D5.2
Project Dissemination Plan

Project number:	238811
Project acronym:	**UNIQUE**
Project title:	Foundations for Forgery-Resistant Security Hardware
Start date of the project:	September 1, 2009
Duration:	30 months

Deliverable type:	Report
Deliverable reference number:	238811 / D5.2 / FINAL | 1.0
Deliverable title:	Project Dissemination Plan
WP contributing to the deliverable:	WP5
Due date:	2010-02-28 (M06)
Actual submission date:	2010-02-28

Responsible organisation:	TEC
Authors:	TEC (Ulrike Schnitzer)
Abstract:	The following document gives an overview of the dissemination activities planned for the UNIQUE project. It describes the dissemination strategy as well as the actual events and activities carried out by the partners.
Keywords:	Dissemination, Strategy, Activities

Dissemination level:	Public
Revision:	FINAL | 1.0

Instrument:	STREP
Thematic Priority:	ICT

Table of Contents

List of Tables

List of Figures

1 Introduction

The purpose of the dissemination is to make UNIQUE a successful and sustainable project by raising the awareness and publicity of the UNIQUE project as well as its outcome. In this context the target groups for external dissemination activities are on the one hand the general public and on the other hand potential business partners as well as specific scientific experts. A further target audience are public institutions like governmental and European audiences.

In order to reach the particular awareness level intended, the **partners have to work continuously in the field of dissemination and public relation**. For their support as well as for the graphical identity within the consortium the partners have to be provided with templates (for presentations and reporting) and various communication materials (web site, fact sheet, press release etc.).

The purpose of this plan is to collect information on the dissemination activities already completed or planned during the 30 month run time of the UNIQUE project. It contains a plan for already carried out and prospectively upcoming activities based on a form collected from each partner; it describes the dissemination channels to be used and the dissemination material to be produced and it indicates their schedule. So the dissemination plan gives an overview via the various activities and enables their coordination. At this point it is important to note, that the focus of the mentioned dissemination activities of the UNIQUE partners is in the first half of the project. The reason for this is in the impreciseness of planning of activities that are lying ahead. So this dissemination plan can be regarded as a guideline and will be supplemented in the course of the project duration.

The dissemination plan of the UNIQUE project has been arranged into a logical sequence of various activities, which will be described in the following "Dissemination strategy" section, whereas the real planned activities will follow later in the second section "Planned dissemination of knowledge". Additional activities have to be expected when the partners have prepared more detailed plans for their work. Invitations to contribute to both publications and conferences are expected as the project receives more attention throughout Europe and the rest of the world. These activities will be reported during the periodic reporting after the end of each project period.

However, as the first step, the dissemination strategy will be described. This information dissemination plan consists of a collection of planned and already completed activities to disseminate the knowledge and results generated during the project. Additionally a list of approaches is given as basis for planning future activities.

2 Dissemination strategy

The dissemination strategy of the UNIQUE project consists of three consecutive phases which require different methods and activities to be initiated in order to be able to achieve the goals:

1. **Awareness-oriented phase**

    The goal of the first phase is to raise awareness about the project and its objectives. This involves the setting up of the basic marketing materials and awareness-raising presentations at different related events. The main activities of this phase are:

    - Setting up a common project design, such as a UNIQUE 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 UNIQUE in order to raise awareness among the scientific and industrial stakeholders and to establish the basic brand name of UNIQUE.

2. Result-oriented phase

The second phase aims to promote the results of the project, in order to allow potential interested parties to get to know the achievements and the related benefits of the UNIQUE project. This will be done by addressing stakeholders in programmable Hardware related Security issues and take the following activities in account:

- 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 introduction the findings of the UNIQUE project. These presentations will still be research-oriented.
- High-quality papers will be submitted to scientific and industry conferences such as RSA, ICISC, IEEE Security and Privacy, CHES, Usenix Security, ACSAC, ASMCCS, ISC, ISSE, CHES.
- The UNIQUE consortium will publish and disseminate press release after having reached important milestones. These press releases will be circulated to representatives of the international press focusing on Hardware security.

3. Exploitation-oriented phase

During the final dissemination phase specific activities will be undertaken in order to actually start the exploitation. The exploitation is targeted at potential clients of the UNIQUE security framework. 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.
- Publishing of the UNIQUE security framework in order to lay the foundation of potential commercial projects.
- Participation at Hardware security-oriented exhibitions, fairs and workshops, where the results of the project should be presented to business stakeholders and contacts for potential commercial projects could be built.
- Individualised demonstrations at interested stakeholders during the negotiation of business projects.
- Finally, a follow-up-project from the UNIQUE results at an industrial research level could be possible.

