



WHITE PAPER DIGITAL TRUST TOWARDS EXCELLENCE IN ICT

Acknowledgments

The *Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services* (ILNAS) would like to acknowledge Mr. Robert Van Wessel (ApexIS) for his huge contribution provided on the three first chapters of the white paper, in the frame of the dedicated collaboration between ILNAS and ApexIS.

ILNAS also thanks the Luxembourg Ministry of the Economy (*Direction du commerce électronique et de la sécurité informatique* – Mr. François Thill) for its contribution on the second chapter on the national strategy in the area of information security.

Finally, ILNAS would like to thank the GIE ANEC (*Agence pour la Normalisation et l'Economie de la Connaissance* – Mr. Hervé Peter and Mr. Nicolas Domenjoud), OLAS (*Office Luxembourgeois d'Accréditation et de Surveillance* – Mr. Dominique Ferrand) and the ILNAS Digital trust department (Mr. Jean-Philippe Humbert and Mr. Alain Wahl) for their continuous involvement in the update of the white paper.

Table of Contents

Foreword	1
Abbreviations	3
Introduction	9
CHAPTER 1: Digital trust, a definition and an introduction to the concept	11
I. The concept of trust	11
II. Digital Trust	14
III. New regulation.....	16
IV. Recent developments.....	17
1) Big Data	17
2) A framework of trust in online transactions	18
3) Reputation systems.....	19
4) Trust mechanisms for Cloud Computing.....	20
V. Conclusion.....	24
CHAPTER 2: Digital trust through information security	27
I. Introduction.....	27
II. ISO/IEC 27000 series.....	29
1) Information security and ISMS.....	29
2) ISO/IEC 27000	30
3) ISO/IEC 27001	31
4) ISO/IEC 27002	33
5) ISO/IEC 27003	34
6) ISO/IEC 27004	35
7) ISO/IEC 27005	35
8) ISO/IEC 27006	36
9) ISO/IEC 27007	36
10) ISO/IEC TR 27008	37
11) ISO/IEC WD 27009.....	37

12)	ISO/IEC 27010	37
13)	ISO/IEC 27011	38
14)	ISO/IEC 27013	38
15)	ISO/IEC 27014	39
16)	ISO/IEC TR 27015	39
17)	ISO/IEC TR 27016	40
18)	ISO/IEC TR 27019	40
19)	ISO/IEC 27031	41
20)	ISO/IEC 27032	41
21)	ISO/IEC 27033	41
22)	ISO/IEC 27034	42
23)	ISO/IEC 27035	43
24)	ISO/IEC 27036	43
25)	ISO/IEC 27037	43
26)	ISO/IEC 27038	44
27)	ISO 27799	44
28)	Synthesis	46
III.	ISO/IEC 15408 series, “Common Criteria”	50
1)	Introduction	50
2)	History	50
3)	Certification	52
4)	Issues & Criticisms	60
5)	Synthesis	61
IV.	Strategy of the Ministry of the Economy in the area of information security ...	62
1)	From an activity and competence point of view	62
2)	A model for information security governance	62
3)	The target group	63
4)	Structures of the Ministry of the Economy	63

CHAPTER 3: Technical tools for digital trust..... 75

I. Introduction.....	75
II. Cryptographic tools.....	76
1) Symmetric and asymmetric encryption	77
2) Common Uses of Encryption.....	80
3) Synthesis	84
III. Identity and Access Management.....	85
1) Business rationale	87
2) From RBAC to ABAC	88
3) Synthesis	88
IV. Mobile device management.....	89
1) Mobility	89
2) Reduce security risk across the mobile enterprise	90
3) Guidelines for securing and managing Mobile Devices	91
4) Mobile Device Management (MDM)	92
5) Synthesis	94

CHAPTER 4: Digital trust through the knowledge of standardization and certification..... 97

I. ICT international standards and their development through standardization .	97
1) Introduction to standards and standardization	97
2) ICT standardization and the ISO/IEC JTC1 committee	101
3) Initiatives and tools in Luxembourg.....	108
4) Conclusion.....	114
II. Certification and accreditation	115
1) Introduction to certification.....	115
2) The trust chain of accreditation and certification	118
3) OLAS: the accreditation body of Luxembourg	122
4) Conclusion.....	126
III. European regulation on electronic identification and trust services	127
1) Status of "Qualified Trust Service Providers"	127
2) Supervision scheme	127

3)	Examples of trust services.....	129
4)	Trust Service Provider in Luxembourg	129
IV.	The national law on electronic archiving.....	130
1)	Status of "PSDC"	130
2)	Technical regulation requirements and controls for certifying PSDCs	130
3)	Supervision scheme	131
	General Conclusion	135

Foreword

The *Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services* (ILNAS) is an administration under the supervision of the Luxembourg Minister of the Economy. It was created based on the amended 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. ILNAS thus corresponds to a network of skills for competitiveness and consumer protection.

As an innovative initiative for digital economy, a Digital trust department has been established within ILNAS in 2008, specifically in order to pursue excellence in Information and Communication Technology (ICT) by achieving quality and security. Nowadays, this Digital trust department has three legal attributions:

- To promote instruments to ensure the competency of Digitisation or Archiving Service Providers (PSDCs) and Qualified Trust Service Providers regarding the quality and security of provided services;
- To apply new patterns of supervision, certification, notification or accreditation of Digitisation or Archiving Service Providers (PSDCs) and Qualified Trust Service Providers defined in national and European legislation;
- To establish, maintain and publish on the web site set up for this purpose by ILNAS, the national trusted list within the meaning of the amended Commission decision 2009/767/EC of October, 16th 2009 as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

Strictly in this legal frame, the Digital trust department manages the follow-up and promotion of the instruments of digital trust. Related, this department guarantees the constant development of an internal project dedicated to the quality system for the supervision of the Qualified Trust Service Providers (QTSPs) and of the Digitisation or Archiving Service Providers (PSDCs).

Currently, ILNAS stresses the importance, at the national level, of an information and exchange network for ICT standardization knowledge, by assuring the chair of the national ICT standardization technical committee ISO/IEC JTC1. This development aims to achieve excellence in the ICT sector and beside to support the national (digital) economy in order to remain competitive and effective. Formally the implementation of the national ISO/IEC JTC1 activity is performed directly by the economic interest grouping GIE ANEC (Standardization department).

Under the Digital trust department development, and with the huge growth of information technology, its specifications, requirements and references (like related standards), ILNAS has decided to update the previous version of the white paper according to the last changes in these fields:

- Recent developments in research for digital trust;
- New tools in the field of digital trust;
- The current normative knowledge-based Economy in order to establish the links between standards, digital trust, innovation and competitiveness;
- The standardization activities currently in progress in Luxembourg, mainly related to the ICT field, for delegates involved in technical committees and for standards users.

Jean-Marie REIFF, Director
Jean-Philippe HUMBERT, Deputy Director
ILNAS

Abbreviations

AES	Advanced Encryption Standard
AFNOR	<i>Association Française de Normalisation</i>
ANEC GIE	<i>Agence pour la Normalisation et l'Economie de la Connaissance (Groupement d'Intérêt Economique)</i>
ANSI	American National Standards Institute
API	Application Programming Interface
APLAC	Asia Pacific Laboratory Accreditation Cooperation
APT	Advanced Persistent Threats
BIOS	Basic Input Output System
BS	British Standard
BSI	British Standards Institution
BYOD	Bring Your Own Device
CA	Certification Authority
CAB	Conformity Assessment Body
CASCO	Committee for Conformity Assessment
CASES	Cyberworld Awareness and Security Enhancement Structure
CC	Common Criteria
CC	Certification Committee
CCTV	Closed-Circuit TeleVision
CD	Committee Draft
CD-ROM	Compact Disc - Read Only Memory
CE	<i>Conformité Européenne</i> (European Conformity)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CIRCL	Computer Incident Response Center Luxembourg
CNPD	<i>Commission Nationale pour la Protection des Données</i>
CRP	<i>Centre de Recherche Public</i> (Public Research Center)
CSSF	<i>Commission de Surveillance du Secteur Financier</i>
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAPS	Distributed Application Platforms and Services
DDoS	Distributed Denial-of-Service
DES	Data Encryption Standard
DIN	<i>Deutsches Institut für Normung e. V.</i>
DIS	Draft International Standard
DNS	Domain Name System
EA	European co-operation for Accreditation
EAL	Evaluation Assurance Level
EC	European Commission
EETS	European Electronic Toll Services

EFTA	European Free Trade Association
eID	Electronic Identification
ENISA	European Network and Information Security Agency
eTS	Electronic Trust Services
ETSI	European Telecommunications Standards Institute
EU	European Union
FDE	Full Disk Encryption
FDIS	Final Draft International Standard
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GNP	Gross National Product
GSM	Global System for Mobile Communication
HHC	Horizontal Harmonization Committee
HTTP	HyperText Transfer Protocol
IAAC	Inter American Accreditation Cooperation
IaaS	Infrastructure as a Service
IAF	International Accreditation Forum
IAM	Identification and Access Management
IBE	Identity-Based Encryption
IC	Inspection Committee
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
ILAC	International Laboratory Accreditation Cooperation
ILNAS	<i>Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services</i>
IoT	Internet of Things
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITS	<i>Informationstekniska Standardisering</i> (page 99)
ITS	Intelligent Transport Systems
ITSEC	Information Technology Security Evaluation Criteria
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector
IWA	International Workshop Agreement
JTC	Joint Technical Committee
L2TP	Layer 2 Tunneling Protocol
LC	Laboratory Committee
LDAP	Lightweight Directory Access Protocol

LoTL	List of Trusted Lists
LTE	Long Term Evolution (4G LTE)
LuSI	Luxembourg Safer Internet
MAC	Message Authentication Code (page 80)
MAC	Multilateral Agreement Council (page 125)
MD2	Message-Digest 2
MD5	Message-Digest 5
MDM	Mobile Device Management
MLA	Multilateral Agreements
MRA	Mutual Recognition Arrangements
MRB	Master Boot Record
MSP	European Multi-Stakeholder Platform on ICT standardization
NAB	National Accreditation Body
NBN	<i>Bureau de normalisation</i> (Belgium)
NF	<i>Norme Française</i> (French Standard)
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NP	New Proposal
NSB	National Standards Body
NWIP	New Work Item Proposal
OASIS	Organization for the Advancement of Structured Information Standards
ODR	Online Disruption Resolution
OLAS	<i>Office Luxembourgeois d'Accréditation et de Surveillance</i>
O-member	Observing-member
OS	Operating System
OSS	Open Source Software
PaaS	Platform as a Service
PAC	Pacific Accreditation Cooperation
PAS	Publicly Available Specification
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
PED	Personal Electronic Device
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
P-member	Participating-member
PP	Protection Profile
PPTP	Point-to-Point Tunneling Protocol
PSDC	<i>Prestataire de Services de Dématérialisation ou de Conservation</i> (Digitisation or Archiving Service Provider)
PSF	<i>Professionnels du Secteur Financier</i> (Professionals of the Financial Sector)
QTSP	Qualified Trust Service Provider
RBAC	Role-Based Access Control
RFID	Radio Frequency Identification

RTP	Real-time Transport Protocol
SaaS	Software as a Service
SADC	South African Development Cooperation in Accreditation Committee
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirements
SC	Subcommittee
SCADA	Supervisory Control And Data Acquisition
SCIM	System for Cross-domain Identity Management
SDO	Standards Development Organization
SEK	<i>Svensk Elstandard</i>
SFR	Security Functional Requirements
SHA-1	Secure Hash Algorithm -1
SHA-2	Secure Hash Algorithm -2
SIP	Session Initiation Protocol
SIS	Swedish Standards Institute
SLA	Service Level Agreement
SME	Small-to-Medium Enterprise
Smile GIE	<i>Security Made In Lëtzebuerg (Groupement d'Intérêt Economique)</i>
SMTP	Simple Mail Transfer Protocol
SNJ	<i>Service National de la Jeunesse</i>
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Security Target
SVG	Scalable Vector Graphics
SWG	Special Working Group
TaaS	Trust as a Service
TC	Technical Committee
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TOE	Targets Of Evaluation
TR	Technical Report
TS	Technical Specification
UDP	User Datagram Protocol
UMDP	Universal Mobile Telecommunications System
UN	United Nations
USB	Universal Serial Bus
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WD	Working Draft
WG	Working Group
XaaS	Anything as a Service
XACML	eXtensible Access Control Markup Language
XBRL	eXtensible Business Reporting Language

XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol

This white paper presents an overview of the essential knowledge to understand why the concept of digital trust is so significant. Today, Information and Communication Technology (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. And finally how can we address this economy in its development without a consistent 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 considered as an emerging topic, with very few analyses already published, although it is a very active domain. Indeed, for example, in the digital agenda for Europe¹, trust and security are key topics. Many projects and events are organized in this frame by the European Commission, and a lot of initiatives have been developed in order to promote and foster different concepts in connection with the notion of digital trust. Concretely, on June, 4th 2012, the European Commission proposed a draft regulation on electronic identification and trust services for electronic transactions in the internal market. This regulation has been formally endorsed by the European Parliament in the April 2014 plenary session and by the Council of Ministers in June 2014. It will come into force in autumn 2014 and will be henceforth directly applicable across the EU from that date. The economic effect will be immediate, overcoming problems of fragmented national legal regimes and cutting red tape and unnecessary costs.

In the same way, it is important to mention the fact that standardization is a real force multiplier for ICT innovation, and that is really what ISO/IEC JTC1 permits to bring at the international level. This potential should not be underestimated and that is the reason why ILNAS has taken the national chair of that international standardization committee: "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"².

The main purpose of this white paper is to investigate and develop the knowledge areas of digital trust. The topics developed here are thus the concept of digital trust and the tools and techniques allowing to improve digital trust in Luxembourg. The white paper consists of four chapters. Chapter 1 and chapter 3 are based on research results. Chapter 2 and chapter 4 correspond principally to statements provided by national public authorities.

The first chapter is dedicated to the concept of digital trust. The rapid development of commerce through the Internet has resulted in an increased interest in trust in digital environments. An introduction to this concept is provided based on a multi-disciplinary state-of-the-art. An analysis of digital trust is performed through the study of the scientific literature. The theory is presented and associated models of digital trust are then defined. A number of recent developments including Big Data, online transactions, reputation systems and Cloud Computing are tackled from the digital trust point of view. Finally, the chapter concludes with the related challenges.

The second chapter deals with information security, which is a cornerstone for digital trust. Two series of international standards related to information security management and security of computer products are described. Such series set benchmarks to help ensure that an adequate level

¹ *The Digital Agenda is the EU's strategy to help digital technologies, including the internet, to deliver sustainable economic growth* (<http://ec.europa.eu/digital-agenda/>).

² http://www.iso.org/iso/fr/pressrelease.htm?refid=Ref1505&utm_source=ISO&utm_medium=RSS&utm_campaign=News

of security is met and that resources are used efficiently and effectively. The first one concerns the family of information security management systems (ISMS) standards (ISO/IEC 27000 series). These provide good practice recommendations on ISMS. The series is broad in scope and is applicable to organizations of all types and sizes such as commercial enterprises, government agencies and non-governmental organizations. By far the most popular standards are ISO/IEC 27001 and 27002, and certification against ISO/IEC 27001 provides a number of business benefits, including aspects related to digital trust. The second series concerns the “Common Criteria” (ISO/IEC 15408 series). ISO/IEC 15408 contains three parts and is a referential for security evaluation of computer products. It defines a common set of terms and procedures that must be followed by customers, product developers as well as security evaluation authorities to allow certification of security functions of computer products. Subsequently the strategy of the Luxembourg Ministry of the Economy in the field of information security is presented. This strategy currently lies on three structures: BEE-SECURE, CASES and CIRCL, that are all described in the chapter.

The third chapter of the white paper presents technical tools for digital trust. Three security techniques and related technologies, that are currently relevant for Luxembourg, are developed: Cryptographic tools, Identity and Access Management (IAM), and Mobile Device Management (MDM). To protect information, cryptographic tools are used for both data at rest and in transit. Then Identity and Access Management ensures that only authorized entities can access such information. Lastly, Mobile Device Management is a tool that helps in a secure way of dealing with the growing number of mobile devices that customers use for both business and personal use.

Finally, the fourth chapter considers digital trust through the knowledge of standardization and certification. An introduction to ICT international standards is proposed and the standardization process is explained. The second section is about certification and accreditation, defining together a trust scheme. The third section presents the European regulation on electronic identification and trust services, and describes the supervision scheme for qualified trust service providers. Then, the fourth section explains the national supervision scheme of Digitisation or Archiving Service Providers in order to get the “PSDC” status.

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

In this chapter digital trust is studied through its various characteristics and measures that companies use to build and maintain trust. Firstly the concepts of trust and digital trust are described, as part of the fundamentals in human society. Secondly, after an overview of the European regulation related to digital trust, a number of recent developments in this field are investigated, which include Big Data, a framework of trust in online transactions, how to secure reputation systems and trust mechanisms for Cloud Computing.

I. The concept of trust

Trust is one of the fundamental constructs to any interaction in our society [1.1] [1.2] and relates to the presumption about the dependability of, reliability of, and/or confidence in a person, process, system or other entity. In this frame, it requires an interaction between an actor (*trustor*) and another entity to be trusted (*trustee*). The trustor is the entity that holds belief, confidence, dependence, expectation, faith, hope or reliance on the competence, goodwill (including intention or motivation), integrity, kindness, strength, and reliability of another entity which is the object of trust, the trustee.

A classical sociologists' point of view relates to a state involving a confident positive expectation about another's motives in situations that are uncertain and entail risk with respect to oneself [1.3]. The structure of trust-based interaction often involves multiple actors in mutual and enduring relations and is thus difficult to investigate. Furthermore, the complexity with the construct "trust" is that it is multifaceted and, therefore, it is investigated in many scientific disciplines, such as economics, information systems and psychology. Consequently, little consensus has been reached about its definition and characteristics [1.4] [1.5] [1.6].

In many studies trust is usually narrowly scoped [1.7] such as social structures, choice in economics or risk management. According to Wang and Emurian [1.8], researchers disagree on basic definitions and argue that 'trust is often conceptualised by researchers according to the features of a particular context'. In addition, trust is subjective as the level of trust considered sufficient, differs per individual situation. Trust shifts and is valid only at a certain moment in time and it depends on how the actions of the trustor are affected by the trustee's actions and *vice versa*. Furthermore, trust could be affected by actions that we cannot monitor digitally. If complete knowledge in all situations would be possible, then trust is no longer an issue.

Nevertheless trust comprises three fundamental elements that relate to expectations, beliefs and the risk appetite of trustor and trustee. Huang and Nicol [1.9] describe it as follows: 1) expectancy – the trustor anticipates a specific behaviour from the trustee; 2) belief – the trustor has confidence that the expected behaviour occurs, based on the evidence of the trustee's competence, goodwill and integrity; 3) willingness to take risk – the trustor is prepared to take a risk for that belief. The behaviour of the trustee is of course beyond the control of the trustor. The trustor's belief in the trustee's expected behaviour is based on the trustee's competence, goodwill and integrity. The trustee's integrity gives the trustor confidence in the predictability of the trustee's behaviour.

What are the main properties of trust, how can it be categorised and in what manner is trust influenced? In this whitepaper the definition of Mayer et al [1.10] has been adopted: “*the willingness of a party [trustor] to be vulnerable to the actions of another party [trustee] based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party*”.

Li et al. [1.11] discuss the main *properties* of trust, as identified by earlier research. Trust involves at least two parties, that often are in an uneven relationship and usually varies over time. It has the following properties: it is asymmetric, it is bi-directional and it is context dependent. Furthermore trust is dynamic as it varies over time, it is non-transitive and inherently subjective. This basically shows the complex nature of trust, which is described in more details in Table 1.

Trust property	Description
Asymmetry	Trust of party A in party B does not imply trust of party B in party A.
Bi-directionality	Trust exists for parties A and B in an interaction for one or more specifications or services, such as delivery of products.
Context-dependence	Trust of party A in party B is inextricably tied to a specific context, representing the specific action or service performed and the safeguards which are present.
Dynamism	Trust varies over time since factors that influence trust change.
Non-transitivity	Trust of party A in party B and trust of party B in party C, does not necessarily imply the trust of party A in party C.
Subjectivity	Trust in other parties is established and maintained by different parties in diverse manners.

Table 1: The main properties of trust [1.11]

Li et al. [1.11] also show that trust can be classified into three *categories*:

- Interpersonal trust, which is the trust that one agent has in another agent. It is based on specific characteristics of the agents involved, such as integrity, competence and benevolence. This category of trust is agent and context specific;
- System trust, or Impersonal trust, which is based on the perceived reliability of a system or institution and is primarily derived from structural assurances (regulations and laws) such as the monetary system;
- Dispositional trust, also referred to as ‘basic trust’, which describes the general trusting attitude of the trustor. It relates to the aptitude to trust and dealing with risks and uncertainties and is independent of any party or context.

Furthermore, Yan and Holtmanns [1.5] have identified both objective and subjective *influencing factors* regarding the decision to trust that are:

- Related to trustor’s objective properties: assessment; a given set of standards; trustor’s standards;
- Related to trustor’s subjective properties: confidence; expectations or expectancy;
- Related to trustee’s objective properties: competence; ability; security; dependability; integrity; predictability; reliability; timeliness; observed behaviour; strength;
- Related to trustee’s subjective properties: honesty; benevolence; goodness; probability; willingness; belief; disposition; attitude; feeling; intention; faith; hope; trustor’s dependence and reliance;
- Related to the context: situations entailing risk; structural; risk; domain of action.

Hoffmann et al. [1.12] argue that research in trust indicates that it is hard to address trust itself. They suggest that it may be easier to use so-called trust *antecedents* instead. Trust antecedents are factors or elements that lead to and/or increase trust (such as knowledge of a person, a contract or sharing of information). These antecedents are often referred interchangeably as underlying dimensions, determinants, attributes, basics or principles of trust [1.8]. Trust antecedents express what is perceived by the trustor, so influencing the user (i.e. trustor) perception is key. “A technical improvement of a system, e.g., using a better encryption algorithm, will have absolutely no effect if this improvement is not communicated to the users in a way allowing them to understand the benefits for themselves” [1.12].

In previous studies many trust antecedents have been identified. These antecedents can be grouped into six broad categories [1.11]:

- Identification-based trust antecedents: trust that is guarded by identification with others’ desires, intentions and empathy;
- Knowledge-based trust antecedents: trust that ‘is grounded in the other’s predictability and relies on information rather than deterrence’;
- Calculative trust antecedents: trust that is based on economic calculations that balance potential costs against the benefits of co-operation;
- Institutional trust antecedents: trust that refers to one’s sense of security from guarantees, safety nets, or other impersonal structures inherent in a specific context;
- Cognition-based trust antecedents: trust that stems from individual, rapid, cognitive cues or first impressions and it is context-dependent;
- Dispositional trust antecedents: trust that stems from individual propensity to trust, described as ‘the general willingness to trust others’.

Instead of trust categories, these different trust antecedents are not mutually exclusive. These antecedents will be used in a framework of digital trust in online transactions (see Chapter 1 – Section IV - 2).

The classical social trust concept has been stretched into to a concept that includes digital processing, as depicted by Giustiniano and Bolici [1.6] who position trust in two different classes: 1) social trust and 2) technological trust (see Figure 1).

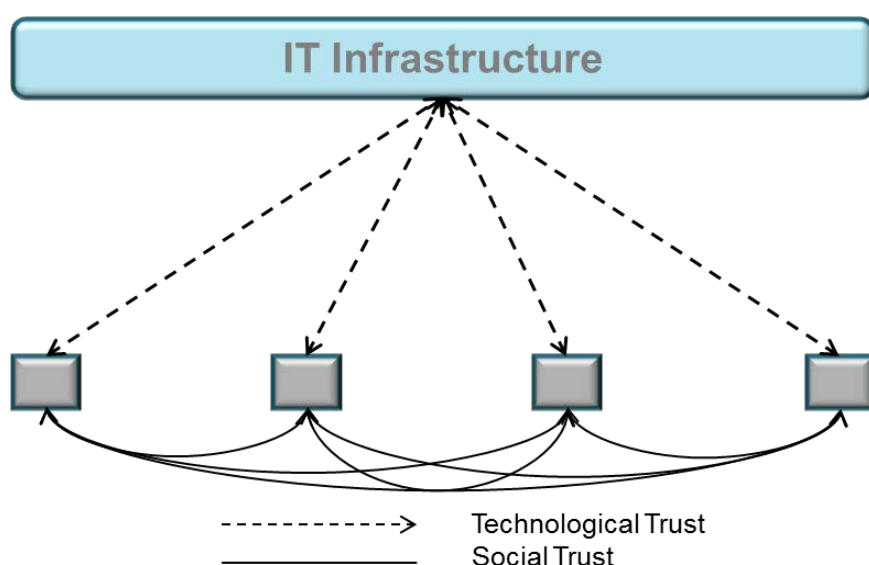


Figure 1: Trust in the digital information age [1.6]

II. Digital Trust

Trust in the digital information age, called **digital trust** (or e-trust, or online trust) indicates a *“positive and verifiable belief about the perceived reliability of a digital information source, leading to an intention to use”* [1.13]. Of course the scope of this definition can be further stretched to include e.g. service providers on the Internet that deliver digital information. There is increasing evidence that trust is a precursor to ongoing commitment in doing business using the Internet. The steady development of commerce through the Internet, after the dot-com bubble in the early 21st century, has resulted in an increased interest in trust in digital environments which is reflected in similar research [1.11]. This kind of research is mainly focussed on trust in online transactions. It considers the role of trust, and its relationship with other constructs, such as risk, user confidence and user satisfaction.

Building and maintaining digital trust involves more aspects than in a world without electronic communications, because digital communications rely not only on human beings and their relationships, but also on computer components. The Internet is used for, among others, online transactions, applications for governmental documents, entertainment and building personal relationships, consequently the estimation of trustworthiness of information, goods and services of enterprises, and users in online systems becomes more and more important. Due to the anonymity of the Internet there is always a risk concerned in such interactions as users are faced with the dilemma as to which information to trust or distrust and accept or discard. The main reason of this uncertainty risk is caused by an information asymmetry as one party has information that the other party does not have [1.14]. For example, will a web shop deliver a product on time and has that product the quality as described? Information can be easily manipulated and faked identities can be created.

Wang and Emurian [1.8] discuss the characteristics of digital trust that share similar characteristics to those of “traditional” trust. However, there are some important distinctions that are specific to online environments. The *characteristics* of digital trust can be described according to these authors as follows:

1. As in traditional trust the trustor and trustee are fundamental in establishing and maintaining a trust relationship, but with digital trust they involve specific entities. In digital trust, the trustor is for instance a consumer who is browsing a web site on the Internet, and the trustee is a governance organisation or merchant that the website represents.
2. Because of the anonymity of doing business using the Internet trustees may behave in an unpredictable manner. Consumers are, therefore, often uncertain about the risks and its consequences when passing information or executing online transactions. Therefore, consumers are typically more vulnerable to specific trust violations such as privacy violations or loss of money.
3. When customers visit websites, leave personal information or purchase goods and services online on websites, the associated data can be exploited by trustees for e.g. potential future sales. Consumers must be aware of this situation and they should consider whether they have more to gain than to lose when they engage in such activities.
4. Digital trust is inherently a subjective matter because the level of trust considered sufficient for a customer activity on the Internet is different for each individual and depended on situational factors.

Jøsang et al. [1.15] list five digital trust *classes* (based on Grandison and Sloman's [1.16]) that play a role when a trustor is active in an online environment (Table 2).

Digital trust classes	Description
Provision trust	Describes the trust in a service or resource provider when the trustor seeks protection from malicious or unreliable service providers.
Access trust	Describes trust in principals for the purpose of accessing resources owned by or under the responsibility of the trustor.
Delegation trust	Describes trust in an agent (the delegate) that acts and makes decision on behalf of the trustor.
Identity trust	Describes the belief that a trustee's identity is as claimed. Trust systems that derive identity trust are typically authentication schemes such as X.509 / PKI, PGP, and IBE ³ .
Context trust	Describes the extent to which the trustor believes that the necessary computer systems and institutions (e.g. legal systems, law enforcement) are in place to support an online activity and to provide a safety net in case something should go wrong.

Table 2: Digital trust classes [1.15]

Because of the importance to attract and keep on-line customers, companies use various measures in their websites. The most common ones to build and maintain digital trust are listed in Table 3.

Measures	Description
Third party certificates	Attestation of attributes of seller from third party.
Reputation systems	Aggregated feedback based on opinions of buyers.
Tips and recommendations	Advice, suggestions, and guidance to increase knowledge of buyers.
Dispute services	Services provided by commercial organisations to facilitate disputes between partners.
Privacy policy	Policy on providing sensitive personal data.
Security policy	Policy on exchanging information, payments.
Web site design	Graphical design, overall structure due to navigation, presentation of sellers, products.
Communication with buyers	Communication through mail, telephone, and online forms.
Payment services	Payment administration and escrow services.
Returns policy	Money-back guarantees.
Insurances	Transference of risk to third party.
Transference	Affiliations with trustful online providers, brands, trademarks, logos.

Table 3: Common measures by websites for building and maintaining trust [1.11]

³ X.509 is an ITU-T standard for a Public Key Infrastructure (PKI) and Privilege Management Infrastructure; PGP (Pretty Good Privacy) is software to encrypt and decrypt data; IBE (Identity-Based Encryption) is a type of PKI

III. New regulation

The European commissioner for Digital Agenda (Neelie Kroes) states on the value of Internet that *"people and businesses should be able to transact within a borderless Digital Single Market"*. Therefore, the Digital Agenda for Europe (<http://ec.europa.eu/digital-agenda>) currently focuses on electronic identification (eID) and electronic trust services (eTS), which are inseparable elements to ensure legal certainty, trust and security in electronic transactions. The directive on a community framework for electronic signature [1.17] recognised the validity of electronic signatures. This directive established the basic legal framework at European level for electronic signatures and certification services.

Note: the proposal for a "Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market" [1.18], was published in June 2012. This regulation comes into force at autumn 2014 and is directly applicable cross the EU from that date (it abrogates the EU Directive 1999/93/EC on a Community framework for electronic signatures) (see also Chapter 4 - Section III) for more details about the national context).

Electronic identification (eID) is an important enabler of data protection and the prevention of online fraud in electronic transactions. It ensures secure access to online services since it guarantees unambiguous identification of persons and makes it possible to get the service delivered to the entitled persons. Unfortunately there is insufficient cross-border interoperability of national eIDs because of a lack of common legal basis between Member States of the EU. Recognition and acceptance of the various eIDs issued by the various Member States prevents from benefiting fully from the digital single market.

