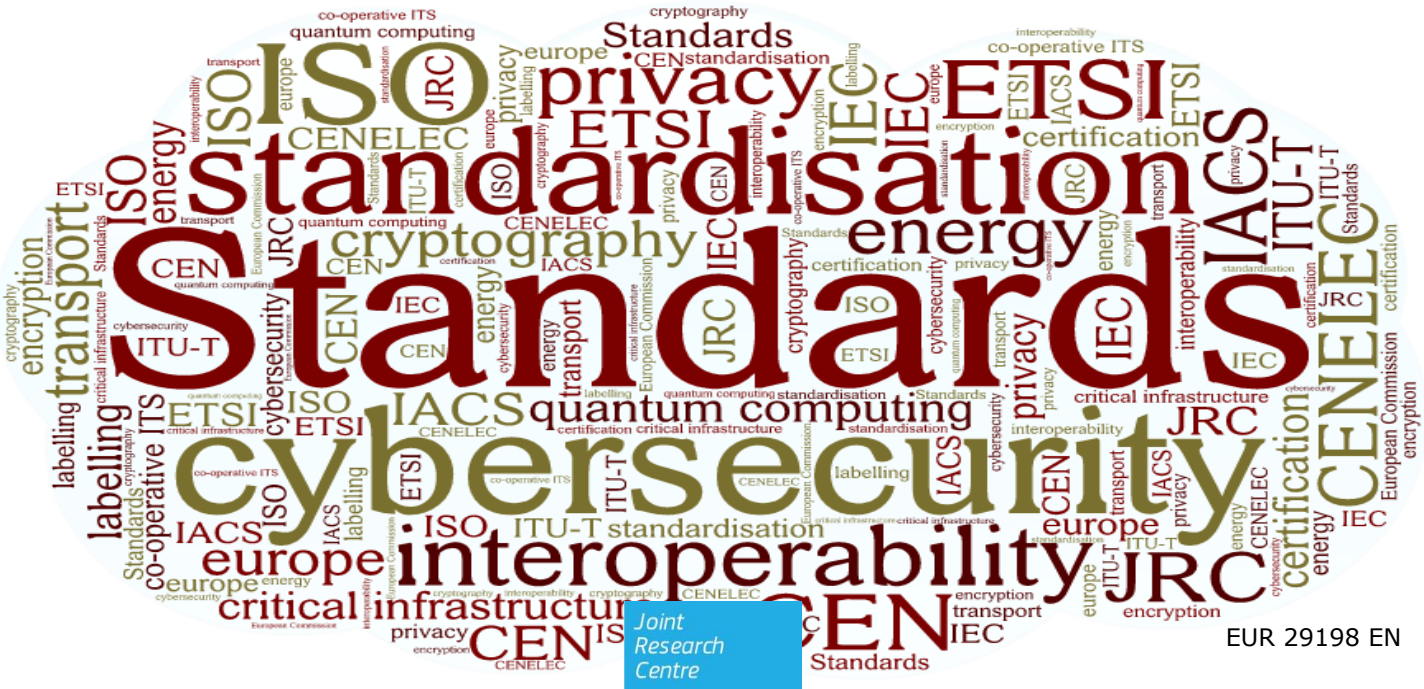
European Commission

An analysis on the development and application of cybersecurity standards

Authors

Scott Cadzow, Ignacio Sanchez, Gianmarco Baldini

2017



Joint Research Centre

EUR 29198 EN

This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Ignacio Sanchez
Address: Joint Research Centre, Via Enrico Fermi 2749, 21027 Ispra, Italy
Email: ignacio.sanchez@ec.europa.eu
Tel.: +39 0332 78 5998

JRC Science Hub
https://ec.europa.eu/jrc

JRC110858

EUR 29198 EN

PDF ISBN 978-92-79-81856-1 ISSN 1831-9424 doi:10.2760/287101

Ispra: European Commission, 2018

How to cite this report: Author(s), *Title*, EUR, doi

Table of Contents

Executive Summary

This report was produced in the context of the Administrative Arrangement Id 34294 between the JRC and DG CNECT to investigate and propose recommendations for the establishment of a European ICT security certification framework and to assess the feasibility of a European cybersecurity labelling framework.

One of the key elements for the establishment of a European ICT security certification framework is the role of cybersecurity standards and their application in the market. Because cybersecurity standards have an important role in security certification and in general for the security of the ICT infrastructures, an analysis is needed to investigate the current status of cybersecurity standards, their role and their effectiveness to support the cybersecurity market and the European cybersecurity industry.

To this purpose, the cybersecurity expert Scott Cadzow was requested to provide an analysis on the role and the current status of cybersecurity standards, which could support the European cybersecurity industry. The outcome of the analysis, finalised in February 2017, was to provide potential recommendations to improve the process of production and application of cybersecurity standards in Europe. JRC complemented this analysis with additional considerations on the parallel effort performed by organizations like ECSO and ENISA and the link to the European ICT security certification framework.

This report does not aim to provide a detailed view of cybersecurity standards in Europe. A number of reports by ECSO, ENISA and ETSI have recently addressed this task and this report refers to them for additional details on the current cybersecurity standards. The present report provides complementary considerations and recommendations on how to potentially support the European cybersecurity industry from standardisation work.

The key recommendations provided as the conclusion of the analysis carried out in this report, are the following ones.

- EU member states should define measures that mandate certain provisions for ICT devices and services prior to them being placed on the market
- Policy measures should place security proof and assurance within the market access framework.
- SDOs should be requested to reinforce the Harmonised Standards approach for security functions.
- The EU should consider sponsoring research and standardisation of means that give authoritative measurement of system integrity in mutable systems.
- The EU should consider sponsoring research and standardisation of means that allow for autonomic reporting of security events to CERTs for analysis and distribution.

1 Context and Background

On May 2015 the European Commission issued a Communication (COM(2015)192) for a Digital Single Market (DSM) Strategy for Europe. The reinforcement of trust and security in digital services and in the handling of personal data is a main priority of the Strategy. To that end, one of the 16 initiatives set in the strategy is the launch of a contractual Public Private Partnership (cPPP) on cybersecurity. This initiative aims to strengthen the EU cybersecurity industry and make sure that European citizens and businesses have access to more innovative, secure and user-friendly solutions that take into account European rules and values. The cPPP on cybersecurity was launched by Communication COM(2016)410, adopted by the Commission on 5th of July 2016.

DG JRC is working together with DG CNECT in the identification, mapping and collection of evidences to support the development of the accompanying measures described in the Staff Working Document SWD(2016)216 of the Communication, designed to complement the establishment of the cPPP on cybersecurity. In this respect, cybersecurity standardization has been identified as one of the areas to be further analysed given its potential to support the development of the European cybersecurity industry.

The present document reviews the landscape of standards able to support a secured DSM. For the purposes of the present document the security functions include the following: Support to identification and authentication by sector; Support to anonymization and pseudonymisation as required by sector (ensuring accountability of actions in the DSM); Support to enable verification of the integrity of data transfers and data stores; Means to support the availability of the DSM (e.g. by trapping and preventing denial of service attacks, treatment of the DSM as national and regional Critical Infrastructure); Means to exchange data related to attacks on, or misuse of, the DSM and its supporting infrastructure.

In parallel to this JRC activity, which produced this report, other organizations have also investigated and identified cybersecurity standards, which are relevant to this analysis. In particular:

- The European Cyber Security Organisation (ECSO) has drafted an extensive State-of-the-Art Syllabus in 2017, with an Overview of existing Cybersecurity standards and certification schemes. ECSO[1] represents the industry-led contractual counterpart to the European Commission for the implementation of the cPPP described above.
- ENISA has also produced a report on Definition of Cybersecurity, Gaps and overlaps in standardisation[2]. The first purpose of the ENISA report is to provide a guide for determining an appropriate understanding of the term 'Cybersecurity' to be used in the context of the intended use of the stakeholders and policy makers. The second purpose is to list organisations taking part in standardisation in the area of Cybersecurity, provide an overview of activities and identify gaps and overlaps.
- ETSI has also produced ETSI TR 103 306[3], which also provides an overview on cybersecurity standardization activities. In particular, the report aims to provide an insight on the various forums that develop techniques, technical standards and operational practices, global and national centres of excellence and major IT developer forums affecting cyber security.

Other organizations, which produced similar reports, are also referenced in this report.

