





D6.2

Initial report on project dissemination, exploitation and standardisation

Project number:	317930
Project acronym:	HINT
Project title:	Holistic Approaches for Integrity of ICT- Systems
Start date of the project:	1 st October, 2012
Duration:	36 months
Programme:	FP7/2007-2013

Deliverable type:	Report
Deliverable reference number:	ICT-317930 / D6.2 / 1.0
Work package contributing to the deliverable:	WP06
Due date:	September 2013 – M12
Actual submission date:	1 st October, 2013

Responsible organisation:	CEA-LETI
Editor:	Jacques Fournier
Dissemination level:	Public
Revision:	1.0

Abstract:	This report details the dissemination activities which have been ongoing during the first year of the HINT project, mainly focused on increasing its visibility and the public awareness of the project. A couple of technical papers have been submitted and one has been published. Given the technical orientation taken by the project, the standardisation & exploitation prospects are still in line with those defined in the DoW.
Keywords:	Dissemination, Standardisation, Exploitation, IPR



Editor

Jacques Fournier (CEA-LETI)

Contributors (ordered according to the beneficiary numbers) Verena Brunner, Sonia Pichler, Klaus-Michael Koch (TEC) Holger Bock (IFAT) Jean-Baptiste Rigaud (ARMINES) Dave Singelee (KUL) Carsten Rust (MOR) Julien Francq, Marc Mouffron (CCS)

Disclaimer

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 317930.



Executive Summary

The HINT project follows three dissemination phases defined in the project's description of work: awareness-oriented phase, results-oriented phase and exploitation-oriented phase. The dissemination activities for the first year have been mainly focused on awareness-oriented dissemination activities towards the professionals of the semiconductor & security industry and the general public. The following dissemination tools & features have been created: the project's logo, the project's announcement letter, the project's leaflet and the project's newsletter for year 1. The HINT project website is up and running with a public part and a private section. The project is also present in the social media via a dedicated Twitter account and a LinkedIn group. To allow the project partners to efficiently use all those communication tools, as well as the other more technical tools, a project handbook has been edited and distributed.

Dissemination activities are ongoing as planned in the DoW, with opportunities taken as they come: ICT 2013, ChiptoCloud 2013 and the interview in EU yearbook. Technical work has been presented at the HOST workshop, with the corresponding peer-reviewed papers published in the conference's proceedings. Other technical articles have been submitted to CT-RSA, IEEE Transactions on circuits and systems and DATE. Dissemination by aliasing with the following project and events are under consideration: French GDR-SoCSip, PUFFIN project, IMEC's technology days, Romanian Cryptology Days, PANDA summer workshop (China). Standardization activities are still within the scope of the project and will be more thoroughly followed once the technical results are more mature. The project partners (especially those from industry) envisage to adapt their exploitation plan based on the technical work initiated and the first results obtained (test bench, first measurement results, Trojan detection & PUF design).

IPR issues have been taken care of in the consortium agreement. Most partners are planning to file patents based on the current work done on Trojan detection schemes, PUF designs, PUF processing techniques or on-chip power measurements.

Contents

Chapte	r 1	Dissemination	4
1.1 lr	ntrodu	uction	4
1.2 C	Disser	nination Strategy	4
1.3 C	Disser	nination Activities	5
1.3.1	Indiv	vidual Dissemination Plans	5
1.3.2	Scie	ntific articles and publications	
1.3.3	Part	cipation in conferences and workshops/ further dissemination activitie	s 9
1.3.	3.1	Upcoming Events	11
1.3.4	The	HINT Project Website	11
1.3.5	Furt	ner means of dissemination	16
1.3.	5.1	Project Logo	16
1.3.	5.2	Project Announcement Letter	16
1.3.	5.3	Project Leaflet	16
1.3.	5.4 5.5	Social Media: HINT Twitter Account and HINT LinkedIn-Group	17 17
1.3.	5.6	Cooperation with other projects	
1.3.	5.7	Interview for EU Yearbook	18
0	_		
Chapte	r 2	Standardisation & Exploitation	19
2.1 S	r 2 Standa	ardisation Plans of the Partners	19 19
2.1 S	r 2 Standa Exploi	Standardisation & Exploitation ardisation Plans of the Partners tation Plans of the Partners	19 19 20
2.1 S 2.2 E 2.2.1	r 2 Standa Exploi Preli	Standardisation & Exploitation ardisation Plans of the Partners tation Plans of the Partners minary Market Overview	19 19 20 21
2.1 S 2.2 E 2.2.1 2.2.1 2.3 J	r 2 Standa Exploi Preli oint E	Standardisation & Exploitation ardisation Plans of the Partners tation Plans of the Partners minary Market Overview Exploitation Plan	19 20 21 22
2.1 S 2.2 E 2.2.1 2.2.1 2.3 J 2.4 II	r 2 Standa Exploi Preli oint E PR is	Standardisation & Exploitation	19 20 21 22 22
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1	r 2 Standa Exploi Preli oint E PR is Prer	Standardisation & Exploitation	19 20 21 22 22 22
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1 2.4.2	r 2 Standa Exploi Preli oint E PR is Prer Draf	Standardisation & Exploitation	19 20 21 22 22 23 23
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1 2.4.2 2.4.3	r 2 Standa Exploi Preli oint E PR is Prer Draf Con	Standardisation & Exploitation	19 20 21 22 22 23 23 24
2.1 S 2.2 E 2.2.1 2.3 J 2.4 IF 2.4.1 2.4.2 2.4.3 2.4.3	r 2 Standa Exploi Preli Oint E PR is Prer Draf Con 3.1	Standardisation & Exploitation	19 20 21 22 22 23 23 24 24
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1 2.4.2 2.4.3 2.4.3 2.4.	r 2 Standa Exploi Preli Oint E Prer Draf Con 3.1 3.2	Standardisation & Exploitation ardisation Plans of the Partners tation Plans of the Partners minary Market Overview Exploitation Plan. Sues identified in the HINT project equisites for the HINT project ting of Proposals. tracts Grant Agreement (GA) Consortium Agreement (CA)	19 20 21 22 22 23 23 23 24 24 24
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1 2.4.2 2.4.3 2.4. 2.4. 2.4. 2.4.4	r 2 Standa Exploi Preli Oint E PR is Prer Draf Con 3.1 3.2 Stat	Standardisation & Exploitation ardisation Plans of the Partners	19 20 21 22 22 23 23 23 24 24 24 25
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1 2.4.2 2.4.3 2.4. 2.4.3 2.4. 2.4. 2.4.4 2.4.5	r 2 Standa Exploi Preli Oint E PR is Prer Draf Con 3.1 3.2 State Lice	Standardisation & Exploitation ardisation Plans of the Partners	19 20 21 22 22 23 23 23 24 24 24 24 24 25 26
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1 2.4.2 2.4.3 2.4. 2.4. 2.4. 2.4.4 2.4.5 2.4.6	r 2 Standa Exploi Preli oint E PR is Prer Draf Con 3.1 3.2 Stati Lice Pate	Standardisation & Exploitation	19 20 21 22 22 23 23 23 24 24 24 24 24 25 26 26
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.1 2.4.2 2.4.3 2.4. 2.4.3 2.4. 2.4.4 2.4.5 2.4.6 2.4.7	r 2 Standa Exploi Preli Oint E PR is Prer Draf Con 3.1 3.2 State Lice Pate Cop	Standardisation & Exploitation	19 20 21 22 22 22 23 23 23 24 24 24 24 25 26 26 26
2.1 S 2.2 E 2.2.1 2.3 J 2.4 II 2.4.2 2.4.3 2.4.2 2.4.3 2.4.4 2.4.4 2.4.5 2.4.6 2.4.7 2.4.8	r 2 Standa Exploi Preli Oint E PR is Prer Draf Con 3.1 3.2 Stat Lice Pate Cop	Standardisation & Exploitation ardisation Plans of the Partners tation Plans of the Partners minary Market Overview Exploitation Plan sues identified in the HINT project sues identified in the HINT project equisites for the HINT project ting of Proposals tracts <i>Grant Agreement (GA) Consortium Agreement (CA)</i> us of the project with regard to IPR issues mces yrights	19 20 21 22 22 22 23 23 24 24 24 24 24 26 26 26 26



