becomes to deploy and manage techniques and systems that confer that trust.

Digital trust techniques have many different forms, including (but not limited to):

- fundamental cryptographic tools, such as digital signatures;
- cryptographically supported systems with a specific security purpose, for instance that of guaranteeing the integrity of digital documents over time, known as electronic archiving;
- the issuance of official documents, typically cybersecurity certificates, attesting to the implementation within systems or organizations of various information security controls; and
- worldwide processes to agree upon collectively – and encode in technical specifications - what adequate controls should be.

Altogether, these techniques form a chain of digital trust, layer after layer. Note that even higher layers exist, at the accreditation, governance, nation-legal, and even EU-legal levels.

As the Grand Duchy of Luxembourg pushes forward with its digitization goals, so too does the development of its digital trust-providing efforts. In particular, ILNAS – the *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*[1] – has been assigned a number of legal missions related to both European and national initiatives in support, directly or indirectly, of digital trust. These include the surveillance of providers of trust services and the management of the national trusted list, the surveillance of providers of digitization or e-archiving services, the surveillance of European cybersecurity certificates, and, also in this frame, the serving as the country's National Standards Body.

Raising the Luxembourg market's awareness in the existence and the substance of these tools is of utmost importance for economic actors to be in a position to take advantage of them based on their digital trust needs. Thus, ILNAS regularly conducts activities to reach this objective, for instance:

1 https://portail-qualite.public.lu/fr.html

- publishing white papers and technical reports in digital trust, such as those on trust service providers [1], e-archiving [2], or smart ICT [3], or in technical standardization, such as those on Quantum Technologies [4] or Artificial Intelligence [5];
- conducting research with other Luxembourgish partners - such as the research program "Technical Standardisation for Trustworthy ICT, Aerospace, and Construction (2021-2024)"[2], jointly with the University of Luxembourg[3] (which has yielded a white paper of its own [6]), or the European CORAL project[4], jointly with the Luxembourg House of Cybersecurity[5] and ANEC GIE[6]; and
- co-designing-and-managing educational projects, such as the Master in Technopreneurship: "mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions"[7], with the University of Luxembourg and the Luxembourg *Chambre des salariés*[8] through the Luxembourg Lifelong Learning Center[9].

This white paper is a continuation of these efforts, providing an update in particular on the work done by ILNAS' Digital Trust Department, and the services offered, for the benefit of the market.

Jean-Marie REIFF
Director
ILNAS

Jean-Philippe HUMBERT
Deputy Director
ILNAS

2 https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/normalisation-recherche.html
3 https://www.uni.lu/en/
4 https://coral-project.org/, co-financed by the Connecting Europe Facility of the European Union.
5 https://lhc.lu/
6 https://portail-qualite.public.lu/fr/acteurs/gie-anec.html
7 https://www.uni.lu/fstm-en/study-programs/master-in-technopreneurship/
8 https://www.csl.lu/fr/
9 https://www.csl.lu/fr/lllc/

Acknowledgements

The working group involved in the preparation of this White Paper is:

Name of the contributor	Institution/Organization
Mr. Jean-Marie REIFF	ILNAS
Dr. Jean-Philippe HUMBERT	ILNAS
Mr. Alain WAHL	ILNAS
Dr. Michèle FELTZ	ILNAS
Mme Leslie FOUQUERAY	ILNAS
Mr. Jean-François GILLET	ILNAS
Mme Anna JADACH	ILNAS
Dr. Jean LANCRENON	ILNAS
Dr. Michel LUDWIG	ILNAS

Table of contents

	Foreword	**4**
	Acknowledgements	**7**
	Abbreviations	**10**
	List of Figures	**12**
	List of Tables	**12**
1.	**Introduction**	**15**
1.1.	**The drive towards digitization**	**15**
1.1.1.	Europe's digital decade	15
1.1.2.	Digitization goals in the Grand Duchy of Luxembourg	15
1.2.	**The need for digital trust**	**16**
1.2.1.	Trust-building initiatives in the EU	16
1.2.2.	Digital trust in Luxembourg, and ILNAS	17
1.3.	**Purpose and structure of the white paper**	**18**
2.	**Electronic identification and electronic signatures**	**21**
2.1.	**Trust Services**	**22**
2.1.1.	Electronic signatures	22
2.1.2.	Electronic seals	24
2.1.3.	Legal effects	25
2.2.	**Trust services under eIDAS**	**26**
2.2.1.	Definition and description of trust services	26
2.2.2.	Qualified trust services	29
2.2.3.	Remote signing services	33
2.3.	**ILNAS Supervision Scheme for qualified trust service providers**	**35**
2.3.1.	Initiation of the Supervision	36
2.3.2.	During the Supervision	37
2.3.3.	Termination of the Supervision	38
2.4.	**Trusted lists**	**39**
2.4.1.	National trusted list	39
2.4.2.	European List of Trusted Lists (LOTL)	42
2.5.	**The revision of the eIDAS Regulation (eIDAS2)**	**43**
3.	**E-archiving and dematerialization**	**47**
3.1.	**The Electronic Archiving Framework in Luxembourg**	**49**
3.2.	**The Law of 25 July 2015 on Electronic Archiving**	**54**
3.3.	**Supervision scheme for PSDCs**	**56**
3.3.1.	Initiation of the Supervision	57
3.3.2.	During the Supervision	59
3.3.3.	Termination of the Supervision	60

3.4.	**Certification of PSDCs**	**61**
3.4.1.	The ISO/IEC 27000 Family of Standards	61
3.4.2.	ISO/IEC 27000:2018	62
3.4.3.	ISO/IEC 27001:2013	62
3.4.4.	ISO/IEC 27002:2013	63
3.4.5.	ISO/IEC 27006	63
3.4.6.	ISO 14641:2018	63
3.4.7.	The National Standard ILNAS 106:2022	65
4.	**Cybersecurity certification**	**69**
4.1.	**The Cybersecurity Act**	**69**
4.1.1.	General purpose and major features	69
4.1.2.	Market actors and their interactions	72
4.1.3.	The European Cybersecurity Certification Group and other EU-level governance bodies	73
4.2.	**Cybersecurity certification schemes**	**74**
4.2.1.	Scheme content requirements	74
4.2.2.	Scheme creation process	75
4.2.3.	Upcoming schemes	76
4.3.	**Relation of the CSA to other pieces of EU legislation**	**82**
4.4.	**ILNAS' role**	**84**
5.	**Technical standardization**	**87**
5.1.	**Technical standards**	**87**
5.2.	**Major international and European standards bodies**	**88**
5.2.1.	ISO and IEC Standardization Committees	89
5.2.2.	CEN and CENELEC Standardization Committees	89
5.2.3.	ETSI - European Telecommunications Standards Institute	89
5.2.4.	ITU-T - International Telecommunication Union - Telecommunication Standardization Sector	90
5.2.5.	Cooperation between standards-developing organizations	90
5.3.	**ILNAS and ANEC GIE in technical standardization**	**91**
5.3.1.	ILNAS	91
5.3.2.	ANEC GIE	91
5.4.	**Standardization committees relevant to Digital Trust**	**92**
5.5.	**Participating in technical standardization**	**94**
5.5.1.	Benefits	94
5.5.2.	How to get involved in Luxembourg	94
6.	**Conclusion and outlook**	**97**
	References	**99**

Abbreviations

AI	Artificial Intelligence
AIA	AI Act
ANEC GIE	*Agence pour la Normalisation et l'Economie de la Connaissance*
CAB	Conformity Assessment Body
CB	Certification Body
CC	Common Criteria
CEM	Common Evaluation Methodology
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
COFRAC	*Comité Français d'accréditation*
CRL	Certificate Revocation List
CSA	Cybersecurity Act
CRA	Cyber Resilience Act
CSSF	*Commission de Surveillance du Secteur Financier*
DMA	Digital Markets Act
DTD	Digital Trust Department
EA MLA	European Cooperation for Accreditation Multilateral Agreement
EC	European Commission
ECCF	European Cybersecurity Certification Framework
ECCG	European Cybersecurity Certification Group
EDP	Electronic Data Processing
eIDAS	Regulation (EU) No 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
ESO	European Standardization Organization
ETSI	European Telecommunications Standards Institute
EU	European Union
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ILNAS	*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*
IoT	Internet of Things
IS	International Standard
ISG	Industry Specification Group
ISO	International Organization for Standardization
IT	Information Technology

ITSEF	IT Security Evaluation Facility
ITU	International Telecommunications Union
ITU-T	ITU's Telecommunication standardization sector
LOTL	List of Trusted Lists
MRA	Mutual Recognition Agreement
MS	Member State
NAB	National Accreditation Body
NCCA	National Cybersecurity Certification Authority
NIS	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
OLAS	*Office Luxembourgeois d'Accréditation et de Surveillance*
OLN	Organisme luxembourgeois de normalisation
PSDC	*Prestataire de Services de Dématérialisation ou de Conservation*
QCertSeal	Qualified Certificates for Electronic Seals
QSealCD	Qualified Electronic Seal Creation Device
QSigCD	Qualified Electronic Signature Creation Device
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate
REM	Registered Electronic Mail
SAR	Security Assurance Requirement
SCCG	Stakeholder Cybersecurity Certification Group
SDO	Standards Developing Organization
SFR	Security Functional Requirement
SG	Study Group
SOG-IS	Senior Officials Group – Information Systems' Security
TC	Technical Committee
TLSO	Trusted List Scheme Operator
TR	Technical Report
TS	Technical Specification
TSA	Time Stamping Authority
TSP	Trust Service Provider

List of Figures

Figure 1:	The departments of ILNAS	17
Figure 2:	Venn diagram of electronic signature classes and examples	22
Figure 3:	Venn diagram of electronic seal classes and examples	24
Figure 4:	Signature validation process	28
Figure 5:	National supervision scheme	34
Figure 6:	The Luxembourg trusted list	40
Figure 7:	The trusted list browser	41
Figure 8:	Typical workflow of digitization	51
Figure 9:	Typical workflow of electronic archiving	52
Figure 10:	Supervision scheme for digitization and e-archiving service providers	57
Figure 11:	The major features of the CSA certification framework	70
Figure 12:	A generic view of the interactions between the different market actors in the CSA certification framework	73
Figure 13:	An overview of the certification scheme creation process	76
Figure 14:	A view of the interactions between the different market actors in the CSA certification framework in the case of Luxembourg	85
Figure 15:	Relative positioning of the main standards developing organizations	89

List of Tables

Table 1:	Simplified List of PSDCs as of 17 October 2023	58
Table 2:	Some legislative texts that may benefit from the CSA	83
Table 3:	International, European, and national standardization committees encountered in this report	93

1

1 Introduction

1. Introduction

1.1. The drive towards digitization

It is no secret that society is becoming ever more digitized, whether this is for entertainment, commerce, business, communications, social interactions, or industrial development, to name just a few domains. It is simply now a matter of fact.

Digitization has many advantages, such as accelerating the transmission of information, providing services online rather than in person, reducing the usage of hardcopies, and enabling near-instantaneous interactions between entities all over the world. The implications in terms of efficiency and simplicity are extremely promising. Thus, in this vein a real effort towards digitization has been taking place, and continues to do so, at all levels of societal governance.

1.1.1. Europe's digital decade

Taking as a first example the European Union (EU), there is a true strategic embrace of digitization, as evidenced by the push towards a digital Europe through a digitization roadmap: Europe's Digital Decade[10], setting goals for 2030 in terms of citizens' skills, digitization of businesses and public services, and sustainable infrastructures. This vast roadmap lays out objectives in the proficiency of the general public in the usage of digital tools, the development of sectoral electronic services (such as e-health), and the effective uptake by European market actors of emerging information technology paradigms such as Cloud Computing and Artificial Intelligence, among other things.

The roadmap is to be followed in accordance with citizens' fundamental rights, which are also affected by this ever-growing digital space. Thus, a European Declaration on Digital Rights and Principles [7] was adopted, laying out how the digital world should, and should not, affect key principles such as the protection of democracy, the transition towards a more sustainable society, and the provisioning of safety and security.

1.1.2. Digitization goals in the Grand Duchy of Luxembourg

At the national level, Luxembourg has digitization goals as well. The government has had over the past few years many different initiatives driving digitization[11]; currently, the strategy is pushed along four axes that are the development of e-government, the advancement of administrative reform (namely its continued digitization), the promotion of digital inclusion, and the integration of new technologies[12].

It is also the case that Luxembourg's economy is highly ICT-oriented. In 2020, the number of companies working in the field of information and communication was estimated at just under 3000, representing roughly 7.7% of the total number of companies counted in STATEC's 2020 *Répertoire des entreprises luxembourgeoises* [8], and in the fourth quarter of 2022, it represented 4.4% of total employment[13]. Furthermore, the European Union's Digital Economy and Society Index (DESI) 2022 [9] indicates that Luxembourg has particularly strong showings in certain categories of digital development, such as broadband connectivity, the rate of internet connections in households, digital public services for citizens and businesses, and cross-border services, to name a few.

10 https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

11 https://digital.gouvernement.lu/fr.html

12 https://digital.gouvernement.lu/fr/axes.html

13 Per the Luxembourg statistics portal: https://statistiques.public.lu/en.html

1.2. The need for digital trust

Of course, not everything can be digitized, and among those things that can – yielding concepts such as digital identities or electronic health records, for instance - considerable care must be taken to make sure that this is done not just effectively, ensuring the desired functionality, but also *securely*, that is with adequate guarantees that users' digital artefacts – such as their data – are at all times protected from unauthorized access, disclosure, tampering or other misuse. The uptake by citizens and other market players of digital solutions is conditioned on the level of trust that is perceived in these very solutions. As a result, tools for both providing digital trust, and demonstrating thorough assessments attesting to trustworthiness, come into play.

These considerations are also part of the picture at European and national levels.

1.2.1. Trust-building initiatives in the EU

Broad tools at the EU level in the direction of digital trust come for example in the form of policy and strategy decisions, and as legislation to enforce the implementation of those policies.

As an illustration of the former, since 2020 there has been an EU Cybersecurity Strategy [10] in place, specifically geared at accompanying the European digital decade roadmap to ensure trustworthiness of deployments throughout the transition. Directly citing an EU source[14]: *"the Strategy will bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools"*. Pillars upon which the overall strategy is built include technological and digital sovereignty, capacity-building in the activities of detection of, and response to, cyberattacks, and ensuring an open and safe cyberspace.

In the latter category, both existing and upcoming legislation address trustworthiness and cybersecurity head-on. Most relevant to the present white paper are:

- The eIDAS Regulation [11], its upcoming revision [12], and the NIS2 Directive [13], collectively tackling the topics of digital identities, trust service provisioning, and the cyber-resilience requirements of categories of essential and important market entities; and
- The Cybersecurity Act [14] and its proposed amendment [15], laying the groundwork for a digital single market of cybersecurity certification for ICT products, services, processes, and potentially soon managed security services[15].

Thus, it is clear that the EU is viewing digital trust as something that must be built into its digitization process from the start, as opposed to having it patched on after the fact.

14 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391, last accessed 23/10/2023

15 This depends on how the proposed amendment is eventually processed.

1.2.2. Digital trust in Luxembourg, and ILNAS

Again mirroring what exists at the EU level, Luxembourg recognizes the importance of digital trust for its national market.

As an example of this, currently in force is the Luxembourg Cybersecurity Strategy IV [16], paving the way for developments in the areas of reinforcement of trust in the digital world, the consolidation of security and resilience of identified national critical entities, the development of a secure digital economy, and doing so in the context of an adequate governance framework for the country with additional emphasis on education, awareness raising, and capacity-building.

Another example is the launch of the Luxembourg Cybersecurity Portal[16] to federate a community of cybersecurity-mindful entities and individuals for the benefit of the whole country. One can generally turn to this resource for all kinds of expertise and support. The platform itself is managed by the Luxembourg House of Cybersecurity[17].

In this general context, ILNAS[18] (*the Institut luxembourgeois pour la normalisation, l'accréditation, la sécurité et qualité des produits et services*) has several legal missions (encoded in the law of 23 December 2022 [17]) in direct relation with the development of a secure digital market. ILNAS is a public administration under the authority of the Minister of the Economy of the Grand Duchy of Luxembourg. Founded in 2008, ILNAS represents a network of competencies relating to quality, safety and conformity of products and services (see Figure 1), and its mission is to support national competitiveness. Details on ILNAS' activities can be found online, on the *Portail Qualité*: https://portail-qualite.public.lu/fr.html.

Figure 1: The departments of ILNAS

16 https://www.cybersecurity.lu/

17 https://lhc.lu/

18 https://portail-qualite.public.lu/fr/acteurs/ilnas.html

More specifically related to digital trust, ILNAS serves:

- As the national surveillance body for Trust Service Providers (Qualified or not) in the frame of the EU's eIDAS regulation, also in charge of the management of the national trusted list;
- As the national surveillance body for "providers of digitization or e-archiving services" *(Prestataire de Services de Dématérialisation ou de Conservation,* or PSDC*)*, a status encoded in a national framework [18], and;
- As the National Cybersecurity Certification Authority (NCCA) in charge of supervision activities in the context of the EU's Cybersecurity Act.

These tasks are taken on by ILNAS' Digital Trust Department (DTD).

Furthermore, it is well known that in matters of information security, cybersecurity, and digital trust, it is best to not reinvent the wheel. Accordingly, the aforementioned legal and technical frameworks - whether European or national - are supported as much as possible by references to the good practices found in international and European standards. On this topic, at the European level, one can turn to the European Rolling Plan for ICT Standardisation[19] to learn about the EU's standardization priorities, in particular in Cybersecurity/Network and Information Security within the "Foundational Drivers" chapter. At the national level, ILNAS serves also as Luxembourg's national standards body. Thus, in addition to supporting the country's market in specific digital trust and cybersecurity matters, ILNAS also provides a doorway to those actors who wish to remain aware of - and even influence - the relevant standards landscape. The department within ILNAS handling this is the *Organisme luxembourgeois de normalisation* (OLN).

1.3. Purpose and structure of the white paper

This white paper gives a snapshot of ILNAS' missions regarding digital trust and related standardization activities as they exist today, for the benefit of the Luxembourg economy's actors. The main departments of ILNAS that are focused on in this document are the Digital Trust Department (DTD) and the *Organisme luxembourgeois de normalisation* (OLN). More specifically:

- Chapter 2 covers the topics of trust service providers and electronic signatures, as an update to the previously published report "Trust Services under the eIDAS Regulation" [1];
- Chapter 3 provides an overview of activities in e-archiving and dematerialization, as an update to the previously published report "An Introduction to the e-Archiving Framework in Luxembourg" [2];
- Chapter 4 delves into the subject of cybersecurity certification; and
- Chapter 5 explains related technical standardization activities.

Finally, a conclusion and some outlooks are provided in Chapter 6.

19 https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2023

2

2

Electronic identification and electronic signatures

2. Electronic identification and electronic signatures

This first technical chapter deals in trust services articulated around the cryptographic tool that is the digital signature.

Trust in the digital world is essential for making individuals and organizations use and adopt electronic services. Such services allow their users, for instance, to sign electronic documents with the help of electronic signatures, or to authenticate the website they are connecting to. Moreover, users may want to make sure that the integrity of electronic data that they store (e.g., electronically signed contracts, logging events) is preserved and that the data can be traced back to a particular point in time establishing evidence that the data existed at that time.

The eIDAS Regulation [11] entered into force on 17 September 2014 and became applicable on 1 July 2016 (except for certain articles). The eIDAS Regulation replaces the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [19] (the eSignature Directive). As a Regulation of the European Union, it is directly applicable in all the EU Member States and hence also in Luxembourg.

The eIDAS Regulation mainly covers the following topics:

- **Electronic identification**: The eIDAS Regulation sets out conditions for EU Member States under which *electronic identification means*, issued in an EU Member State, have to be recognized in another EU Member State to access public online services and how to notify electronic identification schemes.
- **Trust services**: The eIDAS Regulation provides a legal framework for a range of trust services, including certificates for electronic signatures, certificates for electronic seals, certificates for website authentication, time stamp services, electronic registered delivery services, preservation services for electronic signatures/seals, and validation services for electronic signatures/seals. In particular, it specifies security requirements applicable to trust service providers, requirements for qualified trust services providers, as well as the missions of the supervisory body.
- **Electronic documents**: The eIDAS Regulation dedicates a chapter to electronic documents, that is, any content stored in electronic form [11]. The chapter on electronic documents consists of one article which states that electronic documents benefit from the principle of non-discrimination as evidence in legal proceedings. This principle ensures that an electronic document is not denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form ([11], Article 46). Hence, in the European Union, a judge cannot reject an electronic document as evidence solely on the grounds that it is in electronic form. She or he may however reject the document on other grounds such as the lack of authenticity or the lack of integrity of the document.

The complete list of standards published by ETSI in support of the eIDAS regulation is available at the following location[20].

To enhance consumers' trust in electronic transactions, the eIDAS Regulation introduces the notions of "qualified" trust services (e.g., qualified electronic time stamps services, qualified electronic registered delivery services) which can only be provided by "qualified" trust service providers. Compared to trust service providers who provide non-qualified trust services, "qualified" trust service providers need to meet further and stricter requirements.

In Luxembourg, ILNAS is the supervisory body for trust service providers that are established on its territory [20]. In this context, ILNAS is in charge of the supervision of trust service providers and the trust services that they provide with respect to the requirements of the eIDAS Regulation.

20 https://portal.etsi.org/TB-SiteMap/esi/esi-activities

2.1. Trust Services

The goal of this section is to inform about the different trust services introduced by the Regulation (EU) No 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 (the eIDAS Regulation) [11], to present the supervision scheme for qualified trust service providers that is applied by the Digital Trust Department of ILNAS, and to indicate incentives for using trust services.

2.1.1. Electronic signatures

The eIDAS Regulation distinguishes between three different classes of electronic signatures, namely the class of electronic signatures, the class of advanced electronic signatures, and the class of qualified electronic signatures.

An electronic signature is defined in the eIDAS Regulation as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign" [11], where the signatory is a natural person who creates electronic signatures.

The broad class of electronic signatures includes, for example (see also Figure 2):

- scanned signatures, and
- email signatures, that is, content that is added at the end of an email and which typically includes the name of a person, contact details, and a company logo.

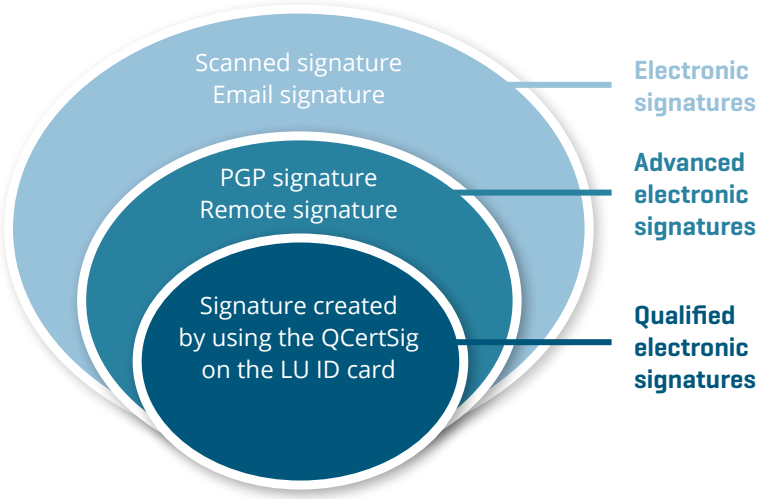

Figure 2: Venn diagram of electronic signature classes and examples

A subclass of the class of electronic signatures is the class of advanced electronic signatures. According to Article 3(11) of the eIDAS Regulation, an advanced electronic signature is an electronic signature that meets the requirements of Article 26 of the eIDAS Regulation [11], that is: "(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable". Digital signatures[21], which are based on public-key cryptography, can satisfy the requirements on advanced electronic signatures given in the eIDAS Regulation.

21 A digital signature is "data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient", [60].

A user U with private/public key pair (sk, pk) can digitally sign data (e.g., an electronic document) using his private key sk. Any other party can verify that a given digital signature of user U on certain data is a valid signature using the corresponding public key pk.

The private signature key that the user uses to create a digital signature corresponds to the electronic signature creation data; it can be stored, for example, on a smart card or on a USB stick, under the control of the user. The private signature key can also be managed and stored by a trust service provider who offers remote signing services; the private key can be activated by the user to create digital signatures via a secure authentication process between the user and the remote signing service.

Digital signatures are used to ensure the authenticity and integrity of data (e.g., electronic documents, emails, software). Moreover, it is difficult for a natural person who created a digital signature on data to subsequently deny having created the signature (non-repudiation). In that sense, they provide higher security guarantees than simple electronic signatures that do not belong to the class of advanced electronic signatures.

The following types of signatures are examples of advanced electronic signatures:

- digital signatures created by using a private key for which a certificate for electronic signatures on the corresponding public key has been issued by a trust service provider,
- digital signatures created by using a private key stored on a smart card which also contains a qualified certificate for electronic signatures on the corresponding public key,
- digital signatures created remotely by a user whose private key and corresponding certificate for electronic signatures are managed by a trust service provider (this type of service is often called “remote signing service”),
- digital signatures created by using a PGP private key ("web of trust" model).

