

UNCLASSIFIED



D3.1
Analysis of relevant existing schemes

EXECUTIVE PUBLISHABLE SUMMARY

A report prepared by:
FOI
Iconal Technology Ltd
Fraunhofer IGD
Morpho
DIN

Date: 2015-10-29
Project No: 606861
FOI Designation No: FOI-2012-1271
Dissemination Level: RE
Total No of Pages: 3

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

UNCLASSIFIED

D3.1
Analysis of relevant existing schemes
EXECUTIVE PUBLISHABLE SUMMARY

Version:	1.0
FOI designation no:	FOI-2012-1271
Responsible:	FOI
Author(s):	FOI: Anders Elfving, Ida Johansson, Anneli Ehlerding Iconal Technology Ltd: Mike Kemp Fraunhofer IGD: Olaf Henniger, Naser Damer Morpho: Pierre Gacon DIN: Christine Fuss, Christopher Liedtke
Number of pages:	3
Dissemination level:	RE - <i>Restricted to a group specified by the consortium (including the Commission Services)</i>
Start date of project:	Sep, 2014
Duration:	3 years

Summary

HECTOS is an EU FP7 project which focuses on harmonisation of evaluation and certification schemes for physical security products. Today there are very few test, evaluation and certification procedures in Europe for physical security products that are mutually recognized by different Member States. As pointed out in the EC Communication on Security Industrial Policy, this leads to fragmentation of the market, with negative impacts on both suppliers and users. HECTOS 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 schemes.

This report presents an analysis of the existing schemes, both within the area of security products but also selected schemes for other product categories. The analysis, which is based on the functional approach structure of the ISO/IEC 17000 standards series, supports the subsequent enhancement, adaption and development of a certification scheme for security products. The scheme types have been identified according to the type definitions in ISO/IEC 17067. Most of the 25 analysed schemes are of type 5, which includes surveillance in form of product assessment as well as periodic assessment of the production process and/or management system. Type 5 schemes are common for locks, building components and intruder detection products. There are also some schemes which are type 1a-like, i.e. without surveillance functions, which are more often applied to e.g. Biometric, CCTV, and IT security products.

Classification of requirements, test methods and results are example of a particular important aspect for security products. Classified information is typically applied to high security products. The main reason for classified requirements is that they contain information about the threat and should therefore not be disclosed for illicit purposes.

There are some national schemes that are recognised at an international level, often because these are using international (e.g. European) standards, which are well-known and widely accepted. Accreditation of organisations involved in a certification scheme is also essential to reach harmonisation. ISO/IEC 17025 for test houses and ISO/IEC 17065 for certification bodies are currently the most important standards for being accredited to.

In particular, existing certification processes for locks have been studied where there are several mature schemes operating with some mutual acceptance. For low-medium security locks aimed at domestic applications there is a mutual acceptance of testing against relevant EN standards, but national standards with more stringent requirements exist. However, the mutual acceptance of tests on high security locks is less certain. These tests rely much more on human skills for the destructive burglary and manipulation attacks. Differences in interpretation in the level of strength, skill and ingenuity required for tests, mean that mutual acceptance is not assured. For adversarial testing of locks this is even more pronounced, which addresses the need for interlaboratory comparisons. A small number of schemes have been identified as carrying out interlaboratory comparisons, especially for high security locks.