For safe electronic commerce of public services to businesses and citizens, a reliable system of electronic trust services (eTS) that work across EU countries is vital. Such digital services consist of digital signatures, electronic seals, digital time stamps, electronic delivery and authentication of electronic documents and websites:

- Digital signatures - authentication of electronic signatures;
- Electronic seal - electronic equivalent applied on documents to guarantee origin and integrity;
- Time stamping - proves that electronic document existed at a point-in-time and that it has not changed since then;
- Electronic delivery - electronic equivalent of registered mail in the physical world;
- Legal admissibility - ensures authenticity and integrity of electronic documents;
- Website authentication - allows users to verify the authenticity of websites.

By means of legal validity of these digital trust services, businesses and citizens in the internal market will be using digital interactions in a natural way.

IV. Recent developments

This section describes a number of recent developments concerning digital trust. Firstly “Big Data” and some challenges related to digital trust are explored. The worldwide increase in online transactions and social media is one of the reasons why Big Data becomes an important topic for both businesses and governments. Then, in this context, online transactions need to be carried out securely and a framework of trust in online transactions is presented. Furthermore, ways to secure online reputation systems, that play an important role in the context of social media, is exposed as well. Finally, the processing of Big Data relies heavily on “Cloud Computing”. As such systems require (information) security technologies to ensure that digital trust is maintained, a number of trust mechanisms for Cloud Computing are also presented.

1) Big Data

In the last decade, the amount of data that flows through the Internet has exponentially increased because of online transactions, social media activities including multimedia usage, and all kinds of devices (smartphones, automobiles, etc.) that generate data. This development in our (information) society has led to the term “Big Data”.

One of the most commonly used criteria for Big Data has been defined by Laney [1.19], who identified three dimensions, the “3V model”:

- Volume: the amount of data; more data crosses the internet every second than were stored in the entire Internet 20 years ago [1.20];
- Velocity: the speed of incoming data and how quickly it can be made available for analysis (e.g. payment data from credit cards and location data from mobile phones);
- Variety: the different types of structured and unstructured data that an organization can collect, such as transaction-level data, text and log files and audio or video.

In those days Laney did not use the term ‘Big Data’, but he predicted that data management in e-commerce would get more and more important and difficult. More recently others (e.g. Zikopoulos et al. [1.21]) added a 4th V:

- Veracity: the trust into the data which might be impaired by the data being uncertain or imprecise.

A real challenge is so called ‘data provenance’. Big Data allows expanding the data sources for processing but it is very hard to be certain that each data source meets the trustworthiness that would be required for analysis algorithms to produce accurate results. Therefore, the authenticity and integrity (correctness and completeness) of such data needs to be considered. Given the variety of data it is quite likely, that there will remain some incorrectness and incompleteness in the data, even after data cleaning and error corrections. However, uncertain data can still be analysed but results must be presented with some probability or trust value.

Furthermore, the privacy of data is also a huge concern, and this increases in the context of Big Data. What data is stored by retailers, by location-based services and by social media websites? What data is kept private, what data is re-sold and how can customers get fine-grained control over data sharing, etc.? Inappropriate use of personal data, particularly through linking of data from multiple sources is becoming a real issue. Several kinds of surprisingly private information like health issues

and type of religion can be revealed by just observing anonymous users' movement and usage patterns over time [1.22].

Although a new single EU law (the General Data Protection Regulation, GDPR⁴) is planned to take effect in 2016 after a transition period of 2 years, there is still a lot of work to be done to better ensure digital trust in relation to Big Data.

2) A framework of trust in online transactions

Li et al. [1.11] propose a holistic framework of trust in online transactions that links the level of perceived trustworthiness by the actors, transactional attributes, context and the decision to participate or not in an online transaction (Figure 2). They suggest to use the trust antecedents that have been described in Chapter 1 - Section I: identification-based, knowledge-based, calculative, institutional, cognition-based and dispositional trust.

Key attributes of an online transaction include its value, volume, frequency and transaction costs. The elements of the transactional context include opinions of buyers and policies on privacy and money-back guarantees (see Table 3). Buyers and sellers will independently assess the transaction attributes through different combinations of the trust antecedents based on a given context.

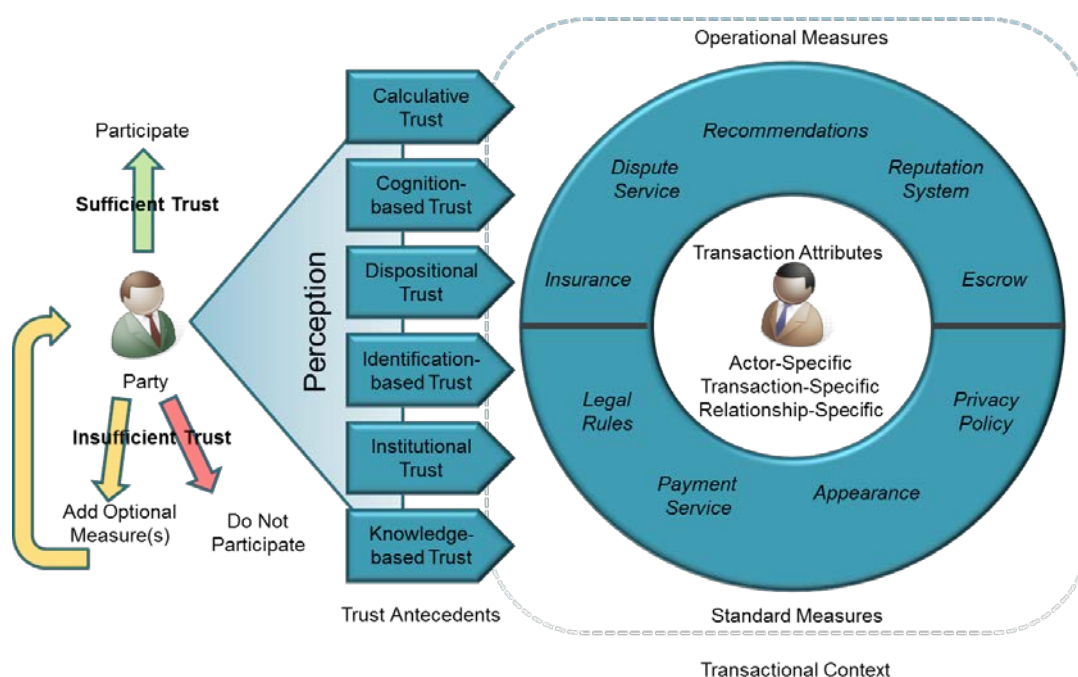


Figure 2: A holistic framework of trust in online transactions [1.11]

The framework identifies possible barriers and solutions to build and maintain digital trust in online transactions, and identifies options for the development of information systems that are required to implement such commercial online platforms.

⁴ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011&qid=1397830334102>

3) Reputation systems

As mentioned in Chapter 1 - Section II, buyers are exposed to an uncertainty risk when buying products or services online, due to an information asymmetry as sellers have information that the buyers do not have. Will a seller at an online auction and shopping website ship the product on time? Does a product at a certain website have the quality as described? Is the advice from an “expert” at a consumer review site trustworthy?

Such questions can most of the time be answered only after the transaction has taken place. So how can the customers protect themselves by judging the quality of unknown sellers of unfamiliar products and services beforehand? This situation can partly be counteracted through the use of reputation systems, also referred to as online rating systems. This is basically the digital version of the word-of-mouth mechanism. Fan [1.23] discusses the rationale why customers comment on products and services of online systems:

- To help other customers who may benefit from it and who will, therefore, possibly also write comments themselves;
- A need of consumers to share positive or negative impressions about a product and/or service;
- A need of consumers to approve or criticise a product and/or service;
- To help or revenge the reputation of the company in question.

User comments reduce the uncertainty and risk due to the nature of the buying goods *via* the Internet. However, because reputation systems play an increasingly important role in mitigating risks of online interactions, attacks against such systems have evolved steadily as well.

Attacks on online reputation systems can be roughly classified into three categories, based on the malicious attackers’ capability and goals [1.24]: independent attacks, single-target attacks and, multiple-target attacks. In all these kind of attacks, dishonest ratings are inserted to mislead the reputation scores of single or more items (products, services, etc.) to either boost or downgrade the reputation score(s), see Table 4.

Types of attack	Attacker	Item	Explanation
Independent	Individual	Single	Simplest and least organised type of attack.
Single-target	Several persons	Single	Most widely known attack.
Multiple-target	Automated	Multiple	Entities that automatically rate on commercial basis.

Table 4: Attacks on online reputation systems [1.24]

Based on related work regarding attacks on online reputation system, Liu et al. [1.24] discuss a number of defence schemes times for independent and single-target attacks based on the evaluation of trust in raters:

- Procedural and cost hurdles in acquiring multiple user IDs (that may be used for such attacks);
- Statistic calculations on rating values, such as sudden changes in the rating distribution and correlations;
- Evaluation of the reliability of a given rating, based on various other mathematical methods such as fuzzy logic.

To address multiple-target attacks as well, Liu et al. [1.24] propose a new anomaly detection scheme for reputation systems that identifies malicious users and recovers reputation scores. It addresses both multiple-target and single-target attacks, and does not evaluate trust in raters. This defence scheme builds thresholds for detecting suspicious items, and identifies targets among suspicious items. Suspicious items whose rating distributions are highly likely to be abnormal are detected first. Subsequently, correlation analysis is carried out among these items to determine the ones with strong correlations as target items. The scheme integrates several techniques: time-domain change detection, system-level visualisation, heterogeneous threshold selection, and item correlation analysis. The authors demonstrate that it improves the detection rate and reduces the false alarm rate in the detection of malicious users compared to other techniques.

4) Trust mechanisms for Cloud Computing

Other important developments take place in the Cloud Computing business. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1.25]. NIST [1.26] identified a three tiered service model cloud stack [1.27], with increasing levels of service provisioning (Table 5), although others [1.28] refer to Cloud Computing provisioning as ‘anything as a service’ (XaaS).

Service model types	Capability description
Infrastructure as a Service (IaaS)	Trustor uses processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
Platform as a Service (PaaS)	Trustor deploys onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.
Software as a Service (SaaS)	Trustor uses the provider’s applications running on a cloud infrastructure.

Table 5: Cloud Computing service models [1.27]

Furthermore, NIST distinguishes four deployment models of Cloud Computing: private cloud, community cloud, public cloud and hybrid cloud:

- A private cloud is operated solely for an organisation, either managed by the organisation itself or a third party and can exist on premise or off premise;
- A community cloud is shared by several organisations and supports a specific community that has common interests either managed by (one of) the organisations or a third party and can exist on premise or off premise;
- A public cloud is provisioned for open use by the general public. It may be operated, managed, and owned by (a combination of) business, academic, or government organization(s) and exists on the premises of the cloud provider;
- A hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together to enable data and application portability.

Cloud Computing continues to gain popularity both with private and business users [1.27]. Cloud Computing without (digital) trust is very unlikely, especially when the computing services are delivered over a network that is open for public use (i.e. public cloud). Every potential user of cloud

services should ask the question whether to trust the providers and their service offerings. The distributed architecture of Cloud Computing is also a reason for lack of user trust in the cloud services [1.7]. Huang and Nicol [1.29] argue that current trust mechanisms for Cloud Computing are, by and large, based on the perceptions of reputations, and self-assessments by the cloud service providers. Examples are trust based on reputation and Service Level Agreement (SLA) verifications. Only in a small number of cases third party audits are in place.

In this paragraph a number of trust mechanisms in the cloud are discussed as identified by Huang and Nicol [1.29]. 'Reputation' based trust is founded on the combined opinion of a community of users towards a cloud service provider. It is only high level and can be used a selection of cloud service vendors. This opinion is partly based on the second type of trust mechanism: 'SLA verification' based trust. This reflects to what extent agreements on service provisioning have been met. A drawback of this mechanism is that a number of difficult to measure agreements can probably not assessed effectively, such as checks on compliance with data protection policies. Another trust mechanism type is 'Cloud transparency' based trust which covers elements of transparency, such as configuration settings, incident, problem and change logs, audit trails, and vulnerability statistics. A fourth trust mechanism is called Trust as a Service (TaaS) in which tasks of cloud trust management have been delegated to third-parties. But also for such third parties trust needs to be established. A fifth type of trust mechanism is based on formal accreditation, audit, and standards. However, a formal assessment method by certified companies of cloud service vendors and its services is still under discussion and does not exist yet.

Trust mechanism	Description
Reputation	Constitutes the aggregated opinion of a community
SLA verification	Examination of agreements on service provisioning
Cloud transparency	Clarity on how cloud service providers operate
Trust as a Service	Third-party delegation of cloud trust management
Accreditation, audit, and standards	Formal assessment by certified third parties

Table 6: Existing trust mechanisms in the cloud [1.29]

These existing cloud trust mechanisms (Table 6) only contribute to a partial view of digital trust in the cloud. To establish a reliable trust context for cloud services and the data within the cloud, Huang and Nicol [1.29] suggest a number of trust mechanisms for Cloud Computing, that integrate evidence, validation and certification to reveal chains of trust in the cloud. They build their framework on *policy-based* trust mechanisms such as used in PKI and *evidence-based* trust mechanisms related to the trustee's attributes.

Policy-based trust mechanisms rely on certificated trust policies for Cloud Computing, but do not exist in the cloud yet. Evidence-based trust mechanisms relate to the trustor's expectation and the source of trust (what makes the trustor trust the trustee). The trustor's expectation includes performance, security, and privacy of cloud services. The source of trust includes the trustee's competency and capability, integrity (consistency in performance and principles) and goodwill (motivation or intention). This can be determined using various sources of cloud service attribute assessments.

The following five cloud entities and their sources of evidence are proposed by Huang and Nicol [1.29] as part of their framework for chains of trust in Cloud Computing: 1) Cloud user observation; 2) Opinions of other peer users; 3) Statements from cloud service providers; 4) Assessment by cloud

auditors; 5) Observation of cloud brokers (an entity that negotiates relationships between cloud providers (trustees) and cloud consumers (trustors) concerning cloud service delivery):

1. Experience of users of cloud services provides valuable first-hand information. Downsides of this source are that the range of usage of the cloud service is limited and samples sizes are low.
2. Opinions of peer users, e.g. from reputation systems, provide second-hand information. Downsides of this source are whether this information can be trusted, as this information could be biased or even manipulated.
3. Statements from cloud service providers about their service offerings and its attributes should typically be commercially understood. However, these can be put on a list of cloud service monitoring and can subsequently be used to check whether trust in that service provider is warranted.
4. A formal assessment of cloud service providers by cloud auditors adds additional value to the source of trust in service providers. Independent assessments of cloud services are conducted which are related to implementation and operational criteria, such as policies and standards compliance, information security, performance and operations aspects of the service provisioning. A limitation is that the trust assessment reflects only the circumstances when the audit is carried out.
5. Observations of cloud brokers are an important source of cloud attribute assessments as these contain feedback from many peer users from different providers and allow real-time cloud service performance monitoring. However, the question can be raised whether to trust a cloud broker but the broker is expected to be formally audited as well.

When all trust based mechanisms are put together (reputation, SLA verification, cloud transparency, etc.) including by the authors suggested policy-based and evidence-based trust mechanisms, an overall framework emerges for modelling and analysing *chains of trust* among cloud entities (Figure 3).

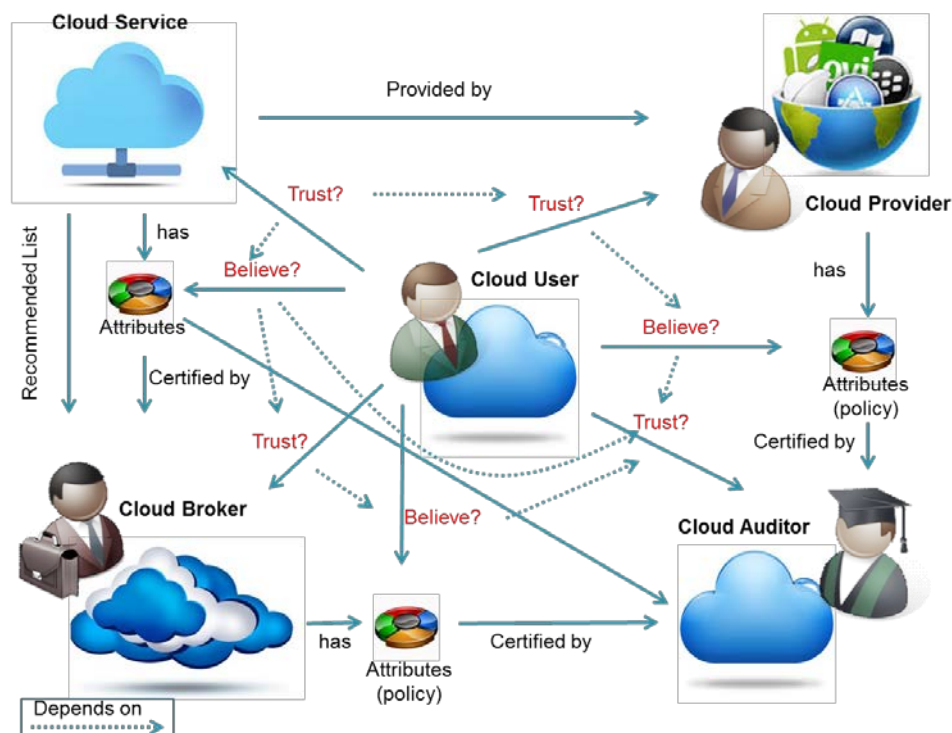


Figure 3: Chains of cloud trust relations [1.28]

Figure 3 provides an integrated view to illustrate the chains of trust relations from a cloud user to a cloud service and related cloud entities, using policy-based and attribute/evidence-based mechanisms. The arrows represent dependence relations between cloud entities (e.g. providers, brokers, auditors) and trust mechanisms (e.g. reputation, SLA, self-assessment, policy compliance) which are also the sources of evidence to support the trust judgements.

The authors have two recommendations to further professionalise cloud service provisioning that will be beneficial to users and vendors of cloud services. Firstly, to initiate a policy-based approach of trust relations, by which cloud trust is derived from official third party audits that prove the cloud entity and its services conform to trusted policies. Secondly, to develop an attribute based approach of trust relations, facilitated with standards, by which attributes of the cloud service provider and its provided services are used as evidence for trust judgements.

V. Conclusion

Trust is a fundamental and multifaceted construct in human society. The classical point of view from sociology relates to a positive expectation about another's motives in situations of uncertainty and risk. Because it is multifaceted trust is investigated in many scientific disciplines, explaining partially why a little consensus has been reached about its definition and characteristics. Trust is subjective as the level of trust considered sufficient differs per individual situation. However some basic ingredients can still be found: expectancy, belief and willingness to take risk. Research in trust indicates that it is hard to address trust itself and that it may be easier to make use of so-called trust antecedents. These are factors that impact trust and are often referred to as underlying dimensions, determinants, attributes, basics or principles of trust.

The rapid development in the last decade of commerce through the Internet has resulted in an increased interest in trust in digital environments, known as digital trust. To build and maintain digital trust, companies use various measures in their websites, such as, third party certificates, reputation systems and security and privacy policies. Also from a government perspective digital trust is high on the agenda to improve cross-border interoperability and currently focuses on achieving EU-wide electronic identifications and electronic trust services.

Recent developments regarding digital trust include a framework to build and maintain digital trust in online transactions that include its value, volume, frequency and transaction costs. Buyers and sellers can independently assess the transaction attributes through different combinations of the trust antecedents (such as perceived security controls or perceived trustworthiness of a participating party). Other developments concern anomaly detection schemes for reputation systems that identify malicious users and recovers reputation scores. Developments in this area are important, as such systems play an increasingly important role in mitigating risks of online interactions. As regards Big Data, its potential is widely being recognised and its application has major impacts, not only from an economic perspective but also for society as a whole. However, there is a major gap between its potential and its realisation, as technical challenges and policy issues must still be addressed (at least concerning privacy and digital trust).

Finally, for the increasingly popular Cloud Computing business model, important developments regarding digital trust mechanisms are being made. New frameworks are proposed that, for example, integrate evidence, validation and certification to reveal chains of trust in the cloud. To gain certifications, policy-based trust mechanisms derived from (national or international) standards are required. However, such standards do not exist yet but are currently under development by ISO/IEC JTC1⁵. Fortunately, there are a number of standards that already play an important role in further professionalising digital trust.

⁵ Work in progress by ISO/IEC JTC1 (Joint Technical Committee 1), Sub-committee 27 "IT Security techniques" and Sub-committee 38 "Distributed application platforms & services"

References

- [1.1] Walsham, G. (2001), "Knowledge management: the benefits and limitations of computer systems", *European Management Journal*, Vol. 19 No. 6, pp. 599-608.
- [1.2] Watson, R (2009), 'Constitutive practices and Garfinkel's notion of trust: revisited', *Journal of Classical Sociology*, 9(4), 475-499.
- [1.3] Boon, S. D., & Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. *Cooperation and prosocial behavior*, 190-211.
- [1.4] McKnight, D. H., & Chervany, N. L. (2000). What is Trust? A Conceptual Analysis and An Interdisciplinary Model. In *Proceedings of the 2000 Americas Conference on Information Systems (AMCI2000)*. AIS, Long Beach, CA (August 2000).
- [1.5] Yan, Z., Holtmanns, S. (2007), "Trust Modeling and Management: from Social Trust to Digital Trust", book chapter of *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, IGI Global.
- [1.6] Giustiniano, L., Bolici, F. (2012). Organizational trust in a networked world: Analysis of the interplay between social factors and Information and Communication Technology. *Journal of Information, Communication and Ethics in Society*, 10(3), 187-202.
- [1.7] Aslam, M. (2012). *Secure Service Provisioning in a Public Cloud* (Doctoral dissertation, Mälardalen University).
- [1.8] Wang, Y. D., Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, 21(1), 105-125.
- [1.9] Huang, J., Nicol, D. M. (2010). A Formal-Semantics-Based Calculus of Trust. *IEEE Internet Computing*, 14(5), 38-46.
- [1.10] Mayer, R.C., Davis, J.H., Schoorman, F.D., (1995) "An Integrative Model of Organizational Trust." *Academy of Management Review*, vol. 20(3), pp. 709-734.
- [1.11] Li, F., Pieńkowski, D., Van Moorsel, A., Smith, C. (2012). A holistic framework for trust in online transactions. *International Journal of Management Reviews*, 14(1), 85-103.
- [1.12] Hoffmann, A.; Söllner, M.; Hoffmann, H. Leimeister, J. M. (2012): *Towards Trust-Based Software Requirement Patterns*. In: *Second International Workshop on Requirements Patterns (RePa' 12)*, Chicago, Illinois, USA.
- [1.13] Rowley, J., & Johnson, F. (2013). Understanding trust formation in digital information sources: The case of Wikipedia. *Journal of Information Science*.
- [1.14] Tan Y. H., Thoen, W. (2011), "A logical model of trust in e-commerce" *Electronic Markets*, vol. 10, pp. 258-263.
- [1.15] Jøsang, A., Ismail, R., Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2), 618-644.
- [1.16] Grandison, T., Sloman, M. (2000). A survey of trust in internet applications. *IEEE Communication Surveys and Tutorials*, 3, pp. 2-16.
- [1.17] EU (1999), "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures", 1999. URL <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT>

- [1.18] EU (2012), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market", 2012. URL <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0238:EN:NOT>
- [1.19] Laney, D. (2001) "3D Data Management: Controlling Data Volume, Velocity and Variety", Technical report, META Group, Inc (now Gartner, Inc.), February 2001. URL <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>
- [1.20] McAfee, A., Brynjolfsson, E. (2012). Big data: the management revolution. Harvard Business Review, 90(10), 60-66.
- [1.21] Zikopoulos, P.C., deRoos D., Parasuraman K., Deutsch T., Corrigan, D., Giles, J. (2013), "Harness the Power of Big Data: the IBM Big Data Platform", McGraw Hill.
- [1.22] Agrawal, D., Bernstein, P., Bertino, E. et al. (2012), "Challenges and Opportunities with Big Data: A community white paper developed by leading researchers across the United States". Whitepaper, Computing Community Consortium, March 2012. URL <http://cra.org/ccc/docs/init/bigdatawhitepaper.pdf>
- [1.23] Fan, J. (2011), "Research on the external factors of consumers releasing online comments". In Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on (Vol. 7, pp. 3819-3823). IEEE.
- [1.24] Liu, Y., Sun, Y., Yu, T. (2011). Defending Multiple-user-multiple-target Attacks in Online Reputation Systems. In Privacy, security, risk and trust, IEEE third international conference on social computing, pp. 425-434, IEEE.
- [1.25] Hogan, M., Liu, F., Sokol, A., Tong, J. (2011), "Nist cloud computing standards roadmap", NIST Special Publication, 35.
- [1.26] Mell, P., Grance, T. (2011), "The NIST definition of cloud computing (draft)." NIST special publication 800.145: 7
- [1.27] Yang, H., Tate, M. (2012) "A Descriptive Literature Review and Classification of Cloud Computing Research", Communications of the Association for Information Systems, 31(1), 2.
- [1.28] Duan, Y. (2012), "Value Modeling and Calculation for Everything as a Service (XaaS) based on Reuse", In Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD), 2012 13th ACIS International Conference on (pp. 162-167). IEEE.
- [1.29] Huang, J., Nicol, D. M. (2013). Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2(9).

2 Digital trust through information security

This chapter deals with information security as a cornerstone for digital trust. Two series of international standards related to information security management and security of IT products are presented. Firstly the family of ISMS standards (ISO/IEC 27000 series) is explored and secondly, the standards defining the “Common Criteria” (ISO/IEC 15408 series) are described. Indeed, studies confirm that companies working with such standards demonstrate improvements in business performance including aspects related to digital trust. In this context, the final section of this chapter is dedicated to the strategy of the Luxembourg Ministry of the Economy in the field of information security which currently lies on three structures: BEE-SECURE, CASES and CIRCL.

I. Introduction

Information security plays an important role in digital trust. Standards for information security management and Information Technology (IT) security set benchmarks to help ensure that an adequate level of security is met and that resources are used efficiently and effectively. This chapter provides an overview of both the management as well as the technical perspective of information security. There are a lot of standards in these managerial and technical domains, and among the best known ones are respectively: ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 15408 series (also known as Common Criteria or CC).

The ISO/IEC 27000 series of information security standards and technical reports, with the designation *Information technology -- Security techniques -- Information security management systems*, provides good practice recommendations on information security management systems (ISMS). The series are broad in scope and are applicable to organisations of all types and sizes such as commercial enterprises, government agencies and non-governmental organisations. At present, twenty-five standards are published in these series and several more are under development. ISO/IEC 27001 offers the possibility of information security management certification.

The ISO/IEC 15408 series, with the designation *Information technology -- Security techniques -- Evaluation criteria for IT security*, consists of three standards for IT security evaluation for computer security certification. It provides assurance that specifying, implementing and evaluating IT security products have been carried out in a strict, repeatable and standard way at a level that is commensurate with its usage.

Both series are published jointly by the ‘International Organization for Standardization’ (ISO) and the ‘International Electrotechnical Commission’ (IEC). They are produced by ISO/IEC JTC1/SC27 (Joint Technical Committee 1/Sub-committee 27 “IT Security Techniques”). ISO/IEC JTC1/SC27 develops standards for the protection of information and IT and includes methods, techniques and guidelines related to security and privacy aspects. This international body meets twice a year and consists of five Working Groups (WG) that deal with the following subject areas:

- WG 1: Information security management systems (incl. ISO/IEC 27000 series);
- WG 2: Cryptography and security mechanisms;
- WG 3: Security evaluation, testing and specification (incl. ISO/IEC 15408 series);

- WG 4: Security controls and services;
- WG 5: Identity management and privacy technologies.

In the next two sections, an overview of these two series of standards is given, which can be used to improve the risk profiles of organisations and the technology which is being used, thereby contributing to improvements in digital trust.

II. ISO/IEC 27000 series

1) Information security and ISMS

Information is considered as an asset that has value for an organisation and requires appropriate protection. Information is available in both physical form (e.g. on paper) and digitally (e.g. databases on electronic media) and is transmitted in various ways, such as mail, email and verbal communications. Either at rest or in transit, information always needs appropriate protection to ensure its reliability and to prevent unauthorised access. The people, processes and technology that create, process, store, transmit and delete information must do so according to the information security requirements of the organisation. The objective of information security is: *“protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity and availability”* [2.1].

Protecting information assets through defining, implementing, maintaining, and improving information security is crucial to achieve the objectives of organisations and to maintain and enhance its image and legal compliance. In addition, correct, complete and timely information to those with an authorised need is a catalyst for digital trust. In Table 7 the three fundamental concepts of information security are further described.

Concept	Description
Confidentiality	Ensuring that information is accessible only to those authorised to have access to it.
Integrity	Safeguarding the accuracy, completeness and timeliness of information and processing methods.
Availability	Ensuring that authorised users have access to information and associated assets when required.

Table 7: Objectives of Information Security [2.1]

Organisations should establish objectives, policies, and controls for information security. However, information security risks constantly evolve with technological and sociological developments. Therefore, organisations need to constantly monitor and evaluate the efficiency and effectiveness of implemented information security controls, identify new risks to be treated and select, implement and improve appropriate controls and procedures. This can be achieved by using a management system for information security. The ISMS family of standards of ISO/IEC assists organisations to implement and operate an information security management system.

An information security management system (ISMS) is a system that *“consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets”*, [2.2]. It is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving (collectively referred to hereafter as adopting) the organisation’s information security. Key elements of an ISMS are risk assessments, risk treatment and risk acceptance of the organisation. Risks that are treated and mitigated must have appropriate controls to ensure the protection of the information assets.

To establish, maintain, monitor and improve an ISMS, an organisation needs to undertake the following steps:

1. Identify information assets and its information security requirements;
2. Assess information security risks;

3. Select and implement controls associated with the organisation's information assets to treat risks that are not acceptable to the organisation;
4. Accept residual risks;
5. Maintain, monitor and improve the effectiveness of these controls.

For effective information risk management it is vital that these five steps are repeated on a regular basis, to identify changes in risks or in the strategy of the organisation.

At the first quarter of 2014 a total of 35 numbers in the ISO/IEC 27000 series have been issued, of which 25 are published and 10 are under development. By far the most popular one is ISO/IEC 27001 with, worldwide, 19577 certificates delivered in 103 countries [2.3]. The second most popular one is the code of practice ISO/IEC 27002. All other standards in the ISO/IEC 27000 series are far less popular, although the number of standards in this ISMS family is still growing.

