



## CACE

### Computer Aided Cryptography Engineering

Project number: 216499

FP7-ICT-2007-1

#### D6.2

#### Project dissemination plan

Due date of deliverable: 30. April 2008

Actual submission date: 02. June 2008

WP contributing to the deliverable: WP6

Start date of project: 1. January 2008

Duration: 3 years

Coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a, 9500 Villach, Austria

Phone: +43 4242 233 550

Email: [coordination@cace-project.eu](mailto:coordination@cace-project.eu)

[www.cace-project.eu](http://www.cace-project.eu)

Revision 1.0

Project co-funded by the European Commission within the 7th Framework Programme		
Dissemination Level		
<b>PU</b>	Public	<b>X</b>
<b>PP</b>	Restricted to other programme participants (including the Commission services)	
<b>RE</b>	Restricted to a group specified by the consortium (including the Commission services)	
<b>CO</b>	Confidential, only for members of the consortium (including the Commission services)	



## **D6.2**

### **Project dissemination plan**

#### **Editor**

Sandra Tscheliesnig (TEC), Angelika Holzweber (TEC)

#### **Contributors**

Input from all CACE partners

02. June 2008

Revision 1.0

## **Abstract**

The following document gives an overview of the dissemination activities planned for the CACE project. It describes the dissemination strategy as well as the actual events and activities carried out by the partners.

# Contents

- 1 Introduction ..... 1
- 2 Dissemination strategy ..... 1
- 3 Planned dissemination of knowledge ..... 2
  - 3.1 Contribution of each partner ..... 2
  - 3.2 Description of planned dissemination activities..... 5
    - 3.2.1 Active participation in conferences and workshops..... 5
    - 3.2.2 Passive participation in conferences and workshops ..... 7
    - 3.2.3 Scientific articles and publications..... 9
    - 3.2.4 Courses, talks organised ..... 9
    - 3.2.5 Web-sites ..... 10
    - 3.2.6 Press releases, newsletters..... 10
  - 3.3 Contributions to standards..... 10
- 4 Cooperation with external organisations..... 11
- 5 Participation in projects..... 12
  - 5.1 Participation in international projects ..... 12
  - 5.2 Participation in national projects..... 17
- 6 List of Abbreviations..... 19

## List of Tables

Table 1: Exploitation plans per partner .....	5
Table 2: Summary of actively participated conferences and workshops .....	7
Table 3: Summary of workshops .....	9
Table 4: Summary of scientific articles, publications, presentations .....	9
Table 5: Summary of courses organised .....	10
Table 6: Summary of relevant web-sites .....	10
Table 7: Summary of press releases, newsletters .....	10
Table 8: Cooperation with external organisations.....	12
Table 9: Overview of FP6 and FP7 projects of CACE partners .....	17
Table 10: Participation in national projects.....	18

## 1 Introduction

The dissemination plan of the CACE 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. However, as the first step the dissemination strategy will be described.

## 2 Dissemination strategy

The dissemination strategy of the CACE project includes scientific publications, publicly accessible web page with download areas for software and technical reports, and several workshops and the cooperation with industry.

To obtain a wider attention, publications in major cryptographic and information security conferences are planned. Furthermore there will be also publications in more specialised workshops on implementation, multiparty computation, zero knowledge proofs and software engineering. The senior researchers in CACE are well-established scientist who are invited as keynote speakers to many conferences, which will help to disseminate the research and its results.

The scientific results are interesting to cryptology and software engineering at large. The subject of CACE has been already recognised by several researchers worldwide and its potential by IT security industry, e.g., smartcard industry. Furthermore through the close cooperation with industrial partners inside and outside the consortium, the CACE project and its results and benefits will be introduced to the relevant industry as well as to standardisation bodies.

Several of the deliverables of the CACE project are in the form of software libraries, which clearly are important for other parts of the project and are therefore of direct use to the partners. The libraries of the CACE consortium will also be of a great worldwide value and interest to software developers and implementers of cryptography. The efforts start from several projects like *qhasm* and *CAO*, which are freely available in the public domain or as open source. Once published these libraries received significant attention demonstrating that there is clear interest in easier and more reliable ways of producing secure and fast software. The libraries produced by WP1 (CAO) and WP2 (NaCl) will be available for download and use.

The first workshop on compilers in cryptography SPEED – Software Performance enhancement of Encryption and Decryption was held already before the project start in June 2007 in Amsterdam. Three members of the CACE consortium were in the program committee and one was acting as an invited lecture. As this workshop was initiated by Tanja Lange (TUE) the CACE consortium plans to organise the SPEED2 as part of the CACE project, extending the scope to also cover compilers for protocols.

Furthermore TEC organised the Trust2008 conference in Villach (Austria) on trusted and secure computing. The world's leading experts in the field of secure computing participated and contributed with their results of the latest research to this event. It is foreseen to create

a series of Trust conferences and within this approach different projects in the field of trusted and secure computing will be integrated. This opens the way for the CACE consortium to disseminate their results to a specific audience.

The general approach of the CACE project is to provide as much as possible a full and non-discriminatory access to all knowledge produced in the project according to the project goal of producing the first set of domain-specific languages and tools for the development of cryptographic software

### **3 Planned dissemination of knowledge**

During the CACE project life-time, the project partners will promote and encourage research on the CACE topic, targeting European and international companies and research centres, as well as create interest in the general public.

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

Exploitation of the project results is clearly defined in the objectives of CACE. As the project consortium and the Advisory Board consists of the major European players in both science and industry the usage of the results will be exploited in both the science and commercial sector. The main exploitation will be through each partner's own organisation.

The first classification is public activities, which are not directed towards commercial revenue, but rather focusing on the general public. The second classification is business activities, which have a clear commercial motivation.

The main aim of the public dissemination activities is to bring the research results of the project back to the scientific world and to channel them to other research and development projects in the mobile communications domain allowing for cross-fertilisation. The CACE supported libraries will be published to the general public. This will, as already mentioned, improve the future development of secure and fast software. An important aspect of public exploitation is the usage and contribution to international standards. CACE aims to contribute to different standardisation groups via the project members, who are already participating in different standardisation efforts. The specific connections of CACE to standardisation will be detailed in a separate section later on.