Chapt	ter 3	List of Abbreviations	30
2.5.2	2 Sci	entific Publications	
2.5.1	1 De	iverables	
2.5	Proje	ct Results	27



List of Figures

Figure 1: Welcome page of the HINT website	12
Figure 2: News page of the HINT website	13
Figure 3: HINT website statistics	14
Figure 4: Content of the restricted area	15
Figure 5: HINT logo	16
Figure 6: HINT leaflet	16
Figure 7: HINT newsletter issue 1	17
Figure 8: Deliverables and Publications Process	27
Figure 9: Deliverable Review Form	28

List of Tables

Table 1: Summary of scientific articles and publications	8
Table 2: Summary of dissemination activities	10
Table 3: Documents viewed	14



Chapter 1 Dissemination

1.1 Introduction

Dissemination activities are provided to ensure the visibility and awareness of the project and to support the widest adoption of its results in industry and research. The strategy for the dissemination of HINT aims at creating this awareness, raising the public interest in the project, and promoting project results to potentially interested parties and within the international research community.

1.2 Dissemination Strategy

The dissemination strategy of HINT is made up of three consecutive phases:

- The **awareness-oriented** phase aims to create awareness and to raise public interest.
- The **result-oriented** phase will promote results of the project to potentially interested parties.
- Finally, during the **exploitation-oriented** phase, specific activities will be undertaken in order to actually start the exploitation.

The three phases of dissemination require different methods and activities to be undertaken in order to achieve their goals.

Awareness-oriented phase

Raising the public awareness involves the setting up of the basic marketing materials and awareness-raising presentations about the project and the problems it aims to tackle. Thus, the main activities are the following:

- Setting up a common project design, such as a HINT logo, templates for documents and presentations.
- Creating and maintaining the project website, which will describe the challenges and the goals of the project and which will introduce the project members.
- Designing the project information materials (such as a leaflet and an introductory off-the-shelf presentation), which can be distributed later on without investing greater efforts.
- Giving introductory presentations at conferences and workshops about the challenges and goals of HINT in order to raise awareness among the scientific and industrial stakeholders and to establish the basic brand name of HINT.

This phase mainly coincides with the first months of the project and this is what has been mainly carried during the Period 1 covered in this report.

Result-oriented phase

For promoting the results of the HINT project, this dissemination phase will address stakeholders in programmable hardware related security issues. The planned activities are:



- Display and promote public deliverables and news for viewing and downloading on the project website in order to show the liveliness and progress of the project and to keep interested parties up-to-date.
- Presentations at international conferences and workshops covering the technical findings of the HINT project. These presentations will be research-oriented.
- High-quality papers will be submitted to scientific and industry conferences.
- The HINT consortium will publish and disseminate press releases after having reached important milestones. These press releases will be circulated to representatives of the international press focusing on hardware security.

Exploitation-oriented phase

The exploitation is specifically targeted at potential clients of the HINT project. Specific planned activities of this phase include:

- Exploitation-oriented upgrade of the project website, including optimisation for search engines and optional registration for specific keywords.
- Individualised demonstrations at interested stakeholders during the negotiation of business projects.

1.3 Dissemination Activities

The following section presents our dissemination activities in order to document the extent to which we have executed our above mentioned dissemination strategy.

1.3.1 Individual Dissemination Plans

Each partner supports its own dissemination plan and to collective dissemination activities as a group. The partner's specific (original) plans have not been changed:

TEC's objective is to provide the HINT-project IT-infrastructure, more precisely the whole set of tools which will foster the project cooperation, communication and dissemination, whereby the project website will serve as the most versatile external information and communication tool for a worldwide audience. In addition TEC will elaborate a HINT-project leaflet, a press release as well as a periodic newsletter together with the other partners. Furthermore we intend to widely disseminate the HINT-project ideas and its results at various conferences and workshops and social media. TEC was able to acquire a project booth for the HINT project at the ICT2013 in Vilnius.

The **CEA-LETI**, as a research organization, shall mainly focus on providing high quality scientific publications covering the technologies developed within the HINT project. The CEA-LETI is an active contributor to several worldwide annual security conferences and workshops (WIFS, CHES, CARDIS, FDTC...), international scientific journals (IJIEI...) and security books. Moreover, every 18 months, the CEA-LETI organizes the PHISIC workshop regrouping academic, industrial and user stakeholders of the hardware security arena mainly from the neighbouring EU countries. This PHISIC workshop shall be a good dissemination opportunity for the HINT project.

IFAT will disseminate HINT results by four main communication channels:



<u>Specialized press:</u> Press releases will lead to articles in technical newspapers, technical press and journals of technical journalism, as well as online media publications.

<u>Papers for scientific conferences and journals:</u> Researchers from IFAT are publishing on a regular basis on international and widely recognized conferences, such as e.g. RSA Conference (http://www.rsaconference.com), EUROCRYPT (<u>http://www.iacr.org/</u>), ASIACRYPT (<u>http://www.iacr.org/</u>), ACM CCS and ASIA CCS, CHES conference (<u>http://www.iacr.org/workshops/ches/</u>), IEEE ISCAS (<u>http://www.iscas2012.org/</u>), IEEE DAC (<u>http://www.dac.com/</u>), IEEE DATE (<u>http://www.date-conference.com/</u>)

<u>Trade fairs, exhibitions, and trade shows:</u> Well established annual trade shows like CARTES & IDentification in France (<u>http://www.cartes.com</u>) or Omnicard in Germany (<u>http://www.omnicard.de/</u>) provide excellent opportunities to pass information on newest advances in technology to customers and to the public. Infineon's sale forces are every year present at these events to spread news on progress in research and development.

In the framework of meetings with selected customers result on new technologies may be discussed to get early feedback on promising applications.

