June 2012

WHITE PAPER

DIGITAL TRUST

TOWARDS EXCELLENCE IN ICT

ILNAS
Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services

&

tudor
PUBLIC RESEARCH CENTRE HENRI TUDOR

Acknowledgments

The ***I**nstitut **L**uxembourgeois de la **N**ormalisation, de l'**A**ccréditation, de la **S**écurité et qualité des produits et services* (ILNAS) would like to acknowledge the Public Research Centre Henri Tudor for the work done on the establishment of the two first chapters of the white paper.

ILNAS also thanks the Ministry of the Economy and Foreign Trade *(Direction du commerce électronique et de la sécurité informatique)* for its contribution on the third chapter on digital trust through information security.

ILNAS also thanks the external peer reviewers, mainly the members of the electronic signature board and the chairpersons of the national mirror committees of the ISO/IEC JTC1 subcommittees, for their comments and suggestions.

Finally, ILNAS would like to thank both the members of ANEC (*Agence pour la Normalisation et l'Economie de la Connaissance*) and of the ILNAS digital trust department for their continuous availability on the white paper.

Table of Contents

Foreword

The *Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services* (ILNAS) is a public administration under the supervision of the Minister of the Economy and Foreign Trade in Luxembourg. It was created based on the law of May, 20th 2008, and started its operations on June, 1st 2008.

For reasons of complementarity, effectiveness, transparency and for an administrative simplification purpose, ILNAS is in charge of several administrative and technical tasks that were previously under the responsibility of different public structures. These assignments were strengthened and new tasks are now assigned to ILNAS. ILNAS thus corresponds to a network of skills for competitiveness and consumer protection.

The Digital Trust department, embodied in ILNAS, pursues excellence in information and communication technology by achieving quality and security. Thus, the Digital Trust department has two major missions.

First, the Digital Trust department manages the follow-up and promotion of the instruments of accreditation and certification of digital trust. In this regard this department guarantees the constant development of the quality system of the Certification Services Providers (CSP) in the general sector of PKI (Public Key Infrastructure). The Digital Trust department of ILNAS is also participating in the management and development of the future national instruments of accreditation and notification of digital trust (e.g., records management).

Second, the Digital Trust department of ILNAS represents an information and exchange network for Information and Communication Technology (ICT) standardization knowledge, by assuring the chair of the national forum of (ICT) standardization entitled ISO/IEC JTC1.

This mission aims to achieve excellence in the ICT sector and beside to support the national (digital) economy in order to remain competitive and effective.

The main goals concerning the Digital Trust department are:

- The guarantee of the systems of PKI at the national level in a transparent, fast, efficient and non discriminatory way;
- The recognition of the quality of the department's performance at the national, European and international level;
- The promotion of digital trust at a national level;
- The satisfaction of the department's partners which are associated in the procedures of digital trust;
- The promotion of digital trust as a tool for developing economic growth.

In the frame of the Digital Trust department development, ILNAS ordered a research project to the CRP Henri Tudor named NormaFi-IT. This research project had four main objectives:

- To define what digital trust is and what the digital trust underlying concepts are;
- To identify what are the tools and methods helping to improve digital trust in Luxembourg (PKI, records management, business continuity management, etc.);
- To develop a normative knowledge-based Economy in order to establish the links between standards, digital trust, innovation and competitiveness;
- To support and develop standardization activities currently in progress in Luxembourg, mainly related to the field of ICT, for delegates involved in technical committees and users of standards.

This white paper presents the main results of this research project.

Jean-Marie REIFF
Jean-Philippe HUMBERT

Abbreviations

AFNOR	Association Française de Normalisation
AIP	Archival Information Package
ANEC	Agence pour la Normalisation et l'Economie de la Connaissance
ANSI	American National Standards Institute
APLAC	Asia Pacific Laboratory Accreditation Cooperation
APT	Advanced Persistent Threats
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BS	British Standard
BSI	British Standards Institution
CA	Certification Authority
CAB	Conformity Assessment Body
CASCO	Committee for conformity Assessment
CASES	Cyberworld Awareness and Security Enhancement Structure
CC	Certification Committee
CCSDS	Consultative Committee for Space Data Systems
CD	Committee Draft
CD-ROM	Compact Disc - Read Only Memory
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CIRCL	Computer Incident Response Center Luxembourg
CRL	Certificate Revocation List
CSP	Certification Services Providers
CSS	Code de la Sécurité Sociale
CSSF	Commission de Surveillance du Secteur Financier
DAPS	Distributed Application Platforms and Services
DIN	Deutsches Institut für Normung e. V.
DIP	Dissemination Information Package
DIS	Draft International Standard
DLM	Document Lifecycle Management
DRP	Disaster Recovery Plan
EA	European co-operation for Accreditation
EDM	Electronic Document Management
EDRMS	Electronic Document and Records Management System
EESSI	European Electronic Signature Standardization Initiative
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency

ERM	Electronic Records Management
ERMS	Electronic Records Management Systems
ETSI	European Telecommunications Standards Institute
FDIS	Final Draft International Standard
GDP	Gross Domestic Product
GNP	Gross National Product
HHC	Horizontal Harmonization Committee
IAAC	Inter American Accreditation Cooperation
IAF	International Accreditation Forum
IC	Inspection Committee
ICA	International Council on Archives
ICT	Information and Communication Technology
ICT DR	Information and Communication Technology Disaster Recovery
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ILAC	International Laboratory Accreditation Cooperation
ILNAS	Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services
IP	Internet Protocol
IPOCM	Incident Preparedness and Operational Continuity Management
IRBC	Information and Communication Technology Readiness for Business Continuity
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITSC	Information Technology Service Continuity
ITSCM	Information Technology Service Continuity Management
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector
IWA	International Workshop Agreement
JTC	Joint Technical Committee
LC	Laboratory Committee
LDAP	Lightweight Directory Access Protocol
LuSI	Luxembourg Safer Internet
MAC	Multilateral Agreement Council
MBCO	Minimum Business Continuity Objective
MiFID	Markets in Financial Instruments Directive 2004/39/EC
MLA	Multilateral Agreements
MLQ	Mouvement Luxembourgeois pour la Qualité
MoReq	Model Requirements for the Management of Electronic Documents and Records
MoReq2010	Modular Requirements for Records Systems
MRA	Mutual Recognition Arrangements
MSR	Management System for Records
MSS	Management System Standards
NAB	National Accreditation Body

NBN	Bureau de normalisation
NP	New Work Item Proposal
NSB	National Standards Body
OAIS	Open Archival Information System
OASIS	Organization for the Advancement of Structured Information Standards
OCR	Optical Character Recognition
OCSP	Online Certificate Status Protocol
OLAS	Office Luxembourgeois d'Accréditation et de Surveillance
PAC	Pacific Accreditation Cooperation
PAS	Publicly Available Specification
PDCA	Plan-Do-Check-Act
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PSDC	Prestataire de Services de Dématérialisation et de Conservation
PSF	Professionals of the Financial Sector
RA	Registration Authority
RM	Records Management
RMS	Records Management System
RTO	Recovery Time Objective
SADC	South African Development Cooperation in Accreditation Committy
SC	Subcommittee
SCADA	Supervisory Control And Data Acquisition
SDO	Standards Development Organization
SEM	Structural Equation Modeling
SIP	Submission Information Package
SME	Small-to-Medium Enterprise
Smile GIE	Security Made In Lëtzeburg Groupement d'Intérêt Economique
SNJ	Service National de la Jeunesse
SSO	Single Sign-On
SWG	Special Working Group
TC	Technical Committee
TLS	Transport Layer Security
TR	Technical Report
TS	Technical Specification
W3C	World Wide Web Consortium
WD	Working Draft
WG	Working Group
WORM	Write One Read Many

Introduction

This white paper presents an overview of the essential knowledge useful to understand why the concept of digital trust is important. Today, ICT is predominant and constitutes a keystone of our economy. ICT can be considered as a horizontal support of all the other sectors in the world-wide economy. But finally how can we consider this economy in its development without a clear digital trust in place? That is the reason why in the current fast moving world, trust is no more a concept only to consider in physical exchanges, but also in the digital ones.

However, digital trust is still an emerging topic and very few analyses have already been published, although it is a very active domain. Indeed, for example, in the digital agenda for Europe, trust and security is one of the main topics. Many projects and events are organized in this frame by the European Commission. In the same frame, a lot of initiatives have been developed in order to promote and foster different concepts in connection with the notion of digital trust. One of these, at the national level was the creation, in 2008, of the digital trust department of ILNAS, with the main mission of the accreditation of Certification Service Providers (PKI). In the new ILNAS bill, the assignments of the Digital Trust department of ILNAS are strengthened (e.g. the accreditation of PSDC), showing the growing importance of this topic. In this context, as a clear output of the research project "NormaFi-IT", the publication by ILNAS of a white paper on the topic of digital trust and its links with the national economy has been seen as relevant.

It is important to mention the fact that standardization is a real force multiplier for ICT innovation, and that is what ISO/IEC JTC1 permits to bring at the international level. We must not underestimate this potential that is the reason why ILNAS has taken the national presidency of that international standardization committee, as a participating member: "ISO/IEC JTC1 is the place where the basic building blocks of new technologies are defined and where the foundations of important ICT infrastructures are laid"[1]. This activity, *inter alia*, is especially supported by the Ministry of the Economy and Foreign trade, because it is levering the competitiveness of organizations in Luxembourg.

The main purpose of the white paper is to investigate and develop the knowledge areas of digital trust. The main topics developed here are thus the concept of digital trust and the tools and techniques allowing the digital trust improvement in Luxembourg. The white paper is built on four main chapters. Chapters 1 and 2 are results of a research project conducted by the Public Research Centre Henri Tudor. Chapters 3 and 4 are statements provided by national public authorities.

The first chapter is about the concept of digital trust. An introduction to this concept is proposed based on a multi-disciplinary state-of-the-art. A deep analysis of digital trust is performed trough the study of the scientific literature in the domain. The theory is presented and associated models of digital trust are then defined. Finally, the chapter concludes with the current challenges.

The second chapter of the white paper is about technical tools for digital trust. Three tools, that are currently relevant for Luxembourg, are identified and presented. The first one is Public Key Infrastructures (PKI) and electronic signature. The second tool explained is electronic records

[1] *http://www.iso.org/iso/fr/pressrelease.htm?refid=Ref1505&utm_source=ISO&utm_medium=RSS&utm_campaign=News*

management. Finally, business continuity management is introduced and the main standards in the domain are depicted.

The third chapter deals with information security, that is a cornerstone for digital trust. In this part, after having defined how information security can contribute to digital trust, the strategy of the Ministry of the Economy and Foreign trade in the area of information security is presented. This strategy currently lies on three structures: BEE-SECURE, CASES and CIRCL, that are all described in the chapter.

Finally, the fourth chapter is about digital trust through the knowledge of standardization and certification. An introduction to Information and Communication Technology (ICT) international standards is done and the development of standards through the standardization process is explained. The second section is about certification and accreditation, defining together a trust scheme. Both of these domains are monitored by ILNAS.

1 Digital trust, a definition and an introduction to the concept

Trust is involved in all bilateral relationships where an exchange takes place, whether it is monetary, contractual, amicable, or implicit. When someone purchases a consumer good, or simply asks directions from a stranger on the street, there is an exchange: financial resources for the ownership of the consumer good in the first case, and information for the "*pleasure of helping*" in the second. These two examples, purposefully extreme, show that in each case the individual must take a decision: the decision to purchase the consumer good or not in the first case, and the decision whether to follow the advice provided by a person met by chance in the second.

The challenge is to understand how the individual decides to accept or reject the terms of the exchange. This is the general concern of decision theory. The theory starts from the assumption that every decision generates positive or negative consequences, which the individual, who we shall call "the decision-maker", may then anticipate with greater or lesser certainty. A *priori*, the consumer has no guarantee of the final quality of the consumer good or the accuracy of the information provided.

Now, negative consequences may be significant: in the first example, the consumer may purchase and consume a product of poor quality or one that is even dangerous to his health. In sum, when the decision-maker takes a decision, he runs the risk of suffering negative consequences. In order to protect himself against the negative consequences of a decision, the decision-maker must be able to identify and measure all the possible outcomes of each of his decisions. To do this, he must mobilize all relevant information that he has in order to weigh each decision.

It is from this information that the decision-maker will determine his behavior and decide whether or not to accept the terms of the transaction. Now, without exception, the decision-maker is in a situation of relative ignorance. In the case of the consumer, relative ignorance may for example bear upon the reliability of the vendor, the quality of the product, or even the extent of after-sales service. Acquiring new information means partially reducing this relative ignorance.

As part of a transaction between the decision-maker and his exchange partner (vendor, producer, employee, etc.) the decision-maker must acquire information that can be grouped into three categories:

- **Information about the exchange partner:** his honesty, competence, reliability, reputation, etc.
- **Information about the product** that is the object of the exchange, whether a consumer good, producer good, or service: its qualities, availability, and compatibility.
- **Information on payment terms:** the payment method, payment date, or the level of payment security, etc.

But this information may be more or less reliable, available, or expensive. In fact, information is certainly similar to a consumer good: it can be bought and exchanged for a certain price (for example, consulting or audit firms sell information) but nonetheless it has its own characteristics. In particular, its real value is known only upon purchase, and its quality, upon usage. Information is also a good whose production cost may be high, but for which the reproduction and duplication cost is very low, and it can be reproduced or duplicated almost infinitely. These uncertainties about the value and

quality of information imply that, before deciding to accept the terms of a transaction or not, the decision-maker must decide whether or not the available information is credible.

This is the level of analysis at which trust comes in. In fact, it is because the future is uncertain that the decision-maker must accumulate information, and it is because the quality of the information is itself uncertain that he must judge whether or not to trust his sources of information. If the future were certain, trust would no longer be of any interest.

I. Why trust?

In order to understand the properties of trust, we must present the consequences of a decision made in a state of ignorance. When the decision-maker must take a decision despite the fact he does not have all the relevant information, decision theory considers him to be in a state of asymmetric information.

1) The consequences of asymmetric information: agent opportunism

Agency theory [1] identifies two problems during a transaction: before the transaction, the decision-maker is faced with the adverse selection phenomenon, and after the transaction, he is faced with the moral hazard phenomenon.

Adverse selection corresponds to situations involving hidden information. In the example of a consumer who wants to purchase a consumer good from a producer, there is adverse selection when the producer knows information about the quality of the product that the consumer does not know. It is then possible for the producer to exploit his information advantage: he may adopt an opportunistic behavior. To continue with our example, if the consumer cannot precisely assess the quality of the product or service that he wants to buy, an opportunistic producer has an interest in overestimating the quality of the product in order to sell it at the highest possible price.

Therefore, the adverse selection phenomenon generates another problem: the consumer is aware of his ignorance; he knows that the price is no longer a precise signal of product quality. On the other hand, he cannot determine whether or not the producer is being opportunistic. By way of caution, the consumer might choose not to trust statements from vendors, whether or not they are honest. "Good" producers are therefore punished by the adverse selection phenomenon: they are unable to sell their products at a fair value because bad producers bring down prices, which is to say below the level at which producing "good quality" is still profitable.

Moral hazard comes after the transaction and corresponds to problems of hidden actions. Even if the decision-maker has accurate knowledge about the quality of the product or service exchanged, he may not be able to ensure that the producer will respect any post-transaction commitments. Problems of moral hazard are typical of employer-employee relationships, or of products that include after-sales service.

The consequences for markets affected by significant structural uncertainty about product quality (organic products, new technologies, and digital products are highly representative of such markets) are then very high. Without any outside intervention, adverse selection and moral hazard phenomena bring these products or services toward a price level that excludes "good producers" from the market, leaving place only for products and services of poor quality.

Therefore, it is essential for good producers to be able to be identified as such, for bad producers to be unable to benefit from these signals, and for these signals to be credible to consumers.

2) Protecting oneself against agent opportunism: transaction costs and trust

Vigilance by the parties to a transaction helps anticipate and predict opportunistic behaviors and thus reduces the negative effects of such behaviors. However, vigilance also has a cost, which is often very high. To illustrate this idea, let us take the example of a transaction where both parties show maximum vigilance.

We can identify three phases in a commercial transaction: the contact phase, the contract phase, and the control phase (Figure 1).

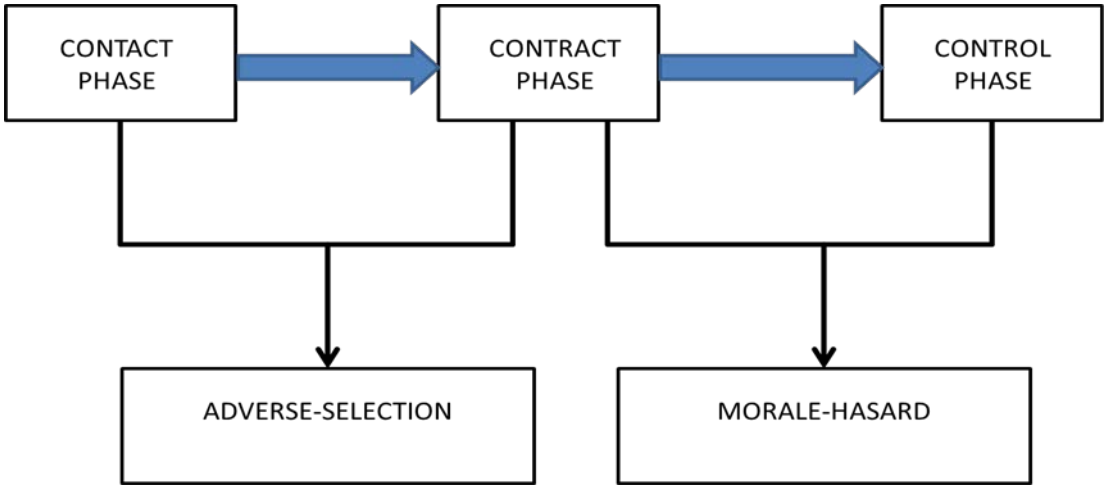

Figure 1: The three phases in a commercial transaction and theirs risks

- During **the contact phase**, the stakeholders in the transaction must protect themselves against problems of adverse selection: they must seek credible information about the reliability of their transaction partners and about the quality of the products exchanged. Depending upon the degree of uncertainty, they must then spend time and money to accumulate information.
- During **the contract phase,** if the parties have judged that there were significant adverse selection of risks, they must also protect themselves against post-transaction moral hazard. The development of the contract and the negotiations concerning shared benefits and related contractual clauses (including the significance of the number of events likely to occur within the relationship) naturally implies a very high cost in terms of time and money.
- Lastly, **the control phase** requires the stakeholders to ensure compliance and the proper execution of the commitments, and potentially the application of sanctions for failure to comply with the contractual clauses.

Thus, for a highly vigilant or extremely paranoid decision-maker, the cost of the smallest transaction may become very high. The significance of the transaction costs, necessary to the proper conduct of business, may then discourage decision-makers who prefer "doing nothing" rather than spending time and money to protect themselves from the opportunistic behavior of economic agents.

Because it allows a reduced level of vigilance, trust facilitates transactions, and therefore reduces transaction costs. In fact, in the first two phases of the transaction, the stakeholders in a transaction will commit fewer resources to protect themselves against opportunistic behaviors (information seeking about the quality of the product exchanged, information seeking about the reliability of the transaction partner, negotiation costs, and contract preparation costs, etc.).

In the post-contractual phase, the parties will have a lower risk of having to incur expenses related to disputes and/or failure to comply with contracts (implementation of control procedures, expenses related to potential legal proceedings, and attorneys fees).

Lastly, a transactional relationship marked by significant trust not only helps reduce the degree of vigilance required to conclude transactions but also allows the stakeholders to commit within a better contract execution dynamic, especially in the case of a long-term contract.

In this sense, trust is a transaction catalyst: by reducing transaction costs, it contributes to a virtuous dynamic in the economy. Understanding the phenomena that govern the process of creating and structuring trust then constitutes an issue that humanities and social science research has attempted to formalize.

II. Defining, formalising, and measuring trust: a complex issue

Trust is a field of research that has always experienced significant academic attention because the concept seems so theoretically fundamental to understand and explain the behavior of individuals and organizations. Undoubtedly a victim of its own success, the conceptual status of trust remains confused and ambiguous, and its definitions vary greatly depending upon the disciplinary field and its applications. The common point remains the concept of uncertainty or ignorance. In this context, trust is a mechanism for coordinating exchanges in a situation of ignorance or uncertainty: it is what helps make decision despite the existence of a risk. This first definition then assumes that an individual will accept being more or less vulnerable to a transaction partner. In general, trust is an "expectation that may or may not be fulfilled" [2].

Then the issue remains of understanding how the expectation of trust is created and structured. This is the level of analysis at which approaches differ. More precisely, these differences bear upon the relationship that individuals have with risk: the perception that individuals have of risk, and the procedures for managing this risk.

Depending upon the case, two types of trust can be distinguished: assured trust (or confidence), and determined trust (or trust).

1) *Assured trust (confidence)*

Trust is acquired *a priori*, without a real risk assessment. In the extreme case, we can talk about "blind trust". Assured trust comes from the fact that individuals believe that the occurrence of the risk is highly improbable and/or the possible drawbacks are minimal in relation to the expected benefits.

Assured trust essentially comes from social structures: for example, citizens generally trust the police and legal institutions with the ability to punish criminals. This trust is called assured in the sense that each person does not systematically carry out a "cost benefit analysis" to decide to trust the authorities.

Sociology explains assured trust as the result of a social construct. From a sociological point of view, trust can come from individual personal experience through regular exchanges, or be founded upon norms or traditions typically stemming from social similarities (ethnic, religious, or professional affiliation), or even from the agreements that structure societies or organizations (laws, codes of good conduct, or internal rules, for example).

The notion of complexity completes the notion of uncertainty: because society is complex by nature, the individual is immersed in this complexity, and must trust to reduce uncertainty. Trust functions to reduce the complexity of modern societies. In this sense, these social structures (norms, traditions, conventions, etc.) are "short cuts" that allow individuals to avoid having to start from the beginning before each decision when faced with uncertainty, as the evaluation process relies upon trust. For example, it is not necessary to know exactly how all institutions that guarantee the proper completion of a commercial transaction operate: simply knowing that these institutions exist, that they are recognized as legitimate, represents a sufficient foundation to take the risk of carrying out a transaction.

In this context, trust is then defined as "the belief in the reliability of a person or system" [3].

2) Determined trust (trust)

Determined trust is the result of a real process of risk assessment, which is to say an evaluation of the expected benefits of a decision and any negative consequences that it may have. In the extreme case, we can talk about calculated trust.

Essentially inspired by economics, this concerns determining the rational components that come into play in creating and structuring trust [4]. Particular attention is paid to predicting individual behaviors through calculations made based on knowledge acquired through experience: the perfectly rational individual would only trust if the likely benefits of a transaction with a partner in a case of "non-opportunism" were greater than the probable losses in a case of opportunism [5].

The article by Knight [6] helps make the distinction between uncertainty and risk by distinguishing several degrees of individual "ignorance" in relation to the future:

- The certain future, where trust is not needed, as the individual has all existing information and is therefore perfectly informed about what will happen.
- The risky future, where the individual has partial information and can therefore identify several possible outcomes based upon objective probabilities.
- The uncertain future, for which the individual cannot predict all possible outcomes. There are only subjective probabilities for anticipating the future.

While assured trust assumes that the realization of risk is highly improbable ("I am *assured* that my expectations will not be disappointed"), determined trust includes a more critical decision-making dimension ("I *decide*" that my expectations will not be disappointed"): the realization of risk is possible, and the individual "bets" that he will not suffer the negative consequences of his decisions.

3) From assured trust to determined trust and vice versa

The distinction between the two types of trust depends upon the individual's ability to distinguish the various degrees of risk (from "derisory" risk to "danger"). However, the relationship between these two forms of trust is a complex research topic, which to date has not been the subject of consensus among researchers.

In distinguishing two compartments of trust, psychology brings an interesting element to this topic. Above all, trust is an emotional state that conditions and defines a second-level behavioral intention. From this point of view, a trusting intention is the result of an individual emotional process. In an equal context, certain individuals have a more marked tendency toward assured trust while others (the "paranoid") have a natural tendency toward determined trust. Therefore, each individual is characterized by a "disposition to trust". Trust, seen as an emotional state, can be defined as a presumption, an expectation, or a positive belief about the exchange partner. Then, the act (the behavior) of trusting can be defined as the desire to count on the exchange partner.

Therefore, trust is a multidimensional phenomenon in the sense that the process that governs its development may be social, economic, or psychological. Undoubtedly, the determinants of this process will change noticeably depending upon whether or not one is considering trust in a company, a government organization, among sovereign Governments, or between a consumer and an e-commerce website.

III. Digital trust

Contrary to traditional interpersonal interactions between a consumer and vendor, the digital environment also assumes another interaction: that between human and machine. In this context, the notion of consumer vulnerability to the negative consequences of a decision is more important because of the presence of a technology between the two actors in the transaction that naturally increases the decision-maker's sources of uncertainty.

1) *The digital environment: physical absence of the vendor and technological complexity*

The consumer is faced with two types of risks related to Internet transactions: behavioral risk stemming from the physical absence of the vendor (or any other transaction partner on the Internet) and technological risk.

(a) The physical absence of the vendor

The consumer who seeks information about vendors in electronic markets takes an approach similar to that which he would follow in traditional markets, even though certain characteristics differentiate these markets. As in traditional markets (physical and non-digital), the consumer who seeks information about potential vendors must do it above all, as much as possible, by his own means. First, he will trust his observations and personal experience. At this point, several characteristics unique to electronic markets become major obstacles to the autonomous search for information.

First, generally the consumer cannot meet the vendor in person or visit the company due to geographic distance. Handshakes, discussion, visits, and visual contact carry information about vendors or suppliers that are not available on the Internet. The individual characteristics of the supplier, typically revealing of information in traditional markets, are unknown to the consumer (for example a clean, well-shaven vendor dressed in a suit provides some clues as to his seriousness and professionalism). The identity of the supplier is not always certain. Moreover, the cost of entering into electronic markets is relatively low. Therefore, it is easy for new suppliers to enter, which favors the presence of merchants that disappear as quickly as they appear.

(b) Technological risk

Directly related to the perceived complexity of Internet technology, this is the risk that the technology used (software, websites, etc.) is outside the control of the consumer. In general, online payment and the conclusion of transactions on the Internet involve the transmission of personal (name, address, telephone number, email address, consumer preferences) and financial (credit card numbers and expiration dates, virtual account numbers) data.

A consumer's fear that the information communicated upon payment will be used for dishonest purposes affects the risk of loss. Personal information may be resold or used for other purposes by the merchant, and financial data can be used to commit fraud.

Beyond these risks, transaction integrity is not completely secure: data are not protected from malicious third parties (software pirates or hackers, to cite only the most well-known). Even though security, anti-virus, and encryption software is now well-known to the public, it must still be admitted that it is now no longer possible to protect oneself absolutely from fraud.

These two categories of risk that stem from the digital environment increase the sources of negative consequences that the consumer may perceive, increasing his anxiety and in time paralyzing his desire to use these technologies. To account for the specificities of this environment that affect consumer decisions, researchers typically mobilize traditional theories on consumer behavior in a dynamic perspective.

2) The dynamic of constructing and structuring trust

The determinants of an individual's degree of trust are therefore a function of one's perception of risk, which stems from various contextual factors (the social environment through norms, values, and conventions), the quality and quantity of information available, and one's natural disposition to trust.

In general, while context and disposition to trust are stable over time, the quantity and quality of information, which establish whether the individual believes that he is in a risky or uncertain situation, vary over time. Trust is therefore a dynamic process marked by various phases of trust development.

Head and Hassanein's model [7], which identifies four phases in this process, can help illustrate this idea (Figure 2):

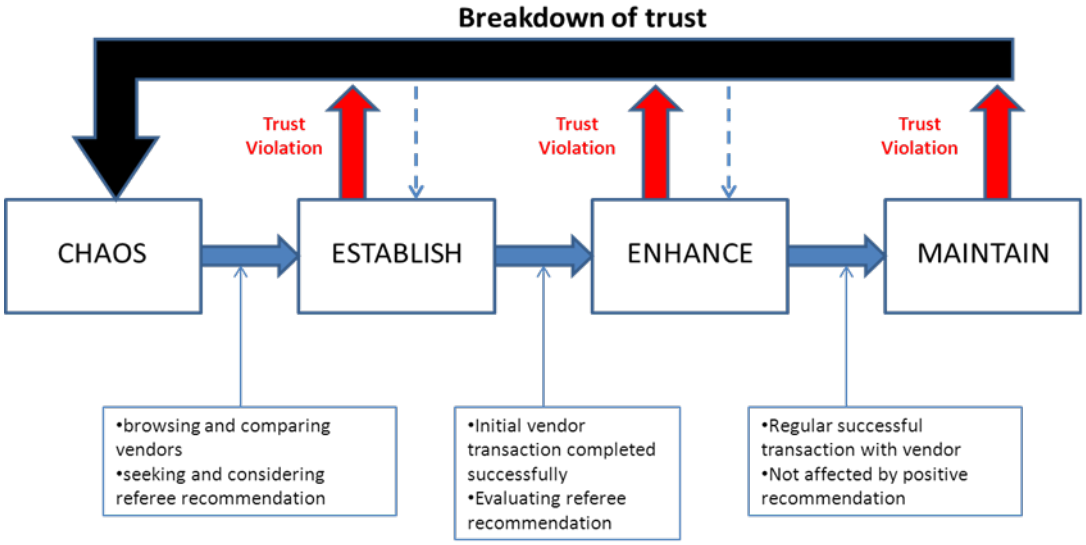

Figure 2: Online trust building model [7]

This model shows consumer behavior at each phase, as well as the consumer's interactions with two other transaction partners: the vendor, obviously, and a third party. This third party provides sources of external information to the consumer: it could be a friend, a consumer website, an advertisement, or even a public certification. Therefore each phase is marked by a distinct mechanism for building and structuring consumer trust. At each phase, the consumer must decide whether or not to engage in a transaction, and at each phase, he must evaluate whether or not to continue this relationship. In sum, he accumulates experience and information that will gradually reduce his ignorance as he moves from the initial phase to the final phase.

The four phases are as follows:

- **The chaos phase:** this is the initial phase of the model where the consumer is in a situation of radical uncertainty.
- **The trust establishment phase:** Having issued the desire to consume a product or service, the consumer will seek to reduce his ignorance. He will seek signals showing

that the vendor merits his trust. This is the phase in which the consumer compares vendors and/or products and, in particular, will seek the advice of third parties.

- **The enhancement phase:** The consumer has successfully completed his first transaction. He is therefore able to evaluate the consequences of this decision with a bit more precision. This first experience is determinant, and conditions the continuity of the relationship with the vendor. Starting with this phase, the consumer is able to judge the quality of the advice from the third party, and he is no longer in a situation of radical uncertainty.
- **The maintenance phase:** At this point, the consumer has conducted several successful transactions. His ignorance has been significantly reduced, and he has broad experience on the subject: previous interactions with the vendor drive this trust. Because of this, the third party no longer has any real impact on the consumer's decision-making process, and there are strong chances that he will engage in a long-term relationship with the vendor.

Therefore, the trust development process differs noticeably according to the consumer's phase. In addition to describing purely strategic interactions between the consumer, vendor, and a third party, the Head and Hassanein model [7] fails to show clearly the nature of the trust and the mechanisms for its production.

The model from McKnight *et al.* [8] contributes some relevant elements on this topic. This model acknowledges the dynamic nature of the trust construction process but considers that the four phases can be regrouped into two steps: exploratory trust and confirmatory trust. Exploratory trust (or initial trust) corresponds to the passage between the chaos phase and the establishment phase, and confirmatory trust moves from the establishment phase to the maintenance phase.

(a) The exploratory stage

As defined above, this model shows the mechanisms that contribute to the trust development process when the consumer is in a situation of radical uncertainty. He is in an exploratory stage as, by definition, this stage is marked by the complete absence of past interaction with the product, vendor, or third party; therefore experience plays no role in the development of trust. The model for building initial trust in the exploratory stage is as follows (Figure 3):

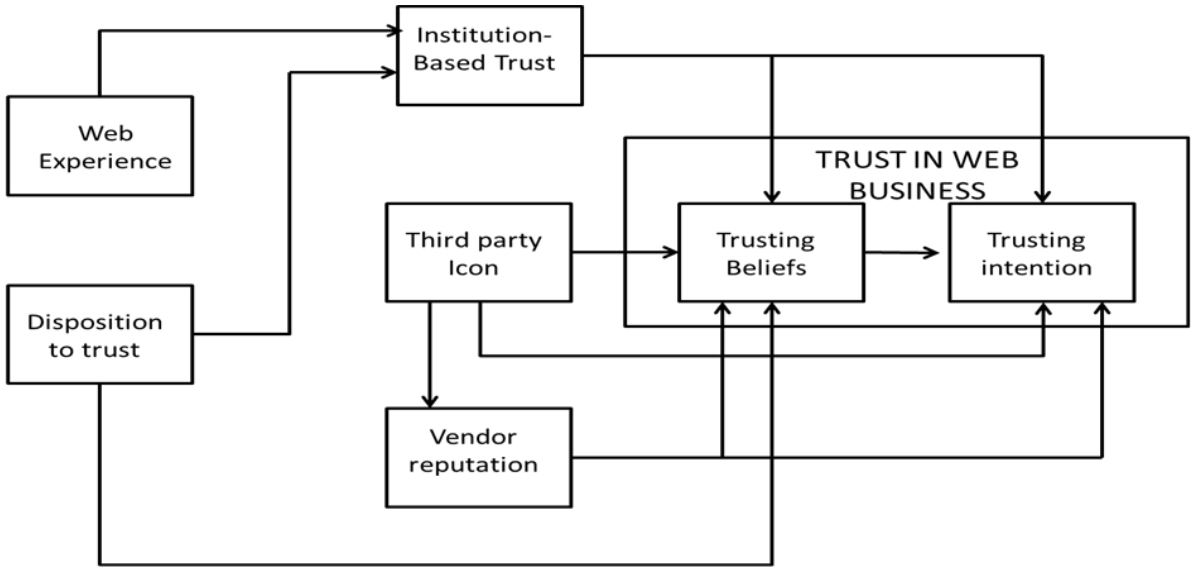

Figure 3: Trust model for exploratory stage [8]

Three compartments should be noted in this model. One compartment characterizing the consumer's own attributes, his disposition to trust, his experience with the Internet, and his institution-based trust. A second compartment characterizes the other stakeholders: the nature of the third party and the reputation of the vendor. Finally, the third compartment characterizes the consumer's digital trust (in transactions): trusting beliefs and trusting intention.