The second but not less important part of the dissemination is constituted the business activities. The commercial dissemination of the project results will mainly take place through the industrial partners in the consortium. The result of the CACE project will be a toolbox that will support the specific domain of cryptographic software engineering. Designing and manufacturing high-quality products will improve Europe's competitiveness and generate qualified jobs within the European territory.

The planned business dissemination activities of each partner are detailed below.

#### ***3.1 Contribution of each partner***

In the following table the plans of each consortium member will be described in more detail the planned exploitation activities of each project partner.

Short name	Exploitation plans
<b>Industry</b>	
<b>Nokia</b>	Nokia intends to gain two exploitable results from participating in the CACE project: (1) enhancing competence of NRC project participants in cryptographic engineering (2) using the tools produced by CACE themselves. Both of these will be used in strengthening/revising the existing Nokia cryptography library implementation, as well as in adding new features in the future. For example, the current implementation has some carefully hand-coded defences against side channel attacks. NOKIA intends to use the knowledge and tools gained from CACE to improve and extend these defences.
<b>Universities</b>	
<b>RUB</b>	RUB started the IT technology transfer and exploitation many years ago through the umbrella Public Private Partnership "eurobits" (European Centre for IT Security) located at RUB. It is the largest centre for IT security of its kind in Europe comprised of two parts. The first part is an internationally renowned research institutes Horst Görtz Institute (HGI) for IT Security, which consist of 6 chairs from the fields Electrical Engineering, Information Sciences, Mathematics, Economics, and Law with 50 researchers. The main focus of HGI is interdisciplinary research in IT security where different areas of expertise: technical, economic, legal and social scientific are combined. HGI also does consulting work, and cooperates with IT security related enterprises. The second part of eurobits consists of several highly specialised SMEs, all of which are active in the field of IT security. The main goal of eurobits is technology transfer to exploit scientific results in cryptography and information security in practice through close and active cooperation as well as joint industrial projects. Eurobits offers a whole spectrum of IT security: from applied research to product development, and from tailored in-house training courses to support integrating new companies under eurobits umbrella. Eurobits also has Europe's leading offerings of academic degree programs and continuing education courses in the area of IT security. The results of CACE will be input to eurobits as a multiplier and made available to a large number of research and industrial partners of eurobits. This allows in particular many SMEs to benefit from the tools and methodologies developed within CACE.
<b>UNIV BRIS</b>	In line with other UK universities, UNIVBRIS has recently invested significant effort in improving industrial exploitation of research results. Specifically, this has resulted in two relevant spin-off companies, Identum and XMOS, to whom cryptographic software engineering is the core business. Beyond facilitating future UNIVBRIS research efforts within the university, we would hope to investigate the exploitation of results from CACE through these spin-off companies.
<b>TUE</b>	The NaCl library will be useful to researchers implementing cryptographic software for real life applications. Like qasm and CAO it will be placed in the public domain. It will actively improve the quality in security and speed of cryptographic software produced in Europe and elsewhere.
<b>MINHO</b>	For MINHO University, the CACE project will have a high impact. MINHO University is a technical consultant for government bodies and national companies in the area of software and information systems security. The outputs of the CACE project are going to address some of the problems that they are confronted with in the development of software for areas such as electronic voting, electronic identification, time stamping, and other aspects of e-Government; electronic invoices and receipts, and e-Commerce in general; information management in health services, etc. On the academic side, the CACE project provides an opportunity to consolidate international collaborations in the area of cryptography, and also offers a novel practical case study for the formal-methods and machine-assisted verification technology that is the focus of MINHO's research (and teaching).
<b>BFH</b>	BFH research activities are strongly focused on applied R&D and technology transfer in collaboration with industry partners, whereas IT security engineering is one of the key areas. The participation in a high-profile applied research project such as CACE will have a substantial impact for BFH and it's industry partners. In fact, the results and the tools developed in the fields of crypto engineering and software verification within CACE will

	<p>further strengthen and widen the security engineering R&amp;D portfolio of BFH. Moreover, through the close collaboration of BFH research with industry partners, they expect to disseminate the project results within industry. On the academic side, the CACE project will allow BFH to consolidate and further expand its international network, and contribute to novel research results in the field. Finally, BFH is committed to incorporate results from its collaboration into teaching activities.</p>
<b>AU</b>	<p>Aarhus University is the Coordinator of a Danish Research project SIMAP (Secure Information Management and Processing) whose activities are closely related to those that will be carried out in CACE on multiparty computation. This year, the first prototype of this project will be deployed, and will be used to do a nation-wide auction on contracts for producing sugar beets. While this is an application that will be developed for this particular case, there is clearly a potential for much more general usage of the ideas in many other domains. The results and tools developed in CACE will enable AU to easily develop a range of much more general applications, thereby demonstrating the general potential of the multiparty computation. This will be a necessary step for the researchers to gain important experience, but also necessary for having these ideas and methods enter the commercial domain.</p>
<b>HU</b>	<p>The University of Haifa has an active research program in cryptography and its applications, with an emphasis on secure computation. It is also actively looking for industrial partners for this research, and for commercial applications. The tools developed within CACE are expected to be fundamental tools for further research activities, by enabling more streamlined development of cryptographic algorithms, and by improving their efficiency and stability.</p>
<b>TKK</b>	<p>In Finland, the units performing cryptologic research are relatively small and usually special skills are limited to one expert. Therefore collaboration at national and European level is necessary to achieve new research results. The results of the CACE project will be exploited in collaboration with NOKIA to create more secure and efficient implementation of cryptographic algorithms.</p>
<b>SMEs</b>	
<b>TEC</b>	<p>The project results will be exploited by using TEC's "Trusted knowledge suite" to run the IT infrastructure and to improve the features and the handling of the tools. The experience gained will increase TEC's capability to run and manage national and international RTD projects. As an SME, the reputation gained from the project will positively influence future acquisition activities.</p> <p>Requirement engineering: TEC industrial services on requirement engineering will profit from the expertise gained in the collaboration with our scientific and industrial partners on development of UML 2.0 based use cases and technology roadmap. This will also positively influence our activities in supporting start-up companies.</p>
<b>SRX</b>	<p>First of all, SRX strongly believes that the developed tools will not only enhance the security properties of commercial of the shelf (COTS) products significantly, but also will increase the efficiency of the development process. I.e., it will lower the costs for crypto related soft- and hardware developments in a clear way. This assessment is due to a long experience with SRX customers and a deep knowledge of the development processes in the security industry. Moreover, it will push the usage of COTS products in more sensitive areas, also saving time and resources. As a whole, providing these tools to the European security industry will enhance the competitiveness of the European ICT industries in a lasting way. In detail, SRX will exploit the CACE results in two different ways: Firstly, SRX intends to transfer the CACE results into a ready-to-use and cryptographic library suite. This ensures that CACE results are bundled and the developed tools are accessible and utilisable by the European security industry. Moreover, commercialisation of the result will ensure a long-term maintenance and further development of these tools. Secondly, SRX will use the results in its own product development as well as to enhance other correlated projects. Hence, SRX is developing products for sensitive and classified environments, including national Governments and the NATO, increasing the efficiency of these products will strengthen the competitiveness of European solutions in these areas.</p>