2) ISO/IEC 27000

ISO/IEC 27000:2014 provides an overview of the ISMS family of standards and describes the fundamentals of an ISMS. It also defines the vocabulary that is used throughout the ISO/IEC 27000 series. In Figure 4 the relationships between the several ISMS standards are illustrated. Three categories of standards can be identified:

- Standards that specify requirements - normative statements that describe ISMS requirements (ISO/IEC 27001) or audit and certification requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001;
- Standards that describe general guidelines - guidance for various aspects of generic process and control-related ISMS guidelines, including risk controls (ISO/IEC 27002), implementation (ISO/IEC 27003), measurements (ISO/IEC 27004) and risk management (ISO/IEC 27005);
- Standards that describe sector-specific guidelines - guidance that provides sector-specific guidelines for ISMS, including telecommunications (ISO/IEC 27011), financial services (ISO/IEC TR 27015) and healthcare (ISO 27799).

The international standard ISO/IEC 27000:2014 (and several others) is available for free download⁶.

⁶ <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

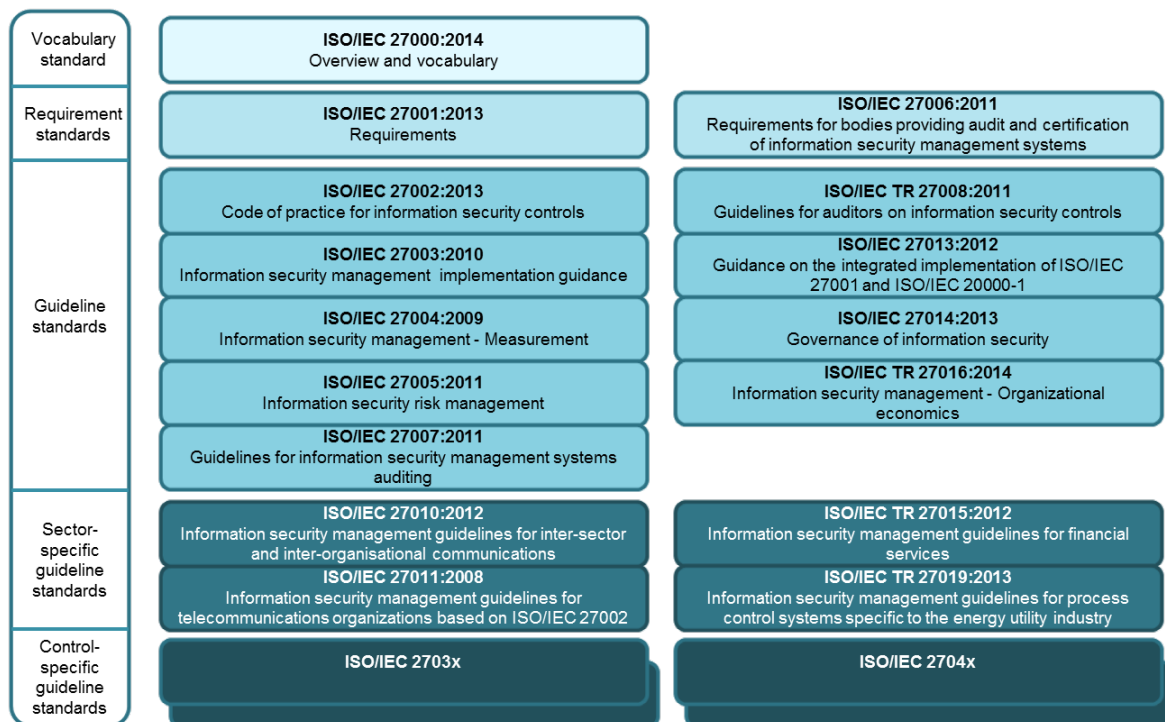


Figure 4: The ISO/IEC ISMS family of standards (ISO/IEC 27000:2014)

The standard enumerates nine fundamental principles (ISO/IEC 27000:2014, p. 13) that contribute to the successful implementation of an ISMS:

- a) Awareness of the need for information security;
- b) Assignment of responsibility for information security;
- c) Incorporating management commitment and the interests of stakeholders;
- d) Enhancing societal values;
- e) Risk assessments determining appropriate controls to reach acceptable levels of risk;
- f) Security incorporated as an essential element of information networks and systems;
- g) Active prevention and detection of information security incidents;
- h) Ensuring a comprehensive approach to information security management;
- i) Continual reassessment of information security and making of modifications as appropriate.

3) ISO/IEC 27001

ISO/IEC 27001:2013 “*Requirements*” originates from British Standard BS 7799-2:2002 (also known as BS 7799 Part-2). It is the successor of the international standard ISO/IEC 27001:2005 that was replaced in October 2013. The standard specifies normative requirements for adopting an ISMS within an organisation and includes a set of controls, both procedural and technical, for the management and mitigation of the risks. The standard is suitable for all types of organisations (commercial enterprises, government agencies, non-profit companies, etc.), all sizes (from SMEs to multinationals giants), and all businesses (retail, telecommunication, financial services, defence, healthcare, education, government, etc.).

Literature shows that organisations adopt ISO/IEC 27001 for a number of reasons, notably to meet legal requirements, to increase customer confidence and to improve their market position [2.4] [2.5]. Organisations adopting such an ISMS must ensure the selection of adequate and proportionate security controls to protect their information assets. The standard contains statements written as

'shall' and is often implemented together with ISO/IEC 27002 that provides suitable information security controls within the ISMS. The control objectives and controls of ISO/IEC 27001:2013 (see standard, table A.1 of Annex A) are closely linked with those from ISO/IEC 27002:2013 (clauses 5 to 18). However, ISO/IEC 27001:2013 does not specifically mandate all these information security controls, because they may vary across the various businesses. Additional or other controls applicable to particular business risks may be required. Furthermore, management may choose to accept or avoid information security risks rather than mitigate them through controls, which remains a risk management decision.

Organisations that pursue an ISO/IEC 27001:2013 certificate have to assess their information security risks, to define their information security objectives and subsequently implement appropriate information security controls according to their requirements. The following documentation is explicitly required for certification:

- ISMS scope (as per clause 4.3);
- Information security policy (clause 5.2);
- Information security risk assessment process (clause 6.1.2);
- Information security risk treatment process – Statement of Applicability (clause 6.1.3);
- Information security objectives (clause 6.2);
- Evidence of the competence of the people working in information security (clause 7.2);
- ISMS-related documents deemed necessary by the organisation (clause 7.5.1);
- Operational planning and control documents (clause 8.1);
- Results of the risk assessments (clause 8.2);
- Decisions regarding risk treatment (clause 8.3);
- Evidence of the monitoring and measurement of information security (clause 9.1);
- ISMS internal audit program and results of conducted audits (clause 9.2);
- Evidence of management reviews of the ISMS (clause 9.3);
- Evidence of nonconformities identified and corrective actions arising (clause 10.1);
- And various other documents related to the control objectives and controls listed in table A.1 of Annex A.

Certification auditors will check if such documentation is present, fit for purpose and properly managed (i.e. with formal creation, authorisation, implementation and maintenance processes). Organisations operating an ISMS based on ISO/IEC 27001 that have its conformity audited and certified, achieve a number of business benefits including improved service quality, higher customer satisfaction, and in some cases, even new business opportunities. Also increased information security staff awareness, mitigated security threats and better data protection has been found [2.5] [2.6] [2.7] [2.8].

Third parties that intend to make use of the services and/or products of an organisation that has obtained the ISO/IEC 27001 compliance certificate should take care of looking into the following crucial aspects of an ISMS. It concerns the ISMS scope (clause 4.3) and the decisions that the certified organisation has taken how to treat risks from the risk assessment process (clause 8.3, also known as Statement of Applicability). Organisations can scope their ISMS as broadly or as narrowly as they want, and could have a very high risk appetite (i.e. accepting many high information security risks).

The former ISO/IEC 27001:2005 standard relied specifically on the well-known Shewhart-Deming PDCA cycle (Plan-Do-Check-Act). ISO/IEC 27001:2013 puts more emphasis on measuring and evaluating how well an organisations' ISMS performs. The standard has the high-level structure, identical sub-clause titles and core text, common terms, and core definitions as defined in the Annex SL of ISO/IEC Directives [2.9]. It is, therefore, compatible with other management system standards

that have follow this Annex SL, such as ISO 9001 and ISO/IEC 27001. This allows a common approach for organisations that choose to work with a single management system that meets the requirements of more than one management system standard.

4) ISO/IEC 27002

ISO/IEC 27002:2013 “*Code of practice for information security controls*” (with former versions designated as ISO/IEC 17799:2000 and ISO/IEC 27002:2005) is an international standard that originates from the British Standard BS 7799:1995 (later known as BS 7799 Part-1). It is intended to be used in conjunction with ISO/IEC 27001:2013. In Backhouse et al. [2.10] an overview is provided of the creation and development of the ISO/IEC 27002 standard.

The standard can be used as a reference for selecting controls within the process of the implementation of an ISMS based on ISO/IEC 27001:2013 or as a guidance document for organisations that wish to implement commonly accepted good practice information security controls. It has been written as a set of guidelines that can be tailored to the specific information risks and needs of an organisation. By implementing a set of *controls, consisting of policies, practices, procedures, organisational structures and software functions*, the preservation of information related to confidentiality, integrity and availability is to be achieved. In many cases organisations use these controls with the accompanying standard ISO/IEC 27001 to achieve ISMS certification compliance against ISO/IEC 27001. ISO/IEC 27002 is well accepted within the information security profession worldwide.

The standard consists of 80 pages (excluding foreword, introduction, etc.) and offers internationally recognised security practices that enable an organisation to meet audit, regulatory and legal requirements. It contains 14 sections (clauses 5 to 18, see Table 8) in 35 security categories and 114 related controls. Per control high level implementation guidance and other related information are provided. Specific implementation guidelines can be found in other standards of the ISO/IEC 27000 series of ISMS standards, such as ISO/IEC 27003 that provides a process oriented approach to an ISMS implementation conform ISO/IEC 27001.

Security clauses	Security categories
5. Information security policies	1. Management direction for information security
6. Organization of information security	1. Internal organization 2. Mobile devices and teleworking
7. Human resource security	1. Prior to employment 2. During employment 3. Termination and change of employment
8. Asset management	1. Responsibility for assets 2. Information classification 3. Media handling
9. Access control	1. Business requirements of access control 2. User access management 3. User responsibilities 4. System and application access control
10. <i>Cryptography</i>	1. Cryptographic controls
11. Physical and environmental security	1. Secure areas 2. Equipment

12. Operations security	<ul style="list-style-type: none"> 1. Operational procedures and responsibilities 2. Protection from malware 3. Backup 4. Logging and monitoring 5. Control of operational software 6. Technical vulnerability management 7. Information systems audit considerations
13. Communications security	<ul style="list-style-type: none"> 1. Network security management 2. Information transfer
14. System acquisition, development and maintenance	<ul style="list-style-type: none"> 1. Security requirements of information systems 2. Security in development and support processes 3. Test data
15. <i>Supplier relationships</i>	<ul style="list-style-type: none"> 1. Information security in supplier relationships 2. Supplier service delivery management
16. Information security incident management	<ul style="list-style-type: none"> 1. Management of information security incidents and improvements
17. Information security aspects of business continuity management	<ul style="list-style-type: none"> 1. Information security continuity 2. Redundancies
18. Compliance	<ul style="list-style-type: none"> 1. Compliance with legal and contractual requirements 2. Information security reviews

Table 8: Security clauses and categories of ISO/IEC 27002:2013

Each security category contains a control objective stating what is to be achieved, and one or more controls (written as recommendations) that can be applied to achieve that control objective. Detailed information about selecting controls and risk treatment options can be found in ISO/IEC 27005. Performance criteria and targets are not included in this standard and it is up to the organisation to set them for their specific needs. The ISO/IEC 27004 standard can assist in this matter.

Compared to the previous version ISO/IEC 27002:2005 (that had 11 sections with 39 security categories and 134 controls) the clauses 'Cryptography' and 'Supplier relationships' have been added and 'Communications and Operations Management' has been split in two. Although ISO/IEC 27002 covers a very broad range of information security risks and controls it has difficulties to keep pace with technological aspects. The latest 2013 version just drops a remark on Cloud Computing⁷ in clause 15.1.3 and complete lacks any reference to BYOD (bring your own device). These are topical and pressing information security issues where the standard does not provide practical guidance.

5) ISO/IEC 27003

ISO/IEC 27003:2010 "*Information security management system implementation guidance*" provides practical recommendations and explanations, based on a process oriented approach, for the successful design and implementation of an ISMS in line with ISO/IEC 27001. It provides instructions how to create an ISMS project implementation plan, and includes how to define the scope of the ISMS, how to plan the ISMS project and how to get management approval for the ISMS project. It also describes the critical activities for the ISMS project and provides examples to achieve the requirements in ISO/IEC 27001. However, this standard does not include operational ISMS activities and does not specify any requirements.

⁷ A new dedicated standard ISO/IEC 27017 will address this topic separately.

The standard is applicable to all types of organisation of all sizes and depending on the size and complexity of the organisation, some implementation activities can be simplified. Implementation of the ISMS project can be carried out using regular project management methods, such as the popular PRINCE2⁸ method.

6) ISO/IEC 27004

ISO/IEC 27004:2009 “*Measurement*” provides a measurement framework for assessments of ISMS effectiveness to fulfil the measurement requirements set out in ISO/IEC 27001. It gives good practice guidance and advice on the development and use of measures and measurements such as collecting data, analysing data and developing measurement results for all relevant stakeholders. The guidance, provided by this standard, results in documentation that contributes to demonstrate that the ISMS control and processes effectiveness is being measured and assessed as part of an organisation’s ISMS continual improvement process.

The implementation of the measurement framework constitutes an Information Security Measurement Program. This program assists in identifying and evaluating non-compliant and ineffective ISMS control processes and procedures. It also prioritises related improvement or changing actions. This includes information security policies, information security risk management, control objectives, controls, processes and procedures. It also includes data verification and data quality auditing. Although this standard can be used to determine whether this needs to be changed, no measurement of controls can guarantee full security.

To summarise this standard describes the following activities to fulfil the ISMS measurement requirements:

1. Develop base measures, derived measures and indicators;
2. Implement and operate an Information Security Measurement Programme;
3. Collect and analyse data;
4. Develop measurement results;
5. Communicate developed measurement results to the relevant stakeholders;
6. Use measurement results as contributing factors to ISMS-related decisions;
7. Use measurement results to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures;
8. Facilitate continuous improvement of the Information Security Measurement Programme.

Also this standard is applicable to all types and sizes of organisations. Depending on the size and complexity of the organisation, the approach by an organisation to fulfil its measurement requirements including the extent of the required measurements may vary in terms of the numbers and frequency.

7) ISO/IEC 27005

ISO/IEC 27005:2011 “*Information security risk management*” provides guidelines for implementing information security risk management, including risk assessment, risk treatment, risk acceptance and risk monitoring and review. By following this standard, effective information security controls can be created based on a risk management approach as specified in ISO/IEC 27001.

⁸ <http://www.prince-officialsite.com/>

The standard starts with establishing the context in which an organisation operates. This provides the scope and criteria required for operating an ISMS. Subsequently a risk assessment is carried out in which an identification of information assets is performed, including the vulnerabilities these assets face and the threats that can exploit the vulnerabilities.

Following, the likelihood and impact of a successful exploit are identified, which constitutes the risk an information asset faces. This risk can be estimated qualitative or quantitative. If the risk is not accepted, the next step involves treatment of the risk by performing risk resolution or mitigation actions and setting up risk controls. Last but not least the risk must be monitored and periodically reviewed to ensure the ISMS remains up to date.

This standard does not provide any specific method for information security risk management and it is up to the organisation to define its approach on information security risk management. The reason is that such an approach depends on, for example, the type and size of the organisation or the scope of the required ISMS. Existing methods can be used to implement the requirements of an ISMS. This version of the standard is better aligned with the international standard for risk management, ISO 31000:2009 "*Risk management -- Principles and guidelines*".

8) ISO/IEC 27006

ISO/IEC 27006:2011 "*Requirements for bodies providing audit and certification of information security management systems*" is the ISMS certification body accreditation standard. It supports the accreditation of organisations that provide ISMS certification. These certification organisations need to meet the requirements contained within ISO/IEC 27006 in an addition to the requirements specified in ISO/IEC 27001 and ISO/IEC 17021.

ISO/IEC 17021:2011 "*Conformity Assessment -- Requirements for bodies providing audit and certification of management systems*" contains principles and requirements for certification organisations regarding audit and certification of management systems. This standard is accompanied with several specific technical specifications: environmental management systems (part 2), quality management systems (part 3), event sustainability management (part 4), asset management systems (part 5), business continuity management systems (part 6, under construction) and road traffic safety management systems (part 7, under construction). For information security management systems, ISO/IEC 27006:2011 must be used instead of providing third-party conformity assessment of ISO/IEC 27001.

The ISMS certification organisations need to demonstrate that they act professionally and impartially to meet the requirements of this standard. Next to its application for accreditation ISO/IEC 27006 can also be used for peer assessments and other audit processes.

9) ISO/IEC 27007

ISO/IEC 27007:2011 "*Guidelines for information security management systems auditing*", provides guidance on conducting ISMS audits and how manage an ISMS audit programme, against the requirements specified in ISO/IEC 27001. This standard complements the guidance on general management systems of ISO 19011⁹ by providing additional ISMS-specific guidance. It also provides

⁹ ISO 19011:2011 "*Guidelines for auditing management systems*"

guidelines on the competence and evaluation of ISMS auditors. ISO/IEC 27007 is also aligned with ISO 17021¹⁰ and ISO/IEC 27006.

The standard covers the following aspects of ISMS compliance auditing:

- Manage an ISMS audit programme (what, when and how to audit; assign auditors; manage audit risks; maintain audit records; continuous process improvement);
- Perform an ISMS audit (planning, fieldwork, analysis, reporting and follow-up);
- Manage ISMS auditors (skills, competencies and evaluation).

10) ISO/IEC TR 27008

ISO/IEC TR 27008:2011 “*Guidelines for auditors on information security controls*” is a technical report that provides guidance for auditors on reviewing the implementation and operation of an organisation’s ISMS controls. It supports an ISMS risk management process that must be in accordance with the description in ISO/IEC 27001, ISO/IEC 27005 and the compliance checking of information system controls of ISO/IEC 27002. Specific guidance on compliance checking on risk measurements, risk assessments and risk audits of an ISMS as specified in ISO/IEC 27004, ISO/IEC 27005 and ISO/IEC 27007 respectively.

11) ISO/IEC WD 27009

ISO/IEC 27009 “*The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications*” is currently in a preparatory stage. It is to provide sector specific and/or service-specific certifications, extended with Sector/Service specific ISMS requirements that are not included within the scope of ISO/IEC 27001.

ISO/IEC 27009 will explain how to include requirements additional to the ones of ISO/IEC 27001 (such as privacy). It will also specify principles on this refinement, which must not contradict any of the original ISO/IEC 27001 requirements. Each sector specific standard may address different risks and risk assessments, which must be integrated with the overall ISO/IEC 27001 risk assessment process.

Sector specific controls are permitted as a replacement for the ones specified in ISO/IEC 27001 Annex A, provided that information is included that can be used in statements of Applicability to justify the changes. The same is true of omitting original controls specified in ISO/IEC 27001 Annex A. The risk management process must include provisions for the determination of controls and production of a Statement of Applicability. This statement contains a reference to the sector specific standard(s) used.

Note: A complete overview of current standards and ones that are being developed is given in Table 9.

12) ISO/IEC 27010

ISO/IEC 27010:2012 “*Information security management guidelines for inter-sector and inter-organisational communications*” is a standard that provides additional guidelines for inter-organisational and inter-sector communications. It specifically relates to initiating, implementing, maintaining, and improving information security for such information sharing communities.

¹⁰ ISO 17021:2011 “Conformity assessment -- Requirements for bodies providing Audit and certification of management systems”

ISO/IEC 27010 helps by laying a common ground for inter-sector and inter-organisational security and is applicable to all forms of sharing or exchange of sensitive information, within and between all industry sectors and/or nations. It can be used under normal business circumstances to meet contractual, regulatory or legal obligations. In case information is highly sensitive it may need to be restricted to certain individuals within the sending and receiving organisations or information sources may need to remain anonymous.

It can also be used in times of crisis, for example during large-scale system outages of the government of DDoS-attacks¹¹ targeted at financial service providers. In those situations information is exchanged under stressful circumstances and time pressure, however it remains vital that information security principles will be respected. Hence, ISO/IEC 27010 should provide the basis and guidance on methods, models, policies, processes, protocols, and controls, for the sharing of information securely with trusted counterparties under all circumstances.

At the national level, Mr. Benoit Poletti, chairman of the national mirror committee ISO/IEC JTC 1/SC 27, has been co-editor of the current version of this standard.

13)ISO/IEC 27011

ISO/IEC 27011:2008 “*Information security control guidelines based on ISO/IEC 27002 for telecommunications organizations*” is the ISMS implementation guide especially suited for the telecommunications industry. It contains a common set of security control objectives with a specific focus on the telecommunications sector and includes an extended control set which provides new controls and implementation guidance.

It was developed jointly by ISO/IEC JTC1/SC 27 and ITU-T¹², originally published in 2004, and was primarily based on ISO/IEC ISMS standards and telecommunication related security standards. The standard will be revised in 2014 to reflect the updated new versions of ISO/IEC 27001 and ISO/IEC 27002.

14)ISO/IEC 27013

ISO/IEC 27013:2012 “*Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*” provides guidelines on implementing an integrated information security and IT service management system that conforms to both standards. It is based on both ISO/IEC 27001:2005 and ISO/IEC 20000-1:2011 (an IT service management specification, derived from ITIL¹³ v2). These two management systems complement and support each other’s objectives.

The standard provides organisations with a better understanding of the characteristics, similarities and differences of ISO/IEC 27001 and ISO/IEC 20000-1 and can be used in various ways:

- Implement both standards simultaneously from scratch;
- Implement ISO/IEC 27001 when ISO/IEC 20000-1 has already been adopted, or *vice versa*;
- Integrate pre-existing ISO/IEC 27001 and ISO/IEC 20000-1 management systems.

¹¹ Distributed Denial-of-Service attack is an attempt to make a computer system or network resource unavailable to its intended users.

¹² The standardization study groups of the International Telecommunication Union (ITU)

¹³ Information Technology Infrastructure Library (ITIL) is a set of IT service management practices to align business needs and IT service provisioning.

The standard proposes a combined framework for organising activities leading to an integrated approach, including:

- A shared vision and common vocabulary;
- Aligned information security and service management improvement objectives;
- A collective system and supporting documents (policies, standards, processes, procedures etc.);
- Co-ordinated multidisciplinary activities, such as incident and change management;
- Re-certification of the management systems simultaneously.

ISO/IEC 27001 and ISO/IEC 20000-1 can be further integrated with other management systems standards, such as the ones based on ISO 9001 and ISO 14001.

15)ISO/IEC 27014

ISO/IEC 27014:2013 “*Governance of information security*” provides guidance on principles and concepts for the governance of information security. The standard should provide the mandate that is key to drive information security initiatives in an organisation. The standard also assists an organisation to make appropriate and timely decisions about information security issues in support of its strategic objectives. ISO/IEC 27014 should help with the following:

- Aligning information security objectives with business strategy;
- Making efficient and effective investments decisions on information security;
- Ensuring information security risks are adequately addressed;
- Providing visibility on information security status;
- Achieving compliance with external requirements (contractual, regulatory, legal).

Governance of information security needs to be aligned with the general business objectives and strategy of an organisation. Therefore it needs to be an integral part of organisational governance. The standard only describes governance at a high level, in 11 pages, and does not detail with common governance aspects such as decision rights, accountability framework and management structures.

16)ISO/IEC TR 27015

ISO/IEC TR 27015:2012 “*Information security management guidelines for financial services*”, provides information security guidance complementing the information security controls defined in ISO/IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within financial service organisations (such as banks, insurance companies, credit card companies, clearing houses, etc.).

The financial services industry relies heavily on information technology, such as for financial transactions, fraud detections and credit risk calculations. This technical report provides sector-specific guidance and extends in a few areas the recommendations of ISO/IEC 27002. An example is the recommendation that security awareness activities should not only be directed at employees but also towards customers. To date, only very few companies have adopted this sector specific standard.

At the national level, Mr. Benoit Poletti, chairman of the national mirror committee ISO/IEC JTC 1/SC 27, has been co-editor of the current version of this technical report.

17)ISO/IEC TR 27016

ISO/IEC TR 27016:2014 “*Organizational economics*”, provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. This Technical Report supplements the ISO/IEC 27000 series of standards by overlaying an economic perspective on protecting an organization’s information assets in the context of the wider societal environment in which an organization operates.

Coupled with a risk management approach (ISO/IEC 27005) and the ability to perform information security measurements (ISO/IEC 27004), economic factors need to be considered as part of information security management when planning, implementing, maintaining and improving the security of the organization’s information assets. In particular, economic justifications are required to ensure spending on information security is effective as opposed to using the resources in a less efficient way.

Typically, economic benefits of information security management concern one or more of the following:

1. Minimizing any negative impact to the organization’s business objectives;
2. Ensuring any financial loss is acceptable;
3. Avoiding requirements for additional risk capital and contingency provisioning.

Information security management may also produce benefits that are not driven by financial concerns alone. While these non-financial benefits are important, they are usually excluded from financial based economic analysis. Such benefits need to be quantified and included as part of the economic analysis. Examples include:

1. Enabling the business to participate in high-risk endeavours;
2. Enabling the business to satisfy legal and regulatory obligations;
3. Managing customer expectations of the organization;
4. Managing community expectations of the organization;
5. Maintaining a trusted organisational reputation;
6. Providing assurance of completeness and accuracy of financial reporting.

18)ISO/IEC TR 27019

ISO/IEC TR 27019:2013 “*Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*”, provides guidance to organisations in the energy utility industry in order to secure their electronic process control systems. This technical report provides additional, more specific guidelines on information security management than the generic advice provided by ISO/IEC 27002. ISO/IEC TR 27019 must be used in conjunction with ISO/IEC 27002 since it does not incorporate its content. The text of this document basically consists of an English translation of the German standard DIN SPEC 27009:2012-04¹⁴.

The energy utility industry relies heavily on electronic process control systems. Because of the nature of such systems with potential safety, health and environmental impact, information security is a key issue. The scope of this technical report covers process control systems used by the energy utility industry such as Programmable Logic Controllers (PLCs), Supervisory Control And Data Acquisition

¹⁴ “Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002”, <http://www.beuth.de/en/technical-rule/din-spec-27009/151100155>

(SCADA) and Industrial Control Systems (ICS), including networks and supporting processes, to direct, monitor, and control the production activities (generation, transmission, storage and distribution of electric power, gas and heat).

19)ISO/IEC 27031

ISO/IEC 27031:2011 "*Guidelines for information and communication technology readiness for business continuity*" provides guidance on the concepts and principles behind the role of IT to ensure business continuity. The standard provides a framework of methods and processes for any organisation (small to large - private, governmental, and non-governmental).

It identifies and specifies all relevant aspects including performance criteria, design, and implementation details, for improving IT readiness as part of the organisation's ISMS, to ensure business continuity. It enables an organisation to measure its IT continuity, security and, therefore, its readiness to survive a disaster in a consistent and recognised manner.

The scope of ISO/IEC 27031 includes all events and incidents that could impact the IT infrastructure of the organisation. It covers and extends information security incident handling and management, IT readiness planning and services. IT readiness (for Business Continuity) is a general term for the processes described in this standard and ensures that the IT services are as resilient as appropriate and can be recovered to pre-determined levels within time scales required and agreed by the organisation.

20)ISO/IEC 27032

ISO/IEC 27032:2012 "*Guidelines for cyber security*" provides guidance concerned with information security risks associated with the Internet. The standard has two focal areas:

1. Technical guidance for addressing common risks associated with the Internet, including social engineering attacks, hacking and malicious software, such as malware and spyware. It also provides controls for addressing these risks, including controls for preparing, detecting and monitoring of attacks and responding to attacks;
2. A framework for information sharing, co-ordination and incident handling between providers and consumers on the Internet. This framework includes key elements for establishing digital trust, processes for collaboration and information interchange and technical requirements for integration and interoperability of systems between different stakeholders.

The standard does not directly address cybercrime and how to deal with it effectively.

21)ISO/IEC 27033

ISO/IEC 27033:2009..2014 "*Network security*" provides guidance on the security aspects of management, operation and use of information system networks, and its inter-connections. ISO/IEC 27033 is a multi-part standard based on the five-part network security standard ISO/IEC 18028:2006 which has been revised to fit into the ISMS family of standards. It consists of several parts (parts 1, 2, 3, 4 and 5 are published at the moment of writing) and more parts may follow.

ISO/IEC 27033 provides detailed guidance on implementing the ISO/IEC 27002 network security controls. The scope of this standard concerns the security and management of network devices,

applications, services and users of the network. It also includes the security of information being transferred through communication networks. Primary audience are network security architects, designers, officers and managers.

Both the number of parts to the standard and its scope are subject to change as the standard continues to develop with the evolving network security technology and concerns. Currently, five parts are published and one is in preparation, as listed below:

- ISO/IEC 27033-1:2009 provides an overview of network security and related definitions (p.73);
- ISO/IEC 27033-2:2012 provides guidelines for the design and implementation of network security (p. 28);
- ISO/IEC 27033-3:2010 concerns threats, design techniques and control issues (p.30);
- ISO/IEC 27033-4:2014, relates to securing communications between networks using security gateways (p. 22);
- ISO/IEC 27033-5:2013 relates to securing communications across networks using Virtual Private Network (VPNs) (p.14).

The following part is still in preparation:

- ISO/IEC 27033-6, relates to securing wireless IP network access.

22) ISO/IEC 27034

ISO/IEC 27034:2011 "*Application security*" provides guidance on integrating security into the processes, the specification, design, programming or procuring, implementation and use of computer applications.

ISO/IEC 27034 is a multi-part standard and consists of seven parts of which part 1 has been published. The objective of the standard is to ensure that computer application systems deliver the required level of security in support of the organisation's ISMS. Primary audience consists of software architects and analysts, programmers, testers, system and database administrators, but also acquisition personnel, managers, auditors, users and suppliers may benefit from it.

ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development and/or operation of the applications has been outsourced. It does not contain a software application development method nor is it a software development life cycle standard.

The full set contains the following standards:

- ISO/IEC 27034-1:2011 presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.

The following parts are in preparation:

- ISO/IEC 27034-2 "*Organization normative framework*";
- ISO/IEC 27034-3 "*Application security management process*";
- ISO/IEC 27034-4 "*Application security validation*";
- ISO/IEC 27034-5 "*Protocols and application security controls data structure*";
- ISO/IEC 27034-6 "*Security guidance for specific applications*";
- ISO/IEC 27034-7 "*Application security control attribute predictability*".