The class of qualified electronic signatures contains all advanced electronic signatures that have been created by a qualified electronic signature creation device (QSigCD), and which are based on qualified certificates for electronic signatures that have been issued by a qualified trust service provider [11]. Qualified electronic signatures provide even stronger security guarantees than advanced electronic signatures as they (a) have to be created by a device that has been certified to satisfy the requirements in Annex II of the eIDAS Regulation, (b) are based on qualified certificates for electronic signatures and (c) those qualified certificates are issued by a qualified trust service provider. The European Commission maintains a list containing QSigCDs [21]. See Section 2.4. for more on the trusted lists.

A concrete example of a qualified electronic signature is:

- a digital signature created by using the private key associated to the qualified certificate for electronic signatures contained in the Luxembourgish identity card issued under the law of 19 June 2013 on the identification of natural persons, as amended [22][22].

A qualified electronic signature can not only be created via the use of smart cards that have been certified as QSigCDs, but also remotely via a hardware security module (HSM) that has been certified as a remote QSigCD and under the control of a qualified trust service provider. We refer the reader to Section 2.2.3. for details on remote signature services.

22 Note that the Luxembourgish identity card contains two public-key certificates, one qualified certificate for electronic signatures and one certificate for authentication purposes [11].

2.1.2. Electronic seals

The electronic signatures can only be created by natural persons. Legal persons have the possibility to create electronic seals on data (e.g., electronic documents, software code) to ensure its integrity and authenticity.

Similar to the classification of electronic signatures, the eIDAS Regulation distinguishes between three different classes of electronic seals, namely the class of electronic seals, the class of advanced electronic seals, and the class of qualified electronic seals (see also Figure 3).

An electronic seal is defined in the eIDAS Regulation as "data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity" [11]. Compared to electronic signatures, electronic seals can only be created by legal persons, not by natural persons.

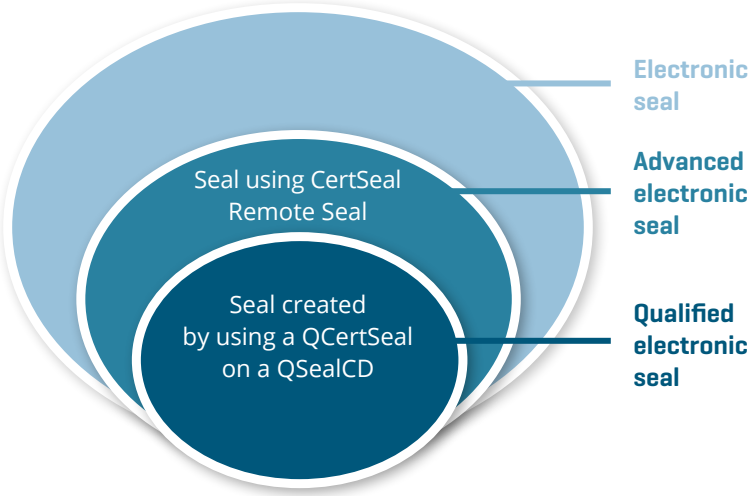

Figure 3: Venn diagram of electronic seal classes and examples

A subclass of the class of electronic seals is the class of advanced electronic seals. According to Article 3(26) of the eIDAS Regulation, an advanced electronic seal is an electronic seal that meets the requirements of Article 36 of the eIDAS Regulation [11], that is: "(a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable", where the "creator of a seal" is defined in the eIDAS Regulation as the legal person who creates the seal.

Digital signatures can satisfy the requirements above. The following types of seals are examples of advanced electronic seals:

- digital signatures created by using a private key for which a certificate for electronic seals (CertSeal) on the corresponding public key has been issued by a trust service provider,
- digital signatures created remotely by a legal person whose private key and corresponding certificate for electronic seals are managed by a trust service provider (this type of service is often called "remote sealing service").

The class of qualified electronic seals contains all advanced electronic seals that have been created by a qualified electronic seal creation device (QSealCD), and which are based on qualified certificates for electronic seals (QCertSeal) that have been issued by a qualified trust service provider [11]. Qualified electronic seals provide even stronger security guarantees than advanced electronic seals as they (a) have to be created by a device that has been certified to satisfy the requirements in Annex II of the eIDAS Regulation, (b) are based on qualified

certificates for electronic seals and (c) those qualified certificates are issued by a qualified trust service provider. Note that the list published by the European Commission also contains QSealCDs [21]. See Section 2.4 for more on the trusted lists.

Applications

Electronic seals can be used by legal persons for various applications:

- Universities can use electronic seals to guarantee the origin and integrity of electronic versions of the diplomas of their students. Future employers of the students can hence readily verify the authenticity of the diplomas.
- Companies can use electronic seals to guarantee the authenticity of invoices that they send to their clients electronically. The verification of the electronic seal on the invoice allows the client to have certainty that the invoice indeed originates from the company and has not been modified.

2.1.3. Legal effects

Non-discrimination as evidence in legal proceedings. The eIDAS Regulation applies the principle of non-discrimination to electronic signatures, electronic seals, electronic time stamps, data sent and received using electronic registered delivery services, and electronic documents. Thus, in particular, electronic signatures and seals cannot be denied legal effect and admissibility as evidence in legal proceedings only on the grounds that they are in electronic form or that they do not meet the requirements for qualified electronic signatures or seals, respectively.

Legal effect of qualified electronic signatures. As qualified trust service providers who issue qualified certificates for electronic signatures on qualified electronic signature creation devices (QSigCDs) have to meet all the applicable requirements in the eIDAS Regulation[23], qualified electronic signatures that have been created by these QSigCDs provide stronger security guarantees and higher legal certainty than nonqualified electronic signatures. Therefore, the eIDAS Regulation grants to qualified electronic signatures the equivalent legal effect of handwritten signatures ([11], Article 25(2)).

Legal effect of qualified electronic seals. According to Article 35 paragraph (2) of the eIDAS Regulation [11], qualified electronic seals enjoy "the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked".

Recognition in all EU Member States of qualified electronic signatures and seals. The eIDAS Regulation regulates the cross-border recognition of qualified electronic signatures and seals on an EU level, which is particularly interesting for companies that carry out digital transactions in more than one EU Member State:

- Qualified electronic signatures based on qualified certificates for electronic signatures issued in one EU Member State are recognized as qualified electronic signatures in all other EU Member States ([11], Article 25(3)).
- Qualified electronic seals based on qualified certificates for electronic seals issued in one EU Member State are recognized as qualified electronic seals in all other EU Member States ([11], Article 35(3)).

23 In particular, the qualified trust service provider has to verify the identity of the natural person to whom the qualified certificate for electronic signatures is issued.

2.2. Trust services under eIDAS

The scope of the eIDAS Regulation is larger than the one of the eSignature Directive as it not only covers the provision of certificates for electronic signatures, but also a variety of other trust services including the provision of certificates for electronic seals, the provision of certificates for website authentication, the creation of electronic timestamps, electronic registered delivery services, and the preservation of electronic signatures or seals.

2.2.1. Definition and description of trust services

Under Article 3(16) of the eIDAS Regulation, a "trust service" is defined as "an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication, or
- the preservation of electronic signatures, seals or certificates related to those services" [11].

For a subset of these trust services, there are specific requirements in the eIDAS Regulation for them to be considered as "qualified trust services". As already mentioned in the introduction of this chapter, trust service providers who intend to provide qualified trust services need to meet additional and stricter requirements which are specified in the Regulation (see Section 2.2.2.).

In the following we describe some of the trust services in more detail. Qualified trust services and the requirements of those services will be addressed in Section 2.2.2.

Provision of certificates for electronic signatures

A certificate for electronic signature is an *"electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person"* ([11], Article 3(14)). In more technical terms, a certificate for electronic signature binds the identity of a natural person to a public key.

Certificates for electronic signature can be used by natural persons to sign data. More precisely, a natural person can create an electronic signature on data using the private key corresponding to the public key contained in the certificate.

Provision of certificates for electronic seals

A certificate for electronic seal is *"an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person"* ([11], Article 3(29)). Compared to a certificate for electronic signature, a certificate for electronic seal binds the identity of a legal person to a public key.

Certificates for electronic seals can be used by legal persons to ensure:

- the authenticity of data (i.e., the data originates from the legal person to whom the certificate has been issued), and
- the integrity of data (i.e., the data has not been modified)

while transmitted over a network or stored on some hardware. Furthermore, a legal person who creates an electronic seal based on a certificate for electronic seal on data cannot later on deny having created the seal (non-repudiation).

Provision of certificates for website authentication

A certificate for website authentication is *"an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued"* ([11], Article 3 (38)).

Certificates for website authentication can be used to authenticate a website (i.e., to confirm that the entity behind the website is who it claims to be). These certificates can be used in the TLS protocol to secure the communication between a web server and a web browser. If a certificate for website authentication is used on the server side, the TLS protocol provides authentication of the server, and integrity and confidentiality of the information transmitted between the web server and the browser.

Creation of electronic timestamps

According to Article 3(33) of the eIDAS Regulation, an electronic timestamp is *"data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time"* [11]. Time stamps are usually used to bind data to a particular point in time in order to be able to prove later on that the data (e.g., scientific publications, electronically signed contracts, electronic files, intellectual property) existed at that point in time and is bound to a certain identity.

Time stamps can be created by a central Time Stamping Authority (TSA) who acts as a trusted third party. The Time Stamping Authority creates time stamps on some data to establish evidence indicating that the data existed at that point in time.

Under Article 41(1) of the eIDAS Regulation, electronic time stamps benefit from a non-discrimination clause as evidence in legal proceedings, meaning that a judge cannot reject them as evidence only on the grounds that they are in electronic form or that they do not meet the requirements of qualified electronic time stamps.

Validation of electronic signatures/seals

According to Article 3(41), the validation of an electronic signature/seal refers to the process of verifying and confirming that an electronic signature or a seal is valid [11].

In Figure 4 we illustrate a signature validation process between a user and a trust service provider (TSP) who provides a signature validation service. We assume a secure channel between the user and the TSP in order to ensure the confidentiality and integrity of the transmitted messages as well as entity authentication of the TSP's server. The signature validation works as follows:

- The user first sends a signature validation request to the TSP via the signature validation client. This request typically includes an electronic document as well as a signature on an electronic document.
- Upon receipt of the request, the TSP executes the signature validation application, which may require accessing information from external sources (e.g., other TSPs, the EU LOTL (see Section 2.5.2.)). The signature validation application may perform different checks, such as:
  - Revocation check: the check whether the certificate was not revoked at the time of signing,
  - Expiration check: the check whether the certificate was not expired at the time of signing,
  - Digital signature check: the cryptographic verification whether the digital signature is a valid signature on the electronic document.
- The TSP returns the signature validation result, via the signature validation application, to the user. The validation result typically contains an indication as to whether or not the signature is a valid signature on the document and may contain additional information such as information about the type of signature (advanced or qualified) or the reasons why the signature is invalid.

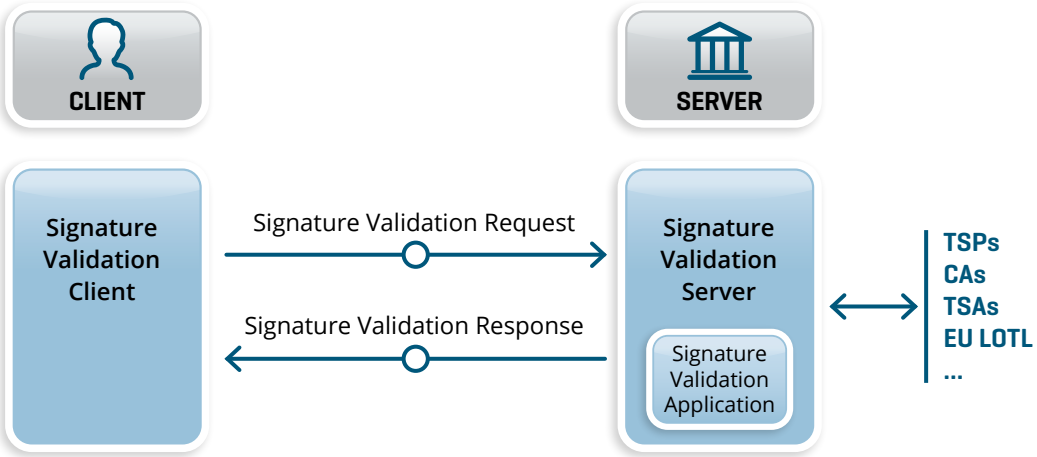

Figure 4: Signature validation process

There are several standards on signature validation available at the following location[24].

Preservation of electronic signatures/seals

Long-term preservation of electronic signatures/seals aims to ensure the legal verifiability of electronic signatures/seals over time. A preservation service for electronic signatures/seals preserves the result of a signature or seal validation, at a certain point in time, over long periods of time during which the technological state of the art might evolve.

Furthermore, if an electronic signature/seal is created by using a private key for which a certificate for electronic signatures/seals on the corresponding public key has been issued by a trust service provider, then the validity of the electronic signature/seal depends on the status of the certificate. A certificate is only valid during a limited time frame (e.g., two years) after which it will expire. During this time frame the issuing trust service provider may revoke the certificate due to some event such as the compromise of the associated private key. Hence, the validation of an electronic signature based on a certificate for electronic signatures may yield "valid" today, but may yield "invalid" at some point in the future due to the change of status of the certificate.

Electronic registered delivery services (ERDS)

According to Article 3(36) of the eIDAS Regulation, an electronic registered delivery service is *"a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations"* [11].

A Registered Electronic Mail (REM) service can be considered as a specific type of Electronic Registered Delivery service. A registered electronic mail service is defined in the ETSI Special Report 019 050 on a framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures as an "electronic registered delivery service based on electronic mail as the underlying technology" [23]. In contrast to traditional email services, registered email services provide to their users a set of evidences, which may include a proof of sending the email, a proof of delivering the email to the intended recipient, and a proof of receiving the email.

The eIDAS Regulation applies the principle of non-discrimination to data sent and received using an electronic registered delivery service. Thus, data sent and received using such a service cannot be denied legal effect and admissibility as evidence in legal proceedings on the grounds that it is in electronic form or that it does not meet

24 https://portal.etsi.org/TB-SiteMap/esi/esi-activities

the requirements for qualified electronic registered delivery services ([11], Article 43(1)). Thus, for example, a judge cannot reject an email, sent with a REM service, in a legal proceeding on the grounds that it is in electronic form; he may however reject the email on other grounds.

2.2.2. Qualified trust services

In this chapter, the different qualified trust services will be presented. In particular, the legal implications of the qualified trust services will be discussed. Furthermore, we describe incentives to the market for using qualified trust services.

The eIDAS Regulation regulates the following nine qualified trust services for which there are applicable requirements in the eIDAS Regulation:

- Provision of qualified certificates for electronic signatures;
- Provision of qualified certificates for electronic seals;
- Provision of qualified certificates for website authentication;
- Qualified electronic time stamps services;
- Qualified validation service for qualified electronic signatures;
- Qualified validation service for qualified electronic seals;
- Qualified preservation service for qualified electronic signatures;
- Qualified preservation service for qualified electronic seals; and
- Qualified electronic registered delivery services.

Note that qualified trust services can only be provided by "qualified trust service providers". According to the eIDAS Regulation, a "qualified trust service provider" is "a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body" ([11], Article 3(20)).

Provision of qualified certificates for electronic signatures

According to the eIDAS Regulation, a qualified certificate for electronic signature is a *"certificate for electronic signatures that is issued by a qualified trust service provider and meets the requirements laid down in Annex I"* ([11], Article 3(15)). Recall that certificates for electronic signatures can only be issued to natural persons.

Annex I of the eIDAS Regulation contains requirements on the certificate profile of qualified certificates for electronic signatures. In particular, they have to contain the identity of the trust service provider, the identity of the signatory (either a name or a pseudonym), a public key, and an indication that the certificate has been issued as a qualified certificate for electronic signature. The indication that the certificate has been issued as a qualified certificate for electronic signatures is commonly included in the certificate extension field "Qualified Certificate Statements" via the object identifier (OID) 0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) (QcCompliance statement) in combination with the OID 0.4.0.1862.1.6.1 (id-etsi-qct-esign) (QcType statement) [24].

Compared to non-qualified certificates for electronic signatures, qualified certificates for electronic signatures can only be issued by qualified trust service providers that have been granted the qualified status for this trust service by the national supervisory body, which is indicated on the national trusted list. Under the eIDAS Regulation, national trusted lists have a constitutive value as they present the only reliable source to verify whether a given trust service provider and its trust service have the "qualified" status. We refer the reader to Section 2.3.1. for the procedure to be followed by trust service providers established in Luxembourg who would like to offer qualified trust services.

Provision of qualified certificates for electronic seals

According to the eIDAS Regulation, a qualified certificate for electronic seal is a "certificate for an electronic seal that is issued by a qualified trust service provider and meets the requirements laid down in Annex III" ([11], Article 3(30)). Recall that certificates for electronic seals can only be issued to legal persons.

Annex III of the eIDAS Regulation contains requirements on the certificate profile of qualified certificates for electronic seals. In particular, they have to contain the identity of the trust service provider, the identity of the creator of the seal (name and registration number as stated in the official records), a public key, and an indication that the certificate has been issued as a qualified certificate for electronic seal.

Incentives for using qualified certificates for electronic seals include, for example:

- Legal and regulatory requirements: for instance, requirements in the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [25] (commonly called PSD2) and associated Regulatory Technical Standards on authentication and communication.
- Standards that require or recommend the use of qualified certificates for electronic seals.

In particular, qualified certificates for electronic seals where the private key related to the certified public key resides in a QSealCD can be used, for example, in the following cases:

- The creation of qualified electronic seals on data where high legal, financial, or strategic risks are involved.
- Legal and regulatory requirements.

Provision of qualified certificates for website authentication

According to the eIDAS Regulation, a qualified website authentication certificate (QWAC) is *"a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV"* ([11], Article 3(39)). Under the eIDAS Regulation, qualified certificates for website authentication can be issued to both natural and legal persons.

Annex IV of the eIDAS Regulation contains requirements on the certificate profile of qualified certificates for website authentication. In particular, they have to contain the identity of the trust service provider, the identity of the natural or legal person to whom the certificate is issued, an indication that the certificate has been issued as a qualified certificate for website authentication, and the domain name(s) operated by the person to whom the certificate is issued.

Incentives for using qualified certificates for website authentication include, for example:

- Legal and regulatory requirements: for instance, requirements in the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [25] (commonly called PSD2) and associated Regulatory Technical Standards on authentication and communication.
- The appearance of a special symbol in the address bar of widely-used web browsers that clearly indicates that the certificate used by the visited website is a qualified certificate for website authentication.
- Standards that require or recommend the use of qualified certificates for website authentication.

The availability and use of browser plugins that enable the visitor of a website to detect whether the website uses a qualified certificate for website authentication (that would otherwise require the manual inspection of the certificate) might also become an incentive for using qualified certificates for website authentication.

Qualified electronic time stamp services

Article 42(1) of the eIDAS Regulation specifies the requirements for a time stamp to be considered as a qualified electronic time stamp: *"A qualified electronic time stamp shall meet the following requirements: (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; (b) it is based on an accurate time source linked to Coordinated Universal Time; and (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method"* [11].

The requirements above can be met by a timestamping service offered by a qualified trust service provider (QTSP), where the time stamps contain a digital signature of a Time Stamping Authority managed by the QTSP.

The legal effects of qualified electronic time stamps are that:

- they enjoy the presumption of accuracy of the date and the time they indicate and integrity of the data to which the date and time are bound ([11], Article 41(2)), and that
- they are recognized as qualified electronic time stamps in all EU Member States, even though they are issued in one Member State ([11], Article 41(3)).

Incentives for using qualified time stamping services include, for example:

- The creation of qualified electronic time stamps on data where high legal, financial, or strategic risks are involved with regards to the existence of that data at some particular point in time (e.g., transactions, trade secrets, inventions).
- The creation of qualified electronic time stamps on data for which cross-border recognition of the time stamps in other EU Member States is relevant.

Qualified validation service for qualified electronic signatures or seals

The objective of a validation service for qualified electronic signatures/seals is to confirm or deny that a given electronic signature/seal on data was a qualified electronic signature/seal on that data at the time of signing.

Incentives for using a qualified validation service for qualified electronic signatures or seals include, for example:

- The validation of qualified electronic signatures/seals by lawyers, notaries, judges, or insurance companies to verify whether or not a given signature/seal is a valid qualified electronic signature/seal on a specific electronic document.
- Legal and regulatory requirements.

Qualified preservation service for qualified electronic signatures or seals

Article 34(1) of the eIDAS Regulation specifies the requirements for qualified preservation services for qualified electronic signatures: *"A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period"* [11]. Similar requirements also hold for qualified preservation services for qualified electronic seals ([11], Article 40).

Incentives for using a qualified preservation service for qualified electronic signatures or seals include, for example:

- The preservation of signed or sealed electronic documents (e.g., contracts, agreements) where high legal or financial risks are involved.
- Legal and regulatory requirements.

Qualified electronic registered delivery services

According to Article 3(37) of the eIDAS Regulation, a qualified electronic registered delivery service is *"an electronic registered delivery service which meets the requirements laid down in Article 44"* [11].

Legal effects of a qualified electronic registered delivery service. The principle of non-discrimination of data sent and received using an electronic registered delivery service as evidence in legal proceedings also applies to data sent and received using a qualified electronic registered delivery services. Compared to non-qualified electronic registered delivery services, data sent and received using a qualified electronic registered delivery service enjoys "the presumption of:

- the integrity of the data,
- the sending of that data by the identified sender,
- its receipt by the identified addressee and
- the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service" ([11], Article 43(2)).

The eIDAS Regulation does not define an equivalence between qualified electronic registered delivery services and registered postal mail. However, Member States can establish this equivalence at the national level.

Incentives for using a qualified electronic registered delivery service or a qualified registered electronic mail service include, for example:

- E-government and administrative simplification: Qualified electronic registered delivery services could be used by citizens and companies to interact with public administrations.
- Legal and regulatory requirements.

2.2.3. Remote signing services

A remote signature service allows users to create remote electronic signatures, where the private signature keys of the users as well as the signature creation device are managed by a trust service provider on behalf of the signatory.

The eIDAS Regulation allows the creation of remote advanced and qualified electronic signatures.

Hence, under the eIDAS Regulation, qualified trust service providers can provide remote signing services to create qualified electronic signatures as long as the qualified trust service provider and the associated qualified trust service (namely, the provision of qualified certificates for electronic signatures) meet the applicable requirements in the eIDAS Regulation.

Remote qualified electronic signatures

Description of a remote signature creation process. Prior to using the remote signing service, the user needs to request a qualified certificate for electronic signature from the qualified trust service provider (QTSP). The QTSP generates a new private/public key pair (sk, pk) for the user and creates a qualified certificate for electronic signature which binds the user's identity to the public key pk. The user's private key (sk) and the associated certificate are stored and managed by the QTSP on behalf of the user.

Qualified trust service providers who issue qualified certificates for electronic signature in the case where the electronic signature creation data (that is, private keys) are managed by the qualified trust service provider on behalf of the signatory have to meet the following requirements:

- The QTSP complies with the applicable requirements of the eIDAS Regulation.
- The conformity of the qualified electronic signature creation device shall be certified in accordance with Article 30 of the eIDAS Regulation.
- The QTSP implements the qualified electronic signature creation device in accordance with the conditions of use specified in the Certificate of Conformity of the qualified signature creation device and in the corresponding certification report.
- The QTSP maintains an up-to-date risk analysis that covers the risks associated with the use of the qualified electronic signature creation device.

There are several standards and technical specifications on remote signing services. They are available at the following location[25].

Relation between remote signing services and qualified trust services

First, only qualified trust service providers can offer remote signing services to create remote qualified electronic signatures where the management, including the generation and storage, of the user's private key is done by the qualified trust service provider ([11], Annex II(3)).

Second, the associated qualified trust service to remote signing services to create qualified electronic signatures is the "provision of qualified certificates for electronic signatures". The creation of qualified electronic signatures via a remote signing service is not a qualified trust service.

25 https://portal.etsi.org/TB-SiteMap/esi/esi-activities

The indication that a qualified trust service provider who provides the service "provision of qualified certificates for electronic signatures" (service type = "CA/QC") and manages the private keys on behalf of the users is done in the trusted list via the qualifier "QCQSCDManagedOnBehalf"[26] [26], which indicates that the private keys associated with the certificates that are issued under this service are residing in a QSigCD "for which the generation and management of that private key is done by the qualified TSP on behalf of the entity whose identity is certified in the certificate" [26].

26 http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf

2.3. ILNAS Supervision Scheme for qualified trust service providers

In this section, we describe the supervision scheme of ILNAS for qualified trust service providers. In particular, the relationship between the different actors in the supervision scheme will be explained.

Figure 5 shows the supervision scheme for qualified trust service providers applied by the ILNAS Digital Trust Department. The supervision scheme relies on the following actors:

- The national accreditation body of a Member state (e.g., the *Office Luxembourgeois d'Accréditation et de Surveillance* (OLAS)[27] in Luxembourg, or the *Comité français d'accréditation* (COFRAC) in France) that has signed the European cooperation for Accreditation multilateral agreement (EA MLA), accredits the competence of conformity assessment bodies to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides against the requirements of the eIDAS Regulation[28].