3 Planned dissemination of knowledge

The Dissemination plan is part of Work Package 05, 'Dissemination'. This work package foresees the following tasks:

- **Dissemination**
  This task involves the supply of structures and processes as well as templates for presentations and publications and other dissemination activities. The purpose is to coordinate and plan the dissemination activities on consortium and partner level because one of the goals of the UNIQUE project is to widely disseminate the results at different levels. The dissemination activities ensure that the public will be aware of the project, interested parties will be able to learn about the project and have access to up-to-date information.

- **Contribution to portfolio and concertation activities at FET-Open level**
  The consortium members will ensure within the areas of interest of the project, that the project results shall be published widely throughout the duration of the project in order to support scientific cooperation at the FET-Open level and broad public awareness of project achievements.

- **IPR and exploitation framework**
  Intellectual Property Rights and Exploitation Framework will be realized by the establishment of rules for the use of knowledge and its distribution.

During the UNIQUE project life-time, the project partners will promote and encourage research on the UNIQUE topic, targeting European and international companies and research centres, as well as create interest in the general public. The dissemination activities will be ongoing during the entire project duration. Accordingly, the dissemination plan will have to be adapted and updated several times.

An overview table presented later in the report summarises all planned dissemination activities, that have been carried out or which are currently planned to take place in the future.

3.1 Contribution of each partner

Within the project, dissemination activities will be divided under two categories, which reflect the difference between activities based on possible benefits. The first category covers those public exploitation and activities which are not interested in commercial revenue, but instead focused on social issues. The second category covers business activitieswith clear commercial motives. An overview on the potential dissemination contributions of the project partners as well as their main exploitation activities in both the science and commercial sector, are given below.

TEC

Dissemination Activities	TEC provides the UNIQUE-project IT-infrastructure – more precisely the whole set of tools which will foster the project cooperation, communication and dissemination, whereby the project website serves as the most versatile external information and communication tool for a worldwide audience. In addition TEC elaborates a UNIQUE-project leaflet as well as a press release together with the other partners. Furthermore we intend to disseminate the UNIQUE-project ideas and its results widely. at various conferences and workshops.

Exploitation Activities	The UNIQUE 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 requirements engineering. As an emerging SME, the reputation gained from the project will positively influence our future acquisition activities. We provide workflow based management support systems for cooperative research efforts at the national and European level. Project experience will trigger improvements of TEC's "Trusted Knowledge Suite". Any novelties introduced will elevate the market position of this IT tool. As the national representative of the European Women in Science, Engineering and Technology (WiTEC) network Technikon will also use the project to promote the objectives of WiTEC.

RUB

Dissemination Activities	The main results of the project will be published in international conferences or journals on information security and privacy as well as on embedded systems. With its series of conferences and workshops RUB will organize research workshops and conferences on this topic, in particular in cooperation with industry from various market branches. In 2008 RUB has organized a very successful research workshop on security hardware with worldwide well-known experts in the renowned conference centre Dagstuhl (Germany). In addition RUB will announce and present the project results to industrial and academic associations within Europe. Furthermore, within various RUB international Masters and PhD programs students can benefit from the achievement of the projects in an emerging high-tech field.
Exploitation Activities	RUB works very close with many international IT enterprises (automotive, machines and plant manufacture, hardware manufacturers) and standardization bodies such as ISO that are interested in the topic of UNIQUE, and aim at presenting the project results to them.

KULEUVEN

Dissemination Activities	KULEUVEN has an active policy of publishing its research results. COSIC publishes in the major conferences and journals associated with cryptographic research, both theoretical and application oriented. Its participation into European projects is also an excellent training for its Ph.D. students to learn to perform research in an international context. KULEUVEN also organizes several training programs for industry, among others in collaboration with LSEC and secappdev.org.
Exploitation Activities	The knowledge acquired through the project will add to the background knowledge of COSIC to stay at the forefront of research in computer security and cryptography. It will also form the basis of further bilateral contract research.

