

Information Security Certifications

A Primer:
Products, people,
processes

Carsten Casper and Alain Esterle

European Network and Information Security Agency
Technical Department

Deliverable 2.1.5/2007

December 2007



Index

| | | |
|----------|---|-----------|
| 1 | SUMMARY | 1 |
| 2 | INFORMATION SECURITY CERTIFICATIONS IN GENERAL | 2 |
| | 2.1 WHY IS CERTIFICATION IMPORTANT? | 2 |
| | 2.2 WHAT IS THE DIFFERENCE BETWEEN ACCREDITATION AND CERTIFICATION? | 4 |
| | 2.3 WHY SHOULD I TRUST A CERTIFICATE? | 4 |
| | 2.4 HOW AM I EVALUATED TO GET THE CERTIFICATE? | 5 |
| 3 | DIFFERENT TYPES OF INFORMATION SECURITY CERTIFICATIONS | 6 |
| | 3.1 WHICH CERTIFICATION SHALL I CHOOSE? | 6 |
| | 3.2 CERTIFICATION OF PROCESSES | 6 |
| | 3.3 CERTIFICATION OF PEOPLE | 7 |
| | 3.4 CERTIFICATION OF PRODUCTS | 9 |
| 4 | TRENDS IN CERTIFICATION | 11 |
| | 4.1 ARE CERTIFICATES LEGALLY REQUIRED? | 11 |
| | 4.2 WHY ARE MOST CERTIFICATIONS NOT MANDATORY BY LAW? | 12 |
| | 4.3 WHAT IS THE GOVERNMENT DOING ABOUT ALL THIS | 12 |
| 5 | FUTURE AND RECOMMENDATIONS | 13 |
| 6 | APPENDICES | 16 |
| | 6.1 TERMS & DEFINITIONS (EXTRACT FROM SC 27 STANDING DOCUMENT 6 (SD 6) - GLOSSARY OF IT SECURITY TERMINOLOGY) | 16 |
| | 6.2 LIST OF REFERENCES | 16 |



1 Summary

The availability of accreditation and certification schemes can contribute to the trustworthiness of electronic products and services by raising the level of security. Information about such schemes should be widely disseminated. In order to be able to promote the use of existing schemes, ENISA has made an assessment of the need to facilitate the functioning and accessibility of accreditation and certification schemes and how this could be done in co-operation with the relevant standardisation bodies. This work included consideration of IT security certification of management systems as well as product and people certification.

ENISA brought together organisations that are active in the field of information security certifications to present and discuss their schemes, with the aim of identifying commonalities and differences between them. This was done in the form of a mailing list and online collaboration platform, about a dozen **position papers**, a **questionnaire-based survey** which collected answers from 30 certification experts, and finally a **workshop** held in November 2006 which attracted more than 20 contributions. This report is based on information from all these sources, edited by ENISA. For the most part, the Agency simply captured opinions and contributions from the participants and added information wherever it was necessary to maintain the flow of the document.

This report is intended as an introduction to information security certifications – be it certifications of products, people or processes. It begins by addressing common concepts (Chapter 2), elaborates on certifications of different types (Chapter 3) and analyses trends in certification, offering some general recommendations (Chapter 4). In Appendix 6.1 the reader will find definitions of the main terms used in this report (evaluation, certification, accreditation...).

Examples are given from a number of providers throughout the paper. These should be taken as illustrations only and there is no intention to single out a specific provider for criticism or praise. They are not necessarily those most representative or important, nor is the aim of this paper to conduct any kind of market survey, as there might be other providers which are not mentioned here which are equally or more representative of the market.

In addition, Appendix 6.2 contains a number of external sources where certifications are listed, categories explained and hence, in some way, rated.



2 Information Security Certifications in General

2.1 Why is certification important?

How a certification scheme can improve security and mitigate risks

The value of a certificate is very subjective. What precisely this value is depends on the user's perspective – and on the certificate.

What does it stand for?

Certification Highlights

- Value is very subjective
- Describe clearly what the certificate stands for
- Value of certificate is only as high as its reputation
- The unjustified issuing of a certificate may damage the reputation of the whole scheme
- Certificates are meaningful for comparison with competitors
- Stimulus for improvement
- Following the certification principles helps, even without the final certificate
- Loyalty instrument to attract customers

It is important for every information security certificate that it clearly describes what it stands for. It must describe how it is relevant for the activities that are being performed. If the scope of the certification scheme is too narrow, then it might be easy to obtain a certificate, but this certificate would probably not be relevant for all the activities to be carried out. If the scheme covers all possible aspects, then the evaluation procedure might either be too easy to pass or hardly anyone would actually achieve the certificate.

A good certification scheme also strikes a reasonable balance between the resources that have to be invested and the benefits that can be obtained. In order to achieve this, an organised and clearly written and defined certification scheme is an initial requirement. However, the problem often lies in the interpretation of the certification requirements by the implementers and in the application and usage of the resulting certified item by the organisation.

• Certification (often) prolongs and complements standardisation

The requirements defining a standard are the result of an agreement between professional and, to some extent, consumer representatives at a national, European or international level¹. The use of standards helps to ensure interoperability between different brands of products or services, to facilitate migration between brands and to enhance the flexibility of the market.



A certificate is the successful conclusion of a procedure to evaluate whether or not a professional activity actually meets a set of requirements. These requirements can be those defining a standard or can be chosen without reference to any standard. The certificate gives information to the potential customer on, for instance, the level of security attached to the product or service he is buying, and facilitates a comparison between products or services of different types or brands. The more acknowledged and widespread a certificate, the more valuable the information it provides and the easier the comparison between products and services.

Certification often means compliance with a standard. By way of illustration, the so-called 'Common Criteria' is a certification scheme where the security level of a product is evaluated according to a set of criteria defined in the international standard ISO/IEC 15408. Concerning the organisational security of entities, more and more certificates are delivered based on compliance with the international standard ISO/IEC 270001 (see more detailed discussion in Chapter 3).

• Certification provides guidance

Starting a certification process requires the future certificate holder to explain and document capabilities and evaluate weaknesses, based on information from the certification scheme. Appropriately designed certification schemes can also help to use and configure a product or service in a secure and legally compliant way (because such a configuration has to be elaborated on during the certification process). Organisations could even follow the principles of a certification scheme without actually achieving the certificate. Certification schemes also improve security because they are a stimulus for improvement, as companies and individuals aspire to the reputation attached to the certificate.

