



technikon

New Technology for Trust and Security

presented on June 10th 2008 at the 1st Japan EU Symposium on the
"New Generation Network" and the "Future of the Internet"

Klaus-Michael KOCH
CEO TECHNIKON Forschungsgesellschaft
koch(at)technikon(dot)com

technikon

Overview

New Technology for Trust and Security

- Introduction
- New technology for Trust and Security
 - ↪ Clients/Servers/Operating Systems (OpenTC)
 - ↪ Infrastructure/Embedded platforms (TECOM)
 - ↪ Cryptographic software engineering (CACE)
- Future work/projects proposed
 - ↪ Trusted Computing Pilot
 - ↪ Security Hardware
- Summary



- Technikon: Austrian SME Partner for security related projects
 - ✚ Private research company, founded 1999 by Françoise Jouffre and Klaus-Michael Koch
 - ✚ Located in Austria, 20 people from 8 nations, 90% multidisciplinary academics
 - ✚ 2006 Winner of Carinthian Innovation Prize, 2007 Winner of the TRIGOS Prize
 - ✚ Headquarter for WITEC Europe "Women in Science, Engineering and Technology"

- Security Research, Products and Services
 - ✚ Requirement and System Engineering
 - ✚ Security Architectures and Security Policies
 - ✚ Secure web tools and collaboration services: Trusted Knowledge Suite
 - ✚ National and International Project Coordination FP5, FP6, FP7

- Technology Based Services
 - ✚ Standardisation Work (ETSI, CEN, CENELEC, ISO, ANSI, TCG)
 - ✚ Technical documentation and training



status	project	topic	role
closed	SMART-USB 1999	IST-1999-20323 Smart Card with USB interface	Subcontractor
closed	SETIC 2000	IST-2000-25167 Secure Integrated Circuits for Peripherals	Subcontractor
closed	USB-CRYPT 2000	IST-2000-25169 Cryptographic Module with USB Interface	Subcontractor
closed	FINGERCARD 2000	IST-2000-25168 Smart Card with Biometric Sensor	Assessor
closed	INSPIRED 2000	IST-2000-28013 Integrated Photodiodes for DVD Applications	Subcontractor
closed	SCARD 2002	IST-2002-507270 Side Channel Proof Smart Card Design	Coordinator
closed	Stereotypes 2004	EC-Gender-Equality-2004 Tackling Stereotypes	Partner
running	OPENTC 2005	Open Trusted Computing	Coordinator
running	SEA-NET IST 2005	Semiconductor Equipment Assessment for Nanoelectronics	Subcontractor
running	HYMNE Medea 2005	High Yield driven CMOS Manufacturing Excellence	Subcontractor
running	HIMISSION Medea 2005	High Frequency Microsystems on Silicon	Subcontractor
running	TSC Medea 2006	Hardware for Trusted Secure Computing	Partner
running	TECOM FP7 ICT 2007	Trusted Embedded Computing	Coordinator
running	TECOM ITEA-2 2006	Software for Trusted Embedded Computing	Partner
running	CACE FP7 ICT 2007	Computer Aided Cryptography Engineering	Coordinator
running	COPPER FP7 ICT 2007	Copper Interconnects for Advanced Performance and Reliability	Coordinator
running	MULTIBASE FP7 2007	Scalable Multi-tasking Baseband for Mobile Communications	Coordinator
running	OMEGA FP7 ICT 2007	Home Gigabit Access	Partner
starting	MEMFIS FP7 ICT 2008	Ultrasmall MEMS FTIR Spectrometer	Coordinator



➤ Open Trusted Computing Project

- ↳ Parameters
- ↳ Partners
- ↳ Motivation
- ↳ Objectives
- ↳ Architecture
- ↳ Use Cases



Public web page www.opentc.eu



➤ OpenTC Project Parameters

- ↳ Duration: 3,5 years (October 2005 – April 2009)
- ↳ Budget: € 17,1m Effort: 175 person years

➤ 23 Contractors

- ↳ Covering the whole value chain for trusted computing
- ↳ 7 industry partners, 3 SMEs, 13 universities and research institutes from 12 countries

➤ Links to standardisation

- ↳ Trusted Operating Systems (TCG)
- ↳ Trust enhanced processors (OMA)
- ↳ W3C, OASIS, IETF, CEN, ISO, ETSI