23)ISO/IEC 27035

ISO/IEC 27035:2011 “*Information security incident management*” deals with the processes for managing information security incidents and vulnerabilities. It is based on the upgraded technical report ISO/IEC TR 18044:2004, which has been replaced by this standard.

ISO/IEC 27035 provides a structured and planned approach to: 1) detect, report, assess, respond and manage information security incidents; 2) detect, assess and manage information security vulnerabilities; 3) continuously improve information security incident management. It specifically provides guidance for medium-sized and large organisations. Smaller organisations can use subset of documents, processes and routines depending on their requirements and controls.

24)ISO/IEC 27036

ISO/IEC 27036:2013 “*Information security for supplier relationships*” provides guidance on the evaluation and treatment of information security risks involved in the acquisition of IT-related products and services from other organisations.

ISO/IEC 27036 is a multi-part standard and consists of four parts of which part 1 and 3 have been published and the others are under development:

- ISO/IEC 27036-1:2014 “*Overview and concepts*”;
- ISO/IEC 27036-2 “*Requirements*”;
- ISO/IEC 27036-3:2013 “*Guidelines for information and communication technology supply chain security*”;
- ISO/IEC 27036-4 “*Guidelines for security of cloud services*”.

ISO/IEC 27036-3:2013 focuses on managing the information security risks caused by today’s complex IT supply chains (multi-layered and physically dispersed). It also concerns how to respond to organisational as well as technical risks stemming from products and services of these IT supply chains. Finally it deals with integrating information security processes and practices into the computer system and application lifecycle processes.

25)ISO/IEC 27037

ISO/IEC 27037:2012 “*Guidelines for identification, collection, acquisition and preservation of digital evidence*” provides guidance on specific activities in the handling of digital evidence of potential digital forensic evidence that can be of evidential value i.e. “digital data that may be of value for use in court”.

ISO/IEC 27037 assists organisations in their disciplinary procedures facilitates the exchange of potential digital evidence between jurisdictions. It also provides guidance to individuals regarding the digital evidence handling process. It relates to various devices and/or functions that are used in diverse circumstances (underneath a non-exhaustive list quoted from this standard):

- Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions;
- Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards;
- Mobile navigation systems;
- Digital still and video cameras (including closed-circuit television, CCTV);

- Standard computer with network connections;
- Networks based on TCP/IP and other digital protocols.

The key purpose of ISO/IEC 27037 and other ISMS standards in this series that are currently in development (ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC 27043) is to promote good practice methods and processes for forensic investigation of digital evidence. Maybe these forensics standards will be grouped into a multi-part standard later on, as these all cover different aspects of the same forensics process.

26)ISO/IEC 27038

ISO/IEC 27038:2014 “*Specification for digital redaction*” specifies characteristics of techniques for performing digital redaction on digital documents but it does not include the redaction of information from databases. It also specifies requirements for software redaction tools and methods of testing that digital redaction has been securely completed.

It can be possible to identify redacted information in a redacted digital document by context. For example, the length of the redaction replacement text can indicate the length of the redacted information, and thus the information itself. This international standard introduces two levels of redaction:

- BASIC redaction where context is not taken into consideration;
- ENHANCED redaction where context is taken into consideration.

Redaction techniques can be used for the anonymisation of the information in a document, for example by the removal of some names within sentences. It can also involve the removal of numbers within sentences and their replacement by “XXX”.

27)ISO 27799

ISO 27799:2008 “*Information security management in health using ISO/IEC 27002*” defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002. This standard, part of the ISMS family of standards, deals with the security of personal health information and complement ISO/IEC 27002 in the context of healthcare organisations. However, it was not prepared by ‘Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security Techniques’. The ISO Technical Committee 215 is responsible for its contents and publication.

Personal health information of individuals is regarded by many as one of the most important types of information that needs adequate treatment regarding confidentiality, integrity and availability. Protecting the confidentiality of health information is essential if the privacy of individuals that need healthcare is to be maintained. Its integrity must be protected to ensure patient safety, and it is essential that the health information’s life cycle is fully auditable. Last but not least, the availability of such information is critical to effective and efficient healthcare delivery.

To this end, ISO 27799 specifies a set of detailed controls for managing health information confidentially, integrity and availability and provides good practice guidelines in this respect. It applies to health information in all its aspects, irrespectively of its form (conversations, audio and video recordings, medical images etc.), the way it is stored (writing or printing on paper or electronic storage, etc.) and the means it is transmitted (post, email, courier, etc.).

All security control objectives of ISO/IEC 27002 remain relevant to health informatics. However, because there are additional health-sector-specific requirements this standard places constraints upon the application of certain security controls specified in ISO/IEC 27002. The standard also provides health information security good practice guidelines in such a way that staff responsible for health information security can readily understand and adopt it. By implementing ISO 27799, healthcare organisations will be able to ensure a minimum level of security that is appropriate to their organisation's circumstances and that will maintain the security of personal health information.

28/Synthesis

Information security is a broad topic with implications in all parts of an organisation. It is relevant to any organisation that handles and depends on information, from SMEs to multinationals, from not-for-profits, government departments, to commercial enterprises. An information security management system (ISMS) assists in preserving the confidentiality, integrity and availability of information. It consists of policies, procedures, guidelines, resources, activities and software functions, to protect the information assets of an organisation. To establish, maintain, monitor and improve an ISMS, an organisation needs to undertake at least the following steps: 1) to identify information assets and its information security requirements; 2) to assess information security risks and treat these risks; 3) to select and implement controls associated with the organisation's information assets; 4) to maintain, monitor and improve the effectiveness of these controls.

ISO/IEC 27001 is a well-known and recognised standard that specifies normative requirements for adopting an ISMS and includes a set of controls for the management and mitigation of information security risks. Many organisations worldwide obtained certification for this standard, which helped them to improve service quality with a lower risk exposure, to improve customer satisfaction and to gain new business opportunities.

The accompanying good practise standard ISO/IEC 27002 helps in setting up an ISMS in conformity with ISO/IEC 27001. Although specific information security risk and control requirements may differ per organisation, there is a lot of common ground, for example regarding information security risks related to employees. Unfortunately, some latest developments and its technical ramifications, such as Cloud Computing are not specifically covered in ISO/IEC 27002.

Other standards in the ISO/IEC 27000 series address specific topics, such as ISMS implementation guidance (ISO/IEC 27003), setting performance criteria and targets (ISO/IEC 27004) and selecting controls and risk treatment options (ISO/IEC 27005). However, most of those lack specific and pragmatic guidance and consequently have a low uptake despite the obvious needs.

Of all standards in this ever growing ISMS family ISO/IEC 27001 and 27002 (and the overview and vocabulary in ISO/IEC 27000) are by far the most important and widely used ones. Because of their general set-up they cover the large majority of information security controls that any organisation would require. Maybe that is a reason why the sector-specific guidelines are not very popular and do not allow directly specific certifications. Possibly ISO/IEC 27009 "*The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications*", which is currently under development, will assist in this matter.

ISMS adoption and certification against ISO/IEC 27001 provides a number of business benefits. This standard and ISO/IEC 27002 accommodate a common language, improve awareness, communication and understanding of information security, help to increase customer satisfaction and enable the organisation to offer more products or even create new business opportunities.

It is advised that companies that would like to adopt ISO/IEC 27001 and/or 27002 take notice of a number of success factors [2.11]:

1. Ensure that ISO/IEC 27001 and ISO/IEC 27002 implementation is a business- rather than an IT-driven activity;
2. Ensure commitment and endorsement for ISO/IEC 27001 and ISO/IEC 27002 at senior management levels;
3. Create information security awareness at business and IT departments, at both management and staff levels;

4. Do not blindly implement all 114 controls as stated in ISO/IEC 27001 and ISO/IEC 27002 and make sure the risk treatments are based on a risk assessment process that not only addresses IT related risks but also business risks;
5. Ongoing improvements of the ISMS are vital to achieve and sustain long-term business benefits;
6. An adequate waivers and dispensation process that allows to (temporally) deviate from the ISO/IEC 27001 and ISO/IEC 27002 control measures, if accompanied by sound business rationale and mitigating factors;
7. Integrate controls, templates, etc. into existing processes and governance structures of the organisation as much as possible;
8. Earlier experience with other management system standards such as ISO 9000 or ISO/IEC 20000 eases implementation and acceptance by the organisation;
9. Decisions about information security investments are primarily driven by the level of risk or based on regulatory requirements;
10. Information security staff should be attentive to changes in the organisation by anticipating changes in business needs, changes in management (structure), or new technology.

Other companies can benefit from these learned lessons and have a head start when adopting these important ISMS standards.

Name	Year of publication	Contents	Type	Pages
ISO/IEC 27000	2014	Overview and vocabulary	standard	31
ISO/IEC 27001	2013	Requirements	standard for certification	23
ISO/IEC 27002	2013	Code of practice for information security controls	standard	80
ISO/IEC 27003	2010	Implementation guidance	standard	68
ISO/IEC 27004	2009	Measurement	standard	55
ISO/IEC 27005	2011	Assist implementation (includes risk assessment, treatment, acceptance, monitoring & review)	standard	68
ISO/IEC 27006	2011	Requirements for bodies providing audit and certification	standard for accreditation	37
ISO/IEC 27007	2011	Guidelines for information security management systems auditing	standard	27
ISO/IEC TR 27008	2011	Auditor guidelines on information security controls	technical report	36
ISO/IEC 27009	In preparation	Sector-specific application of ISO/IEC 27001 — Requirements	standard	N/A
ISO/IEC 27010	2012	Guidelines for inter-sector and inter-organisational communications for ISO/IEC 27001	standard	34
ISO/IEC 27011	2008	Guidelines based on ISO/IEC 27002 for telecommunications organizations	standard	44
ISO/IEC 27013	2012	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	standard	38
ISO/IEC 27014	2013	Governance of information security	standard	11
ISO/IEC TR 27015	2012	Guidelines for financial services for ISO/IEC 27001	technical report	18
ISO/IEC TR 27016	2014	Organizational economics	technical report	31
ISO/IEC 27017	In preparation	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	standard	N/A
ISO/IEC 27018	In preparation	Code of practice for PII protection in public clouds acting as PII processors	standard	N/A
ISO/IEC TR 27019	2013	Guidelines for process control systems specific to the energy utility industry	technical report	37
ISO/IEC 27031	2011	Guidelines for information and communication technology readiness for business continuity	standard	36
ISO/IEC 27032	2012	Guidelines for cyber security	standard	50

ISO/IEC 27033	2009..2014	Network security (6 parts)	standard	167+
ISO/IEC 27034	2011	Application security (7 parts – parts 2 to 7 under development)	standard	67
ISO/IEC 27035	2011	Information security incident management	standard	78
ISO/IEC 27036	2013..2014	Information security for supplier relationships (4 parts – parts 2 and 4 under development)	standard	36
ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition and preservation of digital evidence	standard	38
ISO/IEC 27038	2014	Specification for digital redaction	standard	9
ISO/IEC 27039	In preparation	Intrusion detection and protection systems	standard	N/A
ISO/IEC 27040	In preparation	Guideline on storage security	standard	N/A
ISO/IEC 27041	In preparation	Assurance for digital evidence investigation methods	standard	N/A
ISO/IEC 27042	In preparation	Analysis and interpretation of digital evidence	standard	N/A
ISO/IEC 27043	In preparation	Digital evidence investigation principles and processes	standard	N/A
ISO/IEC 27044	In preparation	Guidelines for Security Information and Event Management (SIEM)	standard	N/A
ISO/IEC 27050	In preparation	Electronic discovery (4 parts)	standard	N/A
ISO 27799	2008	Information security management in health using ISO/IEC 27002	standard	58

Table 9: The ISO/IEC 27K ISMS standards (as per June 2014)

III. ISO/IEC 15408 series, “Common Criteria”

1) Introduction

The *Common Criteria for Information Technology Security Evaluation* (abbreviated as Common Criteria or CC) is a referential for security evaluation of computer products which defines a common set of terms related to the evaluation of security requirements. It defines procedures that must be followed by customers, product developers as well as security evaluation authorities to allow certification of security functions of computer products at several levels of assurance.

It is a framework in which customers of computer products can specify their security requirements, manufacturers can then implement and/or make statements about the security aspects of their products, and third parties can evaluate these products to determine if these actually meet the security requirements. As such it provides assurance that the process of specification, implementation and evaluation of security aspects of computer products has been conducted in a rigorous, repeatable and standardised manner. The evaluation results may help customers to determine whether these computer products fulfil their security needs.

Products that are evaluated against the Common Criteria, which may be implemented in *hardware, firmware or software*, have a defined level of assurance related to its information security capabilities and are recognized in large parts of the world. The governments of 26 countries (17 as authorising and 9 as consuming members)¹⁵ formally acknowledge the Common Criteria and have mutual recognition of each other's product evaluations up to a certain level of assurance.

The Common Criteria for evaluation of IT security are available as the international standard from the ISO website as well as are freely downloadable from the Common Criteria Portal¹⁶. Both texts are identical and consist of three parts: an overview part and two other parts that deal with security functional and assurance requirements. The ISO/IEC version is based on CC version 3.1 and dates from 2008 and 2009 whereas the latest version, obtainable from the portal for free, dates from September 2012 (version 3.1 release 4).

2) History

The CC is the outcome of a number of efforts to develop criteria for evaluation of IT security which are of general use globally. The Common Criteria was developed through collaboration between the governments and national security and standards organisations within Canada, France, Germany, the Netherlands, the United Kingdom and the United States. The objective was to facilitate internationally buying and selling computer products for government markets (mainly for Defence or Intelligence use) using a single evaluation system.

The CC stakeholders have worked with the International Organization for Standardization (ISO) to make sure that the CC could become the international series of standards *ISO/IEC 15408*. It replaced existing security evaluation criteria in Europe (ITSEC v1.2), the US (TCSEC/FC-ITS) and Canada (CTCPEC):

- The ‘Information Technology Security Evaluation Criteria’ (ITSEC) was an European standard published in 1991 by the European Commission after joint development by France, Germany,

¹⁵ <http://www.commoncriteriaportal.org/ccra/members/>

¹⁶ <http://www.commoncriteriaportal.org/cc/>

the Netherlands and the United Kingdom and was an integration of earlier security evaluation approaches;

- The 'Trusted Computer System Evaluation Criteria' (TCSEC) was a standard developed in the United States in the 1980's and had a number of successors such as the draft Federal Criteria for Information Technology Security (FC-ITS v1.0);
- The 'Canadian Trusted Computer Product Evaluation Criteria' (CTCPEC v3.0) was published in 1993 as a combination of the ITSEC and TCSEC approaches.

The international standard ISO/IEC 15408 is applicable to risks arising from human activities (malicious or otherwise) as well as risks arising from technical (non-human) activities. ISO/IEC 15408 is intentionally flexible, which allows for a range of evaluation methods to be applied to various security properties of IT products. This flexibility also constitutes a risk as using this standard in conjunction with irrelevant security properties and unsuitable evaluation methods can result in meaningless evaluation results.

ISO/IEC 15408 is a multipartite standard, under the general title "*Information technology -- Security techniques -- Evaluation criteria for IT security*", and consists of the following parts:

- ISO/IEC 15408-1 "*Introduction and general model*" defines concepts and principles of IT security evaluation and specifies a general model of IT security evaluation. It also describes how to specify IT security objectives and requirements, and high level security specifications for products and systems;
- ISO/IEC 15408-2 "*Security functional components*" establishes a set of security functional components to specify security functional requirements for so-called Targets of Evaluation (TOEs);
- ISO/IEC 15408-3 "*Security assurance components*" establishes a set of assurance components to express the assurance requirements for Targets of Evaluation. It lists the set of assurance components, families and classes, defines evaluation criteria for Protection Profiles (PPs) and Security Targets (STs), and presents a scale for rating assurance for TOEs, which are called Evaluation Assurance Levels (EALs).

A number of topics are not in scope of the ISO/IEC 15408, because they are secondary to IT security or because they involve specialized techniques, including:

- The evaluation method under which the security evaluation criteria should be applied. This methodology is provided in ISO/IEC 18045 "*Information technology -- Security techniques -- Methodology for IT security evaluation*"¹⁷;
- Criteria for the assessment of cryptographic algorithms;
- Criteria related to (technical) physical aspects of IT security;
- Criteria regarding administrative security measures, which are not directly related to the IT security functionality¹⁸;
- The administrative and legal framework under which the security evaluation criteria are applied by evaluation authorities;
- Procedures for use of evaluation results in accreditation.

¹⁷ The corresponding 'Common Methodology for Information Technology Security Evaluation' (CEM) can also be downloaded from the Common Criteria Portal. It is a companion document to the CC which explains in detail the principles and processes with which the security evaluations are performed using the CC criteria.

¹⁸ Here the ISO/IEC 27000 series would be appropriate.

3) Certification

Certification for ISO/IEC 15408 has a number of advantages [2.12]:

- To allow customers to compare security functions of computer products in an objective way;
- To warrant a minimal level of confidence for security; some businesses need a minimal security level for its products (such as in financial services an EAL4+ for credit cards);
- To benefit from marketing and business opportunities by the vendors that have CC accredited products;
- To allow the governmental certification bodies to make sure those products used in their countries are secured.

However, ISO/IEC 15408 certification cannot guarantee security, it “just” makes sure that claims of the vendors about the security attributes of their products were independently verified. In other words, products evaluated against a Common Criteria standard were created according to the prescribed CC method regarding specification, implementation, and evaluation of security functions of computer products. Furthermore, the process of achieving CC certification allows vendors to restrict the analysis to certain security features, in relation to a particular set of threats and assumptions about the environment. Later versions of the same products require in principle re-testing. For example various Microsoft Windows versions were certified at a specific security level (EAL4+) without the later applied necessary security patches. This shows a limitation of the practical value of an evaluated CC configuration.

In the next subsections the specific concepts and components of ISO/IEC 15408 will be presented using the tri-partite structure of this international standard.

a. ISO/IEC 15408-1:2009

ISO/IEC 15408-1:2009 provides an overview of the three parts of ISO/IEC 15408 and defines principles, terms and core security concepts that are necessary for evaluation of IT products and services. ISO/IEC 15408 does not use the term “IT product” as this could be interpreted as restrictive in scope. Instead, it introduces the general term “Target Of Evaluation”.

The intended audience of this part of the standard (and the two other parts) consists of consumers, developers and evaluators. For consumers the CC provides an implementation independent structure in which they can express requirements for IT security measures. For developers/vendors, requirements can be based on specific customer needs, or vendors may identify a market niche to exploit. For vendors, the main goal of the security evaluation is to obtain a degree (CC certificate) that validates the security level of their products. Certificates are awarded by national schemes on the basis of evaluations that are usually carried out by commercial organisations in testing laboratories according to ISO/IEC 17025¹⁹. Table 10 shows how the three parts of ISO/IEC 15408 will be of interest to these key user groups.

¹⁹ ISO/IEC 17025:2005 “General requirements for the competence of testing and calibration laboratories”

Parts	Consumers	Developers	Evaluators
1: Introduction and General Model	Use for background information and reference purposes. Guidance structure for PPs.	Use for background information and reference for the development of requirements and formulating security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
2: Security Functional Components	Use for guidance and reference when formulating statements of requirements for security functions.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Use as a mandatory statement of evaluation criteria when determining whether a TOE meets claimed security functions.
3: Security Assurance Components	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

Table 10: Road map to the “Evaluation criteria for IT security” (ISO/IEC 15408-1:2009, p.22)

ISO/IEC 15408-1 defines and describes the concepts of Target of Evaluation (TOE), Protection Profiles (PP) and Security Targets (ST). The standard also provides the various operations by which functional (ISO/IEC 15408-2) and assurance (ISO/IEC 15408-3) components that can be tailored using the permitted operations. It also discusses what kinds of results are expected from an evaluation. Moreover ISO/IEC 15408-1 describes the organisation of components throughout the model and provides detailed information on the relationship between security objectives and security requirements. The scope of evaluation schemes and general information on the evaluation method, available in ISO/IEC 18045, is provided as well.

As this standard is filled with acronyms, we will describe the core concepts that are defined in this part of the standard:

- **Target Of Evaluation (TOE):** the IT product/system or service and its accompanying user and administrator documentation that is subject to a security evaluation.

This evaluation has to validate claims made about the TOE and it must verify the target's security features. This could be done through two forms of TOEs: a Protection Profile (PP) or a Security Target (ST).

- **Protection Profile (PP):** is an implementation-independent set of security requirements that meet specific consumer needs for a category of TOEs.
- **Security Target (ST)** and its corresponding product: is a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

A Protection Profile (PP) is a document that distinguishes security functional requirements (SFRs) for a class of security devices that are relevant for a particular purpose. The CC User Guide [2.13] gives a few examples when a PP is appropriate:

- A consumer group wishes to specify security requirements for an application type (e.g. electronic funds transfer);
- An organisation wishes to purchase an IT system to address its security requirements (e.g. patient records for a hospital);
- A government wishes to specify security requirements for a class of security products (e.g. firewalls).

Product vendors can implement products that comply with one or more PPs, and have those products evaluated against these PPs. The developers of an ST will ensure that all requirements in relevant PPs also appear in the target's ST document. Customers looking for particular types of products that meet their requirements can focus on those certified against that PP. Some other examples include: operating systems, biometrics, intrusion detection systems, PKI, trusted databases, antivirus on workstations.

A Security Target (ST) is a document that identifies the security properties of a TOE and may refer to one or more PPs. It specifies the security measures offered by the product to meet security requirements. A ST contains the TOE security threats, objectives, requirements, and a specification of security functions and assurance measures. A ST can be publicly available to allow potential customers to find out the particular security features which have been certified. It is the developer's responsibility to provide evidence that the security provisions for a TOE have been designed and implemented to meet the requirements of the CC. The TOE is evaluated against the security functional requirements established in the ST. This makes it possible for a vendor to tailor the evaluation to precisely match the intended capabilities of their IT product or service. This means that a e.g. a fingerprint scanner does not have to meet the same functional requirements as a device that provides digital signatures, and that different fingerprint scanners can be evaluated against completely different lists of requirements.

The normative annexes A and B of ISO/IEC 15408-1 define the outline structures for PPs and STs respectively (see Table 11).

Outline of a PP	Outline of a ST
<ul style="list-style-type: none"> • PP Introduction: <ul style="list-style-type: none"> - PP identification; - PP overview. • TOE description. • TOE security environment: <ul style="list-style-type: none"> - Assumptions; - Threats; - Organizational security policies. • Security objectives: <ul style="list-style-type: none"> - Security objectives for the TOE; - Security objectives for the environment. • IT security requirements: <ul style="list-style-type: none"> - TOE security requirements: <ul style="list-style-type: none"> ▪ TOE security functional requirements, 	<ul style="list-style-type: none"> • ST Introduction: <ul style="list-style-type: none"> - ST identification; - ST overview; - CC conformance claim. • TOE description. • TOE security environment: <ul style="list-style-type: none"> - Assumptions; - Threats; - Organizational security policies. • Security objectives: <ul style="list-style-type: none"> - Security objectives for the TOE; - Security objectives for the environment. • IT security requirements: <ul style="list-style-type: none"> - TOE security requirements: <ul style="list-style-type: none"> ▪ TOE security functional requirements,

<ul style="list-style-type: none"> ▪ TOE security assurance requirements; <ul style="list-style-type: none"> - Security requirements for the IT environment (OPTIONAL). • Application notes (OPTIONAL). • Rationale: <ul style="list-style-type: none"> - Security objectives rationale; - Security requirements rationale. 	<ul style="list-style-type: none"> ▪ TOE security assurance requirements; <ul style="list-style-type: none"> - Security requirements for the IT environment (OPTIONAL). • TOE summary specification: <ul style="list-style-type: none"> - Statement of TOE security specifications; - Statement of assurance measures. • PP claims: <ul style="list-style-type: none"> - PP reference; - PP tailoring; - PP additions. • Rationale: <ul style="list-style-type: none"> - Security objectives rationale; - Security requirements rationale; - TOE summary specification rationale; - PP claims rationale.
---	--

Table 11: Protection Profile (PP) and Security Target (ST) outlines

Up to now, most PPs and evaluated STs/certified products have been for IT components. The current list of certified products is available from the CC portal²⁰.

b. ISO/IEC 15408-2:2008

ISO/IEC 15408-2:2008 defines an extensive catalogue of predefined security functional components which can be used in combination as the basis for *specifying security functional components*. These that can be used to create trusted products (TOEs) reflecting the needs of customers which can be assessed in ISO/IEC 15408 security evaluations. The functional requirements are expressed in a Protection Profile (PP) by customers or a Security Target (ST) by developers which describe the desired security behaviour of a TOE.

The catalogue of security functional components is supported by detailed user notes, and is organised by means of a hierarchical structure of classes, families and components. Moreover, this part of the standard provides guidance on the specification of customized security requirements in case no suitable predefined security functional components exist. The three main stakeholders in this standard can use this part as follows:

- Consumers, select functional components to (the TOE) functional requirements that satisfy security objectives;
- Developers, create a TOE security functionality and mechanisms to meet consumer security requirements;
- Evaluators, verify that the TOE functional requirements, expressed in the PP or ST, satisfy the IT security objectives and whether a given TOE satisfies the stated requirements.

The documentation created in this phase is later used for evaluation evidences. It consists of: the TOE development and guidance documentation, life-cycle definition, configuration management, delivery, flaw remediation, development security, testing, and vulnerability assessment issues.

²⁰ <http://www.commoncriteriaportal.org/products/>

The catalogue of security functional components described in ISO/IEC 15408-2, which cover the major elements of any security product or process, is divided into eleven groups as listed in Table 12. When preparing a TOE with either a Protection Profile (PP) or a Security Target (ST) for evaluation, the author is advised to identify security functionality from this catalogue. The main contents of this part of the standard are the detailed descriptions of the Common Criteria catalogue of Security Functional Components.

Functional groups	Description
Security audit	Information related to security related activities is recognized, recorded, stored, and analysed; resulting audit records can be retrieved and examined.
Communication	Non-repudiation: the originator of a message cannot deny having sent it; the receiver of a message cannot deny having received it.
Cryptographic support	Essential management capabilities; support the general use of cryptographic keys.
User data protection	User data is protected during use, transport and storage; access to user data is adequately controlled.
Identification and authentication	Users are associated with valid and meaningful security attributes such as identity, role and integrity level; basic capabilities for the implementation of access control.
Security management	Management of security attributes, security data and security functions.
Privacy	Provide protection against discovery and misuse of a user's identity by other users.
Protection of TOE Security Functions	The management and integrity of security functions provided by the TOE; the management and integrity of data associated with the security functions provided by the TOE.
Resource utilization	Availability of TOE resources such as processing capability and storage capacity.
TOE access	Controlling the establishment of user sessions.
Trusted path/channels	Establishing trusted communication paths between users and the TOE Security Functions; establishing trusted communication channels between the TOE Security Functions and other trusted IT products.

Table 12: Groups of security functional components (ISO/IEC 15408-2:2008)

Annexes of ISO/IEC 15408-2:2008 provide explanatory information for the functional groups and are normative instructions on how to apply relevant operations and select appropriate information to document or audit.

c. ISO/IEC 15408-3:2008

ISO/IEC 15408-3:2008 describes the process of evaluating the security capabilities of a TOE through a catalogue of assurance classes, families and components and the associated actions expected of an evaluator. It defines a set of *security assurance components* based on the assurance classes that serve as standard templates to measure assurance requirements for TOEs. It also provides guidance on how to organize new assurance requirements. The degree to which a product's development and support process ensures that security objectives and requirements have been understood and met is measured using a number of assurance levels. The evaluation process is performed by an independent body and should leading to the certification of a TOE.

More specifically, this part of the standard includes:

1. Seven Evaluation Assurance Levels (EALs) that define the predefined ISO/IEC 15408 scale for rating assurance for *component* TOEs with increasingly strict assurance requirements;
2. Composed assurance packages that define a scale for measuring assurance for *composed* TOEs;
3. Individual assurance components based on assurance families and classes;
4. Evaluation criteria of PPs and STs.

The Evaluation Assurance Level (EAL) constitutes a numerical rating, from EAL 1 to EAL 7, and describes the depth and rigor of the verification process. It is not a measurement of the actual security that the TOE provides and higher EALs do not necessarily mean "enhanced security" of the TOE. It "only" means that the security assurance was more extensively verified.

The evaluation process described in this part of the standard expresses the product's security features through so-called Security Assurance Requirements (SAR). This describes the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. The requirements for particular targets or types of products are documented in the ST and PP, respectively.

Each EAL corresponds to a package of SARs that cover the complete development of a product, with a given level of rigorousness. The vendor has to provide evidence that the corresponding rigor was applied during the development and test phases. Hardware, firmware and software can be evaluated based on these EAL in accredited testing laboratories to certify the level the product or system can attain. A list of accredited companies as well as a list of evaluated products can be found on the Common Criteria portal.

Common Criteria lists seven levels with EAL 1 as the entry level and therefore the least expensive to implement and evaluate. Up to EAL 4 increasing rigor is introduced, but without the obligation to use specialised security engineering techniques. EAL 1 to 4 can be used for TOEs that were developed without specific security evaluation assurance in mind. For evaluations at the two highest levels, EAL 6 and 7, formal methods should be used such as those for functional specifications and security policies.

The governments of 10 countries²¹ mutually recognise each other's evaluations performed by testing laboratories in each other's countries, up to EAL 4. Above EAL 4 the national laboratories certify products themselves because of national security reasons [2.14]. More details on the seven Evaluation Assurance Levels are listed in Table 13.

²¹ France, Germany, Italy, the Netherlands, Norway, Spain, Sweden, the United Kingdom (as Certificate Authorizing Members) Austria, and Finland (as Certificate Consuming Members);
More information on http://www.sogisportal.eu/uk/status_participant_en.html

Level	Evaluation	Applicability	Prerequisites
EAL1	Functionally tested	Confidence in correct operation is required, but threats to security are not serious.	Sufficient to simply state the Security Requirements that must be met rather than deriving them from threats.
EAL2	Structurally tested	A low to moderate level of independently assured security is required in the absence of a complete development record.	Requires availability of design information and test results but should not demand more effort on the part of the developer than is consistent with good commercial practise.
EAL3	Methodically tested and checked	A moderate level of independently assured security is required based on a thorough investigation of the TOE and its development without substantial re-engineering.	Requires positive security engineering at the design stage but without substantial alteration of existing sound development practises.
EAL4	Methodically designed, tested and reviewed	A moderate to high level of independently assured security is required in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.	Requires positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills and other resources.
EAL5	Semi-formally designed and tested	A high level of independently assured security is required in a planned development and requires a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.	Requires security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques.
EAL6	Semi-formally verified, designed and tested	Applicable to the development of security equipment for application in high risk situations where the value of the protected assets justifies additional development costs.	Requires security engineering techniques within a rigorous development environment.
EAL7	Formally verified, designed and tested	Applicable to the development of security equipment for application in extremely high risk situations and/or where the high value of the assets justifies higher development costs.	Currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

Table 13: CC Evaluation Assurance Levels (ISO/IEC 15408-3:2008, p.14..21)

ISO/IEC 15408-3 defines eight Assurance Classes which are general groupings of security assurance requirements. Each is subdivided into a number of Assurance Families (see Table 14). Each Assurance Family has a number of assurance components at a level that is commensurate with the target environment for use²². The evaluator will consider these classes, families and components in detail when evaluating the security capabilities of a product.