<b>AI</b>	AI is a company that is jointly owned by the university and some 40 companies in the Danish and International IT industry. Its purpose is to deliver research-based technological service to companies in the IT industry, and to facilitate matchmaking between companies and researchers in the field. AI therefore has a widespread network of contacts to large and small companies in the ICT business and is ideally placed to disseminate the results and further the process of having them be used in industry. More concretely, AI has established a centre for IT security, where we have direct contact with a range of companies that are interested in security and whose products use cryptography in various ways. These contacts will be used to further exploitation of the results.
-----------	--

**Table 1: Exploitation plans per partner**

### 3.2 Description of planned dissemination activities

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

#### 3.2.1 Active participation in conferences and workshops

Active participation in conferences and workshops is defined as: The participation in conferences and workshops is considered active if the CACE project partner is in the role of a speaker, presenter or moderator.

Full name of the conference	Date	Location	Type and size of the audience	Topic and goal of the event	Relevance to CACE (Partners involved)
Financial Cryptography and Data Security 2008, <a href="http://fc08.ifca.ai/">http://fc08.ifca.ai/</a>	28.01-31.01.2008	Cozumel, Mexico	International, approx. 80	Information assurance in commerce, Financial cryptography	Speaker (TUE), Poster and TPC member (Nokia), Speaker (RUB)
BSF/DIMACS/DyDAn Workshop on Data Privacy, <a href="http://dimacs.rutgers.edu/Workshops/DataPrivacy/">http://dimacs.rutgers.edu/Workshops/DataPrivacy/</a>	04.02 – 07.02.2008	Piscataway, NJ USA	International, approx. 100	Workshop on data privacy	Organiser (HU)
Trust2008, <a href="http://www.trust2008.eu/">http://www.trust2008.eu/</a>	11.03 – 14.03.2008	Villach, Austria	International, approx. 160	Trusted computing	Discussions on the project topic, cooperation with other relevant EC projects. (TEC)
Open Space for European Research, <a href="http://www.ffg.at/content.php?cid=26&amp;sid=176">http://www.ffg.at/content.php?cid=26&amp;sid=176</a>	02.04.2008	Vienna, Austria	National, approx. 400	Discussion of the topics in workshops; Distinction "Austrian Champions in European Research"	Participation in workshops as speaker and distinction for being coordinator of CACE (TEC)
Sicherheit 2008, <a href="http://www.sicherheit2008.de/content">http://www.sicherheit2008.de/content</a>	02.04. – 04.04.2008	Saarbrücken, Germany	International, approx. 130	IT-security, safety	General chair, program chair, contributor,

<a href="#">nt/pages/sicherheit2008.htm</a>					Conference organiser, discussion on project topic (SRX)
RSA Conference 2008, <a href="http://www.rsaconference.com/2008/US/home.aspx">http://www.rsaconference.com/2008/US/home.aspx</a>	07. 04. – 11.04.2008	San Francisco , CA, USA	International, about 1000	General IT-Security, plus special crypto track	Participant and demonstration (Nokia), Present papers, Contacts and discussions with relevant scientific collaborators (AU), Participation (SRX)
EuroCrypt 2008 conference, <a href="http://www.iacr.org/conferences/eurocrypt2008/">http://www.iacr.org/conferences/eurocrypt2008/</a>	13.04-17.04.2008	Istanbul, Turkey	International, approx. 400	Cryptography	Organiser (RUB), Program Chair (UNIVBRIS), Presenting papers, contacts and discussions with relevant scientific collaborators (AU)
ICT-MobileSummit 2008, <a href="http://www.ict-mobilesummit.eu/2008/">http://www.ict-mobilesummit.eu/2008/</a>	10.06. - 12.06.2008	Stockholm, Sweden	International approx. 600	Identify opportunities for international research collaboration	Member of Technical Programme Committee (TEC)
Africacrypt, <a href="http://www.africacrypt.org/">http://www.africacrypt.org/</a>	11.06-14.06.2008	Casablanca, Morocco	International, approx. 80	Cryptography	Speaker (TUE)
EuroPKI 08, <a href="http://www.item.ntnu.no/europk08/">http://www.item.ntnu.no/europk08/</a>	16.06. - 17.06.2008	Trondheim, Norway	International, approx. 75	Research aspects of Public Key Applications, Services and Infrastructures	Paper presentation on fast point decomposition. WP1 and WP2 can make use of high speed ECC. (TKK)
ICALP 2008, <a href="http://www.ru.is/icalp08/">http://www.ru.is/icalp08/</a>	06.07-13.07.2008	Reykjavik , Iceland	International, approx. 600	Automata, Languages and Programming (RUB), Theoretical Computer science, plus special track on cryptography (AU)	Program chair of cryptography track. Contacts and discussions with relevant scientific collaborators (AU), Speaker (RUB)
SAM 08, <a href="http://www.world-academy-of-science.org/worldcomp08/ws/conferences/sam08">http://www.world-academy-of-science.org/worldcomp08/ws/conferences/sam08</a>	14.07. – 17.07.2008	Las Vegas, USA	International, approx. 100	Network security and management	Paper presentation on high speed ECC on Koblitz curves, again useful to WP1 and WP2. (TKK)
CHES 2008, <a href="http://www.chesworkshop.org/">http://www.chesworkshop.org/</a>	10.08.-13.08.2008	Washington, USA	International, approx 200	Hardware, implementation, cryptographic hardware and security for embedded systems	Speaker (TUE), Organiser (RUB)
ISSE 2008, <a href="http://www.isse.eu">http://www.isse.eu</a>	07.10 – 09.10. 2008	Madrid, Spain	International		(SRX)