TUD

Dissemination Activities	Dissemination of results will mainly be performed through publication of papers in international conferences or journals (such as ACM Computer and Communications Security, IEEE Symposium on Security and Privacy or IEEE Transactions on Dependable and Secure Computing). Furthermore, the consortium will organize a workshop at the end of the project in order to disseminate the results. TUD is a partner of the "Center for Advanced Security Research Darmstadt" (CASED), which maintains a graduate school on IT security (see http://www.cased.de/en). Graduate students benefit from close collaboration between research and practice: 19 professors attend to their students within a master's program and a well structured PhD program in IT security. We expect to disseminate the results of UNIQUE within the CASED graduate school and make hardware security issues a central topic in IT security education.
Exploitation Activities	CASED has extensive contacts to the important players of the German IT security industry. We plan to demonstrate the results of UNIQUE within the partner network of CASED and discuss their market potential.

TCF

Dissemination Activities	Thales Communications will disseminate the UNIQUE results at three levels. First, internally in the THALES group, where research results are exchanged between all the laboratories working in the Information Security System domain in France, Norway, UK, Germany and Australia. Secondly, in the French national security community where TCF is highly involved in many projects for crypto and secure IC. Thirdly, by TCF active policy to promote patents and publications in international conferences.
Exploitation Activities	For the design and production of security IC, TCF is concerned by IC counterfeit and malicious hardware. The results of this project can improve trust in third party IP and third party manufacturing process. It will also deliver methodologies and building blocks to mitigate counterfeit threats.

SIRRIX

Dissemination Activities	Sirrix has a very high rate of publications in various local and international conferences and is willing to leverage the theoretical and conceptual results of the project for further publications. Moreover, Sirrix is often responsible for organizing research events (FIDIS) and conferences that relate to IT Security, which would give it the chance to disseminate the findings within the project in high-profile conferences and events. Sirrix is also high involved in projects for the German Federal Agency for Information Security (BSI), and is keen to share the security frameworks achieved within UNIQUE for potential governmental projects.

Exploitation Activities	Sirrix is highly interested to commercially exploit the results of the UNIQUE project and expects strong opportunities in getting the results to the market in the medium term. Sirrix already addresses the market for solutions, identifying malicious or counterfeit hardware and plans to provide a software library that can be used by companies who want to use the results of UNIQUE in their commercial applications. Thus and together with Intrinsic-ID, a full solution for identifying malicious and counterfeit hardware can be realized.

IID

Dissemination Activities	Intrinsic-ID visits the most important security conferences in the field of anti-counterfeiting. Our goal is to have a booth at the major one(s). In the past we have often contributed to various academic (CHES) as well as industry related conferences (ESCAR, RSA,...) with scientific work. We also have an active collaboration with the academic world (Pim Tuyls is a visiting professor at COSIC). Intrinsic-ID is also one of the founding parties of the SECSI (Secure Component and System Identification) Workshop in Berlin 2008.
Exploitation Activities	Intrinsic-ID is a security company targeting anti-counterfeiting solutions. The results of this project can further be developed into components that can be used in the anti-counterfeiting products and key storage products key (e.g. Quiddikey) of Intrinsic-ID which will be provided to the European electronics industry to help them grow by securing outsourced manufacturing to the far-east and protecting services such as public transportation and pay-TV.

INTEL

Dissemination Activities	Intel attends most of the important conferences in the fields of interest in Europe and internationally, and has several lablets (small labs linked to the universities) in Europe, including Barcelona, Braunschweig, and the Innovation Center in Ireland. Intel researchers maintain active relationships with academics researchers, through formal and information activities.
Exploitation Activities	FP7 projects, in which Intel is participating, are directly connected with representatives of business units who provide feedback on the applicability and improvement of the results of the research.

3.2 Description of planned dissemination activities

The dissemination activities of the UNIQUE consortium that are planned until this point are collected below. Each different activity includes the relevant description and participants from the UNIQUE consortium.

3.2.1   Active participation in conferences and workshops

The participation in conferences and workshops is considered active if the UNIQUE project partner is in the role of a speaker, a presenter, a moderator or an organiser.