[1] https://www.ecs-org.eu/
[2] https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport
[3] http://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.02.01_60/tr_103306v010201p.pdf

1.1 Scope of report

This report provides a high-level analysis of the role of standardization and the ecosystem of cybersecurity standardisation, describing their evolution and identifying future challenges and opportunities.

The present report does not aim to duplicate or overlap the results already provided in the other reports, but instead reference them and provide complementary considerations and recommendations on how to potentially support the European cybersecurity industry from standardisation work.

1.2 Target Audience

The target audience of this report is the European Commission, Member states, consumer associations and industry associations.

1.3 Structure of the report

Section 2 of this report provides a high level analysis on the role of standardization, the evolution of cybersecurity standards and future challenges and opportunities. Section 3 provides an analysis on cybersecurity standards to identify potential areas of improvement and related actions. Section 4 concludes the report and provides high-level recommendations.

2 Detailed mapping of cybersecurity standards

2.1 Overview

The purpose of this chapter is to produce a mapping and description of the ecosystem of cybersecurity standards including also those ICT standards that could be of the interest of the European cybersecurity industry. The latter group should include a) process standards (risk management, information sharing, certification processes), b) security and privacy requirements in technical standards (e.g. smart cards, 5G, IoT/M2M, cloud interoperability, eHealth, ITS, smart meters, smart grids), and c) specific cybersecurity standards including emerging technologies such as quantum-safe cryptography or quantum key distribution. In addressing such a mapping, the existence of already published documents is acknowledged and where appropriate the mapping is made by reference to the published documents (the referenced documents are listed in the Bibliography at the end of this document).

2.2 Role of standardization

2.2.1 General overview

This report adopts the definition of 'standard' from ETSI[4]: "a 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" (Derived from ISO/IEC Guide 2:1996, definition 3.2).

A very broad generalisation of the role of standards is that their role is to provide interoperability of "things". This is particularly important for open markets, where users, can use different equipment providing the same service or function on the basis of a common standard. In this way, standards promote economies of scale and promote competition. It is also a broad generalisation that standards provide requirements to be met and do not provide instruction on how to implement a requirement (which is left to suppliers and manufacturers).

Regarding security, these statements apply in a broad interpretation but with the slight modifier that many security standards, or more likely the security functions defined in standards, give assurance of the interoperability of "things" when subject to attack by hostile parties. Thus standards may address functionality (e.g. an encryption algorithm), application of that functionality (e.g. use of specific encryption mode (say counter mode)), and contextual use of that functionality (e.g. application of encryption to provision of confidentiality protection services).

For cryptographic security parties that are required to interoperate will also require to share knowledge and functionality that will include the identification of keys and algorithms. Thus security standards have to address simple mechanical interconnection, semantic and syntactic shared meaning, and management of attributes and organisations to react to security transgressions in an appropriate manner. There is some overlap of cyber-security to wider societal functions and this is addressed in part by developments in the fields of "lawful interception" (to give law enforcement agencies authorised and confidential access to real time communications of explicitly identified targets), to "retained data" (to give appropriately authorised agencies access to the communications meta-data of explicitly identified targets), and in general the use of "critical infrastructure".

One problematic domain in the security continuum is the protection of privacy. For the purposes of the present report the role of a security standard is to support some aspects of privacy such as confidentiality of data in storage or in transfer, to enforce proof of identity and authority to access data and so on. The policy aspects of privacy, the right to

[4] ETSI What are the standards. http://www.etsi.org/standards/what-are-standards

publish, the right of self-determination, and so forth are not fully addressed by security standards and they should be complemented by additional measures.

2.2.2 Organisational interoperability

There are classes of organisational management standards in security that define roles within organisations that seek to enforce a "need to know". From a security perspective when two organisations share data, they may transfer data securely by having a common Communications Security (ComSec) framework, but the ComSec exchange cannot make any inference on how data is treated prior to, or after, transfer. Thus the local IT security policy of the sending and receiving organisations is trusted to be equivalent and this trust may be reinforced by measures in the organisation. One important aspect in organisational interoperability is about the type of relationship: one to one, one to many or many to many. In the first case the interoperability is only between two organizational entities, while in the other cases a set of organizations have agreed on a common framework to exchange information. This aspect is relevant for setting up secure communication protocols among European entities, where a many to many relationship is preferred for European-wide regulation.

2.2.3 Syntactic and Semantic interoperability

Syntax cannot convey meaning and this is where semantics is introduced. Semantics derives meaning from syntactically correct statements. Semantic understanding itself is dependent on both pragmatics and context. There are a number of ways of exchanging semantic information although the success is dependent on structuring data to optimise the availability of semantic content and the transfer of contextual knowledge (although the transfer of pragmatics is less clear). The most obvious examples of semantic containers for syntactically correct information are protocols whereby the protocol (e.g. an authentication protocol) gives context to message sets. This may be further extended using the concept of shared state as a means of identifying context and this is often embedded in protocol (e.g. an authentication protocol may go through states that include "Identified", "Challenge issued", "Response pending" prior to finalising on the state "Authenticated").

2.2.4 Electrical and mechanical interoperability

Quite simply a device with a power connector using, for example, a Type- IEC 60906-2 connection cannot accept power from anything other than a IEC 60906-2. Similarly, for example, a serial port complying to USB-Type-A will not be able to connect with a USB-Type-C lead. In addition to simple mechanical compatibility there is a requirement to ensure electrical interoperability covering amongst others the voltage level, amperage level, DC or AC, frequency if AC, variation levels and so forth.

2.2.5 Radio communication interoperability

Radio (wireless) communication requires shared knowledge of frequency band, modulation technique, symbol rate, power, and so forth.. The nature of the physical media requires that radio protocols make provisions to maximise link reliability.

2.3 Overview of published work

ETSI TR 103 306 [1], from November 2015, has made a first attempt to outline the global cyber security ecosystem and has subsequently entered a regime of continuous update with every meeting of ETSI's CYBER group moving the picture forward. As such it can be stated that ETSI's TR 103 306 is the definitive statement on the makeup of the global cyber security ecosystem and in its scope addresses the role and interaction of SDOs, government, and industry. In addition to the ETSI report other analyses have asserted that the ecosystem is a bigger consideration than that normally made in

standards, and as was noted in the ENISA report "Definition of Cybersecurity - Gaps and overlaps in standardisation" (see ISBN 978-92-9204-155-7) even the definition of the boundary between cybersecurity and security in ICT in general is blurred. Further in developing a response to the Network Information Security Directive (NISD) it has been noted that the definition of what constitutes a standard or a specification in the Directive is fundamentally at odds with recognition of the bodies involved in development of standards. In particular, for Europe, the referencing Regulation (EU) No 1025/2012 excludes almost all of the bodies identified in ETSI TR 103 306 as only CEN, CENELEC, ETSI, ISO/IEC and ITU are recognized as standards bodies whereas industry and society at large recognises a much greater number of bodies. Thus, the present report mimics the approach taken by ETSI TR 103 306 and the ENISA publications in that it considers the nature of cyber security and from this addresses the contributors to standards.

NOTE	This report should be considered as an addendum to ETSI TR 103 306 and to the ENISA report " Definition of Cybersecurity - Gaps and overlaps in standardisation" as it seeks to supplement the material in those documents with a view to making recommendations that are found in the final part of this report.

The present document does not intend to re-write the content of existing work and as ETSI TR 103 306 is a comprehensive study that when combined with other publications from ETSI TC CYBER provide an active resource for analysing the current eco-system of global cyber-security initiatives adding another document to the pile is more likely to muddy the understanding of the environment than to simplify it. However, building on TR 103 306 allows for a few alternative views of how the standards work that is being done is interrelated. This allows us to perform a gap and overlap analysis.

The requirements for standards in the cybersecurity domain can be modelled as a cycle of actions that between them assist the community to:

- Identify threats to, and vulnerabilities of, ICT devices and the services that run on them
- Protect against those threats and vulnerabilities by providing mitigations
- Detect by means of implementation of mechanisms and process that identify a current or imminent cybersecurity event (this requires prior work to identify where such events may occur)
- Respond (implement ability to take action following a cybersecurity event)
- Recover (implement resilience and restoration of impaired capabilities)

Underpinning each of these activities is a core requirement to share security knowledge in a trusted and timely manner. Within Europe and in several other global regions the concept of CERT (Computer Emergency Response Team) has been adopted as a sharing scheme and these have been further developed to use a set of standardised schemes (data definitions and transfer protocols) to categorise incidents.

Figure 1. The security cycle recognised by CERTs.