<a href="#">.com/</a>					
ECC 2008, <a href="http://www.hyperelliptic.org/tanja/conf/ECC08">www.hyperelliptic.org/tanja/conf/ECC08</a>	22.09.- 24.09.2008	Utrecht, NL	International, approx 150	Elliptic curves & implementation	Organiser (TUE)
ACM-DRM, <a href="http://www.ece.unm.edu/DRM2008/">http://www.ece.unm.edu/DRM2008/</a>	27.10.2008	Alexan- dria, Virginia, USA	International, approx. 150	Digital Rights Management	Organiser (RUB)
STC 2008, <a href="http://www.sisa.samsung.com/innovation/stc08/">http://www.sisa.samsung.com/innovation/stc08/</a>	31.10.2008	Fairfax, VA, USA	International	Trusted Computing	(SRX), TPC member (Nokia)
MILCOM 2008, <a href="http://www.milcom.org/">http://www.milcom.org/</a>	17.11. – 19.11.2008	San Diego, CA, USA	International	Secure Communication, esp. in military domain	(SRX)
ICT 2008 conference, <a href="http://ec.europa.eu/information_society/events/ict/2008/index_en.htm">http://ec.europa.eu/information_society/events/ict/2008/index_en.htm</a>	25.11. - 27.11.2008	Lyon, France	International	Identify opportunities for international research collaboration	Discussion and identify collaborations on project relevant topics. (TEC)
TRUST 2009, (web site non yet available)	N/A	N/A	International	Trusted computing	Discussions on the project topic, cooperation with other relevant EC projects

**Table 2: Summary of actively participated conferences and workshops**

### 3.2.2 Passive participation in conferences and workshops

Passive participation is defined as: The participation in conferences and workshops as audience with no active role.

Full name of the conference	Date	Location	Type and size of the audience	Topic and goal of the event	Relevance to CACE (Partners involved)
BCRYPT ECC Workshop, <a href="https://www.cosic.es.at.kuleuven.be/bcrypt/announcements.php-news_4">https://www.cosic.es.at.kuleuven.be/bcrypt/announcements.php-news_4</a>	20.03.2008	Leuven, Belgium	International, 30	Lectures on theoretical aspects of elliptic curves and practical aspects of curve-based cryptography.	Many topics of interest to WP1 covered, including side-channel security with respect to elliptic curves. Implementation aspects, hardware, software, curve-specific. (TKK)
EUROCRYPT 2008, <a href="http://www.eurocrypt2008.org/">http://www.eurocrypt2008.org/</a>	13.04- 17.04.2008	Istanbul, Turkey	International, approx. 200	Cryptology	Short meeting of WP1, 2, and 4 (TUE, UNIVBRIS, AU); Discussions on the project topic with cryptography experts (most

					academic partners will be represented) (MINHO).
Security Hardware in Theory and Practice – A Marriage of Convenience, <a href="http://www.dagstuhl.de/de/programm/kalender/evhp/?semnr=2008253">http://www.dagstuhl.de/de/programm/kalender/evhp/?semnr=2008253</a>	18.06. - 20.06.2008	Schloss Dagstuhl, Germany	International, 20-30 upon invitation only	Building secure hardware	Discussion of crypto implementations in HW and embedded systems. (BFH)
Monte-Verita ISIS Conference, <a href="http://isis.epfl.ch/MV">http://isis.epfl.ch/MV</a>	6.07 – 11.07.2008	Monte Verita, Switzerland	International, upon invitation only	1 - Economics of IS, chaired by Jean Camp 2 - Human factors, chaired by Bruce Schneier 3 - Legal and regulatory issues, chaired by Bertil Cottier 4 - IS risk management, chaired by Tim Voss 5 - Technical issues, chaired by Kevin McCurley	Positioning and awareness of computer aided crypto in the international security research community. (BFH)
CRYPTO 2008, <a href="http://www.iacr.org/conferences/crypto2008/index.html">http://www.iacr.org/conferences/crypto2008/index.html</a>	17.08-21.08.2008	Santa Barbara, USA	International, approx. 200	Covers all aspects of cryptology	Meetings with other WP's and other cryptographers (TUE); Audience, knowledge relevant for all WPs, advancement of cryptographic knowledge (RUB)
Pairing'08, <a href="http://www.pairing-conference.org/">http://www.pairing-conference.org/</a>	01.09-03.09.2008	London, UK	International, approx 80	Pairings	Meetings with other WP's and other cryptographers (TUE)
ESORICS 2008, <a href="http://www.isac.uma.es/esorics08/">http://www.isac.uma.es/esorics08/</a>	06.10-08.10.2008	Malaga, Spain	International, approx. 170	All theoretical and practical aspects of information security	Audience, knowledge relevant for all WPs, advancement of cryptographic knowledge (RUB)
ACM CSS 2008, <a href="http://www.sigsac.org/ccs/CCS2008/">http://www.sigsac.org/ccs/CCS2008/</a>	27.10.-31.10.2008	Alexandria, USA	International, approx. 170	All theoretical and practical aspects of information security	Audience, knowledge relevant for all WPs, advancement of cryptographic knowledge (RUB)
ASIACRYPT 2008, <a href="http://www.ics.mq.edu.au/conferences/asiacrypt2008/">http://www.ics.mq.edu.au/conferences/asiacrypt2008/</a>	07.12-11.12.2008	Melbourne, Australia	International, approx. 200	Covers all aspects of cryptology	Audience, knowledge relevant for all WPs, advancement of

					cryptographic knowledge (RUB); Meetings with other WP's and other cryptographers (TUE)
--	--	--	--	--	--