Full name of the conference (abbreviation if applicable), official web-site (no hyperlink, underlined)	Date (dd.mm.yyyy)	Location (city, country)	Type (international/ national) and size of the audience	Topic and goal of the event	Role of the partner, relevance to UNIQUE, benefit gained by partners. (Partners involved)
ICT 2010	27.9-29.9.2010	Brussels	International ICT Conference	ICT research in Europe	TEC representing Unique Project
ISSE 2009	06.-09.10.2009	The Hague, The Netherlands	International, 400+	Hardware assurance / RFID Security	Speaker (INTEL)
COSADE	04.-05.02.2010	Darmstadt, Germany	International	Constructive side-channel analysis and secure design	Invited Speaker (KULEUVEN)
Provable Security against Physical Attacks	15.-19.02.2010	Leiden, The Netherlands	International, 50+ registered participants	To bring together people from theory and applied research working on physical attacks as well as to advance the field and produce relevant, state-of-the-art methods and tools related to physical attacks.	Invited Speaker (KULEUVEN)
RFIDSEC	08.06.1010	Turkey	International	RFID Security	Invited Speaker (IID), planned submission(s) (RUB)

TRUST 2010	21.-23.06.2010	Berlin, Germany	International, 100 – 200	Trust and Trustworthy Computing	Organizer (RUB), Presentation (IID), Participant (INTEL)
Workshop on Security Hardware(co-located with Trust 2010)	21.-23.06.2010	Berlin, Germany	International	Security Hardware	Organizer (IID and RUB)
CHES	18.08.2010	Santa Barbara, CA, USA	International	Workshop on Cryptographic Hardware and Embedded Systems	Planned submission(s) (KULEUVEN), planned submission (RUB), planned submission (IID)
Possible outlets include: IEEE SecureComm, ACM CSS STC (Scalable Trusted Computing), CHES (Cryptographic Hardware and Embedded Systems)	TBA	TBA	International		SIRRIX will publish papers and participate in conferences and workshops in this area. They are targeting IEEE SecureComm, ACM CSS STC (Scalable Trusted Computing), CHES (Cryptographic Hardware and Embedded Systems) and a lot more. Which conferences to participate in or the exact content of the papers cannot be proposed yet, since the results are still in development. (SIRRIX)

Table 1: Summary of actively participated conferences and workshops

3.2.2 Passive participation in conferences and workshops

Full name of the conference (abbreviation if applicable), official web-site (no hyperlink, underlined)	Date (dd.mm.yyyy)	Location (city, country)	Type (international/ national) and size of the audience	Topic and goal of the event	Role of the partner, relevance to UNIQUE, benefit gained. (Partners involved)
3rd International Conference on Trust and Trustworthy Computing (TRUST 2010), http://www.trust2010.org/	21.-23.06.2010	Berlin, Germany	International	Trust and Trustworthy Computing - International conference on the technical and socio-economic aspects of trustworthy infrastructures.	Participation to the UNIQUE workshop hosted by the conference. (To be confirmed) (TCF) … (KULEUVEN),

Table 2: Summary of workshops

3.2.3 Scientific articles and publications

Author(s) (eg E. Example), Date (year of publishing)	Title	Journal title, volume, issue, page numbers	Type (international/ national)	Topic of the article/ publication/ presentation, connection to UNIQUE. (Partners involved)
A.-R. Sadeghi, I. Visconti, C. Wachsmann, 2010	Enhancing RFID Security and Privacy by Physically Unclonable Functions	(under submission)	International	Shows how Physically Unclonable Functions (PUFs) can be used to enhance security and privacy in RFID systems. (RUB)
A.-R. Sadeghi, I. Visconti, C. Wachsmann, 2010	Enhancing RFID Security and Privacy by Physically Unclonable Functions (Extended Abstract)	In Foundations for Forgery-Resilient Cryptographic Hardware, volume 09282 of Dagstuhl Seminar Proceedings, pages 10-11	International	Extended abstract on how Physically Unclonable Functions (PUFs) can be used to enhance privacy in RFID systems. (RUB and others)