ARMINES plans to publish the results of HINT in journals (for example the "Journal of Cryptographic Engineering") and in the conferences on cryptographic hardware and embedded systems cited above. ARMINES also plans to organize a session dedicated to hardware integrity in the workshop "PHISIC". People who are involved in HINT will also address to problematic of HINT during their courses on hardware security (given in the engineer school "Ecole des Mines de Saint Etienne") and also during the supervision of master and PhD students.

KUL: The main outcome of the research group COSIC of the KU Leuven is through research publications. As a public university, KUL's main goal is the training of PhD students, who will be the next generation of researchers. The main focus is therefore advanced research beyond state-of-the-art with realistic input from endusers and industrial partners. During the course of the project, a dedicated workshop on integrity technologies will/can be organized in cooperation with the other academic partners and with the support from the industrial partners. The obtained research results will in the long term be integrated in the teaching material of advanced courses on secure embedded systems.

MOR plans to disseminate project results in conferences, exhibitions, and trade fairs. A speech application for the Chip to Cloud Security Forum 2013 (former e-Smart) has already been accepted. The partner will apply for further presentations at this conference as well as at the CARTES conference in the following years. Further dissemination activities are planned in standardization bodies related to Smart Cards and application areas of Smart Cards. Exploitable assets of the project, in particular possible applications with Smart Card technology, will be promoted in press releases, customer newsletters and workshops with stakeholders. In this context, the project will also be promoted inside the Morpho group. Finally, the partner can also contribute to scientific publications in collaboration with academic project partners, based on Morpho's technical work on PUFs, Side Channel Analysis based detection of Hardware Trojans, and the application of HINT technology for an unclonable ID card.

CCS: The HINT project tackles to many different known threats to integrated circuits (hardware Trojans, unauthorized cloning, counterfeiting), and then this project will interest the European research community. Moreover, HINT will contribute to alert industrial and economic actors to these emerging threats. The consortium will



publish scientific articles in international workshops and conferences such as Hardware-Oriented Security and Trust (HOST), Cryptographic Hardware and Embedded Systems (CHES) or Design, Automation and Test in Europe (DATE). It will also manage a website and update it regularly.

CCS will also supply VHDL sources of infected circuits by Trojans for allowing public scrutiny. It will be the first step to a possible collaboration with other research labs, like American ones.

All partners are fully committed to the dissemination of technical results in refereed conferences (when possible), journals and of the project's objectives in industry-oriented events. During the first year of the project the dissemination activities were based on the theoretical and practical project ideas and derived specifications. As a follow-up action we will target with our first technical results workshops like PHISIC or events like CARTES during the second and third years of the project.



1.3.2 Scientific articles and publications

Even if the HINT project is still in the first year, HINT partners already submitted scientific articles whereas one paper has already been accepted for one very renowned conference in this area namely HOST 2013.

Title	Main Author	Title of the Periodical or the Series	Number, Date or Frequency	Publisher	Place	Year	Relevant Pages	Is/Will open access ¹ provided to this publication?	Status
Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise	J. Delvaux, I. Verbauwhede	HOST	2013	IEEE	Austin TX, USA	2013	6	Yes	accepted
Fault Injection Modeling Attacks on 65nm Arbiter and RO-based Sum PUFs	J. Delvaux, I. Verbauwhede	IEEE Transactions on circuits and systems	12	IEEE	USA	2013	14	Yes	submitted
Attacking PUF-Based Pattern Matching Key Generators via Helper Data Fault Injection	J. Delvaux, I. Verbauwhede	CT-RSA	2014	Springer	USA	2014	14	Yes	submitted
Key-recovery Attacks on Various RO PUF Constructions via Helper Data	J. Delvaux, I. Verbauwhede	DATE	2014		Germany	2014	6	Yes	submitted

Table 1: Summary of scientific articles and publications

¹ Open access is defined as free of charge access for anyone via internet. Please answer "yes" if the open access to the publication is already established and also if the embargo period for open access is not yet over but you intend to establish open access afterwards.



1.3.3 Participation in conferences and workshops/ further dissemination activities

							Type of Audience ²			2			
Type of Activities	Main Leader	Title	Month	Year	Place	a)	b)	c)	d)	e)	Size of Audieno	Type and Goal of the Event	Countries Addressed
Other	TEC/All partners	HINT Homepage / Logo	12	2012	Online	x	x	x	x	x	/	Official project website: http://www.hint- project.eu / Logo will be used for HINT deliverables/publications	International
Press Release	TEC/All partners	HINT Announcement Letter	1	2013	Online	x	x	x	x	x	/	HINT Announcement letter is available at the HINT website: https://www.hint- project.eu/downloads/HINT_Announceme nt_Letter_Website.pdf	International
Conference	KUL	Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise	6	2013	Austin, TX, USA	x	x				100+	IEEE Int. Symposium on Hardware- Oriented Security and Trust	International
Web	TEC/All partners	HINT Project Leaflet	2	2013	Online	x	x	x	x	x	/	HINT Project Leaflet giving a project overview is available at the HINT website: https://www.hint- project.eu/downloads/HINT_Leaflet.pdf	International
Web	TEC/All partners	HINT Newsletter Issue 1	9	2013	Online	x	x	x	x	x	/	HINT first newsletter giving an overview of WP1-results and upcoming events is available at http://www.hint- project.eu/downloads/HINT_Newsletter_Is sue_September_2013.pdf	International
Web	TEC/All partners	HINT Twitter Account	4	2013	Online	х	х	х	х	х	/	Social medium at http://twitter.com/hint_project	International

² a) Scientific Community (higher education) b) Industry c) civil society, d) policy makers, e) medias



D6.2 - Initial report on project dissemination, exploitation and standardisation

							Туре	of Aud	lience	2			
Type of Activities	Main Leader	Title	Month	Year	Place	a)	b)	c)	d)	e)	Size of Audieno	Type and Goal of the Event	Countries Addressed
Web	TEC/All partners	HINT LinkedIn Account	6	2013	Online	x	x	x	x	x	/	Social medium at http://www.linkedin.com/groups?gid=5065 713&trk=myg_ugrp_ovr	International
Exhibition	TEC	ICT 2013 – Create, Connect, Grow	11	2013	Vilnius, Lithuani a	x	x	x	x	x	4000+	conference, exhibition, networking sessions, investment forum, activities for students and young researchers	International
Presentation	MOR	HINT Presentation	2	2013	Brussels	x	x		x			Trust & Security Clustering Open Communications Event, Brussels, 7 th Feb. 2013	International
Poster	MOR	HINT Presentation	4	2013	Brussels	x	x		x			TDL and CSP EU Forum Conference	International
Presentation	MOR	HINT Presentation	9	2013	Nice	x	x		x			Chip-to-Cloud Security Forum	International
Presentation	CCS	HINT Presentation	10	2013	Munich, Germany	x	x	x	x	x	40	Present a large spectrum of cyber- physical systems topics and challenges	International

Table 2: Summary of dissemination activities



1.3.3.1 Upcoming Events

• ICT-2013

The HINT project management team at TEC applied for a Technology and Innovation Stand at the exhibition of "EU ICT 2013 – Create, Connect, Grow" taking place in Vilnius (Lithuania) on 6-8 November 2013. The HINT project has been selected and will be presented at a booth 4B1 during this event. This important networking event includes a conference, an exhibition, networking sessions, an investment forum as well as activities for students and young researchers. The idea is to present the HINT project and to get in contact with potential partners for future projects.

