REASSURE

Project ID: 731591, Horizon 2020
http://www.reassure.eu

REASSURE

Deliverable D4.3

Final Report on Standardization

Editor:	V. Verneuil
Deliverable nature:	R
Dissemination level: (Confidentiality)	PU
Delivery date:	March 31, 2020
Version:	1.0
Total number of pages:	12
Keywords:	ISO, Standardization, Dissemination

Horizon 2020
European Union funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 731591.

Executive summary

A declared goal of REASSURE was to have an impact on standardisation and evaluation schemes via influencing stakeholders and decision makers. To do so, the consortium identified relevant targets, e.g. established consortia such as JHAS, ongoing standardisation efforts within ISO, as well as emerging efforts like SESIP, and liaised with them over the past three years.

The consortium provided input to two ISO standards (20085-1 and 20085-2), which matured to publication during the duration of the project. These standards cover technicalities around side channel setups and the calibration of them. The consortium also contributed to the analysis of an existing ISO standard (17825). This standard covers testing methods in the context of side-channel attacks.

Consortium members made several presentations to the JHAS group during the regular group meetings, contributing in particular in the context of the ongoing and rapid developments around the use of deep learning.

The consortium is also represented in EMVCo, and a presentation of project results in the context of deep learning is scheduled.

SGDSN held yearly meetings with CB GIE, which were informed by REASSURE results.

An initiative initially launched by NXP (known as SmartCC) and now run by the Global Platform consortium under the name SESIP (Security Evaluation Standard for IoT Platforms) aims at driving the harmonisation of standardisation in the context of Internet of Things (IoT) devices. REASSURE results, in particular intended for the IoT use case (leakage detection as "conformance style testing") have been discussed with the relevant NXP liaison people, w.r.t. to implications for the SESIP scheme.

List of authors

Company	Author
NXP	V. Verneuil
UNI-KLU	E. Oswald

Revision history

Revision number	Date	Comment
1.0	2020/03/31	Final version

Contents

Abbreviations

CB Carte Bancaire (Banking Card)

CC Common Criteria

GIE Groupement d'Intérêt Économique (Economic Interest Group, or joint-venture)

IEC International Electrotechnical Commission

ISCI International Security Certification Initiative

ISO International Organization for Standardization

IT Information Technology

JTC Joint Technical Committee

SC Subcommittee

WG Working Group

1 Introduction

The overarching goal of the work package 4 (WP4) is to transfer REASSURE's results to stakeholders such as policy makers and standardisation bodies, thereby influencing existing and future certification practices. To do so, the REASSURE consortium has identified and reviewed existing standards, selected and contacted liaison officers to represent the project within the relevant working groups, coordinated their actions, and organised follow-on activities. This deliverable covers the effort of the REASSURE consortium in these areas over the whole project's time frame.

As the general awareness towards the need for coordinated measures to strengthen cyber-security is growing in the public sphere, several initiatives have arisen shortly before or during the project's time frame. Some of them, such as the Charter of Trust, are targeting high-level principles and rely on other schemes for in-depth specification of evaluation procedures. The consortium's focus was therefore to monitor such emerging works in international standardisation bodies or industry consortia and select the ones to target depending on their relevance and uptake.

1.1 Overview of Stakeholder Groups, Standardisation Bodies, Emerging Initiatives

1.1.1 JHAS

The International Security Certification Initiative (ISCI) brings together stakeholders from every aspect of smart card security evaluation: certification bodies, evaluation laboratories, hardware vendors, software vendors, card vendors and service providers. They have two working groups: ISCI-WG1, which aims to define methodology and best practice for smart security device evaluation, and ISCI-WG2 (also known as JHAS), which defines and maintains the state of the art in potential attacks against smart security devices.

All non-academic partners of REASSURE are represented in JHAS: NXP, IDM, Riscure, and SGDSN.

1.1.2 EMVCo

EMVCo is a consortium of financial services companies: Visa, Mastercard, JCB, American Express, China UnionPay, and Discover. It manages the EMV standard for credit and debit card transactions and in particular it defines the evaluation requirements for the security certification of these products.

All industrial partners of REASSURE are represented in EMVCo: NXP, IDM, and Riscure.

