CEN

WORKSHOP

AGREEMENT

CWA 17147

May 2017

ICS 13.310

English version

Guidelines for the evaluation of installed security systems, based on the STEFi dimensions

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

European foreword

CWA 17147:2017 was developed in accordance with CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – The way to rapid agreement" and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was agreed on 2017-03-30 in a Workshop by representatives of interested parties, approved and supported by CEN following a public call for participation made on 2016-09-13. It does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

The final text of CWA 17147:2017 was submitted to CEN for publication on 2017-04-07. It was developed and approved by:

1. European Association for the Co-ordination of Consumer Representation in Stándardisation (ANEC)
2. Belgian Association for Non Destructive Testing (BANT)
3. Ductis GmbH
4. Euralarm
5. Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (by participation of Dr. Erik Krempel)
6. Garante per la protezione dei dati personali (GPDP)
7. Infomation Commissioner of the Republic of Slovenia
8. LINK GmbH
9. Nederlands normalisatie-instituut NEN
10. Slovenian Institute of Quality and Metrology (SIQ)
11. Technological Educational Institute of Central Macedonia, Serres, Greece
12. Technische Universitat Berlin – Zentrum Technik und Gesellschaft/Center for technology and Society (CTS)
13. Technische Universitat Berlin – Fachgebiet Innovation Economics (INNO)
14. Trilateral Research
15. Universitat Jaume I de Castellon
16. VICESSE
17. Vrije Universiteit Brussel (VUB)

It is possible that some elements of CWA 17147:2017 may be subject to patent rights. The CEN-CENELEC policy on patent rights is set out in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patents (and other statutory intellectual property rights based on inventions)". CEN shall not be held responsible for identifying any or all such patent rights.

The Workshop participants have made every effort to ensure the reliability and accuracy of the technical and non-technical content of CWA 17147:2017, but this does not guarantee, either explicitly or implicitly, its correctness. Users of CWA 17147:2017 should be aware that neither the Workshop participants, nor CEN can be held liable for damages or losses of any kind whatsoever which may arise from its application. Users of CWA 17147:2017 do so on their own responsibility and at their own risk.

Introduction

This CWA is based on the results of CRISP (Evaluation and Certification Schemes for Security Products)[1] that was a research project funded by the European Commission[2]. The aim of that project was to develop an innovative evaluation and certification methodology for security systems. The results of this project together with this CWA will be used to establish a certification scheme that will:

— contribute to measures that increase citizen trust and confidence in security technologies through the evaluation of social and legal impacts of security systems as a basis for certification of these systems;

— promote that the use of security systems is based on demonstrated evidence of their security effects and societal impacts;

— enhance dialogue and co-operation between the various stakeholders involved in the operation of security systems in a specific context;

— facilitate a more harmonized playing field for the European security industry by providing pan-European certification for security systems. The aim is to get this scheme accepted across Europe, which would enhance competitiveness by reducing commercialisation costs for the industry;

— support the goal to provide security in an efficient manner.

The innovative part of the methodology for the evaluation of security systems described in this CWA is the assessment of systems from the perspective of four different, though interrelated dimensions:

a) **security** (the functionality and effectiveness of a security system in identifying and mitigating threats and reducing risks related to e.g. accuracy, circumvention, robustness, system interference and performance);

b) **trust** (experiences and perceptions of the users of security systems in regard to their actual performance, both employees and persons subject to scrutiny related to e.g. availability, usability, reliability, system integrity, transparency, and accountability);

c) **efficiency** (economic dimension of the security system related to e.g. the product life cycle costs, such as the purchasing costs, the implementation costs, the operating costs, throughput);

d) **freedom infringement** (impact of security systems on the freedoms and rights of persons, related to e.g. enhanced personal data collection, processing, and retention, due process, complaint mechanisms).