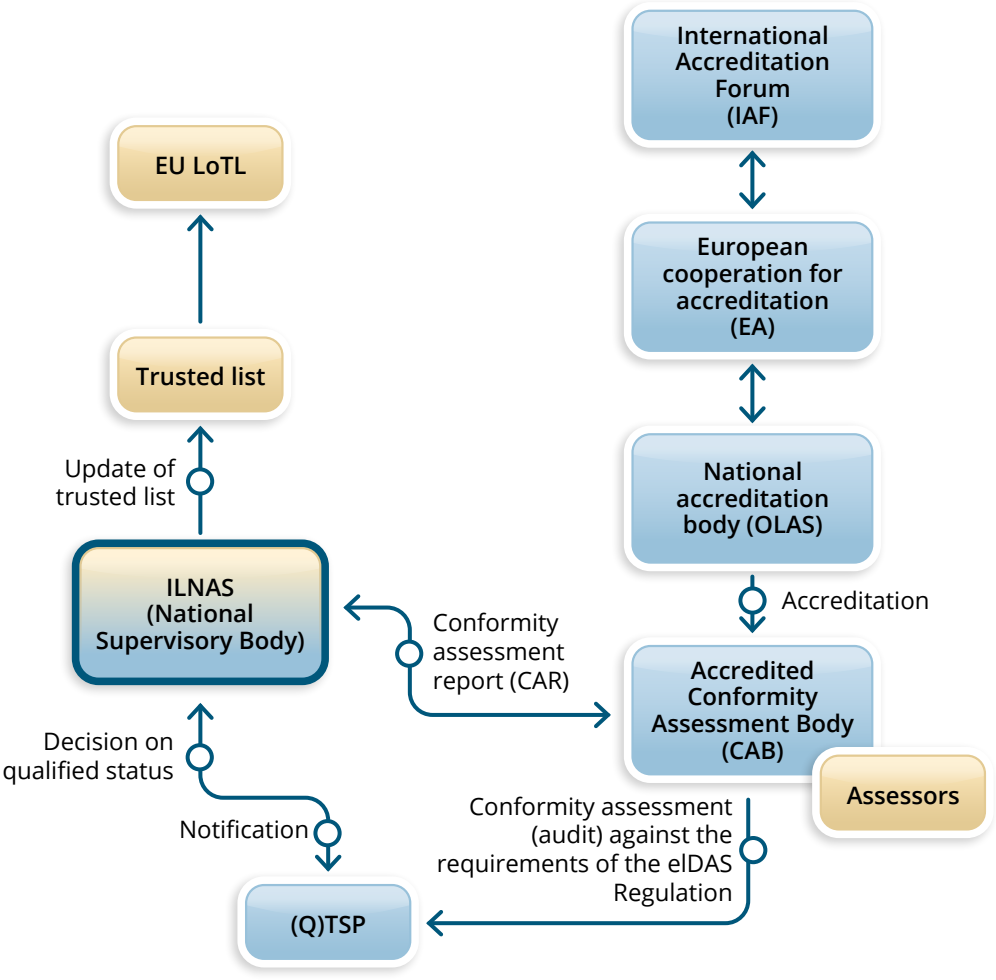

Figure 5: National supervision scheme

27 https://portail-qualite.public.lu/fr/acteurs/ilnas/olas.html

28 Note that the national accreditation body in Luxembourg (OLAS) does not perform accreditation regarding the conformity assessment activities related to the eIDAS Regulation.

- A conformity assessment body (CAB) is *"a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides"* ([11], Article 3(18)). Recall that Regulation (EC) No 765/2008 defines a conformity assessment body as a *"body that performs conformity assessment activities including calibration, testing, certification and inspection"*. ILNAS requires that the conformity assessment body is accredited by the national accreditation body of a Member state in accordance with Article 3(18) of the eIDAS Regulation [11] and recommends that the conformity assessment body is also accredited according to the requirements of the ISO standard ISO/IEC 17065:2012 [27] as well as those in ETSI EN 319 403-1 [28].
- The Digital Trust Department of ILNAS is the supervisory body in Luxembourg, responsible for the supervision of trust service providers, and is also the body responsible for establishing, maintaining and publishing the national trusted list [20].
- A trust service provider, without qualified status, who intends to start providing qualified trust services, has to submit to the Digital Trust Department of ILNAS a notification of its intention together with a conformity assessment report issued by a conformity assessment body. Further details on the initiation process of a qualified trust service are given in Section 2.3.1.

The national trusted list is a list which includes information about the qualified trust service providers established in Luxembourg and supervised by ILNAS as well as information about the qualified trust services they provide.

2.3.1. Initiation of the Supervision

A trust service provider established in Luxembourg, without qualified status, who intends to start providing qualified trust services, has to submit to the Digital Trust Department of ILNAS a notification of its intention together with a conformity assessment report issued by a conformity assessment body. The notification has to include the completed notification form as well as several documents such as the trust service policies that apply to the trust services for which a qualified status is requested, the termination plan of the TSP and the certificate from the conformity assessment body that demonstrates compliance with the applicable requirements of the eIDAS Regulation. For further details, we refer the reader to the ILNAS procedure for the supervision of QTSPs [29].

If the applicable requirements in the eIDAS Regulation are met by the TSP and the notified trust services, then the qualified status is granted to the TSP and the notified trust services are included in the national trusted list.

If the applicable requirements in the eIDAS Regulation are not met by the TSP or the qualified trust services it intends to provide and if the QTSP fails to resolve non-conformities as requested by the Digital Trust Department of ILNAS, then ILNAS does not grant the qualified status to the TSP. In this case the TSP needs to start the supervision process again via a new notification to the Digital Trust Department of ILNAS.

It is important to note that, according to Article 21 paragraph (3) of the eIDAS Regulation, qualified trust service providers may only start to provide the trust service for which the qualified status has been requested in the notification after the qualified status has been indicated in the national trusted list.

2.3.2. During the Supervision

The supervision shall ensure that the QTSP and its qualified trust services meet the applicable requirements laid down in the eIDAS Regulation. In this regard the certification shall be renewed every two years (via a reassessment audit) and a surveillance audit shall be conducted yearly. Furthermore, an Electronic Data Processing (EDP) audit shall be conducted every two years. ILNAS recommends to conduct the EDP audit with respect to the requirements in the technical specification CEN/TS 419 261:2015 "Security requirements for trustworthy systems managing certificates and time-stamps" [30].

During the supervision phase, the Digital Trust Department of ILNAS organizes a supervision meeting with each QTSP at least every 6 months, which allows the department to review the recent activities of the QTSP. In particular, the QTSPs that are supervised by ILNAS shall inform ILNAS of any change in the provision of its qualified trust services (e.g., change of subcontractor, change of hardware/software, change of algorithms, intention to cease activities).

According to Article 19 paragraph (2) of the eIDAS Regulation, qualified trust service providers shall, *"without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein."*

The standards and technical specification in the scope of the TSP activity are available at the following location[29].

In certain cases, the QTSP also has to notify the customers who are affected by the breach of security or loss of integrity without undue delay.

Besides the yearly surveillance audit and the two-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 such ad hoc audits is to confirm that the qualified trust service provider and its qualified trust services fulfill the requirements laid down in this eIDAS Regulation. Ad hoc audits can be triggered by the occurrence of events such as:

- Events detected by ILNAS; or
- Events notified by the QTSP to 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 but under significantly different policies;
  - Security incidents;
  - Personal data breaches; and
  - Complaints.

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

29 https://portal.etsi.org/TB-SiteMap/esi/esi-activities

2.3.3. Termination of the Supervision

The QTSP has to inform ILNAS of its intention to cease one or more of its qualified trust services. In this case, the Digital Trust Department of ILNAS verifies the correct application of the provisions contained in the trust service provider's termination plan, including as to how information is kept accessible in accordance with point (h) of Article 24 paragraph (2) of the eIDAS Regulation. This verification is necessary to maintain the trust and confidence of the affected users in the continuity of the qualified trust services (e.g., the availability of the certificate revocation list) as well as for the purpose of providing evidence in legal proceedings.

In case of the cessation of some of the qualified trust service provider's qualified trust services, the scope of the supervision by ILNAS changes and the status of the concerned qualified trust services on the national trusted list is updated by ILNAS.

In case of the cessation of all of the qualified trust service provider's qualified trust services, the supervision by ILNAS according to the ILNAS supervision procedure for QTSPs ceases and the status of the trust service provider and of the trust services on the national trusted list is updated by ILNAS.

2.4. Trusted lists

"Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision." ([11], *Recital (46)*).

Each EU Member State manages a national trusted list which contains information about the qualified trust service providers under its supervision and their qualified trust services. Details on national trusted lists are provided in Section 2.4.1. The national trusted lists contain a pointer to the European List of Trusted Lists (LOTL) which is managed by the European Commission. We provide information on the LOTL and the Trusted List Browser in Section 2.4.2.

2.4.1. National trusted list

The eIDAS Regulation requires EU Member States to establish, maintain and publish trusted lists, which include information about the qualified trust service providers supervised by the supervisory body of the Member State as well as information about the qualified trust services that they provide. Trusted lists not only contain information on currently active qualified trust service providers and the qualified trust services that they currently provide, but also historical information on the trust services that they provide (or that they provided in the past) such as their prior statuses. The lists also include information on trust service providers that have been supervised by the supervisory body in the past as well as information on the trust services that they provided.

Each national trusted list is digitally signed by the Trusted List Scheme Operator (TLSO), the legal entity in charge of managing the trusted list, to ensure origin authentication of the trusted list. Thus, users are able to verify that a given trusted list was indeed issued by a certain entity.

Under the eIDAS Regulation, national trusted lists have a constitutive value as they present the only reliable source to verify whether a given trust service provider and its trust service had the "qualified" status at a given point in time. A necessary condition for a qualified trust service to benefit from the legal effects associated to it is that the trust service has the "qualified" status in the national trusted list.

As indicated before, trusted lists are mainly used to validate objects (e.g., qualified electronic signatures or qualified timestamps) that have been created by using a qualified trust service. For example, to verify that an electronic signature on a document, created with a public-key certificate, can be considered as a "qualified electronic signature" in the sense of the eIDAS Regulation, one would need to first verify that:

- Qualified status check: the trust service under which the certificate was issued had the "qualified" status in the trusted list at the time when the signature was created[30].

Additional checks include:

- **Suspension and revocation check**: the verification whether the certificate was neither suspended nor revoked at the time of the signature (Certificate Revocation List (CRL) distribution points are included in the certificate),
- **Expiration check**: the verification whether the certificate was not expired at the time of the signature (the expiration date of the certificate is included in the certificate),
- **Cryptographic verification of the digital signature**: the cryptographic verification whether the digital signature is a valid signature on the document, and
- **QSigCD check**: the verification whether the private key corresponding to the certified public key resided in a qualified signature creation device (this information may be included in the trusted list or in the certificate).

30 If PKI technology is used, then a trust service is identified on the trusted list via an X.509 certificate in the "Service Digital Identity" field

The trusted list of Luxembourg includes information about the qualified trust service providers established in Luxembourg and supervised by ILNAS as well as information about the qualified trust services they provide.
The Digital Trust Department of ILNAS is Luxembourg's Trusted List Scheme Operator, responsible for maintaining and publishing Luxembourg's trusted list. It is available in three formats HTML, XML, and PDF, and can be accessed on the ILNAS website[31].

Figure 6 shows an extract of the Trusted List Luxembourg when accessed via the Trusted List Browser, a web application made available by the European Commission (see also Section 2.4.2.).

As shown in Figure 6, at the time of writing, LuxTrust S.A. and BE INVEST International S.A. are the only active qualified trust service provider in Luxembourg providing qualified trust services (indicated in yellow in Figure 6):

- Qualified certificate for electronic signature;
- Qualified certificate for electronic seal;
- Qualified validation service for qualified electronic signature;
- Qualified validation service for qualified electronic seal;
- Qualified electronic registered delivery service;
- Qualified time stamp; and
- Qualified certificate for website authentication.

The trusted list not only contains information on currently active qualified trust service providers supervised by ILNAS and the qualified trust services that they currently offer, but also historical information on trust service providers that have been supervised by ILNAS in the past.

The trusted list also contains a link to the European List of Trusted Lists (in XML format), information on the trusted list itself such as the date and time when it was issued, the date and time by which an updated trusted list will be issued, as well as a digital signature by the head of the Digital Trust Department of the ILNAS.

Trusted lists have to comply with the technical specifications given in Annex I of the Commission Implementing Decision (EU) 2015/1505 [31]. These technical specifications rely on the requirements in the ETSI Technical Specification 119 612 [26]. Due to the constitutive value of the trusted lists on which users and applications rely to verify the status of trust services, the trusted lists have to be highly available. More precisely, national trusted lists have to be available 24 hours a day and 7 days a week with a minimum availability of 99,9% over one year, as required by Clause 6.4 of the ETSI Technical Specification 119 612 [26] which is referenced in the Commission Implementing Decision (EU) 2015/1505 [31].

31 https://portail-qualite.public.lu/fr/confiance-numerique/prestataires-services-confiance/liste-confiance.html

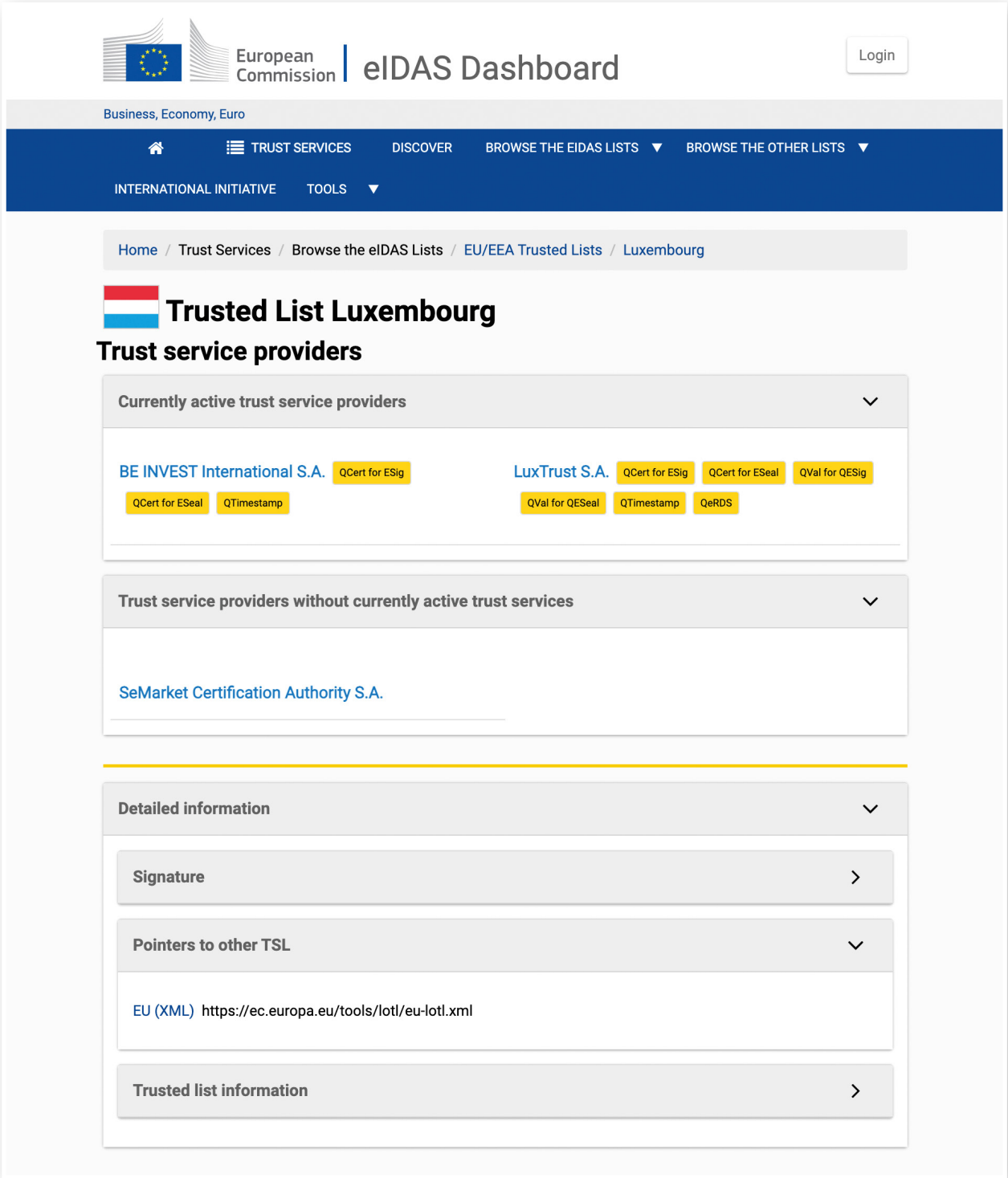

Figure 6: The Luxembourg trusted list

2.4.2. European List of Trusted Lists (LOTL)

According to Article 22 paragraph (4) of the eIDAS Regulation the European Commission makes available information to the public about national trusted lists published by the EU Member States. This information is included in a list, called the European List of Trusted Lists (LOTL).

In particular, the LOTL contains pointers to the locations where the national trusted lists of the EU Member States are published. It is available in a machine-readable format (XML) on the website of the European Commission[32].

Figure 7: The trusted list browser (https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home)

In 2017, the European Commission launched the Trusted List Browser [32]. The trusted list browser is a user-friendly web application (see Figure 7) that allows users to browse national trusted lists and verify the status of trust services offered by trust service providers established in the European Union or in Norway, Liechtenstein, or Iceland. In particular, users can verify whether a specific trust service offered by some trust service provider had the qualified status at a given point in time.

32 https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

2.5. The revision of the eIDAS Regulation (eIDAS2)

In June 2021, the Commission proposed a framework for a European digital identity that would be available to all EU citizens, residents and businesses, via a European digital identity wallet.

In December 2022, the Council adopted its common position ("general approach") on the proposal for a regulation on a European digital identity framework ("proposal for an eIDAS2 regulation") amending Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions within the internal market and repealing Directive 1999/93/EC (eIDAS Regulation) [12].

The main objective of the proposed regulation is to introduce the European digital identity wallet which would allow citizens of the European Union to identify themselves to public or private services online, through for example their mobile phone.

The eIDAS2 draft regulation also covers several new trust services, such as electronic archiving of digital documents, recording of electronic data in electronic registers, issuance of electronic attestations of attributes and the management of remote signature and electronic seal creation devices.

The general approach of the Council has also retained the provision of Article 45 paragraph 2 which requires internet browsers to recognize qualified website authentication certificates. This provision is viewed critically by internet browsers due to the different functioning of the trust schemes applied.

The adoption of the general approach will allow the Council to enter negotiations with the European Parliament ('trilogues') once the latter adopts its own position with a view to reaching an agreement on the proposed regulation.

The main objective of the proposed regulation requires member states to issue a digital wallet under a notified eID scheme, built on common technical standards, following compulsory certification. To set up the necessary technical architecture, speed up the implementation of the revised regulation, provide guidelines to member states and avoid fragmentation, the proposal was accompanied by a recommendation for the development of a Union toolbox defining the technical specifications of the wallet.

The European digital identity wallet. One of the main policy objectives of the proposal is to provide citizens and other residents, as defined by national law, with a harmonised European digital identity means based on the concept of a European digital identity wallet.

As an electronic identification means ('eID means') issued under national schemes at assurance level 'high', the Wallet would be an eID means in its own right based on the issuing of personal identification data and the wallet by member states. The text of the Council's general approach therefore further develops the concept of the wallet and its interplay with national electronic identification means.

Assurance levels. Assurance levels should characterise the degree of confidence in the electronic identification means, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity is assigned. In this respect, the wallet must be issued within an electronic identification system meeting the assurance level 'high'.

Furthermore, a specific provision on the on-boarding of users has been added to address the concerns of member states where a significant number of national eID means at assurance level 'substantial' has already been issued.

The provision enables a user to use their national eID means in conjunction with additional remote on-boarding procedures to make identity proofing at assurance level 'high' possible and, ultimately, to obtain a wallet.

Since the draft eID regulation relies on cybersecurity certifications schemes that should bring a harmonised level of trust in the security of wallets, the secure storage of cryptographic material is expected to become subject to cybersecurity certification as well.

The text therefore contains a new recital addressing these technical preconditions of achieving of assurance level 'high' and enabling a follow-up process within the implementation of European digital identity wallets.

Notification of relying parties. The part of the proposal on the notification of relying parties has been rephrased. As a rule, the notification process by means of which the relying party communicates its intent to rely on the wallet should be cost-effective, proportionate-to-risk and ensure that the relying party provides at least the information necessary to authenticate to the wallet.

By default, only minimum information is required, and the notification should allow for the use of automated or simple self-reporting procedures.

A specific regime may, however, be necessary due to sectoral requirements, such as those applicable to the processing of special categories of personal data. A provision has therefore been introduced aiming to cover cases where a more stringent registration or authorization procedure is required.

Conversely, where Union or national law does not lay down specific requirements to access information provided by means of the wallet, member states may exempt such relying parties from the obligation to notify their intent to rely on wallets.

Certification. The regulation should leverage, rely on, and mandate the use of relevant future or existing Cybersecurity Act (see Chapter 4 for more information on the Cybersecurity Act) certification schemes, or parts thereof, to certify the compliance of wallets, or parts thereof, with the applicable cybersecurity requirements.

Consequently, the Cybersecurity Act framework applies fully, including the peer review mechanism between national cybersecurity certification authorities provided within the Cybersecurity Act.

To align the eID regulation and the Cybersecurity Act to the extent possible, member states will designate public and private bodies accredited to certify the wallet in accordance with the Cybersecurity Act's relevant certification schemes.

Implementing period for the provision of the wallet and fees. Based on guidance by member states, the Council's text proposes that the implementing period of 24 months be counted from the adoption of the implementing acts.

The text also clarifies that the issuance, use for authentication, and revocation of wallets should be free of charge to natural persons.

Access to hardware and software features. The text provides for explicit articulation with existing legislation, which ensures access to hardware and software features as part of core platform services provided by gatekeepers.

A newly added provision clarifies that providers of wallets and issuers of notified electronic identification means acting in a commercial or professional capacity are business users of gatekeepers within the meaning of the definition in the Digital Markets Act (DMA, [33]).

Wording has been also added to outline the implication of the interlink with the DMA, namely that gatekeepers should be required to ensure, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features that are available or used in the provision of its own complementary and supporting services.

Alternate possibilities to issue electronic attestation of attributes by public bodies. The issuance of qualified electronic attestation of attributes by qualified providers has been retained, including the obligation for member states to ensure that attributes can be verified against an authentic source within the public sector.

In addition, a possibility has been introduced that electronic attestation of attributes with the same legal effects as qualified electronic attestation of attributes be issued to the wallet directly by the public sector body responsible for the authentic source or by designated public sector body on behalf of a public sector body responsible for an authentic source, provided that the necessary requirements are met.

Record matching. Regarding record matching, the concept of unique and persistent identifier has been retained for Wallets. The relevant definition clarifies that the identifier may consist of a combination of several national and sectoral identifiers if it serves its purpose.

It is explicitly stated that record matching may be facilitated by qualified electronic attestation of attributes. Furthermore, a safeguarding provision has been added, under which member states must ensure the protection of personal data and prevent the profiling of users. Lastly, member states, in their capacity as relying parties, must ensure record matching.

3

E-archiving and dematerialization

3. E-archiving and dematerialization

After having explored trust services fundamentally based on digital signatures, we now turn to another type of trust-providing service: that of electronic archiving.

Traditionally, the archiving of physical documents, such as paper documents, involves storing documents for a long period of time while ensuring their integrity during that time, i.e. archived documents should not be lost, damaged, or destroyed. Often it is also important to protect the confidentiality of the documents that were archived. As archiving can be costly, business organizations typically only archive documents that are valuable to them and essential to their business interests, or documents that have to be archived because of legal requirements. Documents that are archived may hence possess a legal value. For instance, an insurance company might archive insurance contracts signed by customers to keep physical and legal proof that customers have entered into a contractual relationship with the company.

The aim of electronic archiving is to transpose the concept of long-term document storage to the digital world. Digital documents can be ultimately seen as sequences of bits, i.e. sequences of the values 0 or 1, which can be easily duplicated. Moreover, unlike paper documents, the copies of digital documents are indistinguishable from the originals. In that way, digital documents can be easily protected against destruction by storing multiple copies of the documents at different locations, for instance. On the other side, paper documents can be copied as well, but typically only the original document is fully recognized in legal settings. The manipulation of digital documents can also present its own challenges: ensuring the long-term readability and confidentiality of digital documents may be harder to achieve than for paper documents. For example, in the world of information technology, formats used for storing data, or even the technologies used for physical data storage, may evolve very fast and they can become obsolete in a matter of years (e.g. floppy disks). One particular challenge is therefore to ensure that data stored in a specific format on some data storage device can still be read in ten or twenty years' time. Electronic archiving services therefore also have to incorporate solutions for guaranteeing the long-term readability and confidentiality of digital documents.

Despite these challenges, the lower storage & handling costs and physical space requirements of electronic archives, as well as the possibility of providing additional electronic processing, has sparked the interest in electronic archiving solutions. One aspect that had still been missing for allowing electronic archiving to replace traditional archiving is the recognition of the legal value of digital archives. In the Law of 25 July 2015 on electronic archiving [18], the Grand Duchy of Luxembourg was one of the first countries to define the conditions under which the conformity of electronic archives with the original digital documents is legally recognized. However, the Law on electronic archiving does not stop there: it also introduces the legal conditions under which a digitized version of an analog document, e.g., a scan of a paper document, is considered to have the same probative value as the original document. The Law on electronic archiving in the Grand Duchy of Luxembourg therefore establishes all the required components for replacing traditional archiving with its electronic counterpart. In particular, it even permits paper documents to be destroyed after digitization without losing the legal value that the paper documents offered.