¹ For more detailed analysis of standards and standardisation bodies for network and information security, see for instance "Overview of Current Developments in Network and Information Security Technologies – version 2006, annex 1", in: www.enisa.europa.eu/doc/pdf/deliverables/enisa_overview_of_nis_developments.pdf

2 Information Security Certifications in General

- **Certification as a marketing instrument**

On the one hand, certificates give organisations confidence that they have done enough to protect their assets. It enables risk managers to gain credibility in the eyes of management. On the other hand, certificates are proof to the outside world, to customers, suppliers, shareholders etc. that their information is secure and that the organisation is worthy of their trust. A certificate is a way of showing that someone, an individual or an organisation, is committed, or even good at something. And a certificate gives its holder an advantage over a possible competitor. If two companies, candidates or products are certified according to the same scheme, the level reached can be compared. Certificates give customers the chance to compare worldwide products and solutions which have been checked and verified with the same criteria. For this reason, certification as a loyalty instrument is an effective way to attract customers.

- **Certification (usually) does not avoid liability**

Only in very rare cases does a certificate free the certificate holder from any liability if something goes wrong. For example, in the US, holders of an ASIS certificate², cannot be sued for incompetence after a terror attack. In most information security scenarios, however, a person or organisation is liable for failures – with or without a certificate.

- **Certification value**

Managing Certifications (1)

- Identify certifiable process, person or product
- Set objectives for certification
- Identify appropriate certification scheme
- Manage evaluation process
- Obtain certificate
- Review against objectives
- Retire certification if objectives are no longer met

The value of a certification depends on the context in which it will be used and might change over time³. Ideally, organisations would develop a process around the choice and use of certifications. This could include the identification of certifiable processes, people or products, the setting of objectives, the choice of an appropriate scheme, the management of the evaluation and re-evaluation, a review as to whether the certification meets the objectives and finally an option to stop using a specific scheme. Relevant questions could be: Do the benefits still justify the costs? Is my organisation more secure or simply more compliant? Who cares? Is it relevant for customers, suppliers, partners and staff?

- **Value has its price**

Managing Certifications (2)

- Assign a value to each certification scheme
- Can choose more service-oriented or more security-oriented certification
- Avoid a 'certification race'
- Do not create wrong notion of security
- Easy certifications are often useless

Naturally, everything that comes with a value has a price. For certifications, this means an investment in training, documentation and procedures to obtain the certificate. If a certificate brings a high value to an individual or an organisation, then this may justify a high initial investment, e.g. in training and in the certification process. If this high value is achieved with a low initial investment, then the net return is even higher.

- **Avoid wrong notion of security**

A certificate may also generate an unjustified feeling of security, which should be avoided. This can occur if certification happens under very specific circumstances which do not take into account the actual implementation. Such certification tends to decrease the level of information security.

- **Inflation of the value**

The *value* of certification is as high as the reputation attached to it. When certificates are issued to under-par companies, products or individuals, this damages all other certificate holders. It is important to avoid a 'certification race' where the value of a certificate becomes diluted and eventually everybody becomes certified until it is necessary to create a new certification scheme to distinguish real quality from valueless compliance.



² Founded in 1955 as the American Society for Industrial Security (ASIS), the organisation officially changed its name in 2002 to ASIS International, a not-for-profit organisation which disseminates information and educational materials to enhance security knowledge, practice and performance.

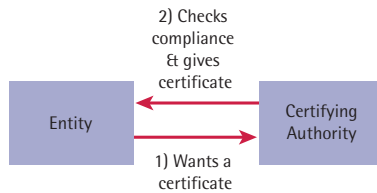
³ For instance, the national British standard BS7799 later became ISO/IEC 27001, giving it international recognition and hence broader acceptance and more value. Another example of value change is when a new vulnerability is identified, which was not included in product evaluation tests.

2 Information Security Certifications in General

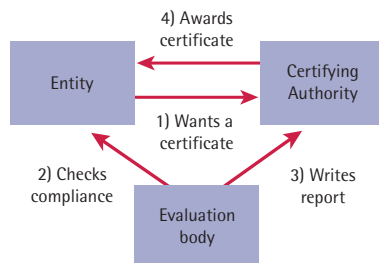
2.2 What is the difference between accreditation and certification?

How to create a hierarchy of trust

In order to obtain a certificate, an entity (people, process, product) has to go through an evaluation. A third party checks whether the entity complies with a standard or with a certain set of rules. If the entity passes this check, the certificate is issued. In some cases, acquiring an information security certificate is as easy as that.



However, the question is whether the certification body or 'certifying authority' treats all candidates in the same way. Since the certification body wants to promote its certificate, it may not be particularly difficult to obtain one. Also, creating and promoting a certification and conducting an evaluation are not the same type of activity. They require different skill sets. To obtain a certain degree of independence, evaluation and certification are often separated. A candidate asks for a certificate, an evaluator checks compliance and, based on the evaluation report, the certification body issues (or does not issue) the certificate.



However, there can still be a close relationship between certifying authority and evaluation body. Moreover, the concept of a 'certifying organisation' is not protected, so in principle any private or public entity can issue certificates. To obtain recognition by the government, a certifying authority has to be 'accredited'. Many product certification organisations are accredited according to the European Standard EN 45011. These EN 45011 requirements on certification bodies are very important. They guarantee the absence of commercial interest in the certification activity. In some cases, the government can also directly empower an organisation with authority for a certain type of certificate: e.g. the BSI in Germany is authorised by law to issue certificates and hence no accreditation is required for the BSI Certification Body; the evaluation labs involved in the certification process are accredited in accordance with ISO 17025. A similar situation occurs in France with DCSSI and the evaluation centres (CESTI).



To make the picture complete, one should include the perspective of the client. In many cases, the desire for a certificate is triggered by a public or private client of a vendor or provider, or the (potential) employer of an information security expert. The entity in question asks for a certificate, the certifying authority asks an evaluation body to check for compliance and the certifying authority issues the certificate. This process is overseen by an accreditation organisation, which itself was created with a government mandate. Such a feature can be seen as a chain of trust where the trust emanates from the top level (accreditation organisation) down to the lowest level (client).

2.3 Why should I trust a certificate?

A certification scheme deserves confidence....