These dimensions are referred to as the STEFi dimensions (**S**ecurity, **T**rust, **E**fficiency and **F**reedom **i**nfringement) and the methodology integrates these in its evaluation phase. This is an innovative approach as certification has, to date, primarily focused on the evaluation of technical requirements for security systems (the security dimension) or singled out other relevant dimensions (e.g. privacy or data protection in the freedom infringement dimension). The methodology described in this CWA, however, is not (over)simplifying the complexity of assessing security systems but acknowledges and addresses this complexity by identifying potential conflicts between the various assessment dimensions and

1 www.crispproject.eu

2 This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607941.

related criteria and by providing an approach to resolve these conflicts in specific situations. The methodology does not single out technical, legal, social or economic aspects, but integrates these in a multidimensional and multi-stakeholder assessment. This novel concept to integrate different dimensions of security systems in a single evaluation and certification methodology will first be piloted for video surveillance systems, to test and refine the STEFi approach. It is foreseen that the methodology and the future certification scheme in which it will be applied can be extended to include other types of security systems. The combination of evaluation and certification of systems is based on the widely accepted functional approach to conformity assessment as described in ISO/IEC 17000 and implemented in conformity assessment of products as specified in ISO/IEC 17065 and ISO/IEC 17067.

The methodology described in this CWA will serve as the basis for a certification scheme that will be developed after finalization of the CRISP project. The future scheme will not redefine the technical requirements that are already included in e.g. European and international standards or existing certification schemes. The future scheme is intended to contribute to the protection of fundamental rights and promote compliance with relevant EU laws, with a particular focus on the General Data Protection Regulation (GDPR) 679/2016[3], by including social, legal and economic requirements in the evaluation and certification of security systems. Certification according to this scheme is initially intended for organizations that install video surveillance systems in a specific context and organizations that procure or employ these systems on their premises.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1 Scope

This workshop agreement describes the methodology for the evaluation of security systems that are or will be applied in a specific context, applying the STEFi approach. The evaluation involves application of STEFi criteria in four dimensions, namely security, trust, efficiency and freedom infringement. These criteria are not only applied individually but also their interrelationships are taken into account and the STEFI approach thus provides a holistic view on the aspects and impacts of security systems. The aim is that the evaluation process described in this CWA will provide reproducible results; i.e. different evaluation bodies that apply the methodology to similar systems in a similar context, should reach similar conclusions.

NOTE 1 It will be part of the management and maintenance of the future certification scheme to enhance reproducibility of results of STEFi evaluation, e.g. by exchange and discussion of experiences, discussing case studies as a basis for further refining the requirements for the evaluation method.

While the methodology that is described in this CWA is generally applicable to all types of security systems, the examples given and the list of assessment questions and requirements in Annex A are specifically related to planned and installed video-surveillance systems in a specific context.

NOTE 2 Application of the video-surveillance systems in specific context implies that the system is already installed or designed and to be installed in specific and already known situations. This is a boundary condition, because otherwise full application of the STEFi evaluation is not possible.

The overall goal of the CWA is to provide a basis for including the STEFi approach for the evaluation of security systems in a certification scheme. The CWA excludes the certification scheme itself. The target group of this CWA are organizations that deal with evaluation of security systems and that are willing to enhance the scope of their evaluation in order to take into account the overall societal impact of these systems.

The methodology is applicable to security systems in a specific context (i.e. installed or planned to be installed). A system is defined as a set of interrelated or interacting components. Individual components of security systems can be certified separately against applicable technical and other relevant standards; if so, it shall be taken into account as evidence for conforming with specific STEFi criteria.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

2.1 Methodology

2.1.1
assessment question
question for assessing a **security system** (2.1.20) in the **evaluation phase** (2.1.13)

Note 1 to entry: The assessment question can either be a yes/no question or a question requesting a qualitative answer.

2.1.2
assessment requirement
requirement to be met by a **client** (2.1.7) and/or a **security system** (2.1.20) that is assessed by a certification body during the **certification phase** (2.1.6) as a basis for the certification decision

Note 1 to entry: Assessment requirements are related to **assessment questions** (2.1.1)