1.1.3 CB GIE

The Groupement des Cartes Bancaires CB, aka CB Groupement d'Intérêt Économique (GIE), is the French national interbank network. It represents over 120 financial institutions and providers in payment services. One of the missions of the CB GIE is to ensure that best security measures are in place to prevent fraud.

SGDSN has regular contacts with the CB GIE.

1.1.4 NIST FIPS

The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce. It develops the Federal Information Processing Standards (FIPS) that establish requirements for computer systems used by non-military American government agencies and contractors.

In particular, the FIPS 140 series (currently 140-2) specifies requirements for cryptography modules. The new revision 140-3 was approved on March 22, 2019 and will become effective on September 22, 2019. It aligns the NIST requirements around two ISO/IEC standards: 19790 and 24759 (see below).

1.1.5 ISO/IEC JTC1/SC27 WG3

ISO/IEC JTC 1 is a joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission. Its purpose is to develop, maintain and promote standards in the field of information technology (IT). The subcommittee 27 (SC 27) is dedicated to the standardization of IT security techniques and its working group 3 (WG3) is responsible for "Security evaluation, testing and specification". WG3 deals with two "families" of standards that are of particular relevance to side channel attacks.

The first "family" of standards specifies the common criteria framework in ISO/IEC 15408, testing laboratories must comply with ISO/IEC 17025, and certification bodies will normally be approved against ISO/IEC 17065. Common criteria evaluations are based on protection profiles for defined security targets, and in the context of smart card evaluations, the details of what and how evaluation laboratories should test is largely developed in the JHAS group.

The second "family" of standards is comprised of ISO/IEC 19790:2012(E) and ISO/IEC 24759:2017(E), which effectively specify the testing regime for cryptographic modules under the FIPS 140-3 framework. The main difference that the introduction of FIPS 140-3 distinguishes from FIPS 140-2 is the requirement to test against side channels, for which a methodology is described in ISO/IEC 17825:2016.

Specifically, ISO/IEC 17825:2016 defines the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4.

At the beginning of REASSURE, WG3 was actively working on:

ISO/IEC CD 20085-1 (eventually published in October 2019) Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules – Part 1: Test tools and techniques

ISO/IEC CD 20085-2 (eventually published in March 2020) Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules – Part 2: Test calibration methods and apparatus

1.1.6 Global Platform

Global Platform[1] is an industrial consortium bringing together over a 100 companies to develop certification standards for digital services and devices including smartphones, tablets, set top boxes, wearables, connected cars, other Internet-of-Things (IoT) devices and smart cards. Its three main focuses are: secure element (SE), trusted execution environment (TEE), and mobile messaging.

Two partners of REASSURE, IDM and NXP, are members of the Global Platform consortium.

Global Platform promotes a new certification standard called Security Evaluation Standard for IoT Platforms (SESIP). This new standard is based on the Common Criteria methodology (ISO/IEC 15408) principles, but tailored to the IoT field. Its aim is to offer an harmonization of the evaluation of common security features and avoid redundancy by allowing reuse of evaluation results and composition and mapping of other certification schemes.

1.1.7 Charter of Trust

The Charter of Trust[2] was launched at the Munich Security Conference (MSC) in 2018 at the impulse of Siemens and was grew to a total of 17 members until now. The Charter of Trust calls for binding rules and

[1] https://globalplatform.org
[2] https://www.charteroftrust.com

standards to build trust in cyber security around 10 key principles covering a wide scope, e.g. supply chain, innovation, education, certification, regulation, etc.

The actions of this industrial consortium are shaped around three angles:

- technology: establishing, piloting and adopting global baseline requirements and concepts to secure the digital world;
- politics: promoting a global approach to the regulatory framework for cyber security;
- business: accompanying the digital transition of the industry and business models towards cyber security.

NXP is a member of the Charter of Trust.

1.1.8 ENISA Cybersecurity Certification Framework

In 2019, with the Cybersecurity Act (Regulation 2019/881), ENISA has been working on "European cybersecurity certification schemes". Such schemes are meant to serve as the basis for certification of products, processes and services that support the delivery of the Digital Single Market.

The European Cybersecurity Act introduces processes for the cybersecurity certification of ICT products, processes and services. The idea is to establish EU wide rules and European schemes for cybersecurity certification. It is therefore a high-level framework that builds on existing standards and stakeholder groups.