It is recognised that whilst there are a very large number of bodies that develop standards, it is also recognised that many service providers, manufacturers and governments are involved in a significant number of them. An unfortunate consequence is that each standards body is often in competition with each other, thus generating overlap in the provision of standards. This can constitute a risk to security because ICT infrastructures may be built on overlapping and conflicting security standards, which could generate vulnerabilities (in addition to increase the cost of implementing secure and interoperable systems). An additional concern is that competing standards may not still be able to provide a complete set of standards for a particular function or service. The so called "standards gaps" are often due to this phenomena, which prompt additional effort to address the gaps and generate even more standards, while a more effective way to address the gaps wold be a redaction of existing standards.

ASSERTION Gaps in standards present the risk that additional standardisation effort is started without a structured plan. An effective wat to address standardization gaps would be to redact existing standards.

The plain text variant of the above assertion is that it is not always right to add more standards when a gap is found. Similarly, if conflicting standards exist adding more standards may lead to increased conflict and all conflict increases risk, thus reducing risk requires removing standards from the market to remove the underlying conflict.

Taking the model from ETSI TR 103 306, the global cyber security ecosystem can be visualised as six forms of group that are key categorisations for the identification of who

is involved in cyber security standardisation and in the development of collaborative mechanisms that support the CERT model for cyber security:

1. forums that develop techniques, technical standards and operational practices;
2. major IT developer forums affecting cyber security;
3. activities for continuous information exchange;
4. centres of excellence;
5. reference libraries, continuing conferences; and
6. heritage sites and historical collections.

The security standardisation development eco-system has also got a very large number of complex relationships. Some of that complexity is shown in Figure 2 where industry led forums adopt and adapt standards from (say) ETSI, but ETSI also adopts and adapts standards from these same industry-led forums. As an example IEEE develops standards for Wireless LAN (802.11), adopted by the WiFi Alliance as WiFi standards, adapted in turn in 3GPP to define the use of 802.11 as a coexisting technology with (say) LTE, and then fed back into ETSI to determine use in transport (e.g. ITS group for LTE based V2X communications). It is also important to recognise that generic but wide ranging technical standards such as IEEE's 802.11 encompass a very large number of technologies, not all of which appear in the WiFi set, but some, such as variant 802.11p set the basis of co-operative ITS in both Europe and in wider global regions.

As it has been indicated above, the analysis of cyber-security standardisation can be viewed in many different ways. From the CIA paradigm it can be asked who is addressing what in standards? Thus in Figure 2 core technology domains have been labelled with the principal standards bodies addressing technology aspects.

Security standardisation can be viewed in many ways. In Figure 3 the view shown is of domains including protocols, which encompass semantics and syntax but that may also be considered independently. Similarly, whilst there is work on standardisation of cryptographic algorithms, their value does depend on their availability in specific domains and their role in a structured protocol. It is reasonable to state that all of the domains have standards leaders, but it is also fair to say that the causal and essential links between domains is not well defined.

As described before, a similar survey and landscaping effort has been performed by ECSO in the 'State-of-the-Art Syllabus, Overview of existing Cybersecurity standards and certification schemes' [5]. In this report, the cybersecurity standards have bene classified for categories of applications. Standards and schemes are also identified and described. The report is quite exhaustive but (as described in the report itself), it is meant to be updated periodically to reflect changes in the status of the standards (update, termination or creation of new standards).

For each of the standard, the report briefly discusses (extracted from [5]):

- Focus: What is (main) area of applicability of this standard?
- Associated Scheme and Governance: Does a scheme exist to assess, test or certify people, products, services, organisations or infrastructures against this standard? If there is an associated scheme, how is the scheme governed? Who is the Standard Developing Organisation, who is the certification scheme owner? What are the accredited third-party labs, if any?
- Process: how does the assessment or certification process work? Is self-declaration allowed? Are several different levels of security defined?

- Practice: Is this standard actually being used in practice for assessments or certifications? If so, what is the experience and perceived value in the market? How many subjects are certified?
- Formal Status: Is there any associated legislation, official mandate or other government involvement?
- Relation to other standards/schemes: Is there any official relation with other standards or schemes described in this document?

The ECSO report does not provide specific general recommendations apart from the analysis on specific sets of standards

ENISA has also produced a report on the identification of gaps in standardization in the cybersecurity domain [6]. The report provides an overview of the main standardization bodies involved in the drafting of cybersecurity standards and provides recommendations on mitigating standardization gaps. The first purpose of the ENISA report is to provide a guide for determining an appropriate understanding of the term 'Cybersecurity' to be used in the context of the intended use of the stakeholders and policy makers. The second purpose is to list organisations taking part in standardisation in the area of Cybersecurity, provide an overview of activities and identify gaps and overlaps.

The conclusions of the ENISA report on standardization gaps and related mitigation techniques, which are relevant for this report, are (extracted from [6]):

1. In some areas of standardisation, overlaps exists (like e.g. competing organizations as well as competing technical standardization approaches) and will probably persist due to the political interests of commercial as well as non-commercial organizations.
2. Looking at the dynamically changing landscape of tools and technologies, the lack of applicable standards leads to the situation where technology vendors keep proprietary solutions, while consumers are left without transparency on their systems. Classic approaches to verification of technical requirements (e.g. Common Criteria Protection Profiles) are complex and hard to keep-up with in dynamic markets, technologies and changing threat landscape.
3. Privacy is one of the core European basic rights. It is evident that especially this aspect seems to have been left-out in the technical standards. Some industry practice standards (e.g. PCI DSS) as well as specific requirements exist, but this is not sufficient to enable neutral evaluation of technologies nor services to the national or European privacy regulations.
4. One useful initiative at European level would be to set the overall requirements for security, privacy, and other related security requirements. There are many examples of these from ISO/IEC JTC 1, NIST, and other similar frameworks. What is lacking is a coherent method for bringing together these various frameworks, so when a System, Service or Product has been developed, then the appropriate framework can be used. The number of these frameworks should be minimised or, at least, the relationships between them need to be better understood. There are also of course legal requirements, such as those for Data protection, law enforcement, and Business such as trading information, which may be sensitive. These requirements need also to be put into the framework.
5. Identification of security risks and threats. Too often security products and services are developed without understanding these important issues, and without considering the flexibility (such as replacing algorithms) and life cycle requirements from start to withdrawal from service.
6. It is probably true to say that there are many different standards on several technologies available; what needs to be addressed is the reduction of the proliferation of very similar but incompatible tools and techniques and the provision of essential services to non-expert users.