Those seeking certification opt for a specific certificate without being able to analyse all the relevant details of the underlying scheme. They need to trust others who did that before them. They are *confident* that other people evaluated the scheme, its reputation, the evaluation process, its value and usefulness. Ideally, a certification scheme's properties have already been analysed by reputable, independent, well-known parties. There are just different opinions on which these parties are.

...because the government says so

- The government certainly plays a role. It can mandate certification in general (as it does for example for electrical safety standards) or it can require public bodies at least to use only certified products and services. It can install an accreditation mechanism that guarantees the quality of certifying organisations or it can directly empower organisations to issue certificates.

The reputation of the certification body is also important for the trustworthiness of a certificate, strengthened by a strict accreditation scheme and by public mandate and control. Most people agree that independent accreditation, mandated by governments, is the most effective way for a certification to gain and maintain trust.

However, some also say that it is important for a certification scheme to be acknowledged (used) by the public sector or government entities. It is not necessary that the government makes certification according to that scheme mandatory, but it is useful if government entities

2 Information Security Certifications in General

which have a certain authority recognise the value of the certificate and award the organisation with 'points' or other values (such as cutting down on government audits, reducing insurance fees etc).

- **... because independent parties say so**

Not everybody agrees that it is absolutely necessary to have the government involved in information security certification. The most effective way to gain and maintain trust is simply to demonstrate independence from interested parties (vendors, users, evaluators). However, the question then becomes: who is independent? Independent parties (sometimes also called third parties, because they are not directly involved in the interaction) are often foundations, researchers, membership associations or consulting firms which have other sources of income besides selling their opinion on certification. Judging which party is independent can be as challenging as deciding which certificate to trust.

- **... because the market says so**

Information security is evolving rapidly; it takes time for governments to adjust laws and accreditation and to co-ordinate this internationally. New certification schemes are created, without mandate from the government and without being accredited by a government-supported entity.

Then the market decides: people trust schemes because others do so. A certificate is trusted especially if it is used or supported by other widely respected organisations. More importantly, a certification scheme also has a certain brand name. Branding and marketing are very important for a certification scheme that is not accredited by a government entity and that cannot rely on its promotion by independent parties. Moreover, the target audience's view on certification can play a role. A decision-maker who had, for example, a positive experience with an ISO 9000 certification might accept an ISO 27001 certification more readily than someone who perceived a previous certification only as a tedious paperwork exercise without any value.

2.4 How am I evaluated to obtain the certificate?

In terms of security, certificates are often expected to provide evidence of competence (people) or quality (product, process). What they actually show, however, is only compliance. Most of the time third party evaluation consists of checking documents, and rarely includes tests as to whether the implementation works. Examination results (if passed) demonstrate a grasp of the subject, but will never

show how the results are applied. As such, it is similar to an MBA⁴. It only says that you have some knowledge; it does not guarantee that you will be successful in your business. Consequently, certification should not be about what something is, but about how to use it.

It's all about the scope

Certification schemes provide a framework for issuing certificates. This typically includes a scope, rules for evaluation and usually also aspects of renewal. It is very important to describe the scope of the object to be certified ('target of evaluation') precisely and at the beginning of the process. Is it the company or just a department? Is it the professional or just a specific role? Is it the product or just a component? Some certification schemes can be applied narrowly, but may be assumed to be comprehensive by the parties that rely on them. Here, some means of providing a simple scope categorisation would help. Moreover, the appropriate method of evaluation also depends on the size of an organisation and the level of detail that is needed for a given context.

What is often forgotten is that non-transparent certifications involve unclear (and often high) costs. Submitting something to the certification authority and then receiving a simple 'passed' or 'failed' does not make for improvements in the next round. From an end-user's point of view, certifications are not useful if the certificate is easy to obtain and if there is no obligation to renew it.

Types of evaluation

Compliance with a certification scheme can be evaluated in various ways: with an examination/test/checklist, a peer review or with a formal analysis. Although experts have different opinions on the most appropriate method, there seems to be some agreement that people certifications need 'soft' criteria whereas organisation and product certifications need 'hard' criteria.

For people, an examination is considered to be a rather basic form of evaluation and for a more advanced evaluation, a peer review is necessary (although some argue that peer review is vulnerable to 'inbreeding'). For products and organisations, an analysis by an independent third party is required, which often focuses on development or operational processes. However, third party analysis can only work if there is no benefit for the evaluator to just please the client or if there is a surveillance mechanism in place (e.g. distinct entities to conduct the evaluation and to issue the certificate, both accredited as described in 2.2 supra).

A formal evaluation is usually not possible because of its complexity; it also includes numerous error-prone modelling tasks. However, in special environments it is feasible and it is then the best solution (e.g., in the aviation industry).

⁴ *Master of Business Administration*

3 Different Types of Information Security Certifications

3.1 Which certification shall I choose?

The number of certificates issued is often taken as a measure of success. Unfortunately, new (and perhaps valuable) certification schemes suffer from the chicken and egg situation. Few certificates will be awarded until a scheme becomes successful and a scheme will not become successful until a good number of certificates have been awarded. Other ways of perceiving the success of a certificate include the number of references in print and online media or the general reputation of a certification scheme. However, a certificate that is considered a success in one country or in one industry sector may be perceived as a complete failure in another.

Choosing Certifications

- Successful schemes build trust between parties
- Provide useful information, not just a certificate
- Certificate must be relevant for performed activities
- Scheme may be good even if single products fail
- Balance resources invested and benefits obtained
- Promote usage without diluting the value

It is a common belief that the more widespread a scheme, the more successful and the more valuable it is. Global organisations in particular will look for global certifications, rather than local solutions or variations. A broad distribution of a certification scheme also enables an exchange of experience, and facilitates benchmarking.



Some of the experts involved in the preparation of this report emphasised that the uptake amongst larger companies is a factor which particularly helps make a certification scheme successful. In any case, it is safe to assume that a certification organisation would usually want

to increase the visibility of its certifications. At the same time it must not dilute the value of certificates that have already been issued by reducing certification requirements. Consequently, the quality of the content of a certification scheme is also a key criterion, although it is difficult to measure this objectively. Successful certification schemes strike a reasonable balance between increasing visibility and acceptance of the scheme on the one hand, and maintaining a thorough evaluation process for it on the other.

In addition, having a certificate does not guarantee success and – vice versa – not having a certificate does not imply failure. Nor does the failure of a certified product, a person or an organisation mean that the certification scheme as such is flawed. This must be judged on a case-by-case basis. In general, the key for success is that a scheme builds trust between all the parties involved.