We established contact with the ENISA and in particular the "Ad hoc Working group to support the preparation of a candidate cybersecurity certification" ENISA is currently setting up[3].

1.2 Strategic Selection of Initiatives

The JHAS group is central to existing evaluations in the CC framework. It is hugely influential and therefore was considered as particularly important for the REASSURE project.

EMVCo shares a large portion of its membership with JHAS, but is a unique and similarly influential group for the banking sector. Therefore we considered it to be a key stakeholder group to interact with as well.

Evaluation schemes such as CC and FIPS 140-3 are represented via a collection of ISO standards. Some standards map out respective higher level elements of the schemes, but 20085-1/2 and 17825 touch on several practical, detailed requirements around side-channel attacks (such as the setup, calibration, and testing methods). Because REASSURE focuses on these details, we decided to engage with these specific WG3 efforts (two of which were still in progress at the start of REASSURE).

Initiatives such as SESIP and the Charter of Trust emerged in their current form towards the end of REASSURE only. NXP as a project partner plays a key role in these and channels project findings appropriately to them. The above mentioned ENISA working group considers framework level questions, but REASSURE mainly deals with concrete, low-level technical details.

2 REASSURE Contributions

2.1 ISO/IEC JTC 1

Initially the consortium followed the (a that time) established practice of issuing a request for joining the ISO/IEC JTC 1/SC 27/WG 3 as a category C partner to contribute to the drafts ISO/IEC WD 20085-1 and 20085-2. Whilst the request was initially acknowledged and positively received, it was ultimately turned down because the European Commission, who was asked to validate our eligibility didn't provide us with the

[3] See https://www.enisa.europa.eu/news/enisa-news/enisa-cybersecurity-certification-preparation-underway.

necessary endorsement.

This was of course disappointing and unexpected because previously EC funded projects had been granted CAT C liaison status. Further conversations with the EU project officer confirmed that the EC's position is unlikely to change and thus it an official REASSURE liaison person cannot be expected to be accepted.

The consortium therefore utilised the partners with representatives in WG3 (SGDSN and UNIVBRIS had members placed in WG3) and direct feedback to S. Guilley (one of the REASSURE Strategic Advisory Board members, and co-editor of said standards).

WG3 worked on:

ISO/IEC CD 20085-1: This standard defines test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules. It was eventually published in October 2019. We provided input regarding the exposition of key concepts such as horizontal vs. vertical and univariate vs. multivariate attacks; we also provided input regarding trace storage formats.

ISO/IEC CD 20085-2: Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules – Part 2: Test calibration methods and apparatus. It was eventually published in March 2020. We provided input regarding the need for documentation of the calibration process and the difficulty of calibrating a setup/test tool based on one single target.

WG3 had previously published ISO/IEC 17825 but it was due for a potential revision. REASSURE's work on leakage assessment for "low cost" devices (targeting the IoT domain, in WP2) coincided with the philosophy of FIPS 140-3 which is the use case for ISO/IEC 17825. REASSURE therefore build on the work that had been carried on in WP2 and utilised the new understanding to analyse the leakage detection process as described in ISO/IEC 17825. This analysis revealed a number of important ways to improve ISO/IEC 17825. This was acknowledged and a revision of the standard is envisioned.

2.2 CB GIE

Contact has been initiated with the CB GIE to present the REASSURE project in 2017.

SGDSN held meetings with CB GIE, approximately once a year. A major topic addressed in these meetings is the evolution of evaluation methods and common interests to enhance the security of smart cards. Works realised by the REASSURE project have been presented and pushed towards CB GIE during these discussions.

2.3 EMVCo

We established contact with EMVCo, providing them with a description of our activities and offering our contribution.

EMVCo expressed interest in our research related to the application of deep-learning techniques to side-channel analysis. A presentation on this subject by Riscure was scheduled for March 2020. However, due to the Covid-19 virus situation, this meeting had to be cancelled. Nonetheless, EMVCo confirmed its interest and announced that the meeting will be rescheduled to a future date.