• Chip-to-Cloud Security Forum

The Chip-to-Cloud security forum, formerly known as the *e-smart* conference, is one of the main chip oriented security conferences (<u>www.chip-to-cloud.com</u>) gathering "*the finest expertise*" from R&D and Academia to address security issues pertaining to embedded security, Trusted mobile devices & services and Cloud Security & Internet of Things. This congress provides its delegates rich opportunities to network, share knowledge and develop businesses in a unique environment involving the industry and academia. In this context, the presentation of the HINT project has been assigned the first slot of the first day in the track 'Latest advances in Security Architectures' of Chip-to-Cloud 2013. At the time this report was written, the Chip-to-Cloud 2013 was actually taking place (25-27th of September 2013) and for this reason a written feedback on this event will only be available in next year's dissemination report.

1.3.4 The HINT Project Website

Public HINT Website http://www.hint-project.eu

For the visibility of the project the project website was launched in month 3 of the project. It provides an overview of the project and up-to-date information on its activities and results, as well as contact details, partner information and information on events. The website, which is hosted by the project coordinator Technikon, is based on the Content Management System (CMS) "Joomla!", and a whole tool set including web servers which provide the public website of the project and additionally functionalities within the restricted areas for members only. The website can be viewed with a standard web browser and will be kept alive throughout the project period and at least 3 years afterwards. The project website has been designed such that it can be handled intuitively to give an introduction to the project.

The HINT project website is available on the following link: <u>http://www.hint-project.eu</u>.

The project website has been updated continuously by the Project Coordinator, whereas all partners participate in the process by notifying the Coordinator of important news and developments.

The following illustration shows the Welcome page of the HINT website. Project details of HINT are summarized on the right, while on the left the content of the respective section is given.





Figure 1: Welcome page of the HINT website

The structure of the official part of the website includes the following links:

<u>Home</u>

• General introduction to the project – Mission and Motivation of the HINT project

<u>News</u>

- Conferences, Workshops and Meetings (date, topic and location)
- Press releases (date and link to the press releases)

Publications & Deliverables

• Publications by HINT partners (Public and approved Deliverables, other Publications, e.g. HINT Leaflet or Newsletter)

Partners

• Consortium of the HINT project



Feedback

• A template for website visitors' feedback.

<u>Login</u>

• Login area for project internal use.

The project website serves as the most versatile information and communication tool, because on the one side it provides information for a worldwide audience and on the other side it enables a working platform for the project team. Therefore, it provides a user-friendly and informative environment.

As mentioned above, the website offers the users general information about the HINT project, its activities, achievements as well as background information, contact details and events. By clicking on the "News"-button a list of conferences, workshops and meetings as well as press releases appears, which is illustrated in the following figure. Furthermore, the user can access the adequate site of the preferred news.

Home News Publications & Deliverables	Partners Feedback Login
You are here: Home & News	
News	Search
Conferences, Workshops and Meetings	Project Details
September 2013	Project reference: 317930 Start date: 2012-10-01
Chip-to-Cloud Security Forum 2013 September, 25th - 27th Nice/France	End date: 2015-09-30 Duration: 36 months
HINT Technical Meeting September, 5th - 6th Paderborn/Germany	Project cost: € 5.103.893 Project funding: € 3.350.000 Programme type:
June 2013	Seventh Framework Program
HOST 2013	Programme acronym: EP7-ICT-2011-8
June, 2nd - 3rd Austin/Texas (USA)	Contract type:
Way 2013	Collaborative project
May, 21st - 22nd Paris/France	Follow 2 followers
April 2013	
Cyber Security & Privacy EU Forum 2013 April, 18th - 19th Brussels/Belgium	
February 2013	
Trust and Security Clustering Open Communications Event 2013 February, 7th Brussels/Belgium	
January 2013	
HINT Technical Meeting January, 30th - 31st Graz/Austria	
October 2012	
HINT Kick Off Meeting October, 3rd Gardanne/France	
Press releases	
January 2013	
HINT-Announcement Letter	



A statistical analysis of access to the HINT project website (graphical visualisation) has been created which can be found below. In order to obtain these figures, we used two different statistical tools.

The following figures give attention to the first project period from the launch of the website in December 2012 to end of August 2013.



Figure 3: HINT website statistics

In total, the page was visited 9.247 times by 2.755 unique visitors. Until mid of September 2013, the HINT Announcement Letter was viewed about 110 times and the HINT Leaflet 361 times.

The newsletter, which has been launched on the 10th of September 2013, has already been viewed 69 times in the first week, which seems to be strongly related to the announcement on the HINT Twitter account.

Document	Views		
Newsletter	69		
Leaflet	361		
Announcement Letter	113		
Total (up to 18 th September 2013)	543		

Table 3: Documents viewed



Restricted Area of HINT Website •

Beside the public area there is a password-protected area, which is reserved for project participants in order to share project-internal data only. Thus, only registered partners are able to enter it and can benefit from the options offered there, e.g.:

- Documentation and Tutorials related to HINT,
- Calendar for appointments and meetings, 0
- Mailing lists for reaching special mailing groups, 0
- Archives of the mailing list emails, 0
- SVN Repository, 0
- Your Profile for managing details
- Internal project handbook

The goal of the HINT internal project handbook is to summarize all important rules and procedures of the HINT project. It aims at providing a short introduction to new project members and should be a useful "reference book" for any other project member.



Figure 4: Content of the restricted area



1.3.5 Further means of dissemination

1.3.5.1 Project Logo

To improve of its visibility, the HINT project has adopted a project logo. The logo is used on all internal templates as well as on external dissemination tools.



Figure 5: HINT logo

1.3.5.2 Project Announcement Letter

The intention of the HINT Announcement Letter was to communicate the project start and ideas towards the general public. It was released in January 2013 giving a summary of the project addressed to non-specialist citizens and outlines what the project is about and how its planned results would matter for citizens and consumers. It can be found on the HINT-website by following the link:

https://www.hint-project.eu/downloads/HINT_Announcement_Letter_Website.pdf.

1.3.5.3 Project Leaflet

The official HINT leaflet is a four page informative and graphically appealing A4 flyer, highlighting the objectives and the work programme of HINT. It has already been used on several events and will of course also be used for distribution at the Chip to Cloud Security Forum 2013 in Nice and at ICT 2013 in Vilnius in order to provide further visibility to the HINT project. TEC was mainly responsible for the design of the leaflet and distributed it to all partners after finalisation. An electronic version of the leaflet is available on the HINT website following https://www.hint-project.eu/downloads/HINT_Leaflet.pdf.