- **Consumer attributes**

Each consumer is characterized by a natural disposition to trust and a certain experience with the Internet. These two attributes will condition the consumer's level of institution-based trust, which will then condition the consumer's digital trust.

The disposition to trust was defined by McKnight and Chervany [9] as a consumer's propensity to trust regardless of the interlocutor and regardless of the context. The disposition to trust has been approached from two angles: the consumer's belief in humanity (in sum, the belief in the honesty of others) and a trusting attitude (the propensity to trust from the beginning). Experience with the Internet is of course defined by the consumer's familiarity with the Internet (amount of daily use, registration in forums, e-mail usage, etc.).

The consumer's institution-based trust is his propensity to trust the social structures of which he is a part (standards, conventions, rules, etc.). Institution-based trust can be divided into two sub-dimensions. The first is the "perceived normality of the situation", which is to say the consumer's belief that the situation in which he finds him or herself can be deemed "normal" (habitual, routine), which is to say without any special threats. The second dimension is "structural insurance", knowing whether the context in which the consumer finds him or herself is influenced by norms or a legal framework that he deems reassuring and compatible with his own values.

- **The other stakeholders**

Along with the consumer's own attributes, the consumer's perception and judgment on the identity, quality, and reliability of the other parties to the transaction also helps structure the consumer's digital trust.

In the exploratory stage, the consumer will seek to reduce his ignorance through external information provided by a third party. The third party comprises several dimensions: the consumer's propensity to trust his friends and family, the consumer's propensity to trust private sources (discussion forums, prices or advice provided by the media or retail sector), and lastly his propensity to trust public certifications (international standards, and government labels).

The vendor's reputation also plays a significant role. It is important to distinguish two cases:

- Vendors whose existence is known outside of the Internet (retail), for whom digital transactions are only an additional distribution channel. They benefit from the transfer of trust capital that they acquired in "the real world" into "the digital world".
- For vendors whose only distribution channel is the Internet, their reputation for integrity and reputation are essential to the consumer's choice.

- **Initial digital trust**

Therefore, the two compartments presented participate in the formation of the consumer's digital trust. It is divided into two dimensions: the consumer's "trusting belief", which will then condition the "consumer's trusting intention" toward the vendor.

- **Trusting beliefs**

Trusting beliefs are all of the consumer's beliefs about the benevolence, competence, honesty, and predictability of the vendor.

Beliefs in the competence of the vendor consist of the consumer's belief that the vendor has sufficient capacity to meet its commitments. More specifically, the perception of the vendor's expertise is determinant, as the latter is typically the consumer's first interlocutor. Beliefs in benevolence start from the principle that the consumer believes that the vendor will act in the consumer's interest, even going beyond the contractual framework of the relationship. Beliefs in honesty consist for the consumer in believing that the vendor will make arrangements based on the truth, and will act honestly to keep his promises. Predictability consists of the fact that the vendor's actions are sufficiently clear that the consumer can anticipate future behavior. In this way, the consumer is assured that the vendor will not attempt any opportunistic action likely to cause negative results for the consumer.

- **The trusting intention**

McKnight and Chervany [9] define the trusting intention as the consumer's desire to depend on the vendor in a given situation, with a feeling of relative security (despite the possibility of the occurrence of negative consequences).

The trusting intention is composed of three dimensions: the consumer's belief in the occurrence of negative consequences, the consumer's desire to depend on the vendor, and finally, the feeling of security experienced by the consumer in the specific transaction situation.

Thus, initial trust intervenes at a highly exploratory stage in the relationship between the consumer and vendor. This model can help describe the process of adopting an e-commerce website and in time initiating the first transaction with the vendor. The purpose of the initial trust model is to integrate the fact that the consumer will determine the outcome of his decisions based solely on assumptions. Lacking prior experience, the consumer can only assume that the vendor is worthy of trust. External signals or clues, especially those from third parties, guide his decisions in terms of trusting beliefs and his trusting intention.

It is completely different after the consumer has successfully carried out his first transaction, and even more so when he has a long history with the same product or the same vendor. The initial trust model becomes the confirmatory trust model.

(b) Confirmatory trust

At this stage in the relationship between the consumer and vendor, prior interactions with the vendor are what determine the degree of trust. If the consumer is satisfied with his past experiences, there are strong chances he will engage in a long-term relationship with the vendor. However, this relationship can be terminated by the first betrayal. Maintenance of trust by an Internet vendor and building customer loyalty, especially in a highly competitive market, is no easy task. The model from McKnight *et al.* [8] is as follows (Figure 4):

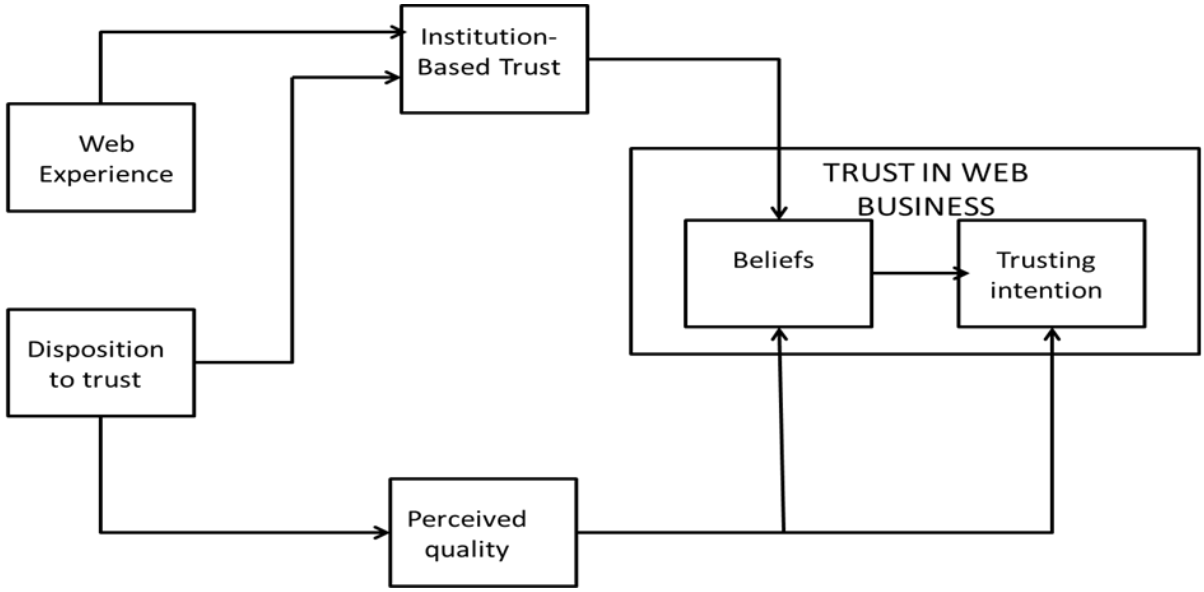

Figure 4: Trust model for confirmatory stage [8]

The trust development process during the consumer's confirmatory stage is no longer dependent upon the characteristics of the vendor and the third party. Similarly, trusting beliefs become the consumer's beliefs. These changes come from the fact that the consumer no longer bases his beliefs on assumptions, but on experience: he is no longer in a situation of radical uncertainty, and all of his information is of better quality.

Trusting beliefs thus become beliefs, and the perceived quality of the website is substituted for characteristics of the vendor or third party.

- **Perceived quality of the website**

The website is the mediator between the consumer and vendor. Therefore, the site's characteristics and an evaluation of its quality are fundamental to the consumer's choice. All research has shown a positive link between site quality and consumer trust. However, research differs on the notion of site quality. McKnight *et al.* [7] use dimensions related to the ease of navigation and relevance of the information displayed by the site (its freshness and quantity). Other authors add the feeling of security given by the site [10] [11] [12]. Thus, in the sense that the site provides a first image to consumers, just as a vendor in a physical space must present an appearance that translates its seriousness and professionalism, the website must also be designed in a way that reflects these qualities.

Trust in general and digital trust in particular are quite familiar concepts, – complex because trust is a multidimensional concept, and heterogeneous because the process differs on the one hand according to consumer experience, and on the other hand according to the context and product under study.

IV. Measuring digital trust

Measuring digital trust involves the use of methods that help emphasize phenomena not directly or precisely observable. In fact, while it seems clear on the surface how to make accurate and valid measurements of physical quantities (population density, per capita GDP, etc.), measuring the determinants of individual trust is not as simple.

Phenomena such as "the disposition to trust" are special personality traits and because of this, measuring them is systematically indirect and relative. It is indirect because phenomena such as intelligence, anxiety, and trust cannot be evaluated directly, but rather by their observable manifestations. They are relative, as it is impossible to consider all of the manifestations of this type of phenomena in a test setting. Therefore, there is always an element of error in the measurement.

Thus, it is important to understand these biases, and to mobilize methods that help minimize measurement errors as much as possible. To do this, one must first have a measurement scale (by associating numbers with each phenomenon), and then one must test the relevance and validity of these measurements in order to be able to assess the properties of the phenomenon. "Factorial" methods are statistical tools that meet these concerns.

1) Measurement scales

Measurement scales are tools that help quantify a phenomenon such as digital trust. Most often, they take the form of a fixed and highly precise questionnaire. Each item in the questionnaire is of course not selected by chance, but comes out of a long tradition of psychological or sociological research. The example of the study by McKnight *et al.* [13] on measuring trust disposition illustrates these ideas. The "disposition to trust" comes out of two dimensions: "belief in humanity" and "trusting stance". These two dimensions will be quantified by a measurement scale that takes the form of a questionnaire composed of statements or assertions called Items (Figure 5):

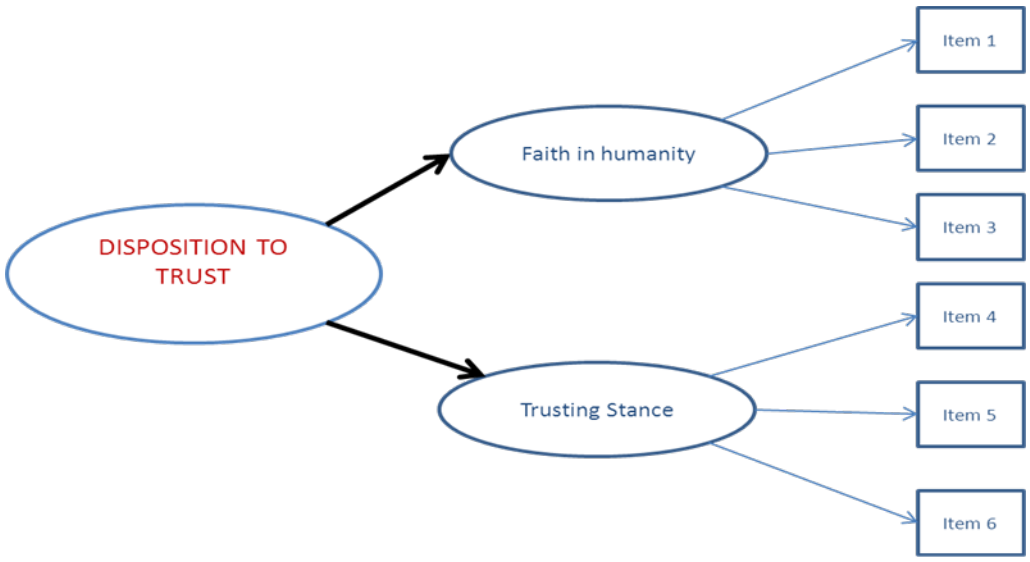

Figure 5: Measurement model for "disposition to trust"

The items are fixed questions where each person subjected to these questionnaires must respond using a "7-point Lickert scale" in this example. The Lickert scale requires the person being questioned to express his agreement or disagreement with an assertion or statement. The example of the questionnaire measuring belief in humanity is as follows:

1. *In general, people really do care about the well-being of others.*
2. *The typical person is sincerely concerned about the problems of others.*
3. *Most of the time, people care enough to try to be helpful, rather than just looking out for themselves.*
4. *In general, most folks keep their promises.*
5. *I think people generally try to back up their words with their actions.*
6. *Most people are honest in their dealings with others.*

To each of these assertions (items) the person being questioned must express his degree of agreement by allocating a rank between 1 (I do not agree at all with this assertion) to 7 (I agree completely with this assertion) on a 7-point scale (which might be a 4, 5, or 10-point scale depending upon the research topic).

The same process is carried out for all phenomena one wishes to measure (perceived quality, trusting intention, belief in vendor competence, etc.). In this way, when a survey is given to a sufficiently large number of people (administered in the laboratory, on the street, or by the Internet), this can provide a database illustrating all the phenomena of interest (shown by the study by McKnight for example) and thus to be able to mobilize the entire statistical and mathematical arsenal to show the existence, intensity, and relevance of the interrelation between these phenomena.

But before showing relationships, such as "the *disposition to trust* positively influences *institution-based trust* which in turn positively influences *the trusting intention*", there is a second stage of ensuring that "*disposition to trust*", "*institution-based trust*", and "*trusting intention*" are actually measured properly. These are what factorial methods call measurement models.

2) Measurement models

Each item (question, assertion, or statement) contributes to measuring a given phenomenon. The process of validating a questionnaire (measurement model) then aims to ensure that the manner in which each phenomenon is measured is suitable. It is important to ensure that measurement instruments produce reliable and valid results, that they measure the target phenomenon without bias (without error), which would lead to erroneous conclusions.

Two criteria can help judge the quality of a measurement model: the criterion of reliability and the criterion of validity.

The criterion of reliability is the ability of a measurement scale to produce the same result if one measures the same phenomenon several times: if one can accurately reproduce the conditions in which one asks a question of a person, will the model give the same response? Several statistical methods can help evaluate the criterion of reliability.

The criterion of validity is the ability of an instrument to measure the right thing, the proper phenomenon, and not a related but different phenomenon: does it actually measure *trusting beliefs* and not *trusting intention*? Are both phenomena actually distinct or do they make up a single phenomenon in the end?

Once assured that each phenomenon is being properly measured, that the criteria of reliability and validity have been confirmed, it is then possible to implement structural equation modeling (SEM).

3) Structural equation modelling

These relatively recent statistical methods, on the cutting edge of current research, provide an effective tool for showing the existence or absence of a relationship between the phenomena measured, and to measure their intensity.

It can help us know if, for example, the model from McKnight *et al.* [8] is compatible with data collected in Luxembourg. Is the disposition to trust as critical a phenomenon in the construction and structuring of digital trust in Europe as it is in the United States? Does trusting belief necessarily and automatically lead to trusting intention, and if so, to what degree?

For example, we can show the following relationships (Figure 6):

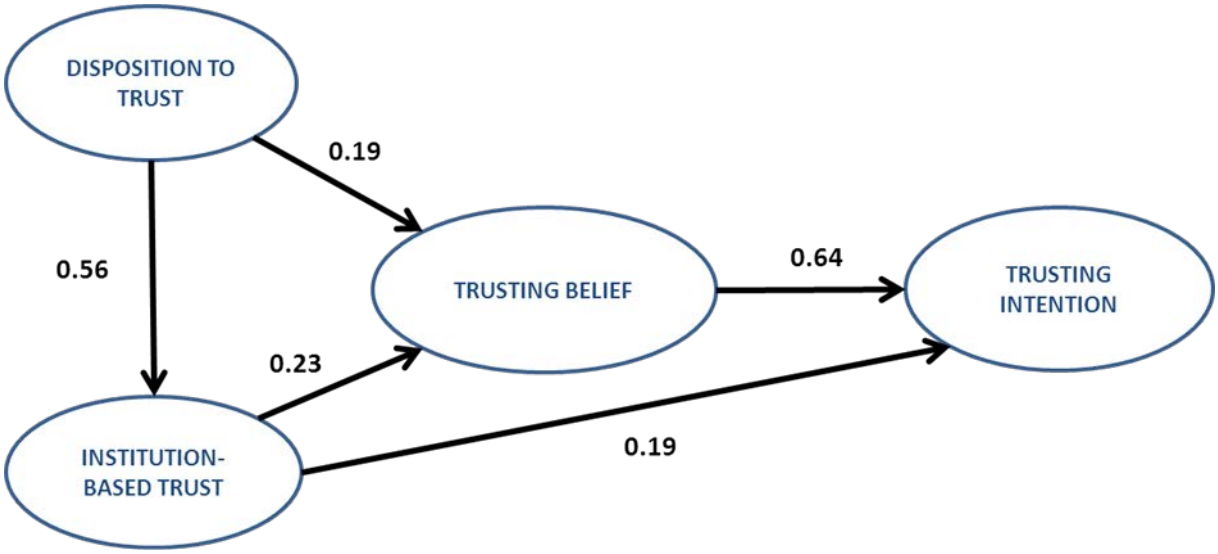

Figure 6: Structural modelling example

SEM can help respond to these issues, by providing an effective tool for assisting public or private decision-making, which is to say based on information coming out of maximum methodological and statistical rigor (in the current state of the research) or at least that suffers from a minimum of subjective bias.

V. Conclusion

Without a minimum of trust, transactions are not possible. The challenge for the digital economy, which is marked by intense competition and a significant degree of structural uncertainty, is even more important. In fact, in electronic markets, information is especially cheap to produce and circulate on the one hand, and it is relatively easy to duplicate or falsify on the other. Because of this fact, these markets are marked by an over-abundance of information available from third parties but whose reliability cannot always be guaranteed. Drowning in this mass of information, the consumer then must "determine to trust" rather than being "assured of trusting".

The challenge is to identify and implement procedures that help move from a "determined trust" model to an "assured trust" model. To do this, it is important to organize this mass of information so as to reduce the complexity of the electronic market:

- "Good" vendors and "good" products must be able to benefit from a credible signal that effectively differentiates them from "opportunists" or poor quality products.
- Consumers must be able to accurately judge the level of protection that they will have.

The challenge is significant but the development of the digital economy and its daily and growing presence in most private or public transactions requires governments to ensure that this economy is profitable for the general well-being. These are the concerns to which this chapter attempts to respond.

References

[1] Jensen, MC and Meckling, WH (1976), "Theory of the firm: managerial behavior, agency costs and ownership structure", Journal of Financial Economics 3, no. 4, p 305-60.

[2] Luhmann N. (1989), "Familiarity, confidence, trust: problems and alternatives". In: Gambetta DG, editor, Trust. New York: Basil Blackwell, p. 94 - 107.

[3] Giddens, A. (1990). "The Consequences of Modernity", Cambridge: Polity Press.

[4] Kreps, D (1990), "Game theory and economic modeling", Oxford: Clarendon Press.

[5] Coleman (1990), "Foundation of social theory", Cambridge. Harvard University press.

[6] Knight, F.H. (1921), "Risk, Uncertainty and Profits", London School of Economies.

[7] Head, M. and Hassanein, K. (2002), "*Trust in e-Commerce: Evaluating the Impact of Third-Party Seals*", Quarterly Journal of Electronic Commerce, Volume 3, No. 3, p. 307-325.

[8] McKnight, DH, Choudhury, V and Kacmar, C (2002), "Developing and validating trust measures for e-commerce: An integrative typology", Information Systems Research, 13(3), p. 334-359.

[9] McKnight, DH, and Chervany, N L (1996), "The meanings of trust", University of Minnesota MIS Research Center, working Paper series, WP 96-04

[10] Yoon, SJ (2002). "The Antecedents and Consequences of Trust in On-line Purchase Decisions", Journal of Interactive Marketing, 12, 2, 47-63.

[11] Suh B and Han I, (2003), "The Impact of Consumer Trust and Perception of Security Control on the Acceptance of Electronic Commerce", International Journal of Electronic Commerce, p. 135-161.

[12] Corbitt BJ, Thanasankit T and Yi H (2003), "Trust and e-commerce: a study of consumer perceptions", Electronic Commerce Research and Applications, 2, 3, p. 203-215.

[13] McKnight, DH, Cummings, LL and Chervany, NL (1998), "Initial trust formation in new organizational relationships", Academy of Management Review n°23, vol. 3, p 473-490.

2 Technical tools for digital trust

A) Public Key Infrastructures (PKI) and electronic signature

This chapter deals with Public Key Infrastructures (PKI) and electronic signature. The first section is about the key concepts related to PKI: public key cryptography, public key certificate, hash functions and actors of a PKI. The second section presents the mechanisms of PKI, i.e. some of the most common uses of a PKI. Then, the third section explains what an electronic signature is and describes the different kinds of electronic signature. Finally, the last section presents the national initiatives on PKI, such as the national legislation, the accreditation system, the national trusted list and the accredited organization in Luxembourg.

I. Concepts

PKI is "the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke Public Key Certificates based on public-key cryptography" [2].

The objective of a PKI is to provide authentication, as well as data integrity, non-repudiation mechanism, and confidentiality. The system is based on public key cryptography in which each user has a key pair: one of the keys called the public key may be revealed as widely as the owner wants. The other key called the private key is never revealed to another party.

First, public key cryptography, which is the core technology in order to create a PKI, is explained within this section. Second, public key certificates, which are a support technology for PKI, are depicted. Then, hash functions, which provide a support technology in order to create an electronic signature, are presented. Finally, the different actors playing a role in a PKI are identified and described.

1) Public key cryptography

Public key cryptography is an encryption method based on the use of a public key (widely distributed) and a private key (kept secret), to encrypt a message respectively to decrypt it.

A sender can use the recipient's public key to encrypt a message that only the recipient could decrypt using his private key, ensuring the confidentiality of the exchange. Conversely, the sender can use his own private key to encrypt a message, that the receiver could decrypt using the sender's public key – this is the mechanism used by digital signature in order to provide authentication of the sender.

Thus, using a public key, anyone is able to **encrypt a message** that only the holder of the paired private key can decrypt, as illustrated in Figure 1. The whole security (i.e. confidentiality and integrity) of the message depends on the secrecy of the private key.

[2] *Internet Engineering Task Force*

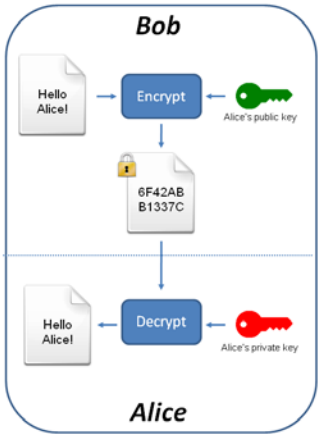

Figure 1:
Public key encryption

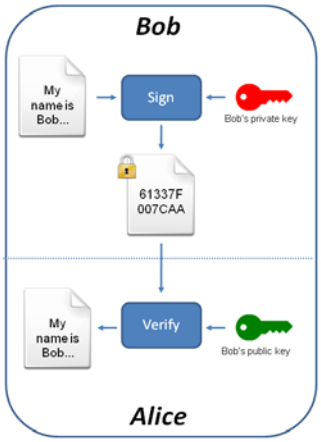

Figure 2:
Public key signing

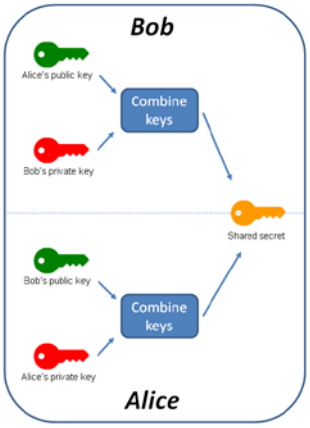

Figure 3:
Public key shared secret

In some related signature schemes, the private key is used to sign a message. Anyone, using the paired public key can verify (i.e. decrypt the message) by checking if the message was really signed by the public key holder, as presented in Figure 2. The whole security (i.e. authenticity) still depends on the secrecy of the private key.

Depending on the length of the keys used, public key cryptography can be considered as very secure, however a major drawback is the relatively slowness of encryption (due to complex calculations). That is why public key cryptography is only used to compute a session key offline, the key used afterwards for symmetric cryptography, as illustrated in Figure 3.

Note: A session key is a single-use symmetric key used for encrypting all messages in one communication session. In the context of Figure 3, one's public key is combined with the other's private key to compute the session key. Then, the messages are only encrypted with the help of this unique session key that is a shared secret between **Alice** and **Bob**.

IN A NUTSHELL

A **public key** is used to:

- encrypt a message (that can only be decrypted using the corresponding private key)
- verify a document signature (by decryption)

A **private key** is used to:

- decrypt a message (encrypted using the corresponding public key)
- sign a document (by encryption)

2) Public key certificate

As explained on the previous section, public key cryptography enables users to exchange messages securely under certain conditions. However, to use a public key with total security, the receiver must be able to answer at least the following two questions:

- Who owns this public key?
- What is this key?

For this, the public key should be accompanied by descriptive information of its owner and its use (a kind of business card presenting the owner, the key value and the intended use). Furthermore, this information should be made impossible to forge (in order to prevent any modification), that the reason why its content is guaranteed by a trusted third party.

This is done by the public key certificate, which is using a digital signature to bind together a public key with the identity of its holder (information such as a name of a person or an organization, their address and so forth).

3) Hash functions

A hash function will transform a large and variable number of bytes into a fixed number of bytes. The result of the hash function - often called hash value, hash code, hash sum, checksum or simply hash – does normally not enable to retrieve the original input data.

These hash functions are widely used in the field of PKI, in particular for electronic signature, where, in order to save time and storage volume, it is not the document itself but its hash value that is signed.

However one of the major problems of this type of functions is their susceptibility to collisions as several different inputs can produce the same hash value. Figure 4 illustrates the collision problem, using a totally fictitious example of hash function.

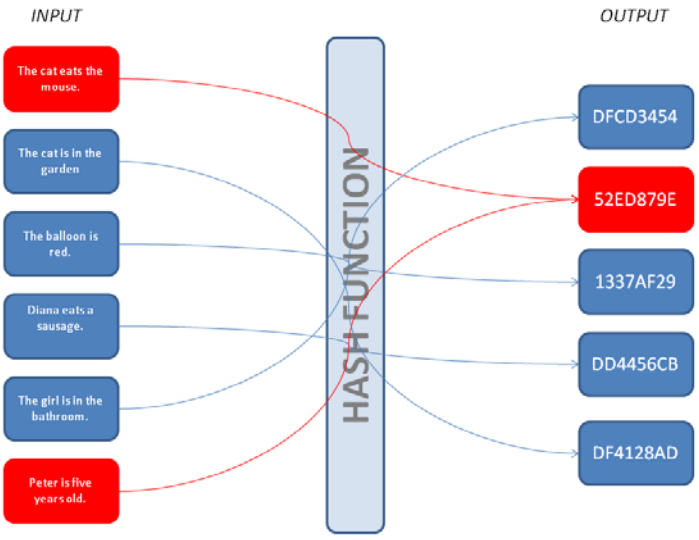

Figure 4: Illustrative example of hash functions collisions

This issue may facilitate the function's attack; thus hash functions used for cryptography must meet the following criteria:

- It has to be very difficult (technically impractical) to find the contents of the original message from the hash value (first preimage attack).
- It has to be very hard to generate another message with the same hash value from a given message, its hash value and the source code of the hash function (second preimage attack).
- It has to be very difficult to find two random messages that give the same hash value (collision resistance).

4) Actors of the PKI

Even if all the standards on the topic do not agree on a common definition, it is widely accepted that a PKI consists of five different distinct entities:

- **Certification Authorities** (CAs) that issue and revoke Public Key Certificates.
- **Registration Authorities** (RAs) that guarantee bonds between a public key, the identity of the holder of the certificate and other attributes.
- **Certificate owners** that use certificates for signing or decrypt documents.
- **Certificate users** who verify digital signatures or encrypt data, and validate certification paths of certificates from a trusted CA.
- **Repository,** which includes directories, that contains and makes available public key certificates and Certificate Revocation Lists (CRLs).

Figure 5 below introduces these five entities organized on three areas of responsibility:

- The **certificate owner** – the one whose identity is contained in the certificate
- The **certificate user** – the third party who will use certificates
- The **trust infrastructure** – a set of actors (CA, RA, repository…) that helps to establish a level of trust expected by the two other areas.

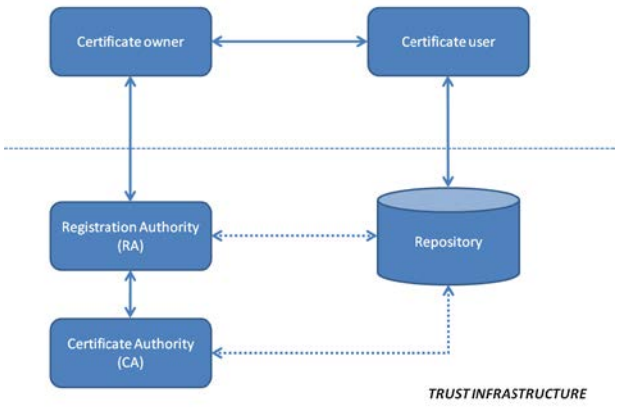

Figure 5: PKI actors

❖ Certificate owner

The certificate owner is the entity referenced in the certificate. Thus this entity owns both the public key and the corresponding private key. Depending on the context, the certificate owner can be named differently: Certificate holder, subject, subscriber, end-entity, or signatory.
Whatever the name used, the entity referenced in the certificate is not always a person. Indeed, a PKI architecture may involve intermediate components (such as RA or sub-CA) or network components (such as routers) which also require key pairs and certificates.
In theory, the holder of a public key certificate must be the only holder of the associated private key. To that purpose, he is equipped with software and/or material necessary for the storage and management of its certificate and private key, protected by secret data (such as password, or more sophisticated systems such as strong authentication).

Note: Strong authentication is an identification procedure that requires the concatenation of at least two elements or factors of authentication, for example something you know (as a password), something you have (as a key), something you are (as fingerprints), etc.

❖ Certificate user

Contrary to popular opinion, the certificate holder is not the certificate user. Indeed, the certificate holder owns the certificate but does not use it. He provides it to its interlocutors, who will use it to check signatures or encrypt messages.
The certificate user is the entity (human, organization or even technical) selecting and validating the certificate of the entity with which he/it communicates, in order to use the corresponding public key for encrypting or verifying a signature. In Figure 1, **Bob** is the certificate user, as he simply uses **Alice**'s certificate to encrypt a message. The certificate user must know the Key Usage certificate, i.e. the conditions of use set by the certificate issuer to determine the guaranteed level of trust. To that purpose, the certificate user is equipped with appropriate software to conduct audit and analysis of the certificate.

Depending on the context, the certificate user can be named differently:

- *Certificate acceptor* – This name is given to a user receiving a signed message and the corresponding certificate used to verify the signature.
- *Checker* – This name is given when the user uses the certificate to verify a signature of a document. The certificate user will have to validate the certificate and to verify the signature.

The certificate user should rely on the certificate which will be used to establish the level of trust necessary to complete the transaction with its interlocutor. This level of trust is largely based on the conditions under which the certificate was issued, and therefore policies and procedures governing the management of the certificate. Thus, the receiver of a signed document (certificate user) will follow this general process:

- Verify that the supposed identity of the signer matches the identity of the subject contained in the certificate.
- Verify that none of the certificates in the certification path was revoked by checking appropriate CRLs and that these certificates were not expired at the time of signing.

- Verify that data are not supposed to be subject to some conditions that the receiver of a signed document does not meet (e.g. hierarchical position in a company).
- Verify that data have not been modified since the signature of the document, by using the public key attached to the certificate. At the same time, verify that data have been signed by the indicated signatory.
- If all these checks are successful, the receiver can consider the signature as valid and can use these trustworthy signed data.

❖ **Trust infrastructure**

The trust infrastructure makes a relationship of trust possible between two partners. As previously introduced, the main components of the trust infrastructure are the Certification Authority, the Registration Authority and the Repository. However, some other optional components can be found such as the Policy Management Authority, the Time Stamping Authority or the Key Escrow. In real PKI implementations, they are often included in the principal components or can be derived from.

(a) Certification Authority

A Certification Authority (CA) is an entity trusted by one or more users. It is in charge of issuing, signing and maintaining certificates and CRLs. This authority can also optionally create user keys.

A CA has overall responsibility for the provision of certification services.

There is however a terminological ambiguity regarding the CA. Indeed the term CA can refer to several concepts depending on the use made by professionals:

- The concept of legal authority that issues certificates for a community, as generally retained in Europe.
- The concept of functional entity that is used to build a technical architecture as a hierarchy of CAs. This is generally the approach retained by the Internet Engineering Task Force (IETF), PKI software editors or certification service operators.

Thus, the standard PKI Practices and Policy Framework (Accredited Standards Committee X9 Incorporated, 2001) defines a CA by these four roles:

- Certificate Issuer – organizational aspects of issuing and managing certificates, including revocation.
- Provider of certification services – technical and operationnal aspects of certificates management.
- Registration Authority.
- Repository – certificates and CRLs storing.

On its side, the European Electronic Signature Standardization Initiative (EESSI) clearly separates the roles linked to legal liability to those relating to operational use. In any case, the signing key of the CA is always used to sign certificates and its name as Issuer name always appears in such certificates.

(b) Registration Authority

A Registration Authority is an optional entity which is responsible for administrative tasks related to the management of certificates applicants and holders such as:

- Verify the identity of applicants by checking documents required by the certification policy.
- Confirm that an applicant is empowered to obtain the rights or qualities mentioned in the certificate.
- Get the public key of the applicant (from himself or by the entity in charge of generating keys).
- Verify that the applicant owns the private key corresponding to the public key for which he requests a certificate.
- Submit applications for generation of certificate to the certificate issuer.
- Receive and process applications for certificate revocation, suspension or reactivation.