However, for a digitized copy to benefit from the same probative value as the original analog document, or a digital archive with respect to the original digital document, it must have been created by an organization or service provider that has been given the legal status of *prestataire de services de dématérialisation ou de conservation* (PSDC), i.e. "provider of digitization or e-archiving services" in English.

ILNAS is the sole government agency in the Grand Duchy of Luxembourg authorized to grant the status of PSDC. Organizations that want to obtain the PSDC status need to fulfill a certain number of conditions. For instance, they must be certified with respect to the national standard ILNAS 106 *Archivage électronique - Référentiel d'exigences*

pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC). At the time of writing, the 2022 edition of ILNAS 106 is applicable for obtaining the status of PSDC [34]. ILNAS 106:2022 is written as a sector-specific application of the international standards ISO/IEC 27001 and ISO/IEC 27002 concerning information security to digitization or e-archiving services. ILNAS 106:2022 also builds upon the international standard ISO 14641 relating to electronic archiving systems.

The Digital Trust Department of ILNAS is Luxembourg's supervisory body for providers of digitization or electronic archiving services according to the Law of 25 July 2015 on electronic archiving that are established in Luxembourg. The legal missions of the Digital Trust Department of ILNAS are described in [20].

In the following sections, we provide an overview of the e-archiving framework that has been created in the Grand Duchy of Luxembourg with the aims of

1) providing an introduction to the topic for readers who are unfamiliar with the legal context relating to e-archiving in Luxembourg, and
2) giving guidance to organizations that plan to provide digitization or e-archiving services.

We also introduce the procedure that is applied by the Digital Trust Department of ILNAS for the supervision of organizations that have obtained the PSDC status.

3.1. The Electronic Archiving Framework in Luxembourg

The Law of 25 July 2015 on electronic archiving Luxembourg covers the following two aspects:

- digitization of analog documents, and
- archiving of digital documents.

A document is said to be "digital" if it consists of a sequence of bits and it can only be visualized or manipulated with the help of information processing equipment (e.g. laptops, desktop computers, servers, or smartphones). In the following, "electronic documents" is used as a synonym for "digital documents". On the other hand, "analog documents" are documents that are not digital, i.e. documents that are bound to physical objects such as paper, microfilm, photographic film, vinyl records, etc.

"Digitization of analog documents" refers to transforming analog documents into identical reproductions in the form of digital documents. Typically, paper documents are digitized with the help of scanners.

The aim of "archiving digital documents" is to preserve certain properties of digital documents, such as their integrity or confidentiality, over extended periods of time.

The Law of 25 July 2015 on electronic archiving [18] (in the following also simply referred to as "Law on electronic archiving") introduces the conditions under which digital documents benefit from a presumption of conformity with respect to the respective original documents, i.e. the conditions

1) under which the digitized (digital) version of an analog document has the same probative value as its analog version, and
2) under which the probative value of an archived digital document is maintained over time with respect to the digital document that was entered into the archiving process.

Informally, a document has probative value if it provides sufficient evidence to prove a disputed point in a trial.[33] Note that the process of archiving cannot modify the legal value of the document that was originally archived. For instance, if a digital document is a digital reproduction of a paper document that does not enjoy the same probative value as the original paper document, then the archiving of such a digital document only maintains the probative value with respect to the digital document that was archived and not with respect to the original paper document.

In the following we use the term "copy with probative value" to denote a copy that is assumed to have the same probative value as the original.

One can argue that the revolutionary aspect of the e-archiving framework in the Grand Duchy of Luxembourg concerns the digitization of analog documents as it opens up numerous possibilities for providing additional services that are difficult to implement for analog documents. Moreover, the digitization of analog documents may help to reduce operational costs. For instance, the digitization of documents can bring the following advantages.

- As digitized documents may benefit from the same probative value as the original analog documents, it becomes unnecessary to store the original analog documents. Consequently, large, physical archives for storing the analog documents and the associated manipulations of such archives are no longer needed.
- Using digital documents also mitigates several threats that affect analog documents. If only the original analog document has a certain legal value, then it becomes even more important to protect its integrity. Threats such as fire or theft may lead to grave consequences when the only document that possesses a legal

33 See also, e.g., https://www.law.cornell.edu/wex/probative_value.

value is no longer available. As digital documents can be easily duplicated, an organization can protect itself against the loss of important documents by storing them redundantly (in multiple locations).

- Another important advantage of digital documents is that they can be easily accessed and examined. Instead of having to search through a large physical archive, digital documents can be accessed instantaneously in databases or file stores, even from remote locations.
- The process of searching through documents can also be accelerated if the documents are in digital form. For instance, by indexing keywords in digital documents, it becomes possible to quickly find all the documents in which certain keywords appear. For analog documents that were digitized, one can first extract the keywords through an optical character recognition (OCR) process.

The Law of 25 July 2015 on electronic archiving introduces the main legal context regarding digitization and electronic archiving in the Grand Duchy of Luxembourg. The technical conditions that govern the provision of digitization and electronic archiving services are defined in the national standard ILNAS 106:2022 *Archivage électronique - Référentiel d'exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC)* [34].

One aim of the legal context concerning digitization and electronic archiving in Luxembourg is to reverse the burden of proof. If an analog document has been digitized and archived according to the Law of 25 July 2015 on electronic archiving, then the digital document is presumed to have the same legal value as the original analog document by default. To contest the legal equivalence of the digital document, one would have to prove that some of the requirements of the Law of 25 July 2015 on electronic archiving were not followed during the digitization or archiving step.

We have to point out that the legal context concerning digitization does not apply to every type of analog document, but only to "private deeds" or to the types of documents referred to in Article 16 of the "Code de commerce" (see also Section 3.2). Regarding the archiving of digital documents, the Law of 25 July 2015 on electronic archiving is applicable to any private deed in electronic form and to any document that was originally created in electronic form.

The Law of 25 July 2015 on electronic archiving introduces the legal status of

prestataire de services de dématérialisation ou de conservation,

or **PSDC**, i.e. "digitization or e-archiving service provider" in English. Although the Law on electronic archiving permits any legal person to obtain the PSDC status, we simply refer to "organizations" instead of "legal persons" in the following to simplify the presentation. Legal persons can be individuals, companies, government agencies, etc.

ILNAS is the sole government agency in the Grand Duchy of Luxembourg authorized to grant the status of PSDC to organizations. To that end, organizations need to fulfill a certain number of conditions. For instance, they must be certified with respect to the national standard ILNAS 106:2022 by a certification body that is accredited according to the international standards

- ISO/IEC 17021-1:2015 "Requirements for bodies providing audit and certification of management systems" [35][34] and
- ISO/IEC 27006:2015 "Requirements for bodies providing audit and certification of information security management systems" [36].

Only documents that have been digitized or archived by PSDCs according to the policies, processes, and procedures that were certified in the electronic archiving context will be deemed to have the same probative value as the corresponding original documents.

34 All standards referenced in this document can be purchased from the ILNAS eShop, which can be accessed at https://ilnas.services-publics.lu/ecnor/home.action.

In the following we describe the digitization and electronic archiving workflows that the Law of 25 July 2015 on electronic archiving considers. Figure 8 illustrates the typical workflow for the digitization of analog documents.

- **Pickup or delivery of analog documents**: the first step consists in making the analog documents that should be digitized available to the organization that performs the digitization. To that end, the analog documents are either picked up by the organization itself or the client delivers them to the organization. Typically, after delivery or pickup, the analog documents are stored in a secure temporary storage site under the organization's responsibility until the digitization of the analog documents can begin.

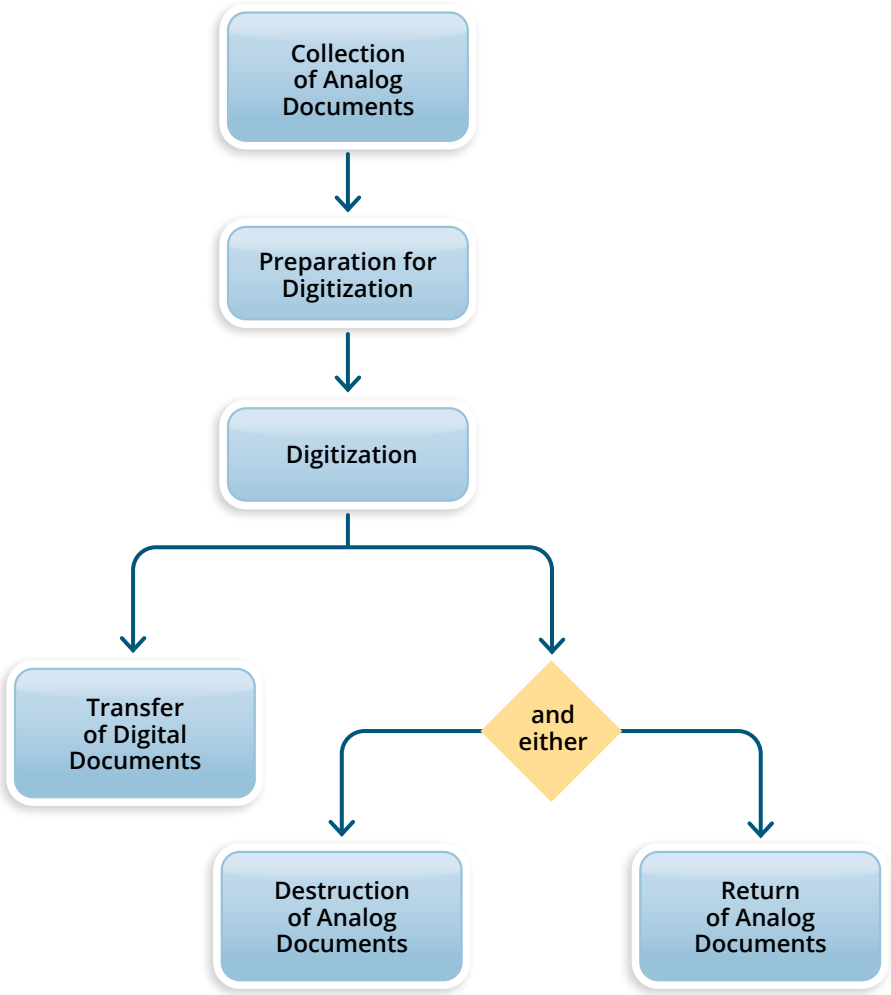

Figure 8: Typical workflow of digitization

- **Creation and temporary storage of digital documents**: in the next step, the analog documents are prepared for scanning (by aligning stacks of papers or by removing staples, for instance). Subsequently, the scanning takes place and digital documents are created out of the analog documents. Digitization metadata are associated with the digitized documents, and the digitized documents are temporarily stored in a secure file store. The metadata typically contain information about the scanner settings, such as the number of colors or the scanning resolution, but also information for protecting the integrity of documents, such as their cryptographic hash values.
- **Temporary storage of analog documents**: after the digitization, the analog documents are stored in a secure storage site under the organization's responsibility until either the analog documents can be returned to the client, or they can be destroyed.

Transfer and return of documents: the last step consists in transferring the digital documents (with associated metadata) to the electronic archiving system or to the client, which can be done in the form of an electronic file transfer or through a physical transport of storage media. Regarding the analog documents, there are two options:

- they can be returned to the client, either through a delivery set up by the organization, or through a pickup organized by the client; or
- the analog documents are destroyed by the organization.

In the last step, the organization deletes the digital documents and associated metadata, unless the organization also proceeds with archiving the digital documents.

Figure 9 depicts the typical workflow of electronic archiving.

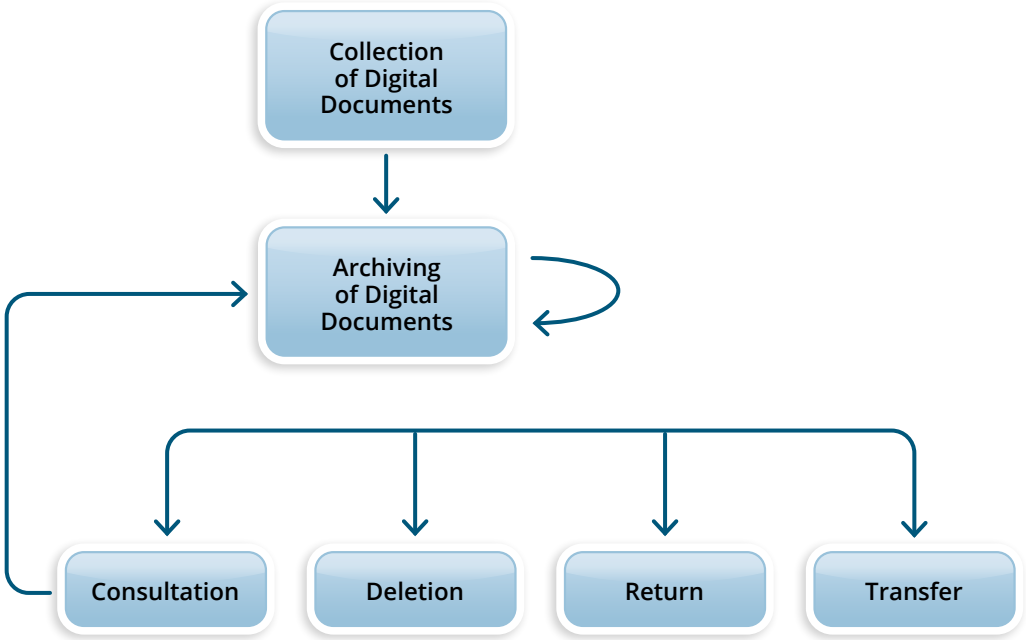

Figure 9: Typical workflow of electronic archiving

- **Collection of digital documents**: the digital documents that should be archived are made available to the organization that carries out the electronic archiving, either through electronic file transfer or through physical transport (or pickup) of storage media,
- **Creation of digital archives**: the documents are prepared for archiving, and they are then injected into the electronic archiving system, where the digital documents are converted into digital archives and archival metadata are associated with the digital archives. The archival metadata may contain information necessary for ensuring the integrity of the digital archives, such as cryptographic hash values. Additionally, the details of every manipulation that concerns a digital archive may be recorded in the archival metadata. The conversion into digital archives may be accompanied by a file format conversion. Once the correct submission of the digital documents into the electronic archiving system has been confirmed, the digital documents can be deleted. The digital archives need to be stored securely for as long as required.
- **Consultation, transfer, and deletion of digital archives**: Digital archives may be
  - consulted: the client (or an authorized third-party) may request a copy of the digital archive from the organization, which can be transferred to the client either through electronic file transfer or through a physical transport of storage media. The digital archive itself is not modified. Note that the consultation request may be limited only to the metadata associated with the digital archive. Such metadata can be useful for proving or verifying that the archiving process has been executed correctly.

- deleted: a maximum retention period may be assigned to digital archives. Once the maximum retention period has elapsed, the digital archive will be deleted from the archiving system. Alternatively, the client may also request that a digital archive is deleted from the archiving system.
- returned: at the request of the client, a digital archive may be returned to the client together with its associated archiving metadata. For returning a digital archive, a copy of the digital archive is transferred to the client in the same way as for consulting a digital archive. Subsequently, the organization deletes the digital archive from the archiving system.
- transferred: at the request of the client or when the organization ceases to provide digitization or e-archiving services, a digital archive may be transferred to another digitization or e-archiving service provider. In that case, the organization has to delete the digital archives that have been transferred away from its archiving system.

The Law of 25 July 2015 on electronic archiving also introduces special types of digitization or e-archiving service providers for the financial sector.

Digitization or E-Archiving Service Providers for the Financial Sector

The Commission de Surveillance du Secteur Financier, CSSF[35] is a public institution in the Grand Duchy of Luxembourg tasked with the supervision of the financial sector in Luxembourg. Besides supervision, regulation, and inspection, the CSSF also enforces laws relating to financial consumer protection and it aims at promoting transparency, simplicity, and fairness regarding financial products and services.

By law, every organization that wants to provide financial services in the Grand Duchy of Luxembourg is subject to regulation by the CSSF. For that purpose, the modified Law of the 5 April 1993 relating to the financial sector [37] introduces the legal status of "Professionals of the Financial Sector" (*"Professionels du Secteur Financier"* in French), abbreviated with PSF. Moreover, the modified Law of 5 April 1993 relating to the financial sector defines a sub-category of "support PSF" ("PSF de support" in French), which are organizations that do not carry out financial activities but which are sub-contractors that provide operational services to proper PSF (which do carry out financial activities themselves).

In particular, the modified Law of 5 April 1993 relating to the financial sector defines the following types of support PSF:

- Art. 29-1: client communication agents,
- Art. 29-2: administrative agents of the financial sector,
- Art. 29-3: IT systems and communication networks operators of the financial sector,
- Art. 29-5: digitization service providers of the financial sector, and
- Art. 29-6: e-archiving service providers of the financial sector.

Note that an organization that wants to obtain the "digitization service provider of the financial sector" or the "e-archiving service provider of the financial sector" status needs to have been granted the PSDC status by ILNAS first.

In the following, we will provide a short description of the Law of 25 July 2015 on electronic archiving, the supervision scheme for PSDCs applied by ILNAS, and the national standard ILNAS 106:2022.

35 See also https://www.cssf.lu

3.2. The Law of 25 July 2015 on Electronic Archiving

The objectives of the Law of 25 July 2015 on electronic archiving [18] are stated in its Chapter 1:

- to introduce the relevant notions and definitions for the digitization of original documents and for the archiving of digitized documents and of original documents in digital form;
- to determine the conditions under which digitized documents or original documents in digital form benefit from a presumption of conformity with the respective original documents;
- to define the rules that digitization and e-archiving service providers need to adhere to.

Note that in the Law on electronic archiving the term "original document" refers to a "private deed" or to the types of documents referred to in Article 16 of the "Code de commerce", i.e. certain documents relating to accounting and associated supporting documents. Similarly, an "original document in digital form" is defined as a "private deed in electronic form" or any document that was originally created in digital form (not limited to the types of documents referred to in Article 16 of the "Code de commerce").

Article 3 stipulates that additional requirements for the digitization and e-archiving of documents are specified in a Grand-Ducal Regulation. The modified Grand-Ducal Regulation of 25 July 2015 on rules for the implementation of article 4, paragraph 1 of the Law of 25 July 2015 on electronic archiving [38] has been introduced for this purpose. The latest modifications to this Grand-Ducal Regulation have been published in the Grand-Ducal Regulation of 7 August 2023 [39], which defines that the certification of digitization or e-archiving service providers is based on the national standard ILNAS 106:2022.

The legal requirements under which digitization or e-archiving service providers have to operate are introduced in Chapter 2. Article 4 of the Law of 25 July 2015 on electronic archiving defines the supervision procedure of digitization and e-archiving service providers, and it determines ILNAS as the national supervisory body of such service providers. A more detailed description of the supervision procedure can be found in Section 3.3. Article 4 also introduces the concept of a List of digitization or e-archiving service providers, which is published on the website of ILNAS. Moreover, it is specified that only organizations which appear on that list can make use of the denomination "prestataire de services de dématérialisation ou de conservation" or "PSDC". More details regarding the List of PSDCs can be found in Section 3.3. The last paragraph of Article 4 establishes that organizations that carry out digitization & e-archiving activities exclusively for their own purposes or only for one or several companies that belong to the same group can also apply for the legal status of PSDC. In that case, the last paragraph of Article 4 states that fewer conditions apply on disclosure requirements, on ownership and guarantees regarding data storage equipment, and on the cessation of PSDC activities.

Article 5 defines the conditions under which the inscription of an organization into the List of PSDCs may be suspended or revoked. For instance, ILNAS may proceed with suspending or revoking the inscription of an organization into the List of PSDCs when it discovers an event or an incident that may violate, or that has already violated, one of the legal requirements of the Law on electronic archiving or the applicable edition of national standard ILNAS 106. Article 5 also forces digitization or e-archiving service providers to inform ILNAS without undue delay of any (suspected) violation of the Law on electronic archiving or the applicable edition of the national standard ILNAS 106. Every organization must also inform all interested parties that legally need to be in possession of an original document digitized or archived by the organization of a suspension or revocation of its PSDC status. The affected parties then have the right to demand the return of every document, analog or digital, that is kept by the organization as well as the metadata relevant for e-archiving, without having to pay excessive fees.

Disclosure requirements that digitization or e-archiving service providers need to observe are specified in Article 6. Every time before a digitization or e-archiving service provider enters a new contractual relationship with a client, it has to inform the client at least about:

- the procedure that is followed for digitization or electronic archiving;
- the procedure that is followed for restoring copies with probative value in a legible form while guaranteeing the faithfulness of the reproduction to the respective originals;
- the conditions for a possible outsourcing of data storage activities to subcontractors, including the storage location;
- the legal obligations that digitization or e-archiving service providers need to follow;
- the contractual conditions for providing digitization and e-archiving services, including the limits of the legal responsibilities of digitization or e-archiving service providers;
- the standards and the procedures that are being followed, as well as the essential technical characteristics of the technical installations used for providing digitization or e-archiving services.

Article 7 introduces the obligation for employees of a digitization or e-archiving service provider to observe professional secrecy regarding all information obtained (including the contents of the digitized or archived documents) during their professional activities, except if permitted by the owner of the information. The obligation to observe professional secrecy does not apply if the disclosure of information is authorized or required by law, or during interactions with ILNAS in the context of its supervisory activities.

Article 8 stipulates that every e-archiving service provider must ensure at all times that at least one data copy of the digital documents that have the same probative value as the originals or of original documents in digital form is stored on hardware that the service provider fully owns. Such storage hardware cannot be confiscated as long as the digital originals or the copies that have the same probative value as the original documents have not been returned to the respective owners.

The transfer and cessation of PSDC activities is addressed in Article 9. A digitization or e-archiving service provider may transfer a part or all of its activities to another digitization or e-archiving service provider under the following conditions:

- the digitization or e-archiving service provider has to inform the owner of the documents at least one month in advance of its intention to cease its PSDC activities and to transfer the copies with probative value and original documents in digital form that it keeps to another digitization or e-archiving service provider;
- at the same time, the ceasing digitization or e-archiving service provider needs to specify the identity of the digitization or e-archiving service provider to which the digital documents are being transferred;
- the owners of the documents also need to be informed that they may refuse the planned transfer of PSDC activities, in which case the ceasing digitization or e-archiving service provider must return all analog or digital documents (including relevant metadata) to their rightful owners (or to any other organization named by the owner of the documents);
- the document transfer has to take place on the date when the PSDC activities cease, at the latest.

Similarly, when a digitization or e-archiving service provider ceases its PSDC activities without transferring its activities to another digitization or e-archiving service provider, the ceasing service provider must return all analog and digital documents (including relevant metadata) to their rightful owners, or to any other organization named by the owner of the documents. Every digitization or e-archiving service provider that cannot or does not want to continue its PSDC activities must also inform ILNAS immediately. Moreover, within three months, the ceasing service provider has to ensure that its PSDC activities are taken over by another digitization or e-archiving service provider or that all analog and digital documents, including archiving metadata, are returned to their rightful owners.

The sole Article 10 in Chapter 3 of the Law of 25 July 2015 on electronic archiving refers to fines that can be imposed on organizations that make use of the denomination *"prestataire de services de dématérialisation ou de conservation"* (digitization or e-archiving service provider) or of the acronym "PSDC" without having been granted the PSDC status by ILNAS.

Modifications regarding the "Code civil" are introduced in Chapter 4. More precisely, Articles 11 and 12 modify the "Code civil" by declaring that, without proof to the contrary, digital copies that were made by a digitization or e-archiving service provider have the same probative value as the original document. It is also specified that a judge cannot reject a copy only because it is in electronic form (analogously to the eIDAS regulation) or because it has not been created by a digitization or e- archiving service provider.

Article 13 introduces two new types of organizations that fall under the supervision of the CSSF: digitization or e-archiving service providers of the financial sector, which provide digitization or e-archiving services for certain types of financial organizations. The legal status of "digitization service provider of the financial sector" and of "e-archiving service provider of the financial sector" can only be granted to legal persons. Article 13 defines minimum requirements on share capital for these two types of service providers. Note that the status of "digitization service provider of the financial sector" or of "e-archiving service provider of the financial sector" can only be granted to an organization by the CSSF after that organization has already obtained the PSDC status from ILNAS.

3.3. Supervision scheme for PSDCs

As we have seen before, ILNAS is the sole government agency in the Grand Duchy of Luxembourg authorized to grant the status of PSDC to organizations. The supervision of digitization or e-archiving service providers is carried out by the Digital Trust Department of ILNAS. In this section we will describe the corresponding supervision procedure that is applied by the Digital Trust Department (for organizations that are applying for the PSDC status or that have been granted the PSDC status already). The detailed supervision procedure can be found in [40].

Figure 10 depicts the supervision scheme that is followed by the Digital Trust Department. The scheme relies on the following actors:

- the national accreditation body, called *Office Luxembourgeois d'Accréditation et de Surveillance* (OLAS) in French, which accredits the competence of conformity assessment bodies according to the international standards ISO/IEC 17021-1:2015 [35] and ISO/IEC 27006:2015 [36];
- conformity assessment bodies (CABs), independent bodies of assessors, accredited by the national accreditation body on the basis of the standards ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015, for assessing the conformity of organizations with respect to the Law of the 25 July 2015 on electronic archiving and the national standard ILNAS 106.
- the Digital Trust Department of ILNAS, the national supervisory body, which is responsible for the supervision of PSDCs under the Law of 25 July 2015 on electronic archiving.