Figure 6: HINT leaflet



1.3.5.4 Project Newsletter

In September 2013, the first newsletter of the HINT project was issued in order to disseminate project related news. The newsletter offers current information and points to important events. The newsletter can be found on the HINT website on http://www.hint-project.eu/downloads/HINT_Newsletter_Issue_September_2013.pdf and is also posted via the HINT Twitter and HINT LinkedIn account (see chapter 1.3.5.5) to catch further public awareness. It is planned to publish newsletters on a regular basis, in order to keep external partners and the public updated.

Newsletter Extention Detail Barnet or 200	A me we
Hair Project Information Be first year of the HNT project has alread passed. The first year of the HNT project has alread passed. The first year of the HNT project has alread passed. The first year of the HNT project has alread passed. The first year of the HNT project has alread passed. The first year of the HNT project has alread passed. The first year of the project was alread passed. project, which a characterised by the place of early project has alread passed. project, the HNT coordination has mill be paps in the first HT coordination has mill be paps of early coordination has alread paper has a set all to amounteen the first HT coordination has mill be paps of early coordination has mill be paps of early coordination. Characterised of the project has a coordination. Characterised be paper has a coordination. Characterised be paper has a coordination. Characterised be paper has a coordination. Characterised be paper has a coordination. Characterised be paper has a coordination. Characterised be early be paper has a coordination. Characterised be paper has a coordination. Characterised be paper has a coordination. Characterise has a coordination.	Definition of targeted applications based on use case analysis To applications the spinel of the targeted in HVT, one or Uncloselie D cards and one on Professional Mole analysis of accurity and terrate in the targeted in HVT, one or Uncloselie A card terrate and the analysis of accurity and terrate that the target and end the spinel of the targeted in the target and the spinel of the target applications Science VM and Molecular States (States Card States Card
Key Data: Statute 1 October 2012 Consortium: 7 partners (4 countries) Data Date: 3 Single-Inder 2015 Project Countries 7 partners (4 countries) Data Date: 3 Single-Inder 2015 Project Countries 7 partners (4 countries) Project Outcome 3 Single-Inder 2015 Project Countries 7 partners (4 countries) Project Outcome 5 Single-Inder 2015 Project Project Inder Gene Arrows Project Webole: Det HIMT Project Ana received funding from the Date Long The Transport France United Single-Inder 2015 partners (1 countries) PSP2007 2011 United Transport Long The Transport partners (1 countries) partners (1 countries) PSP2007 2011 United Transport Long The Transport partners (1 countries) 17306 Seventh Framework Project Inder Countries) partners (1 countries)	For the integration of HM-based releases is 60. Scrach. No required adjustation of existing Protectora Pro- fer a Protection Profile were specified. The security analysis in VIPS will be based on these achievements. HINT Project Coordination Team Dr. Klaus-Aldichael Account of the Protections Profile County of the Profile Security. Development Terrivation Constrainings - user Protections Biological County of the Profile Security. Development Terrivation Constrainings - user Protections Biological County of the Profile Security. Development Terrivation Constrainings - user Protections Biological County of the Profile Security. Development Terrivation Constrainings - user Protections Biological County of the Profile Security of the Pro

Figure 7: HINT newsletter issue 1

1.3.5.5 Social Media: HINT Twitter Account and HINT LinkedIn-Group

Making use of the advantages of social media helps spreading project information to a large audience. As a consequence, they are valuable means to disseminate project ideas and results.

<u>Twitter</u> is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets". The HINT project is available on <u>http://twitter.com/hint_project</u>.

<u>LinkedIn</u> is a social networking site for people in professional occupations or simply a social network for business. The HINT group is a closed group. This ensures that only people who have been approved by the manager or admin can see the content of the group. It can be accessed via:

http://www.linkedin.com/groups?gid=5065713&trk=myg_ugrp_ovr.

On the HINT-website direct links to the HINT Twitter Account and the HINT LinkedIn-Group can be found.





1.3.5.6 Cooperation with other projects

As part of HINT's project management and dissemination activities, other FP7-projects in the same area have been identified. The HINT project management team at TEC contacted the coordinators of the PUFFIN and the TOISE projects and provided them with the most important information on the HINT-project.

The intention is to place the links to the websites of the related projects on the HINT-website allowing interest groups to come across related projects when visiting the HINT homepage as well as an exchange of experiences between the project consortia.

1.3.5.7 Interview for EU Yearbook

Based on an interview given by the HINT project coordinator TEC, an article about the HINT project will be published in the EU Yearbook, which will be compiled by the Effectplus/SecCord project team. This article is another way of making the public community aware of HINT.



Chapter 2 Standardisation & Exploitation

The HINT project aims at providing disruptive technologies in terms of hardware integrity and authenticity. Like for all disruptive technologies, their adoption and "standardisation" by the community shall be a long process. However, the HINT partners are committed to start the ground work for promoting the HINT technologies within the concerned standardisation groups as initially described in the DoW as soon as significant and mature-enough technical results are available.

At this early stage of the project where specifications have just been finalised and first designs & tests are just starting, exploitation initiatives, especially for the industrial partners, have not yet concretely started. However, based on the specifications made and first experiments carried, some partners are envisaging adaptations of the exploitation plans initially specified in the project's DoW as detailed in this chapter.

2.1 Standardisation Plans of the Partners

No major change to the initial standardisation plans expressed by each partner in the initial description of work is to be noted at this stage. Since we are in the first year of the project, the technical results are not mature enough to have been concretely presented to standardisation bodies. However, the project partners have the feeling that since the integrity and authenticity of integrated circuits is a major concern worldwide, it would be to no one's surprise that before the end of the project, international initiatives to standardise the detection of hardware Trojans or the insertion or use of PUFs might appear, in which case the HINT project partners will fully contribute to those initiatives.

TEC, as coordinator, will actively support the standardisation activities of the consortium and will provide assistance where needed and appropriate.

The **CEA-LETI** is a Common Criteria and ITSEF certified laboratory and hence participates and contributes to several security evaluation standards both at the national and international levels. Through this channel, the CEA-LETI shall push HINT technology and disseminate about the project into those standardization bodies whenever relevant. In particular, innovative security solutions will be checked for vulnerabilities related to the technologies and their implementation. Information about adequate testing methodology will be done towards the French Certification Body (ANSSI) and the other French laboratories during periodical workshops of the French Scheme.

IFAT participates and contributes – directly or through national bodies – to various standards involved (ISO, ETSI, NFC Forum...) and will promote standardization relevant outcomes of the HINT project in proposals for standardization, where appropriate. IFAT is sending delegates to all relevant standardization groups for technologies needed for government-ID (eID as well as ePassport) applications. Also in this case cooperation with her mother company will serve as a fruitful means for instance in the field of trusted computing, where Infineon is represented e.g. by the chairing the Trusted Computing Group's Certification Program Committee.

ARMINES will support the industrial partners of HINT in their contribution to standards.

KUL supports the industrial partners in the contribution to standards.