3.2 Certification of processes

The rise of a standard

Years ago, there were a number of standards to certify a process for information security. Countries or industry associations had their own ideas about how to implement information security. Many of these standards are still widely used, be it with a focus on national requirements (such as a specific (non-English) language) or with a focus on a specific industry sector. However, more and more often, and especially in organisations which are equally active in more than one country, ISO 27001 is becoming the standard of choice for the certification of an organisation's information security management system. This is particularly convenient in countries where its predecessor, the British Standard BS7799, or one of its national variations had already been used (e.g. UNE71502 in Spain). There are now more than 70 countries involved in certifications based on 27001, and over 47 certification bodies.

Do we need an 'ISO 27001 light'?

One of the major questions surrounding ISO 27001 is whether it is appropriate for organisations of different sizes. Some critics say that the standard is complex and expensive to implement, and that it is not feasible for smaller organisations – that a simplified, 'ISO 27001 light' is required. However, ISO 27001 supporters warn that a light version would dilute the value of the certification. All that is actually needed is specific guidance for small and medium-sized companies on how to implement ISO 27001 successfully. A light version would also add to the naming confusion caused by the transition from the British Standard to an International Organization for Standardization (ISO) standard, and the ongoing extension of the ISO 27xxx standard family⁵.

⁵ For clarification, see "Clarifications around the BS7799/ISO27xxx family of standards": www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/ICT/Information-Security/BS-ISO/IC-270012005-FAQs/ or "Clarifications around the BS7799/ISO27xxx family of standards": www.atsec.com/01/isms-iso-iec-27001-bs-7799-faq.html

3 Different Types of Information Security Certifications

Supporters also point to the database of certified companies⁶, which includes a large number of small companies, from Europe and elsewhere. Others argue that there are already around 3000 organisations in that database, but there are, for example, 5 million small and medium enterprises (SMEs) in the UK alone. As with other standards, some people are calling for legal requirements, asking that ISO 27001 should be made mandatory, which would also help attract EU funding. However, if such certifications were mandatory, they would lose their value in reducing the cost of projects. Only large companies could afford an ISO 27001 certification. It would be beneficial if smaller companies were able to take part too. This again supports the idea of an ISO 27001 light (see also a concrete proposal for SMEs in 4.3).

A model for improvement

It is important to note that ISO 27001 is not a technical standard. It is mostly about risk management. It is also not a capability maturity model that would tell an organisation how well positioned it is with regard to information security. Rather it is a model for continuous improvement. When a company seeks this certification, it does not just want a seal to display; it wants something that is valuable in context. However, an ISO 27001 certified company can of course use this certificate as a marketing tool, for example on brochures, company stationery and advertisements, although they cannot use it to advertise a product, because ISO 27001 is a system certification and not a product one.

3.3 Certification of people

Profession versus knowledge

There are numerous information security certification schemes for individuals. Most of them are issued by private organisations following a more or less thorough evaluation of the person's capabilities in information security. Some certificates are issued by vendors of security products, basically certifying that the individual is able to operate a specific product.

In most cases, certification of an individual relates to specific information security knowledge. Rarely an individual can obtain the academic credit of an information security professional. This is unlike medicine, for example, where an individual is evaluated and finally awarded the title of doctor which allows him to work in the medical profession. That profession is regulated by law and overseen by accredited bodies. Most information security certification schemes do not have that official mandate, although some are accredited to ISO/IEC 17024.

There are attempts to establish information security as a profession in some countries. According to its supporters, this needs a code of ethics, entry requirements, a common body of knowledge and an examination of judgement, skill level and competency. This should be complemented with a professional development programme, a disciplinary process and a register of practitioners.



Do we need this variety of schemes?

There are lists on the Internet with dozens if not hundreds of different information security certification schemes for individuals, leading to a dynamic 'certification market'.

There might be too many schemes, but this variety also has its value. First, there are different certifications because there are different areas of information security and one person does not have to be an expert in everything. Second, some schemes address the same topics but require a different depth of expertise. Finally, some personal certification schemes are dominant in one region of the world, some in another. Sometimes the language of the certification training and examination is important. The challenge, of course, is to understand the scope and characteristics of each of these certifications.

To train – or not to train?

For many of these certifications, training and evaluation of the obtained knowledge go hand in hand. However, training is not a prerequisite for certification. Often individuals just want to prove the expertise that they already have. Moreover, there is the danger that people who have time or are sponsored can study, attend training courses and take the examination more easily, whereas people who are fully engaged in their work (on information security) do not have the time and resources to obtain a certificate, even though they have provable experience in information security.

⁶ International Register of ISMS Certificates: www.iso27001certificates.com

3 Different Types of Information Security Certifications

Peer-review, paper and perusal

Most certification schemes make their candidates sit an examination. Often this is organised by a third-party examination facility or provider. Many people consider it important that training and certification are not provided by the same company. An additional criterion for certification is sometimes the endorsement of experience by another certificate holder or by current or previous employers. This mechanism goes beyond a test of pure knowledge and provides some proof that the knowledge can be applied in context. Writing a paper on information security can also be part of a certification, as a contribution to the community.

Knowledge expires, so a review of an individual's expertise after some time is important, especially in an area that evolves as quickly as information security. The question, however, is how this can be done. Some schemes count on their certificate holders to continuously update their knowledge. This can happen in various ways, by attending a training course or a conference, or by simply reading a book. Year after year, the certificate holder accumulates education credits. Other schemes believe that this is not good enough. They require their certificate holders to re-sit the examination after a number of years (thus helping the 'certification market' to thrive).

The role of the employer

A major driver – or rather motivator – for an individual to obtain a certificate is the attitude of the employer, be it the current or – more importantly – the future one. The employer's advantage is that he does not have to check in detail the experience of an applicant who has a certificate. Of course, certification is not the only criterion considered and it will only be decisive if two applicants' CVs are equivalent but only one has a certificate. Unfortunately, many recruiters (including company-internal ones who hire external security consultants), do not understand the many certificate abbreviations and thus are not aware of the coverage and the value of each scheme. It is important to ensure that employers pay attention to what candidates do as well as the fact that they can produce a certificate.