The purpose of an accreditation body, such as OLAS in the Grand Duchy of Luxembourg, is to act as a supervisory authority of conformity assessment bodies. According to ISO/IEC 17000:2020 [Definition 7.7] [41], accreditation is defined as a "third-party attestation related to a conformity assessment body, conveying formal demonstration of its competence, impartiality and consistent operation in performing specific conformity assessment activities". Hence, the goal of accreditation bodies is to ensure the compliance of conformity assessment bodies with respect to certain standards. The evaluation process of conformity assessment bodies is called accreditation.

In accordance with the Law of 25 July 2015 on electronic archiving, the Digital Trust Department maintains a list of all the organizations that have been granted the PSDC status, the so-called "List of PSDCs", which is published on the website of ILNAS [42]. A simplified version of the List of PSDCs from 17 October 2023 is shown in Table 1: five organizations have been granted the PSDC status. Every organization that is included in the List of PSDCs falls under the supervision of the Digital Trust Department.

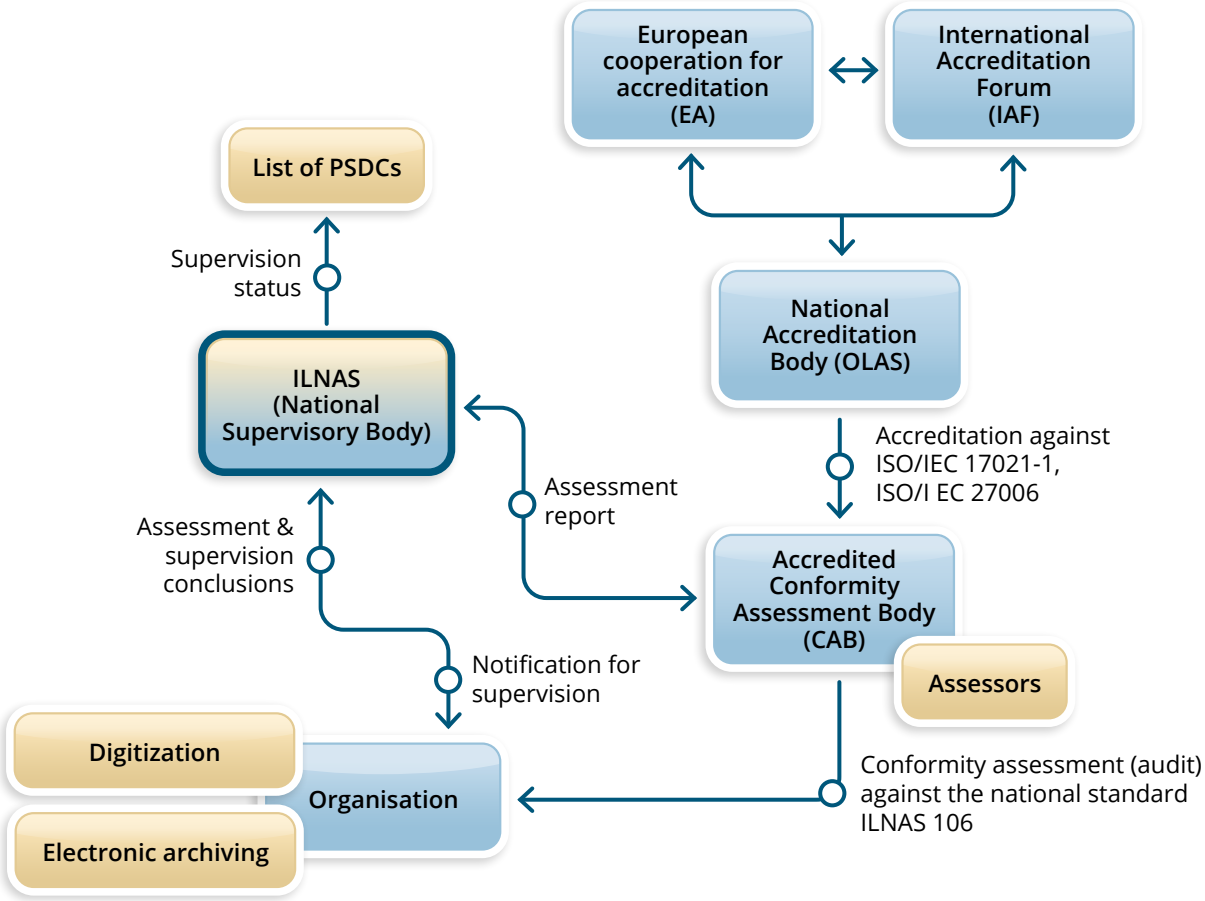

Figure 10: Supervision scheme for digitization and e-archiving service providers

3.3.1. Initiation of the Supervision

To apply for the PSDC status, an organization needs to notify its intent by submitting the form "ILNAS/PSDC Form F001a – Notification for supervision" to the Digital Trust Department. The organization also has to specify the scope of its intended activities, i.e. whether it wants to provide digitization and/or e-archiving services. The submission of this form allows the organization to officially notify its intent of applying for the PSDC status and it constitutes the "triggering event" for the supervision process.

In conjunction with form F001a, the applying organization needs to submit a certificate issued by the CAB that demonstrates the conformity of the organization with the Law of 25 July 2015 on electronic archiving and the applicable edition of the national standard ILNAS 106 (as well as some other documents). The certificate is issued by the CAB after the organization has successfully passed an initial certification audit carried out by the CAB.

Organization	Supervision ID	PSDC Status Since	Scope
Lab Luxembourg S.A. 3, rue Dr. Elvire Engel L-8346 Grass	2016/9/001	1 February 2017	Digitization & E-archiving
Numen Europe S.A. 2, rue Edmond Reuter L-5326 Contern	2016/9/002	26 September 2017	Digitization & E-archiving
Syndicat Intercommunal de Gestion Informatique 11, rue Edmond Reuter L-5326 Contern	2017/9/005	26 February 2018	E-archiving
KPMG Services S.à.r.l. 39, avenue John F. Kennedy L-1855 Luxembourg	2017/9/004	20 August 2018	Digitization & E-archiving
Centre des technologies de l'information de l'Etat 560, rue de Neudorf L-2220 Luxembourg	2017/9/006	23 August 2018	E-archiving

Table 1: Simplified List of PSDCs as of 17 October 2023

Initial certification audits are typically composed of two phases: the CAB reviews the organization's documentation during the first phase and the second phase consists of a more detailed inspection taking place on the organization's premises, which includes members of staff being interviewed by auditors. The aims of the first phase are to determine the readiness of the organization for the second phase of the audit. The minimum duration of such audits is also fixed in the PSDC supervision procedure that is applied by the Digital Trust Department [40]. The audit duration depends on the audit type (initial vs. surveillance audit) and on the pre-existing certifications that the organization may have obtained.

During the audit, nonconformities can be found, i.e. areas or aspects in which the organization is not compliant with the Law of 25 July 2015 on electronic archiving or the applicable edition of the national standard ILNAS 106. According to ISO/IEC 17021-1:2015, a nonconformity is defined as a non-achievement of a requirement. Typically, nonconformities are classified into two categories: minor and major. A major nonconformity is a nonconformity that affects the ability of a management system to reach the intended outcome. Dually, a minor nonconformity is a nonconformity that does not affect a management system's ability to attain a desired outcome. A major nonconformity is raised, for instance, if there is significant doubt that certain services fulfill the specified requirements. Also, several minor nonconformities that affect one requirement of a standard may give rise to a major nonconformity. A minor nonconformity may be raised, for example, if a problem has been detected that only affects one part of a requirement in a standard and that does not endanger the intended outcome of the management system.

All major nonconformities have to be resolved before the CAB can issue a conformity assessment certificate. Minor nonconformities do not have to be fixed immediately, but it suffices to provide a corrective action plan for each minor nonconformity, which has to be accepted by the CAB. After an analysis of the corrective action plans, the CAB may issue a conformity assessment certificate to the organization.

We refer the reader to [40] and [43] for the complete list of documents that have to be submitted by an organization to the Digital Trust Department to apply for the PSDC status. Note that the Digital Trust Department

may ask the applying organization to provide additional documents that are not indicated in [40] and [43] before a decision about granting the PSDC status can be made.

Recall that the aim of the supervision by the Digital Trust Department is to ensure that PSDCs meet the applicable requirements laid down in the Law on electronic archiving and in the applicable edition of the national standard ILNAS 106. During the review of the application for the PSDC status the following points are analyzed in particular:

- validity and scope of the accreditation of the conformity assessment body;
- validity and scope of the conformity assessment of the applying organization against the Law of 25 July 2015 on electronic archiving and the applicable edition of the national standard ILNAS 106;
- knowledge of the Law of 25 July 2015 on electronic archiving and the applicable edition of the national standard ILNAS 106 by the auditors who carried out the accreditation assessment of the CAB;
- knowledge of the Law of 25 July 2015 on electronic archiving and of the applicable edition of the national standard ILNAS 106 by the auditors who carried out the conformity assessment of the applying organization;
- completeness of the conformity assessment report, i.e., whether the conformity assess report covers all the requirements introduced in the Law of 25 July 2015 on electronic archiving and in the applicable edition of the national standard ILNAS 106;
- if applicable, the resolution of major nonconformities detected during the conformity assessment.

Note that, by the Law of 25 July 2015 on electronic archiving, an organization may only use the designation "PSDC" once it has appeared on the List of PSDCs.

3.3.2. During the Supervision

After an organization has been included into the List of PSDCs, it will be under the supervision of the Digital Trust Department of ILNAS.

During the supervision phase, the Digital Trust Department aims to organize a supervisory meeting with each PSDC at least every 6 months, which allows for a review of the PSDC's recent activities. PSDCs are also obliged to inform the Digital Trust Department of every major change in their organization. Major changes include significant changes to the structure of the organization or to the resources that are used for carrying out activities that fall under the supervision of the Digital Trust Department. PSDCs may apply for an extension of their PSDC status (e.g., if they additionally want to provide digitization services after only carrying out e-archiving activities so far) by notifying the Digital Trust Department using the same form as for the initiation of the supervision.

PSDCs are obliged to annually demonstrate to the Digital Trust Department that they still fulfill all the conditions from the beginning of the supervision (see Section 3.3.1.). To that end, the conformity assessment scheme applied by the CAB requires a conformity assessment every 12 months. These conformity assessments are organized in the form of a conformity assessment program that extends over three years. A full conformity assessment is carried out in the beginning, which is followed by yearly surveillance conformity assessments in the two following years. Three years after the initial conformity assessment, the assessment cycle starts anew with a full conformity assessment. PSDCs must submit conformity assessment reports issued after conformity assessments to the Digital Trust Department.

Note that the Digital Trust Department may request a conformity assessment of a PSDC at any time with the help of a CAB, at its sole discretion.

Also, PSDCs are obliged to inform the Digital Trust Department of any event, circumstance, or incident that may violate requirements of the Law of 25 July 2015 on electronic archiving or the applicable edition of the national standard ILNAS 106.

3.3.3. Termination of the Supervision

Each PSDC may opt at any time for a reduction, a suspension, or a revocation of its PSDC status by notifying the Digital Trust Department. The List of PSDCs will then be updated accordingly and the changes will be communicated to the applying organization.

A suspension of the PSDC status leads to the interdiction of using the designation “PSDC”. Each voluntary suspension that lasts for longer than 18 months after the date of receiving the suspension notice by the Digital Trust Department will result in a withdrawal of the PSDC status.

3.4. Certification of PSDCs

In this section, we will provide a more detailed overview of the technical conditions that must be observed for obtaining the status of PSDC, which are in fact based on the national standard ILNAS 106 *Archivage électronique - Référentiel d'exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC)* [34]. Recall that the technical requirements for the digitization and e-archiving of documents are specified in the modified Grand-Ducal Regulation of 25 July 2015 on rules for the implementation of article 4, paragraph 1 of the Law of 25 July 2015 on electronic archiving [38], which was last modified by Grand-Ducal Regulation of 7 August 2023 [39]. At the time of writing, the certification of PSDCs is based on the 2022 edition of the national standard ILNAS 106.[36] As that national standard is based on the international standards ISO/IEC 27001:2013, ISO/IEC 27002:2013, and ISO 14641:2018, we will briefly introduce those standards as well.

We begin with an introduction to the ISO/IEC 27000 family of standards.

3.4.1. The ISO/IEC 27000 Family of Standards

In a nutshell, the goal of the ISO/IEC 27000 collection of standards is to ensure the security of information. The standards are generic in the sense that information assets which should be safeguarded can originate from any type of source, such as financial data, health records, or personal details about employees. The ISO/IEC 27000 standards are therefore well-suited for guaranteeing the integrity and confidentiality of digitized documents and of electronic archives. All ISO/IEC 27000 standards are developed in a collaboration between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The notion of Information Security Management System (ISMS) has been introduced in the ISO/IEC 27000 family of standards. According to ISO/IEC 27000:2018, an ISMS "consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets." An ISMS can be seen as a method for managing information in an organization in such a way that its security is ensured. During the design of an ISMS, an organization needs to analyze all the risks that threaten information security and devise appropriate policies, procedures, and measures for reducing the likelihood of their occurrence or their impact on information security if they should materialize. Note that the deployment of an ISMS involves the implementation of security measures on IT equipment as well as the participation of employees in the sense that specialized procedures have to be followed by them.

In the following we briefly present four members of the ISO/IEC 27000 family of standards that are relevant in the context of electronic archiving:

- ISO/IEC 27000:2018: "Information technology – Security techniques – Information security management systems – Overview and vocabulary" [44],
- ISO/IEC 27001:2013: "Information Technology – Security Techniques – Information Security Management Systems – Requirements" [45],
- ISO/IEC 27002:2013: "Information Technology – Security Techniques – Code of Practice for Information Security Controls" [46],
- ISO/IEC 27006:2015: "Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems" [36].

We also refer the reader to [47] for additional information about the standards ISO/IEC 27000, 27001, and 27002.

36 The Grand-Ducal Regulation of 7 August 2023 [39] also introduces a transition period until 1 June 2024 during which PSDCs can also be certified with respect to the Technical Regulation for a management system and security measures for digitization and e-archiving service providers (v3.1) [61].

3.4.2. ISO/IEC 27000:2018

The standard ISO/IEC 27000:2018 introduces terms and definitions that are commonly used throughout the ISO/IEC 2700x standards and it gives an introduction to information security management systems. In particular, the principles & benefits of an ISMS as well as the aspects of establishing, maintaining, and improving an ISMS are discussed. ISO/IEC 27000 concludes with an overview of the ISO/IEC 27000 collection of standards.

The latest version of the standard has been published in 2018, and it is available for download free of charge.

3.4.3. ISO/IEC 27001:2013

The goal of the ISO/IEC 27001:2013 standard is to provide guidelines that allow an organization to develop policies, processes, and procedures for preserving the confidentiality, integrity and availability of information. By following the ISO/IEC 27001 standard, an organization will be able to "establish, implement, maintain, and continually improve an information security management system" (ISMS) [45].

The latest edition of ISO/IEC 27001 has been published in 2022, but the currently applicable edition of the national standard ILNAS 106:2022 still refers to the 2013 edition of ISO/IEC 27001.

The standard mandates the use of the "Plan-Do-Check-Act" model for accomplishing information security goals.

"Plan:" The aim of the planning part is to design an ISMS that can achieve the information security goals. To that end, the organization is supposed to determine the intended scope of the ISMS and identify all internal and external issues that might affect the proper operation of the ISMS. The organization has to develop a risk assessment process that can identify all the risks which threaten the correct operation of the ISMS. For each identified risk, one has (1) to assess the gravity of the consequences that will occur if the risk materializes and (2) to evaluate the likelihood of the occurrence of the risk. By combining these assessments, one can derive a "risk level" for each identified risk that expresses its harmfulness for the operation of the ISMS. At the same time, the organization has to define a risk acceptance level, which is a risk level that the organization deems acceptable. Risks that have a risk level that falls below the risk acceptance level do not require any further treatment. For risks that have been associated a risk level above the risk acceptance level, the organization will have to treat the risks, commonly by applying the measures that are described in Appendix A of ISO/IEC 27001, where they are called controls, to mitigate their consequences or the likelihood of their occurrence. Note that the organization is free to implement additional controls that are not contained in Appendix A. The choice of controls needs to be formalized in an information security risk treatment plan. For some risks, a viable alternative might be to purchase insurance to protect against their occurrence. The standard also mandates that the organization maintains a document called "Statement of Applicability", which lists all the controls that were implemented by the organization (i.e. controls from Annex A as well as supplemental controls not listed in Annex A) and the controls from Annex A that were excluded, together with justifications for doing so.

The standard also requires the management of the organization to provide sufficient resources to support the implementation and operation of the ISMS and to ensure that the employees have the necessary skills. Another requirement of ISO/IEC 27001 is that the organization adopts a document management system and that the organization maintains documented information on their processes, procedures, and the actions of employees.

"Do:" The implementation and the operation of the ISMS according to the planning phase are the focus of the "Do"-part. The standard mandates that all the processes and the risk treatment plan that were previously devised need to be implemented. Moreover, the organization needs to develop a procedure for handling changes to the ISMS. The assessment of information security risks needs to be reviewed at regular intervals, or whenever changes to the ISMS occur. As always, every action concerning the implementation of the ISMS and every review needs to be documented.

"Check:" The "Check"-part of the standard concerns the monitoring and the analysis of the operation of the ISMS, aiming at guaranteeing its adequacy & effectiveness. To that end, ISO/IEC 27001 mandates that the organization develops an internal audit program through which the organization itself assesses its conformity with respect to the standard at regular intervals and monitors the performance of the ISMS with respect to internal performance criteria. Another instrument that the standard requires is the management review. This review needs to be carried out by the top management at regular intervals with the aim of analyzing and endorsing all activities relating to the ISMS. For example, during the management review, updates to the assessment of risks or the results of internal audits need to be examined. Also, the top management is responsible for identifying opportunities for improvement and for taking decisions regarding modifications to the ISMS.

"Act:" Finally, the continual improvement of the ISMS for guaranteeing its future adequacy and effectiveness is addressed in the "Act"-part. One major aspect thereof is the reaction to nonconformities with respect to the standard. Whenever a nonconformity has been detected, the organization needs to analyze its root causes, identify the consequences and implement corrective actions. Also, the organization needs to make sure that such a nonconformity will not occur again.

3.4.4. ISO/IEC 27002:2013

The ISO/IEC 27002:2013 standard aims to be a reference for organizations to choose controls when implementing an ISMS based on ISO/IEC 27001. Furthermore, the standard provides guidelines for implementing commonly used information security controls. In that way, the standard can be helpful for organizations to develop their own strategies for information security management.

ISO/IEC 27002:2013 considers 35 main security objectives that fall into 14 global categories (indicated as main clauses in the standard). For each security objective, several controls are listed that contribute to achieving the stated security objective. Overall, the standard describes 114 controls.

Security objectives that are covered in the standard range over human resource security, asset management, cryptography, communications security, supplier relationships, compliance, etc.

The latest edition of ISO/IEC 27002 has been published in 2022, but the currently applicable edition of the national standard ILNAS 106:2022 still refers to the 2013 edition of ISO/IEC 27002.

3.4.5. ISO/IEC 27006

The standard ISO/IEC 27006:2015 can be seen as an extension of ISO/IEC 17021-1 to auditing and certifying ISMS based on ISO/IEC 27001.

ISO/IEC 17021-1 defines requirements for organizations that provide audits and certifications of management systems, e.g. conformity assessment bodies. ISO/IEC 27006 is intended to support the accreditation of organizations that provide certification services of ISMS according to ISO/IEC 27001.

3.4.6. ISO 14641:2018

The international standard ISO 14641: "Electronic document management – Design and operation of an information system for the preservation of electronic documents – Specifications" is developed by the technical committee ISO/TC 171/SC 1 *Quality, preservation and integrity of information*. The aim of ISO 14641 is to provide requirements for digitizing analog documents and storing electronic documents whilst preserving the integrity of the digitized documents with respect to the original documents, as well as the integrity of electronic documents, over long periods of time.

In the following we provide a short overview of the different chapters contained in the 2018 edition of ISO 14641.

The first chapters introduce the scope of the standard, normative references as well as the terms and definitions that are used in the document.

Chapter 4 then mandates the development of an archival policy that lists the general characteristics of the archiving system and introduces the procedures that have to be applied to ensure the confidentiality, integrity and availability of the archived documents. Chapter 4 also lists the levels of requirements that organizations which implement the ISO 14641 standard can adhere to.

Chapter 5 requires the creation of a technical description manual of the archiving system, covering important aspects such as its hardware & software components, its architecture, physical security aspects, etc. Organizations that follow ISO 14641 will also have to devise profiles that can be used to characterize documents in terms of their archiving properties. The profiles would define, for example, the duration of archiving, access rights, etc.

Procedures will have to be devised that cover the complete archiving process, ranging from the scanning of analog documents to the storage and return of archived documents.

Regarding security, Chapter 5 requires organizations to have a procedure in place for managing the security of the digitization or e-archiving system. ISO 14641 refers to ISO/IEC 27001 for information security aspects. In particular, a risk assessment needs to be carried out. Organizations that operate a digitization or e-archiving system need to guarantee its physical security as well as the security of its hardware and (custom) software components. The archival system must be maintained and changes to the archiving system need to be managed. Exhaustive backups need to be made, and procedures for recovering from disasters need to be set up. Important aspects of time stamping in relation to electronic archiving are also covered in Chapter 5.

ISO 14641:2018 also introduces the important notion of **audit trail**, which refers to all the events that have occurred during the lifetime of the archiving system and the archived documents. The integrity of the audit trail needs to be protected at all times.

Several types of storage media for use in an archiving system are discussed in the Chapters 6, 7, 8, and 9. Specific requirements are imposed for each type of storage media.

Chapter 10 imposes that the format of documents that were initially created in electronic format, so-called "electronically born documents", needs to be taken into consideration when such documents are archived. ISO 14641 imposes certain conditions depending on which file format is used. Integrity checks have to be performed before archiving a document in the archiving system and procedures for handling metadata associated with archived documents need to be in place.

ISO 14641 also contains specific requirements for scanning documents on paper or on microform, ranging from the preparation of the documents to be scanned to verifying the quality of the resulting electronic documents. The archiving of audio and video objects, as well as compression techniques relating to image, audio, and video objects are also covered in ISO 14641:2018. Requirements on the conversion of file formats are introduced in the last section of Chapter 10.

Chapter 11 contains provisions relating to accessing, returning and disposing of archives.

Requirements concerning regular audits of the digitization or e-archiving system, including its processes and procedures, are detailed in Chapter 12.

Chapter 13 imposes requirements on organizations that carry out archiving operations for third-parties, e.g. organizations that provide archiving services to external customers. The requirements for archiving the documents of external customers complement those for archiving internal documents. In particular, such organizations have to set up contracts with their external customers that cover the essential aspects of the archiving services.

In the final Chapter 14, ISO 14641:2018 introduces the requirements that have to be respected by an organization when a part of a digitization or electronic archiving service is subcontracted to a service provider.

3.4.7. The National Standard ILNAS 106:2022

The national standard ILNAS 106:2022[37] was developed by the technical committee ILNAS/TC 106, which was founded in 2018 with the aim of developing a national standard on digitization and e-archiving that can serve as the basis for the certification of PSDCs. In June 2022, the first edition of the Luxembourgish standard entitled

ILNAS 106:2022 - Archivage électronique - Référentiel d'exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC)

was finalized. It was then referenced in the Official Journal of the Grand Duchy of Luxembourg on 18 July 2022, turning it into a national standard on 22 July 2022 (i.e. on the day the publication in the Official Journal of the Grand Duchy of Luxembourg came into force).

It is important to note that every interested party can participate in the normalization process and contribute to the development of the next national standard on electronic archiving.

The national standard ILNAS 106:2022 is based on the international standards ISO/IEC 27001:2013, ISO/IEC 27002:2013, and ISO 14641:2018.

One of the main goals of ILNAS 106:2022 is to introduce the properties of authenticity, trustworthiness, and operability into the scope of the ISMS. Such an extended ISMS is then suitable for managing all the required properties of digitization or e-archiving services.

The standard ILNAS 106:2022 does not impose the implementation of a certain solution for digitization or electronic archiving. Instead, it introduces requirements, measures and it gives implementation guidelines that an organization needs to take into consideration for obtaining the PSDC status.

Note that the standard ILNAS 106:2022 mandates that the trust services introduced in the eIDAS Regulation [11] are taken as a basis for establishing the security of information in the context of digitization and electronic archiving[38].

ILNAS 106:2022 requires the use of cryptographic techniques to protect the integrity and trustworthiness of digitized documents and digital archives. In particular, it recommends the deployment of qualified trust services as introduced in the eIDAS Regulation.

The cryptographic techniques that ILNAS 106:2022 advocates include:

- authentication based on cryptographic mechanisms;
- computation of cryptographic hashes of digitized documents and digital archives;
- validation and approval of internal documents (like activity reports) with the help of qualified electronic signatures;
- qualified timestamping of log files; and
- secure transfer of documents with the help of cryptographic techniques.

In the following, we provide a short description of the different clauses contained in the national standard ILNAS 106:2022.

37 The standard is available free of charge through https://portail-qualite.public.lu/content/dam/qualite/fr/normes-normalisation/achat-consultation-normes/normes-nationales/ilnas-1062022-f.pdf

38 cf. Chapter 2: Electronic identification and electronic signatures

Section 3 of ILNAS 106:2022 introduces the terms and definitions that will be used throughout the document.