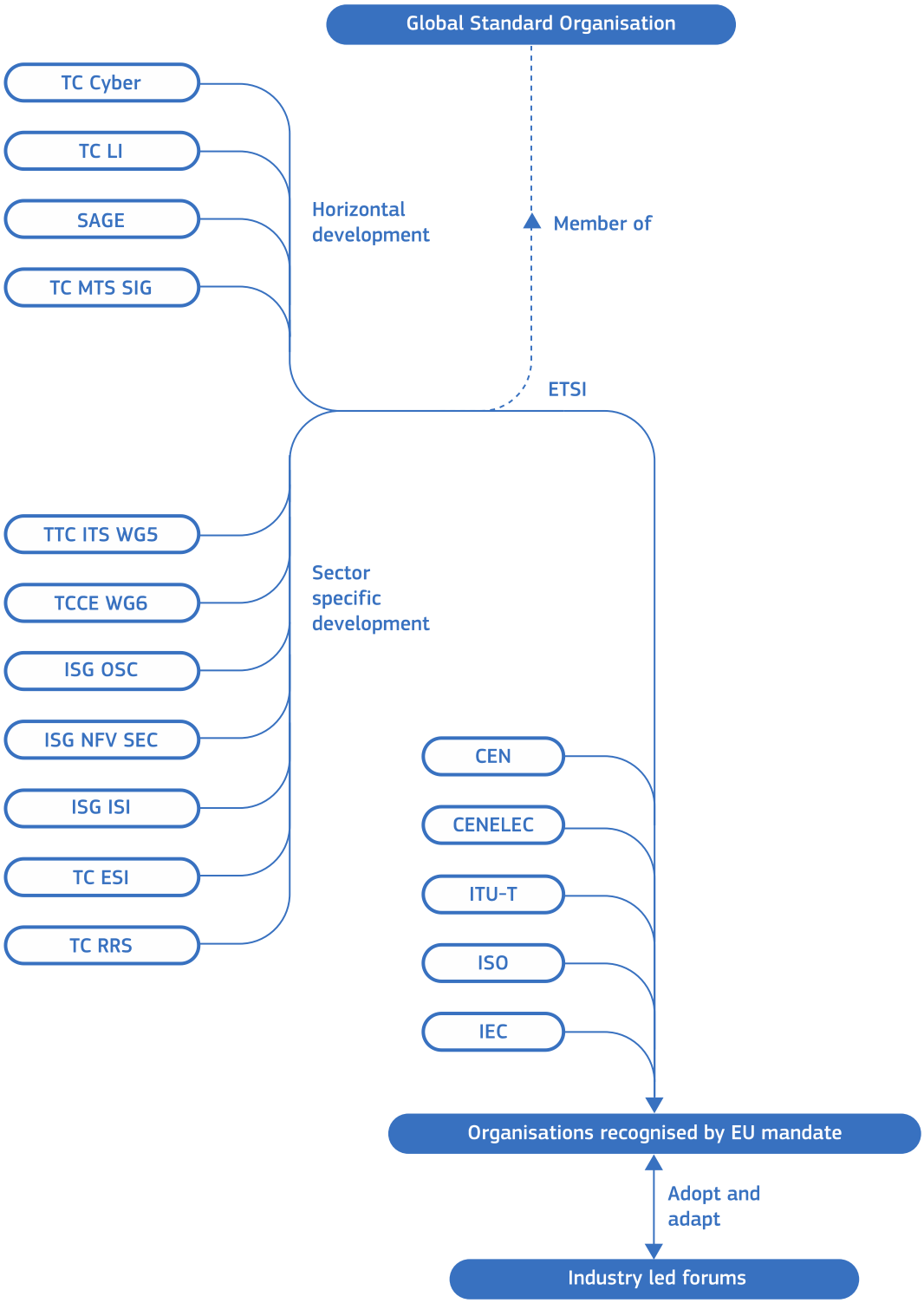


Figure 2. Relationships in the security standardisation development eco-system.

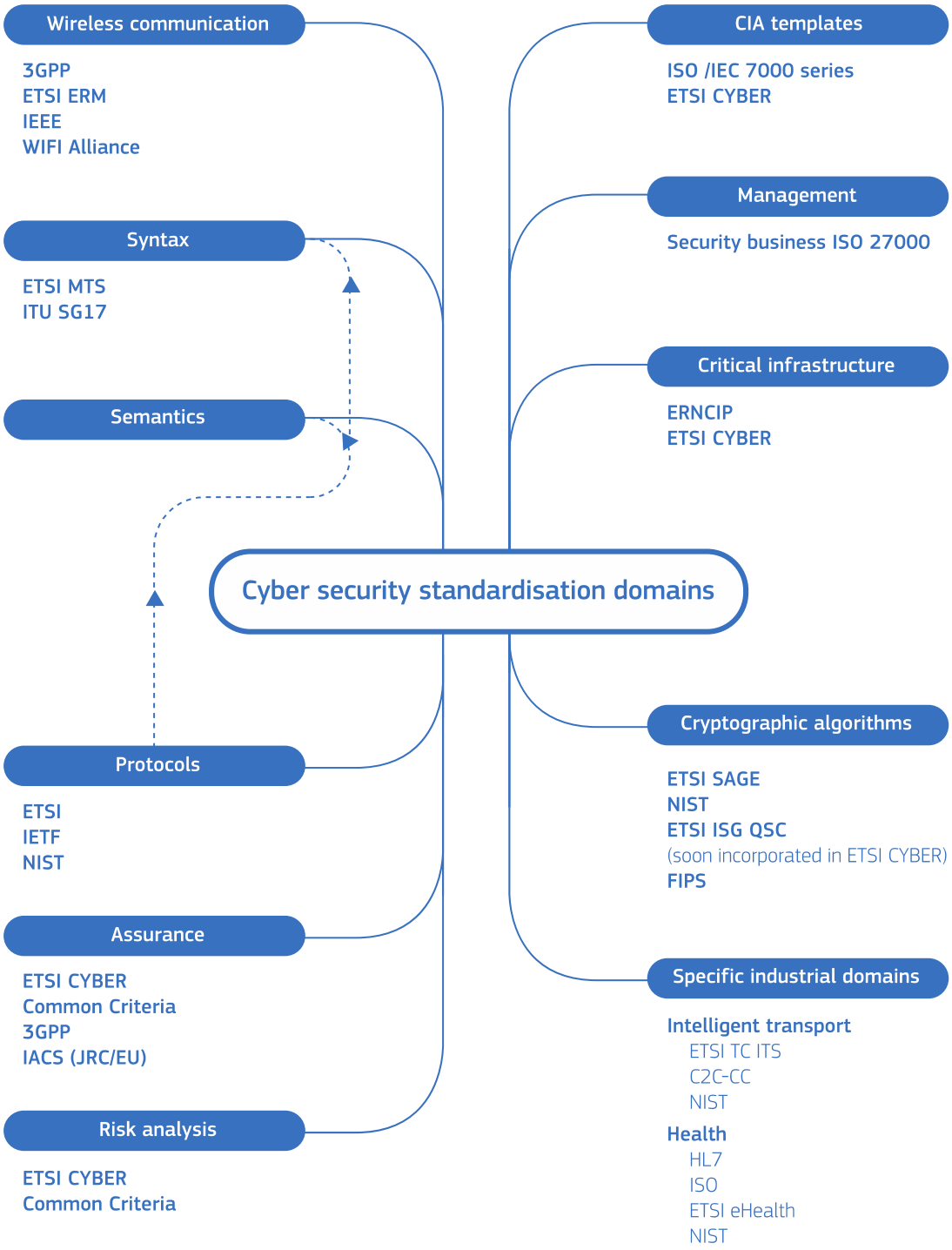


Figure 3. Standardisation domains and key players.

2.4 Testing, verification and assurance

Testing is the root of proof in the core aspects of protocols and code. Tied to the role of testing is a wider concept of certification - a tactile proof of the tests. Illustrated in Figure 4 is the conventional view of standards in testing

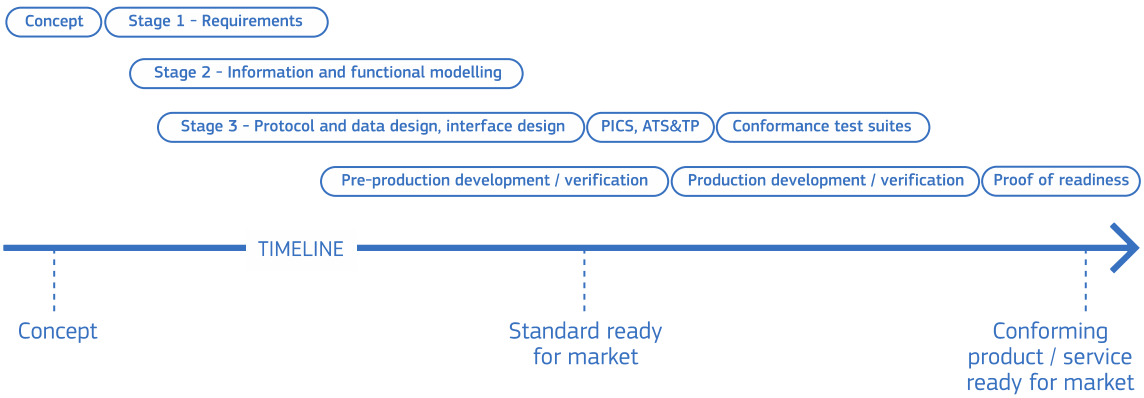


Figure 4. Standards development lifecycle.

Open source projects offer significant support at the start and end of this timeline. They offer a platform for proofs of concept, and they offer a platform for implementation. The bit in the middle, the 3-stage requirements model and the test models are almost entirely missing in open source projects.

Open Source = Code to be implemented
Open Standards = Abstract model of requirements

Whilst conventional formal testing is essential to prove that normal behaviour is achieved the concern in security is that an attacker will seek to subvert the system's operation. Thus to give assurance through testing of a security function, the testing effort requires to attempt to subvert normal operation, or to gain access against the wishes of the system (e.g., in the intrusion detection tests or penetration test). Security breaches however may be evident (i.e. the attacker is prepared to break the system and to leave proof the system is broken) or non-evident (i.e. the attacker wishes to breach the system without leaving evidence of the break). Thus testing has to cover any means to subvert the system and in this case, standards and processes for achieving "penetration testing" of the system have to be written and the resulting tests performed. The problem here is that in complex systems many channels may be used in parallel to mount an attack and the attack may be built up over a long period of time.