MOR is an active member in a couple of standardization bodies related to smart cards and their associated application areas. They are involved for instance in various ETSI groups, in Global Platform, in associations of Smart Card manufacturers like Eurosmart and



SIMalliance, and in initiatives related to the development of European and national ID cards. Moreover, the company is contributing to certification bodies in the context of Common Criteria evaluation. The involvement of Morpho Cards in standardization bodies will be used for the project in both directions, to align the RTD work of the company in HINT with the relevant technical standards as well as to propose project results for standardization where appropriate.

CCS is the editor of and a contributor to many standardization bodies, like ISO. As far as we know, no ISO standard is related to hardware integrity. So, Cassidian can be at the end of the project a contributor/editor of a new ISO standard on Hardware Trojan detection and Physically Unclonable Function (PUF) design and test.

2.2 Exploitation Plans of the Partners

With respect to the exploitation plans initially described in the description of work, some of the partners have refined their exploitation plans based on the technical work that has been initiated in the project. The detailed plans are listed below.

TEC: HINT project will reinforce and extend Technikon's knowledge in hardware security architecture development and modelling. Experience gained will be funnelled into our industrial services on requirement engineering and security engineering services on physically unclonable functions. As an emerging SME, the reputation gained from the project will positively influence our future acquisition activities. As far as TEC's contribution on requirement engineering is concerned it will benefit from the expertise gained in the collaboration with the scientific and industrial partners on development of use cases and the technology roadmap. This will also positively influence TEC's activities in supporting and establishing start-up companies.

CEA-LETI: One of the CEA-LETI's objectives, as an industry focused research organisation, is to devise and exploit, from an industrial point of view, state-of-the-art technological innovations. In the case of HINT, the work done in WP3 on the design of innovative technologies for the detection of unexpected hardware modifications is expected to generate IPs that can be exploited by the CEA-LETI's industrial partners to allow them propose new security functionalities to their security devices. Moreover, the work that shall be done in the security evaluation WP shall contribute to reinforce the CEA-LETI's position in national and international security evaluation standardisation bodies as a technical leader in security profiling of ubiquitous security systems for market driven applications

IFAT: Infineon Technologies Austria AG plans – together with her mother Infineon Technologies AG based in Munich/Germany – to exploit the results of the HINT project in all potential application areas in the field of chip card and security ICs. There are several options for enhancements of future products by holistic approaches of integrity checking or bindings of Silicon integrity to system integrity. Firstly, in the application field of trusted embedded systems – where Infineon has been providing and successfully brought to market a certified hardware based security solution according to the Trusted Computing Group's Trusted Platform Module (TPM) specification – holistic integrity checking could offer a further trust enhancing component. Depending on maturity of the technology and progress in standardization such a feature could either act as a unique selling proposition (USP) or – if adopted in time by standardization bodies – could represent a mandatory feature for trusted systems.

Secondly, in smartcard like systems – as e.g. used in government-ID applications – testability for authenticity and/or uniqueness of a dedicated piece of hardware in an eID document in the field could potentially increase the level of fraud-protection.

Thirdly in mobile devices, integrity based on hardware components with hardware integrity anchors may serve as secure elements with additional barriers against attacks based on



component replacements. IFAT will thoroughly investigate all various exploitation potentials to defend its world-wide leading market position in chip card and security ICs.

As of the time being (end of year one of the HINT project) PUF technologies are not yet considered mature enough to be incorporated into high security products. New publications on attacks upcoming with a rather high frequency imply that so far not enough research has been performed on attacks and countermeasures. If later during the HINT project such ongoing research would provide evidence that PUFs may be securely implemented and would help to increase the security level of IT security systems the exploitation strategy could be adapted.

ARMINES: With this project, ARMINES aims at strengthening its position in the research community by tackling the challenges of the integrity checking of integrated circuits. Therefore, breakthrough innovations are expected in WP3 for the design methods and experimentation platforms. The consolidation of a strong expertise in the design of secure devices at ARMINES will also attract industry. The above exploitation plan for the academic partners is also expected to raise the level of education by giving engineering, Masters and PhD students the opportunity to work on cutting-edge research topics in a European-wide network of highly skilled partners.

KUL aims at presenting its research results at top level conferences and symposia, such as the CHES (Cryptographic Hardware and Embedded Systems) workshop of IACR. It also publishes its results in top journals such as the IEEE and ACM Journals.

MOR: The main technical contributions of Morpho Cards GmbH to HINT include integration and evaluation of physical unclonable functions in Smart Cards and related secure elements. Within the project, components of at least one concrete application will be prototyped, of a PUF-based ID-card with enhanced integrity. Accordingly, exploitation of project results is mainly planned in terms of developing Smart Card products that integrate PUF technology, like the aforementioned unclonable ID-card. During the course of the project, exploitation will be prepared by the partner's dissemination activities, e.g. by promoting project results to stakeholders and potential customers through customer newsletters, showcases at exhibitions, and in meetings with business partners. This will enable the analysis of technical requirements as well as of business requirements for later product development. Moreover, project results will be promoted inside the Morpho group in order to identify further potential for exploitation not directly related to Smart Cards.

Cassidian CyberSecurity is expecting to exploit (through technical publications) the 4 main results it shall be deriving from the HINT project:

- A generic side-channel detection test-bench of Hardware Trojans based on SAKURA-G board. A paper shall be submitted to the DATE 2014 conference (deadline: September 2013).
- Techniques for the fine-grained insertion of Hardware Trojans shall also be published.
- Progress in Hardware Trojan Detection by side-channel analysis shall be a major focus of the project and shall be published.
- Cassidian CS shall also communicate on the experimental set-up and the demo for on-board HT detection.

Patents fillings are also envisaged for those 4 results.

2.2.1 Preliminary Market Overview

CASSIDIAN is a world-leading manufacturer and provider of Professional Mobile Radio (PMR) systems. CASSIDIAN solutions enable professional organizations to communicate together effectively, reliably, and securely. CASSIDIAN is the sole company in the world that can offer specialized PMR solutions based on TETRAPOL, TETRA, and APCO-P25



technologies. CASSIDIAN has already delivered 160 mission-critical PMR networks worldwide, more than 30 of which with nationwide coverage.

More than one million professional users operate daily over these networks, and around 700 000 of them use hardware-based cryptographic chips. CASSIDIAN Secure Networks sells around 100 000 secure PMR handhelds per year, thus the requirement for an equivalent yearly quantity of high-assurance security modules such as considered in the HINT project.

CCS will transform the project outcome into production-grade cryptographic modules to be embedded in next generation of Professional Mobile Radio systems (network cipher boards, mobile terminals), with a security target compliant with the higher levels from ISO/IEC 19790 standard (targeting security level 3 and above). This will induce an added -value compared to its competitors and increase its market share (an increase of 10% is expected in medium-term).

Despite the over-a-decade-old research that exists on PUF technologies, the latter are still 'young' concepts. Unless the concepts of security and robustness of the PUF cells through shrinking technology nodes are fully understood and mastered (one of the objectives of the HINT project is actually to help into that), the project partners cannot predict what will be the impact of the current research work on the market of secure devices. This might be feasible when more mature results are available during the course of the project.