**Table 3: Summary of workshops**

### 3.2.3 Scientific articles and publications

Author(s), Date	Title	Journal title, volume, issue, page numbers	Type	Topic of the article/publication/presentation, connection to CACE (Partners involved)
U. Kühn, Andrei Pyshkin, E. Tews, R.-P. Weinmann	Variants of Bleichenbacher's Low-Exponent Attack on PKCS#1 RSA Signatures	Proc. Sicherheit 2008	International	Cryptanalysis of implementation flaws in RSA signature verification (SRX)
P. Backs, N. Pohlmann	Einfluss von Sicherungsmaßnahmen auf die Übertragungsqualität von VoIP	Proc. Sicherheit 2008	International (mostly german-speaking)	Influence of network-layer cryptographic means on quality of VoIP (SRX)
Vladimir Kolesnikov, Thomas Schneider	Improved Garbled Circuit: Free XOR Gates and Applications.	35th International Colloquium on Automata, Languages and Programming (ICALP 2008), 6-13 July, Reykjavik, Iceland	International	Foundations of Secure Multiparty Computation (RUB)
Vladimir Kolesnikov, Thomas Schneider	A Practical Universal Circuit Construction and Secure Evaluation of Private Functions	Financial Cryptography and Data Security (FC 2008), 28-31 January, Cozumel, Mexico	International	Foundations of Secure Multiparty Computation (RUB)
Frederik Armknecht, Alberto Escalante, Hans Löhr, Mark Manulis, Ahmad-Reza Sadeghi	Secure Multi-Coupons for Federated Environments: Privacy-Preserving and Customer-Friendly.	The 4th Information Security Practice and Experience Conference (ISPEC 2008), 21-23 April 2008, Sydney, Australia	International	Practical application of Proof of Knowledge (RUB)

**Table 4: Summary of scientific articles, publications, presentations**

### 3.2.4 Courses, talks organised

Partners involved	Date, location	Course title, content	Type and size of the audience
MINHO	12. 12. 2007, Porto, Portugal	Computer Aided Cryptography Engineering, Thematic Network on Information Security	National, 20 people

RUB	Ongoing activity, Bochum, Germany	"Zero-Knowledge Protocols", Seminar at the Chair for System Security	National, 6
HU	25. 2. 2008, Ramat Gan, Israel	Security and pseudo-random number generators	National (12 <sup>th</sup> Annual Conference of the Israeli Internet Society) Audience: ~50 in this session
TKK	19. 03. 2008, Leuven, Belgium	COSIC seminar, Algorithms for Koblitz Curve Cryptography	International, 10
RUB	10. 04. 2008, Bochum, Germany	Jesse Walker, Intel Corp., "Distributed Trust", HGI-Seminar	International, Approx. 40
RUB	11 .04. 2008, Bochum, Germany	Giovanni di Crescenzo, Telcordia Technologies, "Perfectly Secure Password Protocols in the Bounded Retrieval Model", HGI-Seminar	International, Approx. 40

**Table 5: Summary of courses organised**

### 3.2.5 Web-sites

Web-site	Description of the main CACE related information	Partners involved
<a href="http://www.cace-project.eu">http://www.cace-project.eu</a>	The official web-site of the CACE project	TEC, all
<a href="http://www.cs.bris.ac.uk/news">http://www.cs.bris.ac.uk/news</a>	Notification of CACE kick-off	UNIVBRIS
<a href="http://www.daimi.au.dk">http://www.daimi.au.dk</a>	Home page of the computer science department in Aarhus. Announced here the start of the project under news section, also permanent link on the crypto-groups's homepage to the project	AU
<a href="http://www.trust.rub.de">http://www.trust.rub.de</a>	Web-site of the Chair for System-Security	RUB
<a href="http://www.technikon.com">http://www.technikon.com</a>	Short project description and link to the official homepage	TEC

**Table 6: Summary of relevant web-sites**

### 3.2.6 Press releases, newsletters

Title	Publication details	Partners involved
HGI-Newsletter	Newsletter of the Horst Görtz Institute for IT Security	RUB
Official Press release of CACE	Official Press release to present a short overview of the CACE project to the public	TEC
CACE Leaflet	Official CACE leaflet including important project related information	TEC

**Table 7: Summary of press releases, newsletters**

## 3.3 Contributions to standards

One of the goals of the CACE project is to widely disseminate the results at different levels and to different communities in order to spread the culture and technologies in the field of design. One target for such dissemination is a set of standardisation working groups whose

activities are or can be put in relation with the knowledge developed in CACE. The activities in the field of standardisation will be performed at different levels as appropriate: setting up working groups specifically targeted by the CACE topics, creation of formal liaisons between already existing bodies and the CACE consortium, direct participation in existing bodies, or by interaction with members of existing bodies.

Influencing standardisation activities will be achieved through the CACE project partners. In fact many of them have strong and active links with relevant specification and standardisation bodies such as:

- IEEE [TEC, UNIVBRIS via the P-1363 group],
- ETSI telecommunication standard [UNIVBRIS via ECRYPT project; Nokia via the ETSI SAGE expert group],
- SECG elliptic curve standards [UNIVBRIS],
- CEN (Cryptography and Machine Readable Cards Group) [RUB via industrial contacts],
- ISO/IEC JTC 1/SC 27 "IT Security Techniques" [RUB via industrial contacts],
- Teletrust standardisation body [SRX – leading standardisation efforts for establishing general specification for Trusted Computing Systems]
- Trusted Computing Group (TCG) [Nokia, TEC, RUB, SRX],
- Third Generation Partnership Project (3GPP) [Nokia],
- Internet Engineering Task Force (IETF) [Nokia], and
- Bluetooth Special Interest Group [Nokia]

These and other relevant standardisation bodies can benefit from CACE results either directly or indirectly.

CACE will focus on the enhancement in the following areas:

- architectural aspects
- security aware languages
- compilers for designing security protocols
- component interfaces and libraries
- evaluation and rating criteria
- testing methodologies

Key areas of standardisation activities are:

- cryptographic implementations at different systems layers (close to hardware layer, protocol layer)
- interaction with the standardisation bodies (e.g. through the Public Private Partnership between eurobits and RUB)
- propose results from CACE as draft standards to corresponding technical communities

## 4 Cooperation with external organisations

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

Actual/ planned dated	Type, content of the cooperation	Cooperation partners	Countries addressed	CACE partners involved
Actual	Ongoing research cooperation	IBM Zurich Research LAB	International – Switzerland	SRX