It is clear that the test strategies for most protocols and services do not adequately address the problem space of penetration testing and further work has to be done.

An addition consideration is that the testing phase can be further subdivided in a) conformance testing to a specific standard, where the product under test is tested against functional and non-functional requirements and b) interoperability testing where the focus is to ensure interoperability in general and secure interoperability in particular.

2.5 Evolution of the connected world

The world is connected and the model of connection that dominates is the Internet, using the Internet Protocol stack developed in the IETF. However, the Internet is not the actual infrastructure and the infrastructure is dominated by evolution of the telecommunications infrastructure. The telecommunications infrastructure is evolving towards domination by mobile devices and movement from fixed function nodes to virtualised functions that may be moved between physical nodes. This latter activity is exemplified by the activity in ETSI ISG NFV (ETSI Network Functions Virtualisation Industry Specification Group), and has been extended in other groups including ETSI ISG MEC (ETSI Industry Specification Group Mobile Edge Computing), and ETSI TC RRS (ETSI Technical Committee Reconfigurable Radio Systems)

Communications services have similarly evolved from point-to-point circuit oriented telephony through packet oriented telephony and towards server based communication.

The nature of the evolved (evolving) connected world has also led to a significant change in societal mores. Communication has changed for many individuals away from a set of discrete one-to-one conversations, and has embraced a slew of semi-broadcast notifications as stepping off points to shared discussion. This is perhaps best exemplified by postings on Facebook and similar social networking sites, and by the use of Twitter and similar short message posting sites.

The technology of communications services has also evolved with a growth in the deployment of server based communications services. In such a communications model that has evolved from chat services many applications open a shared space on a central server provide communication services from that point. This is in contrast to the conventional "circuit" connection paradigm between the communicating parties. In addition, there is increasing use of Over The Top (OTT) services, those services that are offered on the telecommunications network (most often associated to the Internet) without the awareness of the network provider and for which security is determined by the OTT provider and not by the traditional CSP.

2.6 Design paradigms

2.6.1 End to end security

The classical model for good security is that it should provide end-to-end security. Unfortunately, this is a misnomer and a misdirection. One party's end-to-end may be another party's network security, or end-to-end security may imply only ComSec whereas in a data oriented world it may imply only ITSec (from birth to death of a data object). End-to-End security may be achievable in a system where the designer and deployer has appropriate control on all the main elements and interfaces. On the other side, these are often rare cases in the market. For example, the majority of IoT systems have different interfaces and this increase the complexity and difficulty in implementing end-to-end security.

A more accurate model is peer-to-peer and is the model most suited to networks or elements. Each peer has to trust its partner peers and this should address all topologies: Point to point; Point to multi-point; Broadcast. It should also address all forms of symmetry: Symmetric bi-directional loads, asymmetric bi-directional, uni-directional.

2.6.2 CIA

Security standardisation is complex as suggested above. The technical domain of security however has tended to address security as a set of core attributes that can be considered as a design paradigm. The most common of these is in the context of the CIA (Confidentiality Integrity Availability), as security dimensions. The security capabilities are selected from the CIA paradigm to counter risk to the system from a number of forms of cyber-attack. The common model is to consider security in broad terms as determination of the triplet {threat, security-dimension, countermeasure} such that a triple such as {interception, confidentiality, encryption} is formed. The threat in this case is the interception, which risks the confidentiality of communication, and to which the recommended countermeasure is encryption.

Underpinning the CIA paradigm, and the triplet model, is a clear understanding of risk and threat, which should be complemented by a appropriate risk model like the National Institute of Standards and Technology (NIST)'s Risk Management Framework (NIST SP 800-37) [7] or the Computer Emergency Response Team (CERT)'s OCTAVE model.[8].

2.6.2.1 People or user centric security modelling

In recent years the impact of ICT and in particular the Internet and increasingly the development of M2M and IoT technologies has introduced the concept of privacy protection as an element of security provisions. This offers a new paradigm of person centred security design. An example of the increasing complexity of this is shown in Figure 5 for the health sector. In this mode security technology falls under a supporting role to Privacy Enhancing Technology (PET) and this will include conventional CIA capabilities. A detailed description of privacy aspects and standards is out of scope of this report.

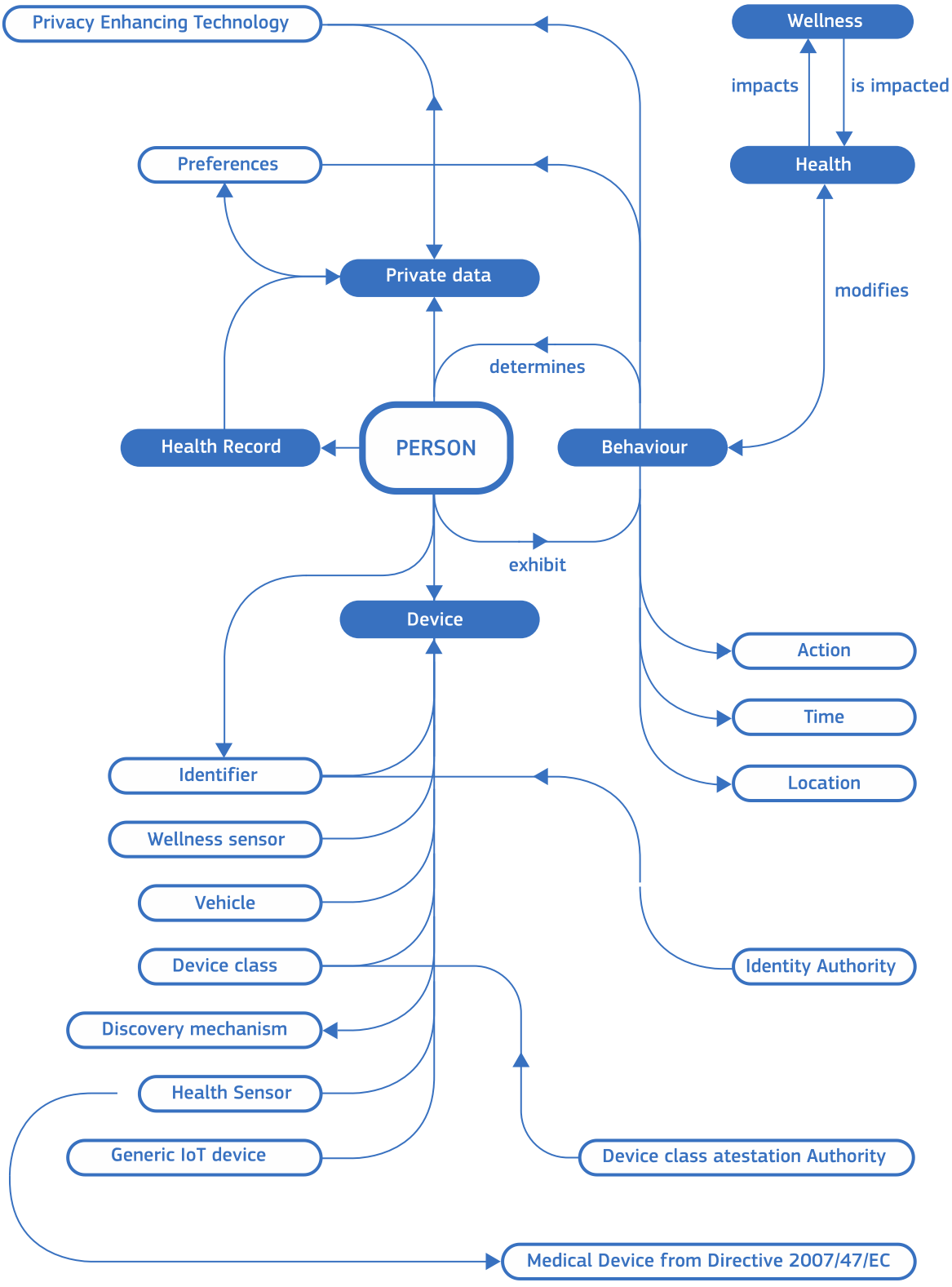


Figure 5. Person centric view of security and privacy (health sector viewpoint).

2.7 Long term evolution of security provisions

Many observers have noted that security is not a technology but a long term process. This is fairly well reflected in the management standards typified by the ISO 27000 series [9] that have broad similarities to the quality management series ISO 9000, the environmental management series ISO 14000 etc.