In general, the role of RA is performed by business registrars, banks, human resources department or other competent authorities.

This role is very important, as once the certificate generated, it becomes cryptographically tamperproof since it is signed by the CA private key. So during this phase, an attacker can try to obtain a certificate instead of someone else. For this reason, the RA and its registration agents have significant responsibilities, and rarely delegate these tasks to sub-contractors. Similarly, actions related to certificate revocation need to be executed thoroughly in order to avoid an attacker to compromise the certificate or even worse the corresponding private key.

(c) Repository

The Repository or Publication Service is a component of a PKI that makes available public key certificates issued by a CA to all potential users of these certificates. It publishes a list of certificates recognized as valid and a list of revoked certificates (CRL). This service can be provided by a directory (e.g., X.500), a web information server, a hand to hand grant, a messaging application, etc. The Lightweight Directory Access Protocol (LDAP) is an example of repository. It is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

A Publication Service has some requirements on CRL update frequency and availability. In addition, it can sometimes be an online service that allows real-time monitoring of the presence or absence of a CRL, just like bank cards red list control.

The Online Certificate Status Protocol (OCSP) is another protocol used for obtaining the revocation status of a digital certificate. It was created as an alternative to CRL.

(d) Policy Management Authority

The Policy Management Authority (PMA) is a high level authority which assumes security authority functions, and sometimes management functions. It has a decision-making power within the PKI and is generally held by a steering committee within a company.

The PMA is responsible for:

- Establishing certification policies which the PKI must meet,
- Enforcing rules,
- Verifying through audits their effective implementation.

In addition, it is also responsible for validating or not the cross-certification applications with other PKIs. It guarantees the management of changes that may occur within the PKI, in particular the development of policies, standards or practices.

(e) Time Stamping Authority

The Time Stamping Authority is a PKI component issuing time marks, used to prove the existence of certain data at a certain point.

Time stamping is an essential function in the management of PKI, since it helps to situate events in time; typically, the dates of beginning and end of life are contained in the certificates for checking certificates validity.

Time Stamping can be provided by a Trusted Third Party that will provide a full trusted time stamping, independent of the parties in communication and designed to produce evidence relating to temporal acts or facts.

(f) Key Escrow

In some PKI implementations, security policies can require that keys needed to decrypt data were held in an authorized third party, called Key Escrow. Therefore, under certain circumstances, this third party may gain access to those keys. Such circumstances can be:

- A user has lost the support containing the key or it has been deteriorated,
- A user has forgotten the code to activate the private key,
- The security policy of a company allows the managers to read the encrypted emails issued by their employees,
- Critical information was encrypted by an employee who has died or left the company without compromising its decryption key.

In all these cases, the PKI must provide a service that allows reconstructing the key, while minimizing their risk of compromise. This procedure should remain exceptional and should provide logs in case of subsequent audits.

Currently, there are two techniques for safeguarding keys:

- The encryption key pairs are generated by an entity under the control of the CA, who keeps a copy of private keys. In case of loss, the CA may retrieve the private key.
- If the key pairs are generated directly by the user, the user, to obtain its certificate, must provide a copy of the private key to the CA or RA.

Whatever the method chosen, the aptitude of the Key Escrow to maintain the confidentiality of the key is a controversial matter both technical and legal.

The following figure (Figure 6) positions the different actors in a PKI and puts forward their activities and relations.

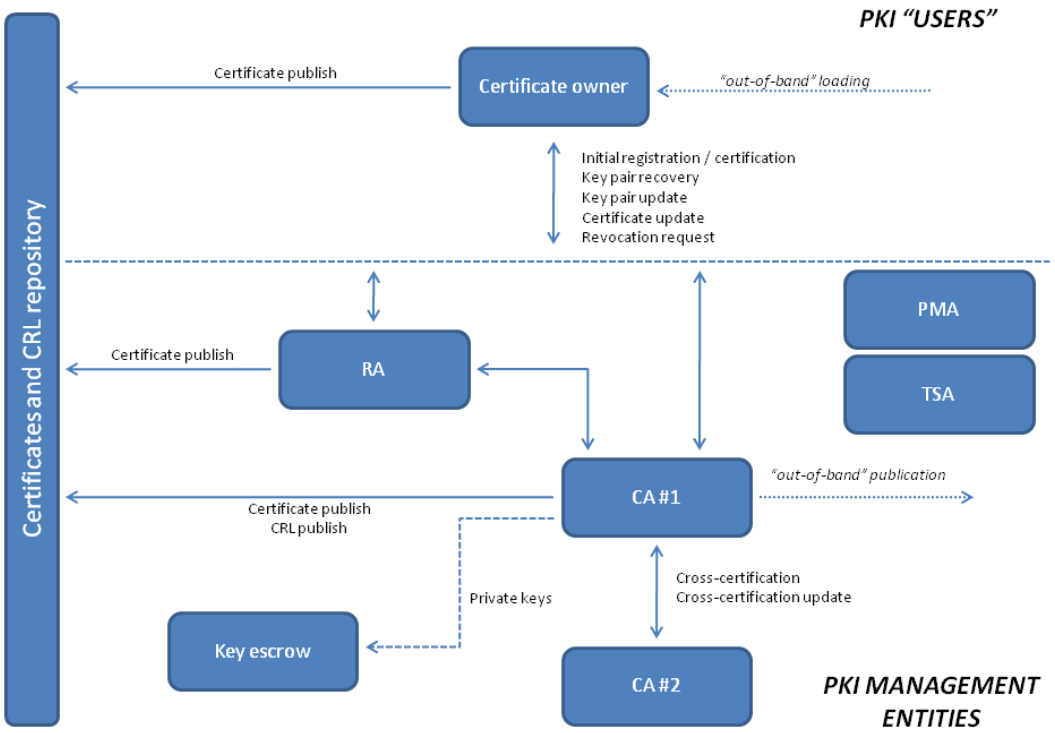

Figure 6: PKI global organization

II. Mechanisms

This section lists some examples of the most common uses of a PKI.

1) Web server identification

In security-sensitive applications, like for example e-banking, it is important for the client to firmly identify the website consulted. In this context, any Internet user regularly uses PKIs without knowing it. Indeed, one of the common uses of PKI is to identify a server using digital certificate during TLS (formerly SSL) handshake through HTTPS secured web server connection (bank server, online stores, etc.). Part of the TLS protocol allows authentication between two parties, cryptographic algorithms negotiation and session key selection.

Figure 7 presents a TLS handshake, which produces cryptographic parameters for a session initiated by the client (1). In (2), the server sends its digital certificate containing its public key. In (3), the client will check the certificate, in order to identify the server. If this check is ok the client is able to state that the server is the right server: the server is identified. The client can generate a symmetric key that will be used during the whole session. This key will be encrypted with the server's public key and transmitted (4). As the client and the server share a common session key, they can communicate securely (5).

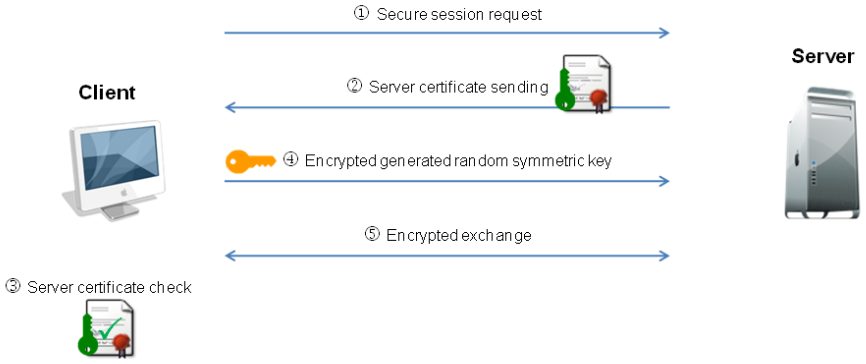

Figure 7: TLS handshake

2) Authentication and authorization for web applications

The server identification by clients (a client is either human or virtual), as presented in the section above, is common but more and more web applications need to verify the identity of the client to ensure they are communicating with the right client. This is particularly the case of applications dealing with sensitive information such as e-banking applications. Logins and passwords can enable identification, but a PKI can provide a good alternative while bringing real added value. Indeed, based on TLS, a server may require the client authentication before initiating a secure session. Furthermore, in doing so, the identity of the client is certified by the PKI. To implement this solution, the client uses a certificate issued in his name, usually stored as software or as hardware (e.g. smart card, token, etc.). This adds to mutual authentication, strong authentication for client side.

Another relevant advantage of this authentication means lies in the fact the server does not need database for passwords as the password is stored and managed locally by the client.

Figure 8 below presents an overview of TLS client authentication.

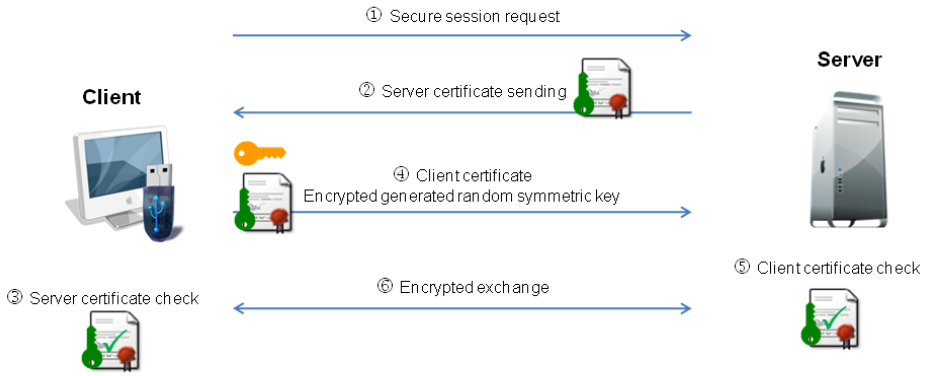

Figure 8: TLS Client authentication

3) Electronic documents and forms signature

Another possibility offered by a PKI is the signature of electronic documents or forms. The approach is the following: a person willing to sign a document computes the hash of the content of this document and attaches a signature using the private key.

As explained earlier, only the owner of the private key can sign, but everyone bearing the public key can decrypt the signature and verify the hash. This allows verifying that the document has not been modified since the signing.

In this way, such a signature guarantees data integrity in addition to authentication. The digital signing of electronic documents provides more security than traditional handwritten signature, and is easy to sign and to verify. Thus, many processes requiring individuals signature now use digital signature instead of traditional one.

4) Authentication for VPNs

A VPN is a virtual private network built on another network, generally public and/or with a non-guaranteed level of security, such as the Internet. It allows the transit of information between the different members of the VPN, while guaranteeing a level of security previously defined.

Within a VPN, a PKI can be used to provide digital certificates for authentication to establish a connection. Some VPN implementations use information contained in the certificates, in order to grant access and special privileges to the holder of the certificate. The PKI can then in addition provide authentication and authorization.

5) S/MIME Email signing and encryption

On the same principle as the signing of electronic documents and forms, a PKI combined with the S/MIME standard (dedicated to electronic messaging applications) can enable the encryption and signing of emails. S/MIME standard allows signing MIME data (extension of the format of email support).

Users own a certificate with a public key and their mail address, and use their private key to sign messages and to decrypt received messages encrypted with their public key. This ensures that only the owner of the private key can sign a message and decrypt a message encrypted with his public key.

6) Email list server

Based on the use of PKI coupled with S/MIME standard, email list server provides secure exchange of messages through a mailing-list.

Indeed, when sending a message to a mailing list, recipients are not necessarily known from the sender and each recipient has a different public key; it is then not possible to encrypt a message with a public key. To this end, the server acts as an intermediary, receiving messages encrypted with its own public key. The received messages are decrypted using the server's private key, then individually encrypted with public keys of users and then sent to each recipient. The server has therefore a list of public keys to keep, and users have only the server's public key to take into account.

In Figure 9, User#1 sends an encrypted message to the server using the server public key. The server decrypts the message using its private key, and encrypts the message with the public keys of the recipients using the users' public key repository containing all the public keys. The server can then send encrypted message to all the recipients.

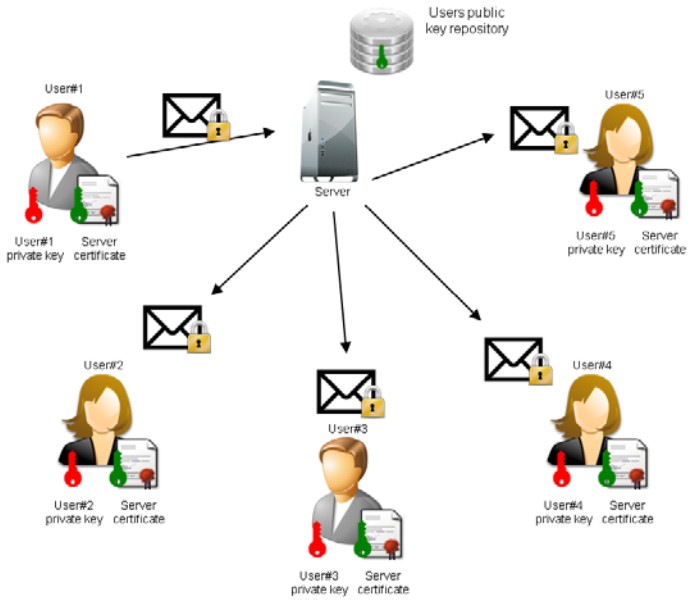

Figure 9: Overview of PKI use in email list server

7) Single Sign-On

PKI-based Single Sign-On (SSO) solutions use a PKI to identify users. Users need to authenticate only once to access multiple applications or secure websites.

Once a user is authenticated, using its signed certificate, the authentication service ensures user authentication besides applications and secure websites.

Figure 10 introduces the user authentication using such SSO: when a user tries to access a remote access, the user creates a request including his own certificate (containing its public key) and signs it with its private key. The request is received by the server. The server checks the certificate using the directory and check if the user is allowed or not to access the requested target.

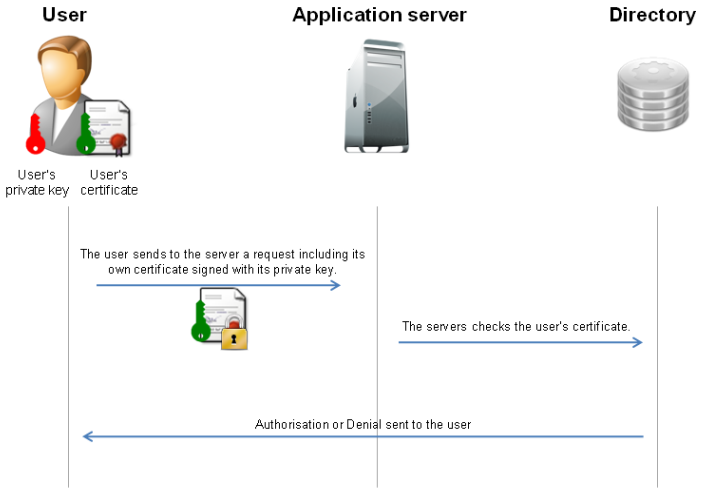

Figure 10: PKI-based SSO user authentication

8) Transaction and electronic publishing

A PKI can be used to provide and guarantee trustworthiness of transaction and electronic publishing. Thus, a trusted third party (CA) is responsible for ensuring non-repudiation and to provide if necessary legal evidence. This mechanism can be used for example in the context of electronic registered mail, or electronic archiving.

Figure 11 introduces the global functioning of an e-registered mail platform. In the presented approach, only the platform uses a PKI, but it is possible that the PKI is also used by users to encrypt and/or sign the document or even to identify and authenticate on the platform.

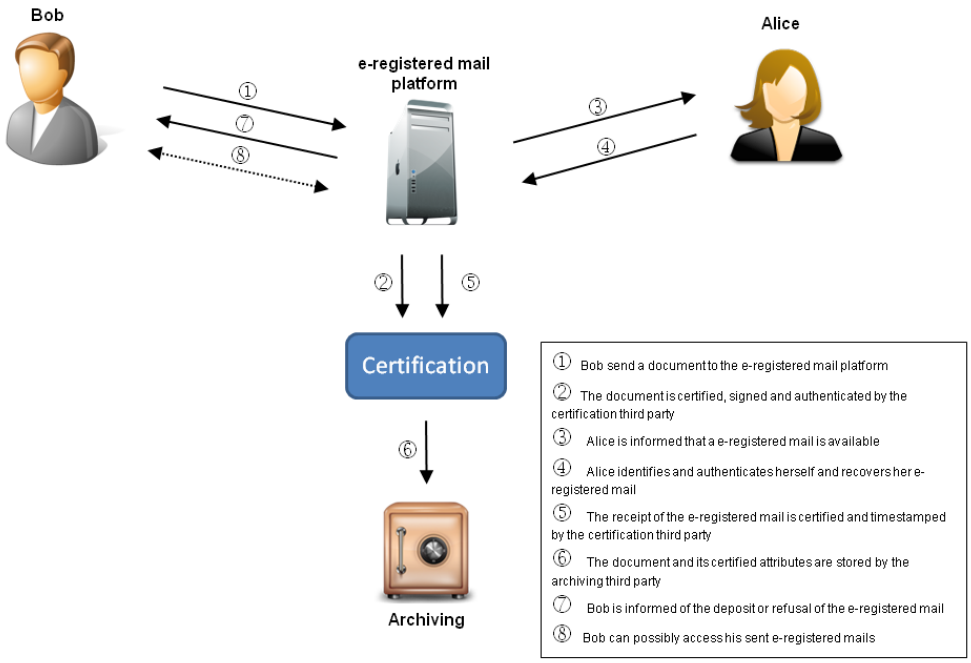

Figure 11: e-registered mail platform

III. Electronic signature

An electronic signature is a mechanism to authenticate the author of an electronic document (like the handwritten signature for a paper document), and to ensure its integrity.

The European electronic directive (Dir 1999/93/EC) establishes a harmonized electronic signature similar to the handwritten signature. There are three kinds of electronic signature, each with a different probing value.

1) *Electronic signature*

An electronic signature, also called weak electronic signature or light electronic signature is "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"[3].

2) *Advanced electronic signature*

An electronic signature is qualified as advanced providing:[3]

[a] it is uniquely linked to the signatory;

[b] it is capable of identifying the signatory;

[c] it is created using means that the signatory can maintain under his sole control; and

[d] it is linked to the data to which it relates that any subsequent change of the data is detectable.

An advanced electronic signature guarantees integrity of the signed document as well as the authentication. Such a signature can be used to prove that a text was not modified since the sender signed it. Moreover, it has a stronger probing value in front of a court than the standard electronic signature.

3) *Qualified electronic signature*

A qualified electronic signature is an advanced electronic signature based on a qualified certificate, which guarantees authentication, integrity, confidentiality and non-repudiation. A qualified certificate is a certificate which meets the requirements laid down in Annex I of the EU Directive 1999/93/EC on a Community framework for electronic signatures and is provided by a certification-service-provider who fulfills the requirements laid down in Annex II of this same EU Directive.

This gives the qualified electronic signature the strongest probing value in front of a court.

[3] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*

In Luxembourg, in addition to international and European texts and agreements, the following texts frame the electronic signature:

- *Code civil* (Art. 1322-1, 1322-2, 1325 and 1326)
- *Loi modifiée du 14 août 2000* [4] *relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers* (Art. 18)
- *Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement et à la création du comité «commerce électronique* (Art. 1-4)
- *Règlement grand-ducal du 22 décembre 1986 pris en exécution des articles 1348 du code civil et 11 du code de commerce*
- *Règlement grand-ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés, mettant en place un système d'accréditation des prestataires de services de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes*

From the point of view of the *Code Civil*, the article 1322-2[5] stipulates that an electronic private deed has the same value as the original one if there are reliable guarantees that the deed was not modified. The article 1322-1[6] defines the electronic signature as a group of data linked to the deed which guarantee its integrity.

The *Loi modifiée du 14 août 2000*, modified by the *Loi du 19 décembre 2003* and the *Loi du 5 juillet 2004* on electronic commerce defines the juridical effects of the electronic signatures namely the definition of an electronic signature according to the Code civil, the fact that the signature cannot be dismissed by a judge simply for its electronic nature, and finally the fact that no one may be compelled to use such a signature.

[4] *Loi modifiée par Loi du 19 décembre 2003 et Loi du 5 juillet 2004*

[5] *« L'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive. », art. 1322-2., Code civil.*

[6] *« La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article. », art. 1322-1, Code civil.*

IV. National initiatives on PKI

Each country has one or more Certification Service Provider (CSP), which is an "entity or a legal or natural person who issues certificates or provides other services related to electronic signatures" [7].

1) Legislation

The *Règlement grand-ducal du 1er juin 2001* defines requirements for qualified certificate, requirements for CSP issuing qualified certificates, requirements for secure signature-creation devices, electronic payment and creates the e-commerce committee.

In addition, the *Règlement grand-ducal du 21 décembre 2004* defines the organization of the notification for CSP delivering qualified certificates, by putting in place an accreditation system for CSP, setting up an electronic signature committee and determining a procedure for approving external auditors.

The national legislation is available on the ILNAS website[8].

2) Notification, accreditation and monitoring system

The *Loi modifiée du 14 août 2000* stipulates that *ILNAS (Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services*) is the authority responsible for the CSP accreditation and for the supervision of CSP providing qualified certificates. The documents describing the accreditation system are available on the ILNAS website[9].

This same law also defines the notion of surveillance and conditions for obtaining such accreditation.

In parallel, a CSP accreditation committee (Electronic Signature Committee) has been created. It is mainly in charge of:

- Making proposals on general guidelines for accreditation of CSP issuing and managing certificates or providing other services related to electronic signature.
- Giving advises on each grant, extension, continuation, renewal, supplemental, refusal to grant or extension, suspension or suspension lift, reduction and complete or partial withdrawal of an accreditation.
- Providing reports of serious and/or repeated failures to respect of a CSP accredited by ILNAS.
- Providing reports of serious and/or repeated failures to respect of an auditor registered in the quality and technical auditors' compendium.
- Bringing proposals on ILNAS functioning in the field of accreditation of CSP.

[7] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Art 2.11*

[8] *http://www.ilnas.public.lu/fr/legislation/index.html*

[9] *http://www.ilnas.public.lu/fr/confiance-numerique/pki/systeme-qualite-pki/index.html*

3) National Trusted List

Each Member State is required to maintain an official Trusted List, which is the list of its accredited (and optionally supervised) Certification Service Providers.

A Trusted List aims at:

- Listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by Luxembourg for compliance with the relevant provisions laid down in Directive 1999/93/EC;
- Facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSP.

Additional information on other supervised/accredited CSP not issuing qualified certificates but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

In Luxembourg, ILNAS through its Digital Trust department is responsible for managing and updating this list every six months. Furthermore, ILNAS electronically signs this list[10] to ensure both its authenticity and integrity.

4) Accredited CSP in Luxembourg

In Luxembourg, one CSP is accredited under the current standards[11]: LuxTrust S.A., under the accreditation number 2011/8/001, valid till October 13th, 2013.

LuxTrust S.A. was created by the government of Luxembourg and some important actors of the private sector, and proposes various applications and products, such as:

- Login application (e.g. banks)
- Single login
- mySecretID: anymous client authentication
- Transaction (legal signature), which can be used as an evidence before a court.
- Contract signature (legal value)
- Contract archiving, responding to the issue raised by the different lifetimes of archived documents and signing keys used.

[10] *http://www.ilnas.public.lu/fr/actualites/evenements/2011/12/liste-de-confiance-nationale1/index.html*
[11] *http://www.ilnas.public.lu/fr/confiance-numerique/pki/psc-accredites/index.html*

B) Electronic records management

Records are the evidence of **what the organization does or has done in the past**. They capture its business activities and transactions, such as contract negotiations, business correspondence, personnel files, and financial statements, just to name a few. In order to be compliant with regulations or for management purpose, records have to keep their legal value. They need therefore to have the following properties: authenticity, reliability, integrity and usability.

Records on solid support (paper documents, for example) are difficult to manage, essentially when an organization wants to retrieve a specific one.

The use of digital records is then the common answer of organizations to face the amount of data to be preserved, to increase efficiency and to reduce storage cost. However, the constraints related to security, optimization and reliability of records are prominent. It is therefore necessary to use efficient Electronic Records Management Systems (ERMS).

This chapter proposes an overview of the field of ERM. The first section presents the key concepts related to Electronic Records Management (ERM) such as records, archives, Electronic Document Management (EDM) and ERM. The second section presents the document lifecycle in ERMS workflow. Then, the third section is about international and European standards. Finally, the last section deals with the current national legislation in Luxembourg.

I. Concepts

This section aims at introducing the fundamental concepts in ERM such as records, archives, EDM and ERM.

1) Records

Records are "information created, received, and maintained **as evidence** and information by an organization or person, **in pursuance of legal obligations or in the transaction of business**" [1].

Records are a subgroup of documents, as depicted in Figure 1. A document is a support with information readable by humans, a "recorded information or object which can be treated as a unit" [1].

For a record to keep its legal value, it must respect the following **main characteristics:** authenticity, reliability, integrity, and usability [1].

- **Authenticity** is proved when a record is what it purports to be, when the creator or sender is the person purported to have created or sent it, and when it was sent or created at the time purported.
- A record is **reliable** when it describes fully and accurately transactions, activities or facts for which it had been created (for example, created right after the transaction, not long after).
- **Integrity** of a record refers to its completeness and non-modification, thanks to protection against unauthorized alteration.

- **Usability** is linked with a traceability process. Indeed, a record is useable when it can easily be located, retrieved, presented and interpreted.

Records need to be managed in order to be useful and to preserve their legal value and their characteristics. **Records Management (RM)** gives solutions to deal with records and ensure their authenticity, reliability, integrity and usability.

RM (or recordkeeping, depending on the country) is the "field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records" [1].

RM addresses the life cycle of records, i.e., the period of time that records are in the custody of the organization. The life cycle usually consists of three stages:

- creation or receipt and validation;
- maintenance and use; and
- disposition.

The term 'record' has a slightly different meaning in a Records Management System (RMS). Indeed, in the organization a record is identified thanks to some documentation (internal procedures, regulations, etc.), whereas an electronic record managed in a RMS refers to information that has been "classified, registered and locked against change" [2]. Furthermore in a RMS "records are made from documents. Each record can comprise one or several documents; and each document can appear in several records" [2].

2) Archives

Archives are "records of the same provenance accumulated by an organization or person in the course of the conduct of affairs, and preserved because of their enduring value" [3]. An archive is "the whole body of records of continuing value of an organization or individual" [4]. Archive is sometimes called **'corporate memory'**.

An archive is thus a **collection of historical records.** They contain records which have been accumulated over the course of an individual or organization's lifetime. The archives of an organization tend to contain certain types of records, such as administrative files, business records, memos, official correspondence and meeting minutes. Archives consist of records which have been selected for permanent or long-term preservation, due to their enduring research value and as a memory aid.

Constraints for archives are much less important than for records, because the probing value of the document does not need to be maintained. In addition archives tend to be used less frequently, and therefore can be less accessible (fewer access time constraints).

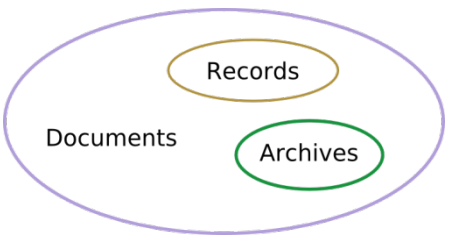

Figure 1 shows the relationship between concepts: '**documents**' is the global concept; records and archives are documents. '**Archives'** are different from **'records'** as archives do not need to have the four main characteristics of a record (authenticity, reliability, integrity and usability); an archive is thus not usable as a legal proof though archives can have been records before.

Figure 1: Document is the global concept

3) Document Management vs Records Management

EDM and ERM are usually two misinterpreted concepts.

EDM is a way to store, manage and easily retrieve documents, whereas ERM is a way to manage the probing value of records and to manage the records themselves. ERM has to allow overseeing records until an eventual disposition, and then controlling specifications of this disposition. From this point of view, ERM opposes itself to EDM.

A major difference between both is that a **record cannot be modified or erased** (except under certain circumstances): a record will be preserved and will keep its integrity.

Records managed into a RMS will have a much stronger probing value than documents in a Document Management System where documents can be modified.

Some systems can have characteristics from EDM and from ERM. These systems are called Electronic Document and Records Management System (EDRMS).

II. Document lifecycle in Electronic Records Management System Workflow

Records managed into a RMS go through three main steps: creation and validation of the document, maintenance and retrieval of this document, and disposition. These steps are illustrated on the workflow on Figure 2. The steps of the workflow are detailed below.

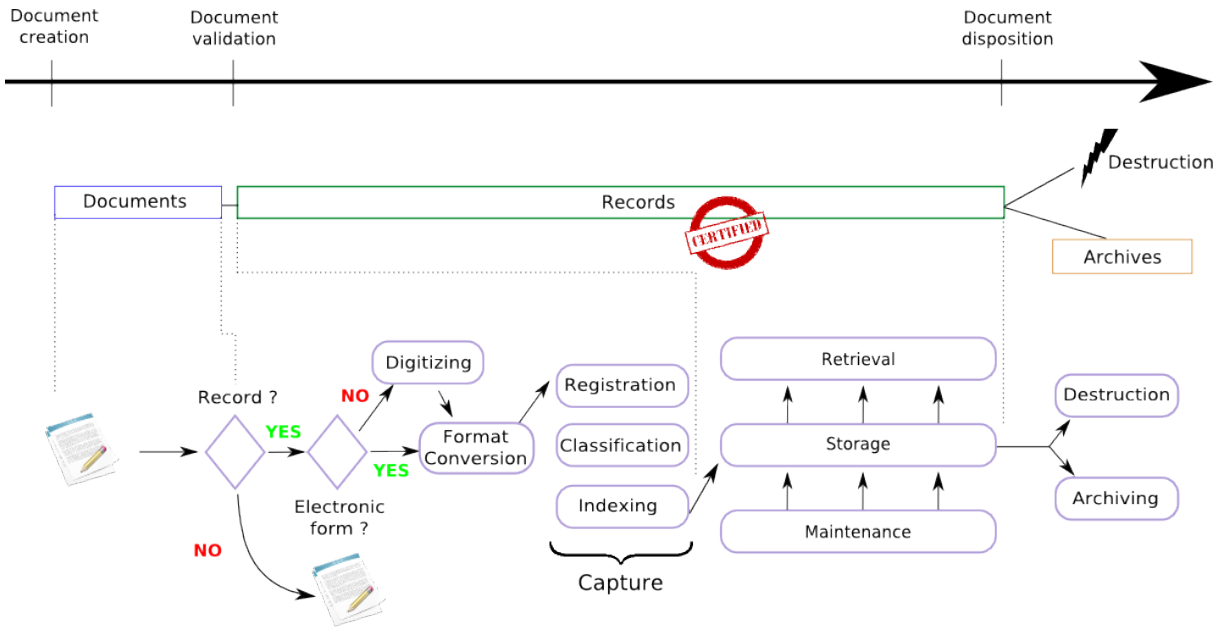

Figure 2: Workflow of an Electronic Records Management System

1) Document Creation / Document Validation

A **document** that has been previously created is transmitted to one or more recipient for advice. If that document is recognized to have value for the organization, then it has to be preserved. It is then validated by a person having the authority to do that, and it can no longer be modified, except with this person's agreement. The document can now be considered as a **record** for the organization.

This document now recognized as a record by the organization will become an **electronic record** as soon as it is locked on a digital support against change.

This Creation / Validation step encompasses the status identification of the document, the digitization if it is a non-digital document, a format conversion if needed, and the capture of the document.

(a) Status identification: record or simple document

The ERMS will only manage documents that contain information that are evidence of what the organization does or has done in the past and that are called records, as defined in the organization capture policy (based on legislation and internal procedures).

Before a hypothetical validation, each document will be analyzed according to the capture policy as illustrated in Figure 3 and, when a document meets the requirements, it is validated, and can pass through the other steps of the workflow.

Example: the bank Banko gives a property loan to Mr. Smith. If there is litigation, the document proving the property loan conditions needs to be afforded. Thus, the signed document needs to be captured by the ERMS because of the law or internal procedures as soon as it is validated. Once validated, the document is considered to be a record.

Figure 3: Status identification

(b) Digitizing

If the information is not at the origin available under electronic format, the document needs to be digitized (Figure 4), and its content can be converted into machine readable text through optical character recognition (OCR).

Metadata may be added to the digital copy in order to give additional information on the scanning process (the used scanning method, its characteristics, the person who made it, etc.). Metadata (literally meaning 'data about data') are data attached to a record or a document to give information about its structure, its ownership, its history, etc.

Example: the bank Banko digitizes the signed document with a scanner. The bank can choose if the document will be stored as a text, as an image, or as both (image for the proof and text (PDF) for text-searching and easier retrieval).

Figure 4: Digitizing the record

(c) Format conversion

The numeric document (digitally born or digitized) can then be converted (Figure 5) into a *durable* file format that ensures maintainability and useable through time if the original format is not supported by the system, or if it is not considered as a long-term format.

A lot of formats exist on the market. The table in Annex A gives an overview of the most used standards[12], in which format these kinds of files have to be retained, and which format is considered to be best suitable for the access to these kinds of files.

[12] *Overview done in 2011*

Example: the bank Banko could convert an electronic document with a '.doc' extension to a PDF/A file, because PDF/A is considered as a durable format.

Figure 5: Format conversion

(d) Capture

The capture of the record is "the process of lodging a document or digital object into a recordkeeping system and assigning metadata to describe the record and place it in context, thus allowing the appropriate management of the record over time"[13].

The capture of the records encompasses three main activities described below: registration, classification and indexing of records.

- **Registration**

The record is first registered (Figure 6) and receives "a unique identifier on its entry into the system" [1]. This unique identifier allows ERMS to manage the record through time.