Section 4 describes the relationship between the national standard ILNAS 106:2022 and the international standards ISO 14641:2018, ISO/IEC 27001:2013, and ISO/IEC 27002:2013. The national standard ILNAS 106:2022 builds upon these three international standards and extends them with some specific requirements.

Section 5 lists the optional requirements from ISO 14641:2018 that need to be applied for certifications in the context of the PSDC status, such as strong authentication, timestamping by relying on a trusted timestamping authority, etc.

Section 6 lists additional requirements with respect to ISO/IEC 27001:2013 that are specific to the digitization or e-archiving context. Note that the numbering of the subsections in Section 6 and in Section 7 is not linear as these subsections introduce additional requirements with respect to ISO/IEC 27001:2013 and ISO/IEC 27002:2013, respectively. Consequently, they have been assigned numbers that are not used in ISO/IEC 27001:2013 and in ISO/IEC 27002:2013.

For example, Sections 6.2.4.0 and 6.2.4.3 require an organization to run a management system for the processes of digitization or of e-archiving that is integrated into an ISMS (or that follows the same requirements) to ensure

- the correct operation of the processes relating to digitization or e-archiving;
- the financial stability of the organization; and
- the ability of the organization to fulfill its contractual, legal, and regulatory responsibilities relating to the processes of digitization or e-archiving.

When determining the scope of the ISMS, the organization needs to take the digitization or e-archiving process itself, the type of documents, and the type of clients into account.

Section 7 of ILNAS 106:2022 introduces additional security objectives, measures, and recommendations that are relevant in the digitization or e-archiving context. In line with ISO/IEC 27002:2013, ILNAS 106:2022 introduces new security objectives that are accompanied by measures for achieving the objectives. Recommendations for implementing the aforementioned measures may be given as well.

For example, Section 7.5.2. introduces a new security objective aiming at ensuring management support for the digitization or e-archiving processes to follow best industry practices and all applicable legal requirements. ILNAS 106:2022 introduces two security measures to support the aforementioned security objective. A first measure recommends the introduction of a “digitization or e-archiving policy” that has to be approved by the management of the organization, applied throughout the organization, distributed and communicated to the employees and affected third parties. A second measure recommends that the digitization or e-archiving policy is reviewed at regular intervals, and whenever major changes occur, to guarantee its appropriateness, adequacy, and effectiveness.

4

4

Cybersecurity certification

4. Cybersecurity certification

The third chapter of the document describes another category of trust-enabling tool: the attestation through a certificate that a certain level of cybersecurity is actually achieved for an ICT product, ICT service or ICT process.

4.1. The Cybersecurity Act

The Cybersecurity Act (CSA) [14] is a European regulation that aims to create an EU-wide framework for cybersecurity certification schemes covering ICT products, ICT services and ICT processes. It also gives ENISA – the European Union Agency for Cybersecurity[39] – a permanent mandate as the EU's official cybersecurity agency, and assigns to ENISA specific tasks regarding cybersecurity certification in the defined framework ([14], see Title II).

More precisely, the CSA defines rules for creating and managing cybersecurity certification schemes that allow for certificates obtained in one Member State to be recognized across the entire single market. The text dictates in particular the minimal contents of a given scheme, and also creates a governance system englobing all actors involved.

4.1.1. General purpose and major features

First and foremost, the Regulation aims to increase the level of cybersecurity of the European Union through the uptake by market actors of certification, since certified products, services, and processes carry with them a guaranteed baseline of cyber-defense mechanisms. Secondly, it has the objective of eliminating market fragmentation in the specific activity of cybersecurity certification. Indeed, having an EU regulation confers a single-market-harmonized set of requirements to certification schemes, rather than a collection of nation-dependent ones. This second objective is also in support of the first, as it allows creating conditions under which all Member States achieve an equal, high level of protection.

Below, we give a description of the main features (see Figure 11) of the thus-defined European Cybersecurity Certification Framework (ECCF, [14], see Title III).

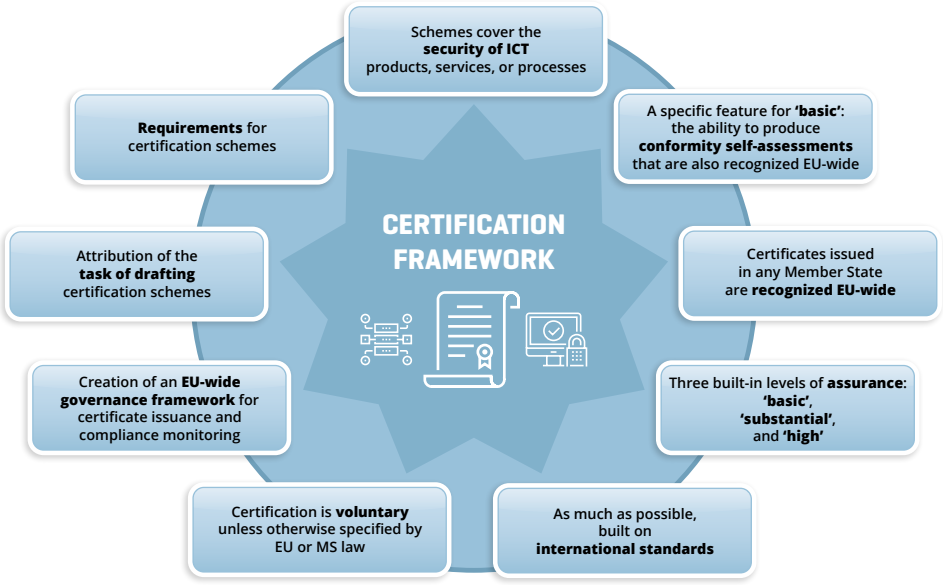

Figure 11: The major features of the CSA certification framework

39 https://www.enisa.europa.eu/

Schemes cover the security of ICT products, ICT services, or ICT processes. The three main categories of certification targets are precisely defined in the CSA text ([14], see Article 46), but are intuitively well understood. Products cover elements such as hardware or software in information systems or networks. Services generally are data processing (transmission, storage, other forms of processing) procedures taken up for the benefit of a customer. Finally, processes are sets of activities in support of ICT product or service life-cycle steps.

The exact topics to be the subject of a certification scheme are designated by the European Commission, following market needs and stakeholder feedback. (More on this is explained in Section 4.1.3.) Currently, three schemes are under preparation, covering respectively ICT products in general, Cloud Services, and 5G equipment. (See Section 4.2.3. for a description of the existing draft schemes under preparation.)

Three built-in levels of assurance: 'basic', 'substantial', and 'high'. Schemes shall specify at least one among three assurance levels that the target is to be evaluated against: 'basic', 'substantial' and 'high' ([14], see Article 52).

Security assurance can be understood as the degree of confidence one has that measures or controls are in place for a certain level of security to be achieved. To gain more assurance, one seeks out additional or more rigorous evidence from an evaluation. Thus, the deeper the evaluation, the higher the assurance, and the greater the confidence one gains in the purported level of security claimed by the product, service, or process.

In practice, the three levels of assurance correspond to actual levels of security, from least stringent – defending against low-level and low-skilled attackers, working in an isolated manner and only capable of launching known attacks on simple vulnerabilities – to most stringent – defending against high-skilled, high-resource, state-of-the-art attackers, working in teams and able to research or purchase sophisticated vulnerabilities.

Requirements for certification schemes. Each scheme shall contain a number of mandatory elements specified by the Regulation ([14], see Article 54). Among the most important, one finds information pertaining to the scheme target itself, such as the exact topic of the scheme, the assurance levels covered, and a reference to (or a specification of) the security and assurance requirements the target is to conform to for each given stated assurance level. One also finds requirements on how, and by whom, evaluation against the scheme is to be conducted; this concerns those entities involved in conformity assessment. Finally, rules regarding the surveillance of the scheme by CSA governance are also given. See Section 4.2.1. for more details.

Attribution of the task of drafting certification schemes. The Regulation mandates that ENISA take on the actual drafting of the technical description of the certification schemes on the selected topics. Once a topic has been set, ENISA then forms an ad hoc working group (which runs according to internal ENISA rules [14], see Articles 49(4) and 20(4)) to achieve this task. More on the process of scheme construction is in Section 4.2.2.

Creation of an EU-wide governance framework for certificate issuance and compliance monitoring. This EU-wide governance framework is a mix of pre-existing and CSA-created entities.

On the one hand, certificate issuance is handled by a network of Certification Bodies (CBs), themselves supported - whenever necessary - by IT Security Evaluation Facilities (ITSEFs). (Concretely, ITSEFs are cybersecurity evaluation laboratories.) CBs and ITSEFs are collectively referred to by the Regulation as Conformity Assessment Bodies (CABs), and they are to be accredited by National Accreditation Bodies (NABs, [14], see Article 60(1)). Historically, conformity assessment in general covers many topics besides cybersecurity (e.g. food safety, medicine, biology, etc.). Thus, regardless of whether or not cybersecurity-specialized CABs are established, a collective framework of CABs and NABs is essentially already in place[40].

40 See for instance the European Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93: https://eur-lex.europa.eu/eli/reg/2008/765/oj.

On the other hand, each Member State is instructed to designate at least one National Cybersecurity Certification Authority (NCCA), the primary roles of which are ([14], see Articles 58(7) and 62(2)):

- to monitor that certified products, services, and processes remain compliant with their certificates;
- to support NABs in monitoring that CABs comply with the Regulation; and
- to support the European Commission in managing the Regulation itself, in particular through participation in the European Cybersecurity Certification Group (ECCG, see Section 4.1.3.).

NCCAs may also, under certain conditions, act as CBs themselves ([14], see Article 58(4)).

In Luxembourg, the NCCA role is assigned to ILNAS, solely in charge of supervision activities (see Section 4.1.2.). An illustration of how market actors interact in the context of an activated certification scheme can be found in Figure 12 in Section 4.1.2.

As much as possible, built on international standards. Schemes are as much as possible technically grounded in internationally recognized technical specifications – typically international or European standards – in order to 1) have a base on well-established good practices, thus facilitating market uptake and recognition, and 2) not duplicate work in requirements establishment. Typical standardization committees that are involved in cybersecurity and information security include:

- The international technical standardization sub-committee ISO/IEC JTC 1/SC 27 *Information security, cybersecurity and privacy protection*[41];
- The European technical standardization joint technical committee CEN/CLC/JTC 13 *Cybersecurity and data protection*[42]; and
- The European technical standardization committee ETSI TC CYBER on cybersecurity[43].

More information on technical standardization in general and on how Luxembourg is involved is available in Chapter 5.

Certificates issued in any Member State are recognized EU-wide. This is a fundamental feature in support of market harmonization in the business of cybersecurity certification ([14], see Article 56(10)). In concert with this feature, the Regulation also lays down rules on how Member States shall handle nationally-defined certification schemes ([14], see Article 57):

- National certification schemes that have the same scope as a CSA certification scheme shall be progressively de-activated and replaced by the CSA scheme. (In practice, active certificates remain valid until their expiration date.) CSA schemes are required to identify national schemes that are concerned by this rule;
- Member States shall notify the European Commission and the ECCG of any plans to create new national schemes and on which topics.

It is also important to note that organizations seeking to achieve certification may do so through CABs operating anywhere in the EU. This is particularly important in cases where certain competencies may not be available in a given MS.

Certification is voluntary unless otherwise specified by EU or MS law. The Commission shall regularly assess the need for a scheme to become mandatory ([14], see Articles 56(2) and 56(3)), taking into account a variety of factors, notably market needs or EU security requirements.

41 https://www.iso.org/committee/45306.html

42 https://standards.cencenelec.eu/dyn/www/f?p=205:32:0::::FSP_ORG_ID,FSP_LANG_ID:2307986,25&cs=1ED41A3D97E9C0D226A9087045F5D181C

43 https://www.etsi.org/committee/cyber

A specific feature for assurance level 'basic': the ability to produce conformity self-assessments that are also recognized EU-wide. Schemes that allow for certification at assurance level 'basic' shall also indicate whether conformity self-assessment is allowed in the scheme ([14], see Article 53).

Conformity self-assessment allows providers to simply declare that their product, service, or process indeed conforms to the stated scheme requirements at the 'basic' level of assurance. This has the advantage of avoiding the costs of undergoing a certification process. However, it comes with the additional responsibility of being solely accountable for the content of the declaration of conformity.

It is also important to note that a given scheme covering level 'basic' needs to explicitly state whether or not conformity self-assessment is permitted; in other words, a scheme covering level 'basic' does not automatically authorize conformity self-assessment. The term used for the document produced declaring that a conformity self-assessment is being employed is "EU declaration of conformity".

Finally, EU declarations of conformity issued in a given MS are also recognized across the whole single market, and are subject to NCCA monitoring.

4.1.2. Market actors and their interactions

Figure 12 gives an overview, for any given Member State, of market actors and their interactions in the context of an active CSA certification scheme.

The Member State nominates one or more NCCAs. One NCCA at least is nominated to conduct supervision activities, that is to monitor the continued compliance of certified (or self-declared conform) products, services, and processes on the MS' territory to the certification scheme. The primary targets of supervision in this case are the provider and associated product, service, or process. However, the NCCA may also, in collaboration with the NAB, conduct supervision activities of the CBs.

If the Member State also nominates an NCCA that acts as a CB, that NCCA shall have these activities strictly separated from supervision activities.

The task of issuing certificates remains the remit of CABs that are accredited by NABs. CABs can:

- be Certification Bodies, responsible for certificate issuance;
- be IT Security Evaluation Facilities, responsible for conducting actual IT security tests, if this is necessary; or
- take on both CB and ITSEF tasks, respecting a strict separation of duties.

These two broad activities are covered by different requirements for accreditation. If an organization claims to do both, it shall be accredited separately for each.

In general, the ecosystem of CABs accredited by NABs is already in place on a wide scope of domains, and NABs are already tasked with the primary supervision of the CABs that they accredit.

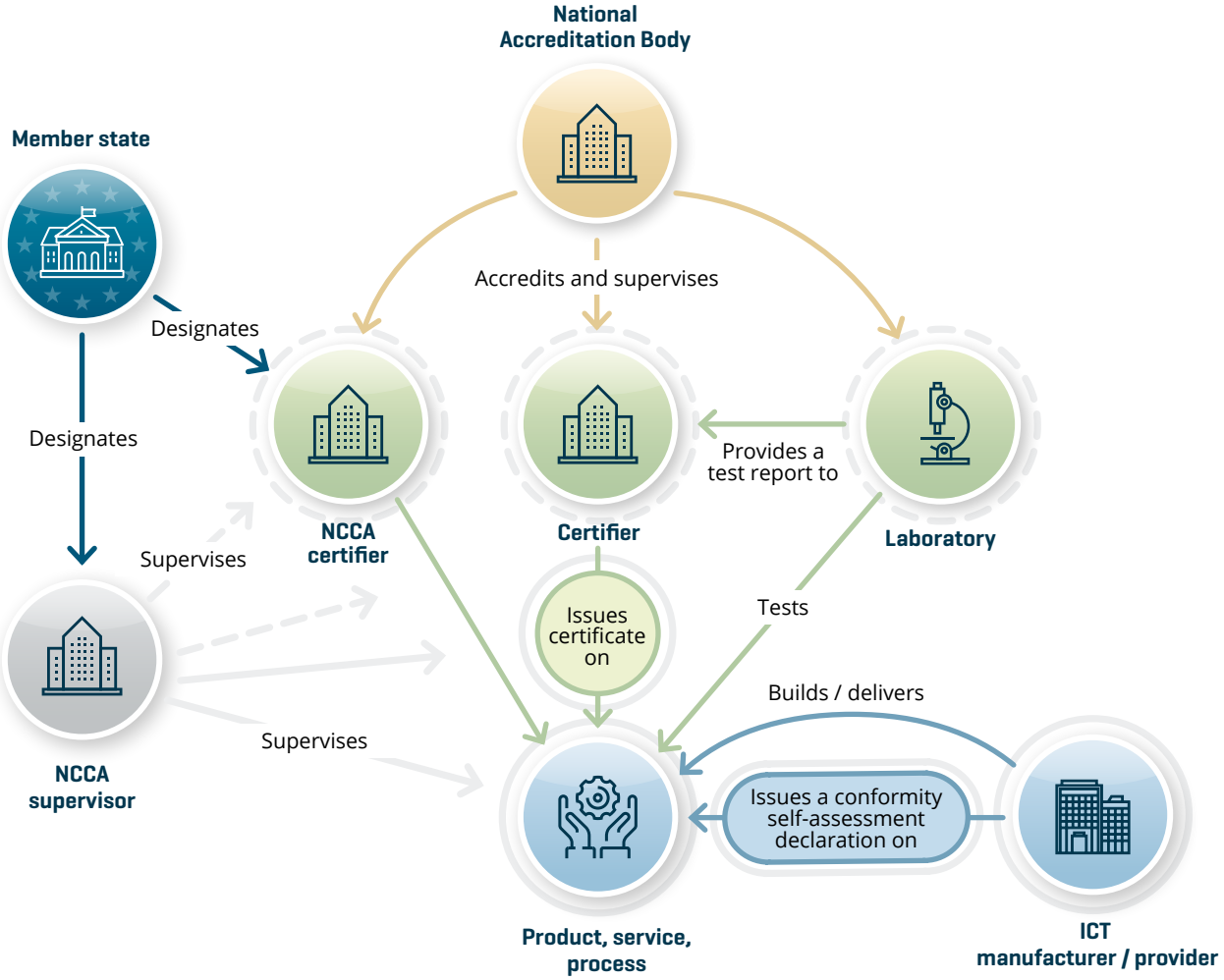

Figure 12: A generic view of the interactions between the different market actors in the CSA certification framework

4.1.3. The European Cybersecurity Certification Group and other EU-level governance bodies

The European Cybersecurity Certification Group

An important actor in the governance of the CSA is the European Cybersecurity Certification Group, or ECCG. Established and structured in part by the Regulation ([14], see Article 62), it serves as the primary working group within which the European Commission, ENISA, and the Member States run the collaborative effort to manage the CSA as a whole, and schemes in particular. Each MS is represented in ECCG meetings, usually by individuals within those Member States' NCCAs, although it can be from other related national authorities. Specific tasks assigned to the ECCG include advising the Commission on CSA implementation and maintenance and adopting formal opinions on draft schemes.

In the case of Luxembourg, ILNAS regularly joins ECCG meetings.

The Stakeholder Cybersecurity Certification Group

Another noteworthy actor in the governance scheme is the Stakeholder Cybersecurity Certification Group, or SCCG, also established by the Regulation ([14], see Article 22). While the ECCG is more about managing the overall governance of the CSA and the ECCF, the SCCG's primary task is advising the Commission on which topics to select for certification schemes.

The SCCG is composed of certification market stakeholder representatives, selected so as to respect a certain balance in terms of supply and demand in particular. Entities represented include SMEs, research organizations, standard developing organizations, relevant national authorities, and consumer organizations, to name a few.

4.2. Cybersecurity certification schemes

4.2.1. Scheme content requirements

In the interest of readability, and given that the text of the CSA regulation giving scheme content requirements is already concise and quite self-explanatory, the exact content of Article 54(1) is reproduced in italics below, with, in bold, some essential keywords:

*Article 54.1. A European cybersecurity certification scheme **shall include** at least the following elements:*

*(a) the **subject matter and scope** of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;*

*(b) a clear description of **the purpose of the scheme** and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;*

*(c) **references to the international, European or national standards applied in the evaluation** or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;*

*(d) where applicable, one or more **assurance levels**;*

*(e) an indication of **whether conformity self-assessment is permitted** under the scheme;*

*(f) where applicable, specific or additional **requirements** to which **conformity assessment bodies** are subject in order to guarantee their **technical competence** to evaluate the cybersecurity requirements;*

*(g) the specific **evaluation criteria and methods to be used**, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;*

(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;

(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

*(j) rules for **monitoring compliance** of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;*

(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;

*(l) rules concerning the **consequences** for ICT products, ICT services and ICT processes that have been **certified** or for which an EU statement of conformity has been issued, but which **do not comply with the requirements** of the scheme;*

*(m) rules concerning how **previously undetected cybersecurity vulnerabilities** in ICT products, ICT services and ICT processes are to be reported and **dealt with**;*

(n) where applicable, rules concerning the retention of records by conformity assessment bodies;

(o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;

(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;

(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;

*(r) maximum **period of validity of European cybersecurity certificates** issued under the scheme;*

(s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;

(t) conditions for the mutual recognition of certification schemes with third countries;

(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;

(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

4.2.2. Scheme creation process

The creation and launch of a certification scheme follows a strict process, which is described below, and illustrated in Figure 13.

1. **The European Commission selects a topic for which a certification scheme is needed**. This selection is based on a variety of factors, such as market needs, specific considerations in the cybersecurity threat landscape, or proliferation of national schemes on a particular topic ([14], see Article 47(3)). It also consults the SCCG. It then instruct ENISA to prepare the draft scheme.
2. **ENISA forms an ad hoc working group to draft the scheme**. The group consists of a wide variety of experts on the topic, which may be external to ENISA. Successive drafts are made public when they are deemed suitable, in order to receive public feedback. Feedback is also regularly sought from the ECCG, which may adopt formal opinion on schemes.

3. **Once a finalized scheme is available, it is made public and the European Commission prepares an implementing act to launch the scheme officially**. Implementing acts are Commission-led legislative texts that support further a harmonized adoption of a given Regulation. A process known as comitology ensures that all Member States have their say in its adoption[44].

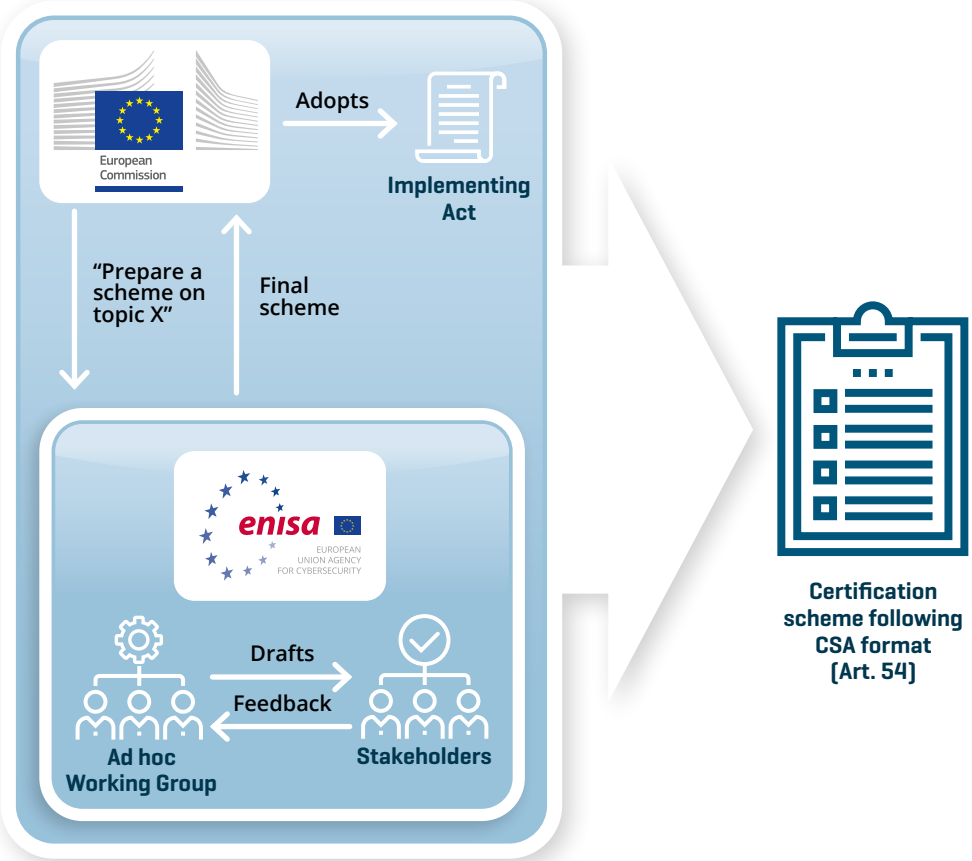

Figure 13: An overview of the certification scheme creation process

4.2.3. Upcoming schemes

At the time of writing, three schemes are under preparation in the CSA framework, with varying degrees of readiness: A scheme for general IT products, a scheme for cloud services, and a scheme for 5G equipment. We give below a few of each scheme's main characteristics[45].

For the first two listed schemes, public drafts of each exist, and so we can give a detailed structure to our exposition. For the third scheme, on 5G equipment, information is much more scarce, leading to a more succinct description.

(A note on the standards that are invoked and on which the schemes are based: we only mention the main ones that pertain to major aspects of the subject matter. The complete list of standards that are used in each scheme can be consulted in the scheme descriptions themselves.)

44 For more on implementing acts, see https://commission.europa.eu/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_en

45 See also ENISA's mini-site for cybersecurity certification: https://certification.enisa.europa.eu/.

The Common Criteria based European candidate cybersecurity certification scheme for IT products

The Common Criteria based European candidate cybersecurity certification scheme for IT products is, at the time of writing, the only scheme for which a finalized description is available, and is awaiting official activation through a European Commission Implementing Act. A draft of this act was made publicly available in October 2023[46].

Reference document

Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 [48]

Subject matter

This scheme is destined to certify ICT products, which can be anything from software (e.g. operating systems) to hardware (e.g. network switches) products. More specifically, the ICT products concerned either serve to provide security, or contain at least one security functionality.