↳ Project results are made available at www.OpenTC.eu



technikon OPENTC Partners

Clients/Servers/Operating Systems



Technikon Forschungs- und Planungsges.m.b.H, A



Infineon Technologies AG, D



Hewlett Packard, UK



Technische Universität Graz, A



Technische Universität München, D



SUSE Linux Products GmbH, D



Royal Holloway, University of London, UK



Forschungszentrum Karlsruhe, D



Tubitak, Turkey



Politecnico di Torino, I



Budapest University of Technology and Economics, HU



Commissariat à l'énergie atomique, FR



Ruhr Universität Bochum, D



Technische Universität Dresden, D

University of Cambridge Computer Laboratory, UK



IBM Research GmbH, CH



Institute for Security and Open Methodologies, ESP



AMD, D



Portakal Teknoloji, Turkey



Intek, RU

Technical University of Sofia, BG



Katholieke Universiteit Leuven, B



COMNEON, D



Klaus-Michael KOCH - June 10th 2008 - Brussels

7

technikon OpenTC Objectives

Clients/Servers/Operating Systems



- Secure open source operating system
 - ⊗ Develop several levels of trusted OS, related protocols and management;
 - ⊗ Trusted Booting and disc volume encryption; Implementation of virtualisation layer; TSS stack for the TPM and first management SW for performing elementary TPM functionalities; General interfaces and control capabilities for intra- as well as inter-OS communication and externally useable security APIs;
 - ⊗ Quality analysis and security evaluation is an important part of the project.
- Get experience and feedback from prototype applications
 - ⊗ Proof-of-Concept for digital signing and verification;
 - ⊗ Integration of Public Key Infrastructure, Authentication methods;
 - ⊗ Adapting the TC APIs to other programming languages for broad use;
 - ⊗ Analysis of special requirements of security sensitive platforms;
 - ⊗ show prototype security application;
- Distribution package for OpenTC results
 - ⊗ OpenTC is an open project, where the results should be widely used and distributed.
 - ⊗ A commercial Linux distributor (Novell/SUSE) is involved in OpenTC to set up a professional distribution environment.



Klaus-Michael KOCH - June 10th 2008 - Brussels

8

technikon OpenTC Use cases

Clients/Servers/Operating Systems



- Personal Electronic Transactions
 - ↳ Trusted Virtual Machine
 - ❖ Banking Transactions via Trusted GUI
- Corporate Computing at Home
 - ↳ Virtual Corporate PC at Home
 - ❖ Trusted computing enables corporation to trust
- Virtual Data Center
 - ↳ Virtual customer infrastructure (machine, network)
 - ❖ Smaller number of physical machines (XEN, L4)

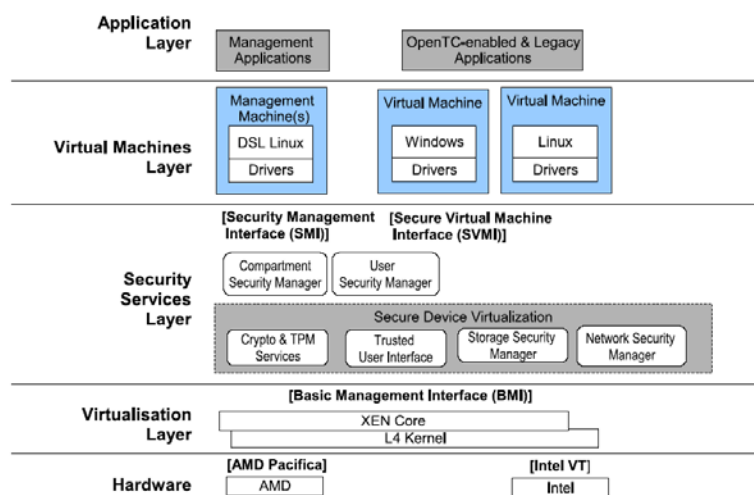


Klaus-Michael KOCH - June 10th 2008 - Brussels

9

technikon OpenTC Architecture

Clients/Servers/Operating Systems



Klaus-Michael KOCH - June 10th 2008 - Brussels

10

➤ Trusted Embedded Computing Project

- ↪ Parameters
- ↪ Consortium
- ↪ Objectives
- ↪ Working areas
- ↪ Folder



see www.tecom-project.eu



➤ TECOM Project Parameters

- ↪ Duration: 3 years (January 2008 – December 2010)
- ↪ Budget: € 9,0 Million Effort: 59 person years

➤ 11 Contractors

- ↪ Covering the whole value chain for embedded trusted computing
- ↪ 3 Industry partners, 7 SMEs, and 1 University from 4 countries