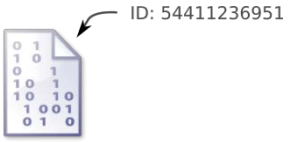

Figure 6: Registration

- **Classification**

The record is then classified (Figure 7), i.e. assigned to one or more categories from the classification scheme of the organization, mainly based on its contents and context. The classification scheme is defined during the creation of the ERMS by the organization following its needs and activities. "A classification scheme is the **foundation** of any ERMS. It allows an electronic record to be stored together with other records that provide its context, by defining the way in which the electronic records will be organized into electronic files, and the relationships between the files" [2].

The classification also includes the determination of user permissions and security restrictions on records.

[13] *http://www.naa.gov.au/records-management/publications/glossary.aspx*

Example: the document can be classified in 'property loan' in 'loan' in the file 'contract', according to the classification scheme of the bank Banko.

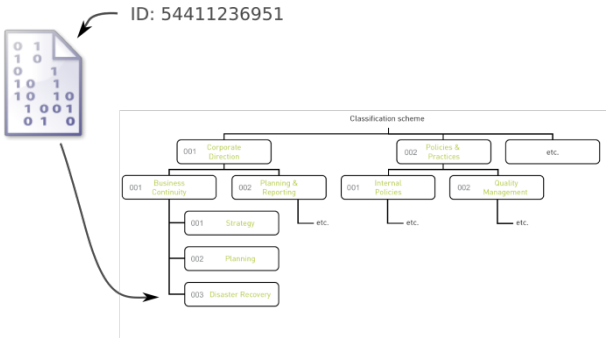

Figure 7: Classification and classification scheme example

- **Indexing**

The record, which is already registered and classified, is then indexed (Figure 8) to "establish access points to facilitate retrieval of records and/or information" [4].

Indexing in an ERMS can for example keep track of unique document identifiers, or of information extracted from the document content (through OCR). This information can also be used to provide inputs to the document metadata, or even to word indexes. Indexing is mainly supporting the records retrieval.

Example: the indexation process will find some information about the document: the Mr. Smith's signature, the date of the loan, the agent's signature the fact, that it is a property loan, etc.

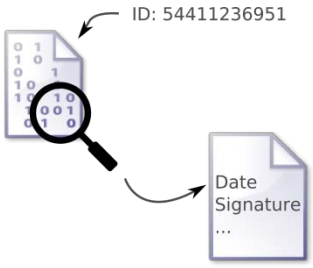

Figure 8: Indexing

2) Maintenance and retrieval

The validated document turned into a record is transmitted to the entity in charge to preserve it. This entity can be an electronic system. The record is preserved in such conditions that it is always readable and intelligible, but also credible and reliable i.e. one cannot suspect that it has been distorted or falsified.

Preservation of the record will last as long as stipulated in the legislation and documentation. This period of preservation of records is called the *retention period*.

During this phase, all the actions made on records are tracked, to prove their good use (who has accessed this record, when, etc.). Tracking is "creating, capturing and maintaining information about the movement and uses of records" [1].

This step encompasses the storage itself, the maintenance and the retrieval.

(a) Storage

Once indexed, the record can be stored in the ERMS. Storage (Figure 9) often includes the management of those records. Indeed, the storage is responsible for the place where the records are physically stored, and has to know for how long it has to keep those records in order to trigger the disposition. Furthermore, the storage must know when the migration of the records from a storage media to another (hierarchical storage management) has to take place.

Example: According to Banko RM policy, the document can be stored on a tape, on a CD, on a DVD, etc., or on several supports at a time (CD or tape to keep safe, hard disk drive to easily retrieve it).

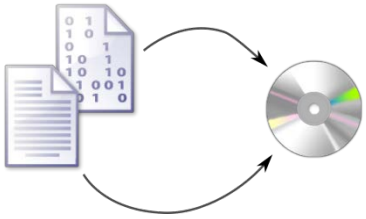

Figure 9: Storage

(b) Retrieval

Records are stored in the ERMS in order to give easy and trustful access to authorized users to specific information when needed. Retrieval (Figure 10) is the "active process of selectively recovering stored data" [3]. It consists of searching records and presenting them, on a screen, on a printed document, or any other media. Retrieval is the core of the ERMS because it allows searching for a record thanks to keywords or navigation into classification scheme, and above all allows the presentation of the record in order to be consulted.

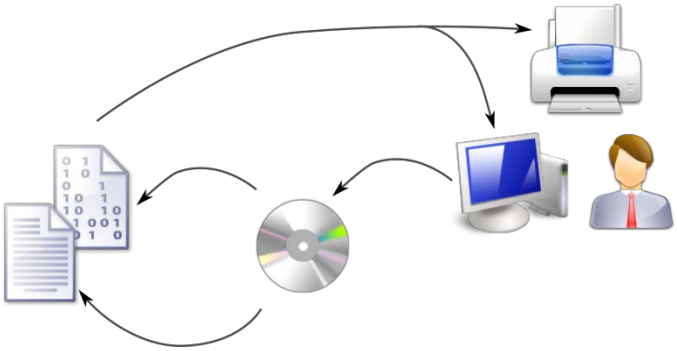

Figure 10: Search and retrieve

Example: Mr. Smith would like to review the interest rate of his loan. A search on his name, first name, loan type (property loan) allows the banker with authorized access to localize the record, and to present it on the screen.

(c) Maintenance

The records also need to be maintained in order to avoid system failure and guarantee system efficiency, including access management and security protection for the records. Maintenance can contain activities like migration and refreshing of records.

Maintenance (Figure 11) is defined as "the process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions" [5].

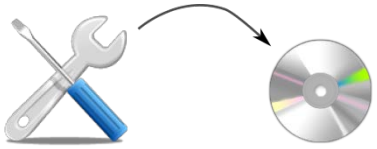

Figure 11: Maintenance

- **Migration**

The maintenance of records can require their migration (Figure 12) i.e. their "moving from one system to another, while maintaining the records' authenticity, integrity, reliability and usability" [1]. This may include conversion of resources from one file format to another, from one operating system to another, or from one programming language to another. Thanks to migration, the records remain fully accessible and usable through time, as technology changes. Migration is a critical process, as all the relevant information has to be preserved, even after a format conversion. Indeed, if any information is lost during the migration, it could be impossible to recover it since the original is usually deleted, the original format being obsolete. Newer formats may be incapable of capturing all the functionalities of the original format, or the converter itself may be unable to interpret all the nuances of the original format.

Example: the bank Banko notices that the new PDF version meets better their requirements (gain of storage space). The organization decides to do a migration of all PDF data.

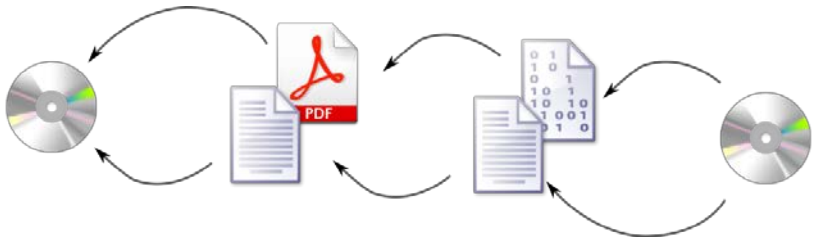

Figure 12: Migration

- **Refreshing**

Refreshing records (Figure 13) is often necessary due to the deterioration of physical media (e.g. due to media deterioration after some time).

Refreshing is the transfer of data between two similar storage media so there are no bitrate changes or alteration of data. This strategy may need to be combined with migration when the software or hardware required to read the data is no longer available or is unable to understand the format of the data.

Example: the bank Banko RM policy specifies that a CD has a 10-years-lifetime. Before reaching this deadline, the records it contains need to be transferred to another CD, to avoid a loss of the information.

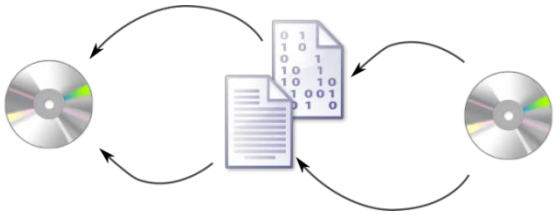

Figure 13: Refreshing

3) Disposition

Once the retention period is over (when a record reaches its end of legal or intern use duration), the document needs to be disposed of. This disposition can lead to its deletion or its archiving, depending on its historic value.

(a) Destruction

The record will be deleted with all data and metadata bond to it if the law gives such instruction or if the organization does not need it anymore (for preserving the organizational or collective memory). The ERMS will generally track this deletion, to keep a trace of the deleted record.

Example: the redemption date of the property loan was thirty years ago, the bank Banko in Luxembourg has to delete the record, according to the law.

Figure 14: Destruction

(b) Archiving

If the record has a value for preserving the organizational or collective memory, and the regulation framework does not force to its destruction, it will be transferred to the archives (organizational archives, city archives, national archives, etc.).

Example: the first contract ever signed by the organization has reached the end of its retention period, to preserve the organizational memory this contract will be transferred to the archives, as the law does not force to its destruction.

III. International and European standards

Several standards or manuals deal with RM or ERM. This section briefly describes some of the major ones. Some standards cover the whole RM workflow and some others focus more specifically on parts of the workflow.

1) *Records management/archives*

These standards give general principles and rules to define the RM strategy and the organization to put in place to reach the required efficiency and security. They are generic, unlike implementation and exploitation standards (with a strong aspect of implementation of the RMS) or technical standards (dealing with technical aspects, like specification of file format).

❖ ISO 15489 (Information and documentation -- Records management)

The objective of ISO 15489 is to define the field of RM. ISO 15489 was published in 2001 by the ISO TC 46/SC 11 (Information and documentation - Archives/records management), based on the Australian Standard AS 4390:1996 [6]. It is composed of two parts:

- ISO 15489-1:2001 [1] gives requirements and advices on managing records for the activities of an organization. It formulates guidance for RM operations;
- ISO/TR 15489-2:2001 [7] is an implementation guide for ISO 15489-1, containing a methodology and overview of RM processes.

Its objectives are to:

- give scope and benefits of RM;
- provide guidance on determining the responsibilities of organizations for records and records policies, procedures, systems and processes; and
- provide guidance on the design and implementation of a records system.

ISO 15489 targets the field of RM but does not address the specificities of ERM. It does not include the management of archival records within archival institutions either.
ISO 15489 is considered to be the reference for RM system providers, either electronic or not. Its concepts are widely adopted.

After defining the scope, giving some normative references and the definition of specific terms, the ISO 15489-1 standard explains the benefits of RM. Then, it lists the different aspects to take the regulatory environment into account. It recommends define a policy for RM, and define and assign RM responsibilities and authorities. The next section gives the RM requirements, expanding a list of principles that a RM policy should do.

It gives the main characteristics of a record: a record must be authentic, reliable, complete and unaltered, and useable. It will help to design and implement a records system. The standard gives some characteristics of a records system, such reliability, integrity, compliance, comprehensiveness and systematic management. The records system and methodology design, implementation and processes are close to the concepts and methodology treated in ISO/TR 15489-2.

Finally, ISO 15489-1 gives indications to monitor and audit the records system, and to train employees and any other individuals responsible for the whole or part of a business activity in making records.

- **MoReq (Model Requirements for the Management of Electronic Documents and Records)**

Published for the first time in 2001, MoReq has been developed by Cornwell Affiliates plc with support and management from experts from different countries, on behalf of the European Commission.

MoReq2 [2], the first major revision of MoReq, was published in 2008. It was developed by Serco Consulting and managed and supervised by the General Secretary of the European Commission in close collaboration with the DLM Forum (Document Lifecycle Management Forum), with the funding of IDABC's program[14] of the European Union for the European Commission.

MoReq2 focuses on the management of electronic records. It can be seen as an operational approach of ISO 15489. MoReq2 is an assembly of detailed technical requirements for ERM. It gives functional requirements to implement RM functions in an electronic system, or to evaluate such a system. About two thirds of the 800 requirements are mandatory ("the ERMS must…") and a third is desirable ("the ERMS should…"). The main objective is to describe how to create specific software for ERM.

MoReq2 mostly describes application software that is expressly designed to manage records. It includes some preservation features, as physical environment control, monitoring of error rate, comparison of copies. It also introduces some tools that are useful in an ERMS: classification scheme, access control, capture of the records, searching and presentation of records, and administrative functions. Organizational aspects are hardly covered.

MoReq2 can be used as a reference for the certification of RM software. However MoReq2 is heavy to implement, as the system has to fulfill many requirements to be compliant.

To meet this issue MoReq2010 (Modular Requirements for Record Systems specification for ERMS) has been published by the DLM Forum in May 2011. MoReq2010 is indeed lighter thanks to a new approach based on a core module (the mandatory requirements) coupled with some plug-in (optional) modules.

MoReq is used in Europe, but tends to become a worldwide reference in terms of requirements to create a system. However, at the moment very few systems are fully tested and certified as MoReq compliant. However most system providers use MoReq as a basis to create their own systems.

- **OAIS (ISO 14721: Space data and information transfer systems -- Open archival information system -- Reference model)**

The ISO 14721 standard [8] defines a conceptual model (OAIS) targeting long term archiving of electronic information. This conceptual model aims at describing a way to represent the interactions between the actors in an archive system. The OAIS model is a CCSDS (Consultative Committee for Space Data Systems) work at the request of ISO to establish general technical recommendations to encourage and facilitate spatial data exchange. OAIS became the ISO 14721 standard, first published in 2003 by the ISO TC 20/SC 13 (Aircraft and space vehicles - Space data and information transfer systems), and under periodical review at the end of 2011.

OAIS covers the durability problem of the archives, the recurrent migration problem of electronic data which must be indefinitely maintained. The standard does not cover the entire RM process described

[14] *Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*

in Chapter II.B.2 as it deals with archives and not with records. "An OAIS is an archive, consisting of an organization of people and systems, that has accepted the responsibility to preserve information and make it available for a Designated Community." OAIS is used in long-term preservation services. It is implemented worldwide, as it is the reference.

The goals of OAIS are to ensure that:

- the information provided to be preserved remain understandable to the Designated Community (people who understand content of archives documents without any sort of explanation);
- the information is managed in order to preserve the information content and authenticity;
- the preserved information makes available to the Designated Community;
- the information is preserved against all reasonable contingencies, which enable the information to be disseminated as authenticated copies of the original, or as traceable to the original.

The model presents the organization to put in place between a contributor, a user and the management of an OAIS, and describes their roles, their responsibilities and their interactions, as shown in Figure 15. The OAIS environment is made of Producers, Consumers (users) and Management.

Three information package types are introduced: Submission Information Package (SIP) from the producer to the system, Archival Information Package (AIP) inside the system and Dissemination Information Package (DIP) to present the information to the consumer, as shown in Figure 15. In OAIS, almost everything is information: information is a kind of knowledge that could be exchanged.

The OAIS model is divided in six main functional entities: entries (Ingest), storage (Archival Storage), data management, administration, preservation planning, and access. The detailed process mapping of each main entity enlightens secondary functions: interfaces and information flow between the different functions are described and characterized. Figure 15 describes the interactions between the actors of the OAIS.

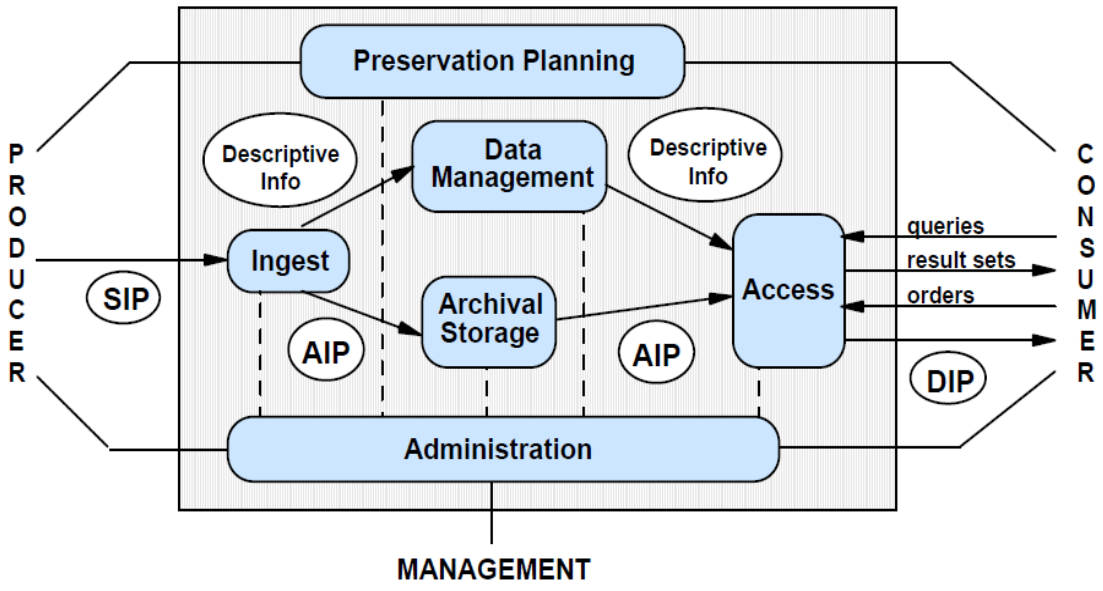

Figure 15: OAIS model

- **NF Z 42-013**

The first version of the AFNOR NF Z42-013 (*Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes*) French standard [9] was published in 1999 by the French ISO TC 171 mirror committee *Commission de Normalisation 171* (*Archivage - Cycle de vie du document et sécurité des données*). This standard was revised in 2001, and the last version was published in 2009 by the AFNOR board of directors. This standard has been introduced to ISO in 2003 under the reference ISO 18509, but it was not adopted. However, the updated standard of 2009 has been submitted in an adapted version to ISO in the ISO TC 171 under the reference ISO 14641 where it is still under discussion.

The standard provides specifications for technical and organizational measures for capturing, storing and retrieving electronic records in an Information System, to assure integrity and preservation during the whole records lifetime.

After an introduction explaining why this document has been created, the scope of the standard is summarized. Next, after giving some normative references, the standard gives a glossary of the terms used.

The RM principles are mentioned, where it is said that a RMS must assure integrity, durability, security, and traceability. Organizations do not have the same requirements level; the standard thus gives minimal requirements, and complementary requirements.

After that, the standard gives the general specifications of an ERMS, such as creating a file with a technical description of the system, listing RM profiles to limit access to records, describing exploitation procedures for capturing, storing, retrieving records, creating a security policy, describing methods to protect records such as time-stamp, data logging, security copy, and continuity plan.

It next treats the support in RM: removable and fixed media, physical and logical WORM (Write One Read Many), and rewritable media. The standard gives indication to preserve supports, and gives specifications for each type of support, by insisting on rewritable media and protection to avoid alteration.

The standard explains the capture process for digital documents, microform or paper documents, and analogical documents (magnetic bands). For each type of entry support, the standard gives specifications to capture the document into the RMS. After that, it treats of data compression for images and sound and video data, from paper, microform, sound or video documents. Next step is the format conversion: an entry format table recognized by the system has to be established.

The standard next indicates how to exploit records, for communication or presentation. This part includes the way to destruct records.

The next part describes how audits of the RMS must be done, their objectives, for intern audit as well as for extern audit.

Finally, the standard concludes with third party RM service provider and other third party service provider. It explains the activities of a third part RM services provider, and the different clauses to include for a contract with such a provider. Then the standard indicates the conditions in which a RMS can appeal to other third party service providers.

This standard is very general in the conception of the system, and is mainly axed on integrity and preservation. It is well-referenced by providers of document or RM solution in France.

- **ISO 16175 (Information and documentation -- Principles and functional requirements for records in electronic office environments)**

The International Council on Archives (ICA) is an international organization of archival institutions. It has similar interests in RM as what a national archival institution do: to promote better records, as to support future archives and accountability.

The ICA and its member institutions share resources to build awareness and develop guidance for better records such as standards, toolkits, advocacy materials, etc.

Some of the materials that have been produced to help improve the state of government records in developing countries may be of particular interest to any small organization (public or private sector) - where there is limited skill or resource for building RM solutions.

The standards concerned are the ISO 16175 series, made up of three parts:

- ISO 16175-1 (Overview and statement of principles) [4], defining the scope and the vocabulary: it aims to gives fundamental principles and functional requirements for software used to create and manage digital records in office environments;
- ISO 16175-2 (Guidelines and functional requirements for digital records management systems) [10], giving guidelines and functional requirements for an ERMS, requirements that can apply to electronic records irrespective of the media in which they were created and/or stored; and
- ISO 16175-3 standard (Guidelines and functional requirements for records in business systems) [11], giving general guidelines and functional requirements for keeping records in business systems implemented to automate business activities and transaction. Most business systems were originally not designed to manage records. This standard gives guidelines to identify and manage records of business activities transacted through business systems. This part 3 deals with the business reality as it assumes that records are managed by business systems, as it is usually the case.

The scope of the ISO 16175 series is pretty similar to MoReq2 but is dealing more with the implementation of specific business problems. The ISO 16175 series does not deal with long-term preservation of records.

ISO 16175 series is historically used in Australia, and spreads worldwide since its positive vote at the ISO level (ISO TC 46/SC 11).

- **ISO 30300 series (Information and documentation - Management Systems for Records)**

The ISO 30300 series of standards in Management System for Records (MSR) is a series currently in development by ISO TC 46/SC 11. It intends to be an implementation of Management System Standards (MSS) in the RM field. MSS creates unification between standards by adopting the same structure and using identical clause titles, sequence of clause titles, text and definitions. The only divergences for standards would be on specific differences in managing their fields of application. The MSR is designed to assist organizations in order to implement, operate and improve an effective

management system for records. Indeed, this series accompanies ISO 15489 standard by creating three obligations:

- the obligation to analyze the RMS and align records processes with the management systems;
- the obligation to check the consistency of the ERMS with other MSS of the organization, such as ISO 9000, ISO 27000, ISO 20000, ISO 14000, etc.;
- the obligation to check the good working of the system by an external audit.

Figure 16 gives an overview of the position of the ISO 30300 series in the RM standards.

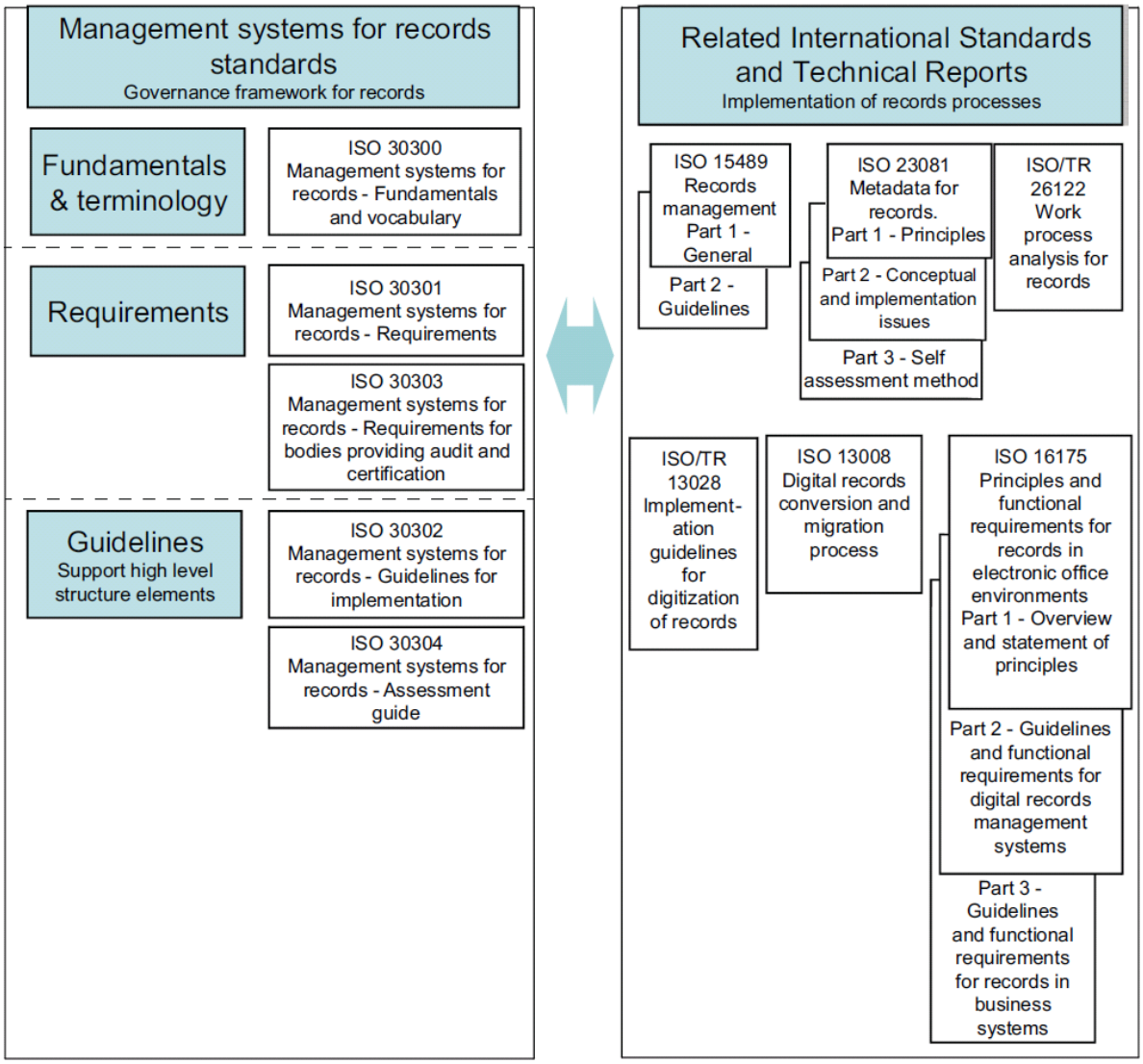

Figure 16: ISO 30300 series and other records management standards (source: ISO/FDIS 30300)

2) Specific standards

Specific standards deal with a part of the RM workflow seen in Figure 2. They are introduced in Figure 17, and have been studied in detail by CRP Henri Tudor in the NormaFi-IT project.

3) Conclusion

A lot of standards deal with RM or with an aspect of this field. The previously introduced standards have been chosen according to their relevance, their usefulness and the actual state of the art and standard status, as well as a subjective opinion.

The Figure 17 depicts the standards introduced in this document with their covered processes in RM, with the standards that cover most of the workflow in red, and the important standard in each step in orange.

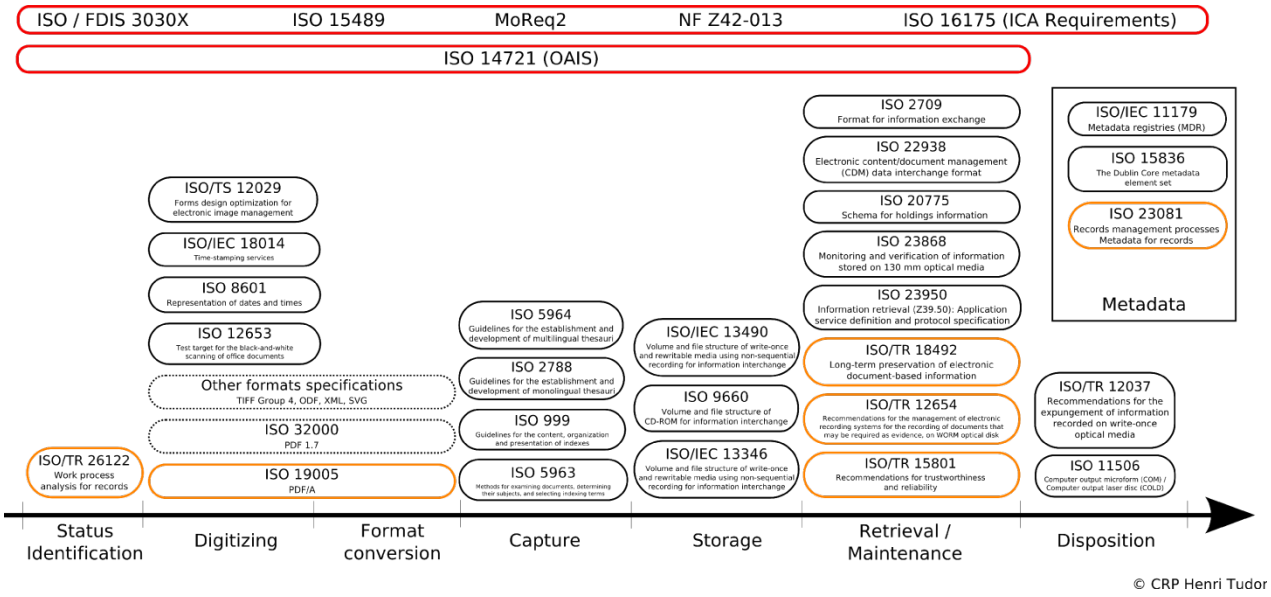

Figure 17: Standards and their covered processes [15]

[15] *See Annex B for a full-sized image*

IV. Context in Luxembourg

At the end of 2011, there is no law, label or international standard giving a 'legal' attribute to a RMS. If there is a conflict on the legal value of a record, the judge will decide of its reliability.

However, some directives, laws, standards or guidelines can help to create a reliable ERMS by giving, for example, a legal value to electronic documents mainly through the definition and use of some concepts, like for example the digital signature.

Furthermore, legislation requires organizations to retain digital information for significant periods of time (sometimes 10 years or more). Such legislation includes for example the Data Protection Directive 95/46/EC or MiFID (Markets in Financial Instruments Directive 2004/39/EC), as enacted in EU, Sarbanes-Oxley and HIPAA in the US and the Basel II Accord worldwide. It applies not only to organizations' core business data but also to day-to-day administration data such as contracts, pension plans, health and safety records, etc. Financial institutions are particularly concerned with compliance and the need to keep audit trails of transactions to minimize liability.

1) Legislation

Electronic signature and electronic proof

One of the most used mechanism to guarantee authenticity and integrity for an electronic document is the **electronic signature.** Indeed, this mechanism uses mathematical algorithms, such as the hash value of the record (a unique value obtained from series of bits: if one of these is changed, the hash value is drastically changed) and a personal certificate to create an electronic signature.

Indeed, in Luxembourg, the Chapter II. Art. 18 of the *Loi du 14 août 2000 relative au commerce électronique* stipulates that an electronic private deed has the same value as the original one if there are reliable guarantees that the deed was not modified, and that **the electronic signature is a group of data linked to the deed which guarantee its integrity**. Furthermore, thanks to the fact that in Luxembourg the signature cannot be dismissed by a judge simply for its electronic nature, the electronic signature is a good way to protect electronic proof.

The article 460 of the CSS (*Code de la Sécurité Sociale*) specifies that electronic images from paper documents stored on an electronic support as specified in the 'standard norm' have the same probing value than these original paper documents. However this 'standard norm' has not been formally specified so far, which makes this article difficult to refer to.

2) Prestataires de Services de Dématérialisation et/ou de Conservation (PSDC)

A *Prestataire de Services de Dématérialisation et de Conservation* (PSDC) is a service provider that offers digitization and paperless office services (*dématérialisation*) and/or storage (preservation) of records. A PSDC can support organizations who want to keep their electronic documents and/or electronic records in an external safe place, and who wish to get rid of paper by creating electronic workflows. For now, there is no framework to regulate PSDC in Luxembourg. Nevertheless, the new legal framework for electronic records will give details on this status. In a future law ILNAS will be responsible for the accreditation of PSDC[16].

[16] *http://www.ilnas.public.lu*

References

[1] ISO (International Organization for Standardization). ISO 15489-1:2001: Information and Documentation - Records Management - Part 1: General, 2001.

[2] Serco Consulting. Model Requirements or the management of electronic records (MoReq2), 2008.

[3] ISO (International Organization for Standardization). ISO 5127: Information and documentation - Vocabulary, 2001.

[4] ISO (International Organization for Standardization). ISO 16175-1: Information and documentation - Principles and functional requirements for records in electronic office environments -Part 1: Overview and statement of principles, 2010.

[5] ISO (International Organization for Standardization). ISO/IEC/IEEE 24765: Systems and software engineering -Vocabulary, 2010.

[6] Standards Australia. AS 4390-1996 : Records Management, 1996.

[7] ISO (International Organization for Standardization). ISO/TR 15489-2:2001: Information and documentation - Records management - Part 2: Guidelines, 2001.

[8] ISO (International Organization for Standardization). ISO 14721: Space data and information transfer systems – Open archival information system - Reference model, 2003.

[9] AFNOR Association Française de Normalisation. NF Z42-013: Archivage électronique- Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes, 2009.

[10] ISO (International Organization for Standardization). ISO 16175-2: Information and documentation - Principles and functional requirements for records in electronic office environments -Part 2: Guidelines and functional requirements for records in electronic office environments, 2011.

[11] ISO (International Organization for Standardization). ISO 16175-3: Information and documentation - Principles and functional requirements for records in business systems, 2010.

Annexe A. Formats

The Table 1 gives an overview of the most used standards and on which format these kinds of files have to be retained, and which format is considered to be best suitable for the access to these kinds of files. The first column gives the media type, the second the file formats that could be met before the capture by the ERMS, the third the format privileged for preservation, the fourth the format that could be used for an easy access, and the last one the tool that could be used to make the format conversion.