A.-R. Sadeghi, I. Visconti, C. Wachsmann, 2009	Anonymizer-Enabled Security and Privacy for RFID	In 8th International Conference on Cryptology And Network Security (CANS), volume 5888 of LNCS, pages 134-153. Springer-Verlag, 2009	International	Shows how trusted hardware can be used to enhance privacy in RFID systems. (RUB and others)
K. Järvinen, V. Kolesnikov, A.-R. Sadeghi, T. Schneider, 2010	Efficient Secure Two-Party Computation with Untrusted Hardware Tokens (Full Version)	(under submission)	International	Considers Secure Function Evaluation (SFE) in the client-server setting where the server issues a secure (hardware) token to the client. (RUB)
D. Naccache (Eds.), A.-R. Sadeghi, 2010	Towards Hardware Intrinsic Security: Foundation and Practice	TBA	International	Book on hardware-based security mechanisms including Physically Unclonable Functions and their applications. (RUB, TUD)
F. Armknecht, R.Maes, A-R. Sadeghi, B. Sunar, P. Tuyls	Memory Leakage-Resilient Encryption based on Physically Unclonable Functions	(under submission) Towards Hardware Intrinsic Security: Foundation and Practice, D. Naccache (Eds.), A.-R. Sadeghi, 2010	International	PUF-based crypto primitives (KULEUVEN, RUB, IID and others)
J. Guajardo, S. S. Kumar, K. Kursawe, R. Maes, A.-R. Sadeghi, D. Schellekens, B. Skoric, P. Tuyls	Physical Unclonable Functions as Security Primitive and Their Applications	(under submission)	International	PUF overview and reconfigurable PUFs (KULEUVEN, RUB, IID and others)
U. Rührmair, H. Busch, S. Katzenbeisser	Strong PUFs: Strong PUFs: Models, Constructions and Security Proofs	TBD		Summary of security models for PUFs (TUD)
Intrinsic-ID	TBA	(under submission)	International	New PUF results (IID)
TBA	TBA	TBA	International	SIRRIX intends to contribute to industrial-oriented conferences by a) publishing at industrial conferences and magazines b) organising own events by dissemination the results in relevant

				industrial and governmental institutions. (SIRRIX)
A.-R. Sadeghi, I. Verbauwhede, C. Vishik, 2009	Future of assurance: Ensuring that a System is Trustworthy	ISSE 2009 Securing Electronic Business Processes, 339 – 349	International	Security assurance in hardware (RUB, KULEUVEN, INTEL)
ISSE 2009 Proceedings	Future of assurance		International	Security assurance in hardware

Table 3: Summary of scientific articles, publications, presentations

3.2.4 Courses, talks organised

Partners involved	Date (dd.mm.yyyy), location (city, country)	Course title, content	Type (international/ national) and size of the audience
TCF	15.12.2009 Rennes, France	*Projets R&D composants SSI* (IT Security Components R&D Projects) Content: overview of Thales involvement in co-operative projects targets the security IC domain. UNIQUE was presented among other projects; the level of information was that of the project leaflet Attendees: French MoD representatives	National, ca. 30 persons
INTEL	21.01.2010	Aspects of Hardware Trust (UCL UK)	National
Open seminar	01.02. 2010	COSIC seminar - Leakage-Resilient Storage (D. Venturi)	
Open seminar	04.02. 2010	COSIC seminar - Leakage-Resilient Signatures (S. Faust)	
All	18.02.2010	UNIQUE Technical Workshop on existing basic technologies relevant to the project.	Project internal

Table 4: Summary of courses organised

3.2.5 Websites

Website	Description of the main UNIQUE related information	Partners involved
www.unique-security.eu	The official website of the UNIQUE project.	**TEC** (in cooperation with all UNIQUE partners)
http://www.esat.kuleuven.be/scd/projectinfo.php?view=2&prid=480	Internal project description	KULEUVEN
Sirrix Website	Short description of the UNIQUE project	SIRRIX

Table 5: Summary of relevant websites

The project website serves as the most versatile information and communication tool, because on the one side it provides the opportunity to provide information for a worldwide audience and enables on the other side a comprehensive provision of information as well as a platform for the project team. So the website's structure aims to provide both easily accessible basic information for external visitors and special information in more detail for registered users.

Figure 1: Homepage of UNIQUE

The webpage informs the user about general information on the UNIQUE project, its activities and its achievements as well as background information, contact details and events. Additional information on each project partner is available by clicking the relevant company logo. Additionally, publications can be downloaded and useful links are given.

In parallel with the general accessible area there is a special domain on the UNIQUE website which is password protected and thus only accessible for registered individuals and/or groups. So the website also serves as a platform of the project and may be used by the UNIQUE members for internal communication. Registered UNIQUE partners with username and password can use special options which are only offered in the password protected area (e.g. calendar for appointments and meetings, forum for information exchange, Wiki function to post and to deal with articles, mailing lists for reaching special mailing groups).

The present version of the website must be seen as the basis for a continuous process because frequent modifications, news and updates on the part of all project partners will make the website more and more informative and give interested people reasons for coming back.