Actual	Ongoing research cooperation	KU Leuven	International – Belgium	SRX
Ongoing activity	Research, Zero-Knowledge Protocols	Claire Vishik, Intel	International – UK	RUB, ALL (as Ms. Vishik is a member of the Advisory Board)
Ongoing activity, multiple events per year	Research, Zero-Knowledge Compiler	Jan Camenisch, IBM Research	International – Switzerland	RUB, BFH, ALL (as Mr. Camenisch is a member of the Advisory Board)
Ongoing activity	Research, Homomorphic Cryptosystems	Pim Tuyls, Philips Research	International – Netherlands	RUB, ALL (as Mr. Tuyls is a member of the Advisory Board)
Ongoing activity	Research, Zero-Knowledge Protocols	Liqun Chen, HP Research	International - UK	RUB, BFH, UNIVBRIS, ALL (as Ms. Chen is a member of the Advisory Board)
Until April 2009	Research project SIMAP (Secure Information Management and Processing)	Danisco, IBM	Denmark	AU

**Table 8: Cooperation with external organisations**

## 5 Participation in projects

### 5.1 Participation in international projects

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

Project name	Topic and description of the project	Project partners involved
<b>ICT FP7</b>		
<b>TECOM</b> , Ref.No 216888 (2008), <a href="http://www.tecom-project.eu">http://www.tecom-project.eu</a>	<p>Trusted Computing (TC) is an established technology for the verification and implementation of integrity and security in personal computers (PCs). PCs have large resources of available code space, specific bus interfaces and computing power. Embedded computing platforms, for which such resources are not available, nevertheless have similar trust and security problems as the PCs. The cause of this lies in the increasing complexity and therefore instability of platforms' operating systems and applications; furthermore, their connection to the Internet is exposing them to additional security threats and attacks.</p> <p>As there are many more embedded computing platforms than PCs in the production and in the field, it has become necessary to adapt the current TC security standard also to embedded platforms.</p> <p>The project will adopt a systematic approach to the development of trusted embedded systems, consisting of hardware platforms with integrated trust components.</p> <p>The results and experience gained from the project will be</p>	TEC (CO), SRX

	used to influence the TC standardisation work. The project findings are expected to give impulses for the new trust based application scenarios and solutions concerning mobile phones, communications, e-commerce, automotive industry and similar.	
<b>COPPER</b> , Ref.No 216474 (2008), <a href="http://www.copper-project.eu">http://www.copper-project.eu</a>	The project Copper Interconnects for Advanced Performance and Reliability (CopPeR) will develop and implement a radically new approach to manufacture a new generation of copper interconnects overcoming the roadblocks for further advances in CMOS miniaturisation	TEC (CO)
<b>MULTIBASE</b> , Ref.No 216541 (2008), <a href="http://www.multibase-project.eu">http://www.multibase-project.eu</a>	Scalable Multi-tasking Baseband for Mobile Communications: The MULTI-BASE project objectives target the elimination of key technical and commercial barriers to ubiquitous broadband access by enabling efficient and sustainable disposition of operation and production factors as spectrum, power engineering cost and silicon process technology.	TEC (CO)
<b>OMEGA</b> , Ref.No 213311(2008), <a href="http://www.ict-omega.eu/">http://www.ict-omega.eu/</a>	Home Gigabit Access: Gigabit home access networks (HANs) are a pivotal technology to be developed if the EU Vision of the Future Internet is to be realised. Consumers will require such HANs to be simple to install, without any new wires, and easy enough to use so that information services running on the HAN will be "just another utility," as, for instance, electricity, water and gas are today. A successful OMEGA project will demonstrate the successful realisation of a gigabit HAN.	TEC
<b>ITEA / MEDEA +</b>		
<b>Trusted Secure Computing (TSC Meda+)</b> , <a href="http://www.trustedsc.eu">http://www.trustedsc.eu</a>	<p>The Trusted and Secured Computing (TSC) project aims at developing a family of HW/embedded SW silicon components enforcing secure and trusted computing in the Consumer, Computer, Telecommunications and Wireless areas</p> <p>It also intends to develop trust concept and architecture elements usable in other European industrial segments such as automotive, industrial, aeronautics (especially in their content acquisition and payment, ticketing and DRM aspects).</p> <p>Finally the TSC project will develop relevant European contributions related to Trusted Computing standards while keeping inter-operability with existing US-led or Asian initiatives.</p>	TEC
<b>TECOM/ITEA</b> , <a href="http://www.tecom-itea.org/">http://www.tecom-itea.org/</a>	<p>The Trusted Embedded Computing (TECOM) project is targeting to develop both a publicly available trusted operating system for embedded systems as well as trusted and secure software technology on the application level. Our results will protect the upcoming generation of embedded systems against the whole variation of security incidents well known from the PC world.</p> <p>Based on the public available standards of the Trusted Computing Group we will work on software modules and operating systems for all areas of trusted and secure computing in the embedded regime like mobile phones, trusted networking, and secure content management for Digital Rights Management (DRM), industrial control,</p>	TEC

	<p>automotive and a lot of similar applications with restrictive security and trust requirements.</p> <p>This project will fulfil today's needs for trusted systems building blocks and transfers already existing standards and theoretical know-how into the real application and product world to support the need for trust and security technology in full variation of emerging and future applications.</p>	
<b>IST FP6 – IPs</b>		
<p><b>HYDRA,</b> Networked Embedded System middleware for heterogeneous physical devices in a distributed architecture, IST-2006-034891, <a href="http://www.hydra.eu.com">http://www.hydra.eu.com</a></p>	<p>The HYDRA project aims to research, develop, and validate middleware for networked embedded systems that allows developers to develop cost-effective, high-performance ambient intelligence applications for heterogeneous physical devices. The first objective is to develop middleware based on a Service-oriented Architecture, to which the underlying communication layer is transparent.</p> <p>The second objective of the HYDRA project is to develop a Software Development Kit (SDK). The SDK will be used by developers to develop innovative Model-Driven applications with embedded ambient intelligence using the HYDRA middleware.</p> <p>The third objective of the HYDRA project is to research and develop a business-modelling framework for analysing the business sustainability of the developed applications.</p> <p>The fourth objective of the HYDRA project is to validate the middleware, the SDK toolkit and the business models in real end-user scenarios in three user domains: Healthcare, facility management and a third domain to be defined.</p>	AU
<p><b>Open_TC,</b> Open Trusted Computing, IST-2005-027635, <a href="http://www.opentc.net">http://www.opentc.net</a></p>	<p>Open Trusted Computing (Open_TC) aims at design and development of trustworthy platforms and infrastructures and involves 23 partners with strong industry participation. It investigates the establishment of an Open Trusted Computing framework for the existing and future computing platforms and infrastructures.</p> <p><b>RUB</b> is one the (academic) partners with considerable contribution and assignments regarding design and development contribution. RUB is actively involved in the work packages where cryptographic mechanisms and protocols are used in conjunction with the Trusted Computing functionalities. Moreover, RUB is leading the working group for Embedded Trusted Platforms and Applications.</p> <p>In Open_TC software engineering capabilities are needed for robust software design which is highly beneficial for the CACE project (all work packages).</p>	TEC (CO), RUB
<p><b>PalCom,</b> Palpable Computing, IST-2004-002057, <a href="http://www.ist-palcom.org">http://www.ist-palcom.org</a></p>	<p>The PalCom vision is to produce the first version of a software architecture for palpable computing, i.e., an architecture that supports going beyond 'traditional' ambient computing. Where ambient computing sees invisibility of computing sources and automation of human tasks as ideals, we also insist on comprehensibility, user control and understanding.</p> <p>Objectives include a conceptual framework for palpable computing, a first version of the specifications of the</p>	AU (CO), AI