However, one of the core aspects of security is that the threat model evolves over time. The investment in early attacks may mean that many attack modes take a significant time to appear but once developed are often made publicly available which modifies the risk calculation by impacting the metrics used to evaluate the likelihood of an attack, (e.g., knowledge and expertise of the attacker or the nature of equipment necessary to launch the attack.

2.7.1 Quantum computing and cryptography

There is considerable speculation in industry on the impact of quantum computing on security. The nature of the threat has been explored and published in ETSI EG 203 310 [2], and is being further explored in the ISG QSC deliverable number 4 due for publication in Q1-2017. In particular, the following text from EG 203 310 [2] states (with some editorial extensions):

> *"… if the promise of quantum computing holds true then the following impacts will be immediate on the assumption that the existence of viable quantum computing resources will be used against cryptographic deployments:*
>
> - Symmetric cryptographic strength will be halved, e.g. AES with 128 bit keys giving 128 bit strength will be reduced to 64 bit strength (in other words to retain 128 bit security will require to implement 256 bit keys).
> - *Elliptic curve cryptography will offer no security.*
> - *RSA based public key cryptography will offer no security.*
> - *The Diffie-Helman-Merkle key agreement protocol will offer no security.*
>
> *NOTE: The common practice is to refer to the key agreement protocol developed by Messrs Diffie, Helman and Merkle as simply the Diffie-Helman or DH protocol as the formal recognition of Merkle's role was made after DH became the accepted term.*
>
> *With the advent of realisable Quantum Computers everything that has been transmitted or stored and that has been protected by one of the known to be vulnerable algorithms, or that will ever be stored or transmitted, will become unprotected and thus vulnerable to public disclosure.*"

The developing text from ETSI ISG QSC-004 identifies the following recommendations to be able to determine the extent of the problem of evolution to a QC safe deployment of cryptography:

- X = the number of years that public-key cryptography needs to remain unbroken.
- Y = the number of years it will take to replace the current system with one that is quantum-safe.
- Z = the number of years it will take to break the current cryptographic toolkit, using quantum computers or other means.
- T = the number of years it will take to develop trust in quantum safe algorithms

Quote from development of QSC-004:

> *"If "X + Y + T > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken. There is some limited ability to control T once a set of primitives are developed and put into applications, there is also some ability to assess Y but the value assigned to Y is very dependent on the nature of the cryptographic deployment and the visibility of the enabled devices. The research community in developing quantum computers, and in developing new mathematical analysis of existing algorithms, will always seek to minimise the value assigned to Z which puts increasing pressure on managing the Y factor to ensure that the simplified equation is always in favour of those at risk.*
>
> *As noted in EG 203 310 [2] the most pressing recommendation is that all users of cryptography are able to document and to trial the business continuity scenarios surrounding migration of their entire cryptographically protected set of assets to new, quantum safe protection. This will give a clear, by industry or by sector, assessment of the Y factor, and steps should be taken to ensure that as far as is possible that Y is minimised."*

Furthermore, the factor of crypto-agility requires not simply replacing keys but has to address changes to algorithms, keys and key management protocols.

2.7.1.1 Quantum key distribution

Quantum Key Distribution (QKD) is not a security capability but a provisioning capability. As the correspondents Alice and Bob can successfully agree a key even in the presence of the adversary Eve, there is some potential for random number agreement across an optical link. On the other side of the coin, the random number that is agreed cannot be pre-provisioned so it cannot be used to support any other security function such as identification or authentication.

Standardisation activity is addressed in ETSI ISG QKD.

2.7.1.2 Quantum encryption

It is somewhat unclear if quantum encryption is a real thing or not. The existence of quantum properties, particularly entanglement, suggests that for a pair of entangled photons, one at Alice, one at Bob, then the action on Alice's photon results immediately in the same action on Bob's photon. So in theory Alice and Bob can communicate securely at any distance. It is infeasible to detect the action by interception as there is no movement, hence entanglement (or as Einstein referred to it -- "spooky action at a distance") offers absolute confidentiality. Practically there is no movement though in this space and it remains very much a science research exercise that is very slowly moving into an engineering R&D exercise.

No current standardisation activity is active. No standardisation effort is foreseen as a requirement to manage cyber security provisions in the EU.

2.7.2 Next generation networks

The nature of telecommunications has evolved in the past 20 years or so to become Internet Protocol centric. However, this tends to mask the level of functionality required and applies a single model for connectivity, QoS, GoS and security to all nodes of a network. This view is being challenged by a number of groups that have identified

difficulties in provisioning and maintaining a network that serves multiple, often conflicting, goals and media types.

3 Analysis of potential support to the European cybersecurity industry from standardisation work

3.1 Overview

As described before there are a number of goals of standards, the principal ones being interoperability, market control through freedom of access, market control through regulation, and market creation. The last of these was probably best seen in the development of digital cellular telephony wherein standardisation was driven into the market by mandates on use of spectrum. However, the environment for standards development has changed since the early days of 2G cellular and whilst standards are still developed through consensus by mostly voluntary effort of the stakeholders there is a market for success in standards that may actually drive fragmentation of the market.

Fragmentation of the standards market is a reality. The impact of this is that standards themselves introduce risks as inevitably there is a need to bridge from one standard to another. Wherever a bridge exists it can be perceived and modelled as a system weakness as at least one aspect of interoperability is weak or non-existent.

In attempting to address where European legislators and leaders should drive standards, and security standards in particular, some relatively arbitrary position has to be taken. The remainder of this report therefore takes the stance that ICT security has to be considered as a very important driver in the design of standards and should be held to a higher degree of accountability and oversight than it has in the past. The proliferation of connected smart or programmable devices on the market and the continual growth in market penetration of such devices is a threat if those devices do not get to the market with some degree of basic security. This has a consequence on market control and access in order to ensure that only those products and services which are able to demonstrate a well-defined level of conformance to security principles are made available for ICT. This has an impact on many areas of life from essential areas such as transport, health and wellbeing, to food supply, energy supply, freedom of movement and freedom from attack.

The traditional model of standards development adopted by ETSI, ITU-T and ISO is being challenged and that has to be recognised. In the traditional development cycle a concept is driven through a relatively traditional waterfall development cycle that is shown in Figure 4. The conventions of this cycle are increasingly challenged by the open source community where the gap in time between a proof of concept and a reference implementation is often eradicated and the reference design, in the form of standards, may never exist.

The role of standards in the market is to achieve interoperability and this does take time. The option of using open source projects to demonstrate the viability of a technology at the Proof of Concept point, and later to address the Reference Implementation point may reduce some of the delay associated to standards. However, the bit in the middle, the traditional heavy standardisation effort still requires to be done if an open market based on open standards is to be achieved.

One aspect of standardisation that is understood by those deeply involved but which is often overlooked in the wider technical world is that standards are very competitive. This aspect of standards development of itself is problematic as in a voluntary market many conflicting technologies appear on the market. This is seen in many markets and has the potential to be destabilising to the market.

In many standardisation areas there are gaps in standards that are in part closed by policy or by proprietary development. It is hopefully obvious that simply creating new standards will not lead to more security but may in fact lead to further fragmentation with more standards and more possibility of insecurity.

The underpinning paradigm that has been followed in the technical security standards work has for many years been the CIA - Confidentiality, Integrity, Availability. However, in large systems it is increasingly difficult to simply apply the CIA paradigm as it has been suggested in ETSI TR 103 303 from which the following concerns have been paraphrased:

- Confidentiality
    - The role of confidentiality protection is to ensure that information shared by Alice and Bob is intelligible only to Alice and Bob, and Eve.
    - Confidentiality has a close relationship to privacy (shared meaning in US- English) and to core concepts such as unobservability, anonymity, pseudonymity and unlinkability. For a generic system the more of the system that is exposed then the greater risk there is that an attacker can identify an attack path. However, making the entire system "secret" does not make it more secure as it may lead the operators of the system to a false sense of security, this model of "security by obscurity" has been discredited over a number of years and whilst making everything public is not to be recommended it is reasonable to assume that those intending to attack a system, even if external to the system, have knowledge of the operations and architecture of a system.
- Integrity
    - The role of integrity protection is that if an unauthorized party modifies transmitted data, that modification is detectable by the authorized parties..
    - Supply chain integrity is a special case of integrity and addresses the entire chain to the end user. In this instance the term integrity is closer to the meaning of the term used in written English and refers to the overall trustworthiness of the supply chain and not to the stability of the supply chain.
- Availability
    - The Availability element of the CIA paradigm covers a wide range of aspects including access control, identification, authentication, reliability, resilience and monitoring (for the purpose of assuring availability).
    - Any system that is classified as Critical, and the services it supports, will almost inevitably become subject to a higher degree of accountability to 3rd parties than non-Critical systems.
    - Provisions for adequate security protection may require to be independently verified. However, many of the existing schemes for such assurance are not scalable to very large and mutable systems.

