HECTOS

Harmonized Evaluation, Certification and Testing Of Security products

D4.4
Summary of findings from application of evaluation and certification schemes from WP3 to biometric security products
EXECUTIVE PUBLISHABLE SUMMARY

NPL
FhG IGD
Safran Identity & Security

Date: 2017-05-19
Project No: 606861
FOI Designation No: FOI-2015-1958
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

D4.4
Summary of findings from application of evaluation and certification schemes from WP3 to biometric security products
EXECUTIVE PUBLISHABLE SUMMARY

Version:	1.0
FOI designation no:	FOI-2015-1958
Responsible:	NPL
Author(s):	Tony Mansfield, Aruna Shenoy (NPL) Pierre Gacon (Safran Identity & Security) Olaf Henniger (Fraunhofer IGD)
Number of pages:	4
Dissemination level:	*PU – valid for the Executive summary*
Start date of project:	Sep, 2014
Duration:	41 months

HECTOS

Executive Summary

HECTOS is an EU FP7 security research project exploring the issue that there are very few evaluation and certification procedures for physical security products that are mutually recognised by EU Member States. HECTOS intends to identify mechanisms to evaluate the performance of security products, also taking into account aspects such as interoperability requirements, regulatory requirements, ethical requirements, and privacy requirements. The project intends to propose elements of a roadmap for the development of new harmonised product certification schemes.

To analyse, develop, enhance, and experimentally validate evaluation and certification schemes, HECTOS conducts case studies in two priority areas: Biometrics and detection of weapons and explosives. For the biometric case studies, the following topics have been selected:

Topic 1: Image quality of contactless fingerprint sensors, evaluated against the established requirements and test methods associated with 2D fingerprint sensors
Topic 2: Presentation attack (spoof) detection capability and presentation attack resistance of biometric systems, evaluated against emerging ISO standards for evaluation of biometric presentation attack detection, which in turn are based on established guidance (Common Criteria)
Topic 3: Products for secure biometric access control to critical infrastructure, evaluated against proposed CEN technical specification for biometric authentication for critical infrastructure access control

HECTOS D4.4 analyses feasibility and effectiveness of the evaluation and certification approaches for each of the biometric case studies addressed. The experience gained in tasks WE4.3, and the conclusions and recommendations are summarised for take up by WP8, to address a broader range of biometric and other security product categories.

General conclusions and findings

- Current certification schemes for biometric products may range from “type 1” schemes to “type 5” schemes.
- Requirements and test method availability :
  - For Topic 1, methods and requirements are public and were adapted to the evolving state of the art technology.
  - For Topic 2, exact methods of presentation attack not publicly available but were shared between test houses.
  - For Topic 3, performance requirements and test methods are specified in the CEN technical specifications and some PAD techniques are not publicly available.
- Geographic scope – with well-established schemes such as PIV certifications, the schemes are recognised worldwide. Most products are developed either to International and European standards.
- Cost of evaluation depends on the infrastructure and resources required for scenario based and technology evaluation. Cost may vary considerably, and be quite expensive

- and time consuming. In some cases, the cost is borne by the product supplier and in some cases by the scheme owners.
- Request procedure for product evaluation is dependent on scheme owners and self-testing by supplier may help inform the test sponsors decision.
- The identification of suitable accredited test organisations for evaluation is under the responsibility of the scheme owners.
- The test house shall be fully accredited to support mutual agreement and understanding between the test organisation and the certification body and it may be necessary to consider security clearances for those test house staff conducting the evaluations.
- Upon evaluation of a product, a review and attestation process would follow and may involve the scheme owners, test organisation and domain experts. The results of the evaluation may be public with limited technical information (some are confidential). To achieve consistency and repeatability of results between different test organisations is difficult particularly with adversarial testing due to issues with publication of confidential information.
- Test methodology for evaluation of different biometric products differ according to the capabilities and performance metrics to be determined. The three topics for case studies addressed different aspects of the system performance such as :
    - PIV certification for contactless fingerprint sensor image quality – optical aspects
    - PAD evaluation –Likelihood of presentation attacks (APCER, BPCER)
    - Secure access control – functional requirements and performance levels (FAR, FRR)
- Evaluation results for various types of tests are different. PIV certification results are a pass/fail decision, PAD result indicate resistance to ‘attack potential’ and may be graded. Secure access control systems are a pass/fail decision with possible grading indicative of its resistance to presentation attacks.
- Reuse of evaluation results depends on the credibility and sufficiency of the previous evaluations. In some cases, the reuse of results is not possible due to confidential information and processes involved.
- Periodic reassessment of certified products is necessary. The scheme owners must be informed of updates and modifications to the certified product within the validity period for certification.