	architecture, a fundamental understanding of the application domains, a range of visions for future palpable usages, a toolbox for constructing palpable devices, and a range of prototypes to concretise and experiment with those usages in order to inform software architecture.	
<b>SECOQC,</b> Development of a global network for secure communication based on quantum cryptography, IST-2004-506813, <a href="http://www.secoqc.net">http://www.secoqc.net</a>	This project includes 38 partners from across Europe. The vision of SECOQC is to provide European citizens, companies and institutions with a tool that allows facing the threats of future interception technologies, thus creating significant advantages for European economy. With SECOQC the basis will be laid for a long-range high security communication network that combines the entirely novel technology of quantum key distribution with components of classical computer science and cryptography.	AU
<b>SPICE,</b> Service Platform for Innovative Communication Environment, IST-2006-027617, <a href="http://www.ist-spice.org">http://www.ist-spice.org</a>	The objective of SPICE was to provide an easy and simple way to create and roll out innovative services. Our primary role was in defining the use cases and contributing to the use of the generic authentication architecture (GAA) in SPICE design.	Nokia
<b>IST FP6 - STREPs</b>		
<b>EU-DOMAIN,</b> enabling users for - Distance-working & Organisational Mobility using Ambient Intelligence service Networks, IST-2004-004420, <a href="http://www.eu-domain.eu.com">http://www.eu-domain.eu.com</a>	The eu-DOMAIN project will develop a new, innovative European ambient intelligence service platform for automatic, context sensitive offering and contracting of mobile web services across heterogeneous networks. The eu-DOMAIN service platform will interconnect people, devices, buildings and content in an interoperable network.  Objectives: The overall objective of the eu-DOMAIN project is to define, develop, prototype and validate a mobile ambient intelligence services platform that integrates mobile users into intelligent surroundings and deliver on-demand content services and support for ad-hoc collaborative workgroups across geographically distributed organisations.	AU
<b>GORDA,</b> Open Replication of Databases, IST-2004-004758, <a href="http://gorda.di.uminho.pt/">http://gorda.di.uminho.pt/</a>	The goal of the GORDA project is to foster database replication as a means to address the challenges of trust, integration, performance, and cost in current database systems underlying the information society. This is to be achieved by standardising architecture and interfaces, and by sparking their usage with a comprehensive set of components ready to be deployed. The research topics of GORDA are distributed systems.	MINHO (CO)
<b>SCARD,</b> Side-Channel Attack Resistant Flow, IST-2002-507270, <a href="http://www.scard-project.eu">http://www.scard-project.eu</a>	The SCARD projects aimed to enhance the typical microchip design flow in order to provide means for designing side-channel resistant circuits and systems. The work concentrated from high-level system description over register transfer layer description down to gate level net lists, and placement & routing of the microchip.  Moreover the project studied the whole phenomenon of SCA and provided appropriate analysis tools and design tools for the designer of secure systems. TEC coordinated	TEC (CO)

	this FP6 project.	
<p><b>UbiSec&amp;Sens</b>, Ubiquitous Sensing and Security in the European Homeland, IST-2005- 026820, <a href="http://www.ist-ubisecsens.org">http://www.ist-ubisecsens.org</a></p>	<p>UbiSec&amp;Sens aims at providing a comprehensive architecture for medium and large scale wireless sensor networks with the full level of security that will make them trusted and secure for all applications. The overall project goals are:</p> <ul style="list-style-type: none"> <li>• focus the work on the intersection of security, routing and in-network processing to design and develop efficient and effective security solutions and to offer effective means for persistent and encrypted data storage for distributed (and tiny) data base approaches</li> <li>• provide secure components for sensor network application development. We aim at extremely energy-efficient and condensed data transmission as well as highly robust and reliable solutions for concrete WSNs that, at the same time, still provide an appropriate level of security.</li> <li>• Prototype and validate the UbiSec&amp;Sens solutions in the representative wireless sensor application scenarios of agriculture, road services and homeland security.</li> </ul> <p><b>RUB</b> contributes to network security aspects and efficient cryptographic implementations</p>	RUB
<b>IST FP6 – NoE</b>		
<p><b>ECRYPT</b>, European Network of Excellence in Cryptology, IST-2002-507932, <a href="http://www.ecrypt.eu.org">http://www.ecrypt.eu.org</a></p>	<p>ECRYPT on research in information security and cryptography. The ECRYPT project includes roughly 30 industrial and academic partners. ECRYPT's goals are to improve research in cryptology, to encourage collaborations within Europe and to generate a united European research community in cryptology.</p> <p>Many of the CACE partners are leaders of ECRYPT and therefore a strong collaboration with the ECRYPT project is strengthened. The participation of CACE partners is as followed:</p> <p><b>RUB</b> and <b>TUE</b> (Tanja Lange) are co-leading the Virtual Lab VAMPIRE that considers amongst others software implementation of cryptographic schemes. Within this virtual lab, Dan Page (<b>UNIVBRIS</b>) is working group leader of VAM1, which is focussed software implementation of cryptography; this is highly relevant to the entire CACE project and WP1 and WP2 in particular.</p> <p>RUB, UNIVBRIS, TUE and <b>AU</b> are also major players in the Virtual Lab PROVILAB that considers design and analysis of cryptographic protocols with special focus on multiparty computation. Berry Schoenmakers (TUE) is workpackage leader of PROVILAB's WG2. The topics covered are important for working groups WP3, WP4 and WP5 within CACE.</p> <p>AZTEC is the virtual lab concerned with public key cryptography. Nigel Smart (UNIVBRIS) is working group leader of AZTEC1 which is focussed on techniques in provable security; this is highly relevant to WP3 and WP5 within the CACE project.</p>	RUB, UNIVBRIS, TUE, AU, TKK (Kaisa Nyberg is a member of the Strategic Board)
<p><b>FIDIS</b>, Future of Identity in</p>	<p>FIDIS (Future of Identity in the Information Society) is a NoE (Network of Excellence) supported by the European</p>	BFH, SRX,