What is required is a transition from certified knowledge into performance. First, we certify knowledge. Then, we decide if this candidate is the right person for the job. We need to understand how the certificate transfers into trust. It is important that certification holders not only know about security, but are also able to demonstrate competence in real-life scenarios, e.g. in actually hardening systems.

Good for the ego

The reward for the certificate holder takes several forms. First, a personal certificate enables individuals to achieve their career goals. In addition, in simple terms it gives individuals recognition of their value in the current workplace. However, a personal certificate is no guarantee of promotion.



Just because someone has a certificate does not mean that he is good at what he does. Remember the saying: "What do you call a doctor who graduated last in his class? – A doctor". But, unlike with medical doctors, in most knowledge certification schemes, there is no code of ethics which, if breached, leads to the revoke of one's license to work.

Universities and certification

It should be noted that academic education and personal certification provided by private or public organisations are usually not seen as being in competition. Universities offer credentials, not certificates. However, it is also necessary to discuss the alignment of different certification schemes with academia. Professional certification bodies often have an academic relations programme and provide course content and materials to professors for use in their classrooms. A few universities also provide courses on Common Criteria, IT-Grundschutz or ISO 27001. However, most people see certifications as an additional step after a university education. First, people need a good education in information security, e.g. a university degree. Certification must be seen as career development and as complementary to education once one has acquired some experience – like medical doctors who first obtain a degree, but then need specialised training together with professional experience.

International considerations

Some Europeans are concerned that many major information security certification schemes are 'in the hands of Americans'. This is particularly relevant because the approach to privacy is different in the US and in Europe. To satisfy the demand for a more European scheme, it has been suggested that Europe should acknowledge those who are already certified by awarding new (European) certificates. Such schemes could, for example, take privacy into account in a different way.

3 Different Types of Information Security Certifications

3.4 Certification of products

There are a number of certification schemes for products, albeit far fewer than there are for people. Probably the most well-known scheme is Common Criteria (also known as ISO/IEC 15408), but there are several other government and commercial schemes which certify a certain level of security for a product.

The scope

The development of 'common criteria' was initiated during the 90s, at a time when vastly different sets of requirements were used in Europe and Canada (ITSEC), the USA (TCSEC) and Japan to evaluate the level of security of IT products. The (ambitious) idea was to define a unique set of requirements so that a certificate issued in any one of these areas would be recognised everywhere, thus boosting the fluidity of the IT market.

The result was a unique set of criteria valid for any IT system in order to describe the security-related functionalities (security functional requirements) and the level of security achieved (assurance requirements), as well as a set of seven levels of security combining a number of assurance requirements (EAL for Evaluation Assurance Level).

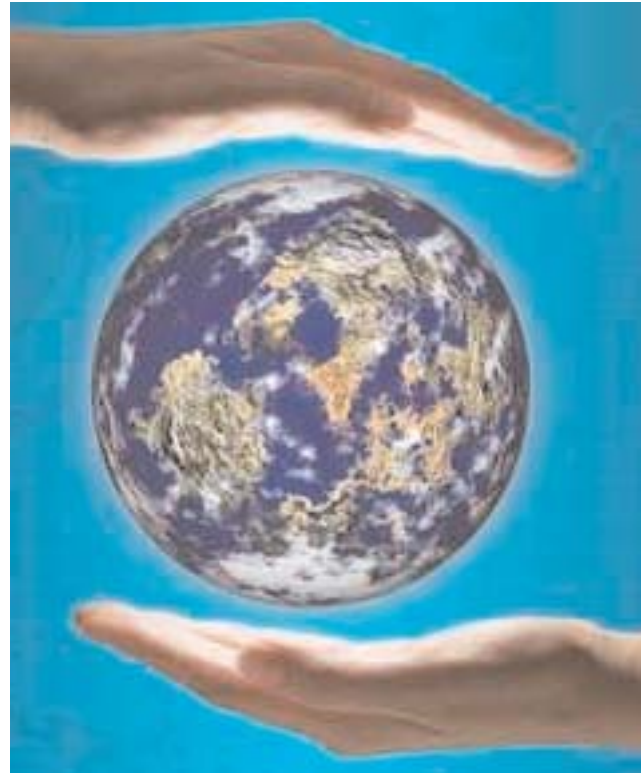
These 'common criteria' were validated by two Mutual Recognition Agreements (MRA), one at the European level in 1999 up to EAL7, the second at the international level (24 countries) in 2000, but restricted to level EAL4. This meant that a certification issued by any of the signing parties would be valid in any other one. Simultaneously, the Common Criteria (CC) became the international standard ISO/IEC 15408.

Since then, the Common Criteria have often been promoted by governments and brought into the spotlight⁷. Such a formal security certification methodology provides a sound foundation on which to build security assurance. It is a toolbox that has to be customised for each area. However it needs to be completed with practical implementation details for specific product ranges, and the Common Criteria Methodology Board meets regularly to discuss the possible interpretation of the criteria, the conditions of implementation and the necessary updates.

Too expensive?

A major inhibitor for widespread certification according to Common Criteria is cost. There are several factors that determine the overall cost of a Common Criteria certification for a product: the desired Evaluation Assurance Level (especially over EAL4, when it includes intrusive actions), the complexity of the product and the choice of the target of evaluation, the control by the developer of the development process and the developer's experience in

security evaluations. Trying to simplify criteria has not proved a successful approach. Cost reduction may be better achieved by enhancing the process, e.g. by interpretation for specific fields where there is recurrence, the reuse of assurance continuity and training.