Assurance Class	Assurance Family
Protection Profile evaluation	PP introduction
	Conformance claims
	Security problem definition
	Security objectives
	Extended components definition
	Security requirements
Security Target evaluation	ST introduction
	Conformance claims
	Security problem definition
	Security objectives
	Extended components definition
	Security requirements
Development	TOE summary specification
	Security Architecture
	Functional specification
	Implementation representation
	TSF internals
	Security policy modelling
Guidance documents	TOE design
	Operational user guidance
Life-cycle support	Preparative procedures
	Change Management capabilities
	Change Management scope
	Delivery
	Development security
	Flaw remediation
	Life-cycle definition
Tests	Tools and techniques
	Coverage
	Depth
	Functional tests
Vulnerability assessment	Independent testing
	Vulnerability Analysis
Composition	Composition Rationale
	Development Evidence
	Reliance of Dependant Component
	Composed TOE Testing
	Composition Vulnerability Analysis

Table 14: Assurance Classes and Family (ISO/IEC 15408-3:2008)

²² For example the Assurance Family "TOE Design" has for EAL 2 the component "ADV_TDS.1 Basic design" and for EAL 7 the component "ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation"

The three main stakeholders of this standard can use this part as follows:

- Consumers, select assurance components to specify assurance requirements. This allows them to satisfy the security objectives expressed in a PP. They also determine the required levels of security assurance of the TOE;
- Developers, meet security requirements when building a ST and interpret statements of assurance requirements and determine assurance approaches of TOEs;
- Evaluators, use the assurance requirements as a mandatory statement of evaluation criteria when they determine the assurance of TOEs and evaluate PPs and STs.

The annexes provide, among others, cross references between the EALs, composed assurance packages and the assurance components.

4) Issues & Criticisms

As already discussed earlier regarding some limitations on the value of CC certification, other issues and side-effects were identified by several authors and will be discussed in this sub-section.

The evaluation process is costly for lower EALs (often measured in hundreds of thousands of Euros) and even extremely costly for the highest EALs. A costs estimate for an EAL 3 evaluation is about 90-150K Euro with an evaluation time of around nine months [2.15]. For higher levels this is even more (EAL 4: 140-250K Euro, etc.). Independent laboratories test up to EAL4. Due to the complex and time-consuming certification process a lot of companies refrain from CC certification. It is therefore not widely used outside of government and defence markets [2.16].

The evaluation at lower levels (EAL 1 through 4) focuses primarily on an assessment of the process and documentation, “*testing the paperwork*” [2.17] not on the concrete security of the product [2.18]. Only at EAL7 a full source code analysis is required.

A vendor can restrict the scope of a TOE in order to exclude some parts of the IT product that could potentially be subjected to flaws [2.12]. In addition Dusart et al. [2.12] mention that the scope of a TOE is very static after the issuance of the certificate. Each change in the scope of the product would imply to re-evaluate the product. CC certification may also impede product development since, for example, patching can invalidate the certified assurance as well.

Wheeler [2.19] argues that CC does not really match Open Source Software (OSS). The CC was developed before the rise of OSS and agile software development models. CC does not credit mass peer review or detailed OSS code review and CC requires mass creation of documentation which is not normally the case in OSS development.

Church et al. [2.20] advise that Common Criteria evaluations should take usability of the products into account as “*the context in which security systems are used, both on the individual and the social level, has a substantial effect on the security properties of the whole system*”. Because this is currently not sufficiently covered this could lead to false perceptions what is being assured by a CC evaluation. It hands over security decisions to the user and may overestimate expectations what a user is capable of.

Finally there could be problems of interpretation. There are known difficulties in the intrinsic comprehension of the criteria, and support for security requirements elicitation and tracking is lacking [2.21] [2.22] but also regarding possible difficulties in terms of translation from English to other languages [2.12].

5) Synthesis

ISO/IEC 15408 “*Common Criteria for Information Technology Security Evaluation*”, is a three tiered standard that provides assurance that the process of specification, implementation and evaluation of security aspects of computer products has been conducted in a rigorous, repeatable and standardised manner. Such products have a defined level of assurance related to its information security capabilities and are recognized in large parts of the world.

Product evaluations have to verify the claims of the vendors about the security features of the product/system (TOE). This is done through two forms of TOEs: a Protection Profile (PP) created by customers or a Security Target (ST) created by vendors. Part 1 of ISO/IEC 15408 provides an overview and defines the key concepts, part 2 contains a catalogue of security functional components that can be used to specify and create the TOE security functionality and part 3 describes the process of evaluating the security capabilities of a TOE through a catalogue of assurance components and the required actions of an evaluator.

ISO/IEC 15408 is especially useful when a customer needs to specify security features of a product or system and this standard can assist developers with building security features into a product or system. It also helps to evaluate security features of products or systems and to support the procurement of products or systems with security features. However, a number of limitations were identified as well. The most important ones are the very costly evaluation process which takes a long time due to the complex and time-consuming certification process. Another limitation is that CC focuses on the assessment of the process and documentation instead of the concrete security of the product. Also, each change in the scope of the product or a patch applied after certification could imply a re-evaluation of the product.

It is advised to apply this standard for large or in security specialised commercial enterprises next to government purposes. For SMEs this standard can be applied when looking for already build and certified computer products. These can be found on the common criteria portal at: <http://www.commoncriteriaportal.org/products/>.

IV. Strategy of the Ministry of the Economy in the area of information security

1) 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.

2) A model for information security governance

Information security sustains the users' trust in electronic media and represents a prerequisite for the development of e-commerce.

Given the convergence of operation systems, the ubiquity of information systems and the high level of inter-connectivity, it is important to consider information security no longer as a private or personal challenge: it is definitely a matter that society is facing as a whole.

Therefore it is essential to reach every citizen and encourage the use of best practices, as well the implementation of effective and efficient security measures. A government can play a unifying role in this process, by leveraging the enormous synergistic potential underlying information systems, through providing tools for self-empowerment.

Raising awareness at stakeholders' level, providing training to government officials, mutualizing security measures on an infrastructural level, developing information and tools to conduct thorough risk analysis, etc.: all these actions will contribute to establish a culture of "information security".

This approach is economically attractive, since it promotes the ability to create protection for all parties, physical and moral. The aim is not to disempower nor create inefficient or unnecessary infrastructures. The aim is to identify necessary and proportionate security measures.

Security governance can be based on this risk assessment approach by providing a common methodology based on objective metrics and providing reliable results, always in view of the necessity and proportionality.

3) 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.

Regulators are the sixth target group. Providing business-friendly, thus effective and efficient governance approaches, is one of the priorities of the Ministry of the Economy.

4) Structures of the Ministry of the Economy

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

In 2007, the Ministry of the Economy 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 L'Étzeburg 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.

a. 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 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.

The 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*” (CNPD), 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 shopping²³, on second place regarding the proportion of people using ICT security software²⁴, first when it comes to uploading self-created contents²⁵, third in the Internet use by individuals and frequency of use²⁶ and number one when it comes to older generations using the web²⁷. Luxembourg also ranks first for the proportion of population accessing the Internet through a mobile phone *via* UMTS according to the Digital Agenda Scoreboard²⁸.

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 shape the future, and 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 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.

²³ http://ec.europa.eu/information_society/digital-agenda/scoreboard/index_en.htm

²⁴ http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisci_f&lang=en

²⁵ http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2009/sec_2009_1103.pdf

²⁶ http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF

²⁷ <http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=1.&pcode=tin00092&language=en>

²⁸ http://ec.europa.eu/information_society/digital-agenda/scoreboard/index_en.htm

b. 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*” has developed a 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.

c. 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 there 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.

References

- [2.1] ITGI (2001), "Information Security Governance: Guidance for Boards of Directors and Executive Management", IT Governance Institute - Information Systems Audit and Control Foundation, IL, USA.
- [2.2] ISO/IEC (2014), "ISO/IEC 27000:2014, Information technology -- Security techniques -- Overview and vocabulary", ISO/IEC
- [2.3] ISO (2013), "The ISO Survey of Management System Standard Certifications - 2012", ISO, Geneva, Switzerland.
- [2.4] Fenz, S., Goluch G., Ekelhart A., Riedl, B., Weippl, E. (2007) Information security fortification by ontological mapping of the ISO/IEC 27001 standard. 13th Pacific Rim International Symposium on Dependable Computing, Proceedings. 381-388, Dec. 17-19, Melbourne, Australia.
- [2.5] Neubauer, T., Ekelhart, A., Fenz, S. (2008) Interactive selection of ISO 27001 controls under multiple objectives. Proceedings of the IFIP TC 11/ 23rd International Information Security Conference, 477-491, 2008. 23rd International Information Security Conference held at the 20th World Computer Congress.
- [2.6] Ezingear, J.N., Birchall, D. (2005), "Information security standards: Adoption drivers - What drives organisations to seek accreditation? The case of BS 7799-2: 2002", Security Management, Integrity, and Internal Control, in Information Systems Book Series: International Federation For Information Processing, 193: 1-20, Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems, George Mason University, Fairfax, VA.
- [2.7] Karabacak, B., Sogukpinar, I. (2006), "A quantitative method for ISO 17799 gap analysis", *Computers & Security* 25: 413-419.
- [2.8] Van Wessel, R., Yang, X., De Vries, H. J. (2011), "Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study", *Technology Analysis & Strategic Management*, 23(8), 865-879.
- [2.9] ISO/IEC (2012), "Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, Annex SL, Proposals for management system standards", ISO, Geneva, Switzerland
- [2.10] Backhouse, J., Hsu, C., Silva, L. (2006), "Circuits of Power in creating de jure Standards: Shaping an International Information Systems Security Standard", *MIS Quarterly*, Vol. 30, Special Issue 2006, pp. 413-438.
- [2.11] Van Wessel, R. M., De Vries, H. J. (2013), "Business Impacts of International Standards for Information Security Management. Lessons from Case Companies", *Journal of ICT Standardization*, 1(1), 25-40.
- [2.12] Dusart, P., Sauveron, D., Tai-Hoon, K. (2008), "Some limits of Common Criteria certification", *International Journal of Security and Its Applications*, 2(4).
- [2.13] CC User Guide (1999), "Common Criteria for Information Technology Security Evaluation User Guide", Syntegra.
- [2.14] Kallberg, J. (2012). Common Criteria Meets Realpolitik Trust, Alliances, and Potential Betrayal. *IEEE Security & Privacy*, 10(4).
- [2.15] Brightsight (2013), "Common Criteria Guidance for Developers - Evaluation Assurance Level 4 - v1.42", Brightsight Common Criteria Explained Series, Brightsight, The Netherlands.

- [2.16] Ekelhart, A., Fenz, S., Goluch, G., & Weippl, E. (2007). Ontological mapping of common criteria's security assurance requirements. In *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 85-95). Springer US.
- [2.17] Jackson, W. (2007), "Under attack", Government Computer News, 26(8).
- [2.18] Beckert, B., Bruns, D., & Grebing, S. (2010), "Mind the Gap: Formal Verification and the Common Criteria" (Discussion Paper), Karlsruhe Institute of Technology & Universität Koblenz-Landau, Germany.
- [2.19] Wheeler, D.A. (2006), "Free-Libre / Open Source Software (FLOSS) and Software Assurance / Software Security". URL http://www.dwheeler.com/essays/oss_software_assurance.pdf, visited 23 February 2014.
- [2.20] Church, L., Kreeger, M. N., & Streets, M. (2008). Introducing Usability to the Common Criteria. In *International Common Criteria Conference*.
- [2.21] Mellado, D., Fernández-Medina, E., & Piattini, M. (2007), "A common criteria based security requirements engineering process for the development of secure information systems", *Computer standards & interfaces*, 29(2), 244-253.
- [2.22] Houmb, S. H., Islam, S., Knauss, E., Jürjens, J., & Schneider, K. (2010). Eliciting security requirements and tracing them to design: an integration of Common Criteria, heuristics, and UMLsec. *Requirements Engineering*, 15(1), 63-93.

3 Technical tools for digital trust

This chapter presents technical tools that are fundamental to ensure digital trust in today's usage of the Internet. Three security techniques and related technologies have been selected as relevant for Luxembourg and are presented: cryptographic tools, Identity and Access Management (IAM), and Mobile Device Management (MDM). Indeed, to protect information, cryptographic tools are used for both data at rest and in transit. Then, Identity and Access Management ensures that only authorized entities can access such information. Lastly, Mobile Device Management is a tool that helps in a secure way of dealing with the growing number of mobile devices that customers use for both business and personal use.

I. Introduction

Big data, Cloud Computing, social network computing, “The internet of things”²⁹ and enterprise mobility (so called “gang of five”) have the potential to disrupt our business environment because of their transformational nature on products, services and processes. They are *the* topics on numerous websites found on the Internet today. Their combination reinforces each other in significant ways and fundamentally changes the way information must be secured.

The core of the “gang of five” consists of the Cloud with its Big Data, at the edges are mobile devices where ubiquitous sensor registrations, and social media interactions make up the connections from one edge point to the other. In addition to the business opportunities these developments offer, digital trust (i.e. privacy and information security) is vital in order to sustain this socio-technical transformation. Therefore, three tools that underpin this transformation will be looked into more detail: encryption, Identity and Access Management, Mobile Device Management.

- The steady increase of the amount of data managed by organisations, much of which are confidential, and the access by mobile users and cloud applications require proper information security techniques. Cryptographic tools help to guarantee an adequate trust level for such data, both in transit and at rest.
- For organisations the management of identities and granting access to computer systems becomes more and more complex because traditional in-house Identity and Access Management (IAM) infrastructures are complemented to support those from mobile devices and Software as a Service (SaaS), such as social media platforms. IAM is one element of the base technology to build digital trust into the organisations' data and business processes.
- Organisations need to be able to deliver apps to consumers and employees on privately owned “Bring Your Own Device” (BYOD³⁰) devices, quickly and securely. To guarantee digital trust in such heterogeneous environments, mobile device management is to ensure that data created and used by such apps is adequately protected.

²⁹ A term attributed to RFID pioneer Kevin Ashton who posits a world of ubiquitous sensors in numerous devices plugged into the Internet.

³⁰ BYOD is part of the ‘consumerization of IT’ and blurs the line between personal and professional life.

II. Cryptographic tools

A trusted computing environment is not complete without duly consideration of cryptographic tools. There are many reasons why someone or an organisation might use cryptographic tools:

- To protect personal or business secrets and intellectual property;
- To protect financial data (credit card numbers, etc.);
- To protect communication from being changed during transmission;
- To protect communication from unauthorised access;
- To authenticate payments;
- To avoid espionage or sabotage;
- Etc.

Basically these relate to the information security concepts of confidentiality, integrity, authentication, authorisation and non-repudiation (see Table 15).

Concept	Description of cryptographic security services
Confidentiality	Ensure that information is not disclosed to unauthorised parties, even if the network traffic is sniffed at the packet level.
Integrity	Ensure that data has not been altered in an unauthorised manner since it was created, transmitted or stored.
Authentication	Verify the identity of a user or system using digital signatures for example.
Authorisation	Provide permission to perform a security function or activity by means of a key or password that allows access to some resources.
Non-repudiation	Prevent an entity from successfully denying involvement in a previous action by means of digital signatures.

Table 15: Cryptographic security services [3.1]

Encryption refers to the process to conceal data by changing it in such a way that it can only be reverted, read and understood by recipients for whom the data is intended. Unencrypted data is referred to as the *plaintext* and encrypted data is referred to as *ciphertext*. Trust can be increased by encryption algorithms, also known as *ciphers*, which generate ciphertext in a process called encrypting or encoding. The ciphertext must not be easily decrypted or encoded to the original plaintext. In order to ensure confidentiality of information, cryptographic tools can be used to provide high levels of digital trust to wired and wireless communication (data in transit), and storage on any kind of media (data at rest).

The required level of trust and security for encrypted data are always relative to the conditions under which it will be used and the task it is intended to accomplish. This involves the kind of data to protect, such as medical records of patients, and the type of operations to be carried out, such as the transfer of sensitive business information between sites. Cryptographic security services can be fulfilled using a large number of different ciphers. In many cases, the same ciphers may be used to provide multiple services.

The application of encryption can be traced back to the ancient Egyptians, Arabs and Romans who used simple codes to protect information. The best known early example of cryptography is the so-called "Caesar cipher", named after Julius Caesar who has used it for communication secret messages. This encryption algorithm, or cipher, is very basic and consists of just shifting each letter

in the alphabet by some arbitrary number, which is called the *key* (or substitution cipher). It results in simply exchanging one letter with another based on the key shift (see Table 16). As an example “Trust” is coded into “Aybza” when the key is 7. The person sending a message has to inform the person receiving that message what cipher and key are used (in this case the Caesar cipher and “7”) to decrypt the ciphertext into plaintext.

Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alphabet with Caesar cipher and key = 7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g

Table 16: The Caesar cipher algorithm (shift cipher)

Obviously the Caesar cipher has a number of weaknesses. For example, using a single key preserves the letter frequency and thus provides a big clue since e, t, a, o are the most common English letters.

1) Symmetric and asymmetric encryption

As time has progressed, encryption algorithms by which data is protected have become more complex and secure. The security and trust of a cryptographic tool is considered strong as it possesses the following properties:

- It produces ciphertext which appears random to all standard statistical tests;
- It has a large key space, meaning that there are very many possible encryption keys (preferably over 10^{100}) with keys up to 60 characters in length;
- The security of a strong system resides with the secrecy of the key.

There are two general categories for key-based encryption which are called symmetric and asymmetric algorithms for cryptography. Both categories are extensively used in *data protection* by encrypting, for example, emails sent over the Internet and files stored on removable media. A third type of algorithms refers to cryptographic hash functions which do not require keys and are primarily used to check *data integrity*.

Symmetric-key algorithms (sometimes called secret-key algorithms) use the same cryptographic keys for both encryption and decryption. This kind of encryption algorithms are not computationally intensive compared to asymmetric encryption. In principle, the keys are identical and represent a shared secret between two (or more) persons. So the Caesar cipher is a symmetric-key algorithm because the same algorithm and the same key are used to carry out both encryption and decryption. The sending person encrypting the message must give the key to the receiving person before it can be decrypted. This key must be sent separately from the ciphertext to the recipient. This represents a major drawback, because if someone intercepts this key, that person is also able to decrypt the message. Another drawback, in comparison to asymmetric encryption, is that the chance of disclosure of the secret key increases with the number of trusted parties involved.

Symmetric-key algorithms come in two forms: 1) stream ciphers, and 2) block ciphers. Stream ciphers encrypt the bytes of a message one at a time, whereas block ciphers take a number of bits (often 64 or 128) and then encrypt it. A well-known symmetric-key block cipher, that has been approved by the US National Institute of Standards and Technology (NIST) in 2002, is the “Advanced

Encryption Standard, AES" [3.2] which is also included in ISO/IEC 18033 [3.3]. AES encrypts and decrypts data in 128-bit blocks, using 128, 192 or 256-bit keys. AES superseded the Data Encryption Standard (DES) [3.4] which was published in 1977. DES was considered strong, until in the late 1990s DES encrypted messages could be broken by computers in matters of days. With DES there are "only" 2^{56} (about 10^{17}) keys possible. Instead of AES also Triple DEA [3.5] can be used which encrypts and decrypts data in 64-bit blocks, using three 56-bit keys.

Asymmetric-key algorithms, also known as public-key algorithms, were first developed in the 1970s to solve the problem of securely exchanging keys. This category of encryption algorithms require two separate keys, one is the private key and the other the public key. They form a pair that is mathematically linked but calculating the private key from the public key is, with the current technology and mathematical knowledge, practically impossible.

- The public key can only be used to encrypt plaintext or to verify a digital signature;
- The private key can only be used to decrypt ciphertext or to create a digital signature.

This allows a person to freely distribute its public key to others that want to *securely communicate* without the worry of compromise. Once a sender has encrypted a message with the public key, it cannot be decrypted. Unlike with identical (shared) keys, in the asymmetric key system only the recipient can decrypt that message with its private key. Asymmetric key algorithms do not require a secure initial exchange of the secret key between the parties, which is a major advantage compared to symmetric key algorithms. Furthermore, it is computationally easy to generate a public and private key-pair. The private key shall never be distributed, therefore, a third party cannot intercept a key to decrypt messages or create digital signatures.

Next to data protection, asymmetric-key cryptography is also used to generate *digital signatures* for authentication of the author of the documents. A message which is signed using the sender's private key can be verified by anyone who has access to the sender's public key. As long as the private key has remained secret to the signer and it is not compromised, it is most likely that the message came from the person associated with the public key. This process is also called message *authentication* and verifies the sender's identity. In addition it ensures the message has not been manipulated and/or corrupted (*integrity*), because any change in the message would result in changes to the encoded message summary (also called the digital fingerprint).

In asymmetric-key cryptography, the public *key distribution* is performed by public key servers. When someone generates a key-pair, the private key is kept secure and the public key is uploaded to a server that is accessible by anyone who wants to send the private key owner an encrypted message. These public key servers are part of a public-key infrastructure (PKI), in which one or more third parties, known as certificate authorities (CA) certify the ownership of key-pairs.

There are many asymmetric-key implementations and one of the first practicable is based on the RSA algorithm [3.6] for cryptographic tools (named after, and patented by, its inventors, Rivest, Shamir and Adelman). This algorithm relies for its security on the difficulty of factoring large prime numbers. It is currently used with key sizes of 1,024 to 4,096 bits (as a 768 bit key has been broken in 2009)³¹. Asymmetric-key algorithms are fundamental security components in many applications and Internet protocols, such as Pretty Good Privacy (PGP) and the Transport Layer Security (SSL/TLS). These implementations provide both data encryption, digital signatures and key distributions and are, therefore, called hybrid cryptosystems.

³¹ <http://en.wikipedia.org/wiki/RSA-768#RSA-768>

Symmetric key algorithms are, by and large, much less computationally intensive than asymmetric key algorithms. For that reason, it is common to exchange a symmetric key using an asymmetric (key-exchange) algorithm and subsequently transmit data using that key and a symmetric key algorithm. In Table 17 the advantages and disadvantages for the two classes of ciphers are summarised.

Cipher	Primary characteristics	Advantage	Disadvantage
Symmetric Key Encryption	One key to encrypt and decrypt. All users share the same key.	Computational easy (fast).	Securely distribution of keys is cumbersome.
Asymmetric Key Encryption	Separate keys to encrypt and decrypt. Public key is shared with everyone. Private key is kept secret.	Fewer key distributions issues. Enables authentication and digital signatures. Can be easily used for one-shot communication.	Computational more complex (slow). Not suitable for bulk encryption. Public key must be validated whether it belongs to the person it specifies.

Table 17: Advantages and disadvantages of Symmetric and Asymmetric Key Encryption

Hash functions, also called message digests or one-way encryption, are a third type of cryptographic algorithms that do not require keys. These functions generate a relatively small digest (the hash value or checksum) from a (possibly) large input, in such a way that is very hard to find an input that will produce a given output. Hash functions are used as building blocks for key management and include the following security services [3.1]:

1. To provide message authentication codes;
2. To compress messages for digital signature generation and verification;
3. To derive keys in key-establishment algorithms;
4. To generate deterministic random numbers.

The hash value represents the *digital fingerprint* of the contents of a message. This fingerprint can be used to check whether a message has not been modified by a virus, attacker or by any other means. With hash algorithms there is an extremely low probability that two different plaintext messages will yield the same hash value. Well known cryptographic hash functions in use today include:

- MD2 – Message-digest 2, is a byte-oriented algorithm that generates a 128-bit (16-byte) hash value from an arbitrary-length message, designed for smart cards. It was developed by Ronald Rivest in 1989 and although MD2 is no longer considered secure it is still in use in PKI implementations.
- MD5 – Message-digest 5, is the successor of an earlier hash function (MD4) and was also developed by Ronald Rivest in 1991. It is a widely used cryptographic hash function, but has suffered from successful attacks as well.
- SHA-1 - Secure Hash Algorithm 1 is designed by the National Security Agency (NSA) and has been published in 1995. It produces a 160-bit (20-byte) hash value and is the most widely used of current SHA hash functions. SHA-1 is being employed in numerous applications and

protocols (such as SSL/TLS, PGP, SSH, and IPsec - see section 3.1.2). Because of reported weaknesses in SHA-1 it is advised to use SHA-2 for future cryptographic tools.

- SHA-2 - Secure Hash Algorithm 2, also developed by the NSA, consists of a set of six hash functions with digests that are 224, 256, 384 or 512 bits. It has not been successfully attacked yet.

The most important international standards related to cryptography, which include symmetric and asymmetric ciphers, are listed in Table 18.

Standard	Description	Multipart
ISO/IEC 9797:2011	Message Authentication Codes (MACs)	3
ISO/IEC 9798:1998..2010	Entity authentication	6
ISO/IEC 10116:2006	Modes of operation for an n-bit block cipher	-
ISO/IEC 11770:2006..2010	Key management	5
ISO/IEC 13888:2009..2010	Non-repudiation	3
ISO/IEC 14888:2006..2008	Digital signatures with appendix	2
ISO/IEC 18033:2005..2011	Encryption algorithms	4
ISO/IEC 19772:2009	Authenticated encryption	-

Table 18: ISO/IEC standards dealing with cryptography (non-exhaustive list)

2) Common Uses of Encryption

In this subsection we will look into two specific applications of encryption related to *data in transit* and *data at rest*. To securely connect to digital resources in case of data in transit, Virtual Private Networks (VPN) are common technical solutions using encryption technologies. For data at rest encryption solutions can be applied at various levels, from individual files containing sensitive information to encrypting complete information systems.

a. Virtual Private Networks: data in transit

Encryption provides a means to securely transmit information between two computer systems. Encryption technologies are used in Virtual Private Networks that are built on top of existing physical networks. A VPN device establishes a virtual point-to-point connection with encrypted data traffic using an asymmetric-key algorithm. One can distinguish two types of VPN: 1) remote-access where an individual computer is connected to a network, and 2) site-to-site where two separate networks are connected.

Remote-access VPNs provide secure remote access to organisations' resources, such as the Intranet of a company. It is used in work from home utilities that allow remote users to connect from home or any other place *via* the Internet by creating an encrypted path to that network. Site-to-site VPNs provide the possibility to share one cohesive virtual network between geographically disparate offices. Site-to-site VPNs can also be used to connect two similar networks over a dissimilar middle network (e.g. two IPv6 networks over an IPv4 network).

To position the various VPN protocols, the Internet Protocol Suite (commonly known as "TCP/IP"), which is used for network communications throughout the Internet, will be shortly described. TCP/IP communications are composed of four interoperating layers. When data is transferred across

networks, it is passed from the highest layer through intermediate layers to the lowest layer. Each lower layer adds layer-specific information, such as addresses. The data from one layer is encapsulated in a larger container by the layer below it. The four TCP/IP layers, from highest to lowest, are listed in Table 19.

TCP/IP layer	Description
Application layer	Sends and receives data for particular applications, such as HyperText Transfer Protocol (HTTP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP).
Transport layer	Provides services (either connection-oriented or connectionless) for transporting application layer services between networks and can optionally assure the reliability of communications. Most common examples are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
Internet layer or IP layer	Routes packets across networks. The Internet Protocol (IP) is the fundamental network layer protocol for TCP/IP.
Link layer or network interface layer	Processes communications on the physical network components. The best-known example is Ethernet.

Table 19: The four TCP/IP layers [3.7]

A security control at a higher layer cannot provide protection for a lower layer, because the lower layer performs functions of which the higher layer cannot be aware. Therefore, security controls exist for network communications at each layer of the TCP/IP model.

- The application layer consists of the actual application data. Separate controls must be established for each application. Security protocols at the application layer include OpenPGP and Secure Shell (SSH) that encrypt application related data³². While application layer controls can protect application data, it cannot protect information such as IP addresses because this information exists at a lower layer.

Most VPNs provide security by the use of tunneling protocols that allow users to use a Web browser to securely access multiple network services, including protocols and applications that are not web-based. To date, many VPN implementations that use asymmetric encryption algorithms are available at these three TCP/IP layers.

- The transport layer provides security at the layer responsible for end-to-end communications. Controls at this layer can be used to protect the data in a single communication session between two hosts. The most common use for transport layer protocols is securing HTTP traffic *via* the Secure Sockets Layer / Transport Layer Security (SSL/TLS)³³ protocol for communications with individual HTTP-based applications. Not surprisingly, the SSL/TLS portal VPN is the most commonly used VPN as transport layer security control. SSL portal VPNs work over TCP port 443 for SSL-protected HTTP. To the user, an SSL portal VPN is a Web site, with URLs that typically use the "https://" and with provides additional services after user authentication. It offers ease of use and versatility because they include the SSL/TLS protocol, which is used in all standard Web browsers, so

³² See <http://www.openpgp.org> and for and open version of SSH <http://www.openssh.com/>

³³ SSL refers to all versions of the SSL protocol as defined by the IETF, and TLS refers to versions 3.1 and later of the SSL protocol. TLS 1.0 is the same as SSL 3.1 and the current version is TLS 1.2.

the client usually does not require configuration by the user. Because IP information is added at the network layer, security controls at this layer cannot protect it.

- The network layer protects network communications at the layer that is responsible for routing packets across networks. At this layer, controls can be applied to all applications because they are not application-specific. The Internet Protocol Security IPsec VPN is a commonly used network layer security control for protecting communications. Since IP information (e.g., IP addresses) is added at this layer, the controls can protect both the data within the packets as well as the IP information for each packet. An alternative is the SSL/TLS tunnel VPN that allow remote users with Web browsers running active content to access the network protected by a VPN gateway. These VPNs have much more capabilities and services than SSL portal VPNs. SSL tunnel VPNs can connect from locations where an IPsec VPN has problems with firewall rules or Network Address Translation.
- The data link layer sends the accumulated data through the physical network. The data is subsequently passed up through the layers to its destination. Data link layer controls are applied to all communications on a specific physical link, such as between a modem connection to an Internet Service Provider. Because of this, data link layer controls cannot protect connections with multiple links, such as establishing a VPN over the Internet. Common examples of VPN protocols at the data link layer are the Point-to-Point Tunneling Protocol (PPTP) and the Layer 2 Tunneling Protocol (L2TP).

