HECTOS

Harmonized Evaluation, Certification and Testing Of Security products

D3.2
Design guidelines for certification schemes
EXECUTIVE PUBLISHABLE SUMMARY

FOI
Iconal
NPL
IGD
DIN

Date: 2017-07-07
Project No: 606861
FOI Designation No: FOI-2012-1271
Dissemination Level: PU(Summary)
Total No of Pages: 4

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 606861.

HECTOS

D3.2
Design guidelines for certification schemes

EXECUTIVE PUBLISHABLE SUMMARY

Version:	1.9
FOI designation no:	FOI-2012-1271
Responsible:	FOI: Anders Elfving
Author(s):	FOI: Anders Elfving, Anneli Ehlerding Iconal Technology: Mike Kemp NPL: Tony Mansfield, Aruna Shenoy Fraunhofer IGD: Olaf Henniger, Naser Damer DIN: Christine Fuss, Christopher Liedtke
Number of pages:	4
Dissemination level:	*PU – valid for the Executive summary*
Start date of project:	Sep, 2014
Duration:	3 years

HECTOS

Summary

HECTOS focuses on harmonisation of evaluation and conformity assessment systems for physical security products, and studies how existing systems and schemes used in other areas could be applied, adapted or developed for products used for physical security of people, property and infrastructure. The project will identify mechanisms to evaluate the performance of security products, as well as compliance with interoperability, regulatory, ethical, privacy and other requirements. Furthermore, elements for a roadmap will be developed as part of the approach towards new harmonised product certification systems.

This report provides design guidelines for certification schemes for security products. Part of the guidelines are originating from a SWER analysis (Strengths, Weaknesses, Enablers, Risks/Issues; a variant of a SWOT analysis) which studies the elements of a certification scheme in the view of stakeholder requirements in order to fulfil them. The approach for achieving the guidelines is schematically shown in the figure below.

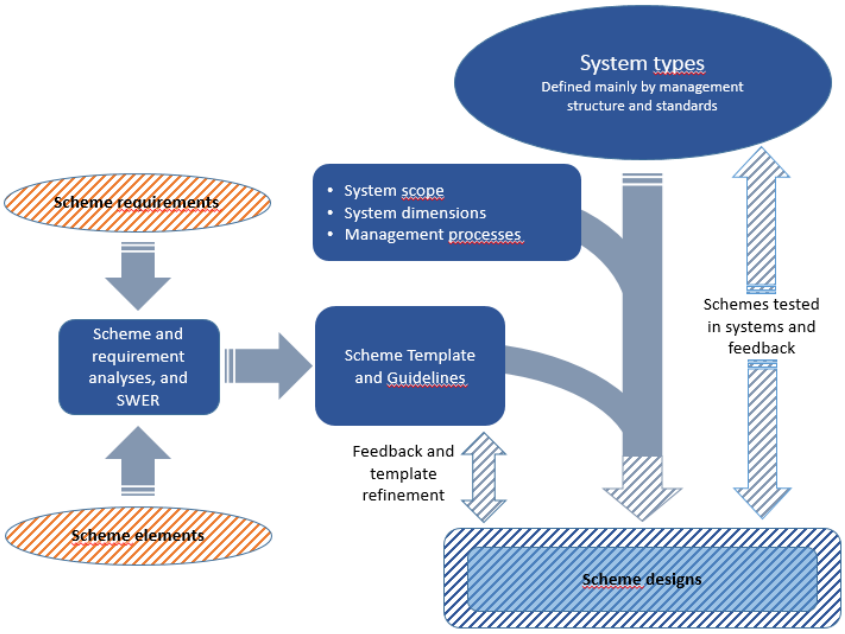

Figure: Schematical structure of the design approach. Dashed activities indicate work outside the scope of this report.

Four certification systems which have the potential to be harmonised have been identified from the analyses and are discussed. Based on the initial studies of these certification systems, it is found that the Keymark and Common Criteria approaches are of particular interest and should therefore be studied further. Both these approaches are well-established for non-security equipment, but they seem to include features and mechanisms which may be applicable to certification of security products with the use of one common certification mark. In case of security product certification against a legislative framework, the CE-scheme is of interest and will be additionally studied.

HECTOS

The design guideline also provides features for a harmonised standard as well as identified management processes for a certification system/scheme. Benefits of evaluation schemes are described as well.

From the scheme template, a few key elements have been identified to be typical or of particular importance for security products. Two important examples are interlaboratory comparison mechanisms for adversarial testing and handling of classified information. Initial studies have shown that the ISO/IEC 17000 standards series is not adapted to some of these security product-specific features. In addition, it does not address the different types of certification system and their relationship sufficiently.

Based on the findings in the design guidelines, recommendations for further activities in the case studies are addressed. For example is verification of inter- and intralaboratory repeatability recommended as a topic for more thorough studies.