Media type	File formats	Preservation format(s)	Access format(s)	Conversion tool
Audio	AC3, AIFF, MP3, WAV, WMA	WAVE (LPCM)	MP3	FFmpeg
Email	PST	MBOX	MBOX	readpst
Portable Document Format	PDF	PDF/A	PDF	Ghostscript
Presentation files	PPT	ODF, PDF/A	PDF	Unoconv/ OpenOffice
Raster images	BMP, GIF, JPG, JP2, PNG, PSD, TIFF, TGA	Uncompressed TIFF, JPEG 2000	JPEG	ImageMagick
Raw camera files	RAW image	DNG	JPEG	DigiKam DNG Converter
Spreadsheets	XLS	ODF, PDF/A	Original format	Unoconv/ OpenOffice
Plain text	TXT	Original format	Original format	None
Vector images	AI, EPS, SVG	SVG	PDF	Inkscape
Video	AVI, FLV, MOV, MPEG-1, MPEG-2, MPEG-4, SWF, WMV	MPEG-2	MPG	FFmpeg
Word processing files	DOC, WPD, RTF, ODT	ODF, PDF/A	PDF	Unoconv/ OpenOffice

Table 1: File formats and preservation / access formats[17]

[17] *Inspired by http://www.archivematica.org/wiki/index.php?title=Media_type_preservation_plans*

Annexe B. Standards in Records Management and their covered processes

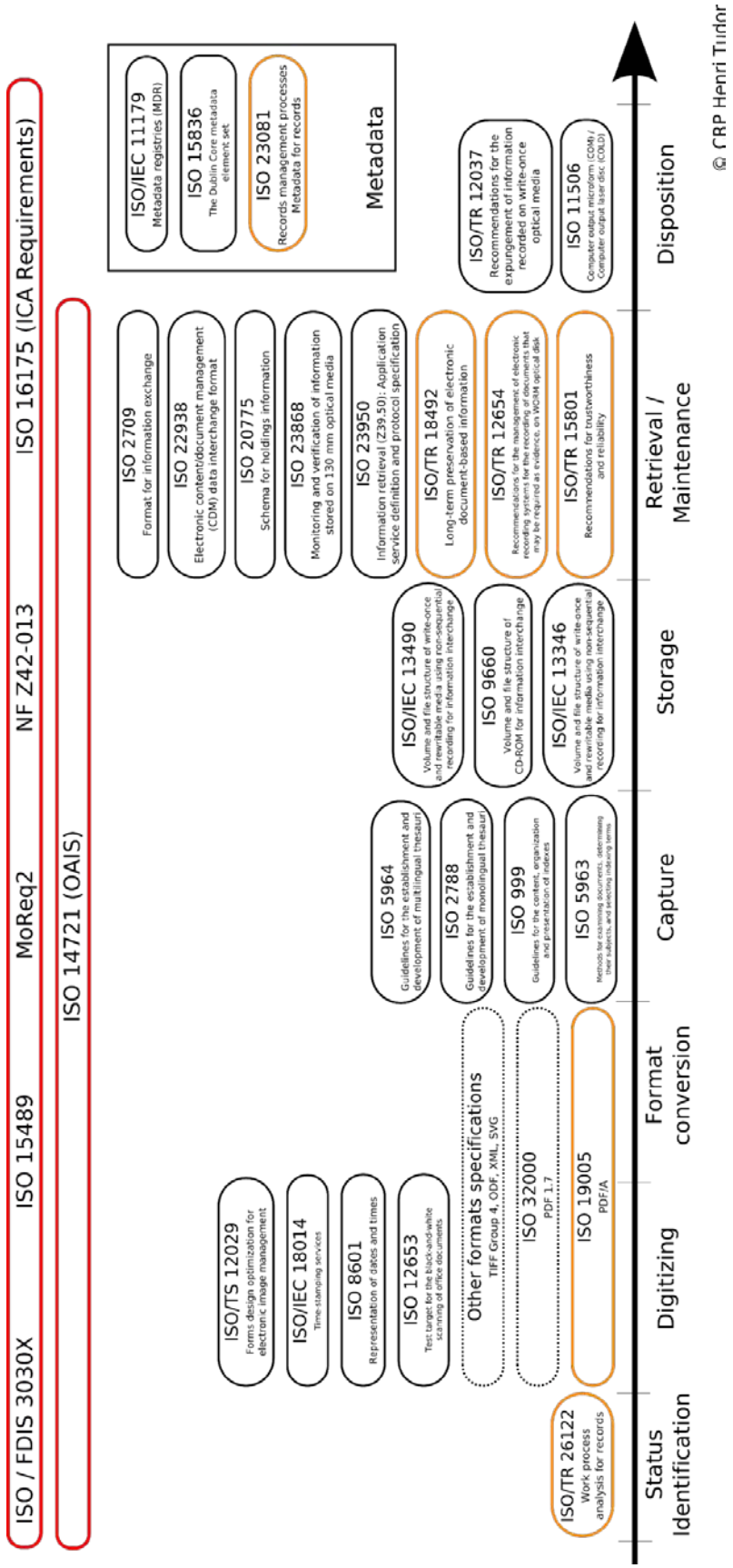

Figure 18: Standards in Records Management and their covered processes

C) Business and IT continuity

As an organization evolves and grows, the ramification and importance of its assets, (i.e. what has a value for the organization), increase. While most organizations invest in systems resilience to prevent the degradation or loss of Information and Communication Technology (ICT) services, there is always a remaining risk of disruption of business services and support, and therefore, disruption of business operations. Moreover, there are some fields of activities where a business disruption of a few minutes can have a dramatic impact, and a longer disruption can even lead to bankruptcy or have a serious impact on the local or national economy (i.e. banking, telecommunication or medical sectors).

In order to cope with such risks, Business Continuity Management emerged in companies as in technical papers, good practices, public specifications and some international standards.

Business Continuity Management (BCM) is defined as a holistic system. It contains all the activities required against design, implement, review and upgrade relevant mechanisms aiming at identifying potential threats to an organization and their potential impacts to business operations. BCM provides a framework for building organizational capability for an effective response to safeguard the objectives and interests of the organization (including its obligations) from business-critical impacts.

BCM is a management activity that supervises among other domains technical aspects such as Information Technology (IT)[18] Service Continuity (ITSC) and Disaster Recovery Plans (DRP). BCM can also be considered at a larger scale as a societal challenge managed in the Societal Security field.

The first section of this chapter presents the key concepts related to business continuity. Then, the second section presents the mechanisms of business continuity management, based on the different steps composing the BCM lifecycle. The third section focuses on ITSC, supporting the overall BCM process. The fourth section is about international standards and guidelines defining best practices in both fields of BCM and ITSCM (Information Technology Service Continuity Management). Finally, the last section describes the national initiatives on ITSCM, through a presentation of the national context and of the regulated framework.

[18] *In this chapter, the "IT" and "ICT" acronyms are used, because they are both mentioned in the different standards studied. However, they have the same meaning all along this chapter.*

I. Concepts

Business Continuity is the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level in case of disruption. This requires organizations to put in place a holistic management process that identifies potential threats against the organization and the impacts to business operations that, if realized, those threats might cause. The underlying idea is to maintain the activity, not only after a natural calamity but also in the event of smaller disruptions including illness or departure of key staffers, supply chain partner problems or other challenges that businesses face from time to time.

This management process provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities [1]. Business continuity is also sometimes called **operational continuity** to emphasize its relevance to all types of organizations in the public and private sectors.

Business Continuity Planning (BCP) deals thus with taking pro-active measures to ensure continuity of business as well as plans to manage the response and recovery from a business interruption.

IT being a major supporting activity for most organizations whatever their size, **ITSCM** supports the overall Business Continuity Management process. It ensures that the required IT technical and services facilities can be recovered within required, and agreed, business timescales. Moreover, it also ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services [2][19]. These activities contribute to building **ICT readiness for business continuity.**

Disaster recovery is the process by which you resume business after a disruptive event. **ICT disaster recovery** is the ability of the ICT elements of an organization to support its critical business functions to acceptable level within a predetermined period of time following a disruption [3]. The IT DRP supports the recovery effort by detailing the IT system recovery priorities and time constraints, plans and strategies for recovery as well as detailed restoration procedures. The priorities and time constraints are driven from the business continuity requirements.

The main purpose of standards and Good Practices Guidelines in this field are to support organizations preparing their ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions that could affect continuity (including security) of critical business functions. BCM processes constitute a framework to:

- enable proactive improvement of the resiliency of the organization
- test and validate the way to recover from disruption within acceptable conditions
- allow the organization to protect its critical activities from disruptions, to the benefit of all its stakeholders

The following concepts are presented in the coming sub-sections: resilience, risk management, minimum business continuity objective, testing / exercising, embedding BCM in the organization's culture, and plan-do-check-act.

[19] *ITIL® is a registered trade mark of the Cabinet Office. This report is making reference to ITIL v3, the most widely spread version of the IT Infrastructure Library. A new version has been edited in the meantime as ITIL 2011.*

1) Resilience

Resilience is defined as the capacity to recover quickly from difficulties or toughness. Resilience is also widely defined as the ability of an organization to resist being affected by an event [4] or by disruptions [3], i.e. to absorb, respond and recover from disruptions [5]. Resilience is not fundamentally about stopping or preventing disruption happening in the first place, it is more about being able to keep the business going after such events occur.

2) Risk management

BCM is focused on identifying vulnerabilities within organizations, especially those that are critical for the business. BCM will use risk management techniques to analyze the potential impact of events on the business. If a threat on a critical product, process or service is identified and cannot be mitigated, then a BCM response is essential to ensure its resilience.

3) Minimum Business Continuity Objective

The business impact analysis is performed against a target Minimum Business Continuity Objective (MBCO) defined by/with the management of the organization. MBCO sets the minimum level of service that needs to be kept or restored for each single critical business or supporting activity in case of threat or disruption. The framework put in place shall be responsible for reducing the impact of disruptions so that the Minimum Business Continuity Objective is reached earlier, as shown on Figure 1 where curve 1 represents the situation after implementation of a BCM program and curve 2 represents the situation without implementation of a BCM program.

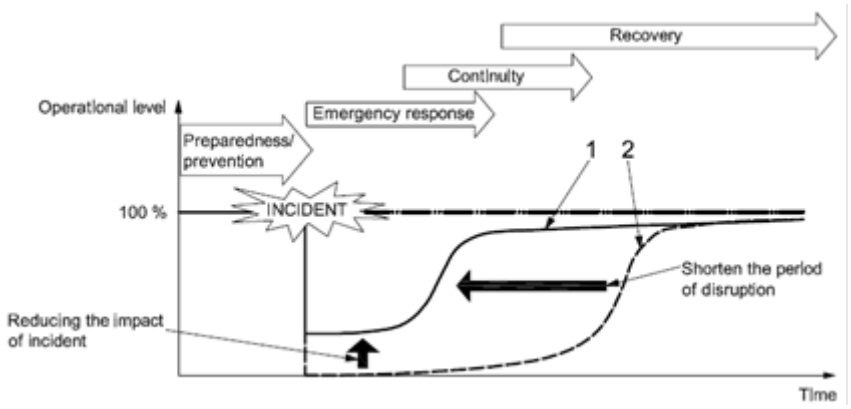

Figure 1: ISO 22399 - How to reduce incident impact on business

4) Testing / Exercising

While Business Continuity is mostly a proactive process, which focuses on avoiding or mitigating the impact of a crisis, Disaster Recovery is often considered to be reactive as it aims at restoring the organization to business after a risk occurs. However both processes are really interconnected, the Disaster Recovery Plan will just be activated *a posteriori,* in case of a crisis. The process itself should have been defined as part of Business Continuity management activities. Moreover the whole framework has to be documented and also tested to make sure operations and business can really recover or survive in case of a real crisis.

5) Embedding BCM in the Organization's Culture

To be successful, Business Continuity should be "owned" by everyone within an organization. All management levels play an essential role in the initial identification of critical activities and processes. Moreover, all staff should be convinced that it is a serious issue for the organization and that each of them has a role to play. Each level of the organization should accept responsibility for working to achieve that. Business Continuity considerations can/should be integrated into all the organization's operational and business decisions.

6) Plan-Do-Check-Act

While they may have been presented differently over time, the Business Continuity processes should be aligned on a continual improvement cycle.

Following this approach helps to measure the results of improvement initiatives towards predefined goals. It also enables to keep the improvement going, as the organization context is keeping on moving, with the introduction of new risks, new priorities, and new challenges with an always higher market pressure.

II. Mechanisms

BCM is a management activity that proactively develops the organization's ability to cope with and respond to service or business disruption. Taking the moving characteristics of today's businesses and society into account, this management activity is most of the time structured on a continuous lifecycle. The BCM lifecycle comprises six steps constituting the BCM program [5].

The scope and structure of the BCM program components can vary and each element should be tailored to the context of the organization implementing the approach (Figure 2).

Figure 2: BCM lifecycle – BCI Good Practice Guide & BS 25999-1

1) BCM Program Management

Based on the BCM Policy, BCM Program Management is at the heart of the BCM process. It establishes the organization's approach to business continuity. It enables the business capability to be established and maintained, taking the context and characteristics of the organization into account. The BCM program must be fully aligned with the organization's strategy, and its short, medium and long term goals. BCM alignment with the organization's strategy cannot be ensured without close and continuous collaboration of key stakeholders at the highest level of management. The participation of top management is crucial to ensure that BCM is correctly introduced, adequately supported, and established as part of the organization's culture.

Top management will help to set the scope of the BCM program by identifying the key (critical) products, services and processes that support the organization's objectives, obligations and survival. Determination of critical assets should be based on a sound Business Impact Analysis (BIA).

A BCM program should be put in place to achieve the objectives defined in the business continuity policy. BCM Program Management involves:

- assigning responsibilities,
- implementing business continuity in the organization, and
- the ongoing management of business continuity.

It is important that a person with appropriate authority has overall responsibility for the BCM and is directly accountable for ensuring its continued success.

2) Understanding the organization

The identification of the organization's critical assets, processes and services is the cornerstone of the BCP program. It is important that the organization understands the interdependencies of its own activities (inside the organization) and any reliance or dependencies it has on external organizations.

The purpose for the organization is to determine what is to put in place to preserve its critical activities from disruption, including parts of these activities or services supported or provided by subcontractors.

The organization should measure the impact of a disruption to the activities that support the organization's business. This should be determined and documented through performing Business Impact Analysis (BIA). The BIA also needs to identify dependencies between activities, and thus to determine the real scope of the processes and functions supporting business activities. These dependencies may include suppliers, people, other business processes, IT services, etc.

The impact of a disruption on business will depend on the patterns of business activities, as business activities tend to vary over time, depending on internal, commercial or legal constraints. BIA will thus have to identify the maximum tolerable period of disruption for each activity over time.

The organization may categorize its activities according to their priority for recovery. Activities whose loss would have the greatest impact and need to be recovered most rapidly may be termed "critical activities". These activities will have the highest priority for recovery, even if less critical activities also need to be recovered.

For each critical activity that needs to be preserved or recovered, the organization should estimate the resources that will be required, e.g.:

- Staff members per skill and knowledge profile
- Facilities and equipment, including ICT infrastructure
- Provision of information, including activity records
- Support services and suppliers

The level of resources needed should be evaluated with the stakeholders.

The level of risk to which each (critical) activity is exposed should be clearly understood. Some risks will be accepted by the organization, but the vulnerability of each type of resource supporting an activity and the potential impact if that threat would become an incident and caused a business disruption are also critical information for the definition of the BCM strategy.

As a result of the BIA and the risk assessment, the organization should identify measures that:

- Reduce the likelihood of a disruption,
- Shorten the period of disruption, and
- Limit the impact of a disruption on the organization's critical activities.

These measures (known as loss mitigation and risk treatment) may consist in: business continuity based on Recovery Time Objective (RTO), risk acceptance, risk transfer to third party, or modification to the critical activity if compatible with the business strategy.

3) Determining business continuity strategy

As a result of the BIA and risk assessment made to understand the risk exposure and potential impact on critical activity, the organization can select the appropriate continuity strategy.

The organization should consider strategic options for its critical activities and the resources that each activity will require to recover from disruption. The most appropriate strategy or strategies will depend on a range of factors such as:

- the maximum tolerable period of disruption of the critical activity;
- the costs of implementing a strategy or strategies; and
- the consequences of inaction.

The organization should ensure that the continuity solution proposed will not be affected by the same incident that causes the business disruption.

The BCM strategy will normally target a mix of all organizational resources: people, premises, technology, information, supplies, and stakeholders.

When IT is concerned, it is important to pay attention to the fact that IT services need complex continuity strategies, which should be closely bound to the Information strategies to ensure that information vital to the organization's operation is protected and recoverable according to the timeframes described within the BIA.

4) Developing and implementing a BCM response

Once the organization has defined its continuity strategy (based on its understanding of its risk exposure and potential impact on critical activities, and on its risk appetite or aversion), it should define an incident response structure that will enable an effective response and recovery from disruptions. This structure should trigger an appropriate business continuity response, and enable the organization to take control of the situation, confirm the nature and extent of the incident, contain the incident, and communicate with stakeholders.

This response should be managed according to predefined plans, processes and procedures to manage the incident, and for the activation, operation, coordination and communication of the incident response. These plans, processes and procedures should support the management of incidents, the continuity of business in case of an incident, and the recovery of business in case of disruption of activity.

5) Exercising, maintaining and reviewing BCM arrangements

The ability to response in case of an incident, service disruption or crisis is crucial for ensuring the continuity of activities. Having worked on plans to define how to react if ever an incident occurs does not guarantee that things will happen as described, that people will know what to do, and that the plans have been well designed.

Verifying the effectiveness of the BCM arrangements is essential and provides assurance that critical activities can be recovered as required after an incident. The maintenance and review of the incident, continuity and recovery plans need to be organized as an ongoing activity to cope with the changing environment and to make sure that any change (internal or external) that impact the organization is reviewed in relation to BCM. Exercising the BCM arrangement helps to solve deficiencies or inaccuracies in the BCP by:

- practising the organization's ability to recover from an incident;
- verifying that the BCP incorporates all organizational critical activities and their dependencies and priorities;
- highlighting assumptions which need to be questioned;
- installing confidence amongst exercise participants;
- raising awareness of business continuity throughout the organization by publicizing the exercise;
- validating the effectiveness and timeliness of restoration of critical activities; and
- demonstrating competence of the primary response teams and their alternatives.

The main challenge in case of incident is to have everyone behaving as expected (i.e. as described in the plans). This can obviously not happen by chance as with the pressure the incident is adding even more complexity on the human interactions. The exercise program should consider the communication and the roles of all parties, including key third party providers, outsourced partners and others who would be expected to participate in recovery activities. An organization may include such parties in its exercises.

Exercise programs should be consistent with the scope of the business continuity plan(s). The exercise program should lead to objective assurance that the BCP will work as anticipated when required. The program should:

- exercise the technical, logistical, administrative, procedural and other operational systems of the BCP;
- exercise the BCM arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.);
- validate the technology and telecommunications recovery, including the availability and relocation of staff.

6) Embedding BCM in the organization's culture

Creating and embedding a BCM culture within an organization can be a long and difficult process which might encounter a level of resistance.

However all staff have to understand that BCM is a serious challenge for the organization and that they have an important role to play in maintaining the delivery of products and services to their clients and customers. Building, promoting and embedding a BCM culture within an organization ensures that it becomes part of the organization's core values and effective management.

Development of a BCM culture is supported by:

- leadership from senior personnel in the organization;
- assignment of responsibilities;
- awareness raising;
- skills training; and
- exercising plans.

III. IT Service Continuity Management

It being a major supporting activity for most organizations whatever their size, **ITSCM** supports the overall Business Continuity Management process. ITSCM ensures that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk) can be recovered within required, and agreed, business timescales, and that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services[20].

ICT disaster recovery is the ability of the ICT elements of an organization to support its critical business functions to acceptable level within a predetermined period of time following a disruption[21]. The IT DRP supports the recovery effort by detailing the IT system recovery priorities and time constraints, plans and strategies for recovery as well as detailed restoration procedures. The priorities and time constraints are driven from the business continuity requirements.

The processes and infrastructure put in place by IT to give the best response in case of incident of disruption should be defined based on sound analysis of the technical (infrastructure) and business context. This should be done through an iterative cycle during which business and IT align their strategies for IT to design its continuity plans as shown on Figure 3 (Adapted from PAS 77:2006 [6]).

Figure 3: Relationship with business and IT strategy

The main purpose of standards and Good Practices Guidelines in this field is to support organizations preparing their ICT services/infrastructures to be ready to support business operations in case of emerging events and incidents, and related disruptions that could affect continuity (including security) of critical business functions.

Failures in ICT services, including the occurrence of security issues such as systems intrusion and malware infections, will impact the continuity of business operations. Thus managing ICT and related continuity with other security aspects form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical business functions requiring business continuity are usually dependent on ICT. This dependence means that disruptions to ICT can constitute strategic risks to the reputation of the organization and its ability to operate.

Effective BCM is frequently dependent on effective ICT readiness to ensure that the organization's objectives can continue to be met in times of disruption, and the BCM structure and program themselves can be dependent on ICT. ICT readiness is thus an essential component for many organizations in the implementation of BCM and information security management.

[20] *ITIL – IT Infrastructure Library*
[21] *ISO/IEC 27031 – Business Continuity Management*

ICT continuity management and ICT readiness will apply the BCM concepts to:

- enable proactive improvement of the ICT resiliency of the organization
- test and validate how an organization's ICT can recover from disruption within acceptable conditions
- allow the organization to protect its critical ICT infrastructure and services from disruptions, to the benefit of the business and all its stakeholders

ITSCM should be closely aligned with the IT strategy to identify information systems and services which require high levels of resilience, availability and capacity. ITSCM should also be part of the overall BCM initiative to ensure that it can give an adequate response to business expectations in terms of business continuity.

IV. International standards and guidelines

Several standards or Best Practice guides deal with Continuity Management at different levels. This section briefly describes some of the major ones. Some standards focus on IT Service Continuity Management, some on IT Readiness for Business Continuity, or just on Business Continuity Management.

1) Generic standards

❖ BS 25999 – BUSINESS CONTINUITY MANAGEMENT (PARTS 1 & 2)

This **British standard** (BS) is internationally renowned as it was **the first to define requirements** for a Business Continuity Management System (BCMS) i.e. a management system dedicated to Business Continuity. It is actually composed of two parts.

Part 1 [1] establishes the process, principles and terminology of **business continuity management** (BCM). The purpose of this standard is to provide a basis for understanding, developing and implementing business continuity within an organization and to provide confidence in the organization's dealings with customers and other organizations. It also enables the organization to measure its BCM capability in a consistent and recognized manner. This standard provides a system based on BCM good practice and is intended for use by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organization; from those with a single site to those with a global presence; from sole traders and small-to-medium enterprises (SME) to organizations employing thousands of people. It is therefore applicable to anybody who holds responsibility for any operation, and thus the continuity of that operation. This document gave birth to ISO/PAS 22399:2007.

Part 2 [7] specifies requirements for planning, establishing, implementing, operating, monitoring, reviewing, exercising, maintaining and improving a documented BCMS within the context of managing an organization's overall business risks. The requirements specified in this British Standard are generic and intended to be applicable to all organizations (or parts thereof), regardless of type, size and nature of business. The extent of application of these requirements depends on the organization's operating environment and complexity. An organization should design a BCMS that is appropriate to its needs and that meets its stakeholders' requirements. These needs are shaped by regulatory, customer and business requirements, the products and services, the processes employed, the size and structure of the organization, and the requirements of its stakeholders. It can be used by internal and external parties, including certification bodies, to assess an organization's ability to meet its own business continuity needs, as well as any customer, legal or regulatory needs. This document is at the origin of ISO 22301 (standard under development).

❖ ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management

Produced under ISO technical committee ISO TC 223 Societal Security, ISO/PAS 22399:2007 [4] has been published in November 2007 and confirmed in 2011. This standard is the **first internationally ratified document** regarding Incident Preparedness and Operational Continuity Management (IPOCM) within the context of societal security. It reflects the international consensus on best practices based on key contributions from existing national standards developed in US, UK, Australia, Israel and Japan.

ISO/PAS 22399:2007 has been developed to address the global awareness that both the public and private sector must proactively prepare for unexpected, disruptive incidents. It establishes the process, principles and terminology for incident preparedness and operational continuity management (IPOCM).

This guideline provides general guidance to develop its own specific performance criteria for incident preparedness and operational continuity, and design an appropriate management system. It provides a basis for understanding, developing and implementing continuity of operations and services within an organization. It allows to provide confidence in business, community, customer, first responder and organizational interactions. It also enables the organization to measure its resilience in a consistent and recognized manner.

This standard is applicable to all sizes of public and private organizations engaged in providing products, processes, or services that wish to:

- understand the overall context within which the organization operates;
- identify critical objectives;
- understand barriers, risks, and disruptions that may impede critical objectives;
- evaluate residual risk and risk tolerance to understand outcomes of controls and mitigation strategies;
- plan how an organization can continue to achieve its objectives should a disruptive incident occur;
- develop incident and emergency response, continuity response and recovery response procedures;
- define roles and responsibilities and resources to respond to an incident;
- meet compliance with applicable legal, regulatory and other requirements;
- provide mutual and community assistance;
- interface with first responders and the media;
- promote a cultural change within the organization that recognizes that risk is inherent in every decision and activity, and must be effectively managed.

ISO/PAS 22399:2007 presents the general principles and elements for incident preparedness and operational continuity of an organization. The extent of its application will depend on factors such as the policy of the organization, the nature of its activities, products and services, and the location in which it functions.

Its scope, however, excludes specific emergency response activities following an incident such as disaster relief and social infrastructure recovery that are primarily to be performed by the public sector in accordance with relevant legislation. It is important that coordination with these activities be maintained and documented.

ISO/PAS 22399:2007 incorporates the key elements and attributes of preparedness and continuity management into a continual improvement management cycle applying the Plan-Do-Check-Act (PDCA) principles to support consistent and integrated implementation and operation with related management standards.

❖ **BCI – Good Practice Guidelines (2010)**

The Good Practice Guidelines [5] developed by Business Continuity Institute are widely known and used in the Luxembourg financial institutions.

With 108 pages, this BCI document is still used as a reference regarding BCM implementation. It presents and explains key activities to set up a BCM within an organization. It has a strong relationship with the BS 25999 standards as it can be seen from the fact that it uses almost the same schema for describing the BCM life cycle. The document states however that this relationship is only on high level, which is confirmed when going through the details of the document.

The document includes the history of the BCM discipline and a glossary that is widely known and accepted among practitioners. Additionally it divides the life cycle into the following phases:

- Policy and Program Management (the term "Policy" in this phase of the lifecycle is the only difference with the lifecycle proposed by the BS 25999 standards)
- Embedding BCM in the organization's culture
- Understanding the organization
- Determining BCM strategy
- Developing and implementing BCM response
- Exercising, maintaining and reviewing BCM

In contrast to the BS 25999 standards, this document goes further into the detail of the different lifecycle phases providing advice on practices and tools that can be used when adopting a BCM strategy in an organization.

2) Standards related to IT matters and digital trust

❖ ITIL® - IT Infrastructure Library

ITIL [2] is a set of best practices for the management of IT services, recognized as the main *de facto* standard in IT Service Management by the industry. ITIL is defining processes and functions that organizations should put in place or adapt to their own context to maximize value for all stakeholders. ITIL focuses on aligning IT to the business needs and strategy. To that respect, ITIL defines an IT Service Continuity Management as one of the processes of the Service Design phase of the service lifecycle. Indeed, the way the service is designed should be influenced by business and IT continuity requirements.

Being service focused, ITIL assumes that Business Continuity is the main driver for ITSCM, which supports the overall business continuity management process by ensuring that the required IT technical and service facilities can be recovered within an agreed business timescale. ITIL divides the ITSCM process in four phases: Initiation, Requirements and strategy, Implementation, and Operationalization.

❖ BS PAS77:2006 IT Service Continuity Management - Code of Practice

This code of practice (produced by the British Standard Institute) provides guidance on ITSCM. It was intended to complete, rather than replacing or superseding, other publications such as PAS 56:2003 [8], ISO/IEC 20000-1:2011 [9, 10], ISO/IEC 17799:2005 [11] and ISO 9001:2008 [12]. However some of these standards have also been reviewed in the meantime.

PAS77:2006 should not be regarded as a step-by-step guide for implementing IT Service Continuity Management but as guidance on the aspects of ITSCM which organizations should consider adapting to their own particular context. PAS77:2006 [6] explains the principles and techniques for IT Service Continuity management. It is intended for use by persons responsible for implementing, delivering and managing IT Service Continuity within an organization.

The document highlights the relationship between business and IT strategies, between business continuity and IT service continuity strategies, and between the latter and both the IT architecture to put in place and the IT service continuity plans to build. The processes and infrastructure put in place by IT to give the best response in case of incident or disruption should be defined based on sound analysis of the technical (infrastructure) and business context. This should be done through an iterative cycle during which business and IT align their strategies for IT to design their continuity plans.

❖ ISO/IEC 24762:2008– Guidelines for information and communications technology disaster recovery services

This ISO/IEC JTC1/SC27 standard provides guidelines on the provision of ICT Disaster Recovery (ICT DR) services (either in-house or outsourced) as part of business continuity management. It specifies the requirements for managing ICT DR services and facilities.

It offers guidance on ICT DR within the context of business continuity management. It supports the operation of an Information Security Management System (ISMS) by addressing the information security and availability aspects of business continuity management in times of crisis. A business continuity plan comprises an organization's strategies to prepare for future national, regional or local crises that could jeopardize its capacity to continue with its core mission, as well as its long term

stability. Business continuity management is an integral part of holistic risk management that involves:

- Identifying potential threats that may cause adverse impacts on an organization's business operations, and associated risks;
- Providing a framework for building resilience for business operations;
- Providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures.

Using the standard, organizations can build greater resilience into their ICT infrastructure supporting critical business activities and complementing their business continuity management and information security management activities.

❖ **ISO/IEC 27031:2008 – Guidelines for ICT readiness for business continuity**

Effective BCM is mostly dependent upon effective ICT readiness to ensure that the organization's objectives can continue to be met in times of disruptions. This is particularly important as the consequences of disruptions to ICT often have the added complication of being invisible and/or difficult to detect.

In order for an organization to achieve ICT Readiness for Business Continuity, it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services. This can be best achieved by applying the PDCA cyclical steps as part of a management system in ICT Readiness for Business Continuity (IRBC). In this way IRBC supports BCM by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization.

The ISO/IEC 27031:2008 standard [3] describes the concepts and principles of ICT Readiness for Business Continuity, and provides a framework of methods and processes for any organization – private, governmental, and non-governmental – irrespective of size, to identify and specify all aspects (such as performance criteria, design, and implementation) for improving its ICT readiness to ensure business continuity. It also enables an organization to measure performance parameters that correlate to its ICT readiness for business continuity in a consistent and recognized manner.

The scope of this standard encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

This standard applies to any organization developing its ICT readiness for business continuity program, and requiring its ICT services/infrastructures to be ready to support business operations in case of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business activities.

3) Conclusion

Continuity management is addressed at different levels in several standards and best practice guides. This activity is now mature enough enabling ISO to publish internationally agreed documents reflecting the state-of-the-art at business level with ISO/PAS 22399:2007 [4] or more technically for IT specifically with the ISO/IEC 27031:2011 [3].

Standardization works in this domain are following the current trends towards the adoption of Management Systems to support the implementation of specific requirements or processes. The two standards just mentioned are making clear reference to such management systems and a specific standard due to publication in 2012 (ISO 22313) will be dedicated to support organization in building their BCMS, whereas another one still at draft stage (ISO 22323) will define requirements and give guidance for the implementation of organizational resilience management systems.

Beside the works done under ISO/IEC JTC1/SC27 (IT Security techniques), it is worth noting that most standardization activities around continuity management are hosted by ISO TC223 (Societal Security), recognizing the societal impact of business continuity concerns.

V. National initiatives IT Service Continuity

1) *The national context in Luxembourg*

In 2002, the *Commission de Surveillance du Secteur Financier* (CSSF), the Luxembourg regulator for the financial sector, conducted a survey on BCP [13] following the numerous questions raised in this field since September 2001. This survey involved all the credit institutions and other professionals of the financial sector under the supervision of CSSF.

The conclusions of this survey were the following:

- Large and medium-sized institutions, either in the financial sector or connected to it, generally defined a BCP covering all the activities, supported by an important redundancy of IT systems and specific premises to be used in case of disaster.
- Small-sized institutions, tended to mix up BCP and backup, i.e. they plan to pursue their activities mainly thanks to an IT backup centre. This conception is in fact equivalent to the notion of Disaster Recovery Plan (DRP) encompassing the means of implementation of a BCP. This kind of approach may be incomplete if the BCP does not take account of the whole resources necessary for their activities, i.e. the personnel, the business premises... According to that study, a high number of medium and small-sized institutions did not have a BCP, but had initiated such a project at that time.
- Finally, the study shows that medium and small-sized institutions engage providers of IT backup infrastructures. There are only a few providers of shared backup centres, and as a result they induce a high risk of affecting several financial institutions in case of disaster despite the fact that they allow to set up backup solutions at lower costs. This risk also depends on the different categories of contracts and their geographical distribution in relation to the place of the disaster.

According to the results of this survey [14] (published in 2004), almost 66% of banks in Luxembourg had a BCP in place, showing a clear raise in awareness regarding continuity in Luxembourg.

The CSSF reports, though somewhat outdated, are the only available publication giving objective figures for describing the Luxembourgish situation.

Since 2002 no such survey on BCP has been conducted in Luxembourg, and very few information has been published on this very sensitive topic. However, Luxembourg is clearly on the rise in terms of technology infrastructure and continuity service offer thanks to the recent presence of some leading technology organizations. Moreover, the country has now excellent high-speed connectivity both internally and throughout Europe. Thus, Luxembourg now has ample availability of state-of-the art data centers offering a variety of services from rack space to fully-managed facilities and business continuity centers. This is an evidence that the situation in 2002, described in the report [13], has probably changed significantly towards a higher level of maturity of organizations to protect their assets.

Despite the lack of up-to-date information on the different BCM initiatives launched by organizations in Luxembourg (from both financial and ICT sectors), the increasing number of high quality facilities that are well built and well run demonstrates that Luxembourg should be considered as one of the major players in the European market.

2) The regulated framework

Figure 4: Commission de Surveillance du Secteur Financier

All institutions under the supervision of CSSF (i.e. all the credit institutions and other professionals of the financial sector) must comply with the requirements stated in the circulars published by the supervision authority. In April 2005, CSSF published the CSSF 05/178 circular [15], which supersedes the initial requirements from the CSSF IML 96/126 circular [16] related to the IT function for banks as well as PSF (professionals of the financial sector). The circular states that "financial professional shall be in a position to ensure normal operations in case of an IT-system outage and shall put in place a backup solution in line with a business continuity plan. The business continuity plan aims at describing the actions to put in place in order to continue the activities in case of an incident or disaster linked to unusual events".