2.4 ISCI/JHAS

Three presentations stemming from REASSURE's work have been given to the JHAS consortium over the course of the project and a fourth one is planned:

- SGDSN gave a presentation regarding the usage of Deep Learning within the context of side-channel evaluations.
- Riscure gave a presentation on leakage assessment in protected AES implementation.

- SGDSN gave a presentation on leakage characterization.
- A presentation by UNI-KLU describing the main outcomes of REASSURE regarding challenges in side-channel evaluation will take place after the project's end (this talk was supposed to take place in March 2020, but had to be postponed due to the Covid19 crisis).

Apart from these specific activities, the results of REASSURE impact indirectly the JHAS guidance through the participation of REASSURE's industrial partners to the discussion and working groups within JHAS, which content is not made publicly available.

2.5 Global Platform

Because SESIP emerged at the end of the project's time frame, it was not possible to plan specific actions at the time of writing this document. Nonetheless we intend to keep promoting the REASSURE's results and recommendations to Global Platform by leveraging the involvement of NXP in SESIP.

3 REASSURE Key Messages

Given the confidential nature of interactions with standardisation bodies such as ISO and stakeholder group such as JHAS, we can only summarise the general themes and messages that REASSURE provided over the course of the project. They are structured around three main axes.

3.1 Warning against conformance-style testing

The first axis naturally ensue from the early works of the consortium around existing standards and testing procedures such as TVLA and ISO 17825 that offer conformance-testing approaches to side-channel evaluation.

Our research clearly demonstrates that statistical leakage detection cannot be used in a "black box" setting. To use statistical tests correctly, they have to be configured for the specific use case. This requires either knowledge or a deliberate choice of the effect size, which can only be done if a target is well understood. Consequently, such techniques can not be used in any meaningful way unless a preliminary study of a target device has already been done and the results are available.

Leakage detection techniques furthermore require a careful consideration regarding the number of leakage observations: ISO 17825 (and in general FIPS 140-3) seem to approach side channel evaluations with attacks in mind, and set trace numbers seemingly in relation to attacks. However, unspecific leakage detection require more traces than specific leakage attacks, and therefore it is not sound to "reuse" trace numbers from attack settings in detection settings.

Consequently, conformance style testing approaches as they are currently described are not only limited but possibly dangerous if misunderstood since they can highly overestimate the actual security level of a sensitive implementation. In that sense, we deem that a proper understanding and use of the statistical tools and a responsible reporting of findings is crucial to structuring an evaluation approach.

3.2 A proposition to structure current and future evaluations

The second axis is our proposition for a structured side-channel testing working "backwards" from the most powerful adversary. It is detailed in the two white papers produced by the project: D1.3 and D1.5.

The motivation for this proposition is based on the difficulty of defining things like "the best practical attack" (e.g. new attacks can be deemed impractical at first, but over time this assessment might change), or "information that is hard to obtain". Such "moving targets" make any development of a rigorous and structured evaluation approach impossible. However, it is possible to define a worst case adversary, and then work "backwards" by relaxing assumptions and considering if an attack could be demonstrated.

Therefore we suggest to first consider giving evaluators strong adversarial capabilities such as the knowledge of implementation details and the access to secret values used in countermeasures to perform a "worst-case" evaluation, following the steps of the detect-map-exploit framework. From that point, we advocate that an evaluator should argue about the implications of each step when "relaxing" assumptions in order to assess the possible "gaps" between worst-case attacks and more practical ones.

3.3 The usage of deep learning (DL) techniques

The last axis is the use and place of DL-based techniques in side-channel evaluations. The recent advent of DL shook up several fields in computer science and perhaps gave a feeling that side-channel evaluation would become a simple task using deep neural networks.

While very promising, we found that DL-based techniques are sometimes misused, or that their benefit is misunderstood, which can also lead to wrong security assessments. In general, we show that DL shifts expertise from one area to another but does not require less expertise.

However, we found that, when properly used, DL provides efficient alternatives to classical side-channel mapping and exploitation steps and may relax some attack assumptions. This can make a difference in an evaluation, for instance when an evaluator cannot get full knowledge and access to the target implementation.

This insight connects with the previous section: it may be that DL based techniques provide a bridge between explicitly knowing something (which may be deemed impossible in a specific evaluation/device context) and implicitly learning it via a deep neural net.