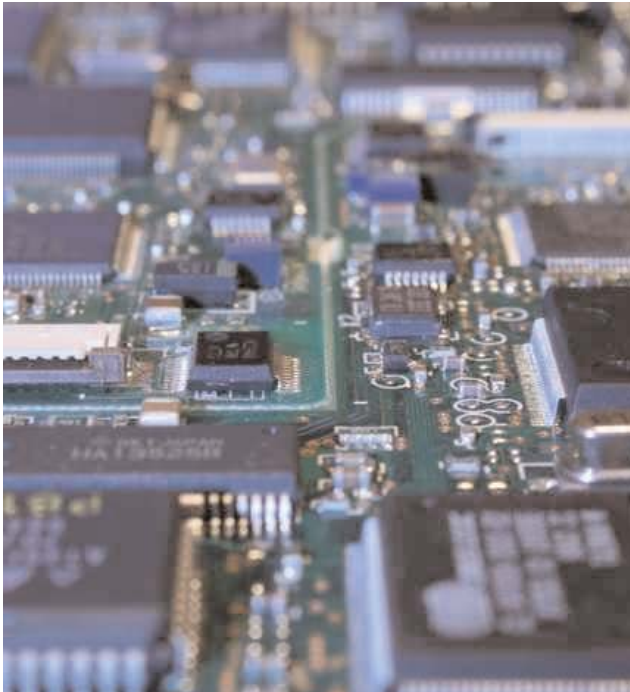
Complex systems, parts versus whole

Critics say that product certifications today (including Common Criteria) focus primarily on product security *features*. There is a lack of standards determining how products should be *built* securely and to prove to the customer that the vendor is making his best efforts to develop his products securely. Rarely can the science of complex systems (systemic) predict the impact of the security of a component part on the security of the whole. Product certifications can only make assertions about the product and select installations of the product. There are no guarantees that the product will not increase risk and exposure to attack once it is deployed in an arbitrary system. For example, although it is certainly valuable to certify smart cards, Europe does not rely on smart cards alone. Europe relies on large open IT infrastructures – where smart cards are used, of course.

Moreover, product evaluations are performed post facto – after the product has been developed and released – so any flaws discovered during evaluation are found too late to be corrected. Also, a product evaluation only assesses product security; it will not by itself *improve* product security.

⁷ List of Common Criteria evaluated products: www.commoncriteriaportal.org/public/consumer/index.php?menu=5

3 Different Types of Information Security Certifications



Product revisions and life cycle

Some of the experts involved in the preparation of this report said that the Common Criteria mechanism is too slow for modern Commercial Off-The-Shelf (COTS) product development cycles. Evaluations are limited to a given version of the product. While COTS products are revised every few weeks or months and CC evaluations take months or years, evaluated products may be obsolete by the time certificates are awarded.

Others argued that the security space is, after all, not that dynamic. The fundamentals are defined and do not change every day.

For similar reasons, no general methodology exists so far for an incremental evaluation of the new version of a product based on the evaluation of the previous version and concentrating exclusively on changes between the two versions. However, maximum reuse of the results of the previous evaluation may reduce considerably the evaluation costs of new versions of certified products.

Coping with emerging threats

A major challenge for all product certifications is the rapidly changing landscape of threats. This makes it difficult to maintain a realistic test bed (e.g. for anti-virus or anti-malware products) against which products could be certified. Individual vendors have only a partial view of the volume of threats, and a community effort to collectively maintain such test-beds requires significant resources. For every step of the evaluation process, the knowledge background of the lab is a major factor in deciding the attacks for the test, but exhaustive tests make the Vulnerability Assessment (AVA assurance requirement)

complex and expensive. Furthermore, there is a delay between the acknowledgement of a new type of threat or vulnerability and its implementation into the test-bed of the evaluation labs.

The extension of a certificate over time is essentially associated with the product's ability to withstand new attacks that appear over time. To assess this ability, some certification bodies offer a certified product surveillance process which consists of regularly revising the vulnerability analysis conducted for the initial evaluation of the product. As long as the evaluation facility in charge of this surveillance does not find any new exploitable vulnerability, the certificate is considered to be monitored.

Security of products is certainly now much better than 10 years ago. Certification according to Common Criteria has helped take security to its current level, and efforts are being pursued to make the 'maintenance' of CC certificates (the certification of a new version of a product, or the validity of the certificate of the same version after emergence of new attacks) more flexible. However, the state of the art of attacks is evolving every day and ongoing research into product security is required. The goal must be that 'state of the art' in terms of threats and vulnerability defines what a product certification must cover, not the other way round.



4 Trends in Certification

4.1 Are certificates legally required?

Why only some certifications are mandatory by law

There is an ongoing debate about the feasibility/appropriateness of making certification mandatory. While those who have to bear the cost and burden of certification resist such legislation, certifying organisations welcome it, arguing that it could be a driver for the certification market and for a more widespread acceptance of certificates.

Unlike with the safety of electrical appliances or aviation security, so far there are only very few legal requirements for certification in information security. Most laws that refer to information security certification are very generic in that respect. They state that certain controls need to be put in place, but do not specify them in detail. However, certification and accreditation complement each other logically. Not only do they indicate that the controls are in place, there is often also a confirmation by a third party.

Examples of a more concrete link between legislation and certification include the following:

- Annex II f and Annex III of Directive 1999/93/EC (the so-called eSignature Directive) establish the requirements for secure electronic signature products. EU Commission Decision C(2003) 2439 regulates that CEN Workshop Agreements CWA14167-1, CWA14167-2 and CWA14169 are generally recognised standards for electronic signature products. Hence it can be argued that products which abide by these standards fulfil the legal requirements of the EU eSignature Directive.

Critics note that, although there are many CWA14619-compliant devices on the market, without a single, secure e-signature application, this picture is not complete. Additional mandatory requirements in this area would help.

- In 2006 the US Government mandated that every product procured for governmental use must have Common Criteria certification, if the product uses encryption. This has boosted the certification market with the creation of a number of new private evaluation teams seeking accreditation.

- The US Department of Defence (DoD) has completed an analysis and Directive 8570 requires that DoD employees achieve one or more of several security certifications. By 2007, 10% of more than 100.000 employees had to be certified, and then every following year another 30% until all these employees are certified by 2010.
- In Switzerland, Federal law on Data Protection⁸ and the Ordinance on certification for data protection⁹ specify that entities certified according to international standards¹⁰ are released from the obligation to notify the data protection authorities of their files containing personal data. The certification bodies have to be accredited by the 'Accreditation Office of Switzerland' (OCDP, art. 2).
- Other examples of legal requirements for certification exist in the area of digital tachographs in Europe¹¹, and Health Care and e-Passports in Germany. The State Data Protection Act of Schleswig-Holstein also refers explicitly to the Privacy Seal issued by the ICPP (Independent Centre for Privacy Protection)¹².
- Concerning information security management systems (ISMS) certification, there are also requirements for paying agencies which deal with the European Agriculture Guidance and Guarantee Fund.

By and large, there are currently not many legal requirements for certifications. However, legal precedents may emerge, particularly in common law jurisdictions, when defendants are given 'credit' for being certified. For example, some governments afford advantages to ISO 9001-certified companies; the same might happen with security certifications.



