D1.3
Evaluation and Certification Requirements
EXECUTIVE PUBLISHABLE SUMMARY

Iconal Technology Ltd
TNO
FOI
Fraunhofer ICT
Fraunhofer IGD
DIN
Morpho

Date: 2015-09-30
Project No: 606861
FOI Designation No: FOI-2012-1271
Dissemination Level: PU (Summary)
Total No of Pages: 5 (Summary)

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

D1.3
Evaluation and Certification Requirements
EXECUTIVE PUBLISHABLE SUMMARY

Version:	1.0 – Summary
FOI designation no:	FOI-2012-1271
Responsible:	Iconal Technology Ltd
Author(s):	Iconal Technology Ltd: Mike Kemp TNO: Martijn Koolloos FOI: Anders Elfving, Ida Johansson, Jonas Tidström, Anneli Ehlerding Fraunhofer ICT: Christian Ulrich Fraunhofer IGD: Olaf Henniger DIN: Christine Fuss, Christopher Liedtke Morpho: Sébastien Brangoulo
Number of pages:	5
Dissemination level:	PU – *Public (Summary)*
Start date of project:	Sep, 2014
Duration:	3 years

HECTOS

1 Summary

HECTOS is a European FP7 research project investigating the harmonisation of evaluation, certification and testing of physical security products. The HECTOS project focuses on the evaluation and certification schemes for physical security products, and studies how existing schemes used in other areas could be applied, adapted or developed for products used for physical security of people, property and infrastructure.

HECTOS will result in elements for a roadmap for the development of harmonised European certification schemes for physical security products, and provide standardization bodies with proposals for new work items.

This report identifies stakeholder requirements for physical security product evaluation and certification schemes. It is based on a questionnaire, interviews and a workshop held with a wide range of stakeholders. Input from previous and ongoing work on evaluation and certification schemes in the EU has also been taken into account, as has the experience and expertise of the partners who are all active in different aspects of the security field.

Requirements are presented and discussed from the perspective of the principal stakeholder groups including end users, specifiers, their representatives and advisers; product manufacturers, distributors, system designers and integrators; others with a financial stake such as insurers; standards, evaluation and certification bodies; national and EU governments and regulators. Requirements often vary between different product categories and between application areas. These differences are also identified, since this is important information for investigating the applicability of different potential schemes and whether or not a single 'generic' scheme can be devised.

The report describes the various different stakeholders and their interests. Relevant previous studies are described, together with the ongoing EC initiatives in explosives and weapons detection in aviation security and intruder alarm products. The main inputs to the work were a stakeholder questionnaire, interviews and a stakeholder workshop held in Brussels in April 2015.

The stakeholder requirements are presented by considering several perspectives: stakeholder type; the evaluation and certification process; product category; and application area, respectively. Similarities and differences are highlighted.

The report concludes with a summary of principal requirements for evaluation and certification schemes that can be generally applicable and accepted across Europe. There should be:

- Consensus between all key stakeholder groups on key performance requirements, definitions & metrics. Each expressed in sufficient detail.
- Differences in requirements between applications and countries to be taken into account, for example through performance grades, or the use of measurement standards in place of threshold performance requirements.
- Standards, preferably at the international level, setting out the product requirements and test methods, elaborated with the full participation of both user and supplier stakeholders.

HECTOS

- Adequate focus on realistic threats and attacks, which will typically involve human skills and expertise in carrying out tests.
- Sufficient access to standards, as well as signposting and guidance material.
- Consistent evaluation across test houses, through a combination of precision in test methods; mechanisms to identify and correct deficiencies; and, proficiency testing through interlaboratory or 'round robin' comparisons.
- Cost and time effective evaluation processes from a choice of test houses, minimising or eliminating unnecessary and repeated tests.
- Rigorous certification, focussing on ensuring consistency of evaluation.
- Rigorous accreditation, focussing on consistency of evaluation over time, and consistency both with and between different member states.
- Recognition of the need for sovereign capability and for security classification in some cases, at the Member State or European level, for aspects of the standardisation, evaluation and certification chain.

HECTOS

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