3.2 Certification and consumer/buyer confidence

A significant step in giving security assurance to users and purchasers is the Common Criteria for Information Technology Security Evaluation (commonly known as Common Criteria or CC). The intent of CC is that its adoption permits comparability

between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

An important note that is found in the introduction of the Common Criteria is:

> *"… the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs."*

As such this reinforces the primary problem of security assurance and certification as being uncertainty regarding the deployment environment and context.

There is a significant risk in using simple markings or certification of products when it comes to security as the environment may be unpredictable. This is why, Common Criteria certification should be (and it is usually true) complemented by a description of the test environment and product configuration against which the Common Criteria evaluation was performed. In a similar way, "label" concepts as it was recently proposed must include a description of the related testing environment and configuration.

3.3 Extension of CE marking and labelling concept.

The well-known CE mark is a pre-cursor of placing many items on the market in Europe and demands that product is compliant with certain standards to give confidence of safety. Specific CE marking is required in many domains including medical devices, toys and cooking equipment, and for Radio devices.

There are no specific security requirements required in existing CE marking domains but it may be argued that for certain environments where a product has a specific security function that the relevant test and protocol standards are cited for the CE mark to be offered.

It is noted that the CE mark has been criticised by ANEC[5] and others in a number of publications. Such criticisms may not be valid, but they should be still taken in consideration in a possible extension of the CE marking to the security domain like the so called labelling concept described in COM(2017)477, Cybersecurity Package Proposal for a regulation[6]. The concern here is that security is contextual as described before. A surrounding concern is that it will take considerable time to develop the mark itself, to develop the standards that will be indicated by the mark, and finally to develop the market confidence in the mark. On the other sides, existing security standards could be used as a basis to support the label concept.

One potential way to go to is the adoption of the collaborative Protection Profile (cPP) approach across SDOs. This has already been proposed in ETSI's "Design for Assurance" scheme in ETSI TS 102 165-1 wherein there is a strong rationale for the application of security measures rooted in a detailed, quantitative threat analysis. The positive element of a cPP approach is that by default a standard is developed by a community of like-minded organisations (i.e. it already meets the community and collaboration element of a cPP). Furthermore, a standard is an abstract set of requirements that have to be met rather than a definitive design to be rigorously adhered to.

[5] http://www.anec.eu/attachments/ANEC-SC-2012-G-026final.pdf
[6] https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en#proposal-for-a-regulation

3.4 Extension of ETSI TR 103 303 as guidance to standards makers.

ETSI's TS 103 303, addressing key characteristics of ICT in Critical Infrastructure, could be extended to address the ICT security general cases.

Taking the base principle in security of that for any system that is at risk of attack a very simplified model of protection is that based on the sequence of events identified in part 1 of this report:

- Identify threats to, and vulnerabilities of, ICT devices and the services that run on them
- Protect against those threats and vulnerabilities by providing mitigations solutions and practices.
- Implement mechanisms and processes, which identify a current or imminent cybersecurity event (this requires prior work to identify where such events may occur. In other words, a training phase of the detection system).
- Implement respond mechanisms (implement ability to take action following a cybersecurity event)
- Implement recover mechanisms (implement resilience and restoration of impaired capabilities)

This can be further simplified as a set of actions to take as:

- Plan (for the CERT recognised Identify and Protect actions)
- Detect
- React (for the CERT recognised Respond action)
- Recover

The key assertion to make is that any reaction without a plan, reaction without knowledge of what is being reacted to, and reaction without a means to recover, is an ineffective reaction. The role of standards in this cycle is to ensure consistency in how each of these actions is performed and to then provide a sound technical basis for both the means to protect and the means to share knowledge to ensure that all systems work together to protect themselves and their neighbours.

For any ICT system the identification of the stable state is a prerequisite to determining it is under attack and with the assertion that immutability is not an achievable or desirable state and that a mathematical statement of the stable or normal state is unlikely to be achievable or accurate the following should be addressed by the responsible parties of the system during the planning and detection phases:

- Identification of normal usage patterns
- Fore-planning of exceptional usage patterns
- Identification of normal hysteresis level in the system
    - This requires knowledge of how long the system requires to become stable (i.e. to resort to a normal state) after an impulse like stimulus (e.g. a step change in network traffic loads either predicted or exceptional).
- Identification of standard deviation from normal behaviour in the system
    - Normal behaviour, as suggested above, is rarely constant or static but operates within certain bounds. Knowledge of these bounds to determine normal versus exceptional behaviour is essential to determine if the behavioural changes in the network lead to CI risk.
- Identification of long term trends in the system (including seasonal trends)
    - As above but noting that there may be seasonal changes in the expectation of normal (e.g. higher demand for electricity in winter as more

households use heating, therefore the summer time normal figure cannot be used as a normal figure in winter).

3.5 Areas for future standardisation mandates.

4.4.1 Policy direction

It is strongly suggested that, as standards proliferation leads to market fragmentation and thus to increased risk, measures should be put in place to withdraw standards from the market and to mandate certain provisions for ICT devices and services prior to them being placed on the market. The policy measures should therefore place security proof and assurance within the market access framework. For standards development bodies this may require reinforcement of Harmonised Standards for security functions as opposed to mass provision of lower level technical specifications.

It is recognised that this is a politically sensitive area and has some impact on market access.

4.4.2 Integrity measures

When considering recovery, the recovered system should exhibit the same overall behaviour but may achieve that in a different way from before the attack. In such an event the same steps as determining the initial stable state have to be taken.

4.4.3 Availability measures

The model for any "at risk" system is to give access to system components and operations on a "need to know" basis. Whilst some systems may require physical isolation and demand only physical access with detailed multi-factor authentication schemes in place, the reality of large scale integration of ICT capabilities suggests that the norm will become that all systems will have some form of remote control or remote monitoring in addition to direct onsite control and monitoring.

Actions which impact the system should be accounted for. This may be achieved by simple logging but accounting records should be protected with tamper resistant systems, which are able to retain evidence of tampering attempts.

Access control systems should not inhibit access where an override may be necessary to allow for instances such as providing critical care or to prevent escalation of an incident.

4.4.4 Resilience and recovery measures

When a system has been compromised it is reasonable to assume that when it is recovered it will perform the same set of functions but the means to perform those functions will be different from those used prior to the compromise.

The key points for successful resilience and recovery are:

- Has the underlying attack been defeated?

- Has the weakness or set of weaknesses in the system that allowed the attack to be launched been isolated?
- Has the weakness or set of weaknesses that allowed the attack been removed?
- Have relevant stakeholders and partners been informed?
- Have the systems of relevant stakeholders and partners been immunised in like manner?

4 Summary and Recommendations

Standards in general are designed to give assurances of interoperability of two or more independently developed implementations of a device or service. Security standardisation extends the interoperability goal to provide assurance that users of devices and services will not be subject to malicious attacks against their identity, their communication content or their communication intent. In addition, the providers of services are given assurance that they are protected from malicious actions of their peers and their customers.

Noting that attackers will evolve their methods of attack over time, and recruit devices, protocols and services in novel ways to cause harm, it is important to ensure that those devices and services are themselves able to evolve their defences over time to limit the level of damage that attackers can inflict. The role of standards in this goal of maintenance of security is itself critical and requires that vendors and operators work together to bring security agility to the market.

The scope of "cyber" is growing with few devices or services being developed that are either not in part enabled by software, or having connectivity capability. The rationale therefore is that devices which have either connectivity or software modifiable functionality should be protected against exploit of these software and connectivity capabilities.

Key recommendations to ensure that security is properly addressed are the following:

- EU member states should define measures that mandate certain provisions for ICT devices and services prior to them being placed on the market
- Policy measures should place security proof and assurance within the market access framework.
- SDOs should be requested to reinforce the Harmonised Standards approach for security functions.
- The EU should consider sponsoring research and standardisation of means that give authoritative measurement of system integrity in mutable systems.
- The EU should consider sponsoring research and standardisation of means that allow for autonomic reporting of security events to CERTs for analysis and distribution.