The scheme serves as a successor to the SOG-IS[47] (Senior Officials Group – Information Systems' Security) MRA (Mutual Recognition Agreement) that has been used between a subset of European countries over the last few decades. Accordingly, much of SOG-IS documentation is taken as input to the EUCC scheme, as seen for example in the EUCC annexes.

Scheme audience

Parties interested in EUCC certification include manufacturers wishing to demonstrate the security of their products, IT service providers wishing to utilize secure equipment for the benefit of their own business, and end-users for procurement purposes.

Standards on which it is based

For defining security and assurance requirements on the product itself, the scheme is based on the ISO/IEC 15408 series of standards entitled *Evaluation criteria for IT security* [49]. This series of standards is jointly maintained by the technical standardization subcommittee ISO/IEC JTC 1 SC 27 *Information security, cybersecurity and privacy protection*[48] and the international Common Criteria community[49]. Hence, the ISO/IEC 15408 series is also known as the 'Common Criteria' (or CC).

The CC consist in a five-part series that includes, among other things:

- A list of generic *Security Functional Requirements* (SFRs), to capture security features to be incorporated to the product;
- A list of generic *Security Assurance Requirements* (SARs), to demonstrate the inclusion of security functionality; and
- An overall framework to express these requirements in a structured manner, in such a way that same-category products can be adequately compared in terms of their security functionality and assurance.

46 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en

47 https://www.sogis.eu/

48 https://www.iso.org/committee/45306.html

49 https://www.commoncriteriaportal.org/

For evaluating security and gaining assurance that the functionalities are in place, the CC are complemented by the international standard ISO/IEC 18045 *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation* [50], which describes in detail the actions that evaluators should take to actually assess that the target product (called the Target Of Evaluation, or TOE, in CC vocabulary) actually conforms to the specified CC documentation. Similarly to the CC series, ISO/IEC 18045 has a CC counterpart in the CC community, named the Common Evaluation Method, or CEM.

The ISO/IEC 15408/CC series and ISO/IEC 18045/CEM are publicly available in full either on ISO's Online Browsing Platform[50], or on the Common Criteria portal[51].

Finally, to be certain that the CABs in charge of running the evaluation and delivering the final results are competent to do so, CBs issuing certificates and ITSEFs conducting the evaluation tests are first and foremost to be accredited following the general international standards ISO/IEC 17065 *Conformity assessment – Requirements for bodies certifying products, processes and services* [27] and ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories* [51].

Other standards to be taken into account to factor in the specificities of the CC in the accreditation context include the international standards:

- ISO/IEC TS 23532-1 *Information security, cybersecurity and privacy protection – Requirements for the competence of IT security testing and evaluation laboratories – Part 1: Evaluation for ISO/IEC 15408 for ITSEFs* [52]; and
- ISO/IEC 19896-1 *IT security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements* [53] and ISO/IEC 19896-3:2018 *IT security techniques – Competence requirements for information security testers and evaluators – Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators* [54] for the ITSEFs' evaluation-conducting personnel.

More precise guidelines on accreditation with a view towards performing these activities are being worked on by ENISA.

Assurance levels covered and conformity self-assessment

The scheme covers the assurance levels 'substantial' and 'high'; more precisely, the scheme maps the CC standards' Evaluation Assurance Levels (EALs) to the Regulation's assurance levels, using vulnerability analysis depth as a main indicator. This mapping roughly places EALs 1, 2, and 3 at assurance level 'substantial', and EALs 4 to 7 at assurance level 'high'.

The scheme does not cover assurance level 'basic'. This is consistent with the intended vulnerability depth encoded in the CC. Even at EAL 1, the CC methodology – which is quite involved - is not suited for products requiring a level of assurance lower than 'substantial'.

Specific evaluation criteria and methods

As already explained above, the CC have a companion document, the CEM, that details how to actually conduct a CC evaluation on a given product. Thus, this is the specific evaluation methodology to be used. It should be noted however that for certain very specific technologies requiring high levels of assurance – known in SOG-IS and EUCC terminology as *Technical Domains* – special guidelines exist in addition to the CEM. The technical domains currently identified by the EUCC are *Smart Cards and Similar Devices* and *Hardware Devices with Security Boxes*. See the EUCC's Chapter 8 and Annexes 3 to 10 for more details.

50 https://www.iso.org/obp/ui/en/

51 https://www.commoncriteriaportal.org/cc/

Other aspects

In the CC framework, there is a specific formal construct used to describe security requirements (SFRs and SARs) on a given category of product. Put another way, the document in question shall have a structure and content prescribed by the CC framework. Such a document is called a *Protection Profile* (PP); the details of a PP's structure and guidelines to writing it are given in Chapter 10 and Annex B of ISO/IEC 15408-1 *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model* [49].

PPs are convenient in that their prescribed structure makes them easily comparable. As such, they are widely used by stakeholders. The CC framework also allows evaluating PPs to make sure that they are sound and complete. Thus, using as a basis an evaluated PP is much more reliable than using an unevaluated one.

The EUCC scheme allows, under certain conditions, to also issue certificates on PPs.

The European Cybersecurity Certification Scheme for Cloud Services

The European Cybersecurity Certification Scheme for Cloud Services is only available in first draft form, dating back to December 2020, at the time of writing of this white paper. Thus, it may undergo significant changes once it is finalized.

Reference document

EUCS – Cloud services scheme [55]

Subject matter

This scheme aims at certifying general cloud services. Paraphrasing the definitions given in the draft scheme, these are defined more precisely as *"ICT services that propose a defined interface with which to access a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand*".

There is also a distinction of the base type of cloud service that is made: this is done according to *capabilities type*, rather than through the often-used "X-as-a-Service" paradigm, considered less precise. The capabilities types that are considered are:

- *Application capabilities* type, wherein the customer gains access to the Cloud provider's applications;
- *Platform capabilities* type, wherein the customer gains access to – and can run applications on – one or more execution environments hosted by the provider; and
- *Infrastructure capabilities* type, wherein the customer gains access to processing, storage, or networking resources.

Scheme audience

The certification scheme is destined to be of use both by cloud service providers, who may seek to certify their service in order to have an adequate level of security and also to gain a competitive advantage across the EU single market over non-certified schemes, and to potential cloud service users, who may want guarantees that the service they are using has necessary and sufficient safeguards in place. The scheme is not necessarily in immediate view of end-users, who typically may not be knowledgeable of the cloud back-ends that their IT service providers are using.

Standards on which it is based

For defining security and assurance requirements on the cloud service itself, at the time of writing, it was assessed that no international or European standard was suitable on which to directly rely in order to specify security requirements for the levels of assurance considered. Thus, the current EUCS draft includes a full list of such requirements in its Annex A, which is in the process of being developed as a European standard by the European standardization technical committee CEN/CLC/JTC 13 *Cybersecurity and Data Protection*. The standard project is FprCEN/CLC/TS 18026 *Three-level approach for a set of cybersecurity requirements for cloud services*[52].

The requirements cover technical and organizational topics such as the organization of information security, asset and risk management, operational security, cryptography, and much more. Inspiration for these requirements was drawn from well-known references, such as the French SecNumcloud[53] scheme, but also the ISO/IEC 27002 *Information security, cybersecurity and privacy protection – Information security controls* [46] and ISO/IEC 27017 *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services* [56] standards. The three levels that are alluded to in the title of the standard project are in reference to the assurance levels that the EUCS scheme covers.

For evaluating security and gaining assurance that the functionalities are in place, special methodologies are defined in Annexes B, C, and D of the scheme. While these methodologies are customized, they remain rooted in

- the ISO/IEC 17065 *Conformity assessment – Requirements for bodies certifying products, processes and services* [27], and ISO/IEC 17021-1 *Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements* [35], standards; and
- the *2018 Handbook of international quality control, auditing, review, other assurance, and related service pronouncements* [57].

Finally, to be certain that the CABs in charge of running the evaluation and delivering the final results are competent to do so, a dedicated standard is under drafting also by CEN/CLC/JTC 13: it is work item JT013044 *Requirements for Conformity Assessment Bodies certifying Cloud Services*[54]. It is essentially a particularization of the ISO/IEC 17065 *Conformity assessment – Requirements for bodies certifying products, processes and services* [27] standard to the case of cloud services.

Assurance levels covered

The EUCS scheme covers all three of the assurance levels proposed by the CSA: 'basic', 'substantial', and 'high'. However, conformity self-assessment is not authorized at level 'basic', although it remains to be seen if this will change in future iterations of the scheme.

52 https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:74247,25&cs=19E6889B88C3ECD7CB6C5AFAF4C31DA2C

53 https://cyber.gouv.fr/prestataires-de-services-dinformatique-en-nuage-secnumcloud

54 https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:74248,25&cs=1430FDDC000D884544B2AFEC3A9145740

Specific evaluation criteria and methods

As explained above, customized methodologies for evaluation of cloud services against the EUCS scheme are defined in Annexes B, C, and D. More specifically:

- Annex B gives an overview of the general methodology to follow (a 'meta-approach' for the assessment, per the document itself);
- Annex C particularizes this methodology to the cases of evaluations at assurance levels 'substantial' and 'high'; and
- Annex D particularizes this methodology to the case of evaluation at assurance level 'basic'.

The difference in evaluation is essentially a matter of depth: in Annex C, one will be looking at establishing *reasonable assurance*, wherein evidence is sought to show that a claim is valid, while in Annex D, one will be looking to establish *limited assurance*, wherein less evidence is sought, and it allows showing that nothing disputes claim validity.

Other aspects

Cloud services are recognized as likely being applied in the context of one or another industrial sector with its own specificities, inviting certain kinds of specific security requirements. As a result, the EUCS scheme is meant to be enriched if necessary for such vertical applications, provided that the resulting specific scheme not weaken the base EUCS and produce the same set of deliverables. Such a particularization of the EUCS scheme is called a security profile. Official security profiles are, before application, to be validated by the ECCG and published by ENISA.

The European cybersecurity certification scheme for 5G networks

This topic was formally launched in 2022; little information on it is currently known. We give some key points from the public terms of reference of the EU5G ad hoc working group[55]:

- It is highly encouraged that the scheme reuse as much as possible elements of the EUCC and EUCS;
- The scheme shall fit into the already defined European 5G set of security solutions, such as the 5G Toolbox[56]; and
- Standards and technical specifications that are to be considered include GSMA's NESAS[57], SAS-SM[58], SAS-UP and eSA[59] schemes, the relevant eUICC protection profile and ETSI/3GPP's 5G standards[60].

There is no timeline available yet for when a draft of the scheme will be public.

55 https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification

56 https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

57 https://www.gsma.com/security/network-equipment-security-assurance-scheme/

58 https://www.gsma.com/security/security-accreditation-scheme/

59 https://www.gsma.com/services/esim/esa-certified-products/

60 https://www.etsi.org/committee/3gpp

4.3. Relation of the CSA to other pieces of EU legislation

The CSA's certification framework can conceivably be applied in any context where cybersecurity is needed on one or more products, services or processes. This includes any legislative text specifying such needs, insofar as the schemes applied actually answer the requirements.

However, there are specific legislative texts – either already in force or in preparation – that invoke usage of the CSA framework explicitly. In Table 2, we show a few of these of particular interest. We stress, however, that this document is not to be taken as a prediction or definite indication of how the CSA is ultimately applied, and how EU law evolves.

CRA - The Cyber Resilience Act

Legal Act: **The Cyber Resilience Act, or CRA**	**Broad subject matter:**	**Status:**	**Relevant links:**
(Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020)	Baseline security requirements on IT products	Proposed regulation	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
Summary: The Cyber Resilience Act proposes to create a CE marking for "products with digital elements" in order for these to have a baseline level of cybersecurity built into them prior to their circulation in the internal single market.			
Potential application of the CSA: Products that are the subject of an appropriate CSA certification may be presumed conform to the CRA.			

AIA - The Artificial Intelligence Act

LEGAL ACT: **The Artificial Intelligence Act, or AIA**	**Broad subject matter:**	**Status:**	**Relevant links:**
(Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS)	A legislative framework for artificial intelligence products	Proposed regulation	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
Summary: The Artificial Intelligence Act proposes a framework to control the application and deployment of artificial intelligence products in the European Union.			
Potential application of the CSA: AI products have, among other requirements that are particular to AI, specific cybersecurity requirements encoded in the proposed text; an appropriate CSA certification could demonstrate compliance to these requirements.			

eIDAS2 – The eIDAS revision

Legal Act: The eIDAS revision, or eIDAS2	Broad subject matter:	Status:	Relevant links:
(Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity)	A framework for defining and implementing digital identity tools for the EU and extending trust services	Proposed revision of the in-force eIDAS regulation	Proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281 In-force eIDAS regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

Summary:
(See also Section 2.5.) The eIDAS regulation's revision aims to create in particular an EU-wide framework for European digital identities in each Member State. In particular, it mandates the creation and implementation of digital identity wallets that can be used all across the single market to prove one's identity – or demonstrate that one possesses certain attributes – to access services.

Potential application of the CSA:
The digital identity wallets are the subject of cybersecurity requirements. It is envisaged that these requirements could be considered fulfilled if the wallet is certified following an appropriate CSA scheme.

NIS2 Directive

Legal Act: The NIS2 Directive	Broad subject matter:	Status:	Relevant links:
(Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148)	A revision of the existing NIS Directive to harmonize the implementation of cybersecurity in identified categories of essential and important market actors	In force	Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/oj Proposed CSA targeted amendment: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208

Summary:
NIS2 mandates in particular the creation of an EU-wide network of nationally appointed Computer Security Incident Response Teams (CSIRTs) to support the implementation of cybersecurity and security incident response in a specific list of categories of entities of critical importance to the EU, such as utility providers, providers of financial services, and others.

Potential application of the CSA:
Via the targeted CSA amendment that would pave the way for managed security service providers – CSIRTs in particular – to be covered by the CSA framework, CSIRTs themselves could be better protected through certification, and entities relying on CSIRTs for managed security services would gain further assurance from certified CSIRTs.

Table 2: Some legislative texts that may benefit from the CSA

4.4. ILNAS' role

ILNAS holds two direct roles in the CSA.

Accreditation. First, ILNAS is Luxembourg's National Accreditation Body. Accreditation tasks are managed by the *Office Luxembourgeois d'Accréditation et de Surveillance* (OLAS), one of the departments of ILNAS[61]. Thus, any Luxembourg-based market actor that wishes to undertake the role of a CAB within the European Union Cybersecurity Certification Framework will have to get in contact with OLAS.

Certification supervision. Secondly, ILNAS was nominated to be Luxembourg's NCCA, in charge of supervision activities only. The associated work is conducted by the Digital Trust Department. At the time of writing, no other entity in Luxembourg has been nominated as an NCCA; in particular, there is no Luxembourg NCCA in charge of certification activities.

Activities that ILNAS' Digital Trust Department are taking on with a view towards conducting its supervision mission include, but are not limited to:

- Updating its internal and external documentation in order to be able to formally accommodate supervision requests;
- Participating in ECCG meetings;
- Informing the market of CSA updates through publications, news items, courses or events;
- Collaborating with OLAS to support in their accommodation of possible accreditation requests linked to the CSA and to organize joint supervision tasks; and
- Supporting ILNAS in its participation in research or implementation projects such as the CORAL project on 'basic' level certification[62].

More information on the Digital Trust Department's work in the CSA can be found on the *Portail Qualité*: https://portail-qualite.public.lu/fr/cybersecurity-act.html

An illustration of the market interactions as specific to Luxembourg is shown in Figure 14.

61 https://portail-qualite.public.lu/fr/accreditation-notification.html

62 https://coral-project.org/, co-financed by the Connecting Europe Facility of the European Union.

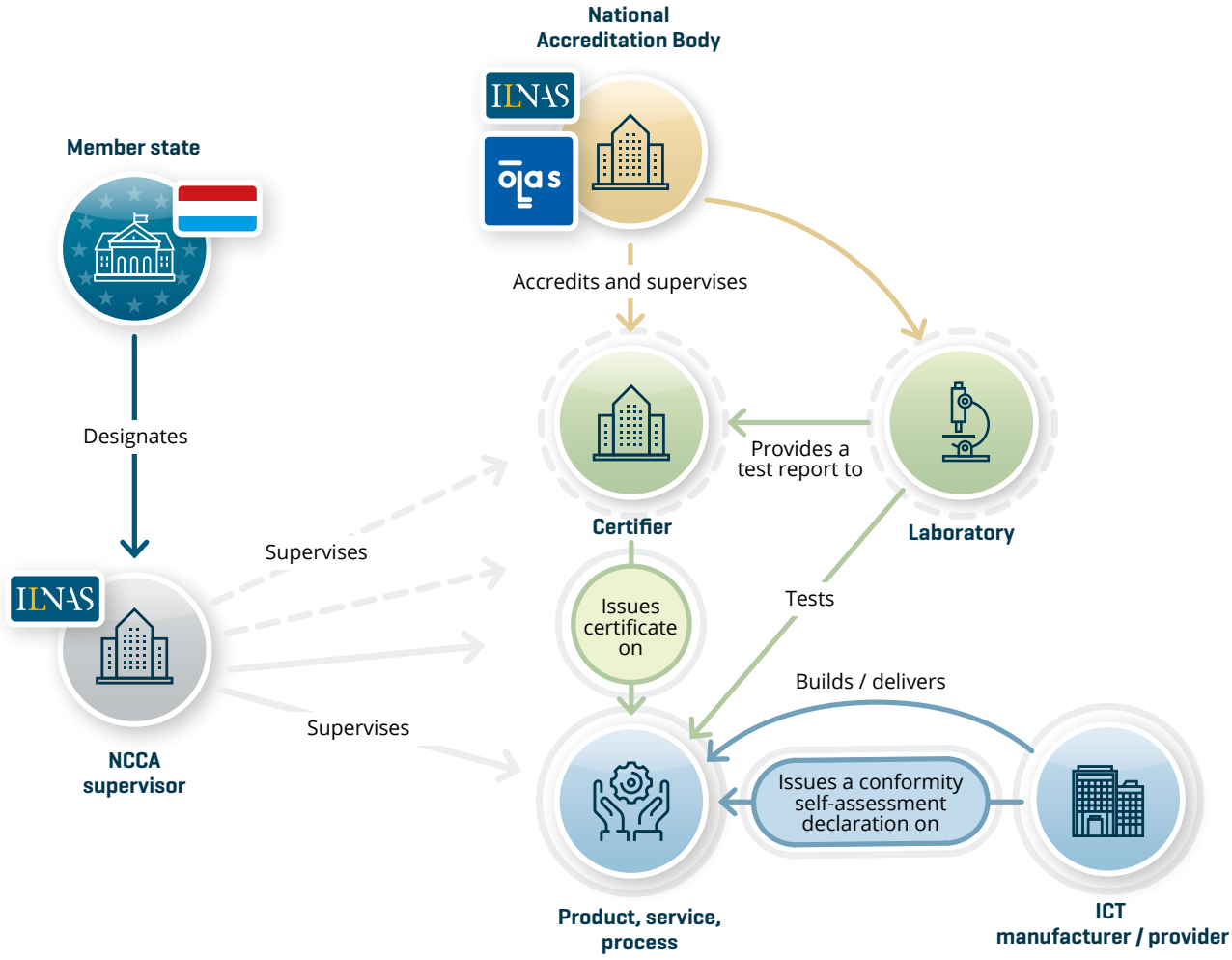

Figure 14: A view of the interactions between the different market actors in the CSA certification framework in the case of Luxembourg

5 Technical standardization

5. Technical standardization

In this last chapter, the document delves into a general tool that is common to the topics of the three previous chapters: that of technical standardization.

5.1. Technical standards

The European Regulation (EU) N°1025/2012 on European standardization [58] gives the following definition of a standard:

> *"[...] A technical specification, adopted by a recognized standardization body, for repeated or continuous application, with which compliance is not compulsory [...]"*

Standards are meant to bring solutions to recurrent technical and business problems, on a broad scale, and may apply to products, services, and processes. The World Trade Organization[63] has listed a set of fundamental principles that international standards and standards development should adhere to in order to be adequate. These are:

- **Transparency of technical work programs**. All essential information regarding current work programs, as well as on proposals for standards, guides and recommendations under consideration and on the results should be made easily accessible to all interested parties;
- **Openness in participation**. Membership of an international standards body should be open on a non-discriminatory basis to relevant bodies;
- **Impartiality and Consensus**. All relevant bodies should be provided with meaningful opportunities to contribute to the elaboration of an international standard so that the standard development process will not give privilege to, or favor the interests of, a particular supplier, country or region. Consensus procedures should be established that seek to take into account the views of all parties concerned and to reconcile any conflicting arguments;
- **Effectiveness and Relevance**. International standards need to be relevant and to effectively respond to regulatory and market needs, as well as scientific and technological developments in various countries. They should not distort the global market, have adverse effects on fair competition, or stifle innovation and technological development. In addition, they should not give preference to the characteristics or requirements of specific countries or regions when different needs or interests exist in other countries or regions. Whenever possible, international standards should be performance based rather than based on design or descriptive characteristics;
- **Coherence**. In order to avoid the development of conflicting international standards, it is important that international standards bodies avoid duplication of, or overlap with, the work of other international standards bodies. In this respect, cooperation and coordination with other relevant international bodies is essential; and
- **Development dimension**. Constraints on developing countries, in particular, to effectively participate in standards development, should be taken into consideration in the standards development process. Tangible ways of facilitating developing countries participation in international standards development should be sought.

63 https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm

The benefits of applying technical standards are numerous:

- **Quality and security.** Technical standards are developed primarily to solve problems and increase the quality of the target solution. A standardized product carries with it the knowledge of good practices from a large pool of experts. Quality is of utmost importance in many fields, for instance whenever there are effects on health and safety;
- **Interoperability and trade facilitation**. Standardized products support the achievement of mutual understanding through the use of common technical languages to describe problems, solutions, and requirements. Thus, they favor interoperability, exchange, and encourage the interchangeability of solutions;
- **Competitiveness**. Adhering to a recognized standard in a field gives a competitive edge, owing to the qualitative benefits that standards provide. This confers a certain level of economic product protection;
- **Efficiency**. Standards are developed with a view towards bringing the most broadly applicable and effective solution in mind, while preserving a large degree of flexibility. This translates to convenience of use; and
- **Societal progress**. Standardized solutions can help disseminate good practices with built-in considerations for emerging important – and world-wide – challenges, such as environmental protection and the management of diversity.

5.2. Major international and European standards bodies

The overall worldwide standards landscape is quite complex, because it contains major international, regional and national standards bodies, in addition to thousands of industrial fora, consortia, associations, etc. that develop technical specifications and other deliverables. Nevertheless, for the purpose of this document, six important bodies stand out: three at the international level and three at the European level.

The three most prominent international standards bodies are:

- the International Organization for Standardization (ISO);
- the International Electrotechnical Commission (IEC);
- the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T).

The three official European Standardization Organizations (identified as such by Regulation (EU) N°1025/2012 on European standardization) are:

- the European Committee for Standardization (CEN);
- the European Committee for Electrotechnical Standardization (CENELEC);
- the European Telecommunications Standards Institute (ETSI).

The governance system for ISO, IEC, CEN, and CENELEC organizes membership per state, while that of ITU and ETSI does so per organization. Thus, any given state involved in ISO, IEC, CEN, or CENELEC has one or more National Standards Bodies (NSBs) representing them within these organizations. Often, these national bodies are also in charge of developing national-level standards. In Luxembourg, the NSB is ILNAS (see Section 5.3.1.), which is also a member of ITU-T and ETSI.

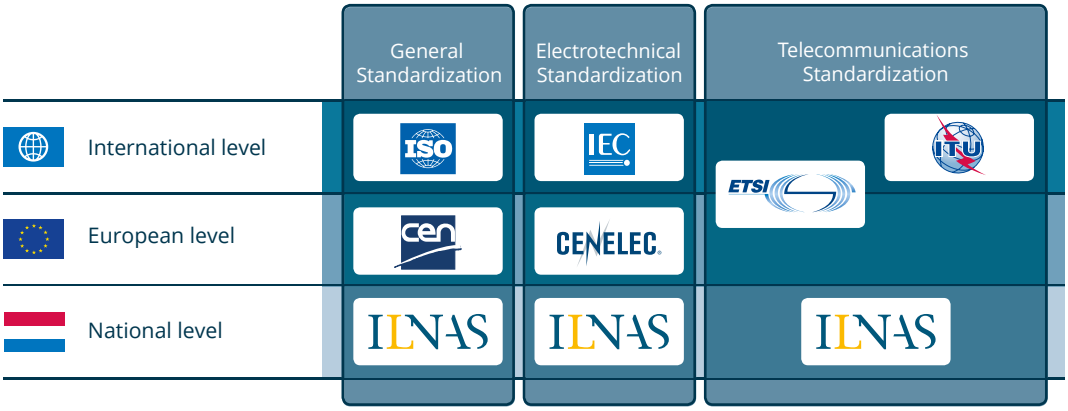

Figure 15: Relative positioning of the main standards developing organizations

5.2.1. ISO and IEC Standardization Committees

ISO is the world's dominant developer and publisher of International Standards in terms of scope. It has over 24,000 standards published and more than 4,000 standards under development[64]. ISO is in charge of developing International Standards for all industry sectors.

IEC prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology".