All these VPN technologies are complementary and address separate network architectures and business needs. Depending on its implementation and configuration both *SSL/TLS* VPNs and *IPsec* VPNs can provide any combination of cryptographic security services listed in Table 15. Network layer VPN protocols are not application-specific and make trusted communications possible without modifying any applications. However, network layer VPNs provide less control and flexibility for protecting specific applications than transport layer ones. VPNs can mitigate risks of transmitting information over networks but one must be aware that any VPN implementation may have flaws in algorithms or software that attackers can still exploit.

b. Storage encryption technology: Data at rest

Encryption of data on storage devices, such as hard disks or removable media can be applied at various levels of granularly, such as an individual file up to encrypting all data on such a device. The appropriate encryption solution depends upon the location, amount and type of the information and the threats to be mitigated. Common types of storage encryption technologies are:

- Full disk encryption;
- Partition and virtual disk encryption;
- File/Folder encryption.

Full disk encryption is sometimes used in conjunction with File/Folder encryption to provide an even more secure and trusted environment. Conventional File/Folder encryption allows different keys for different portions of the disk. Because individual files stored on the disk can be encrypted with separate keys, an attacker cannot extract information from still-encrypted files and folders even if the full disk encryption has been compromised.

Full disk encryption

Full disk encryption (FDE) is a technology that encrypts every bit of data on a disk. Access to its data is allowed only after successful authentication. This encryption technology, using symmetric-key

algorithms, is commonly used for laptop computers but has also its purpose on desktop computers. FDE comes in two forms: software based and hardware based. A difference between software and hardware based FDE is that software-based FDE can be centrally managed and hardware-based FDE is usually only managed locally.

FDE software typically uses a special authentication environment. When at start-up, the computer low level software (BIOS) attempts to access the Master Boot Record (MRB) it is re-directed to a pre-boot kernel. This pre-boot environment consists of a small, highly secure Operating System (OS) that has been locked down and hashed using system variables to verify the kernels' integrity. Authentication is preferably carried out with two factor authentication such as a PIN with smartcard or password with biometrics. When authentication is successful the computer accesses the original MBR and normal operation commences. The FDE software decrypts and encrypts the necessary sectors of the hard drive as needed with almost no latency. When a computer has been booted and the full OS is loaded, FDE provides longer protection for the unencrypted information. The OS and/or supporting tools are now required to protect the decrypted information. The exceptions to this are often the swap space (pagefile) and when the computer is in a hibernation mode as most FDE products also encrypt the hibernation file³⁴.

FDE hardware can consist of hardware integrated in the storage device or hardware located elsewhere, such as an external disk controller. Hardware designed for this purpose should achieve better performance than FDE software implementations. Because the hardware is in principle transparent to the OS, it has no impact on the disk performance and thus works with any OS. The most common type of integrated FDE hardware is called *self-encrypting drives*. Because the encryption key cannot be separated from the disk controller, it is therefore not available to any virus in the OS. Some hardware-based FDE systems can truly encrypt an entire boot disk, including the MBR.

Partition and virtual disk encryption

Partition encryption relates to the encryption of an entire logical storage unit of a storage device. This process can also be applied on volumes³⁵ and is consequently called volume encryption. This type of storage encryption is used on hard disks and volume-based removable media, such as external hard disks and USB flash drives. Encryption of boot and system partitions is in essence a special form of FDE. Virtual disk encryption relates to encrypting a dedicated file that is called a container. This container, which resides within a partition or volume, can hold folders and files and is mounted as a (virtual) disk. Virtual disk encryption is used on all types of end-user storage devices. Examples are boot, system, and data volumes on a desktop computer, and an USB flash drive formatted with a single file system. Access to the data a partition, volume or container is provided only after successful authentication.

Virtual disk encryption has advantages over partition encryption. First of all containers are portable and partitions are not. Furthermore, virtual disk encryption can be applied when partition-based removable media needs to have both protected and unprotected storage. In such a case the partition can be left unprotected and a container with trusted data is stored onto the partition or volume.

File/Folder encryption

³⁴ See http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software#Layering for possible features

³⁵ A volume (or logical drive) is a storage area with a single file system, typically (although not necessarily) resident on a single partition of a hard disk

File/Folder encryption relates to encrypting individual files, or folders containing files, on a storage medium. Many third-party programs offer this functionality and methods for encrypting file and folder data are sometimes included in the file system of the OS. Again, access to the encrypted data is permitted only after proper authentication is provided. File/Folder encryption has the advantage that it allows granular file-based key management and access control, because each file can be encrypted with a separate encryption key, which can be enforced by public-key cryptography.

Although File/Folder encryption and virtual disk encryption look similar, both the encrypted folder and container contain and protect multiple files, there are differences. The files and folders inside the container cannot be seen until it is decrypted. File/folder encryption is more transparent because anyone with access to the file system can view the names of the encrypted files and other metadata, such as directory structures, file sizes and modification timestamps which themselves could provide valuable information to attackers. This same weakness of File/Folder encryption is true in comparison to full disk encryption.

3) Synthesis

The use of cryptographic tools can provide a higher level of trust when sending and receiving information by ensuring that the source and contents are verified. Digital signatures and message fingerprints provide reasonable assurance that the file containing the information originates from the expected party and that it has not been changed. In this sense VPNs are very valuable tools for data in transit because they provide the following security services:

- Confidentiality: scrambles data using encryption algorithms, so that even if the network traffic is sniffed at the packet level it cannot be deciphered;
- Authentication: allows uniquely identifying the sender so that one can verify data transfer is trusted;
- Integrity: verifies that there has been no tampering of the message data during transit.

Encryption is also a valuable tool for data at rest, stored on hard disks or removable media. It can be applied at various levels of granularly, from single files to complete file systems. Depending on the requirements, full disk encryption may be applied. In such a case the decision whether or not to encrypt individual files is not left up to users' discretion. Also for removable media data encryption tools are worthwhile because without the knowledge of the cryptographic key renders the contained data on USB flash drives useless.

To make this all work organisations need to ensure that access to keys used in storage encryption is secured and properly managed. Therefore, organisations should use centralised management for all deployments of storage encryption. This includes policy verification and enforcement, key management, authenticator management and data recovery.

III. Identity and Access Management

Identity and Access Management (IAM) is an information security function that facilitates digital trust and deals with identifying individuals in a system and controlling appropriate, safe access to protected resources within that system. It associates user rights and restrictions with the established identity so that the right individuals can access the right resources at the right time under the right circumstances. In other words it deals with the 'who', 'what', 'when', 'where' of access to IT resources. At the core of any identity management system are policies that define which users and devices are allowed on the network and what users can carry out, depending on their functional role, the type device, time, location, and possibly other factors.

The importance of IAM for information security management is reflected in a separate clause of ISO/IEC 27002:2013 (see Table 8) and a predefined security functional component of ISO/IEC 15408-2:2008 (see Table 12)³⁶. Furthermore, ISO/IEC 24760-1:2011 [3.9] provides a framework for identity management. It defines related terms of identity and identity management and specifies its core concepts and their relationships. In this same series ISO/IEC 24760-2 and ISO/IEC 24760-3 are in preparation. The second part will provide an identity management reference architecture and requirements, and the third part will provide guidance for good practices for administrating identity management systems. Also a framework for access management is being developed will be part of ISO/IEC 29146 (expected end of 2015). Its importance is underlined by the increasingly heterogeneous technological environments (see Figure 5), caused by Platform as a Service (PaaS) and SaaS developments, and increasingly demanding compliance requirements to prove that company data can be trusted and that it is not at risk for being misused or unintentionally disclosed.

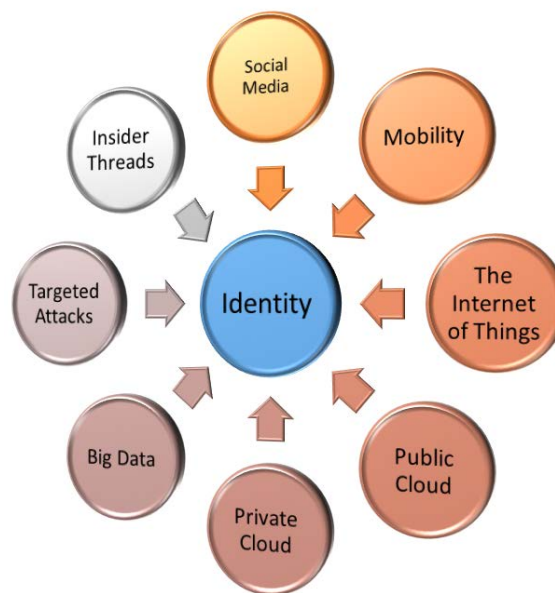


Figure 5: Identity is at the core of current trends

³⁶ Also other types of specifications have detailed sections on IAM. For example NIST SP 800-53 specifies 30 controls in this field: Technical Identification and Authentication controls: IA-1 to IA-8; Technical Access Control: AC-1 to AC-22

Typical cases for Identity and Access Management fall into three categories [3.8]:

- Portal-based access for large populations of users;
- User access to cloud-based services;
- Business partner access and application integration.

The notion of the traditional network perimeter of an IT data centre, which has been carefully constructed with firewalls and VPNs in the last three decades, is no longer a viable approach. Since users and their IT resources are literally everywhere (both inside and outside the corporate network) organisations should *adopt identity as the new security perimeter*. By properly using IAM technology, employees, partners and customers can have authorised access to data and applications any time, any place and from any device. Such access requires secure and trusted IAM that works across all platforms.

IAM technology initiates, captures, records and controls user identities and their related access permissions in an automated way. Access privileges are granted based on the organisation's policy and users and/or services are properly authenticated, authorised and audited. In this context:

- Authentication is the process of confirming the correctness of someone's claimed identity;
- Authorisation is the approval, permission or empowerment for someone to do something;
- Auditing is the process of recording CRUD³⁷ activities of data used by the applications.

For security reasons, IAM products should run on a dedicated server, either on-premises or in the cloud. Because of the developments described in the introduction of this chapter, the latest IAM products put special attention on managing mobile access. Typically the latest IAM tools allow to:

- Define and manage enterprise-wide user roles and associated entitlements in a comprehensive access control administration;
- Authorise access requests for new hires, employees who have changed positions and temporary staff;
- Provide trusted authentication mechanisms to assure each user's identity in physical, virtual, and cloud environments. This includes identity federation that passes authentication information across business and technical boundaries;
- Provide authorisation to access IT assets, both on-premise, in the cloud for SaaS resources and mobile users based on the access control administration;
- Administer the access controls in directory services (such as Active Directory and OpenLDAP);
- Simplified secure (single) sign-on processes;
- Self-service request-driven provisioning in areas such as enrolment and password resets;
- Provide privileged access levels capabilities for IT staff;
- Audit logging and reporting capabilities (e.g. to demonstrate compliance regarding user activities and their associated access privileges).

IAM is also offered as a service in the cloud and it is predicted [3.10] that IAM security SaaS will be around \$1.4 billion in 2016.

³⁷ CRUD stands for: Create, Read, Update and Delete which are four basic activities on data.

1) Business rationale

For several reasons organisations are investing in new IAM technologies that surpass a pure security rationale. Identities are not only vital to protect but also to support companies in growing their business and improve customer satisfaction. The following reasons can be identified:

- Cost savings - Because of the constant pressure for cost reduction, organisations have to reduce their IT administration costs. IAM technologies help to lower Identity and Access Management costs because of saving time and money by automating manual processes;
- Compliance - Organisations face increasingly demanding legal and regulatory requirements to meet digital trust. They have to show who had access to what and when, and what was done with the information. IAM helps to manage and improve compliance and reporting;
- Security - IAM technologies assist in enhancing security by separation of duties and signalling over-privileged access rights. It helps to protect against insider threats and external attacks thereby adding to more digital trust. IAM also forms an important element of forensic investigations;
- Administrative - IAM can be applied to check Service Level Agreement (SLA) conformance and to perform role optimisations.

Furthermore business enabling reasons include:

- Flexibility - IAM allows simplified integration of services including centralised user access to SaaS and mobile endpoints. It can also make employees productive wherever they are;
- Business - Deliver secure new business services contributing to a better user experience;
- Marketing - Identity customer tracking and tracing data for (near) real-time business intelligence usage;
- Analysis - A new field, related to Big Data, is “identity analytics” has it applications in the security, administrative and commercial domains.

A number of the most important good practices access controls can be derived from the ISO/IEC 27002 or NIST SP800-53 [3.11] standards:

- Implement least privileged access (need to use and need to know) with unique user IDs and ensure that user accounts are immediately removed when their employment status ends;
- Users should be aware of their responsibilities in maintaining effective access controls, particularly regarding password usage and the security of mobile equipment, such as USB flash drives;
- Periodically re-assess users’ access rights to prevent over-privileged users. When users’ functional roles change, additional access rights are granted and old one’s are often unnecessary kept (leaving users with more than required access rights);
- Setup a fine-grained access control for administrators on appropriate systems and for necessary activities only. Check related activity log files by an independent party.

To secure the fragmented IT environment, more and more companies are implementing a centralised IAM service which controls access to every application or service regardless of the end-user device and its location. In other words, IAM facilitates the new perimeter control. In the past, this was very difficult as applications required their own user credentials. However, a number of open standards have been developed which makes this IAM technology possible. The Internet Engineering Task Force (IETF) developed SCIM 1.1 for cross-domain Identity Management to make managing user identities in cloud-based applications possible. Other open standards are available for exchanging authentication

and/or authorisation data between identity providers and service providers, such as OpenID, and OAuth 2.0.

2) From RBAC to ABAC

Role-based access control (RBAC) is a traditional approach to restricting system access to authorised users, based on the various roles related to their job functions. The permissions to perform particular computer-system functions are assigned to specific roles. With the advent of cloud and mobile endpoints the RBAC approach is no longer sufficient to securely and effectively grant user access to digital resources. Next to the role of a user, other behavioural characteristics of users and contextual factors must be incorporated into the identification and access decision to guarantee information security and digital trust. These additional attributes may include device identity and type, location (e.g. IP addresses, on/off premises, city, country), entity (e.g. credit card, debit card), transaction types, etc. One can say that this attributed-based access control method (known as ABAC) is a generalisation of RBAC [3.12]. NIST defines ABAC as a logical access control method where authorisation to perform a set of operations is determined by evaluating attributes. These attributes are associated with a subject, object, requested operations, and, in some cases, platform conditions that are evaluated against policy, rules, or relationships that describe the allowable operations for a given set of attributes.

The standard that implements ABAC is XACML 3.0, the eXtensible Access Control Markup Language [3.13]. This standard has been developed by OASIS, a consortium for e-business and web service standards. XACML defines an access control policy language implemented in XML and a processing model that describes how to evaluate access requests according to the rules defined in policies. RBAC can also be implemented in XACML as a specialisation of ABAC. The advantage of such an approach is that the client is decoupled from the access decision and authorisation policies can be updated any time to affects all users immediately.

Another important OASIS standard in this respect is SAML [3.14], which stands for Security Assertion Markup Language. This open standard is an XML-based data format for exchanging authentication and authorisation data between parties both within one organisation and between organisations. It is used in particular between an identity provider and a service provider for web browser Single Sign-On (SSO). SAML 2.0 does not specify the authentication method at the identity provider. It may use a simple username and password combination or more advanced ones such as multi-factor authentication.

3) Synthesis

Identity and Access Management is moving to the next level of maturity. Because of the fading of the traditional network perimeter by cloud adoption, user mobility, and endpoint diversity, new demands are put on IAM tooling. The IAM capabilities increase the level of digital trust because it gives assurances of each user's identity to access IT resources (hardware, software and data) both on-premise and in the cloud, thereby protecting customer information. The value of IAM transcends the traditional functions of provisioning users' access to digital resources and encompasses new business opportunities, increases security, eases the burden of compliance, and increases business efficiency.

IV. Mobile device management

1) Mobility

The massive increase in use of mobile devices has changed the role of IT, as mobility impacts how businesses acquire and interact with customers. Organisations no longer can prescribe what users do with IT, because customers and business partners expect to do business how and when they want to, using mobile devices with a variety of brands and mobile operating systems. Furthermore, organisations need to be able to deliver apps to consumers and employees securely and quickly, and provide an engaging customer experience that will keep them coming back to do more business.

Moreover, consumer technology evolves much faster than traditional enterprise technology. The expectations of staff have changed as they want to use their own mobile devices for enterprise access (BYOD). BYOD is the trend that new IT gadgets emerge in the consumer market first and then are disseminated into business and government organisations. Staff becomes more and more demanding and they expect their organisations to provide many of these innovations close in capability.

This means that data and functions are moving closer to the user and out of the traditional control of the enterprise, as described in the section on IAM. In a way, client-server computing has been re-invented and has now become mobile-cloud. *“The history of computing is about emancipating the computer from the box, from the mainframe and its architecture out to distributed computing and now into mobile computing, where we’re pushing more of the functionality out to the edge”* (transcript, Chris Howard³⁸). This new way of working can be secured and managed, only different from what used to be.

In addition, information security and digital trust can be compromised since endpoint devices, such as smartphones and sensors in automobiles, create massive amounts of data. A few examples of “The internet of things” are GPS location, IP address, camera, microphone, tri-axis accelerometer, gyroscope, magnetometer, compass and sensors that monitor temperature, air pressure, humidity, ambient light, proximity, and fingerprints. It is estimated³⁹ that the current amount of smartphones is 2 billion and 9 billion computing devices connect through the Internet (Figure 6). By 2020 it is expected that as many as 100 billion computing devices will be connected to the Internet and corporations will be managing 50 times the data they do currently⁴⁰.

³⁸ <http://www.gartner.com/technology/research/nexus-of-forces/>

³⁹ http://www.pspinfo.us/FileLibrary/MG2013_E03_Accenture.pdf

⁴⁰ <http://www.coqizant.com/smac>

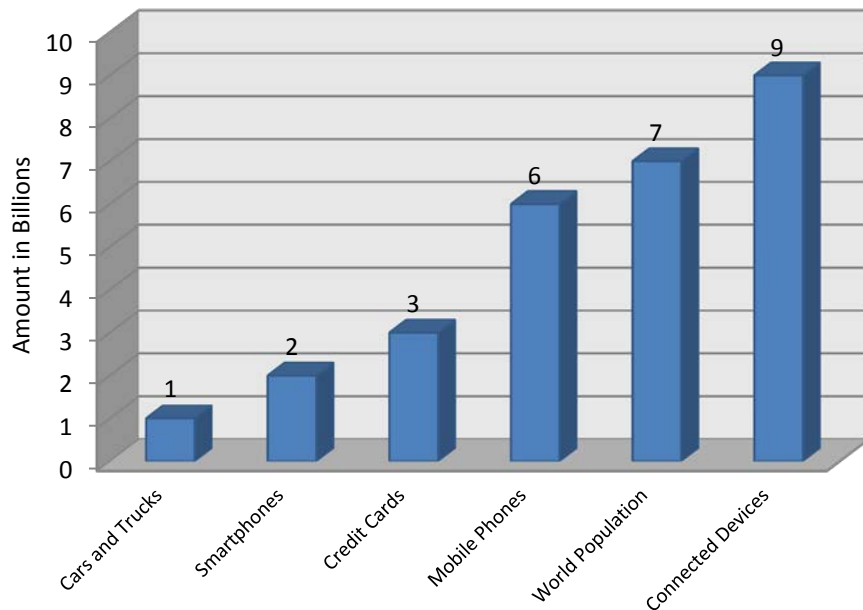


Figure 6: The scale of mobility compared

2) Reduce security risk across the mobile enterprise

Mobile devices with its apps running on smartphones and tables etc., present greater risks of exposing applications and data than the traditional desktop PCs and laptops. The security of mobile devices is a real issue given the many security threats that can occur, such as loss and theft, Wi-Fi and Bluetooth attacks, malware, spam, and phishing.

In the previous section on IAM it was discussed that implementing a separate infrastructure and processes solely for mobile devices is not a viable option. Instead, a unified infrastructure should be secure and manage traditional endpoints as well as mobile endpoints. Including mobile access, means responding effectively to BYOD policies.

The Cloud Standards Customer Council⁴¹ proposes a number of policies and procedures for enterprise mobility security. These relate to what content is allowed to be accessed on mobile devices, how it will be accessed and how an organisation will handle lost or stolen devices. Protect data with on-device encryption of user data, SSL/TSL encryption, secure offline access, and remote data wipe.

- Control access through single sign-on and multi-factor authentication;
- Run an antivirus program on any device with access to the corporate network;
- Run a firewall program on all mobile devices;
- Secure applications with protection against reverse-engineering vulnerabilities, remote disable of applications, and enforcement of client upgrades;
- Enforce compliance with regulatory mandates through secure shells that can be deployed throughout the mobile portfolio;
- Set Bluetooth configurations such that mobile devices are not discoverable.

⁴¹ <http://www.cloud-council.org>

Developments in digital mobility are also reflected at a (national) standards level. NIST released in June 2013 a special publication on how to manage security of mobile devices in the enterprise [3.15]. It is a supplement to the controls specified in SP 800-53 Revision 4 [3.11].

3) Guidelines for securing and managing Mobile Devices

SP 800-124 [3.15] assists organisations to centrally manage and secure mobile devices, such as smart phones and tablets, against a variety of threats. It deals with securing mobile devices throughout their life cycles for both organisations provided and personally owned (BYOD) ones. SP 800-124 gives recommendations for selecting, implementing, and using centralised management technologies. It offers guidance on how organisations can improve the security of their mobile devices.

Before designing and deploying mobile device solutions, organisations should carry out a risk assessment based on existing threats and vulnerabilities to determine which security controls need to be created or improved. At least organisations should create a mobile device security policy and describe how to implement and use the mobile device solution.

A mobile device security policy, which should be consistent and complement existing information security policies, defines:

- Which classes of mobile devices and mobile operating systems are allowed to access what kind of organisation's hardware and software resources;
- The user restrictions on accessing hardware and software of the devices;
- The user and device authentication and authorisation;
- The level of encrypted data communications and data storage;
- The use of location services, such as prohibiting use for particular applications (social networking or photo applications);
- The type of monitoring and reporting when policy violations occur;
- The organisation's centralised MDM.

The mobile device implementation and usage itself details at a minimum the following:

- Configuring mobile devices following sound security practices, such as updates with the latest upgrades and patches;
- Efficiently issuing and resetting authenticators (forgotten passwords, etc.);
- Restrictions on using of synchronisation services;
- Digitally signing applications to be installed on the devices;
- Automatically locking idle devices;
- Managing wireless network interfaces (Wi-Fi, Bluetooth, NFC, etc.);
- Distributing the organisation's applications from a trusted mobile application store;
- Remotely wiping a mobile device if it is lost or stolen;
- Automatically detecting jail broken/rooted mobile devices and revoke access to organisation resources;
- Periodically performing assessments to confirm that mobile device policies, processes, and procedures are being followed;
- Continuously communicate best practises to users how to securely use mobile devices (awareness campaigns, etc.);
- Continuously execute vulnerability assessment and remediation and check for new and emerging threats in mobile platforms.

These measures should ensure a basic level of trust in the mobile device that has access to the organisation's resources.

4) Mobile Device Management (MDM)

As organisations should assume that all mobile device are untrusted, which especially holds for BYOD, there are a number of technical tools for achieving degrees of digital trust. The technical tool that is currently used most frequently is called Mobile Device Management (MDM)⁴². MDM is a fast growing type of software used by enterprises, because of the BYOD move from the traditional well managed and secured devices, to the more consumer-focused mobile. This move represents security risks as operating systems were not explicitly designed for enterprise use. In addition, many users store and share their data with Internet-based cloud file synchronisation systems. MDM is to mitigate such security threats it is described by Burns and O'Such⁴³ as follows:

- Software that secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises;
- Functionality typically includes over the air distribution of applications, data and configuration settings for all types of mobile devices;
- Applies to both company-owned and BYOD devices across the enterprise or mobile devices owned by consumers.

Gartner⁴⁴ defines MDM as a range of products and services that allow organisations to deploy and support corporate applications on mobile devices and enforcing policies and maintaining the required level of IT control across multiple platforms. Gartner⁴⁵ positions MDM as primarily a policy and configuration management tool for mobile devices and discusses that MDM software assists organisations in BYOD initiatives. MDM is instrumental in the transition to a more complex mobile computing and communications environment. This kind technology supports hardware, software, security and network management, across multiple OS platforms. Although the primary delivery model is on-premises, it can also be offered as SaaS or in the cloud. A full MDM¹⁵ solution has four main characteristics: software, hardware, network and security management. This allows software distribution, policy management, inventory management, security management and service management (Table 20):

Characteristics	Description	Component
Software management	Ability to manage and support mobile applications, content and operating systems.	<ul style="list-style-type: none"> • Authorized software monitoring • Background synchronization • Backup/restore • Configuration • Development • Hosting • Managed mobile enterprise application platforms • Patches/fixes • Provisioning • Updates

⁴² Unfortunately "MDM" also stands for Master Data Management, an equally import but quite different subject in enterprise information management.

⁴³ <http://federalcenter.npma.org/Chapters/13/Enterprise%20Mobility%20and%20the%20Cloud%20June%202013.pptx>

⁴⁴ <http://www.gartner.com/it-glossary/mobile-device-management-mdm>

⁴⁵ https://dell.symantec.com/system/files/Magic_Quadrant_for_Mobile_Device_Management_Software.pdf

Hardware management	Asset management, provisioning and support.	<ul style="list-style-type: none"> • Activation • Asset/inventory • Battery life • Deactivation • Imaging • Memory • Performance • Procurement • Provisioning • Shipping
Network management	Gain and utilize device information regain location, usage, and cellular, WLAN and other networks.	<ul style="list-style-type: none"> • Help desk/support • Procure and provision • Reporting • Service and contract • Usage
Security management	Enforcement of standard device security, authentication and encryption.	<ul style="list-style-type: none"> • Antivirus • Authentication • Encryption • Firewall • Mobile VPN • Policy enforcement password-enabled • Remote lock • Remote wipe • Secure configuration

Table 20: Main characteristics of MDM solution

An important part of the existing MDM tools for the end-user consists of a managed information container. In this secure and isolated container, also known as sandbox, runs the organisation's software. This allows the end-user to use a single mobile device for both work and private. The client application (the sandbox on the mobile device) isolates the organisation's data and applications from all other data and applications on the mobile device. It typically manages only the security and configuration settings of the sandbox and its data, and not the entire device. However, this negatively impacts the user experience because users have to switch between enterprise and private contexts (phone books, email addresses, SMS/texting, etc.) with frequent re-authentication to access the sandbox. Furthermore, containers are not available for all mobile devices and mobile operating systems.

Containers typically provide the following security features: authentication, encryption, restrictions on copy/paste and selective wipe. With reference to the two previous sections of this chapter, encryption mechanisms used in the container include algorithms such as the Advanced Encryption Standard (AES) in combination with SSL/TLS for data in transit, and AES key lengths must be sufficient to protect the data stored on the mobile device. Authentication is based on two factors: a username/password combination and the (possession of the) mobile device itself. Containers also have a number of built-in applications, which may include: address book, calendar, document viewer, email, editing files and annotations, phone, secure browser, texting and synchronisation of data and files.

Since the market for managed information containers is young, significant improvements in this area are to be expected, such as native functionality offered by new versions of mobile operating systems or strong authentication *via* advanced biometric controls. Therefore, MDM container products should not be considered as long-term solutions for enterprise mobility needs. Nevertheless, managed

information containers are currently considered as adequate tools to manage the risk related to enterprise information on mobile devices.

5) Synthesis

The emergence of mobile devices within the enterprise context has resulted in a major shift of how business is conducted. Staff has now the means to use critical data and applications wherever and whenever they need it. Apart from staff being productive outside the office and normal office hours, enterprise mobility solutions have the potential to radically change organisations, supply chains, and even markets.

But mobile device management is more than just security technology. Organisations should make responsibilities and accountabilities explicit, by putting in place enterprise mobility policies and processes. The policies provide guidance to users on how they can securely interact with others using mobile devices. The processes include awareness campaigns on the proper use of mobile devices and the communication of leading security practices. This will contribute to more digital trust in the business that is being conducted with mobile devices.

References

- [3.1] Barker, E., Barker, W., Burr, W. P., Smid, M. (2007), NIST SP800-57, Recommendation for Key Management, Part 1: General.
- [3.2] NIST (2001), Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/NIST, November 26, 2001.
- [3.3] ISO/IEC 18033-3:2010 "Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers", ISO, Switzerland.
- [3.4] NIST (1999), Federal Information Processing Standard 46-3, Data Encryption Standard, October 1999.
- [3.5] NIST (2012), Special Publication 800-67, Recommendation for Triple Data Encryption Algorithm Block Cipher, January 2012.
- [3.6] PKCS #1 v2.1, RSA Cryptography Standard, RSA Laboratories, June 14, 2002.
- [3.7] Frankel, S. E., Hoffman, P., Orebaugh, A. D., & Park, R. (2008). SP 800-113. "Guide to SSL VPNs", US Department of Commerce/NIST.
- [3.8] IBM Software (2013), "When millions need access: Identity management in an interconnected world. Best-practice security solutions that scale to meet today's huge numbers of users", February 2013, IBM Corporation.
- [3.9] ISO/IEC 24760-1:2011 "Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts", ISO, Switzerland.
- [3.10] IDC (2012), "Worldwide Security Software as a Service, 2012-2015 Forecast: Delivering Security through the Cloud", document #238553, December 2012.
- [3.11] Ross et al. (2013), "Security and Privacy Controls for Federal Information Systems and Organizations", NIST Special Publication, 800-53, Revision 4.
- [3.12] Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K. (2013). Guide to attribute based access control (ABAC) definition and considerations (draft). NIST Special Publication, 800, 162.
- [3.13] OASIS (2008), Extensible access control markup language (XACML) version 3.0.
- [3.14] OASIS (2008), Security assertion markup language (SAML) v2. 0, technical overview, OASIS Committee, Draft v2.
- [3.15] Souppaya, M., Scarfone, K. (2013), Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST; NIST Special Publication, 800-124.

4 Digital trust through the knowledge of standardization and certification

In this chapter, some aspects of the framework allowing to build digital trust are exposed. The first section constitutes an introduction to ICT standardization at national, European and international level, the second-one focuses on certification and accreditation, two domains that in combination ensure an efficient trust scheme. In addition, two sections are dedicated to applicable regulatory requirements at European level by the European regulation on electronic identification and trust services (describing the supervision scheme for qualified trust service providers) and at national level by the law on electronic archiving (explaining the supervision scheme of Digitisation or Archiving Service Providers in order to get the "PSDC" status).