⁸ See the "Loi fédérale sur la protection des données 235.1, article 11a-5.f" adopted by the Swiss Federal Assembly in 2007: www.admin.ch/ch/f/rs/2/235.1.fr.pdf

⁹ See the "Ordonnance sur les certifications en matière de protection des données, article 4" issued by the Swiss Federal Council, 28 September 2007: www.admin.ch/ch/f/as/2007/5003.pdf

¹⁰ Notably ISO/IEC 9001:2000 and ISO/IEC 27001:2005. The products also have to be certified.

¹¹ See ERCA project: <http://dtc.jrc.it/docs/AA%202005-2006%20and%20Annex.pdf>

¹² See https://www.datenschutzzentrum.de/guetesiegel/eria/information-sheet_icpp_privacy_seal.pdf

4 Trends in Certification

4.2 Why are most certifications not mandatory by law?

The delicate balance between voluntary success and mandated failure

There are also arguments against mandatory security certifications. One argument is that only large companies could afford them, and in particular that costs cannot be justified if information security is not the main objective of the project. Another point is that mandatory certification could backfire because, as a result, the demand for certification might become so high that bogus certificates are issued, devaluing the reputation of the certification. That, of course, depends on the speed with which certification is made mandatory.

There is also concern that the industry would lobby strongly against mandatory certification, rejecting this kind of government help and preferring to leave it to the market to regulate supply and demand. However, some industry representatives say that certification can and should be mandated for special use cases – which is basically the situation we have today. Others point out that there is already adequate entry-level people certification in Europe and that such certification at least could be mandated, as is the case in some Asia-Pacific countries.

Many people agree that government involvement in information security certification should remain limited. A government's role might be to support certifications by defining which certifications have merit and by encouraging the acceptance of these certifications first within their own workforce, then in the private sector. Incentives for (voluntary) use would help promote certifications, for example by reducing obligations for IT security documentation when using certified products and services. Some people also see certification as a minimum requirement in a government procurement process.

Consumers' rights and the free market

Certificates can also be seen as trusted information given to potential customers about the products and services on the market. In that sense, making certification mandatory re-enforces customers' rights. On the other hand, making certification mandatory by law at a time when only few products and services are certified can be seen as suddenly distorting fair commercial competition¹³.

This argument was used in France in 2002 when a decree was adopted to create the certification/accreditation scheme for products; in the event, the decree only *recommended* that the public sector use certified products, rather than mandated it.

4.3 What is the government doing about all this?

Expectations of governments

Apart from requiring information security certification by law, there are some areas where EU and national governments can be of help. First, they have to make sure that internationally recognised certification authorities are adequately resourced, especially those authorities which are responsible for the accreditation of certification bodies.

Another role for governments could be to identify key certifications for Europe. This would help consolidate schemes; promotional activities and additional research could focus on key schemes. Instead of having to try to understand dozens of different certification schemes, users could concentrate on just a few. However, there are concerns that such government intervention would distort the free market. Hence the EU is very careful not to favour one certification scheme over another.

By way of illustration, it is worth remembering that, in early 2002, DG INFSO proposed an extension of the 1999 Mutual Recognition Agreement on the Common Criteria (an intergovernmental agreement) to all Member States through a new directive. The project was eventually abandoned.

The point is that Europe has a very diverse legal base which makes market pervasiveness for certifications more difficult. ENISA or some other European body could co-ordinate the discussion as to whether, and in which specific areas, mandatory certification would add value. Similarly, ENISA could also promote the use of accredited professional security certification schemes.

In addition, the EU and European governments could invest in research to develop more user-friendly schemes, especially for SMEs. A concrete proposal in that direction emerged at the conclusion of the conference co-sponsored by ENISA and INTECO in Barcelona in November 2007, "Risk management: does business need it?": SMEs, certification bodies, Chambers of Commerce and ISO representatives, as well as security experts, agreed an interest in a specific standard of the 27000 family to suit SME conditions. The procedure, timeframe and sharing of roles and responsibilities were briefly discussed.

Finally, there are studies which show that many security breaches occur because of a lack of skills. ENISA or other European bodies could gather empirical evidence to show whether certification helps to address this specific problem.

¹³ See for instance the Directive 1998/34 forbidding the use in national law and regulation of any technical specifications which could distort fair competition throughout the European internal market, and also its extension to all Information Society matters (Directive 1998/48).

5 Future and Recommendations

How will certification schemes develop over the next years?

Those who deal with information security agree that certification against recognised standards will continue to gain wider acceptance over the next years. The challenge is to determine which standards will establish themselves as adding recognised and tangible benefits to information security.

Recommendation 1:

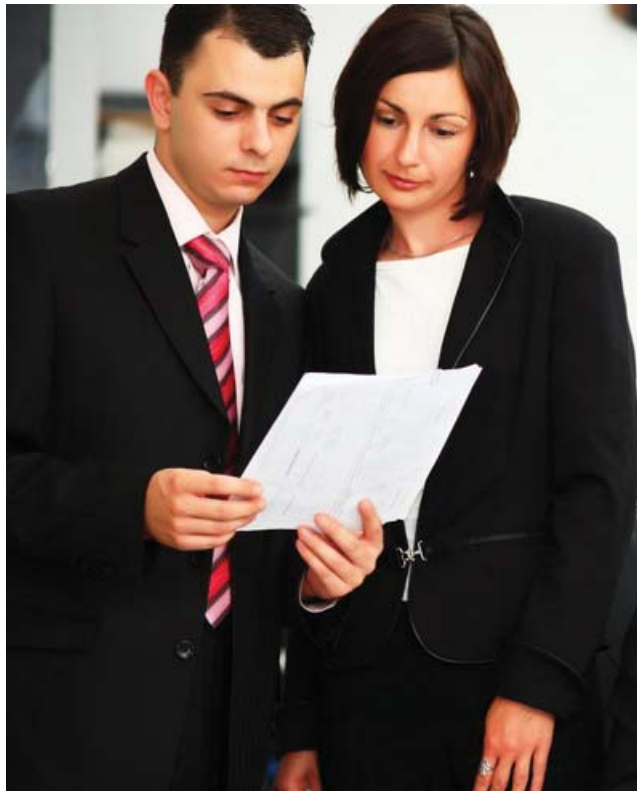
ENISA recommends that organisations should certify their information security management systems, choose certified security products where possible and encourage information security employees to choose one or more appropriate personal information security certifications. For details, please see the recommendations below.