To prevent an overlap in standardization work related to information technology, ISO and IEC formed a Joint Technical Committee in 1987 known as ISO/IEC JTC 1 Information technology. It has taken a leading role in ICT standardization in the last few years with the creation of working groups and technical subcommittees directly responsible for the development of ICT International Standards

5.2.2. CEN and CENELEC Standardization Committees

CEN and CENELEC are two official European Standards Organizations (ESOs) closely collaborating through a common CEN-CENELEC Management Centre since 2010. They are notably in charge of developing ICT standards at the European level. Even if most of the ICT-related topics are being tackled at the international level by ISO/IEC JTC 1, complying with the Vienna Agreement set up between CEN and ISO, as detailed below, CEN and CENELEC have technical committees and additional other groups active in different areas of the ICT sector directly under their supervision. The standardization activities of CEN and CENELEC are detailed in an annual common Work Program[65], the latest of which was published in January 2023.

5.2.3. ETSI - European Telecommunications Standards Institute

ETSI is a leading standardization organization for ICT standards fulfilling European and global market needs. The European Union officially recognizes ETSI as an ESO. ETSI is active in ten ICT "sectors", regrouping a number of technical committees and covering a wide range of technologies, namely: Home and Office, Better living with ICT, Content Delivery, Networks, Wireless Systems, Transportation, Connecting Things, Interoperability, Public Safety and Security[66]. The standardization activities of ETSI are detailed in an annual Work Program [59], whose last edition is covering the period 2022/2023.

64 https://www.iso.org/iso-in-figures.html

65 https://www.cencenelec.eu/media/CEN-CENELEC/News/Publications/2023/workprog2023.pdf

66 https://www.etsi.org/technologies

5.2.4. ITU-T - International Telecommunication Union - Telecommunication Standardization Sector

ITU is the United Nations specialized agency for information and communication technologies. It has three main areas of activity organized in Sectors, including ITU-T, the ITU's Telecommunication Standardization Sector, which brings together experts from around the world to develop international standards known as ITU-T Recommendations, which cover defining elements in the global infrastructure of ICT. ITU-T is currently composed of 11 Study Groups working on different aspects of ICT[67].

5.2.5. Cooperation between standards-developing organizations

Several bridges exist between the national, European and international standardization organizations in order to facilitate the collaboration and coordination of standardization work in the different fields. Indeed, in order to ensure transparency in the work, prevent standards duplication, and avoid conflicting requirements, agreements have been established between international and European standardization organizations.

In 1991, ISO and CEN signed the Vienna Agreement[68], which is based on the following guiding principles:

- Primacy of international standards and adoption of ISO Standards at the European level (EN ISO);
- Work at the European level (CEN), if there is no interest at the international level (ISO);
- When a given project undergoes parallel development, procedures are in place ensuring standardization documents of common interest are approved by both organizations (ISO and CEN).

Similarly, CENELEC and IEC signed the Dresden Agreement in 1996 with the aim of developing intensive consultations in the electrotechnical field. This agreement was superseded by the Frankfurt Agreement[69] in 2016 with the aim to simplify the parallel voting processes, and increase the traceability of international standards adopted in Europe thanks to a new referencing system. It is intended to achieve the following guiding principles:

- Development of all new standardization projects by IEC (as much as possible);
- Work at the European level (CENELEC), if there is no interest at the international level (IEC);
- When a given project undergoes parallel development, ballots for relevant standardization documents are organized simultaneously by both organizations (IEC and CENELEC).

Under both agreements, 34% of all European standards ratified by CEN, as well as 74% of those ratified by CENELEC, are respectively identical to ISO or IEC standards[70]. In that respect, the European and international organizations do not duplicate work.Similarly, ITU-T and ETSI have agreed on a Memorandum of Understanding (MoU)[71] in 2000, lastly renewed in 2016, that paves the way for European regional standards, developed by ETSI, to be recognized internationally.

67 https://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx

68 https://boss.cen.eu/media/CEN/ref/vienna_agreement.pdf

69 https://www.cencenelec.eu/media/Guides/CLC/13_cenelecguide13.pdf

70 https://www.cencenelec.eu/stats/CEN_CENELEC_in_figures_quarter.htm

71 https://www.itu.int/en/ITU-T/extcoop/Documents/mou/MoU-ETSI-ITU-201605.pdf

5.3. ILNAS and ANEC GIE in technical standardization

5.3.1. ILNAS

One of ILNAS' missions, as the Grand Duchy's only national standardization body, is to promote technical standardization.

ILNAS organizes its standardization work according to the 2020-2030 national standardization strategy[72], and associated ICT[73], Construction[74], Aerospace[75], and CASCO[76] national technical standardization policies. Overall, the objectives are to make standards available to the national market, raise awareness on the use of technical standards, promote active participation of national stakeholders in the development and publication of standards, enhance Luxembourg's international visibility in standardization, and develop strong links between standardization, scientific research and education.

5.3.2. ANEC GIE

The ANEC GIE *(Agence pour la normalisation et l'économie de la connaissance)* is an economic interest group whose partners are the Ministry of the Economy, the *Chambre des métiers* and the *Chambre de commerce*. One of its main roles is to support ILNAS in its standardization missions. In particular, it assists ILNAS in implementing the national standardization policies. In practice, this entails pursuing the following activities:

- Regularly informing the national market of the latest technical standardization developments;
- Actively promoting the use of standards and the benefits of participating in the standards development process;
- Animating trainings on technical standardization in relation to technologies of interest;
- Supporting ILNAS in the production of national deliverables, such as white papers, national technical standardization reports, topic-specific standards analyses, etc.;
- Supporting ILNAS in its efforts to strengthen the ties between technical standardization, scientific research, education, and innovation, namely through research programs between ILNAS and the University of Luxembourg[77], and participation in the MTECH Master's degree (Technopreneurship: mastering smart ICT, standardization and digital trust for enabling next generation of ICT solutions[78]).

72 https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-luxembourgeoise-2020-2030.html

73 https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2022-2025.html

74 https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-du-secteur-de-la-construction-2020-2025.html

75 https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-du-secteur-de-l-aerospatial-2021-2025.html

76 https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-normative-nationale-iso-casco-2022-2030.html

77 https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/normalisation-recherche.html

78 https://www.uni.lu/fstm-en/study-programs/master-in-technopreneurship/

5.4. Standardization committees relevant to Digital Trust

In Table 3 we regroup a few of the main technical standardization committees that published, or are working on, the standards or projects that are mentioned in this report. More details on many of these committees can be found directly at their websites, or in other ILNAS publications such as the Standards Analysis on ICT.

Committee	Level	Scope extract or other description
ISO/IEC JTC 1 Information technology[79]	International	Standardization in the field of information technology.
ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection[80]	International	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: ● Security requirements [...]; ● Management of information and ICT security [...]; ● Cryptographic and other security mechanisms [...]; [...] ● Security aspects of identity management [...] and privacy; ● Conformance assessment [...] of information security management systems; ● Security evaluation criteria and methodology. [...]
ISO/CASCO ISO committee for conformity assessment[81]	International	CASCO is the ISO committee responsible for conformity assessment in ISO. CASCO develops policy and publishes standards related to conformity assessment, but it does not perform conformity assessment activities.
ISO/TC 171/SC 1 Quality, preservation and integrity of information[82]	International	● Control processes ● Quality of input and output ● Production control, statistical evaluations ● Physical aspects of storage and preservation (short and long term) ● Operating equipment ● Evaluation of characteristics of use ● Qualification of processes ● Terminology – Vocabulary ● Integrity of information
CEN/CLC/JTC 13 Cybersecurity and Data Protection[83]	European	Development of standards for cybersecurity and data protection covering [...] but not limited to: ● Management systems, frameworks, methodologies ● Data protection and privacy ● Services and products evaluation standards suitable for security assessment for large companies and small and medium enterprises (SMEs) ● Competence requirements for cybersecurity and data protection ● Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices [...] Included in the scope is the identification and possible adoption of documents already published or under development by ISO/IEC JTC 1 and other SDOs and international bodies such as ISO, IEC, ITU-T, and industrial fora. [...]

79 https://www.iso.org/committee/45020.html

80 https://www.iso.org/committee/45306.html

81 https://www.iso.org/casco.html

82 https://www.iso.org/committee/53666.html

83 https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2307986,25&cs=1ED41A3D97E9C0D226A9087045F5D181C

CEN/TC 224 Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment[84]	European	The development of standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations and privacy in a multi sectorial environment. It covers: • Operations such as applications and services like electronic identification, electronic signature, payment and charging, access and border control; • Personal devices with secure elements independently of their form factor, such as cards, mobile devices, and their related interfaces; • Security services including authentication, confidentiality, integrity, biometrics, protection of personal and sensitive data; • System components such as accepting devices, servers, cryptographic modules; CEN/TC 224 multi-sectorial environment involves sectors such as Government/Citizen, Transport, Banking, e-Health, as well as Consumers and providers from the supply side such as card manufacturers, security technology, conformity assessment body, software manufacturers.
ETSI TC CYBER Cybersecurity[85]	European	Broad topics of work that are covered in the TC CYBER Roadmap include: • Understanding the cybersecurity ecosystem; • Protection of personal data and communication; • Consumer Mobile and IoT security and privacy; • Cybersecurity for critical national infrastructures; • Network Security; • Cybersecurity tools and guides; • Direct support to EU legislation; and • Quantum-safe cryptography.
ETSI TC ESI Electronic Signatures and Infrastructures[86]	European	The committee deals with digital signatures and related trust services. This activity covers the format of digital signatures, as well as procedures and policies for creation and validation. TC ESI also covers policy, security and technical requirements for trust service providers (TSP) such as certification authorities, time-stamping authorities, TSP providing remote signature creation or validation functions, registered e-delivery providers, and long-term data preservation providers. [...]
ILNAS/TC 106 Archivage électronique	National	ILNAS/TC 106 was founded in 2018 with the aim of developing a national standard on digitization and e-archiving that can serve as the basis for the certification of PSDCs.

Table 3: International, European, and national standardization committees encountered in this report

84 https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:6205&cs=1E59B4D3EFD280E27AAC0C16CC13CD4FD

85 https://www.etsi.org/committee/cyber

86 https://www.etsi.org/committee/esi

5.5. Participating in technical standardization

In its capacity of NSB for Luxembourg, ILNAS (supported by the ANEC GIE) is the gateway to technical standardization for the country in ISO, IEC, CEN, and CENELEC.

5.5.1. Benefits

Participating in technical standards development has multiple advantages.

Gain advanced knowledge on future specifications. Future products in your field may be influenced by a widely accepted standard. Advanced knowledge of this aids in proactively adapting to the market.

Shape standards according to your needs and knowhow. Standards are a way to spread your ideas and requirements, not just as a way to remain competitive, but also to enhance the value of your expertise and making it known to a wide range of stakeholders.

Gain access to a strategic network of experts. Participating grants access to a larger pool of technical expertise, and knowing who works in standardization sheds further light on current and future interests of partners and competitors.

5.5.2. How to get involved in Luxembourg

ILNAS offers the possibility for nationally established organizations to register actively participating delegates within ISO, IEC, CEN, and CENELEC technical committees (and working groups) free-of-charge. ILNAS also offers support and coaching to new delegates, in order to assist them in their standardization needs. Roles held by delegates can range from being a simple expert that comments and votes on projects to more involved task such as proposing new work items and leading the editing of projects. It only depends on the time one wishes to grant to these activities.

The full range of ILNAS' service related to technical standardization in support of the national market can be found on the *Portail Qualité*[87].

87 https://portail-qualite.public.lu/fr/normes-normalisation.html

6

6 Conclusion and outlook

6. Conclusion and outlook

This white paper gives an overview of ILNAS' legal missions and tasks related to the digital trust market in Luxembourg, stemming from European Union and national developments.

Trust service providers. First, ILNAS is the supervisory body for trust service providers in the context of the eIDAS Regulation. The technical foundation of trust service providers is a cryptographic tool know as public key signatures, which can be used to create all sorts of services, such as authenticating website certificates, creating trustworthy electronic timestamps, implementing electronic seals, and running electronic registered delivery. For these tools to not be misused or misconfigured, the entities proposing them can comply with well-established organizational, security, technical, and quality requirements proposed by the eIDAS framework, in order to earn the status of "qualified trust service provider".

This status is conferred after a process that begins with a formal application made to ILNAS, which has in place a supervision scheme for qualified trust service providers, and also maintains up to date and available to the market the national trusted list.

In this context, ILNAS is also closely monitoring how the proposed revision of the eIDAS Regulation evolves, as this may determine how ILNAS' missions evolve with it, in particular with regards to the upcoming framework for European digital identity wallets, and their relation to future trust services.

Electronic archiving. ILNAS is also the supervisory body in the frame of a national legislation and technical scheme in the area of e-archiving. The legislation is established by Luxembourg's Law of 25 July 2015 on electronic archiving, which grants ILNAS the responsibility of delivering the *"PSDC" (prestataire de services de dématérialisation ou de conservation)* status to entities that demonstrate compliance with the technical framework and overall scheme.

The framework and scheme are laid out in the national standard ILNAS 106 *Archivage électronique - Référentiel d'exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC),* which is grounded in the ISO/IEC 27000 family of standards.

Entities wishing to earn the PSDC status have to launch this process via ILNAS.

Cybersecurity certification. Third, ILNAS has been nominated as Luxembourg's National Cybersecurity Certification Authority in charge of supervision activities in the context of the European Cybersecurity Act. Thus, once the first schemes are activated and certifications begin being issued, ILNAS will be in charge of monitoring that the ICT products, ICT services, ICT processes, and possibly also managed security service providers that are certified comply with the schemes. This will be done via a precise supervision procedure that is still under elaboration, and in collaboration also with OLAS, another department of ILNAS serving as the national accreditation body.

Technical standardization. Finally, ILNAS serves as Luxembourg's only national standards body. As such, it is the gateway for national market actors to get involved in the technical standardization process. This can be a very useful activity to undertake for those actors who wish to influence norms that are often at the technical heart of the frameworks such as those defined by eIDAS, the Luxembourg e-archiving law, and the Cybersecurity Act. Furthermore, the reach extends even beyond those frameworks, as we have seen that often new legislation builds on that which is already in place, as seen for instance with how the CSA may serve in the contexts of the AI Act, the Cyber Resilience Act, or the NIS2 Directive.

As its missions evolve, ILNAS continues to inform the national market of these evolutions, through various other activities:

- the publication of news items on the Portail Qualité: https://portail-qualite.public.lu/fr/actualites.html;
- the publication of technical reports or white papers such as this one, but also the most recent on Technical Standardization and Quantum Technologies [4], or the latest edition of the ICT Sector Standards Analysis [62];
- educational activities, for instance the continued involvement in the Master in Technopreneurship: "mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions"[88], or courses given in the context of the Digital Learning Hub[89], e.g. "Introduction to trust services, including electronic signatures"[90]; and
- research activities, for example the ongoing research program "Technical Standardization for Trustworthy ICT, Aerospace, and Construction (2021-2024)"[91].

More information on ILNAS and its market outreach can be found on the *Portail Qualité*[92].

88 https://www.uni.lu/fstm-en/study-programs/master-in-technopreneurship/

89 https://dlh.lu/

90 https://portail-qualite.public.lu/fr/actualites/confiance-numerique/2022/ilnas-propose-cours-sur-services-de-confiance-cadre-digital-learning-hub.html

91 https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/normalisation-recherche.html

92 https://portail-qualite.public.lu/fr.html

References

[1] ILNAS, "Trust Services under the eIDAS Regulation," [Online]. Available: https://portail-qualite.public.lu/fr/publications/confiance-numerique/etudes/trust-services-under-the-eidas-regulation.html.

[2] ILNAS, "An Introduction to the e-Archiving Framework in Luxembourg," [Online]. Available: https://portail-qualite.public.lu/fr/publications/confiance-numerique/etudes/e-archiving-framework-luxembourg.html.

[3] ILNAS and Ministry-of-the-Economy, "White Paper Digital Trust September 2017," [Online]. Available: https://portail-qualite.public.lu/fr/publications/confiance-numerique/etudes/white-paper-digital-trust-september-2017.html.

[4] ILNAS and ANEC GIE, "Quantum technologies and technical standardization" [Online]. Available: https://portail-qualite.public.lu/dam-assets/publications/normalisation/2023/report-technical-standardization-quantum-technologies-november-2023.pdf

[5] ILNAS and ANEC GIE, "ILNAS White Paper Artificial Intelligence and Technical Standardization," [Online]. Available: https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-artificial-intelligence-and-technical-standardization.html.

[6] ILNAS, University of Luxembourg, ANEC GIE and SnT, "White paper Trustworthiness in ICT, Aerospace, and Construction applications - Scientific Research and Technical Standardization - October 2023," [Online]. Available: https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/white-paper-trustworthiness-in-ict-aerospace-and-construction-applications-scientific-research-and-technical-standardization-october-2023.html.

[7] European-Union, "European Declaration on Digital Rights and Principles," [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

[8] STATEC, "Répertoire des entreprises luxembourgeoises 2020," [Online]. Available: https://statistiques.public.lu/fr/publications/series/repertoire-entreprises/2020/repertoire-2020.html.

[9] European-Commission, "The Digital Economy and Society Index (DESI)," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/desi.

[10] European-Union, "The EU's Cybersecurity Strategy for the Digital Decade," [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[11] "Regulation EU no 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," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

[12] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281.

[13] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E," [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[14] "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 52," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[15] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208.

[16] HCPN, "Stratégie nationale de cybersécurité IV," [Online]. Available: https://hcpn.gouvernement.lu/fr/publications/strategie-nationale-cybersecurite-4/strategie-nationale-cybersecurite-4.html.

[17] Legilux, "Loi du 23 décembre 2022 portant modification: 1) de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS; 2) de la loi modifiée du 17 mai 1882 sur les poids et mesures ; 3) de la loi du 26 janvier 1922 portant certaines modifications au ser," [Online]. Available: https://legilux.public.lu/eli/etat/leg/loi/2022/12/23/a686/jo.

[18] Legilux, "Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification: 1. de l'article 1334 du Code civil; 2. de l'article 16 du Code de commerce; 3. de la loi modifiée du 5 avril 1993 relative au secteur financier," August 2015. [Online]. Available: http://legilux.public.lu/eli/etat/leg/loi/2015/07/25/n1/jo.

[19] "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999L0093.

[20] Legilux, "Loi modifiée 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," July 2014. [Online]. Available: http://legilux.public.lu/eli/etat/leg/loi/2014/07/04/n2/jo.

[21] "Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices," [Online]. Available: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd.

[22] "Loi du 19 juin 2013 relative à l'identification des personnes physiques," [Online]. Available: https://legilux.public.lu/eli/etat/leg/loi/2013/06/19/n3/jo.

[23] "ETSI SR 019 050 V1.1.1 (2015-06) Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures," [Online]. Available: https://www.etsi.org/deliver/etsi_sr/019000_019099/019050/01.01.01_60/sr_019050v010101p.pdf.

[24] "ETSI EN 319 412-5 V2.4.0 (2023-06) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements," [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.04.00_20/en_31941205v020400a.pdf.

[25] "Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015L2366.

[26] "ETSI TS 119 612 V2.2.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Trusted Lists," [Online]. Available: https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf.

[27] "International Organization for Standardization. ISO/IEC 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services. International Organization for Standardization," [Online]. Available: https://www.iso.org/standard/46568.html.

[28] "ETSI EN 319 403-1 V2.3.1 (2020-04) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers," [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31940301/02.03.01_30/en_31940301v020301v.pdf.

[29] "ILNAS – Digital Trust Department. ILNAS/PSCQ/Pr001 – Supervision of qualified trust service providers (QTSPs)," [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/confiance-numerique/surveillance-psc/procedures/ilnas-pscq-pr001-supervision-en/ilnas-pscq-pr001-supervision-en.pdf.

[30] "CEN/TS 419 261:2015 Security requirements for trustworthy systems managing certificates and time-stamps," [Online]. Available: https://ilnas.services-publics.lu/ecnor/displayStandard.action?id=118703.

[31] "Commission implementing decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of eIDAS Regulation," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0005.

[32] "EU/EEA Trusted List Browser," [Online]. Available: https://esignature.ec.europa.eu/efda/tl-browser.

[33] "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/1925/oj.

[34] ILNAS, "ILNAS 106:2022 - Archivage électronique - Référentiel d'exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC)," 2022. [Online]. Available: https://portail-qualite.public.lu/dam-assets/fr/normes-normalisation/achat-consultation-normes/normes-nationales/pr-ilnas-106.pdf.

[35] ISO/IEC, ISO/IEC 17021-1:2015: Conformity Assessment – Requirements for Bodies Providing Audit and Certification of Management Systems – Part 1: Requirements, Geneva, Switzerland: International Organization for Standardization, 2015.

[36] ISO/IEC, ISO/IEC 27006:2015: Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, Geneva, Switzerland: International Organization for Standardization, 2015.

[37] Legilux, "Loi modifiée du 5 avril 1993 relative au secteur financier," April 1993. [Online]. Available: http://data.legilux.public.lu/eli/etat/leg/loi/1993/04/05/n1/jo.

[38] Legilux, "Règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er de la loi du 25 juillet 2015 relative à l'archivage électronique," July 2015. [Online]. Available: http://legilux.public.lu/eli/etat/leg/rgd/2015/07/25/n1/jo.

[39] Legilux, "Règlement grand-ducal du 7 août 2023 modifiant le règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique.," 2023. [Online]. Available: https://legilux.public.lu/eli/etat/leg/rgd/2023/08/07/a500/jo.

[40] ILNAS – Digital Trust Department, "ILNAS/PSDC/Pr001 – Supervision of Digitisation or E-Archiving Service Providers (PSDCs)," [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/confiance-numerique/surveillance-psc/procedures/ilnas-pscq-pr001-supervision-en/ilnas-pscq-pr001-supervision-en.pdf.

[41] ISO/IEC, ISO/IEC 17000:2020: Conformity assessment – Vocabulary and general principles, Geneva: International Organization for Standardization, 2020.

[42] ILNAS, "List of PSDCs," [Online]. Available: https://portail-qualite.public.lu/fr/confiance-numerique/archivage-electronique/liste-psdc.html.

[43] ILNAS – Digital Trust Department, "ILNAS/PSDC/F001A - Notification for supervision of digitization or e-archiving service providers (PSDCs)," [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/confiance-numerique/surveillance-psdc/formulaires/ilnas-psdc-f001a-notification-for-supervision-en/ilnas-psdc-f001a-notification-en.docx.

[44] ISO/IEC, ISO/IEC 27000:2018: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, Geneva, Switzerland: International Organization for Standardization, 2018.

[45] ISO/IEC, ISO/IEC 27001:2013: Information Technology – Security Techniques – Information Security Management Systems – Requirements, Geneva, Switzerland: International Organization for Standardization, 2013.

[46] ISO/IEC, ISO/IEC 27002:2013: Information Technology – Security Techniques – Code of Practice for Information Security Controls, Geneva, Switzerland: International Organization for Standardization, 2013.

[47] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," Journal of Information Security, vol. 4, 2013.

[48] ENISA, "Cybersecurity Certification: Candidate EUCC Scheme V1.1.1," [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.

[49] ISO/IEC, "ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security," [Online]. Available: https://www.iso.org/standard/72891.html.

[50] ISO/IEC, "ISO/IEC 18045:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation," [Online]. Available: https://www.iso.org/standard/72889.html.

[51] ISO/IEC, "ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories," [Online]. Available: https://www.iso.org/standard/66912.html.

[52] ISO/IEC, "ISO/IEC TS 23532-1:2021 - Information security, cybersecurity and privacy protection - Requirements for the competence of IT security testing and evaluation laboratories - Part 1: Evaluation for ISO/IEC 15408," [Online]. Available: https://www.iso.org/standard/77199.html.

[53] ISO/IEC, "ISO/IEC 19896-1 IT security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements," [Online]. Available: https://www.iso.org/standard/71120.html.

[54] ISO/IEC, "ISO/IEC 19896-3:2018 IT security techniques – Competence requirements for information security testers and evaluators – Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators," [Online]. Available: https://www.iso.org/standard/71122.html.

[55] ENISA, "European Cybersecurity Certification Scheme for Cloud Services," [Online]. Available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

[56] ISO/IEC, "ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services," [Online]. Available: https://www.iso.org/standard/43757.html.

[57] IAASB, "2018 Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements," [Online]. Available: https://www.iaasb.org/publications/2018-handbook-international-quality-control-auditing-review-other-assurance-and-related-services.

[58] "Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 200," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2012/1025/oj.

[59] ETSI, "ETSI Work Program 2022-2023," [Online]. Available: https://www.etsi.org/e-brochure/Work-Programme/2022-2023/mobile/index.html#p=1

[60] ISO/IEC. ISO/IEC 9798-1:2010: Information technology – Security techniques – Entity authentication – Part 1: General

[61] Legilux, "Règlement grand-ducal du 21 septembre 2017 modifiant le règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique," August 2015. [Online]. Available: http://legilux.public.lu/eli/etat/leg/rgd/2017/09/21/a865/jo

[62] ILNAS and ANEC GIE, Standards Analysis, ICT Sector, Luxembourg, v13.0, [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2023/standards-analysis-ict-sector-luxembourg-v13-0.pdf


COLLABORATION
PARTNER
OFFICE
SERVICE
EXCELLENCE
INDUSTRIAL
COLLABORATION

WHITE PAPER · DIGITAL TRUST · TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET · Version 4.0 · December 2023 · © ILNAS/ANEC · ISSN 2354-4996

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -00 · Fax : (+352) 24 79 43 -00 · E-mail : info@ilnas.etat.lu

www.portail-qualite.lu