2.3 Joint Exploitation Plan

At this stage of the project, no joint exploitations are officially planned among the project partners. However, given the pieces of joint technical work that have started during the first year of the project on several topics, there is no doubt that some common exploitations shall come up during the second year, at least on the joint dissemination of the technical results through scientific publications:

- IFAT and MORPHO working on prerequisites for unclonable ID cards.
- IFAT & TEC working on modelling and emulation of PUFs.
- IFAT & KUL working on PUF attack strategies.
- CCS, ARMINES, CEA & KUL working on the side channel measurement bench.
- CCS & ARMINES working on the design of hardware Trojans.
- KUL & MORPHO working together on template techniques for Trojan detection.
- KUL, MORPHO, CCS, ARMINES & CEA working on the analysis of the side channel measurements made.

2.4 IPR issues identified in the HINT project

In the environment of international applied research projects with industrial partners such as HINT, the careful handling of IPR issues is of strategic importance. Within the HINT project, many individuals of numerous organisations cooperate across national borders. In order to develop novel technologies, concepts or processes an exchange of information with other parties is a necessity. Furthermore, jointly creating new intellectual properties is common. Therefore, confidentiality is a very important issue for participants in HINT, from the project start-up phase of joint activities to the implementation phase and further to the exploitation of results.



All efforts related to IPR issues aim to create a favourable environment for respecting intellectual property rights (IPR) because of moral and economic reasons. Without IPR protection, the joint creativity of natural persons or legal bodies as well as the dissemination and exploitation of results would be highly restricted not to risk a substantial drain of knowledge. Intellectual property (IP) is an intangible asset and created as a result of intellectual creative effort of the human mind in relation to works of authorship and/or inventions. With the ownership of intangible assets, certain legal exclusive property rights which are established by law or by contractual obligation are connected and maintain the control in relation to the protection of the interests of the creators by excluding these creations from public property. This means that right to permit or deny the use and exploitation of the creative work. So IPR provides a protection of the creations and inventions to the owners by preventing users from using or copying them without reservation or payment for a certain period of time.

Intellectual property can be classified into:

- Industrial property items like inventions which can be a product or a process providing new solutions for solving (technical) problems and which can be protected by registering a patent and
- Copyright items which provide exclusive rights to the creator to prohibit the authorized copying, adaptation and reproduction of its intellectual work.

The protection of the knowledge developed within HINT is vital for each of the participants.

2.4.1 Prerequisites for the HINT project

The management of intellectual property in HINT was already important at the project proposal set-up stage where the first development of appropriate ideas for the joint research activities and the assembling of the project consortium took place.

Even at this early stage discussions and the exchange of information between different people from institutions with different knowledge, background and interests was required and IPR issues needed to be discussed and integrated into the appropriate sections within the proposal.

Later on, the grant agreement (GA) represents a contract which establishes the beneficiaries' rights and obligations towards the European Community and towards each other. It contains a specific provision on confidentiality that defines the obligation and its term. Moreover it also covers an intellectual property related section.

Furthermore, in order to guarantee a uniform approach by the HINT participants, internal rules should be defined, including confidentiality clauses for the use of dissemination of results, which can be incorporated in the consortium agreement (CA).

In the present section, all stages and contracts which are important IPR prerequisites for the project set-up will be briefly explained, with the focus on their implementation in the HINT project.

2.4.2 Drafting of Proposals

In writing the project proposal for HINT, the management of IPR was already outlined because the exchange of information between the partners in such an early stage is of certain risk. Although copyright allows some legal protection against unlawful copying of works, all parties should nevertheless only reveal any such information under terms of confidentiality in order to protect the contained ideas in a broader sense.



During the HINT proposal drafting phase, it was laid down that the consortium agreement, as an outline contract between the partners, would define the rules and measures as well as the rights and duties for protecting the IP within the HINT project. Through signing the consortium agreement and its confidentiality clauses, the HINT partners committed themselves to protecting the confidential information brought into or resulting from the HINT project. Also plans for the use and protection of the results have been considered (more in "Consortium Agreement" chapter).

Additionally, the management structure has been set up with the protection of knowledge in mind, which foresees the permanent monitoring of IPR issues during the project.

2.4.3 Contracts

Within the HINT project two agreements have been prepared which all partners had to sign in order to participate in the project: the grant agreement and the consortium agreement. Both of these agreements include IPR regulations for the project and therefore represent the contractual basis for IPR within HINT.

2.4.3.1 Grant Agreement (GA)

The grant agreement is the contractual basis for the European Commission (EC) funded project HINT which is the principal agreement between the EC and the coordinator. This contract sets out in writing the key project details such as the parties involved, the scope, the duration and start date of the project, the reporting periods, the maximum financial contribution of the EC, the main contact data of the contracting parties as well as some specific issues.

It was clear to the project partners from the beginning that due diligence would be required with regard to confidentiality. Therefore, they determined the level of confidentiality of information that would be provided in deliverables throughout the HINT project when the work to be done in the project was defined and stated in Annex I to the GA.

2.4.3.2 Consortium Agreement (CA)

The consortium agreement is signed between the project participants of the consortium and implements the grant agreement, establishing provisions related mainly to consortium management, the distribution of the Community financial contribution and IP. The CA is a negotiated and agreed mandatory contract between the project partners, which has to be signed by all partners before the entry into force of the Grant Agreement. The legal requirements are singled out in the Grant Agreement but the details regarding the cooperation are given in a specific Consortium Agreement. The HINT Consortium Agreement was signed by all partners in October/November 2012 and it sets out the internal management guidelines for the consortium including established rules, structures and processes for handling IPR.

The CA includes guidelines for the project internal management of the cooperation by providing rules for the following issues:

- the parties' obligations for the implementation of the GA
- project internal organisation and project structure (project bodies and their functions, rights and duties, voting regulations)
- handling of commission payments (distribution of the funding by the coordinator)



- provisions about the ownership and licensing of intellectual property (e.g. foreground, publications, access rights, dissemination of results)
- handling of matters of liability and confidentiality
- procedures for settling internal disputes
- handling of defaults and remedies (exclusion/withdrawing)

Knowledge, or foreground³, generated within the project will be protected by patent filing or publication in accordance with the consortium agreement that also represents an outline contract between the partners. The status of background⁴ and sideground⁵ brought in or developed in parallel is also covered by the CA. Amendments to the CA can be done on a per partner basis as the needs for knowledge and protection varies between the partners. With their signature of the CA, all partners agreed to the content of the binding Agreement.

Besides the general principles relating to access rights, the HINT CA deals with clauses concerning access rights for affiliates as well as special provisions concerning access rights to software, standards and access rights for parties joining or leaving the project. Furthermore, the CA covers rules regarding the confidentiality period, exceptions, disclosure of confidential information in compliance with a court order and to the Commission as well as disclosure of confidential information to affiliates and it covers regulations regarding the disclosure of results to the public as well as the provided information to the EC.