On July 13, 2007 a Grand Ducal regulation related to MiFID (Markets in Financial Instruments Directive 2004/39/EC) on organizational requirements and behaviors in financial sector was published [17], enforcing the importance of managing the continuity of operations in Luxembourg. This regulation goes beyond the continuity of IT services and covers the whole business continuity.

Due to the regulatory framework of the Luxembourg financial sector, not only the credit institutions but also all the other professionals of the financial sector (including IT service providers) have the obligation to design, implement, review and upgrade relevant mechanisms covering the whole business continuity in order to guarantee the recovering from natural or man-made disasters with business-critical impact. Thus, all supervised IT service providers (called "PSF de Support") are expected to meet these Business Continuity requirements, and now benefit from the global improvement of the business continuity practices in Luxembourg.

Moreover, organizations that use the services of these supervised IT service providers do also indirectly benefit from this raise in maturity of their providers, which makes Luxembourg more mature at Business Continuity level.

References

[1] British Standards Institution, BS 25999-1 – Business Continuity Management, 2006

[2] Office of Government Commerce, ITIL® – The IT Infrastructure Library v3, 2007

[3] ISO (International Organization for Standardization). ISO/IEC 27031 – Guidelines for ICT readiness for business continuity, 2011

[4] ISO (International Organization for Standardization). ISO/PAS 22399 – Guideline for incident preparedness and operational continuity management, 2007

[5] BCI (Business Continuity Institute). Good Practice Guidelines, 2010

[6] British Standards Institution, PAS 77 – IT Service Continuity Management – Code of Practice, 2006

[7] British Standards Institution, BS 25999-2 – Business Continuity Management, 2007

[8] British Standards Institution, PAS 56 – Guide to business continuity management, 2003

[9] ISO (International Organization for Standardization). ISO/IEC 20000-1 – Service management system requirements, 2011

[10] ISO (International Organization for Standardization). ISO/IEC 27031 – Guidelines for ICT readiness for business continuity, 2011

[11] ISO (International Organization for Standardization). ISO/IEC 17799 – Information technology – Security techniques – Code of practice for information security management, 2005

[12] ISO (International Organization for Standardization). ISO 9001 – Quality management systems – Requirements, 2008

[13] CSSF - Rapport d'activités 2002 – Chapitre 6: Supervision of Information Systems http://www.cssf.lu/publications/rapports-annuels/news-cat/24/

[14] "Résultats du recensement des BCP et considérations prudentielles" – CSSF, 2004 http://www.cssf.lu/uploads/media/BrochureCSSF_BCP.pdf

[15] CSSF 05/178 circular, 2005 http://www.cssf.lu/uploads/media/cssf05_178eng.pdf

[16] CSSF IML 96/126 circular, 1996 http://www.cssf.lu/uploads/media/iml96_126_modifiee041005_01.pdf

[17] Regulation on organisational requirements and behaviours in financial sector, 2007 http://www.cssf.lu/uploads/media/rgd_exigences_regles_conduite_130707.pdf

[18] ISO (International Organization for Standardization). ISO 15489-1:2001: Information and Documentation - Records Management: Part 1: General, 2001.

[19] National Institute of Standards and Technology, NIST 800-34 – Contingency Planning Guide for Information Technology Systems, 2002

[20] ISO (International Organization for Standardization). ISO/IEC 24762 – Guidelines for information and communications technology disaster recovery services, 2008

[21] ANSI (American National Standards Institute). ASIS SPC.1-2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use

[22] ENISA (European Network and Information Security Agency). Business and IT Continuity: Overview and Implementation Principles, 2008

3 Digital trust through information security

Information security can be a catalyst for trust, but only if the security measures are effective, efficient and proportionate to the potential dangers they initially aim to prevent.

Trust is difficult to apprehend. As a non-material precondition for social as well as for business interactions, it can rapidly be won or lost, collectively or individually. Trust is the only business-enabling asset that is primarily granted for free. It can thus be considered a pre-investment from every business partner and consumer looking for a product or a service.

However, once there is no more trust, it is very hard to get it back again. Losing confidence is a quickly happening process, whereas regaining takes a lot of time and commitment. An unsatisfied customer will talk about his bad experience to up to thirty people, whilst a satisfied customer will share his sympathy with only about 3 peers. The use of new media, especially blogs and social networks, contributes of course to an exponential growth of this phenomenon.

Losing their trust is more catastrophic than just losing the customers themselves, because every unsatisfied customer is going to let others know the reason for his frustration. In case he vents his anger on social networks like Facebook or Twitter, the company's damage can be disastrous due to testimonials rapidly running out of control.

This chapter is composed of two different sections. The first one explains how information security can contribute to digital trust. The second one deals with the strategy of the Ministry of the Economy and Foreign trade in the area of information security. A particular focus is done on the different structures that have been put in place at the national level.

A) How information security can contribute to digital trust

Information security, meaning the guarantee of an appropriate level of confidentiality, integrity and availability, can foster trust.

A customer has a clear expectation of the level of confidentiality that should be ensured for his service or good; it is directly dependent on the criticality of the data he has to provide or is providing voluntarily.

The customer has a clear conception of integrity and availability depending on his quality needs.

Even if the customer may not clearly express his expectations at the moment of the business agreement, in case of an incident, he will measure the impact in accordance to these. After an attack, the customer wants to know how this attack could happen: Was it because the trusted entity neglected its responsibilities, or was the incident inevitable, even with appropriate security measures provided?

Transparency is the key to a trustful relationship between provider and customer. All security measures that have been put in place should therefore be clearly listed, allowing the customer to evaluate whether his expectations can be met or not. If the customer is not an Information and Communication Technology (ICT) expert, the assessment of possible threats is, of course, a challenging exercise, possibly compelling him to re-define his expectations. But beyond all circumstances, this kind of clarification will lead to a much stronger mutual understanding and the establishment of trust.

Considering the precedent conclusions, the major goals of the Luxembourg Government in the sector of information security are to:

- Enable providers to put in place efficient security measures
- Explain why it is important to put them in place
- Strengthen trust between provider and customer by affording an insight to given security measures
- Enable customers to formulate clear security expectations and evaluate if these can be met by the provider

B) Strategy of the Ministry of the Economy and Foreign trade in the area of information security

I. From an activity and competence point of view

The strategy is based on four different kinds of competences, with each one playing an important role in the information security process.

The first competence is **prevention**. An avoided attack is better than a cured one. Therefore, the Ministry invests in structures, projects and initiatives that raise awareness for information security. The more and the better people are briefed on security issues, the lower becomes the possibility of them being successfully attacked. BEE Secure, for example, is an initiative which advises citizens on a safe use of ICT, while CASES aims at a more corporate target audience.

The second competence is **reaction**. Whenever an incident has occurred, there is an urgent need for action. This is why the Ministry's strategy provides emergency aid on two levels: A steadily updated list of advises and guidelines allows victims to solve most problems by themselves, whereas purpose-founded supporting capabilities like CIRCL (Computer Incident Response Center Luxembourg) take care of incidents that cannot be handled by non-pro individuals.

The third competence is **repression**. This means that after an incident, the ministry and national authorities are willing to do everything in their power to find out who committed the crime and to bring the attacker to justice. Here, the police is in charge of forensic research and prosecution.

The strategy's fourth competence is the **adaptation of legislation and research**. The world of Informatics and Cybercrime is developing at an enormous speed. This dynamic process requires adequate and at all times up-to-date research facilities to keep pace with the ever changing methods of attackers. It also requires adapted legislation in order to anticipate possible attacks. An adapted legislation also allows the creation of new online business opportunities. Thus, niche commerce can be created in this fast moving cyber world and help boost the country's economy.

II. The target group

Citizens, meaning adults, children, teachers and educators are the first target group of the Ministry's initiatives. They must be made aware of the potential risks of the information society and be able to act as responsible citizens. Protecting their assets, be it their devices, identities or critical data, is a major goal. Citizens should be able to take full advantage of the digital society without getting caught in the traps. They should be able to estimate the level of trust they can have in goods or services of the different providers and thereupon choose what best meets their expectations.

SME (small and medium-sized enterprises) are also targeted by the governmental initiatives. Security measures, be they organizational, behavioral or technical, should be affordable and available for small entities such as SME, **administrations**, **communes** or **schools**.

Large companies are the third target of governmental initiatives. They should adopt efficient and effective measures and implement an adequate level of security. Here, what is mostly needed, is a partner for the critical and reliable evaluation of threats and vulnerabilities. Large companies need an incident response team, on which they can rely in case of an emergency. They should also be able to rely on the police for the tracking and prosecution of criminals who attacked them.

Operators of critical infrastructures are the fourth group targeted. Due to their importance for Luxembourg, operators of critical infrastructures should be guided and assisted in their attempt to maximize security in order to comply with expectations mostly in the area of resilience. If needed, legislation will force the operators to adapt their security measures to an adequate level.

Central government is the fifth target of the security initiatives of the Luxembourg government because of the mere fact that information security is one of the catalysts of Luxembourg's sovereignty.

III. Structures of the Ministry of the Economy and Foreign trade

The Ministry of the Economy and Foreign trade has defined its strategy in 2004 and got it approved by the governing council the same year.

In 2007, the Ministry of the Economy and Foreign trade has teamed up with the Ministry of Family and Integration as well as with the Ministry of Education and has created a cross-ministerial platform for information security. This platform allowed the awareness raising project LuSI (Luxembourg Safer Internet) to be repatriated into governmental services, which has led to a reorganization of the information-security-related structures driven by the ministries. Thus, the initiative CASES (Cyberworld Awareness and Security Enhancement Structure), which started in 2001 and focused on awareness raising and prevention of all stakeholders, has refocused on SME, governmental agencies and companies, leaving up the awareness raising of citizens to the newly created BEE-SECURE structure. CIRCL, the Computer Emergency Response Team of the Ministry created in 2008 was not affected by this restructuring.

In 2010, the three ministries, together with the municipal union SIGI and the commune lobby SYVICOL, created a group of economic interest called Smile GIE (Security Made In LËtzeburg Groupement d'Intérêt Economique), in order to hire highly specialized experts for the three brands BEE-SECURE, CASES and CIRCL. By the end of 2011, twelve experts had been hired.

1) BEE-SECURE

Before BEE-SECURE came into existence, the Luxembourg Safer Internet project "LuSI" followed CASES as a pioneer in national awareness-raising for the vulnerabilities of the Cyber world. Co-funded from 2006 till 2010 by the Safer Internet Program of the European Commission, LuSI launched many instructive activities for children, youth and their environment including parents and teachers. The LuSI project was operated by a consortium consisting of Telindus S.A., the "Centre de Recherche Public Henri Tudor" and the "KannerJugendTelefon". In the frame of this project, a helpline was launched in 2007 and a stopline, allowing the anonymous denouncement of illegal web-content, got established in 2010.

An agreement, signed in 2009 between the Ministry of the Economy and Foreign Trade, the Ministry of Education and Vocational Training and the Ministry of Family and Integration, charged the "Service National de la Jeunesse (SNJ)" of coordinating the Safer Internet activities targeting children, youth and their environment. Following a smooth transition from the LuSI project, the SNJ fully coordinates the above-mentioned target groups since November 2010. Since then also, SNJ's activities are co-funded under the Safer Internet Plus program of the European Commission.

SNJ and Smile GIE, which was founded in 2010, decided to regroup all common awareness-raising activities under the new brand name BEE-SECURE. Whether a citizen is approached at school, at home or in public areas, he will get the same key messages, only the language or the wording is getting adapted to the context. With the introduction of BEE-SECURE, the Ministry of the Economy and Foreign Trade can now better focus CASES on the needs of the corporate world, especially the small and medium-sized enterprises.

The core of the BEE-SECURE initiative is powered by a symbiosis of staff members from SNJ and from Smile GIE. Smile GIE has strong ties to the information technology area, while the SNJ has a

large background on the social aspects of the topic. BEE-SECURE also benefits from the networking efforts promoted by the European Commission. It is member of both the InSafe and the INHOPE networks. Within both international networks, current incidents are shared and upcoming trends are getting discussed. Partners from associations, public bodies as well as from the private industry are represented in the BEE-SECURE advisory board. These meetings help a lot to improve efficiency of future campaigns.

BEE-SECURE Youth-Panel is a group of pupils who meet regularly to learn about the new media, but also to give back the view of youngsters on information safety related issues and on emerging trends.

There is also a long, continuously growing list of partners that support BEE-SECURE or that rely on services offered by BEE-SECURE. These are, for example, other public administrations and services like the "Commission Nationale pour la Protection des Données", law enforcement structures, educational and scientific research centers and many more.

The mission of BEE-Secure is to raise awareness among citizens, to promote adequate behavior, organizational skills and technical knowhow that one needs in order to take full advantage of the opportunities the Internet offers.

As tool, BEE-Secure manages a web page (www.bee-secure.lu) which gives advice on important security topics like social networks, cyber mobbing, computer games and online safety. It also offers an access to teaching material and educational video clips. More important than the Internet presence, which can only create a virtual contact between BEE-SECURE and the target audience, are the awareness-raising campaigns as well as teaching activities. The latter happen directly in school, allowing an immediate approach to the young people. In fact, Luxembourg is one of a few countries that are able to reach all schoolchildren of one grade with their awareness-raising program. Every year, all the pupils of the first grade in secondary school have to obligatory take part in such a Cyber security workshop held by highly motivated experts.

Whilst the courses are mandatory for high school students, primary schools can have them organized on a voluntary basis. Until the end of 2011, more than 20% of them have participated.

BEE-SECURE is also very well known for its large scale campaigns. Every year such a campaign is launched, reaching an average of more than 10% of all Luxembourgers directly (on fairs and events), and more than 20% indirectly via the media. The thematic campaigns have a large impact and a long-lasting effect because of their clear message. They aim to educate people in a positive way, create a culture of security and establish a broader view on information security.

The very first campaign was launched in 2009. It was called "naked in the net", and aimed to promote a safe usage of social media. The image on the poster depicted a net full of oranges, one of which was peeled – a symbol for the vulnerability of showing too much skin on the Internet. It reminded people that data privacy is not only an important topic but that it is absolutely desirable and that the non-respect of it can be harmful.

A year later, in 2010, the campaign focused on a safe usage of passwords. It became known under the name of "toothbrush campaign". In fact, a toothbrush and a password have a lot in common: you should use them, change them regularly and not share them with others. Keeping this idea in mind, real toothbrushes were distributed, together with a leaflet on how to choose a password that is hard to decrypt but easy to remember. The campaign became a great success and was voted best practice by the European Network and Information Security Agency (ENISA). It continued being promoted in 2011 under the new BEE-SECURE brand. In Slovenia, the same concept was taken over and implemented on a local level in 2011.

In September 2011, the third – and most recent – campaign was launched. It is called "Safer Internet / Safer Sex". In association with the Ministry of Health, the service "Aidsberodung" of the Luxembourg Red Cross and the association "Planning Familial", BEE-SECURE could engage a successful partnership to raise awareness in both ICT and sexually transmitted diseases protection. Condoms with flyers on both topics are distributed at all major events where BEE-SECURE is present to reach its target audiences.

Luxembourg is not only in the heart of Europe, but also in the heart of the Cyber world. ICT and the Internet are playing an extremely important role in the business and private lives of the inhabitants. Statistics prove this: Luxembourg is first in Europe regarding cross-border online shopping[22], on second place regarding the proportion of people using ICT security software[23], first when it comes to uploading self-created contents[24], third in the Internet use by individuals and frequency of use[25] and number one when it comes to older generations using the web[26]. Luxembourg also ranks first for the proportion of population accessing the Internet through a mobile phone via UMTS according to the Digital Agenda Scoreboard[27] .

With more than 90% of the population using the Internet regularly, and huge investments from the government and private sector in projects like e-commerce, e-health, e-education or e-government, the work of BEE-SECURE becomes even more important. ICT-technologies shape the future. If these technologies are struck by vulnerabilities and criminal attacks, it means loss of trust in a sector that is basically indispensable for all.

If one considers the 2007 Estonian case, where a series of cyber-attacks paralyzed political, governmental and individual sites, the Luxembourg situation – with a power and bandwidth beyond Estonian compare – is that of a sleeping volcano. In fact, Luxembourgers are disposing of such a huge bandwidth that a botnet (a collection of compromised computers connected to the internet), remotely controlling these computers, could unleash such an immense power that the Estonian attacks, in comparison, would look pale and risible. It takes only 400 Luxembourg inhabitants, or rather their computers, to provide an incredibly dangerous attacking power of 20 GB/s. So, while on the one hand, e-inclusion has a positive connotation because it leaves no one behind in enjoying the benefits of ICT, on the other hand, it has the bitter aftertaste of a growing security lack. A nationally secured ICT lies in the hands of the country's individual users. Data must be protected and power must be controlled. This can only happen if users adopt a safe and adequate behavior from the youngest age on, and if one can rely on all necessary organizational skills and technical security measures.

In case an incident happens and secret data is revealed, citizens will react according to in how far they are directly concerned. The more they see their own critical data endangered, the higher their loss of trust towards the attacked entity will be manifest. Taking into account the huge amount of confidential data stored in social networks – data which is handled like merchandise by business-oriented operators – as well as the outdated technology and trivially simple passwords used by the operators to access this data, it becomes clear that disastrous incidents are just a few clicks away.

But even more catastrophic than the hacking of Facebook or Twitter or similar networks would be a breach of online services like e-banking, e-government or e-health. Here, the past experiences have shown that a large number of private companies do not accomplish their risk assessment in an

[22] *http://ec.europa.eu/information_society/digital-agenda/scoreboard/index_en.htm*
[23] *http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisci_f&lang=en*
[24] *http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2009/sec_2009_1103.pdf*
[25] *http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF*
[26] *http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=1.&pcode=tin00092&language=en*
[27] *http://ec.europa.eu/information_society/digital-agenda/scoreboard/index_en.htm*

honest way. This is due to the fact that they want to avoid all sorts of extra-costs an eventual updating of security measures would implicate. There are some examples in the world, where the banking sector considered it easier and cheaper to fake its risk analysis results and in case of an incident secretly refund a robbed online banking customer, than invest larger sums in refurbishment. What banks (in this case) often seem to forget is that they are not only gambling with money, but with reputation. And that is not just their own brand name, but the service of e-banking as a whole. If trust in modern Internet services is lost, a decrease in the use of the new media will be the result. But a regression of our modern society's development is not at all desirable.

2) CASES

In order to withstand the security challenges, companies – local as well as central governmental entities – have to secure their critical assets such as information or business processes. The companies have to meet the expectations of their customers and provide the required level of security in confidentiality, availability and integrity. This is a very challenging task due to the fact that the technological, social and political environments are rapidly evolving. Radical changes can, for example, be documented when it comes to online threats. Until 2001, deliberate ICT attacks happened mostly for fun or out of an adventurous motivation. Today, these attacks are highly motivated, either by monetary gain, political views or cyber warfare.

But the landscape of vulnerabilities has changed as well. Due to the convergence of technologies, with a whole bunch of different devices connectable to the Internet, and the omnipresence of the Internet or ICT as such, weak points spring up like mushrooms. The complexity of the operated systems and insufficiently educated operators add to this alarming evolution.

A risk means the probability of a threat exploiting an asset's vulnerability and thereby causing an impact. Considering this definition, it becomes clear that the most influential factor in risk increase is the multiplication of threats or vulnerabilities. This happens for example when different kinds of technological devices are linked to each other, on IP based networks, and connected to the Internet. Today, people want to be reachable at all times and able to keep in touch with the rest of the world. This interconnectivity however implicates a growing menace of cyber-attacks, simply due to the incredible mass of potential offenders and victims.

This interconnection of networks, which initially led to the development of the Internet, has a big potential and is able to not only simplify but also speed up business processes. Yet, at the same time, it makes these processes more vulnerable to accidental or deliberate attacks. This is true for information transmission processes as well as for systems used for industrial supervision and control, the SCADA (*Supervisory Control And Data Acquisition*) systems.

Nowadays, companies and especially industries can become victims of deliberate cyber-attacks due to several reasons.

First of all, companies invest a lot in research and development in order to file patents and be able to produce and offer innovative goods and services. This intellectual property represents a valuable, yet easy to steal asset and can quickly become a target for cyber-attacks.

The second reason why industry is likely to become a victim of cyber-attacks is the fact that it often has large ICT departments that are considered valuable assets for cybercriminals. If these assets are compromised, they offer a lot of calculation power and eventually a huge bandwidth needed for the different tasks in a cybercrime plot.

The third factor is the important role that many industries play as operators of critical infrastructures. Especially the SCADA systems used to control industry plants, sewage, power or other critical assets are potential targets of cybercriminals that might blackmail or harm a company or even an entire country.

For many companies, it also happens accidentally that they become targets of cybercrime. Very often, cybercriminals scan the Internet in order to find a vulnerable system and try to compromise the system in order to be able to accomplish their primary goal.

The probability that a company might get attacked has dramatically risen. Especially the increase of deliberate threats in comparison to accidental or environmental threats has grown. Statistically, it is much more probable to become a victim of a cyber-attack, than it was the case a couple of years ago.

But not only the probability has risen; the potential impact has dramatically grown, as well. ICT systems are nowadays irreplaceable assets in more and more business processes. A loss of confidentiality, integrity or availability can have tremendous consequences. Unfortunately, many companies do not analyze which business process is dependent on which asset and actually have no clue what efforts in time, money and expertise they should invest in order to protect a given asset. Security has become a cost factor, not a necessary asset.

In the same way, when under attack, many companies do not know which business processes risk being affected by the endangerment of a certain asset. For these companies, it will be very difficult to work out an incident response plan in order to most effectively mitigate potential impacts.

Companies have to be aware of the potential risks they run. Somehow, they should be able to estimate the threat exposure level, as well as the vulnerabilities and the easiness of exploiting these vulnerabilities. But most of all, companies should be able to estimate and evaluate the most probable risk scenarios. According to these, companies should organize themselves in order to be able to face the threats, reduce the vulnerabilities and mitigate the impacts as much as possible, reducing risks to an acceptable level.

This cognitive process is called risk management. It requires full management commitment and the analysis of interdependencies between business processes and assets. It also requires an estimation and evaluation of risks. Risk management also includes the elaboration of risk treatment plans and thus the mitigation of risks.

Unfortunately, the skills to protect ICT systems have not spread as quickly as the deployment and the interconnection of technology. Security has in some way become discriminatory, mostly because of the required skills, but also due to the complexity of the available standards. Nowadays, technology is complex and extremely interconnected within components and the Internet. Companies are often afflicted with such a pressure of time ruling the market, that they deploy technically immature products, thus creating insecurity by design.

But not only technological aspects lead to security concerns. The web 2.0 revolution has also changed our way of communicating. The time of basically individual one-to-one communication has passed and been replaced by techniques that allow communication from one to many. Nowadays, it is easy to instantly reach several thousand peers via one single communication channel. Companies are forced to open their networks to these technologies, creating tremendous opportunities for business but also for attackers. Data leakage on social networks is becoming a real threat. The human factor is important in security. Exploiting human vulnerabilities is often easier than exploiting technical flaws. Many social networks give their users incentives to publish as much information as possible. The average user is not aware of the fact that private data has become the new currency on the Internet.

And this is the exact reason why privacy settings are often difficult to configure and why regulations change constantly: Social networks provoke their customers' leaking of private and corporate data.

The content of social media applications can easily be turned against the user, as it reveals many of his human vulnerabilities. A lot of people create their passwords from information published on social media, like names of family members or pets, birthdates or phone numbers. But the information found on social networks can also be used in order to perform attacks of social engineering. The only thing an attacker has to do is to find out about the interests of his victim, then build an interest-based container and send the infected container to the victim. This is how the attacker exploits the human vulnerabilities that got delivered to him like in a goldfish bowl.

The usage of social media as such is not a bad thing, but the user should always be aware of the legislation applicable to the company that stores the data and should be aware of the people he has invited to share his privacy. People generally tend to accept too many followers or buddies and tend not to distinguish between the different groups of peers (is this a real friend, a colleague, someone they just hastily met, or a person they do not know at all). A large number of users doesn't even configure their social media platform correctly and neglects the possibilities for more privacy.

This is also more and more true for supportive tools like smartphones or tablet PCs. Many operating systems offer the possibility of cloud storage in order to synchronize or backup valuable user information more easily, may this be private or corporate information. In some cases, the information stored in the cloud can be used in order to profile private but also corporate users. It can even allow hackers to do industrial espionage. Only a few know that homeland security bills like giving governments access to the data in clouds established by companies falling under their legislation. The most intrusive one is the US patriot act, giving the US governmental services an insight to every information stored within a company that belongs to an US entity, wherever the data might be stored.

The mission of CASES is to provide companies, local and central governments with the necessary organizational skills, behavioral rules, technological competences and above all with appropriate methodologies in order to meet the challenges of a global information society.

Employees of companies need to be educated on the secure usage of modern information and communication technologies. Leakage happens so quickly because of the convergence of technologies on IP based networks and because of the omnipresence of social media. Security reflexes have to be trained and confidential corporate information is not to be shared on social networks.

Due to the policy of social network operators, many people have not developed a culture of security, but rather a culture of sharing. A growing number of citizens are suffering from this behavior and paying the price for it: they have lost their privacy, are getting bullied or stalked, to just name a few of the well-known problems.

The teaching of these reflexes has to be embedded in every company's operation strategy. The correct handling of confidential information, the application of security standards and the separation between information sinks and safe devices has to be understood and enforced. Security must be comprehended; otherwise the security measures will be infringed or circumvented.

But in order to become aware of security needs and to be able to implement effective and efficient security measures, companies have to perform risk assessments. This means they have to estimate and evaluate risks and thereupon plan the installation of adequate instruments.

CASES promotes the recurrent use of risk assessments and the implementation of information security policies. To achieve this, methodologies and standards are at hand, but they are far too complex for small entities to adopt. For this reason, over the last years, CASES has invested, together with his long term partner the CRP Henri Tudor, a lot of efforts in the creation of appropriate methodologies for small and medium enterprises.

Risk assessments are most important in order to become aware of threats that could exploit vulnerabilities of assets and cause impacts. Risk assessments have to be done recurrently, they have to embrace the right scope and give information on the exposure to threats, the existence of vulnerabilities and potential impacts. Risk assessments are very time-consuming and might even be dull regarding the massive number of assets that have to be analyzed.

Smile GIE, the Interest Economic Grouping "Security Made In Lëtzebuerg" is developing a new platform that provides the tools needed in order to use the CASES risk assessment methodologies. The huge advantage of this platform is the reusability of existing content describing business processes, information or secondary assets used in small and medium entities. CIRCL, the Computer Incident Response Centre Luxembourg, is on a regular basis providing the metrics needed for the estimation of threats and vulnerabilities. This enables all stakeholders to perform recurrent (weekly) risk assessments and thus adopt the correct preventive measures.

On this platform a tool will also be available to create, manage and deploy information security policies. This tool is based on templates that have been created around the ISO/IEC 27001 standard as well as policies, procedures and standards implemented according to the ISO/IEC 27002 controls.

This platform will bring together the company, its trusted consultant and the Smile GIE services in order to provide a real-time risk assessment and policy management tool.

By adopting these methodologies, entities can manage their security efficiently and effectively. They can quickly adapt to new threats and they can benefit from the competence and skills of the community using the Smile GIE platform. Sharing knowledge on security becomes a major goal.

This approach fosters trust between the companies, the security providers and Smile GIE experts. But the implementation of adequate security measures can improve the customers' trust, too. If entities know exactly what to do and how to do it in order to increase their level of security, they radiate a self-assurance that is able to convince customers. Businesses are able to work much more efficiently while customers feel assured and their data secure.

Besides the implementation of preventive and protective measures, implemented in accordance to the decisions taken during the risk assessment and the deployment of security policies, the companies have to educate their personnel. This includes the imposition of behavioral, organizational and technical rules.

In order to simplify this huge burden, Smile GIE is creating an e-learning platform that can provide respectively organize four educational modes. This platform enables the organization of frontal teaching, with the help of Smile GIE experts or experts from specialized companies. The tool also provides the possibility to run through self-learning applications or tutored learning. Last but not least it will be possible to organize webinars (web-seminars) via this platform. One type of webinars that are foreseen is the webinars organized by CIRCL in order to discuss emerging threats, vulnerabilities or preventive and protective measures.

3) CIRCL

Incident response means reacting to a security-relevant occurrence. In the worst case, this occurrence might cause a large scale impact due to the loss of confidentiality, integrity or availability of a critical asset or information. However, in many cases, these direct impacts are promptly followed by a major loss of one of the most important business assets: the customers' trust.

At the best, a security relevant incident is discovered before it can deploy its damaging effects. This is possible by activating a security indicator, able to initiate necessary preventive or corrective measures and prevent the incident from becoming a full scale catastrophe, deploying its whole destructive potential.

Managing security relevant incidents is a hard job and only possible if the human mind understands how threats function and what exploitable vulnerabilities exist. Some sort of generic approach certainly facilitates the comprehension but however, a certain level of technological knowhow is always necessary.

Incident response often means the application of corrective and preventive measures in a condition of time pressure and mental stress. This is why it is highly recommended to train these capabilities and be prepared for some potential scenarios, in best case the risk scenarios that have been identified as the most probable by the risk assessment. These scenarios should be regularly practiced. The early warning security indicators should also be put in place and of course be supervised on a regular basis, as often as the situation requires it.

If security indicators have not been deployed or did not trigger an alert, incidents are often only discovered after an impact becomes visible. This is for example the case with loss of confidentiality. An attack, crafted in order to retrieve confidential information from a company, will not necessarily be immediately visible. It is therefore of outmost importance to check logs on a regular basis and check if incidents are visible in the logs even if they did not trigger any impact on security.

This analyses phase is also part of the skills needed during incident response. Forensic skills are necessary in order to be able to identify a threat, understand the way it has been able to circumvent the preventive and protective measures and of course check if the threat is still present within the ICT system of the company. This is very difficult as more and more Advanced Persistent Threats (APT) are discovered, either in advanced industrial or governmental espionage.

The last phase in incident response consists in launching procedures foreseen in the business continuity planning, or directly in re-establishing the health of the affected system. This job might be very difficult, especially when facing APT. The re-establishment of the integrity of the affected system often requires a rebuilding from scratch of the affected components, which demands a tremendous effort from the victim company.

One crucial component in incident management is communication. From the outset, it is important to prepare internal management communication as well as employee communication, especially on preventive and corrective measures. But it is also important to foresee communication with the public in case of a major incident. If the incident is not communicated by the company, press will take the initiative and publish information they have, whether it is correct or incorrect, and they will lead the public discussion in a direction that might not be suitable for the company. It is always better to spread the bad news oneself because at least it allows to communicate the whole context of the incident and explain the incident as well as the potential consequences to the customers.

Incident response is a difficult task and requires high skills. Many companies are not able to fully implement incident response capabilities and therefore will eventually need to ask for assistance by the national "Computer Emergency Response Team" (CERT), CIRCL. The success of this mission however largely depends on the capability of the company to quickly deploy corrective and preventive measures. The company should implement some rudimentary incident response capabilities in order to allow a quick intervention of CIRCL.

The threat as well as the vulnerability landscape is evolving on a daily basis. Every year, attacking schemes that are more complex and thus more difficult to detect are discovered. Business models in cybercrime become more profound to apprehend and due to the multiple existing web currencies, money laundering becomes less evident and thus very hard to detect.

Cybercrime is a global problem and in fact, Luxembourg does not only face national or residential, but worldwide existing cybercriminals. Research and Development has become a crucial early warning system, in order to stay informed on evolutions made in the area of cybercrime and security. Cooperation between security players has become a necessity. Speed and the possibility to quickly apprehend new schemes are vital competences for a national CERT.

But the research done by CIRCL does not only enhance the Luxembourg early warning capabilities. The developed tools become more and more a quality indicator of the Luxembourg cyber-economy. Especially the BGP ranking project, informing on the resilience of malicious activities within an autonomous system - an Internet Service Provider (ISP) for instance - inform on the trustworthiness and the quality of these ISP. The work of CIRCL in quickly reacting to take-down requests proves that Luxembourg is some kind of safe harbor for e-commerce activities, as the hosting economy in Luxembourg quickly reacts to take-down requests issued by CIRCL and thus keeps Luxembourg's cyber-landscape healthy. This is by far not a matter of course in other countries.

CIRCL is becoming the national information sharing hub when it comes to security relevance. This can be information on already known as well as new attacking schemes or malicious IP. CIRCL is the trusted address when talking about applied information security, in a protective sense or a curative sense.

This proactive security approach largely reflects the policy of Luxembourg. The aim of this policy is not to spy on service providers or to threaten them, but to offer a partnership and a collaborative approach. It lies in the interest of the entire Luxembourg economy to keep the country's networks safe. This cannot be done by legislation, nor by repression, but by a collaborative approach including education, application of security standards and assistance. The Luxembourg information security approach is built upon these key factors and promotes trust instead of distrust; it is not based upon spying, but coaching and collaboration.

Security indicators, as they are being evaluated by CIRCL, become an important advantage of the Luxembourg e-economy, besides the large bandwidth, the extremely good connectivity and the abundance of highly secure data centers. Companies looking for a safe harbor for their data start to discover Luxembourg and find out that it is the place to be, because of the key business-enabling factors they find here. Luxembourg is neutral, Luxembourg is reactive and listens to the needs of businesses, Luxembourg is competent and Luxembourg is a trusted partner for a company that wants to develop its market in Europe.

4 Digital trust through the knowledge of standardization and certification

A) ICT international standards and their development through standardization

This chapter starts with an introduction to standards and standardization, highlighting the importance of standards, their impact on the economy and the benefits for an organization to participate in standards establishment. The second part of the chapter focuses on Information and Communication Technology (ICT) in the frame of international standardization, by introducing the International Organization for Standardization (ISO) and its standardization Technical Committee (TC) ISO/IEC JTC1 dedicated to "Information Technology". On one hand, the organization of this committee is presented, on the other hand the standardization process is depicted. Finally, the third part presents the standardization strategy for Luxembourg established by ILNAS and how standardization is managed at the national level.