More certifications of organisations

For certification of information security management systems, ISO 27001 is undoubtedly becoming the standard.

A driver for an increasing number of ISO 27001 implementations is certainly the competitive Information and Communication Technologies (ICT) service market. Companies need a tool that will give them something extra in relation to others. One of these tools is certification. Moreover, vendors say they expect to spend more time over the next year complying with information security certification requirements prescribed in supplier agreements into which their companies have entered. Many clients will request a certificate as a precondition for doing business.

However, there is disagreement as to whether ISO 27001 certification is also appropriate for smaller organisations – with the addition of guidance on how to implement this – or whether a new or customised standard for small and medium-sized organisations would be better. While some maintain that ISO 27001 implementation is not just a question of knowledge but also of complexity, others point to the already large number of organisations, both major and smaller ones, which have successfully implemented ISO 27001. Whether that number is a significant proportion of all organisations that could potentially implement it is another question.



5 Future and Recommendations

At its joint meeting in June 2007, members of the ENISA Management Board and the Permanent Stakeholders' Group proposed that one of the priorities for action for the coming years should be "Building information confidence with Micro-Enterprises", leading to the establishment of a specific certification scheme. ENISA has included a Preparatory Action on this issue in its Work Programme 2008 and the Barcelona event in November 2007 (see 4.3) has already sketched a stepwise approach to facilitate the establishment of a specific standard of the 27000 family and later certification schemes at the appropriate level.

Recommendation 2:

Starting from ISO 27001 as the standard of choice for the certification of information security management systems in private and public organisations, the development of the complementary standards of the 27000 family should be encouraged. However, their value must be verified on a case-by-case basis.

The case of small or medium-sized organisations deserves particular attention.

More certifications of products?

The demand for certification of products is less obvious. Some say that the rising number of certifications alone is already an indicator of need. Certainly, as security and privacy issues become more and more difficult¹⁴ (by growing awareness and the increasing complexity of products and services), customers are less able to evaluate these issues by themselves and will therefore have to rely on certificates. Others point to the difficulties inherent in the certification process, where new patches and releases change the certified product, and the use made of products in the real world might differ significantly from the way they were used in a certification lab environment.

Certainly, Common Criteria remain the certification of choice in the defence and general government arenas, especially in cross-border scenarios where mutual recognition is important. For small systems, e.g. smart cards, Common Criteria also deserve – and receive – recognition in the private sector. However, for larger security systems no solid business model based on Common Criteria has been established to date. Efforts continue to enlarge the use of CC (including making it mandatory in some cases) and to make maintenance of the certification more flexible. However organisations can still consider more private and specific certification schemes e.g. in the area of firewall certification or intrusion detection systems certification¹⁵.



Recommendation 3:

Special attention should be paid to areas where Common Criteria evaluation has become mandatory, and to the impact on the market.

The EC should reconsider the feasibility and benefits of extending the intergovernmental Mutual Recognition Agreement on Common Criteria to all Member States as a shared tool contributing to a more secure e-Communication market.

Government, vendors and security experts should analyse ways of building solid business models for product certification according to various schemes.

Framework Programme 7 should consider sponsoring research to analyse the economics of the certification of products.

¹⁴ See for instance http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

¹⁵ See notably in <http://nsslabs.com> and www.icsalabs.com.

5 Future and Recommendations

Re-skilling Europe

Compared with process and product certifications, the market for people certifications is much more dynamic – and also much larger in terms of the numbers of both certification schemes and issued certificates. Furthermore, personal certification will gain more attention as recruiters need to determine minimum hiring standards. Recruiters will no longer be able to fully assess skill sets without using certificates as a pointer. However, the relative 'value' of the different professional certificates remains at the moment widely subjective and market-driven.

In the future, certification schemes will probably adopt various 'grades', i.e. additional levels and different topics, in some ways similar to the variety of Targets of Evaluation and Evaluation Assurance Levels of the Common Criteria. Moreover, all enterprises have to follow privacy rules. Privacy certifications should progressively cover management and process audit as well as product audits.

With an evolving Europe, the re-skilling of millions of people can only be achieved through ICT and some kind of recognised certificate may become a prerequisite for a place in the labour market.

Recommendation 4:

The European Institutions should consider the feasibility of strengthening accreditation schemes related to people certification in IT security as well as a more systematic reference to recognised standards.

The European Institutions should also encourage the development of people certification adapted to different types of professional use of IT systems, from the end-user level (Computer Driving Licence) to the most professional (e.g. IT security officer).

Recommendation 5:

The European Institutions should consider ways to reinforce bridges between education (schools and universities) and the certification process (private training and certificate providers) throughout a professional career.

Recommendation 6:

At a more individual level, ENISA recommends that the decision to seek a certificate should be based on the following questions: Do I want information security to be my certified profession? Do I want to prove that I can work in information security? Do I want to prove expertise in a very specific area of security? Or do I just want to prove IT skills which include aspects of security?




6.1 Terms & Definitions (extract from SC 27 Standing Document 6 (SD 6) – Glossary of IT Security Terminology)

- **Certificate:** a declaration by an independent authority operating in accordance with ISO Guide 58 ("Calibration and testing laboratory accreditation systems – General requirements for operation and recognition"), confirming that an evaluation pass statement is valid.
- **Certification:** Within ISO the more generally used definition is: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements [ISO/IEC Guide 2].
- **Certification body:** an authority trusted by one or more users to create and assign certificates.
- **Evaluation:** Systematic examination (quality evaluation) of the extent to which an entity is capable of fulfilling specified requirements.
- **Accreditation:** Within ISO the more generally used definition is: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks [ISO/IEC Guide 2].

6.2 List of references

1. List of all types of information security certifications, triggered by an ENISA workshop in November 2006 – by Brian Honan
<http://bhconsulting.blogs365.org/wordpress/?p=107>
2. APEC Information Security Skills Certification Guide – browseable and searchable; for professionals and for SMEs
www.siftsecurity.net/default.aspx
3. International Register of ISMS Certificates
www.iso27001certificates.com





For further information about this Position Paper,
contact Alain Esterle (ENISA) at:
info@enisa.europa.eu

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.



ENISA – European Network and Information Security Agency
PO Box 1309, 710 01, Heraklion, Crete, Greece
Tel: +30 2810 39 12 80, Fax: +30 2801 39 14 10
www.enisa.europa.eu