3.2.6 Press releases, newsletters

Title	Publication details (journal, newspaper, etc.)	Partners involved
Official Press release of UNIQUE	It is intended to publish an official press release as a formal announcement to the national or specialised/technical press in order to present a short overview of the UNIQUE project to the public.	**TEC**

Table 6: Summary of press releases, newsletters

3.2.7 Other

The UNIQUE logo

In order to improve the visibility of the UNIQUE project a logo was designed. The logo shows the name of the project and a specific symbol at the end of the name which stands for the uniqueness and identification of a product which the UNIQUE project targeted. The logo is used in all the dissemination tools, from the internal communication and reporting templates to external communication tools like website, fact sheet and folder. This graphical identity will help to consistently communicate and disseminate the project in external project communications. The reporting templates will also help to save time and effort for the members of the consortium,

Figure 2: UNIQUE logo

since no further design work will be necessary. Templates for documents and representations have been produced and made downloadable for all project members. The templates are important to ensure a united impression and consistent visual appearance of the project.

The UNIQUE Leaflet

The official UNIQUE leaflet is a four sided A4 flyer and includes important project related information. On the one hand it can be circulated in printed form, e.g. it can be handed out at conferences or other events; on the other hand also an electronic version (e.g. PDF file) can be circulated.
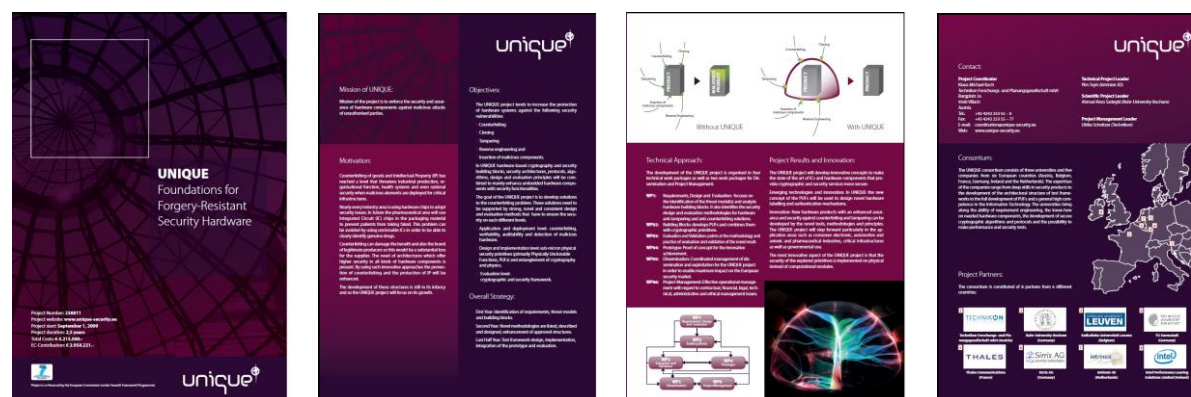
Figure 3: UNIQUE leaflet

The planned UNIQUE Video

A **project promotion video will be produced for dissemination purposes**. It will involve a 3-5 minute clip of the UNIQUE project which will be uploaded to the official project website as well as onto YouTube.

The video is intended for technically oriented people and as **a general awareness tool**. It will provide a general description of the project work and its benefits by introducing the general project idea as well as the workplan strategy and the PUF Technology. In addition to these specific messages the video conveys the ground breaking achievement as well as the implication of the UNIQUE project for the future and the significance of the project for the economy.

The video should use modern technology and techniques to present UNIQUE in a **professional and attractive manner**.

The video's main audiences are expected to be:
- **Researchers and Technicians**, engaging with the PUF technology/UNIQUE project for the first time
- **Non technical people**, who are interested in this project
- **Journalists,** who are potentially an important means of reaching our more immediate target audiences like researchers, politicians and decision-makers
- **Students**

In addition to the presence of the video on the UNIQUE website the **video will be actively played by the project partners at international conferences and events**. As far as possible, showing of the video to seated audiences – e.g. as part of a conference programme, or during a meeting – is being encouraged in preference to simply playing the video on a screen as a "sideshow". In this way, we hope to maximise the impact of the video as far as possible, and ensure it is seen by the largest possible audience.

Concerning the **video production process** we are already considering several offers of potential organizations, who are specialised in the production of video and new media communications for science and technology organisations. After conducting preliminary meetings with several potential suppliers, we hope to get three proposals; on this basis the UNIQUE consortium will conclude a contract with one supplier. The final video should be available this summer.