I. Introduction to standards and standardization

1) *Importance and impact of standards*

Today, every professional sector relies on standards to perform its daily tasks in an efficient manner. An obvious example is the standardization of screw shape and size, which is one of the first application domains of standardization. What would happen if each product designer had its own screw dimensions? It is clearly difficult to imagine each user having as many screwdrivers as the number of different products he has. It is only when standards are not in place that we realize their importance.

The same approach also applies in the digital world. For example, to avoid that each CD-ROM drive has its own data format, the ISO 9660:1988 standard entitled "Information processing -- Volume and file structure of CD-ROM for information interchange" specifies the volume and file structure of Compact Disc - Read Only Memory (CD-ROM) for the information interchange between information processing systems.

In ISO/IEC Guide 2 [1], a standard is defined as: "document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context".

Moreover, it is established that "standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits" [1]. Standards are generally based on voluntary application, at the opposite of a regulation, providing

binding legislative rules, that is adopted by an authority. However a standard can become mandatory if it is declared compulsory by law or regulation.

Using standards is seen as a source of benefits in a lot of economic sectors. In general, standards facilitate trades and guarantee some fundamental characteristics such as interoperability, quality, security and risk management. In this frame, a lot of studies have been performed, demonstrating the importance of standards for the economy:

- In France, standards contribute on average to 0.81% of economic growth that is about 25% growth of Gross Domestic Product (GDP) [2]

- In Germany, the information contained in standards and technical rules was responsible for 1% of Germany's Gross National Product (GNP) [3]

- In the United Kingdom, standards contribute each year to:
  - £ 2.5 billion a year to the UK economy
  - 13% of growth in UK labor productivity [4]

- In Canada, the increasing number of standards has contributed to:
  - 17% of the growth rate of labor productivity
  - 9% of the growth in economic output [5]

2) Standardization: the standards development activity

In spite of such recognition of standards, advantages related to the involvement in the development process of a standard, also called standardization process, are still underestimated. The definition of standardization, as defined in ISO/IEC Guide 2 [1], is: "activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context".

This definition is reflected in the following ISO slogan "Do it once, do it right, do it internationally".

Benefits of participating to the standardization process for an organization can be divided into three main categories:

1. Anticipation of the coming rules and best practices

Following a standardization TC allows to be in touch with the evolution (or the creation) of standards related to a specific domain. It helps to better understand and analyze the standards with regard to the organization's objectives. It is generally seen as a "continuous training". To be part of a TC also leads to a better integration of standards in the organization's strategy, leading to, for example, reduction of delays for products/services release and costs.

2. Transfer of innovations

Participating to a standardization TC means to be a stakeholder in new standards establishment. It is a way to internationally spread the best practices related to its skills, but still keeping confidential what comes under intellectual property.

3. Be part of a network having some of the most influential persons of the domain

Standardization TC are composed of international experts. To be part of the standardization process helps to be in touch with these experts, and thus to collaborate with them as potential partners and customers, or to know what is in development by the potential competitors. International standardization is a way to develop the economy of an organization, and to increase its competitiveness at the national, European and international level.

3) The standardization frames

Standards can be established by different organizations at national, European and international level.

At the national level, each country has its own National Standards Body (NSB) allowed to produce national standards (Table 1). The national standards are preceded by letters characteristic of the country having developed the standard (e.g. "LU" for Luxembourgish standards, "DIN" for German standards, "NF" for French standards, "BS" for British standards, etc.). Examples of NSBs are:

Luxembourg ILNAS (*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*)	ILNAS
Germany DIN (*Deutsches Institut für Normung e. V.*)	DIN
Belgium NBN (*Bureau de normalisation*)	standards for .be
France AFNOR Normalisation (*Association Française de Normalisation*)	afnor NORMALISATION
United Kingdom BSI (British Standards Institution)	BSI

Table 1: Examples of NSB

The European standardization bodies recognized by the European Commission are those listed in the Directive 98/34 [6] (Table 2). The standards produced by these organisms are preceded by "EN" for CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization), and by "ETSI TS" for ETSI (European Telecommunications Standards Institute) standards.

CEN - European Committee for Standardization	
CENELEC - European Committee for Electrotechnical Standardization	
ETSI - European Telecommunications Standards Institute	

Table 2: European standardization bodies recognized by the European Commission

Finally, standards with the largest scope are international standards. They are developed by international standardization organizations such as ISO, IEC (International Electrotechnical Commission) or ITU-T (International Telecommunication Union's Telecommunication Standardization Sector) (Table 3). The best-known standards are ISO standards, having a name preceded by the "ISO" letters.

ISO - International Organization for Standardization	
IEC - International Electrotechnical Commission	
ITU-T - International Telecommunication Union's Telecommunication Standardization Sector	

Table 3: Examples of international standardization organizations

II. ICT standardization and the ISO/IEC JTC1 committee

Many organizations are performing ICT standardization. For example, W3C (World Wide Web Consortium) develops standards for Web technology, OASIS (Organization for the Advancement of Structured Information Standards) mainly for e-business and web services, ITU-T for telecommunication, etc.

The preceding organizations are generally based on industrial consortiums promoting their standards as "*de facto* standards", i.e. having achieved a dominant position, but without having necessarily received a formal approval by way of a standardization process.

"Formal standardization" is standards development through national or international Standards Development Organization (SDO). For example, CEN or CENELEC are two of the most important SDOs at the European level. At the international level, it is clearly established that the committee ISO/IEC JTC1 "Information Technology" is the leading SDO for ICT standardization. This statement is reinforced by the "Vienna Agreement" set up in June 1991 between CEN and ISO. Its aim is to avoid parallel or conflicting standards and provide mutual assistance in the work.

1) *Participation to ISO standards development*

ISO is the world's largest developer and publisher of international standards. There are currently more than 18000 standards already published and more than 4000 standards under development. The objective of documents published by ISO is to define clear and unambiguous provisions in order to facilitate international trade and communication.

The Central Secretariat of ISO is located in Geneva, Switzerland, and only coordinates the system. The activity of standards establishment is performed by national experts, coming from the different ISO members. ISO brings together 163 countries (out of the 204 total countries in the world) as ISO members.

Figure 1: Logo of the ISO

The ISO membership falls into the three following categories:

- **Member bodies** (110 countries): A member body of ISO is the national body "most representative of standardization in its country". Only one such body for each country is accepted for membership of ISO. Member bodies are entitled to participate and exercise full voting rights on any TC and policy committee of ISO (one country = one vote).

- **Correspondent members** (47 countries): A correspondent member is usually an organization in a country which does not yet have a fully-developed national standards activity. Correspondent members do not take an active part in the technical and policy

development work, but are entitled to be kept fully informed about the work of interest to them.

- **Subscriber members** (5 countries): Subscriber membership has been established for countries with very small economies. Subscriber members pay reduced membership fees that nevertheless allow them to maintain contact with international standardization.

Luxembourg is currently member body of ISO through ILNAS, the Luxembourg's Standards Body.

ISO is a generic SDO, developing international standards for all industry sectors. ISO is structured by TC, all of them dealing with a specific standardization area, and generally themselves organized in SubCommittees (SC) and/or Working Groups (WG). 224 TC were active at the end of 2011. Different participation levels in the work of TC and SC are allowed. For each TC (resp. SC), a national member can be:

- **Participating member** (P-member): A P-member has an obligation to vote on all questions formally submitted for voting within TC or SC, and to participate in meetings.

- **Observing member** (O-member): An O-member follows the work as an observer and therefore receives committee documents, and has right to submit comments and to attend meetings.

A national body may choose to be neither P-member nor O-member of a given committee, in which case it will have neither the rights nor the obligations indicated above with regard to the work of that committee.

2) The standardization committee "ISO/IEC JTC1 – Information technology"

As said earlier, ISO is a generic SDO, developing international standards for all industry sectors. The IEC is another SDO preparing and publishing international standards for all electrical, electronic and related technologies – collectively known as "electrotechnology". An agreement[28] reached in 1976 defines responsibilities for both of them: the IEC covers the field of electrical and electronic engineering, all other subject areas being attributed to ISO. However, to deal with the consequences of substantial overlap in areas of standardization and work, this agreement allows creating Joint Technical Committees (JTC) between ISO and IEC. ICT is such an overlapping standardization domain, thus ISO and IEC formed a JTC in 1987 known as ISO/IEC JTC1.

Figure 2: Logo of the IEC

[28] *ISO Council resolutions 49/1976 and 50/1976 and IEC Administrative Circular No. 13/1977*

The title of the standardization TC ISO/IEC JTC1 is "Information Technology" and its scope "Standardization in the field of information technology". The mission of ISO/IEC JTC1 is to develop, maintain, promote and facilitate ICT standards required by global markets meeting business and user requirements concerning[29]:

- Design and development of ICT systems and tools
- Performance and quality of ICT products and systems
- Security of ICT systems and information
- Portability of application programs
- Interoperability of ICT products and systems
- Unified tools and environments
- Harmonized ICT vocabulary
- User friendly and ergonomically designed user interfaces

ISO/IEC JTC1 has the following vision for its standardization activity: "JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technologies (ICT) standards for business and consumer applications. Additionally, JTC 1 provides the standards approval environment for integrating diverse and complex ICT technologies. These standards rely upon the core infrastructure technologies developed by JTC 1 centers of expertise complemented by specifications developed in other organizations." Along with this focus on convergence of technologies, ISO/IEC JTC1 put the emphasis on enabling synergy between the standardization areas, especially through a better coordination and cooperation with other SDOs (e.g., ITU-T, IEEE, ECMA, etc.). ISO/IEC JTC1 also focus on increasing speed and flexibility of the standardization process and on continuing to be a leader in ICT standards development [7].

The TC ISO/IEC JTC1 is currently composed of 19 SC. Figure 3 summarizes the structure of ISO/IEC JTC1. ISO/IEC JTC1 is one of the largest TC in ISO, gathering 37 P-members and 54 O-members in 2012. Luxembourg is registered as P-member of ISO/IEC JTC1. This TC is also one of the most active with 2513 published standards and 628 standards and projects in progress at the end of 2012. The secretariat is currently managed by the American National Standards Institute (ANSI) and the chairperson of the TC is Ms. Karen Higginbottom (USA), reelected in 2011 for three years . Finally, the official website of ISO/IEC JTC1 is: http://www.iso.org/iso/fr/jtc1_home.

[29] *http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/jtc1_home/jtc1_mission_principles.htm*

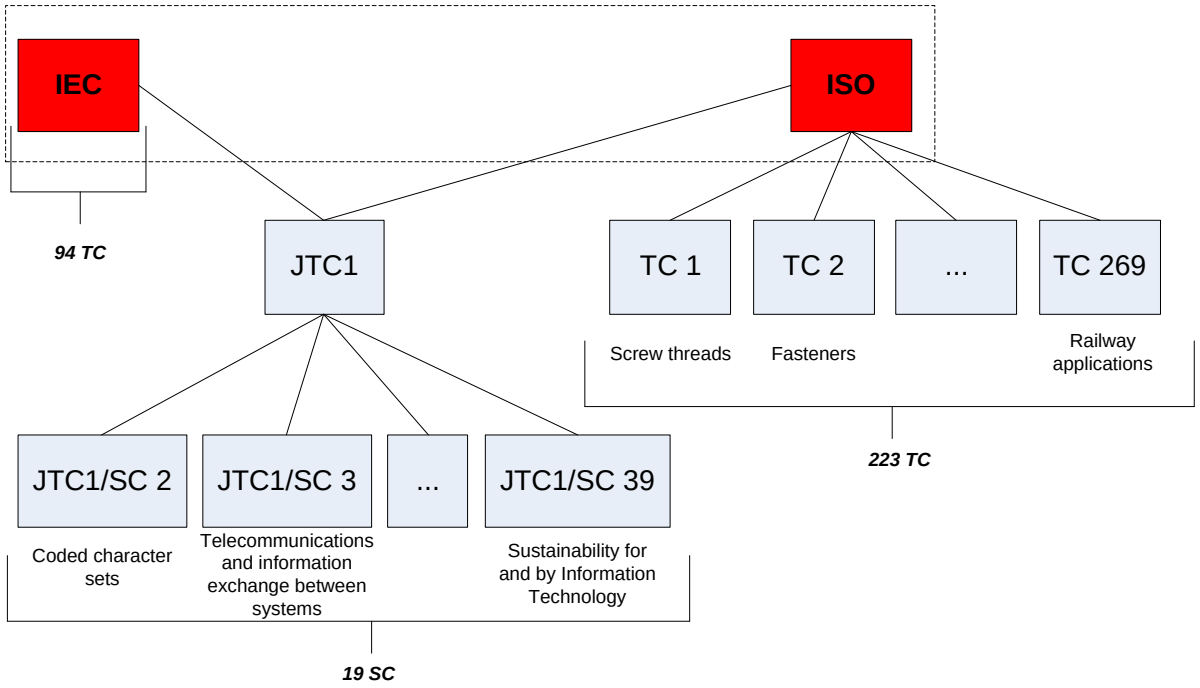

Figure 3: ISO/IEC JTC1 within the ISO structure

The current 19 SC and the 2 WG of ISO/IEC JTC1, dealing all with a different topic of ICT, are listed in Table 4, the last SC opened being SC39. It is important to note that some SC are closed. Most of them are merged in other SC, due to the evolution of ICT standards and ICT in general. However the identification number of a closed SC is never reassigned to another one.

SC/WG	TITLE
JTC 1/WG6	Corporate Governance of IT
JTC 1/WG7	Sensor networks
JTC1/SC2	Coded character sets
JTC1/SC6	Telecommunications and information exchange between systems
JTC1/SC7	Software and systems engineering
JTC1/SC17	Cards and personal identification
JTC1/SC22	Programming languages, their environments and system software interfaces
JTC1/SC23	Digitally Recorded Media for Information Interchange and Storage
JTC1/SC24	Computer graphics, image processing and environmental data representation
JTC1/SC25	Interconnection of information technology equipment
JTC1/SC27	IT Security techniques
JTC1/SC28	Office equipment
JTC1/SC29	Coding of audio, picture, multimedia and hypermedia information
JTC1/SC31	Automatic identification and data capture techniques
JTC1/SC32	Data management and interchange
JTC1/SC34	Document description and processing languages
JTC1/SC35	User interfaces
JTC1/SC36	Information technology for learning, education and training
JTC1/SC37	Biometrics
JTC1/SC38	Distributed application platforms and services (DAPS)
JTC1/SC39	Sustainability for and by Information Technology

Figure 4: SC and WG of ISO/IEC JTC1

Regarding the topics covered by ISO/IEC JTC1, a SWG (Special Working Group) on Planning is continuously investigating for next standardization areas. During the last ISO/IEC JTC1 plenary meeting held in San Diego, USA, in November 2011, the SWG on Planning recommended the following areas as potential new standardization topics for ISO/IEC JTC1:

- Social Networking and Web Collaboration
- Mobile Applications
- Augmented Reality
- Ubiquitous Computing

3) The standardization process

ISO standards development lies on three main principles:

- **Consensus:** The views of all interests are taken into account: manufacturers, vendors and users, consumer groups, testing laboratories, governments, engineering professions and research organizations. Because ISO are voluntary agreements, they need to be based on a strong consensus (which need not imply unanimity) of international expert opinion. It is also interesting to note that ISO processes are in fact based on a double level of consensus:
  - At the level of each national ISO member, the different stakeholders must reach a consensus before supporting a position at the international level.
  - At the international level, the different countries members of the TC must reach a consensus before going on the next stage in the standardization process.

- **Industry wide:** An ISO standard must be applicable at the international level and by any type of organization. This principle lead to the ISO's global relevance policy[30]: "The required characteristic of an international standard is that it can be used and implemented as broadly as possible by affected industries and other stakeholders in markets around the world."

- **Voluntary:** International standardization is market driven and therefore based on voluntary involvement of all interests in the market-place.

The standards development process, or standardization process, is composed of successive and well defined stages, as depicted in Figure 4. Each of these stages is associated to a reference number. The standardization process of ISO is composed of the following stages [8]:

❖ **00 - Preliminary stage**

TC or SC may introduce into their work programs, by a simple majority vote of their P-members, preliminary work items. They are, for example, subjects dealing with emerging technologies, which are not yet sufficiently mature for processing to further stages. They are regularly reviewed by the related committee.

[30] *http://www.iso.org/iso/standards_development/governance_of_technical_work/global_relevance_policy.htm*

❖ **10 - Proposal stage**

The first step in developing an international standard is to confirm that there is a need for the international standard in question. A standard form of new proposal must be completed to provide a (non-technical) statement making clear user requirements satisfied by the project. The New Work Item Proposal (NP) is then submitted to a vote of the members of the TC / SC concerned to decide whether to put the issue to the technical program. Acceptance requires approval of the work item by a simple majority of the P-members of the TC or SC voting, and a commitment to participate actively in the development of the project by 5 P-members approving the work item.

❖ **20 - Preparatory stage**

The preparatory stage covers the preparation of a Working Draft (WD). A WG is defined and a project leader, responsible for the development of the project, is assigned. Several successive WD can be considered until the WG has acquired the certainty of having developed the best technical solution to the problem considered. The preparatory stage ends when a WD is available for circulation to the members of the TC /SC as a first Committee Draft (CD).

❖ **30 - Committee stage**

The committee stage is the principal stage at which comments from national bodies are taken into consideration, with a view to reaching consensus on the technical content. National bodies shall therefore carefully study the texts of committee drafts and submit all pertinent comments at this stage. The decision to progress to the next step shall be taken on the basis of the consensus principle. It is the responsibility of the chairman of TC / SC, in consultation with the secretary of his committee and, if necessary, the project leader, to judge whether there is sufficient support bearing in mind the definition of consensus given in ISO/IEC Guide 2:2004 [1]:

"Consensus: General agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments.
NOTE Consensus need not imply unanimity."

Within ISO, in case of doubt concerning consensus, approval by a two-thirds majority of the P-members of the TC or SC voting may be deemed to be sufficient for the committee draft to be accepted for registration as an enquiry draft; however every attempt shall be made to resolve negative votes.

❖ **40 - Enquiry stage**

The Draft International Standard (DIS) is distributed to all national bodies by the ISO Central Secretariat for voting and comment. All ISO member bodies are allowed to vote and the P-members of the committee responsible for the document are required. The votes are: positive, negative, or abstention

- A positive vote may be accompanied by comments (editorial or technical)
- If a national member considers the project as unacceptable, he shall vote negatively and motivate his vote. He may also indicate any changes it deems necessary for acceptance of the project

For a document to be accepted, it must be approved by at least two-thirds of the ISO national members that participated in its development (P-members), and not be disapproved by more than a quarter of all ISO members who vote on it. This is called the "combined voting procedure".

- **50 - Approval stage**

The Final Draft International Standard (FDIS) is circulated to all national bodies by the ISO Central Secretariat for final vote by positive, negative or abstention. If technical comments are received during this period, they are no longer considered at this stage, but are recorded for consideration at a future revision of the international standard. The text is approved as an international standard if the criteria of the combined voting procedure are filled.

- **60 - Publication stage**

When an FDIS was approved, only minor changes are made to the final text, if necessary, before publication.

- **90 - Review stage**

All ISO standards are reviewed at the least three years after publication (and every five years after the first review) by all the ISO member bodies to decide whether the document is still valid and should be confirmed or, alternatively, be revised or withdrawn.

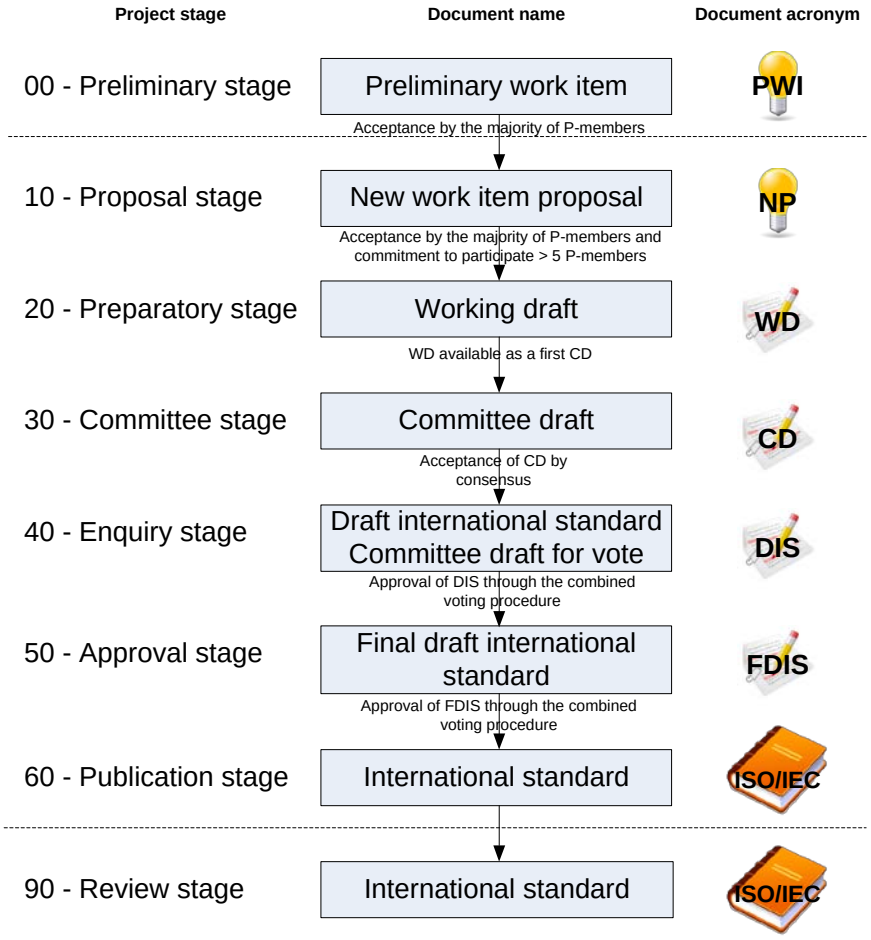

Figure 5: The ISO standardization process

The development duration of an international standard is from 24 months (accelerated schedule) to 48 months (extended planning), the default duration being 36 months.

When the development of an international standard is based on a national standard, or on a standard from another standardization body (e.g., IEEE, W3C, etc.), a "fast track" procedure is usually possible. It is triggered when a document has sufficient maturity to omit certain stages of the classic development of a standard, in order to accelerate its development. The document is submitted for voting and comment to all ISO's member bodies as an enquiry draft (40 - Enquiry stage).

International standards are not the only kind of documents developed within the ISO/IEC JTC1. The other normative documents developed by ISO/IEC JTC1 are:

- **Publicly available specification (PAS):** A normative document representing the consensus within a WG
- **Technical specification (TS):** A normative document representing the technical consensus within an ISO committee
- **Technical report (TR):** An informative document containing information of a different kind from that normally published in a normative document
- **International Workshop Agreement (IWA):** An IWA is an ISO document produced through workshop meeting(s) and not through the TC process
- **ISO Guide:** Guides provide guidance to TC for the preparation of standards, often on broad fields or topics

III. Initiatives and tools in Luxembourg

ILNAS is the national institute in charge of the relations with ISO for Luxembourg. Luxembourg is a member of ISO and was involved in 2012, through national delegates, in the standardization work of 49 TC and SC in areas as diverse as steel, tobacco, ICT, project management, or in policy development committees such as CASCO (Committee for conformity Assessment). Among the 49 TC and SC where Luxembourg is involved:

- 42 are as P-Member
- 7 are as O-Member

1) *The standardization strategy for Luxembourg*

In the government program of 2009, it was highlighted that standardization contributes to labor productivity improvement, trade facilitation and development of new markets[31]. Establishing a standardization strategy for Luxembourg has then become a necessity. ILNAS (*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*), as the Luxembourg's standards body, has been in charge of establishing this strategy, and in June 2010, the standardization strategy for Luxembourg[32] was released. This strategy targets the 2010-2020 decade and is updated every year. The main idea behind this strategy is that participating to the standardization process leads to the development and valorization of the work of the national delegates. This can be summarized in the main principle of the strategy "Setting standards means setting the market".
Furthermore, the standardization strategy for Luxembourg is based on the key concept of "knowledge triangle". The knowledge triangle refers to the interaction between research, education and innovation, which are considered as a foundation of a knowledge-based society. Thus, ILNAS considers as essential to the development of standardization as a support of the national economy:

- The production of normative knowledge, through the involvement of national delegates in the standardization process
- The transfer of this knowledge through training and public awareness
- The use of this knowledge through research and innovation applications

The standardization strategy for Luxembourg consists of 5 pillars:

1. **A sector-based normative approach as a support for the national economy**

In order to support particularly interesting economic sectors in Luxembourg, different sectors will be investigated at the normative level. Examples of such promising sectors are ICT, energy, biomedical technologies, ecotechnologies, etc.

2. **Innovation and research development in the frame of standardization**

Definition and management of research and development projects is a key activity, with regard to the knowledge triangle principle. This white paper is developed, for example, in the frame of a research project about digital trust and standardization. The project has four main objectives:

[31] *http://www.gouvernement.lu/gouvernement/programme-2009/programme-2009/programme-gouvernemental-2009.pdf*
[32] *http://www.ilnas.public.lu/fr/publications/normalisation/etudes-nationales/ilnas-strategie-normalisation-2010-2020.pdf*

- To define what digital trust is and what the digital trust underlying concepts are
- To identify what are the tools and methods helping to improve digital trust in Luxembourg (Public Key Infrastructure (PKI), digital archiving, business continuity management, etc.)
- To develop a normative knowledge-based Economy in order to establish the links between standards, digital trust, innovation and competitiveness
- To support and develop standardization activities currently in progress in Luxembourg, mainly related to the field of ICT, for experts involved in TC and users of standards

3. A sector-based development of the Luxembourg's standards body

In line with the sector-based normative approach, it is necessary to develop the Luxembourg's standards body in a sector-based manner, with the aim to propose new products and services to relevant sectors.

4. Standardization training and public awareness

Public awareness about standardization is a cornerstone to develop standardization activities. For this reason, ILNAS developed and adopted a Strategic Development Plan, describing three main objectives: standardization awareness, standardization training program (presently dedicated to the public sector and to the Luxembourg School for Commerce) and a feasibility study for the development of a training program about standardization and ICT at the Master level. This Strategic Development Plan is accompanied by a monitoring study identifying courses on standardization around the word. ILNAS is also member of several European and international WG (e.g., JWG-EaS, Euras, IFAN) in order to stay aware of best practices in education activities.

5. The establishment and development of the Economic Interest Grouping "*Agence pour la normalisation et l'économie de la connaissance*"

The objective of this Economic Interest Grouping is promotion, awareness, training and monitoring in the field of standardization, and applied research in order to carry out the standardization strategy of Luxembourg, under the control of ILNAS.

2) The national mirror committees of ISO/IEC JTC1

ISO/IEC JTC1 is divided into SC in order to efficiently perform its standardization work. To be efficient at the national level, the same scheme has been used. National mirror committees have been established for ISO/IEC JTC1 and each of its active SC at the national level. A national mirror committee is defined as the mirror committee at the national level of a European or international committee (or SC).

The root committee ISO/IEC JTC1, that can be defined as the strategic level of ICT standardization for ISO and IEC, is followed at the national level by ILNAS. Then, within ISO/IEC JTC1, 6 SC and 1 WG were active in 2012 at the national level. Table 5 summarizes the ICT standardization committees active at the national level and their chairperson with their related economic entity:

Technical committee	Title	Chairperson	Economic actor
ISO/IEC JTC1/WG7	Sensor networks	Reza RAZAVI	AAS
ISO/IEC JTC1/SC6	Telecommunications and information exchange between systems	Pierre BOUTOU	Impact Consulting
ISO/IEC JTC1/SC7	Software and systems engineering	Béatrix BARAFORT	Centre de Recherche Public Henri Tudor
ISO/IEC JTC1/SC17	Cards and personal identification	Benoit POLETTI	Deloitte
ISO/IEC JTC1/SC27	IT Security techniques	Cédric MAUNY	Telindus
ISO/IEC JTC1/SC36	Information technology for learning, education and training	Stéphane JACQUEMART	Centre de Recherche Public Henri Tudor
ISO/IEC JTC1/SC38	Distributed application platforms and services (DAPS)	Jürgen BLUM	Cetrel S.A.

Table 5: The national mirror committees of ISO/IEC JTC1

Moreover, 34 delegates from Luxembourg were involved in 2011 in ISO/IEC JTC1. The list of the delegates is freely available on the website of ILNAS[33]. The number of delegates per national mirror committee is depicted in Table 6.

Committee	JTC1	WG7	SC6	SC7	SC17	SC27	SC36	SC38
Number of delegates	3	2	1	12	1	13	3	1

Table 6: Delegates per national mirror committee

[33] *http://www.ilnas.public.lu/fr/normalisation/participation-aux-travaux-de-normalisation/index.html*

When an international standardization committee is followed by only one person, or several that are all representative of the same economic entity, it is followed by that person (resp. that entity) with the role of chair. It is thus responsible to establish the positions of Luxembourg for the questions and votes of the committee. When at least two delegates, coming from different economic actors in Luxembourg, are registered in a national mirror committee, a chairperson is appointed, which is especially the convener of the group. The chairperson is responsible of reaching a consensus each time it is necessary within the group. This second case is naturally the soundest situation, for Luxembourg to be represented globally, and not by only one stakeholder.

Each national mirror committee is allowed to participate to international meetings. Delegates shall thus be appointed to represent the positions of the national mirror committee, and they shall be communicated to ILNAS prior to the meeting.

3) The tools developed by ILNAS to convene ISO/IEC JTC1 at the national level

Three tools have been established by ILNAS to manage ICT standardization at the national level:

- **ISO/IEC JTC1 national forum**

A communication platform between ICT standardization actors in Luxembourg has been set up through the concept of "ISO/IEC JTC1 national forum". It is composed of the chairpersons of the national mirror committees of the ISO/IEC JTC1 SC, and the delegates of ILNAS that are currently chairing ISO/IEC JTC1 at the national level. The forum meets normally on a quarterly basis. The topics covered are:

- To follow the different topics of ISO/IEC JTC1: votes, comments, feedbacks from the ISO/IEC JTC1 plenary meetings
- To facilitate information exchange between ILNAS and the chairs of the national mirror committees related to ISO/IEC JTC1 SCs
- To promote communication and exchanges between the chairs of the national mirror committees related to ISO/IEC JTC1 SCs
- To prepare the annual ISO/IEC JTC1 national day and the ISO/IEC JTC1 plenary meeting

- **ISO/IEC JTC1 national day**

ISO/IEC JTC1 national day is the event aiming at informing the national market about current trends and developments of ICT standardization and promoting ICT standardization in Luxembourg. In 2011, it took for example the form of a conference, hold on the World Standards Day (14.10.11) in the Chamber of Commerce, on the topic: "International Standards – Creating confidence globally". The focus in 2011 was Cloud Computing, that is a clearly hot ICT standardization topic. Generally each year, such an ISO/IEC JTC1 event will be held in Luxembourg.

- **ISO/IEC JTC1 national chapters**

An ISO/IEC JTC1 national chapter is established when a delegate (or group of delegates) in Luxembourg is (co-)editor of an ISO/IEC JTC1 standard and needs some input from an economic sector to develop the standard. An *ad-hoc* committee, called a "national chapter", is thus established

with representatives of this economic sector, which purpose is to gather relevant input for the standard in progress, and to provide to the editor a regular feedback about its current work. This initiative naturally helps to take into account the point of view of the stakeholders of Luxembourg.

A first chapter was already opened in 2009, in the frame of the ISO/IEC 27015 standard development about "ISMS guidance for financial services". The representatives of the financial sector were linked with the editor of the standard, member of the ISO/IEC JTC1/SC27 national mirror committee.

IV. Conclusion

The standardization committee ISO/IEC JTC1 is today recognized as the focal point of formal standardization in ICT. ISO/IEC JTC1 is also the leading organization for initiation of new areas of standardization, and for progression of specifications developed in other ICT-related *consortia/fora* into true international standards. As mentioned in the ISO/IEC JTC1 Value Proposition [7], the standards developed in ISO/IEC JTC1:

- are globally recognized
- provide global interoperability
- provide sustained development and retention of investment

In terms of added value related to the involvement of an organization in ISO/IEC JTC1, we can first mention the anticipation of future technical regulations and best practices. Innovation dissemination, through an active participation to standards development, is another advantage. Standardization is finally a particularly interesting field towards a knowledge-based economy, aligned with European Union's growth strategy for the coming decade called "Europe 2020" [9]. The preceding advantages well illustrate the principle "Setting standards means setting the market".

Luxembourg, through ILNAS that is its National Standardization Body, is aware of these statements and is positioned as a P-member of ISO/IEC JTC1. In order to inform the economic actors at the national level and to strengthen their participation to ISO/IEC JTC1, ILNAS has set up a standardization strategy clearly mentioning its commitment to ISO/IEC JTC1 and has defined tools dedicated to its management: ISO/IEC JTC1 national forum, ISO/IEC JTC1 national day and ISO/IEC JTC1 national chapters.

Within ISO/IEC JTC1, 6 SC and 1 WG were active in 2012 at the national level. By analyzing the national mirror committees active at the national level (Table 5), and furthermore the number of delegates per national mirror committee (Table 6), the participation in ICT standardization depicts an interest of experts in Luxembourg for the management part of ICT, such as information security and software and system engineering, that are both the most represented committees. The standardization committees proposing standards for ICT products (at the hardware level, such as ISO/IEC JTC1/SC25 on interconnection of ICT equipment, or at the software level, such as ISO/IEC JTC1/SC22 on programming languages and ISO/IEC JTC1/SC24 on language description) are currently of less interest for the national market. However, it would be good for ILNAS to have a delegate from Luxembourg in most SC of ISO/IEC JTC1. Luxembourg being a P-member of ISO/IEC JTC1, it is an asset to be skilled and represented in every SC of ISO/IEC JTC1, in order to strengthen the presence of Luxembourg at the international level.