I. ICT international standards and their development through standardization

This section begins 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 development. The second part of the section focuses on Information and Communication Technology (ICT) in the frame of international standardization, by introducing the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and their standardization Joint Technical Committee (JTC) 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.

1) Introduction to standards and standardization

a. 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 [4.1], 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 [...]"* [4.1]. 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 trade 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 to an average of 0.81% per year, or almost 25% of Gross Domestic Product (GDP) growth [4.2].
- In Germany, the information contained in standards and technical rules was responsible for 1% of Germany's Gross National Product (GNP) [4.3].
- In Canada, the increasing number of standards has contributed to:
 - 17% of the growth rate of labor productivity,
 - 9% of the growth rate in output (real GDP⁴⁶) [4.4].

b. 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 [4.1], 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 good 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.

⁴⁶ Output (or Gross Domestic Product, commonly called GDP) is measured in two ways. Real GDP, also known as Constant dollar GDP, is the measure of GDP most often used by economists and is the measure of GDP that most often discussed in the press. It measures the market value of all goods in services produced in the economy using the prices that prevailed in some fixed base year.

2. Transfer of innovations

Participating to a standardization TC means to be a stakeholder in new standards development. It is a way to internationally spread the good 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 TCs 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/or customers, or to know what is under 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.

c. The standardization frames

Standards are established by different recognized organizations at the national, European and international level.

At the national level, each country has at least one National Standards Body (NSB) allowed to produce national standards (Table 21). 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 (<i>Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services</i>)	
Germany DIN (<i>Deutsches Institut für Normung e. V.</i>)	
Belgium NBN (<i>Bureau de normalisation</i>)	
Sweden SIS (Swedish Standards Institute) SEK (<i>Svensk Elstandard</i>) ITS (<i>Informationstekniska Standardiseringen</i>)	



France AFNOR Normalisation (<i>Association Française de Normalisation</i>)	
United Kingdom BSI (British Standards Institution)	

Table 21: Examples of NSB

The European standardization bodies recognized by the European Commission are those listed in the Regulation (EU) No 1025/2012 [4.5] (Table 22). The standards produced by CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) are preceded by “EN”, and by “ETSI TS” for ETSI (European Telecommunications Standards Institute).

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

Table 22: 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 or ITU-T (International Telecommunication Union’s Telecommunication Standardization Sector) (Table 23). 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 23: Examples of international standardization organizations

2) 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, etc.

These organizations are generally based on industrial *consortia* promoting their standards as “*de facto* standards”, i.e. having achieved a dominant position, but without having necessarily received a formal approval under a standardization process.

At the opposite, “formal standardization” concerns standards development through national, European 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. Based on a mutual agreement between ISO and IEC, the Joint Technical Committee 1 was created in 1987. It can be considered as a SDO as a whole. This statement is reinforced by the “Vienna Agreement” set up in June 1991 between CEN and ISO, which aim is to avoid parallel or conflicting standards and provide mutual assistance in the global work.

a. Participation to ISO standards development

ISO is the world’s largest developer and publisher of international standards. There are currently more than 19500 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 development is performed by national experts, coming from the different ISO members. ISO brings together 162 countries (out of the 197 total countries in the world according to the UN) as ISO members.



Figure 7: Logo of the ISO

The ISO membership falls into the three following categories:

- **Member bodies** (117 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** (41 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** (4 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 (SCs) and/or Working Groups (WGs). 237 TCs are active at the beginning of 2014. Different participation levels in the work of TCs and SCs 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.

b. 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 agreement⁴⁷ 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 8: Logo of the IEC

The title of the standardization TC ISO/IEC JTC1 is “Information Technology” and its scope is “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 concerning⁴⁸:

- 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;

⁴⁷ ISO Council resolutions 49/1976 and 50/1976 and IEC Administrative Circular No. 13/1977

⁴⁸ http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home.htm

- 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 [4.6].

The TC ISO/IEC JTC1 is currently composed of 20 SCs. Figure 9 summarizes the structure of ISO/IEC JTC1. ISO/IEC JTC1 is one of the largest TC in ISO, gathering 33 P-members and 61 O-members in June 2014. Luxembourg is registered as O-member of ISO/IEC JTC1. This TC is also one of the most active with 2711 published standards and more than 600 standards and projects in progress. 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/home/standards_development/list_of_iso_technical_committees/jtc1_home.htm.

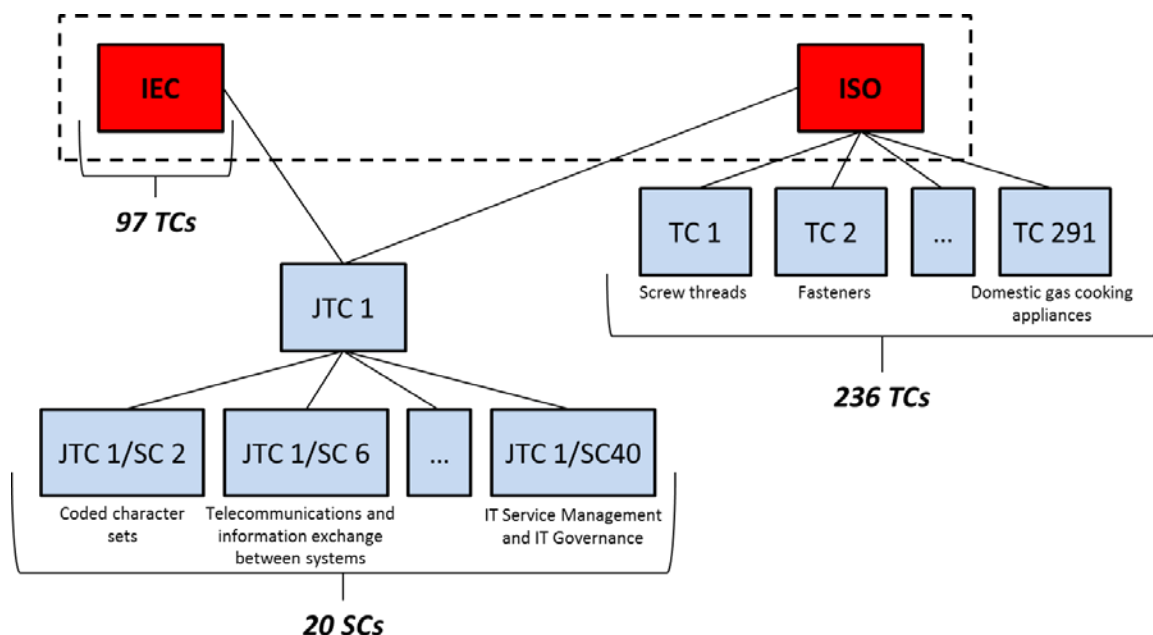


Figure 9: ISO/IEC JTC1 within the ISO structure (June 2014)

The current 20 SCs and the WG of ISO/IEC JTC1, dealing all with a different topic of ICT, are listed in Table 24, the last SC opened being SC40. It is important to note that some SCs are closed. Most of them are merged in other SCs, 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.

Note:

ISO/IEC JTC1/SC40, opened in December 2013, develops standards, tools, frameworks, good practices and related documents for IT Service Management and IT Governance, including areas of IT activity such as audit, digital forensics, governance, risk management, outsourcing, service operations and service maintenance.

SC/WG	Title
JTC1/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
JTC1/SC40	IT Service Management and IT Governance

Table 24: SCs and WGs of ISO/IEC JTC1

Regarding the topics covered by ISO/IEC JTC1, a SWG (Special Working Group) on Planning is continuously investigating for new standardization areas. During the last ISO/IEC JTC1 plenary meeting held in Perros-Guirec, France, in November 2013, the SWG on Planning recommended the following areas as potential new standardization topics for ISO/IEC JTC1:

- Big Data and Data Analytics;
- Smart Cities.

Consequently, ISO/IEC JTC1 has decided to create two new Study Groups (SGs) to provide deeper analysis on these topics: ISO/IEC JTC1/SG1 on Smart Cities and ISO/IEC JTC1/SG2 on Big Data.

c. 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 standards development is based on voluntary agreements, it also requires 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 policy⁴⁹: *"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 10. It has to be known that all of these stages are reiterative in case of a less of maturity or of a disapproval of the draft by ISO members. Each of these stages is associated to a reference number. The standardization process of ISO is composed of the following stages [4.7]:

- **00 - Preliminary stage**

TC or SC may introduce into their work programs, by a simple majority vote of their P-members, preliminary work items (PWI). 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.

- **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 (NWIP) or New 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 content 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

⁴⁹ http://www.iso.org/iso/global_relevance.pdf

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 [4.1]:

"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.

Note:

Committees may decide to skip the CD stage in accordance with Annex SS of the ISO/IEC Directives Part 1. If the committee has opted to skip the CD, the preparatory stage ends when the enquiry draft (DIS) is available for circulation.

- **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".

Note:

Where the DIS meets the necessary approval criteria, the committee leadership can decide to skip the approval stage and go straight to publication.

- **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**

Every International Standard and other deliverable published by ISO or jointly with IEC shall be subject to systematic review in order to determine whether it should be confirmed, revised/amended, converted to another form of deliverable, or withdrawn.

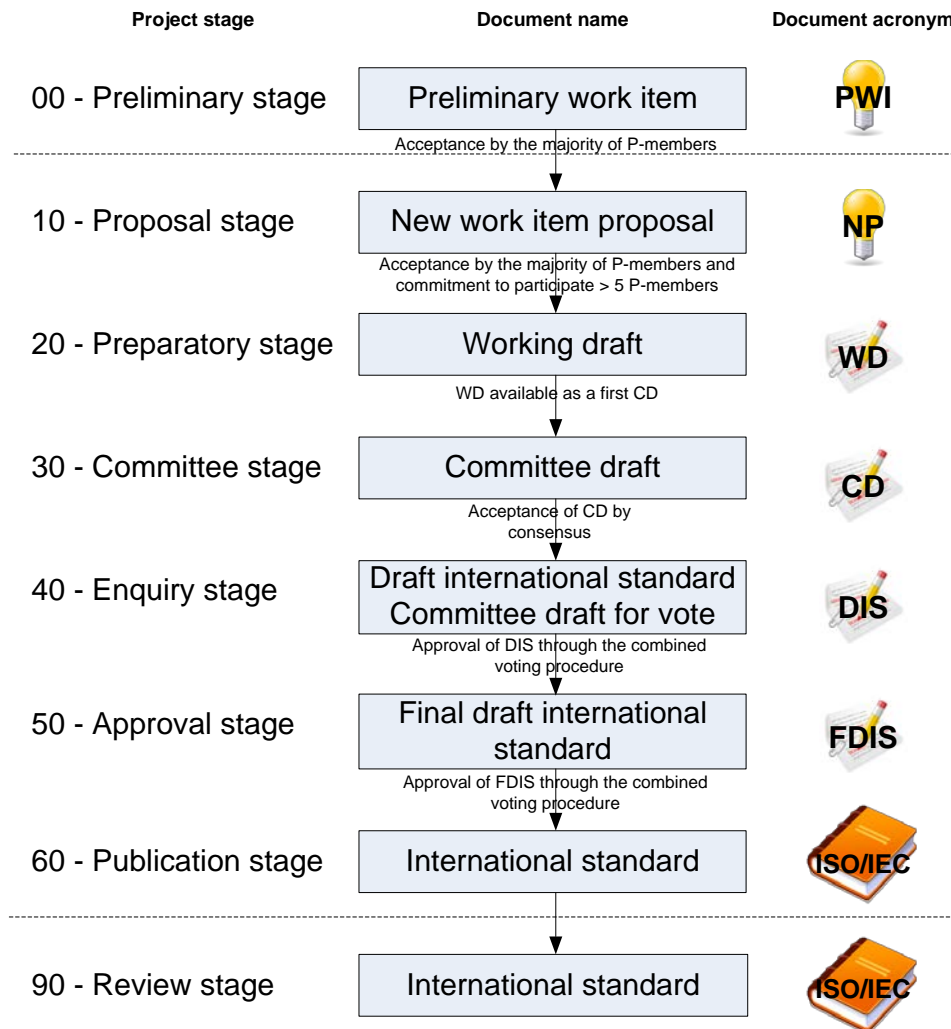


Figure 10: The ISO standardization process

The development timeframe of an international standard is between 24 months (accelerated standards development track) and 48 months (extended standards development track), with an average duration of 36 months.

When the development of an international standard is based on a national standard, or on a standard from another Standards Development Organizations (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 comments 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 the TC for the preparation of standards, often on broad fields or topics.

Note:

Industrial *consortia* can submit an application form to become Publicly Available Specifications (PAS) Submitters⁵⁰ of ISO/IEC JTC1. The application is submitted for voting to ISO/IEC JTC1 members. The work quality of these organizations is recognized by ISO/IEC JTC1, and they are approved to submit PAS as drafts for review and approval as International ISO/IEC JTC1 standards.

3) 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 is involved, through national delegates, in the standardization work of 75 TCs and SCs in areas as diverse as steel, tobacco, ICT, project management, or in policy development committees such as CASCO (Committee for conformity Assessment). In June 2014, among the 75 TCs and SCs where Luxembourg is involved:

- 62 are as P-Member;
- 13 are as O-Member.

a. 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. 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 was released for the decade 2010 - 2020. The main idea behind this strategy was that participating to the standardization process leads to the development and valorization of the work of the national delegates.

Although the many and various initiatives taken for more than three years have helped to establish ILNAS identity and to increase the number of national delegates in standardization, the products and services developed have not been very successful. In this context, to adapt the national standardization strategy in order to effectively answer the needs expressed by the economic market and its stakeholders, ILNAS decided to adapt its strategy with the "Luxembourg Standardization Strategy 2014-2020"⁵¹, published in January 2014. The new positioning can be summarized in the principle of the strategy "Technical standardization as a service".

⁵⁰ http://itc1info.org/?page_id=517

⁵¹ <http://www.portail-qualite.public.lu/fr/publications/normes-normalisation/orientations-strategiques/strategie-normative-2014-2020/strategie-normative-luxembourgeoise-2014-2020.pdf>

The new national standardization strategy 2014-2020 consists of three pillars:

Pillar 1: Information and communication technologies (ICT)

Given the dynamism and the vital importance of the ICT sector for the national market:

- A support and constant development of the standardization field dedicated to Information and communication technologies (including in terms of education and promotion) according to the "Luxembourg's policy on ICT technical standardization 2013-2020" is provided;
- A detection of niche opportunities for economic developments is carried out.

Pillar 2: National influence and compliance with legal responsibilities

In order to increase the influence of Luxembourg:

- A support to national influence in terms of representation at European and international standardization levels, and full compliance with legal attributions (especially European) according to the guidelines and needs of ILNAS is scheduled;
- A detection of opportunities for the national economic market is provided.

Pillar 3: Products and services

A support in terms of implementation of products and services in the field of standardization, mainly on request from the national economic market is carried out.

b. Policy on ICT technical standardization (2013-2020)

According to the national standardization strategy, the "Luxembourg's policy on ICT technical standardization"⁵² has been published in 2013 with the aim to foster and strengthen the national ICT sector in its involvement in standardization work, and to achieve its main objectives consisting in five lead projects:

- Developing yearly the national standards analysis for the ICT sector;
- Defining a national implementation plan for ICT technical standardization (in line with the national standard analysis for the ICT sector);
- Organizing and developing the ICT technical standardization representation at the national level;
- Reinforcing the research and innovation activities related to ICT standardization;
- Representing national interests within European and International entities in the field of ICT technical standardization.

c. The national mirror committees of ISO/IEC JTC1

ISO/IEC JTC1 is divided into SCs 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 SCs 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).

⁵² <http://www.portail-qualite.public.lu/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2013-2020/policy-on-ict-technical-standardization-2013-2020.pdf>

The parent committee ISO/IEC JTC1, which 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, 8 SCs are active at the national level in June 2014. Table 25 below summarizes the ICT standardization subcommittees active at the national level and their chairperson with their related economic entity:

Technical committee	Title	Chairperson	Economic actor
ISO/IEC JTC1	Information Technology	Jean-Philippe HUMBERT	ILNAS
ISO/IEC JTC1/SC7	Software and systems engineering	Alain RENAULT	Centre de Recherche Public Henri Tudor
ISO/IEC JTC1/SC17	Cards and personal identification	Benoit POLETTI	GIE InCert
ISO/IEC JTC1/SC27	IT Security Techniques	Benoit POLETTI	GIE InCert
ISO/IEC JTC1/SC34	Document description and processing languages	David NARAMSKI	NOWINA Solutions S.à.r.l.
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	KBL European Private Bankers S.A.
ISO/IEC JTC1/SC39	Sustainability for and by Information Technology	Didier MONESTES	Systemic Area Network S.à.r.l.
ISO/IEC JTC1/SC40	IT Service Management and IT Governance	Béatrix BARAFORT	Centre de Recherche Public Henri Tudor

Table 25: The national mirror committees of ISO/IEC JTC1

Moreover, 43 delegates from Luxembourg are involved in June 2014 in ISO/IEC JTC1 for a total of 54 registrations⁵³. The list of the delegates is freely available on the dedicated portal⁵⁴. The number of delegates per national mirror committee is depicted in Table 26 below.

(Sub-)Committee	JTC1	SC7	SC17	SC27	SC34	SC36	SC38	SC39	SC40
Number of delegates	2	11	2	19	1	7	3	1	8

Table 26: Registrations per national mirror committee

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 more broadly, and not just by a single 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.

⁵³ A single delegate can be registered in several TCs or SCs

⁵⁴ <http://www.portail-qualite.public.lu/fr/publications/normes-normalisation/information-sensibilisation/ilnas-oln-registre-national-deleques-normalisation/ilnas-oln-registre-national-deleques-normalisation.pdf>

d. The tools developed by ILNAS to manage 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 SCs, 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 2013, for example, ILNAS in collaboration with the CRP Henri Tudor organized a conference held during the World Standards Day (14.11.2013) on the topic: “Standards ensure positive change”. On this occasion, a specific session dedicated to ICT introduced to the participants some strategic aspects of ICT standardization. In this frame, the updated national standards analysis for the ICT sector⁵⁵, which constitutes a sector-based “snapshot” of the normative situation, was presented to national stakeholders in order to spread them awareness about standardization opportunities in the ICT sector. 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.

⁵⁵ <http://www.portail-qualite.public.lu/fr/publications/confiance-numerique/etudes-nationales/Pub-standards-analysis-ict-v3-0/standards-analysis-ict-sector-march-2014.pdf>

e. The European multi-stakeholder platform on ICT standardization

Since January 2012, the Grand Duchy of Luxembourg is represented *via* the Digital trust department of ILNAS in the European multi-stakeholder Platform on ICT standardization (MSP).

The MSP has been created by the European Commission by the Decision of November, 28 2011 (2011/C 349/04)⁵⁶, to advise it on matters relating to the implementation of ICT standardization policy, including the ICT Standardization Work Program, priority setting in support of legislation and policies and identification of specifications developed by global ICT standards development organizations to improve standard setting in the field of ICT to ensure interoperability between ICT applications, services and products.

This platform is an Advisory Expert Group on all matters related to European ICT Standardization and its effective implementation:

- Advise the Commission on its ICT Standardization work program;
- Identify potential future ICT Standardization needs;
- Advise the Commission on possible standardization mandates;
- Advise the Commission on technical specifications in the field of ICT with regard to its referencing in public procurement and policies;
- Advise the Commission on cooperation between standards developing organizations.

The multi-stakeholder platform is composed of representatives of national authorities of Member States and EFTA countries⁵⁷, stakeholder organizations representing industry, small and medium-sized enterprises, consumers and other societal stakeholders as well as European and international standardization bodies and other non-profit making organizations, which are professional societies, industry or trade associations or other membership organizations active in Europe that within their area of expertise develop standards in the field of ICT.

European Rolling Plan on ICT Standardization

The MSP Rolling Plan on ICT Standardization⁵⁸, henceforth called the Rolling Plan (RP), is a document drafted by the European Commission, in collaboration with the European Multi-Stakeholder Platform on ICT Standardization.

This Rolling Plan provides a multi-annual overview of the needs for preliminary or complimentary ICT standardization activities to undertake in support of the EU policy activities. It is addressed to all ICT Stakeholders and gives a transparent view on how the policies are planned to be practically supported. As such, it is the successor of the 2010-2013 ICT Standardization Work Program, and it is a non-binding document.

The Rolling Plan comprises several chapters. The first two chapters provide an introduction to the Rolling Plan, the importance of standardization and standards in the context of policy making and the instruments that are available for working with standardization, standards and technical specifications and promoting their uptake.

⁵⁶ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:349:0004:0006:EN:PDF>

⁵⁷ EFTA: "European Free Trade Association" whose current members are Norway, Switzerland, Iceland and Liechtenstein

⁵⁸ <https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation>

Chapter 3 of the Rolling Plan lists all topic areas identified as EU policy priorities where standardization, standards or ICT technical specifications may play a key role in the implementation of the respective policy. The main EU policy priorities related to ICT standardization are summarized in Table 27 below:

Societal Challenges <ul style="list-style-type: none"> • eHealth • Web Accessibility • Accessibility of ICT products and services • e-Skills and e-Learning • Emergency communications • eCall • Digital Cinema 	Innovation for the digital single market <ul style="list-style-type: none"> • e-Procurement, Pre and Post award • e-Invoicing • Card, Mobile and Internet Payments • eXtensible Business Reporting Language (XBRL) • Online Dispute Resolution (ODR)
Sustainable growth <ul style="list-style-type: none"> • Smart Grids and Smart Metering • Technologies and Services for a Smart and Efficient Energy Use • ICT Environmental Impact • European Electronic Toll Service (EETS) • Intelligent Transport Systems (ITS) 	Key enablers and security <ul style="list-style-type: none"> • Cloud Computing • (Open) Data • eGovernment: • Electronic identification and trust services including e-signatures • Radio Frequency Identification (RFID) • Internet of Things (IoT) • Network and Information Security • ePrivacy

Table 27: EU policy priorities related to ICT standardization

Chapter 4 of the Rolling Plan covers technologies of horizontal importance in the contexts of ICT infrastructures and ICT standardization. It provides an overview of relevant basic horizontal standards and ongoing standardization activities in various technology areas with relevance across the specific topic areas. These technologies are summarized in Table 28 below:

Technology areas		Technologies covered
Physical and Link		Cabling, USB, BUS specifications, Ethernet, WIFI, GSM, LTE, Signaling and framing specifications.
Internet-working technologies		IP level technologies (e.g.: Binding to lower layers, Mobility solutions, Rendez-Vous, Locator/Identifier splits, Home networks, Tunneling, DNS, intra and inter domain routing, virtual networking, multi-cast, congestion control mechanism, TCP maintenance, and various traffic optimization mechanisms).
Applications	Messaging and Media	Application layer protocols (e.g.: various e-mail standards, HTTP, LDAP Internet based telephony (SIP and RTP), internet messaging (XMPP), emergency services, geolocation, and web platform (HTML, Cookies, XML, EcmaScript)).
	Presentation and Interfacing	Fonts, Internationalization, Audio and Video Codecs, Accessibility standards, Fileformats (jpeg, SVG), APIs, Cascading style sheets.
	Business logic	XML based document definitions, business semantics, and Modelling Languages (e.g. invoicing standards).
Security and Privacy		Internet Public Key, Internet infrastructure (x.509 based) web authorization, javascript signing and encryption, transport layer security mechanism (TLS), Authentication information exchange mechanisms (SAML), Privacy enhancement mechanisms.

Table 28: Relevant technology areas and related technologies

4) 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 [4.6], 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 good 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" [4.8]. 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 an O-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 policy on ICT technical standardization clearly mentioning its commitment to ISO/IEC JTC1 and 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, 8 SCs are active at the national level in June 2014. By analyzing the active national mirror committees (Table 25), and furthermore the number of delegates per national mirror committee (Table 26), 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. Luxembourg remains an O-member of ISO/IEC JTC1, in order to follow developments at the strategic level of ICT standardization and to strengthen the involvement of Luxembourg at the international level. Indeed, it would be beneficial for ILNAS to gain more delegates in more SCs of ISO/IEC JTC1.

Finally, in the frame of ICT standardization, the following objectives, defined by ILNAS in the "Policy on ICT technical standardization (2013-2020)", should be achieved in line with the update of the standardization strategy for Luxembourg:

- The strengthening of the national ICT standardization community;
- The organization and development of the ICT technical standardization representation at national level;
- The increasing of the national representation within European and International entities in the field of ICT technical standardization;
- The provision of awareness raising on ICT standardization according to market-sector needs;
- The development of research activities in relation to ICT standardization, in the national interest.

II. Certification and accreditation

In this section, the concepts of certification and accreditation are discussed. Firstly, an introduction about certification and conformity assessment is provided, including some details about the certification process. Secondly, accreditation and its links with certification are described. An overview of accreditation bodies, the mutual recognition principle, and the related regulations and standards is performed. Lastly, OLAS (*Office Luxembourgeois d'Accréditation et de Surveillance*) the national accreditation body is presented. 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 depicted.

1) Introduction to certification

Nowadays, a lot of companies are ISO 9001 [4.9] certified in order to promote, to their customers, vendors, employees, stakeholders and authorities, that they have put in place a quality management system. ISO 9001 is currently the most internationally well-known certification, with more than a million of certifications. 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 [4.10] dealing with “Environmental management systems”;
- ISO/IEC 27001 [4.11] dealing with “Information security management systems”;
- ISO 22000 [4.12] dealing with “Food safety management systems”;
- etc.⁵⁹ (see Figure 11).

a. Certification and conformity assessment

Based on the definitions of ISO/IEC 17000 [4.13], 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 dispositions⁶⁰. 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 [4.13], 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 [4.13].

⁵⁹ The list is not exhaustive

⁶⁰ 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 11) and certification is also continuously progressing in Luxembourg (see Figure 12)⁶¹.

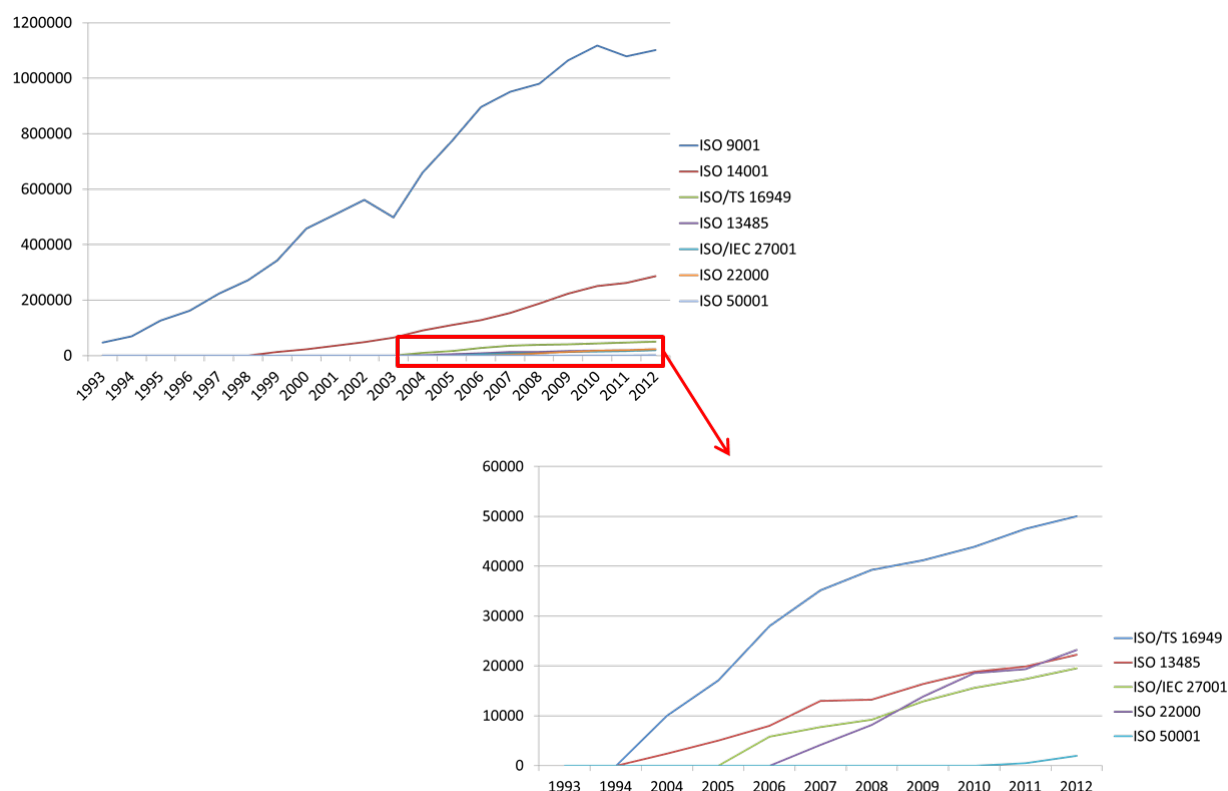


Figure 11: Certification evolution at the international level

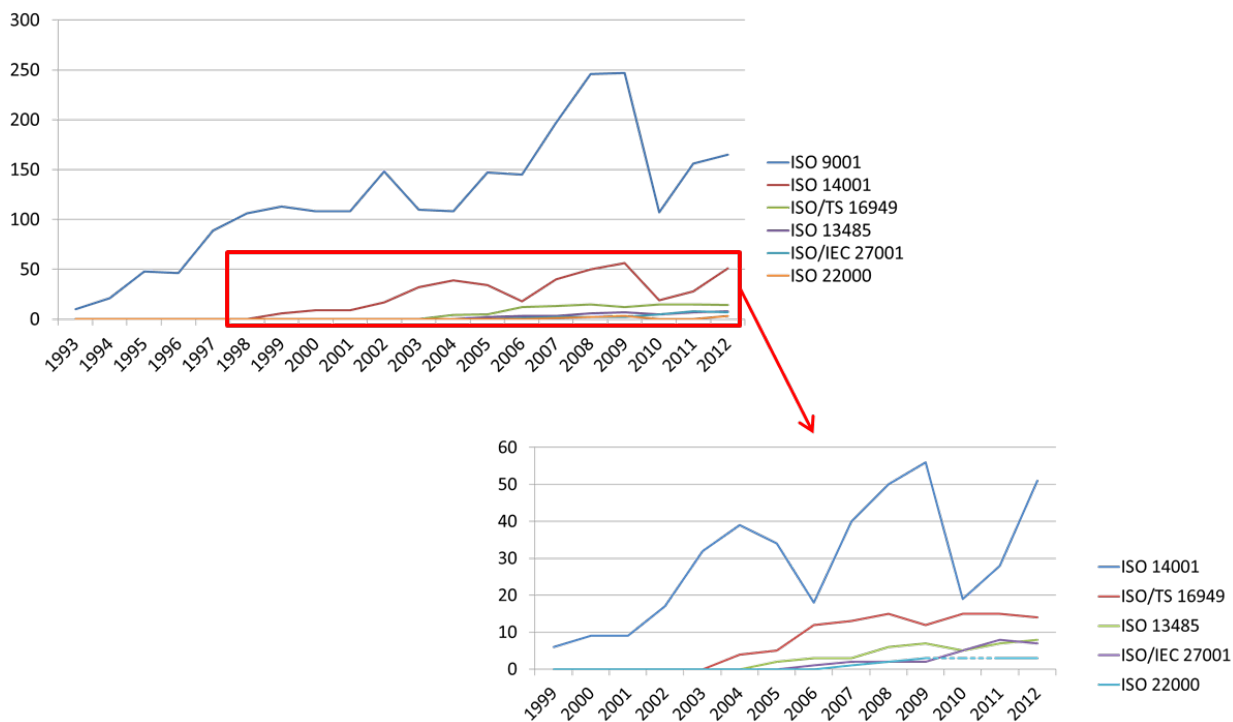


Figure 12: Certification evolution at the national level

⁶¹ Figures based on the ISO Survey (<http://www.iso.org/iso/home/standards/certification/iso-survey.htm>)

Certification can also be issued according to the regulation. Before placing on the market, the certification, by notified bodies⁶², of some categories of products according to “New Approach” directives⁶³, is mandatory before giving the authorization to the manufacturers to use the CE mark. The CE marking attests the conformity of the products to 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.

b. The certification process

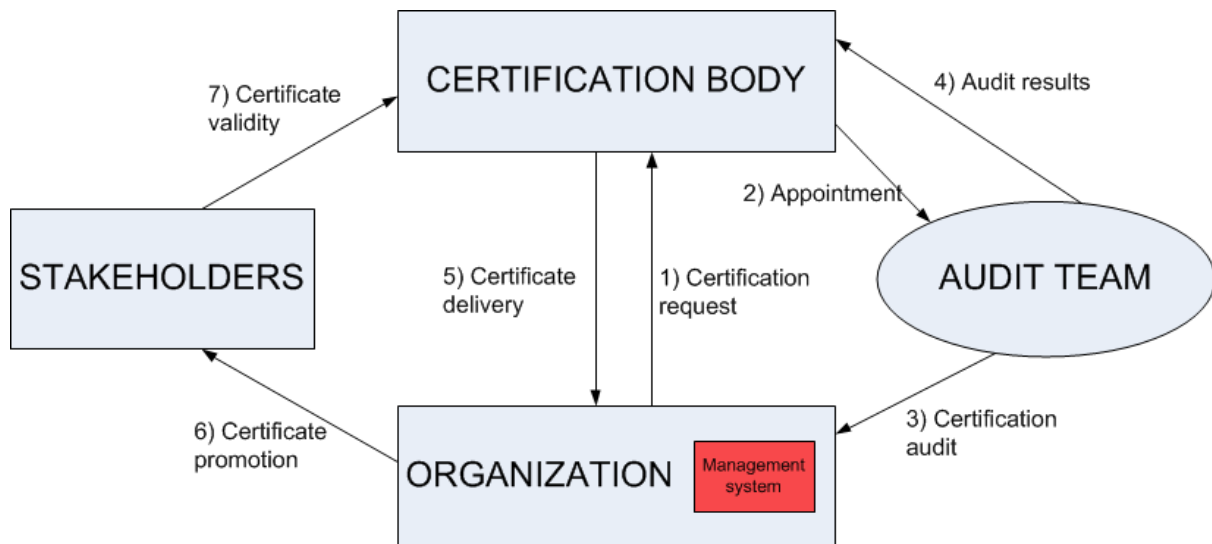


Figure 13: The certification process

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 13):

1. The organization 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 on the conformity of the standard requirements, the certification body delivers the certificate to the organization;
6. Once certified, the organization is allowed to communicate and promote to its customers, vendors, employees, stakeholders and authorities 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 organization conformity is controlled, through surveillance audits, by the certification body. A similar process is applied for the certification of products, systems or persons.

