HECTOS

Harmonized Evaluation, Certification and Testing Of Security products

D1.2
Application Scenarios
EXECUTIVE PUBLISHABLE SUMMARY

Iconal Technology Ltd
FOI
Fraunhofer ICT
Fraunhofer IGD

Date: 08/06/2015
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

D1.2
Application Scenarios
EXECUTIVE PUBLISHABLE SUMMARY

Version:	1.0 – Executive publishable summary
FOI designation no:	FOI-2012-1271
Responsible:	Mike Kemp, Iconal Technology
Author(s):	Iconal Technology: Mike Kemp FOI: Anders Elfving, Ida Johansson Fraunhofer ICT: Christian Ulrich, Frank Schnuerer Fraunhofer IGD: Olaf Henniger
Number of pages:	5
Dissemination level:	PU –*Public (Summary).*
Start date of project:	Sep, 2014
Duration:	3 years

HECTOS

Summary

Physical security products are used to provide solutions to many different security requirements in many different applications and market sectors. Often products from one or several categories are used in combination. The relationships are complex and it is not possible to produce a simple mapping between products, applications, market sectors and security requirements.

This report lists and describes a number of application scenarios which, whilst not exhaustive, are representative of security requirements and the way that physical security products are deployed to help fulfill these requirements. The application scenarios are intended to guide and support the research carried out during the HECTOS project. The scenarios do this in a number of ways. For example as concrete examples to guide and illustrate the development of concepts, as examples for use during the case studies, and as test cases to examine the breadth of applicability of the evaluation and certification schemes developed on the project.

Eighteen scenarios are identified and briefly described in terms of the application area, the types of threat that exist, the physical security measures that are deployed to mitigate the threat and other relevant information about regulations, standards, operator requirements and the impact of the measures on users and others. An indication is given of the number of examples of the scenario in the EU and their value in terms of the physical security products deployed.

Each scenario is described with a brief summary and a text description including, where possible, a specific example (vignette) to help visualise the scenario.

The selected scenarios are as follows, listed by application area:

Household & Industrials

1. Biometric payment security

Industrial & Retail

2. Small business – office/shop – intruder detection alarms
3. Bank – safes/vault – storage of cash and valuables

Public & Semi-Public Venues

4. Security screening – large public event (permanent venue)
5. Security screening – large event (temporary venue)
6. Security screening & surveillance – open crowded place
7. Shopping centre – video surveillance (CCTV)
8. First responder application – suspected CBRNE incident
9. Urban area – air monitoring for CB attack
10. School/Hospital – low security, open building – protection from attack

Government & Critical Infrastructure

11. Perimeter security – critical infrastructure (open site)

HECTOS

12. Perimeter security & access control - government or critical infrastructure building (urban)
13. Access control to secure location
14. Government building – safes - storage of sensitive documents

Transport

15. Aviation security checkpoint
16. Cargo/ Large volume freight screening

Border

17. Automated border control
18. Border crossing point – RN screening of vehicles

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

The content of this document does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the document lies entirely with the author(s).