the Information Society, IST-2004-507512, <a href="http://www.fidis.net">http://www.fidis.net</a>	Union under the 6th Framework Program for Research and Technological Development within the Information Society Technologies (IST) priority in the Action Line: "Towards a global dependability and security framework". It involves 24 partners from all over Europe, conducting research on the future of identity. The objective of FIDIS is to integrate European research with regard to technologies to support identity and identification, interoperability of identity and identification concepts, ID-theft, privacy and security, and profiling and forensic implications.  <b>BFH</b> participates in FIDIS through its Virtual Identity and Privacy Research Centre (VIP).  <b>SRX</b> actively participates in FIDIS by considering and examining the applicability and deployment of Trusted Computing and other emerging technologies for the purpose of secure Identity Management and e-voting. Further, SRX is strongly involved in organising workshops on these topics as well as dissemination and training activities, in particular in the context of doctoral consortium for training PhD students.	
<b>IST FP6 – FET</b>		
<b>SPEED,</b> Signal Processing in Encrypted Domain, IST-2006-034238, <a href="http://www.speedproject.eu/">http://www.speedproject.eu/</a>	Signal Processing in Encrypted Domain aims at designing cryptographic and security mechanisms and systems that allow for secure operation on multimedia data or any other signal related quantities in an untrusted environment. Operations in this context include merge, update, pattern matching, etc. The result of SPEED provide the appropriate tools for realising many applications that require such operations in environments that are potentially adversarial and may defeat privacy or reveal other sensitive information to unauthorised entities.	RUB
<b>IST FP6 – CA</b>		
<b>TYPES subsite,</b> Types for Proofs and Programs, IST-2004-510996, <a href="http://www.cs.chalmers.se/Cs/Research/Logic/Types/index.html">http://www.cs.chalmers.se/Cs/Research/Logic/Types/index.html</a>	The aim of the research is to develop the technology of formal reasoning and computer programming based on Type Theory. This is done by improving the languages and computerised tools for reasoning, and by applying the technology in several domains such as analysis of programming languages, certified software, formalisation of mathematics and mathematics education. The research topics of TYPES are "Theory and Formal Methods"	MINHO

**Table 9: Overview of FP6 and FP7 projects of CACE partners**

## 5.2 Participation in national projects

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

Project name	Topic and description of the project	Project partners involved
<b>Austria</b>		
<b>Trusted Computing for the Austrian Government</b>	Introduction of Trusted Computing for the Austrian Public Administration	TEC (CO)

<a href="http://www.trusted-computing.at">www.trusted-computing.at</a>		
<b>Finland</b>		
<b>BooMCrypt</b>	In this project mathematical and computational methods from the theory of Boolean functions and Boolean logics will be applied to the analysis of security level of cipher systems and development new methods of cryptanalysis. Results from this project will be applied in the analysis and design of cryptosystems, such as block ciphers and stream ciphers.	TKK
<b>Germany</b>		
<b>EMSCB</b> <a href="http://www.emscb.de">http://www.emscb.de</a>	<p>European Multilaterally Secure Computing Base (EMSCB) aims at developing a trustworthy computing platform with open standards that solves many security problems of conventional platforms. The platform deploys</p> <ul style="list-style-type: none"> <li>• hardware functionalities provided by Trusted Computing,</li> <li>• a security kernel based on a microkernel, and</li> <li>• an efficient migration of existing operating systems.</li> </ul> <p>In the sense of multilateral security, the EMSCB platform allows the enforcement of security policies of different parties, i.e., end-users as well as industry. Consequently, the platform enables the realisation of various innovative business models, particularly in the area of Digital Rights Management, while averting the potential risks of Trusted Computing platforms concerning privacy issues. The source code of the EMSCB platform will be published under an open source license. The EMSCB project is partly funded by the German Federal Ministry of Economics and Technology.</p>	SRX, RUB
<b>Verisoft XT</b> <a href="http://www.verisoftxt.de">http://www.verisoftxt.de</a>	The Verisoft project is a long-term research project funded by the German Federal Ministry of Education and Research (bmb+f). It aims at verifying five concrete application tasks, one from academic and four from industrial background. The verification will be formal and pervasive, i.e., computer-aided verification tools will be used throughout all layers of abstractions. This way, human errors are excluded, full coverage is achieved, and the results are based on a well-known small set of assumptions. Hence, the verified systems are of extreme quality as required in many industrial sectors, such as automotive engineering, security, and medical technology. Additionally, productivity is expected to increase, with all tools being specifically developed and enhanced for this task.	SRX
<b>Portugal</b>		
<b>RESCUE</b> <a href="http://twiki.di.uminho.pt/twiki/bin/view/Research/Rescue/WebHome">http://twiki.di.uminho.pt/twiki/bin/view/Research/Rescue/WebHome</a>	The RESCUE project aims at providing innovative, efficient and expressive mechanisms for the secure implementation and execution of code, with an emphasis on problems posed by embedded systems.	MINHO

**Table 10: Participation in national projects**

## 6 List of Abbreviations

CACE	Computer Aided Cryptography Engineering
EC	European Commission
TEC	Technikon Forschungs- und Planungsgesellschaft mbH
RUB	Ruhr Universität Bochum
UNIVBRIS	University of Bristol COMPSCI
TUE	TU Eindhoven
MINHO	Universidade do Minho
BFH	Berner Fachhochschule
AU	Aarhus University
HU	University of Haifa
SRX	Sirrix AG security technologies
TKK	Teknillinen Korkeakoulu
Nokia	Nokia Oye
AI	Alexandra Instituttet A/S