The production of a promotional video is a **substantial project in terms of both cost and time**. This particular activities should result in a video which should be very well-received by the audience and which will justify the limited resources which were committed to it. We are confident that the video will make a significant positive impact in terms of awareness of UNIQUE.

4 Cooperation with external organisations

In addition to the various dissemination activities reported above, the UNIQUE consortium is in close cooperation with external organisations. The involved partners and their existing and planned activities are listed below.

Actual/ planned date	Type, content of the cooperation	Cooperation partners	Countries addressed (international/ national – which country)	UNIQUE partners involved
TBA	Presentation of the UNIQUE project	Relevant working groups (TBA)	International/national	TBA
TBA	Initial cooperation with national agencies like the German Federal Office for Information Security (BSI) in order to communicate the results with relevant stakeholders in governmental institutions.	German Federal Office for Information Security (BSI)	Germany	SIRRIX

Table 7: Cooperation with external organisations

5 Participation in projects

5.1 Participation in international projects

In order to promote knowledge sharing and gathering among the Consortium partners and various organisations within a similar research sphere, project partners are participating in several other complementary projects, which are listed below.

Project name	Topic and description of the project	Project partners
ICT FP7		
CACE Ref.No. 216499 (2008), http://www.cace-project.eu **TECOM** Ref.No. 216888 (2008), http://www.tecom-project.eu	Development of a toolbox that supports the production of a high quality cryptographic software Adoption of a systematic approach to the development of trusted embedded systems	TEC is CO of eight FP7 projects and so there is a great potential for mutual benefit in terms of project management
ECRYPT-II	European Network of Excellence in Cryptology - Phase II	KULEUVEN Belgium, RUB Germany, ENS France, Royal Holloway UK, University of Salerno Italy, University of

		Bristol UK, France Telecom France, IBM Research Switzerland, TUE the Netherlands, Graz UT Austria, EPFL Switzerland
Other Program lines		
Secure Memories and Applications Related Technologies (SMART) (ENIAC)	The mission of the SMART project is to define and develop new HW and firmware technologies for the secure storage and communication of large and multi-form data. The project will address four challenges of smart secure devices: 1) new generation Non-Volatile Memories (phase-change memory, PCM) of high capacity and secure architecture, 2) related crypto engines with configurable firmware and 3) resistance to state of the art attacks The project is expected to start early 2010.	Numonyx (IT) STMicroelectronics (FR, IT) Thales (FR) GEMALTO (FR) TELETEL (GR) Integrated Systems Development (GR) Aristotle University (GR) CNES (FR) Università di Milano Bicocca (IT) MultiCert (PT) Universidade do Minho (PT) Fraunhofer IIS-EAS (DE) Anvo-Systems GmbH (DE)

Table 8: Participation in other EC projects

5.2 Participation in national projects

In addition to the projects that are run on the European level, the partners are also active in national projects.

Project name	Topic and description of the project	Project partners
France		
Plate-formes de Confiance (PFC) (Trusted Platforms)	Development of trusted computing demonstrators based on trusted software and targeting critical infrastructure computers. In this project, Thales contribution was mainly targeted on segregated hardware. The project ended on 31.12.2009.	Industrials: Alcatel Lucent, Gemalto, Bertin, Bull, EADS, SAGEM, Thales, Trusted Logic… Labs: CEA/LIST, GET/INT, LIP6, ENS Cachan, INRIA

Table 9: Participation in national projects

6 List of Abbreviations

CO	Coordinator
EC	European Commission
FET	Future and Emerging Technologies
FET Open	Future and Emerging Technologies Open Scheme - a roots-up approach for exploring promising visionary ideas that can contribute to challenges of long term importance for Europe
ICT	Information and Communication Technologies
IID	Intrinsic ID B.V.
INTEL	Intel Performance learning solutions limited
IPR	Intellectual Property Rights
KULEUVEN	Katholieke Universiteit Leuven
RUB	Ruhr-University-Bochum
SIRRIX	Sirrix Aktiengesellschaft
STREP	Small or medium-scale focused research project
TBA	To be announced
TCF	Thales Communications SA
TEC	Technikon mbH Forschungs- und Planungsgesellschaft mbH
TUD	Technische Universität Darmstadt
UNIQUE	Foundations for Forgery-Resistant Security Hardware
WP	Work package