Finally, in the frame of ICT standardization, the following objectives have been defined by ILNAS in its update of the standardization strategy for Luxembourg:

- To develop communication and public awareness about ICT standardization
- To follow and inform the stakeholders about new standardization activities having a potential impact on the economy in Luxembourg (e.g. Cloud Computing)
- To extend the scope to non-ISO/IEC standardization groups
- To develop research activities

References

[1] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC Guide 2:2004, Standardization and related activities — General vocabulary, 2004.

[2] AFNOR Normalisation (*Association Française de Normalisation*). *Impact économique de la normalisation*, 2009.

[3] DIN (*Deutsches Institut für Normung*). The Economic Benefits of Standardization, 2011.

[4] BSI (British Standards Institution). Standardization as a business investment, accessed in 2011.

[5] SCC (Standards Council of Canada). Economic value of standardization, 2007.

[6] The European Parliament and the Council of the European Union. Official Journal L 204, Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, 1998.

[7] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). The JTC1 value proposition, 2010.

[8] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC Directives, Part 1, Procedures for the technical work, 2009.

[9] European Commission. EUROPE 2020 – A European Strategy for Smart, Sustainable, and Inclusive Growth, COM(2010) 2020, 2010.

B) Certification and accreditation

In this chapter, the concepts of certification and accreditation will be discussed. The first section introduces certification and conformity assessment and gives some details about the certification process. In the second section, accreditation and its link with certification are presented. An overview of accreditation bodies, the mutual recognition principle, and the related regulations and standards is performed. The last section is about OLAS (*Office Luxembourgeois d'Accréditation et de Surveillance*) the national accreditation body. After introducing its structure and missions, a focus is done on its recognition at the European and international level. The accreditation process of OLAS and its involvement in European and international committees is finally presented.

I. Introduction to certification

Nowadays, a lot of companies are promoting on their website they are ISO 9001 [1] certified. ISO 9001 is currently the most internationally well-known certification, with more than a million of certifications, demonstrating that a quality management system has been set up. However, ISO 9001 is not the only standard being the reference for a certification. Some other popular certifications are based on the following standards:

- ISO 14001 [2] dealing with "Environmental management systems"
- ISO/IEC 27001 [3] dealing with "Information security management systems"
- ISO 22000 [4] dealing with "Food safety management systems"
- etc.

The previous list is not exhaustive.

1) Certification and conformity assessment

Based on the definitions of ISO/IEC 17000 [5], certification can be defined as a third-party attestation of the conformity of a product, process, system or person to requirements specified in a standard. A certification is thus different from a label that is not defined through legal or normative dispositions[34]. It is important to note that each type of organization can be certified, regardless of its size, business or type. Furthermore, a certification is a voluntary-based approach, driven by the strategy and motivation of the interested body.

Attestation of the conformity of a product, process, system or person to requirements is performed through a conformity assessment. In ISO/IEC 17000 [5], conformity assessment is defined as the "demonstration that specified requirements relating to a product, process, system, person or body are fulfilled". Conformity assessment can be performed either by the supplier itself, providing its commitment of the quality of its products, services or processes, or by a third-party Conformity Assessment Body (CAB). A certification can only be obtained in the latter case. Regarding the scope of certification, it is applicable to all objects of conformity assessment except for CAB themselves, to which accreditation is applicable [5].

[34] *Labels can be defined as a collective mark established by a professional sector to guarantee a product / service has a given set of characteristics*

At the international level, certifications of management systems are still increasing (see Figure 1).

At the national level, the MLQ ("*Mouvement Luxembourgeois pour la Qualité*") is an association promoting and encouraging the implementation of initiatives for quality and its management in Luxembourg. Based on the figures collected by the MLQ, certification is also continuously progressing in Luxembourg.

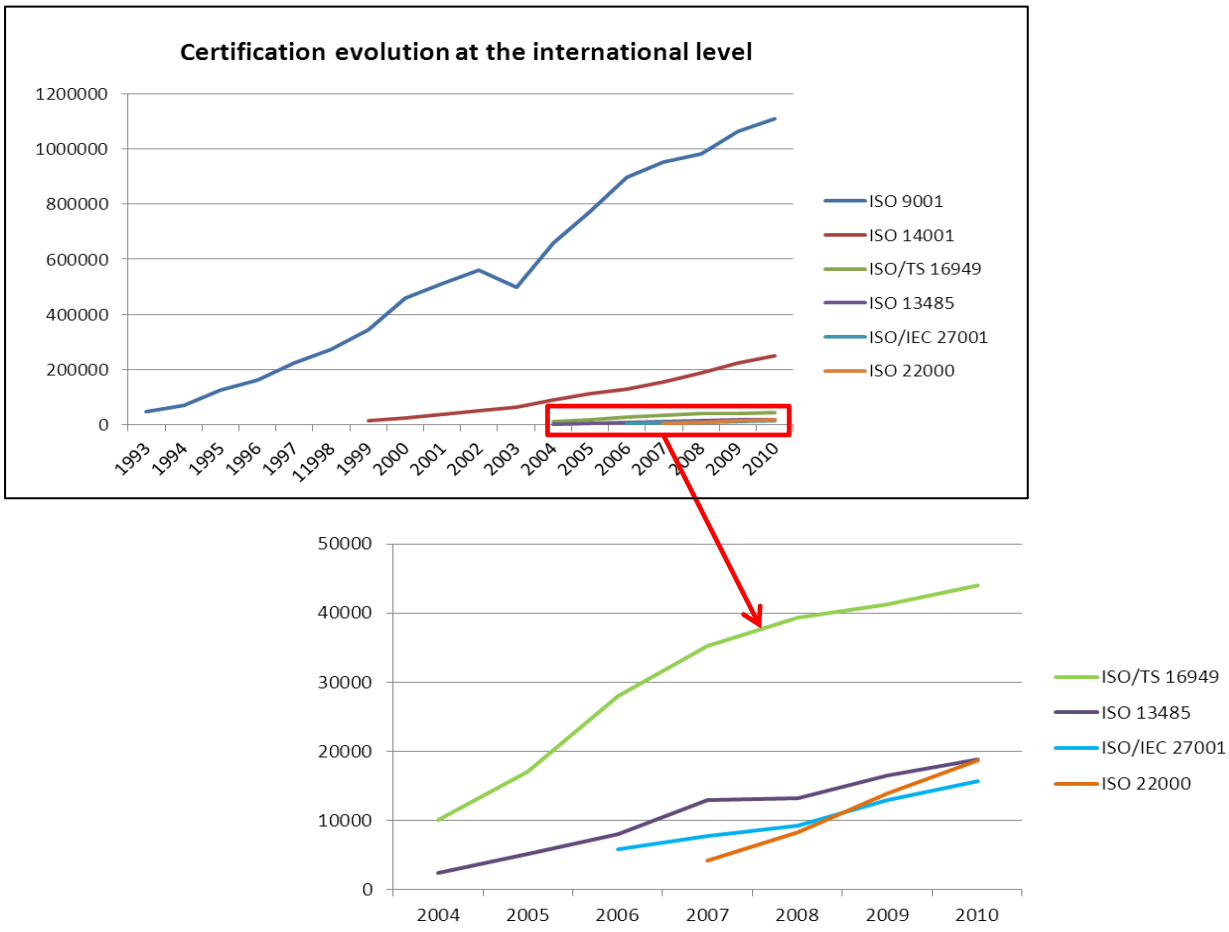

Figure 1: Certification evolution at the international level

Certification can also be issued according to the regulation. Before placing on the market, the certification, by notified bodies[35], of some categories of products according to "New Approach" directives[36], is mandatory before giving the authorization to the manufacturers to use the CE mark. The CE marking attests the conformity of the products with the applicable requirements of the relevant Community harmonization legislation. It is not a quality mark. It can be considered as the passport to free circulation of new products through the Community market. The main purpose of the CE marking is to support market surveillance services activities.

[35] *http://ec.europa.eu/enterprise/newapproach/nando/*

[36] *http://www.newapproach.org/*

2) The certification process

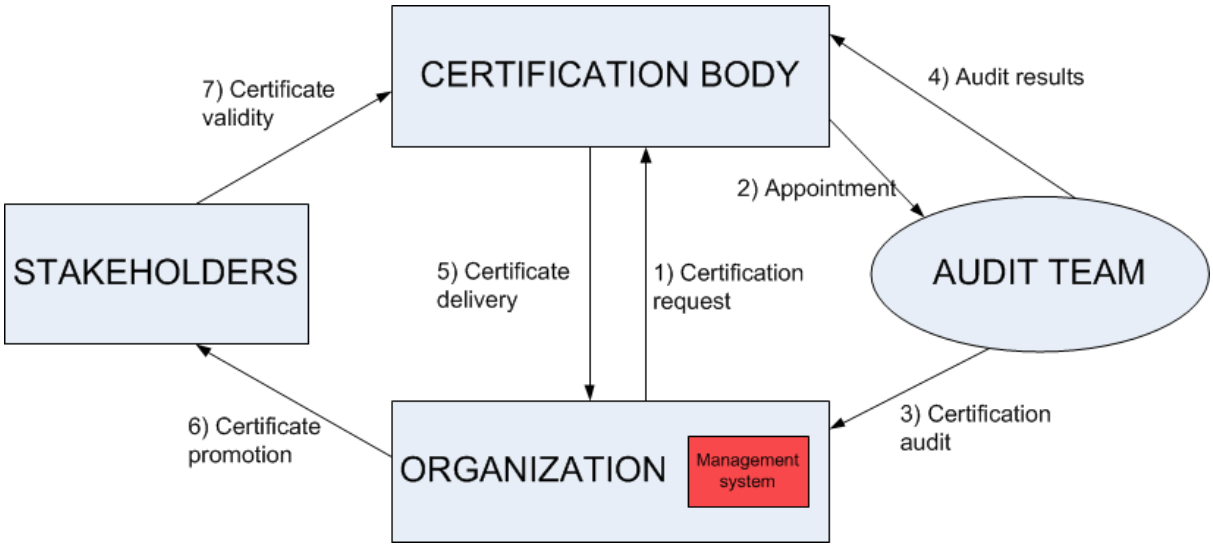

Figure 2: The certification process

Before being certified according to a certification standard, a body has to put in place a quality management system based on the requirements of this standard. The process to be certified is the following (see Figure 2):

1) The body sends an application to a competent certification body in order to be certified.
2) The certification body appoints a competent audit team.
3) The team performs the certification audit.
4) Once the audit is completed, the team transmits the audit results to the certification body.
5) When the audit results give confidence to the conformity on the requirement of the standard, the certification body delivers the certificate to the organization.
6) Once certified, the organization is allowed to communicate and promote to its stakeholders (clients, economic partners, authorities) on its certification.
7) The stakeholders are able to verify the validity of the certificate to the certification body.

In most of cases, a certification is issued for a three years cycle. Within this cycle, the respect of the conformity of the organization is controlled, through surveillance audits, by the certification body. A similar process is applied for the certification of products, systems or persons.

II. The trust chain of accreditation and certification

As explained in the previous section, the aim of the certification is to demonstrate that specified requirements relating to products, processes, systems or persons are fulfilled. This demonstration requires specific competences from the certification body, and it is naturally a cornerstone of such a model to be sure that the certification body is competent enough to perform such a demonstration. Accreditation is the most common and relevant way for a certification body to guarantee its competence to perform its activities. This section defines accreditation, its scope, the related regulations and standards, and finally the regional and international mutual recognition principle.

1) Accreditation definition and scope

As defined in ISO/IEC 17000 [5], accreditation is a "third-party attestation related to a CAB conveying formal demonstration of its competence to carry out specific conformity assessment tasks". The definition proposed by the Regulation (EC) No 765/2008 [6] is "an attestation by a national accreditation body that a CAB meets the requirements set by harmonized standards and, where applicable, any additional requirements including those set out in relevant sectorial schemes, to carry out a specific conformity assessment activity". In summary, accreditation-related activities consist in:

- The formal demonstration of CAB competence to carry out specific conformity assessment tasks
- The independent and authoritative attestation of the competence, impartiality, and integrity of CAB
- The elimination of technical barriers to trade and contributing to the protection of fundamental rights of people
- The harmonization of accreditation rules and procedures at world-wide level

Accreditation means increased confidence in the observance of required level of quality of the provided services. The particular value of accreditation lies in the fact that it provides an authoritative statement of the technical competence of bodies whose task is to ensure conformity with the applicable requirements [6]. Accreditation is a tool to ensure a high level of confidence in the results, reports or certificates issued by the CAB and of the independence and impartiality of accredited organizations. It is commonly used to generate the confidence of national authorities responsible for monitoring the compliance of products and services, economic operators and consumers. It aims to facilitate the free movement of such products and services by helping to remove technical barriers to trade. For laboratories, it is also a guarantee that the equipment used for their activities are compliant with the international system of units.

For many organizations, an accreditation is not mandatory. CAB can apply to be accredited by their National Accreditation Body (NAB). This is a voluntary-based initiative that aims to give confidence to the market by stating that the CAB is competent against the relevant European or international standards. However, for some fields, accreditation may be mandatory. According to the decision (EC) n° 768/2008, accreditation shall now be used as the preferred medium to demonstrate the competence of CAB in view of their notification to the European Commission for monitoring the compliance of certain products to the requirements of the European Union harmonization legislation.

2) Accreditation bodies

Accreditation activities are based on a 3-level chain of trust. First, the NAB provides accreditation to organizations at the national level. Member states should not maintain more than one NAB by country. OLAS is the NAB for Luxembourg and is presented in Section 3 of this chapter in further details. NABs are then monitored at the regional level. Each continent has its own regional body and the European co-operation for Accreditation (EA) is the one for Europe. Finally, at the international level, two organizations are managing accreditation:

- the International Accreditation Forum (IAF) for the certification bodies
- the International Laboratory Accreditation Cooperation (ILAC) for laboratories and inspection bodies

The main role of these organizations is to harmonize accreditation practices implemented by the NAB. This harmonization of accreditation practices is resulting in the drafting and publication of guides for the application and interpretation of standards based on the results of working groups involving the NAB. The harmonization process is guaranteed by peer reviews. This process is one of the bases of the mutual recognition principle between the different NAB, to see in the next sub-section.

At the regional level the five organizations representing the NAB of the five continents are:

- European co-operation for Accreditation (EA), which covers the European region for all types of accreditation
- Asia Pacific Laboratory Accreditation Cooperation (APLAC), which covers the Asia Pacific region for the accreditation of laboratories and inspection bodies
- Pacific Accreditation Cooperation (PAC), which covers the same area for the accreditation of inspection bodies and certification
- Inter-American Accreditation Cooperation (IAAC), which covers the Americas region for all types of accreditation
- South African Development Cooperation in Accreditation Commity's (SADC), which covers the southern Africa region for all types of accreditation

As a member of the European Union, OLAS is member of EA which is in charge to harmonize the accreditation practices in laboratories, inspection bodies and certification at the European level.

Figure 3: Logo of the European co-operation for Accreditation

At the international level, IAF is the world association of conformity assessment accreditation bodies active in the fields of management systems, products, services, personnel and other similar programs of conformity assessment. ILAC is an international cooperation of conformity assessment accreditation bodies active in the field of laboratory and inspection.

Figure 4: Logo of the International Accreditation Forum and of the International Laboratory Accreditation Cooperation

3) The mutual recognition principle

Today, most of states have a NAB responsible for the official recognition of the competence of the CAB. To accredit their customers, the NABs have agreed to use the same standards. Due to this alignment, accreditation of CAB is based on the same rules world-wide.

This joint approach has allowed the states concerned to conclude and sign agreements based on mutual recognition of their accreditation systems. The signature of so called Multilateral Agreements (MLA) (or Mutual Recognition Arrangements (MRA) for ILAC) is essential for the recognition of results, reports or certificates issued by the different accredited CAB. Through these agreements, each signatory state recognizes a CAB accredited by another state as if he had himself granted the accreditation. The MLA eliminates the need for suppliers of products or services to be certified in each country where they sell their products or services, and then simplify the free movement of goods and services within Europe and the world.

At the international level, IAF and ILAC have developed their own peer evaluation system but they rely heavily on the MLA developed and issued by the three regional accreditation groups EA, PAC and IAAC. To be recognized at the international level, the regional peer evaluation systems are also evaluated by representatives of IAF and ILAC. This peer evaluation system represents the guarantee of confidence in the 3 level accreditation systems all over the world.

In Europe, the principle of mutual recognition is fixed in new European legislative framework providing a legal basis to accreditation. At the European level, the MLA is defined as an agreement signed by the NAB members of EA to recognize the equivalence, reliability and therefore recognition of accredited certifications, inspections, calibration certificates and test reports across Europe.

The EA MLA accepts:

- the equivalence of the operation of the accreditation systems administered by EA Members;
- the certificates and reports issued by organizations accredited by EA Members are equally reliable.

NAB are evaluated according to the national and European regulation, the standard ISO/IEC 17011, the guides published by EA, ILAC or IAF, and applicable criteria on behalf of European or National Regulators and industrial schemes. The strength of the MLA is maintained through a robust peer evaluation process. The purpose of these rigorous on-site evaluations is to verify that the CAB are continuously conforming to the internationally accepted criteria. The MLA process is overseen at the European level by the European Commission, the EA Advisory Board and the national authorities.

4) Accreditation standards

Accreditation activities can be classified in three different fields:

- Accreditation of laboratories, for testing and calibration or for medical analyses
- Accreditation of certification bodies, providing certification of products, persons and/or management systems
- Accreditation of inspection bodies

Each field of accreditation is covered by specific standards, providing the requirements an applicant (laboratory, certification body or inspection body) has to comply with. The following table summarizes the accreditation standards:

	Field	Standard
Accreditation of inspection bodies	Inspection	ISO/IEC 17020
Accreditation of certification bodies	Certification of management systems	ISO/IEC 17021
	Certification of persons	ISO/IEC 17024
	Certification of products	ISO/IEC Guide 65 or EN 45011
	Greenhouse gas validation and verification bodies	ISO 14065
Accreditation of laboratories	Testing, Calibration	ISO/IEC 17025
	Medical analyses	ISO 15189

Table 1: Accreditation fields and associated standards

Along with the standards presented in Table 1 the ISO/IEC 170xx series gives specific information on conformity assessment. These standards are developed by the CASCO (Committee on conformity assessment). The following list describes the main standards of this series:

- ISO/IEC 17000:2004 Conformity assessment - Vocabulary and general principles
- ISO/PAS 17001:2005 Conformity assessment - Impartiality - Principles and requirements
- ISO/PAS 17002:2004 Conformity assessment - Confidentiality - Principles and requirements
- ISO/PAS 17003:2004 Conformity assessment - Complaints and appeals - Principles and requirements
- ISO/PAS 17004:2005 Conformity assessment - Disclosure of information - Principles and requirements
- ISO/PAS 17005:2008 Conformity assessment - Use of management systems - Principles and requirements

- ISO/IEC 17007:2009 Conformity assessment - Guidance for drafting normative documents suitable for use for conformity assessment
- ISO/IEC 17011:2004 Conformity assessment - General requirements for accreditation bodies accrediting conformity assessment bodies

5) The European accreditation regulation

Regulation (EC) N° 765/2008 of the European Parliament and of the Council of 9th July 2008, setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EC) No 339/93, establishes a legal framework for accreditation in the EU/EFTA (European Free Trade Association) member states.

The motivation behind this regulation is that "it is necessary to ensure that products benefiting from the free movement of goods within the Community fulfill requirements providing a high level of protection of public interests such as health and safety in general, health and safety at the workplace, protection of consumers, protection of the environment and security, while ensuring that the free movement of products is not restricted to any extent greater than that which is allowed under Community harmonization legislation or any other relevant Community rules".

The operation of this new legislative framework for accreditation is based on the principle of mutual recognition of NAB being EA members. Furthermore, it provides the establishment of EA as the official European accreditation infrastructure, while reinforcing the role of EA and accreditation in both voluntary and regulated sectors. This regulation came into force the 1st January 2010.

In compliance with the Regulation 765/2008, the member states shall:

- appoint a single accreditation body per member state
- recognize the appointed NAB and monitor its operation
- develop accreditation as a service of general interest with a public authority status as the last level of control of conformity assessment services in the voluntary and law regulated fields
- operate at the national level upon suitable mandate of the governments, in full independence and impartiality, on a non-profit-distributing and non-competitive basis
- are fully accountable to accreditation stakeholders and their structure does not allow for predominant interests to take control

This Regulation shall be seen as complementary to Decision N° 768/2008/EC of the European Parliament and of the Council of 9th July 2008 [7]. The Decision lays down common principles and reference provisions intended to apply across sectorial legislation in order to provide a coherent basis for revision or recasts of that legislation. This Decision therefore constitutes a general framework of a horizontal nature for future legislation harmonizing the conditions for the marketing of products and a reference text for existing legislation. It provides, in the form of reference provisions, definitions and general obligations for economic operators and a range of conformity assessment procedures from which the legislator can select as appropriate. It also lays down rules for CE marking. Furthermore, reference provisions are provided as regards the requirements for conformity assessment bodies to be notified to the Commission as competent to carry out the relevant conformity assessment procedures and as regards the notification procedures. In addition, this Decision includes reference provisions concerning procedures for dealing with products presenting a risk in order to ensure the safety of the market place.

III. OLAS: the accreditation body of Luxembourg

1) *Introduction to the "Office Luxembourgeois d'Accreditation et de Surveillance" (OLAS)*

OLAS is the sole accreditation body of CAB in Luxembourg, compliant with the Regulation (EC) N° 765/2008. It is a department of ILNAS which is a governmental administration under the authority of the Minister of the Economy and Foreign Trade.
The national legal basis supporting the accreditation system is constituted by:

- The **law of 20 May 2008,** concerning the creation of a Luxembourg Institute of standardization, accreditation, security and quality of products and services
- The **Grand-Ducal regulation of 28 December 2001**, setting up an accreditation system for inspection and certification organizations, as well as for testing and calibration laboratories, and establishing the Luxembourg Office of Accreditation and Surveillance, an Accreditation Committee and a National Compendium of Quality and Technical Assessors

In order to ensure the impartiality of its accreditation decisions, OLAS is a department operating independently from the other departments. It has its proper management system (based on the standard ISO/IEC 17011 [8]), its own staff, its own logo and it supervises its own expenses and incomes.

OLAS is mainly responsible of the three following missions:

- Accreditation of CAB
- The evaluation and surveillance of notified CAB with respect to the Luxemburgish legislation transposing EU harmonization legislation
- Good Laboratory Practices management

2) *The accreditation committee*

To strengthen the impartiality of its accreditation decisions and to ensure its good functioning, an accreditation committee has been established. Its main purpose is to assist the ILNAS director in the process of decision-making for each decision concerning an accreditation (e.g., granting, maintaining, withdrawal, etc.).
The accreditation committee consists of 14 members appointed by the Minister of Economy and Foreign Trade and 2 experts chosen by the committee members for their technical skills. The objective is to avoid any predominance of interest. The committee members represent a balanced set of:

- Authorities (representatives of ministries and administrations)
- Economic partners (representatives of professional chambers and consumers)
- Customers of accreditation (representatives of laboratories, inspection and certification bodies)

The mission of the accreditation committee also includes the following:

- To provide proposals concerning general orientation about the accreditation of CABs
- To provide proposals concerning the functioning of OLAS
- To propose the eventual removal of a quality assessor, a technical assessor or an expert from the « National compendium of quality and technical assessors »

3) Mutual recognition of OLAS

To meet the requirements of Regulation (EC) N° 765/2008, OLAS has been assessed by his peers according to national and European legislation, the ISO/IEC 17011 [8] standard and the EA, IAF and ILAC guidelines. Since April 14th, 2011, OLAS is signatory of the EA MLA for the following areas:

- Testing and medical laboratories
- Inspection bodies
- Certification bodies for products and management systems

Through the mutual recognition agreements between regional and international organizations, OLAS is also signatory of IAF MLA and ILAC MRA for the previous domains. OLAS is now recognized as equivalent to other accreditation bodies having signed the same agreements. Thus, results, reports or certificates issued by conformity assessment bodies accredited by OLAS are recognized by other NAB as if they themselves had granted the accreditation.

4) The accreditation process of OLAS

Accreditation is issued based on national and European legislation, European and international standards, on other normative documents related to accreditation and on any other document provided by European and international accreditation bodies.

OLAS issues accreditations to:

- testing laboratories according to ISO/IEC 17025
- calibration laboratories according to ISO/IEC 17025
- medical laboratories according to ISO 15189
- inspection bodies according to ISO/IEC 17020
- certification assessment bodies for:
  - management systems according to ISO/IEC 17021
  - products according to EN 45011
  - greenhouse gases verifiers according to ISO 14065
  - persons according to ISO/IEC 17024

For most organizations, the accreditation is done on a voluntary basis. However, accreditation is mandatory in support to the notification of conformity assessment bodies under technical harmonization legislation, as described in the Regulation (EC) N° 765/2008 [6] and in the Decision N° 768/2008/EC [7] of the European Parliament and of the Council. In Luxembourg, the inspection bodies active on the domain of building also have to be accredited before receiving an agreement.

The accreditation cycle is described by the Figure 5.

The accreditation is issued based on quality and technical assessments. The objective of the assessment is to verify the competence of the CAB to perform the conformity assessment activities defined in its accreditation scope. This scope is the most important outcome of the accreditation process because it defines, in a very detailed way, the domains of activities where OLAS is confident in the competence of the CAB.

If the result of the assessment is positive, OLAS will grant the accreditation to the CAB for a 5 years period. Each year a surveillance assessment is organized to check if the quality management system is still conforming to the standard and if the CAB is still competent for the activities covered by the accreditation. After 5 years, a reassessment is organized before starting a new accreditation cycle (see Figure 5). More information can be found in the quality manual of OLAS and the associated procedures[37].

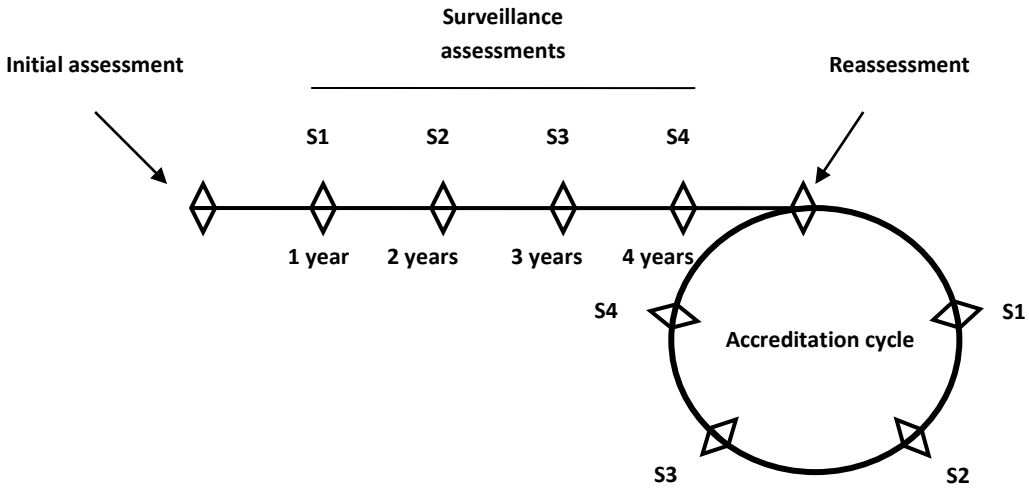

Figure 5: The accreditation cycle

5) OLAS involvement in international committees

To represent the interests of Luxembourg and also to keep itself informed regarding accreditation standards and practices, OLAS is participating to the EA, IAF and ILAC working groups.

At the European level, OLAS is involved in the following committees managed by EA:

- the Certification Committee (CC), the Inspection Committee (IC) and the Laboratory Committee (LC), discussing all technical issues related respectively to the accreditation of certification bodies, inspection bodies and laboratories, with the view of establishing best practice and fostering harmonization;
- the Horizontal Harmonization Committee (HHC), dealing with horizontal technical issues regarding the application of general accreditation requirements on different types of conformity assessment bodies, the assessment of notified bodies and the elaboration of

[37] *http://www.ilnas.public.lu/fr/accreditation-oec/documents-accreditation/manuel-qualite/index.html*

decisions on sector schemes. The Committee focuses on ISO/IEC 17011 and monitors the network sharing of knowledge for EU directives;

- the Multilateral Agreement Council (MAC) managing the peer evaluation process and deciding on MLA signatories. The MAC is also responsible for the evaluators' training, monitoring and harmonization activities;
- The General Assembly, the highest decision-making body of the association, supervises the management and the general course of affairs in the association and gives instructions in respect of the general policies.

At the international level, OLAS participates to the annual ILAC/IAF conference, dealing with the same topics at the international level.

Through its active participation to the committees at the European and international level, OLAS is also involved in policy and guidelines development for CAB accreditation.

Since 2010, through the involvement of OLAS, Luxembourg has become participating member (P-member) of the ISO policy development committee called CASCO, in charge of international guides and standards development related to conformity assessment. Moreover, OLAS is also involved in the ISO Technical Committee (TC) 212 entitled "Clinical laboratory testing and in vitro diagnostic test systems". As in any other standardization domain where Luxembourg is active, a national mirror committee has been established for CASCO and TC 212 in order to support the communication between the national interested parties and to facilitate the commenting and voting activities on the normative documents in progress. Registration and participation to these ISO committees is open and free of charge for anyone having knowledge in these domains[38].

[38] *http://www.ilnas.public.lu/fr/normalisation/participation-aux-travaux-de-normalisation/index.html*

IV. Conclusion

OLAS, as the accreditation body of Luxembourg, is the organism in charge of delivering accreditations at the national level. As seen in the previous sections, accreditation is first the link in the chain of trust between consumers and certifications, guaranteeing the competence of CAB and providing the same value to each concerned certification all around the world. Accreditation is also referenced in European regulations, in order to provide a high level of trust to specific organizations, such as notified organizations.

Through an active participation in international committees, related to accreditation bodies (EA, IAF, ILAC) or to ISO, OLAS regularly represents the interests of Luxembourg at the international level. At the national level, each year an accreditation day is organized to communicate to its auditors, clients and the accreditation committee members. This day is an opportunity for OLAS to inform the different stakeholders of accreditation on the evolutions in the domain of accreditation and notification of CAB. More technical topics such as inter-laboratory testing, metrology equipment, measurement uncertainties are also discussed during this event.

References

[1] ISO (International Organization for Standardization). ISO 9001:2008, Quality management systems — Requirements, 2008.

[2] ISO (International Organization for Standardization). ISO 14001:2004, Environmental management systems — Requirements with guidance for use, 2004.

[3] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements, 2005.

[4] ISO (International Organization for Standardization). ISO 22000:2005, Food safety management systems — Requirements for any organization in the food chain, 2005.

[5] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles, 2004.

[6] The European Parliament and the Council of the European Union. Regulation (EC) No 765/2008 of the European Parliament and 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, 2008.

[7] The European Parliament and the Council of the European Union. Decision No 768/2008/EC of the European Parliament and the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, 2008.

[8] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC 17011:2004, Conformity assessment — General requirements for accreditation bodies accrediting conformity assessment bodies, 2004.

Conclusion

As a conclusion, it is clearly important to note that the outcome of the white paper is not only to describe what digital trust is and what the supporting tools are, but it is also to make people aware of the work performed in Luxembourg to improve digital trust. The digital world has usually a dark brand image, mainly coming from the bad reputation of the Internet, viruses, hackers, etc., and the significant consequences they have on the business of companies. However, it is important to note that, even if some risks always remain, working with an electronic system that is highly reliable and secure — in a nutshell: a trustable system — is something bringing a lot of benefits at the economic and social level.

ILNAS is aware of this statement and that is why digital trust is a core topic with a dedicated department. Indeed, to find new ways of improving digital trust in Luxembourg is still an emerging and promising challenge. This white paper lies currently on the research results already produced at the national level and reflects thus only the current point of view of the different authors. The objective is to regularly update it and, moreover, to keep it open to any new digital trust instrument. The up-to-date version of the white paper will always be available *via* ILNAS. ILNAS aims thus now to carry on working in this field, by defining research projects and developing collaboration with research institutes, in order to reach the objective of bringing Luxembourg as a leader of digital trust at a world-wide level.

In order to develop a digital trust state, you need to understand the concept, to dispose of the related tools and applications, to have a strong security context and be aware of what is relevant in this frame, then some confidence tools related to demonstrate the skills of the different *ad hoc* protagonists, that is what is in place in Luxembourg.

Contacts

Chapter 1 - Digital trust, a definition and an introduction to the concept

Centre de Recherche Public Henri Tudor
29, avenue John F. Kennedy
L-1855 Luxembourg

Email: info@tudor.lu
Phone: (+352) 42 59 91 – 1

http://www.tudor.lu

Chapter 2 - Technical tools for digital trust

Centre de Recherche Public Henri Tudor
29, avenue John F. Kennedy
L-1855 Luxembourg

Email: info@tudor.lu
Phone: (+352) 42 59 91 – 1

http://www.tudor.lu

Chapter 3 - Digital trust through information security

Smile GIE
41, avenue de la gare
L-1611 Luxembourg

Email: info@smile.public.lu
Phone: (+352) 2740098 601

http://www.smile.public.lu

Chapter 4 - Digital trust through the knowledge of standardization and certification

ILNAS
Digital Trust department
34-40, avenue de la Porte-Neuve
L-2227 Luxembourg

Email: confiance-numerique@ilnas.etat.lu
Phone: (+352) 46 97 46 42

http://www.ilnas.public.lu

OLAS
Office Luxembourgeois d'Accréditation et de Surveillance
34-40, avenue de la Porte-Neuve
L-2227 Luxembourg

Email: olas@ilnas.etat.lu
Phone: (+352) 46 97 46 45

http://www.ilnas.public.lu

CONTACT:

ILNAS, Digital Trust department

34-40, avenue de la Porte-Neuve

L-2227 Luxembourg

Phone: (+352) 46 97 46 42

Email: confiance-numerique@ilnas.etat.lu

www.ilnas.public.lu

June 2012