2.4.4 Status of the project with regard to IPR issues

On the basis of the above-mentioned contractual framework defined and agreed in the runup to the project, the relevant intellectual property rights must be maintained during the project. Therefore the management structure, workflows and tools are designed with the protection of knowledge in mind. The project management is responsible for the monitoring of IPR issues. All partners are obligated to report any protection of intellectual property to the project management.

New knowledge produced during the project belongs to the supplying partner and any commercial exploitation or public disclosure of new knowledge can only be done after the owner gives his consent. The decisions to patent any results belong to the owner; the other partners must not interfere in this process. In case of jointly developed new knowledge the ownership needs to be agreed upon before any dissemination and/or exploitation.

The protection of knowledge, or Foreground generated within the project, is vital for each of the HINT participants and is mainly realised by patent filing and/or publications.

The following subchapters should provide an insight regarding the current situation concerning different IPR issues within the HINT project.

³ **Foreground** is understood to be tangible and intangible project results in terms of information, materials and knowledge generated inside the project. Foreground is principally owned by the partner who generated it; when the generation of the foreground is a joint process, it is - unless the partners do not agree on another solution - jointly owned by the participants.

⁴ **Background** is understood to be information, knowledge and any IPR relevant to the project already held by the project partner before the accession to the EC Grant Agreement.

⁵ Sideground is intellectual property created during a contract but which is not considered to be part of the contract.



2.4.5 Licences

No particular licences have been sought by the HINT partners during the first year. Most of the tools used for research purposes are tools available for free following the GNU General Public Licence (like Octave, Perl...). For the design part, copyrights pertaining to the licences of design tools are taken into account.

Infineon identified one of its own patents which it might use: US2012072476 "IDENTIFICATION CIRCUIT AND METHOD FOR GENERATING AN IDENTIFICATION BIT USING PHYSICAL UNCLONABLE FUNCTIONS".

2.4.6 Patents

Several project partners have identified patents which they might file during the course of this project if significant results are obtained:

- CCS will probably seek to file a patent on real-time hardware Trojan detection.
- The CEA envisages filing patents on the on-chip power measurements and/or active schemes for hardware Trojan detection.
- For the KUL, it is quite likely that some of the technical results of the HINT project will be patented. This could both include innovative PUF technology, as buildings blocks related to Hardware Trojan detection.
- Morpho evaluates on a regular basis its work on PUF post-processing and Side Channel Analysis for Trojan detection regarding potential patent applications.

2.4.7 Copyrights

Basically all IFAT presentations and published materials are copyright protected.

2.4.8 Violations

The IP departments of the industrial partners are currently performing anteriority searches on topics pertaining to HINT.

2.4.9 Partnerships with other projects/partners outside HINT dealing with a related topic

The CEA plans to participation to the French national GDR-SocSiP workshops on secure trusted hardware.

KUL carried out research on PUF technology in the UNIQUE project. This European research project, which already finished, is related to WP2 of the HINT project.

KUL is currently involved in the PUFFIN project. This European research project is related to WP2 of the HINT project, as it intends to study and show the existence of SRAM PUFs and other types of PUFs in standard PCs, laptops, mobile phones and consumer electronics. Moreover, KUL also gave several seminars on PUF technology during various workshops and courses, including:

- IMEC
- Romanian Cryptology Days (RCD 2013)



KUL is planning to give seminars on integrity technologies during various courses and workshops. In the near future, a course on PUF technology is planned during the PANDA summer school (Summer Course on Physical Attacks aNd Design Attestation) in China (<u>http://www.sklois.cn/panda/2013</u>).

TEC has been coordinator for the FP7 Project UNIQUE which provided the basis for the PUF related topics in the HINT project.

One project which is currently under negotiation can be seen as follow-up project of HINT in the PUF direction. IFAT and TEC will work together in the project as they already do in HINT.

Another project pointed out by IFAT has been the Austrian FIT-IT project "PUCKMAES" funded by Austrian BMVIT, the results of which could be used as a base for HINT.

2.5 **Project Results**

The following subchapter describes the development of project results (deliverables, reports and scientific publications) as well as the regulations of such results within the HINT project.

2.5.1 Deliverables

All project participants are obliged to take care that the information provided in the deliverables and reports corresponds to the IPR regulations, especially when compiling public deliverables and reports.

In order to ensure that only public content is contained in public deliverables and that IPR rules have been considered the HINT consortium defined an internal review process for deliverables.

This process requires the approval of both the Project Management, and a reviewer external to the work package, before a deliverable is released. This ensures that the qualitative targets are reached with regards to technical content, the objectives of the project and adherence to formal requirements established in the GAs and CAs.





The editor is responsible for appointing an external reviewer and sending a draft to the Project Management at least 21 days before the planned publication or delivery. This draft is also sent to the internal reviewer. A copy is similarly sent to owners of Intellectual Property related to the content. The reviewer and Project Management shall send their comments back to the editor within 5 days. The editor updates the deliverable within 5 days and sends it back to the Project Management for final approval.



The deliverable will be forwarded to the Coordinator who submits it to the Commission. The editor for any deliverable is by default the work package leader. It is the responsibility of the work package leader to ensure that the review form has been filled out correctly.

	PMT: Technikon			Internal Reviewer:		
	Answer	Comments	Type*	Answer	Comments	Type*
1. Is the deliverable in acc	ordance with	1				
i. the Description of Work?	□ Yes □ No		□ M □ m □ ₽	□ Yes □ No		□ M □ m □ ₽
ii. the international State-of- the-Art?	Ves		Пм Пт Па	Ves		_м
2. Is the quality of the del	iverable such					
i. that it can be sent to the EC?	□ Yes □ No		□ m □ m □ ₽	□ Yes □ No		□ M □ m □ ₽
ii. that it needs further editing?	□ Yes □ No		Пм Пт Па	□ Yes □ No		ом от
iii. that the content needs to be improved?	Ves		□ M □ m □ ₽	☐ Yes ☐ No		Шм Пт Пз

Review Form for the Internal Reviewer and the Project Management Team (PMT)

Figure 9: Deliverable Review Form

2.5.2 Scientific Publications

For scientific publications, we use the technical mailing list (technical@lists.hint-project.eu) to notify all partners about any future paper submission in order to prevent possible IPR conflicts. The basic rules are that the notification should be sent 21 days before the submission as foreseen in the Consortium Agreement (CA 8.3.1). The HINT Consortium has agreed that it should contain the following information:

- 1. Working Title
- 2. Authors (at least one contact person)
- 3. Target date and conference/journal



It has to be ensured that the authorship rules are followed: no foreign ideas, no foreign text, all potential authors are in fact authors.

One further rule is that the acknowledgement clause has to be part of the acknowledgements of each article:

"The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n°317930 (HINT project: <u>http://www.hint-project.eu</u>). Opinions expressed are those of the authors. They do not necessarily represent the views of all HINT partners."



Chapter 3 List of Abbreviations

DoW	Description of Work
HT	Hardware Trojan
SCA	Side Channel Analysis
IPR	Intellectual Property Rights
SME	Small and Medium-sized Enterprise
PUF	Physical Unclonable Functions