5 References

5.1 Citations

[1] ETSI TR 103 306: "CYBER; Global Cyber Security Ecosystem"

[2] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection"

[3] IEEE 1609.2: "EEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages"

[4] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats"

[5] Common Criteria Group: "ARRANGEMENT on the Recognition of Common Criteria Certificates In the field of Information Technology Security", from http://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf

[6] ECSO, WG1 State-of-the-Art Syllabus, Overview of existing Cybersecurity standards and certification schemes. April 2017, at https://www.ecs-org.eu (requires registration to ECSO). Status on October 2017.

[6] ENISA Definition of Cybersecurity - Gaps and overlaps in standardisation. https://www.enisa.europa.eu/publications/definition-of-cybersecurity. Published 1 July 2016. Last accessed October 2017.

[7] NIST. NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach. Revision 1 February 2010, w/updates through 6/5/2014.

[8] OCTAVE https://www.cert.org/resilience/products-services/octave/. Last accessed October 2017.

[9] ISO/IEC 27000 family - Information security management systems. https://www.iso.org/isoiec-27001-information-security.html. Last accessed October 2017.

5.2 Additional reading

The following set of documents is not cited in the main body of the report but provide a general background on the status of cyber-security globally and historically.

Recommendation ITU-T X.1205 (04/2008): "Overview of cybersecurity".

ISO|IEC JTC-1 SC 27: "Standing Document 6 (SD6): Glossary of IT Security Terminology," N12806 (2013.10.03), ISO/IEC 27032:2012-07-15.

ENISA, "National Cyber Security Strategies in the World," 2 Feb 2013, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

ETH Zurich, "International CIIP Handbook 2008/2009," available at http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=91952

NATO CCDOE, "National Cyber Security Strategies," 21 November 2014, available at https://ccdcoe.org/strategies-policies.html

Software Engineering Institute, Technical Note, "Generalized Criteria and Evaluation Method for Center of Excellence: A Preliminary Report," December 2009, http://resources.sei.cmu.edu/asset_files/TechnicalNote/2009_004_001_15053.pdf

5.3 Cyber security sources on-line

The following sources are aimed at the development community and contain a number of security recommendations for each platform. In addition the various forums also host discussion on threat mitigation, best practices, user interface design to minimise user uncertainty in the use of security features and so on. A complete and updated list is maintained in ETSI TR 103 306 by ETSI TC CYBER.

Amazon Web Services Forum. A developer forum for services hosted on the Amazon data centre platforms. https://forums.aws.amazon.com/forum.jspa?forumID=30

Android Developers Forum. A developer forum for applications running on the Android OS.http://developer.android.com/develop/index.html

Apple iOS Dev Center. A developer forum for applications running on the iOS OS. https://developer.apple.com/devcenter/ios/index.action

Apple Safari. A developer forum for applications operating via the Safari browser. https://developer.apple.com/devcenter/safari/index.action

Blackberry/QNX. A developer forum for applications operating on the Blackberry OS. http://developer.blackberry.com/

BMC Software. A developer forum for applications running on OS. http://www.bmc.com/solutions/cloud-computing/cloud-computing-management/Cloud-Computing-Management-CCM.html

BSD Unix. A developer forum for applications running on BSD Unix. http://www.freebsd.org/projects/

CA Technologies. A developer forum for applications running on CA Technologies platforms. http://www.ca.com/us/cloud-solutions.aspx

Cisco Developer Network. A developer forum for applications running on Cisco OS platforms.
http://developer.cisco.com/web/partner/search?technologyIds=a0G400000070wGiEAI

GitHub. A developer software exchange forum. https://github.com/

Google Chrome. A developer forum for applications running on the Chrome browser. https://plus.google.com/+GoogleChromeDevelopers/posts

Google Developers. A developer forum for applications running on the Google platforms. https://developers.google.com/

HP Cloud Services. A developer forum for applications running on HP cloud platforms. https://hpcloud.com/content/about-us

IBM developerWorks. A developer forum for applications running on IBM platforms generally. http://www.ibm.com/developerworks/aboutdw/contacts.html

IBM z/OS. A developer forum for applications running on IBM's Z/OS. http://www-03.ibm.com/software/products/en/developerforsystemz

iCloud for Developers. A developer forum for applications running on the Apple Cloud platform. https://developer.apple.com/icloud/index.php

Intel Cloud Builders. A developer forum for applications running on Intel cloud platforms. http://www.intel.com/content/www/us/en/cloud-computing/cloud-builders-provide-proven-advice.html?cid=sem116p9128

Jive apps developers. A developer forum for applications running on Jive. https://developers.jivesoftware.com/community/index.jspa

Linux Foundation. A developer forum for applications running on the Linux OS. http://www.linuxfoundation.org/

Microsoft Azure Community. A developer forum for applications running on the Microsoft cloud Azure OS. http://azure.microsoft.com/en-us/solutions/dev-test/

Microsoft Internet Explorer. A developer forum for applications running on the Microsoft IE browser. http://msdn.microsoft.com/en-us/default.aspx

Microsoft Windows. A developer forum for applications running on Microsoft Windows OS. https://dev.windows.com/en-us

Mozilla Firefox. A developer forum for applications running on the Mozilla Firefox browser. https://developer.mozilla.org/en-US/

Mozilla Thunderbird. A developer forum for applications running on the Thunderbird mail platform. https://developer.mozilla.org/en-US/

OpenShift Developer Community. A developer forum for applications running on the OpenShift Cloud OS. https://openshift.redhat.com/app/platform

OpenStack Developer Community. A developer forum for applications running on the OpenStack OS. http://www.rackspace.com/blog/

Opera Software. A developer forum for applications running on the Opera browser platform.http://www.opera.com/developer

Oracle Cloud Computing. A developer forum for applications running on the Oracle Cloud platform. http://www.oracle.com/us/technologies/cloud/index.html

Oracle Java. A developer forum for applications running on the Java OS. http://www.oracle.com/technetwork/java/index.html

Oracle Solaris/Trusted Solaris. A developer forum for applications running on Solaris OS. http://www.oracle.com/us/sun/index.htm

ProgrammableWeb. A developer forum for applications running on the Programmable Web platform. http://www.programmableweb.com/

Qihoo 360. A developer forum for applications running on the Qihoo 360 browser. http://ir.360.cn/phoenix.zhtml?c=243376&p=irol-newsArticle&ID=1547787

SourceForge. A developer software exchange forum, http://sourceforge.net/

TopCoder. http://www.topcoder.com/

VMware Community. A developer forum for applications running the VMware OS. http://communities.vmware.com/groups/

XDA Developers Forum. A developer software exchange forum. http://forum.xda-developers.com/

List of abbreviations and definitions

3GPP	Third Generation Partnership Project
AC	Alternating Current
C2C-CC	Car to Car Communication Consortium
CC	Common Criteria
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CIA	Confidentiality Integrity and Authenticity
C-ITS	Co-operative Intelligent Transport Systems
ComSec	Communications Security
cPP	Collaborative Protection Profile
cPPP	contractual Public Private Partnership
DC	Direct Current
DDoS	Distributed Denial of Service
DSM	Digital Single Market
ETSI	European Telecommunications Standards Institute
ERM	Radio Spectrum Matters
ERNCIP	European Reference Network for Critical Infrastructure
ESI	Electronic Signatures and Infrastructures
FIPS	Federal Information Processing Standard
GoS	Grade of Service
HL7	Health Level Seven International
IACS	Industrial Automation and Control Systems
ICT	Information and Communication Technologies
IEC	The International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISO	International Standards Organization
ITS	Intelligent Transport Systems
ITU	International Telecommunications Union
ISG	Industry Specification Group
ISI	Information Security Indicators
LI	Lawful Interception
M2M	Machine to Machine
MTS	Methods for Testing and Specification

NIST	National Institute of Standards and Technology
NFV	Network Functions Virtualisation
OTT	Over The Top
PET	Privacy Enhancing Technologies
QKD	Quantum Key Distribution
QoS	Quality of Service
QSC	Quantum-Safe Cryptography
R&RMP	Resilience and Recovery Management Plan
RRS	Reconfigurable Radio Systems
SAGE	Security Algorithms Group of Experts
SCADA	Supervisory Control And Data Acquisition
SDO	Standards Developing Organization
SWD	Staff Working Document
TC	Technical Committee
TCCE	TETRA and Critical Communications Evolution
TR	Technical Report
WiFi	Wireless Fidelity

List of figures

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (http://europa.eu).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

KJ-NA-29198-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/287101

ISBN 978-92-79-81856-1