⁶² <http://ec.europa.eu/enterprise/newapproach/nando/>

⁶³ <http://www.newapproach.org/>

2) The trust chain of accreditation and certification

As explained in the previous sub-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 sub-section defines accreditation, its scope, the related regulations and standards, and finally the regional and international mutual recognition principle.

a. Accreditation definition and scope

As defined in ISO/IEC 17000 [4.13], 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 [4.14] 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 consumers;
- 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 [4.14]. 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 is compliant with the international system of units.

For many organizations, accreditation is a voluntary basis initiative. CAB have to apply for an accreditation to their National Accreditation Body (NAB). This initiative aims to give confidence to the market by stating that the CAB is competent against the relevant European or international standards. However, for some specific domains, 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 [4.14] and in the Decision N° 768/2008/EC [4.15] of the European Parliament and of the Council.

b. Accreditation bodies

Accreditation activities are based on a 3-level chain of trust. Firstly, the NAB provides accreditation to organizations at the national level. According to the regulation (EC) n°765/2008, Member States shall

appoint a single NAB by country. In Luxembourg, OLAS is recognized by the government as the NAB. (See sub-section 3 for more details on OLAS). Secondly, NABs are part of regional associations of national accreditation bodies managing peer evaluation systems. Each international region has its own regional association. In Europe, this association is called European co-operation for Accreditation (EA). 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 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 Committee (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 and certification bodies at the European level.



Figure 14: 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 15: Logo of the International Accreditation Forum and of the International Laboratory Accreditation Cooperation

c. 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 [4.16], 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 is 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.

d. 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. Table 29 below 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 + ISO/IEC 27006 (ISMS certification)
	Certification of persons	ISO/IEC 17024
	Certification of products	ISO/IEC Guide 65 / EN 45011 and ISO/IEC 17065
	Greenhouse gas validation and verification bodies	ISO 14065
Accreditation of laboratories	Testing, Calibration	ISO/IEC 17025
	Medical analyses	ISO 15189

Table 29: Accreditation fields and associated standards

Along with the standards presented in Table 29 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*”.

e. The European accreditation regulation

Regulation (EC) N° 765/2008 [4.14] establishes a legal framework for accreditation in the EU/EFTA (European Free Trade Association) Member States.

The motivation behind this regulation is “[...] *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 (EC) N° 765/2008 [4.14], 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 is completed by the Decision N° 768/2008/EC of the European Parliament and of the Council of 9th July 2008 [4.15]. 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.

3) OLAS: the accreditation body of Luxembourg

a. Introduction to the “Office Luxembourgeois d’Accréditation et de Surveillance” (OLAS)

OLAS is the sole accreditation body of CAB in Luxembourg, compliant with the Regulation (EC) N° 765/2008 [4.14]. It is a department of ILNAS which is a public administration under the authority of the Minister of the Economy.

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 [4.16]), 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;
- Evaluation and surveillance of notified CAB with respect to the Luxemburgish legislation transposing EU harmonization legislation;
- Good Laboratory Practices management.

b. 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 the Economy and 1 expert chosen by the committee members for his 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".

c. Mutual recognition of OLAS

To meet the requirements of Regulation (EC) N° 765/2008 [4.14], OLAS has been assessed by his peers according to national and European legislation, the ISO/IEC 17011 [4.16] standard and the EA, IAF and ILAC guidelines. Since April 18th, 2012, OLAS is signatory of the EA MLA for the following areas:

- Testing, calibration 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.

d. 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, ISO/IEC 17065,
 - 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 [4.14] and in the Decision N° 768/2008/EC [4.15] 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 16.

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 16). More information can be found in the quality manual of OLAS and the associated procedures⁶⁴.

⁶⁴ <http://www.portail-qualite.public.lu/fr/accreditation-notification/accreditation/systeme-qualite/index.html>

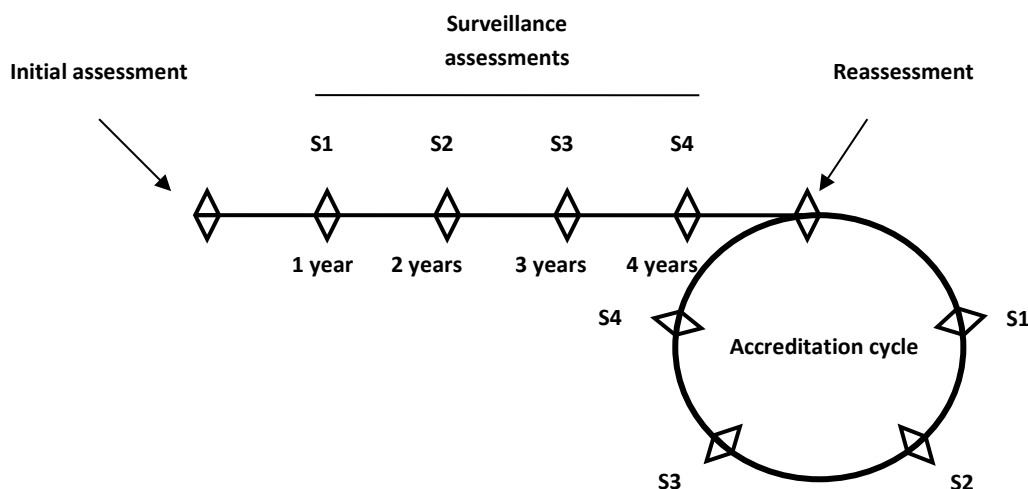


Figure 16: The accreditation cycle

e. 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 good 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 decisions on sector schemes. The Committee focuses on ISO/IEC 17011 [4.16] 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 CASCOT 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 domains⁶⁵.

4) 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.

⁶⁵ <http://www.portail-qualite.public.lu/fr/normes-normalisation/developpement-normes/index.html>

III. European regulation on electronic identification and trust services

The European Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market will repeal the directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures [4.17]. The accreditation of public key infrastructures is replaced by the supervision of qualified trust service providers and certificates containing qualified electronic signatures according to the requirements of this regulation. Electronic identification (eID) and electronic trust services (eTS - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication)⁶⁶ are inseparable by essence when analysing the requirements needed to ensure legal certainty, trust and security in electronic transactions.

In this regard, the European Regulation on trust services will:

- Ensure that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available;
- Create a European internal market for eTS by ensuring that they will work across borders and have the same legal status as traditional paper based processes. Only by providing certainty on the legal validity of all these services, businesses and citizens will use the digital interactions as their natural way of interaction.

eID and eTS, both elements of the Regulation, will create a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. This will increase the effectiveness of public and private online services, eBusiness and electronic commerce in the EU.

At the national level, Digital trust department of the ILNAS is the current supervision body (in the future related to the Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market).

1) Status of "Qualified Trust Service Providers"

Qualified Trust Service Providers⁶⁷ (QTSPs) shall notify their intention to offer a qualified trust service at the national supervisory body and shall then submit a certificate of conformity assessment conducted by an accredited Conformity Assessment Body (CAB), in accordance with the European regulation. If the QTSP meets the requirements of the European regulation, the supervisory body assigns the status of "qualified".

2) Supervision scheme

Guidelines for the conformity assessment according to the European regulation describe the scheme of supervision of qualified trust service providers.

⁶⁶ <http://ec.europa.eu/digital-agenda/en/trust-services-and-eid>

⁶⁷ Fr. Prestataire de services de confiance qualifié

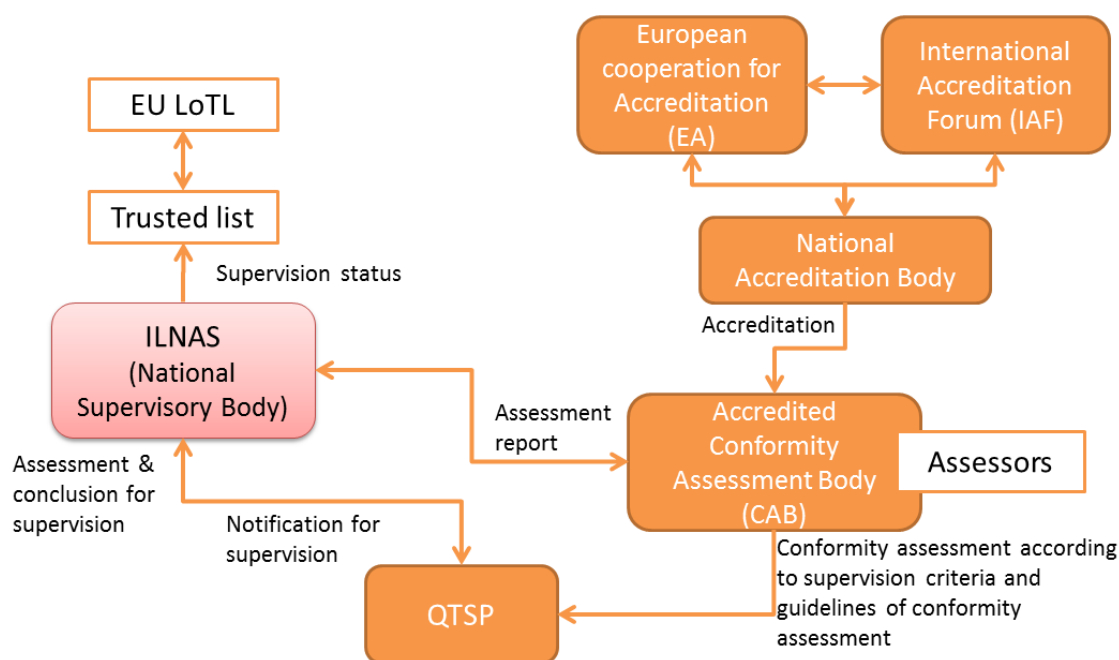


Figure 17: Assessment model for QTSPs

In this context, the Luxembourg supervision scheme (according to the European regulation) is based on the following elements (see Figure 17):

- The national accreditation body: in the Grand Duchy of Luxembourg OLAS (*Office Luxembourgeois d'Accréditation et de Surveillance*) is the single national body that accredits organizations to assess conformity in the context of the supervision system. This accreditation assesses the competence of accredited conformity assessment bodies to perform conformity assessment for needs identified in the supervision system.
Note: Competence of conformity assessment bodies could possibly be accredited by another accreditation body respecting the Multilateral Agreement of European Accreditation (MLA - EA).
- Conformity assessment body (CAB): a conformity assessment body is an independent body of auditors who carries out the conformity assessment of a service provider's compliance against the requirements established in the supervision system. The competence of such a conformity assessment body is accredited by the national accreditation body or by an EA MLA signatory accreditation body. The results of the conformity assessment are notified to the Digital trust department of ILNAS.
- The supervision body: this is the body established in accordance with the European regulation which has all supervisory and investigatory attributions that are necessary for the exercise of its mission. With regard to qualified trust services and the providers of qualified trust services, the Digital trust department of ILNAS is responsible to carry out supervision of these providers. This control ensures that the qualified trust service providers comply with the requirements of the European regulation.

- Trusted list: the Digital trust department of ILNAS is the national body responsible for the notification of the qualified status of the qualified trust service providers and the qualified trust services they provide in the national Trusted list⁶⁸ in accordance with the European regulation. Qualified status results from the verification by the Digital trust department of the compliance of the trust service providers with the requirements of the European regulation. This verification is based on the results of the conformity assessment carried out by an accredited CAB⁶⁹.
- The List of Trusted lists (LoTL) is an additional important element in the supervision scheme. In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission publishes a central compiled list that includes the locations where the national Trust lists are published, as well as the certificate used to verify the authenticity and integrity of the trusted lists. This list of trusted lists is available publicly⁷⁰. Authenticity and integrity are ensured through an electronic signature supported by a digital certificate.

3) Examples of trust services

Examples of trust services are creation, verification, validation, processing and conservation of:

- Electronic signatures;
- Electronic seals;
- Electronic timestamps;
- Electronically signed documents;
- Electronic delivery services;
- Authentication of Web site;
- Electronic certificates, including certificates of electronic signature and electronic stamp.

4) Trust Service Provider in Luxembourg

In Luxembourg, currently one Trust Service Provider is under supervision according to current standards: LuxTrust S.A., under the supervision number 2013/8/001.

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

- Login application (e.g. banks);
- Single login;
- mySecretID: anonymous 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.

⁶⁸ <http://www.portail-qualite.public.lu/tsl-pdf>

⁶⁹ <http://www.portail-qualite.public.lu/fr/confiance-numerique/prestataires-services-confiance/documents-accreditation-surveillance-psc/index.html>

⁷⁰ <http://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers>

IV. The national law on electronic archiving

The development of the information society results in the creation, exchange and storage of an increasing amount of data and information. Meanwhile, citizens, businesses and administrations organize their activities using information technologies to minimize as far as possible the volume of paper documents, for reasons of storage costs, ease of access and information sharing.

The digitisation of information becomes a major issue in a world that is wanted paperless (as the paperless office). The main objectives of the law on electronic archiving are to modernize the rules for digitisation and archiving of electronic documents, as well as to create the activity of Digitisation or Archiving Service Providers (PSDCs).

1) Status of "PSDC"

The national law on electronic archiving will provide that a legal person may, if it holds a certified conformity assessment against the requirements and measures defined in the national *Technical regulation requirements and controls for certifying Digitisation or Archiving service providers (PSDCs)* related to its process of digitisation or archiving, makes a notification to the Digital trust department of ILNAS to obtain the status of "PSDC". Guidelines for audit of the national *Technical regulation requirements and Controls for certifying PSDCs* are published on the web page of ILNAS⁷¹.

To increase the trust of users in the digitization of analogue documents and in the quality and continuity of electronic archiving services, the provider should ensure that data of the PSDC are preserved and remain accessible for the period of time required, even when the PSDC ceases its activities.

If the audit criteria established by the law on electronic archiving and management system of the *ad hoc* quality system of Digital trust department of ILNAS are validated, the ILNAS will proceed to the registration of the legal persons concerned in the list of PSDCs (specifying the supervision processes) thus establishing the status of "PSDC". Any event or significant incident detected and any major changes in the scope of certification, must be notified to the Digital trust department. Any withdrawal, suspension or non-renewal of the certification of compliance causes *de facto* withdrawal of the status of "PSDC".

Note: Any service provider of digitisation or archiving of the financial sector, who wants to get an approval on the part of the CSSF as PSF, must have the status of "PSDC". As part of these activities, the CSSF and the ILNAS can work jointly on the supervision of the PSDC.

2) Technical regulation requirements and controls for certifying PSDCs

Effective certification according to the *Technical regulation requirements and controls for certifying PSDCs* of any legal person allows it to request the "PSDC" status at ILNAS, which is available in the following manner:

- PSDC-DC: Digitisation and Archiving service provider;
- PSDC-D: Digitisation service provider;

⁷¹ <http://www.portail-qualite.public.lu/fr/confiance-numerique/archivage-electronique/documents-surveillance-psdc/index.html>

- PSDC-C: Archiving service provider.

Digital trust department of ILNAS specifically recognizes, *via* this status, the legal person concerned as "PSDC".

The legal entity having the status of "PSDC" must be able to guarantee the results of execution of process of digitisation and archiving for which it received the status. This means that the resulting digital documents of digitization of analogue documents and digital archives will be recognized as complying with the *Technical regulation requirements and controls for certifying Digitisation or archiving service providers (PSDCs)*.

Moreover, a copy shall be recognized as conform to the original when it is validated as such by a PSDC.

Technical regulation requirements and controls for certifying Digitisation or archiving service providers (PSDCs) certification is applicable to any public or private legal person, regardless its type, its size, its processes or activities, for its internal needs or in the context of services offered to its clients independently. It was defined from international standards published and maintained by the International Organization for Standardization (hereinafter "ISO") and must therefore be considered as a supplement to these standards, amending and supplementing their content specifically to the processes of digitisation and archiving.

3) Supervision scheme

a. General information

The primary objective of supervising a PSDC by the Digital trust department of ILNAS is the guarantee of an instance of external audit and of a trust relationship between users and providers of electronic archiving services. Through supervision requirements, Digital trust department of ILNAS intends to provide to electronic archiving services a reliable security level.

The resulting consequence of this reliable level of electronic archiving is, according to the law on electronic archiving, the recognition of the legal value of the documents dematerialized by the care of a PSDC.

The first economic corollary to the supervision of the PSDC and the probative legal value of electronic documents is the branding of "PSDC" and 'marketing' effect for providers of electronic archiving services.

The second economic corollary to the supervision of the PSDC is the reduction of the resulting costs of archiving of analogue records and of loss or accidental destruction of these documents.

Figure 18 illustrates the supervision scheme for the conformity assessment of PSDCs against the requirements and controls laid down in the Technical regulation for certifying PSDCs.

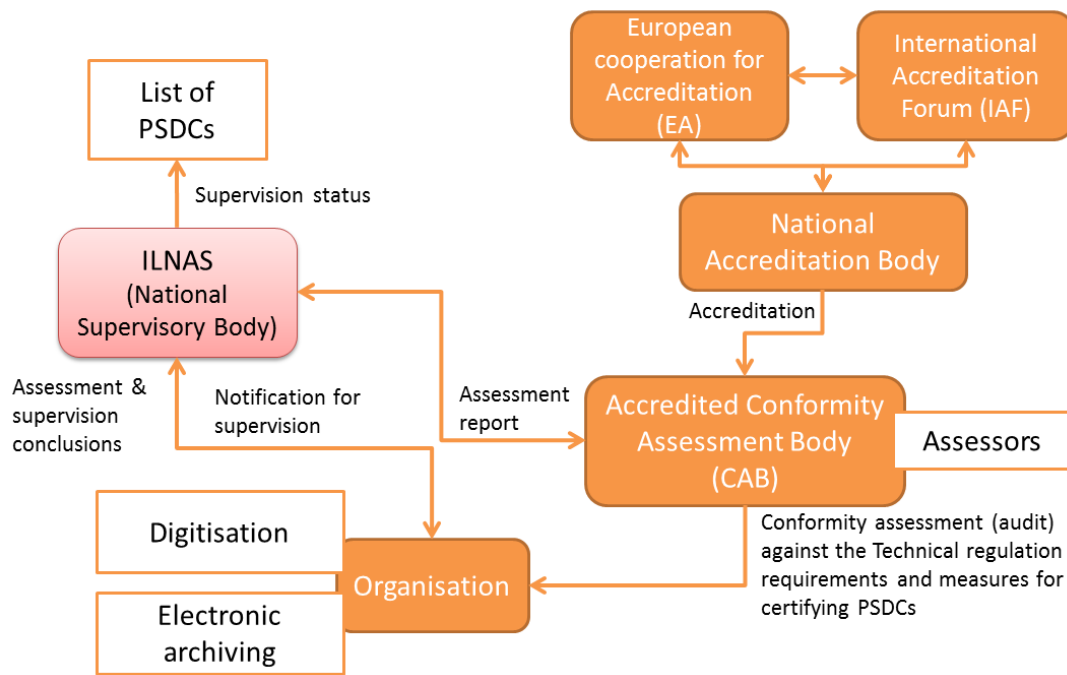


Figure 18: Assessment model for PSDCs

b. The PSDC preparation

To obtain the status of "PSDC", a provider of electronic archiving services has to carry out the following steps:

1. Develop and specify its policy of digitisation and archiving;
2. Create a record for the assessment of the risks relating to its digitisation and archiving activities;
3. Define and specify the practices of digitisation and archiving;
4. Define and establish an information security management system (ISMS);
5. Document and implement the procedures laid down in the ISMS;
6. Perform internal audits;
7. Apply corrective action on identified non-conformities;
8. Involvement and supervising the management of the claimant;
9. Conformity assessment against the national Technical regulation requirements and controls for certifying PSDCs from an accredited "CAB".

c. Conformity assessment

The conformity assessment undertaken by a "CAB" accredited by OLAS or any other "CAB" recognized by OLAS in the context of European or international agreements comprises the following steps:

1. Technical and documentary audit according to the Technical regulation requirements and controls for the certifying Digitisation or Archiving Service Providers (PSDCs);
2. Interim report of the results of the conformity assessment;
3. Corrective actions for non-conformities;
4. Final report of the conformity assessment, which has to be provided to ILNAS in order to get the "PSDC" status.

References

- [4.1] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC Guide 2:2004, Standardization and related activities — General vocabulary, 2004.
- [4.2] AFNOR Normalisation (*Association Française de Normalisation*). *Impact économique de la normalisation*, 2009. URL <http://groupe.afnor.org/economic-impact-standardization/data/catalogue.pdf>
- [4.3] DIN (*Deutsches Institut für Normung*). The Economic Benefits of Standardization, 2011. URL http://www.din.de/sixcms_upload/media/2896/DIN_GNN_2011_engl_akt_neu.pdf
- [4.4] SCC (Standards Council of Canada). Economic value of standardization, 2007. URL https://www.scc.ca/sites/default/files/migrated_files/DLFE-342.pdf
- [4.5] REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European standardisation. URL <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF>
- [4.6] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). The JTC1 value proposition, 2010. URL http://jtc1info.org/wp-content/uploads/2013/01/jtc_1_value_proposition.pdf
- [4.7] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC Directives, Part 1, Consolidated ISO Supplement - Procedures specific to ISO, 2013. URL http://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230452/ISO_IEC_Directives%2C_Part_1_and_Consolidated_ISO_Supplement_-_Procedures_specific_to_ISO%2C_4th_edition_2013_%28PDF_format%29.pdf?nodeid=14883571&vernum=-2
- [4.8] European Commission. EUROPE 2020 – A European Strategy for Smart, Sustainable, and Inclusive Growth, COM(2010) 2020, 2010. URL <http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf>
- [4.9] ISO (International Organization for Standardization). ISO 9001:2008, Quality management systems — Requirements, 2008.
- [4.10] ISO (International Organization for Standardization). ISO 14001:2004, Environmental management systems — Requirements with guidance for use, 2004.
- [4.11] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, 2013.
- [4.12] ISO (International Organization for Standardization). ISO 22000:2005, Food safety management systems — Requirements for any organization in the food chain, 2005.
- [4.13] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles, 2004.
- [4.14] 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.
- [4.15] 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.

- [4.16] 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.
- [4.17] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999. URL <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093>

General Conclusion

The main outcome of the white paper is not only to describe what digital trust is and what the supporting tools are, but also to make people aware of the work performed in Luxembourg to improve digital trust. The digital world faces a number of socio-technological challenges that apart from the well-known computer viruses and crackers, also include unprecedented developments in Big Data analytics, Cloud Computing, social network computing and mobile device proliferation. Improper use of such technologies can have significant consequences on individuals as well as organizations. However, it is important to note that, even if some risks remain, working with an electronic system that is highly reliable and secure — in a nutshell: a trustable system — is something that brings a lot of benefits at economic and social levels. Therefore this white paper presents several topics that contribute to the better understanding and necessary improvements to achieve such trustable systems.

In the first chapter, the subject of trust in relation to technological developments is discussed. Trust, a fundamental and multifaceted construct in human society, has been investigated in many scientific disciplines and has a number of core ingredients: expectancy, belief and willingness to take risk. Research in trust is operationalized using trust antecedents which are factors that impact trust, such as perceived security controls or perceived trustworthiness of a counterparty. The rapid development of commerce through the Internet has resulted in an increased interest in trust in digital environments. Recent developments regarding digital trust relate to frameworks to build and maintain trust and anomaly detection systems for online reputation systems. In this context, the technical and societal impacts of developments in Big Data and Cloud Computing only underline the importance of getting a better understanding on how to improve digital trust for both consumers and providers.

The second chapter presents two international series of standards related to information security: the ISO/IEC 27000 series and ISO/IEC 15408 series. On one hand, ISO/IEC 27001 is the best known and most popular standard that specifies normative requirements for the implementation of an information security management system (ISMS), including a set of controls for the management and mitigation of information security risks. The associated good practices standard ISO/IEC 27002 helps in setting up such an ISMS. Both standards cover the large majority of information security controls that any organization would require. An ISMS accommodates a common language, improves awareness, communication and understanding of information security, helps to increase customer satisfaction and enables an organization to offer more products or even create new business opportunities. Other standards in the ISO/IEC 27000 series address specific topics, such as ISMS implementation guidance, setting performance criteria and targets, selecting controls and risk treatment options, etc. On the other hand, the three parts standard ISO/IEC 15408, also known as Common Criteria, provides assurance that the process of specification, implementation and evaluation of security aspects of computer products has been conducted in a rigorous, repeatable and standardized manner. These computer products have a defined level of assurance related to their information security capabilities and are recognized in large parts of the world. Developers use it to achieve certification when building security features into a product or system. The standards can also be used when a customer needs to specify security features or when they are looking for already built and certified computer products.

The third chapter deals with three technical tools that enhance digital trust: cryptographic tools, Identity and Access Management (IAM) and Mobile Device Management (MDM). Concerning

cryptographic tools, VPNs provide a higher level of trust for data in transit and ensure that the source and contents are verified. Digital signatures and message fingerprints provide reasonable assurance that the data originated from the expected party and has not been changed. Other cryptographic tools can be used for data at rest, such as stored on hard disks or removable media. This can be applied at various levels of granularity, from single files to complete file systems. IAM capabilities increase the level of digital trust because it gives assurances of each user's identity to access hardware, software and data, thereby protecting information. IAM facilitates new business opportunities, increases security, eases the burden of compliance, and increases business efficiency. Because of the ever increasing use of mobile devices within enterprises, companies need to look how to adequately secure the information accessed by and stored on such devices with MDM tools. Users of mobile devices can use critical data and applications wherever and whenever they need it, and such tools facilitate digital trust related to software, hardware, network and security management. The market of MDM tools is immature and significant improvements are to be expected in the near future, such as native functionality offered by new versions of mobile operating systems concerning strong authentication, encryption, restrictions on copy/paste and selective wipe.

The fourth chapter provides an explanation on the ICT standardization and related certification and accreditation aspects. It also details the European regulation on electronic identification and trust services, and the national supervision scheme of Digitisation or Archiving Service Providers (PSDCs) certification.

In summary, ILNAS is convinced that Luxembourg has a major role to play as a "trustable place" in the world. As explained in this white paper, digital trust brings a lot of benefits at the economic and social levels. Nevertheless, still considered as an emerging topic, it needs to be continuously followed and promoted. This will be partly assured at the national level by the ILNAS Digital trust department.

Overall, in order to develop an adequate state of digital trust, the national stakeholders need to understand the concept, to use related tools and applications, to have a strong security context and to be aware of what is relevant in this frame.

Note:

This white paper reflects only the current point of view of the different authors. The objective is to update it regularly, depending on new digital trust development.



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

CONTACT :

ILNAS, DIGITAL TRUST DEPARTMENT

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux

Phone : (+352) 24 77 43 -50 · Fax : (+352) 24 79 43 -50

E-mail : confiance-numerique@ilnas.etat.lu

www.portail-qualite.lu