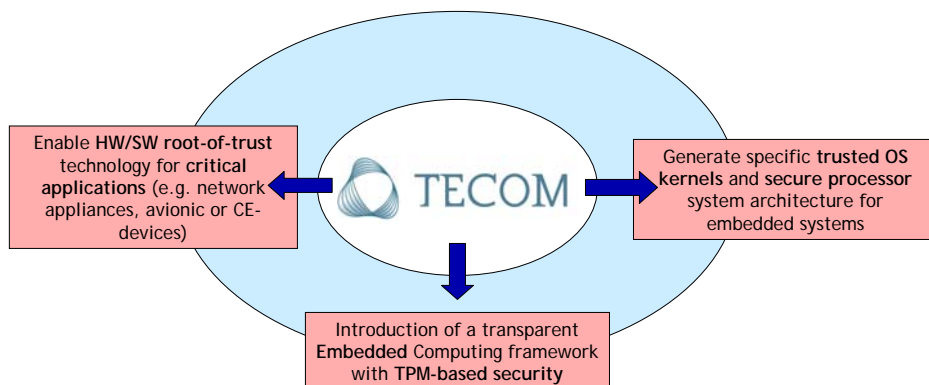
The availability of implicit trust and security will be mandatory for complex, large and critical equipment of the future



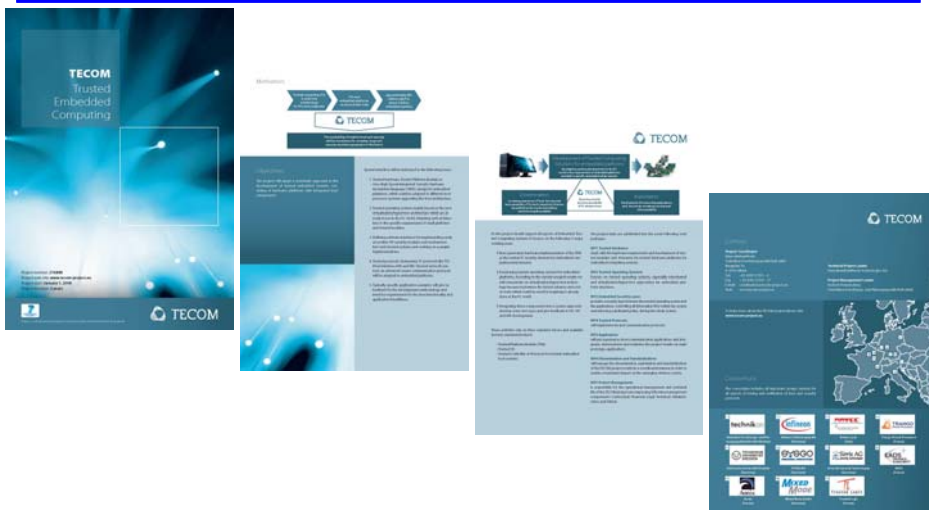
- (1) Technikon Forschungs- und Planungsgesellschaft mbH
- (2) Infineon Technologies AG
- (3) Amtec S.p.A.
- (4) Trango Virtual Processors
- (5) TU Dresden
- (6) SYSGO AG
- (7) Sirrix AG Security Technologies
- (8) EADS
- (9) Aonix
- (10) Mixed Mode GmbH
- (11) Trusted Logic



- R&D of trusted computing principles, requirements and implementation examples for EMBEDDED SYSTEMS



- Embedded platform with TPM
 - ↳ Next generation hardware implementation of the TPM as the central TC security element for embedded computing environments.
- OS for Embedded platforms
 - ↳ Developing trusted operating systems for embedded platforms;
 - ↳ According to the current research results we concentrate on virtualisation/hypervisor technology since it promises the fastest advance by reusing work done at the PC world;
- Prototype development
 - ↳ Integrating these components into a system approach, develop test cases and give feedback to OS, SW and HW developers



➤ Computer Aided Cryptography Engineering Project

- ↪ Mission & parameters
- ↪ Partners
- ↪ Objectives
- ↪ Main principles
- ↪ Expected Results
- ↪ Folder



see www.cace-project.eu



Mission of the CACE project

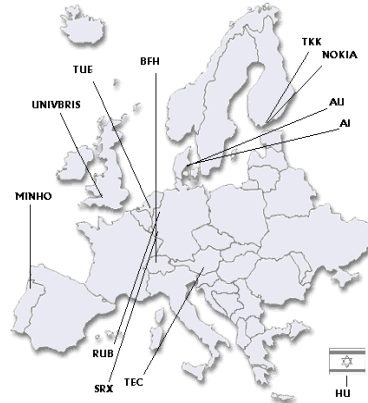
Enable verifiable secure cryptographic software engineering to non-experts by developing a toolbox which automatically produces high-performance solutions from natural specifications.

Project parameters

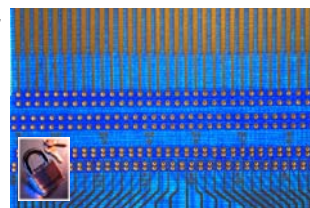
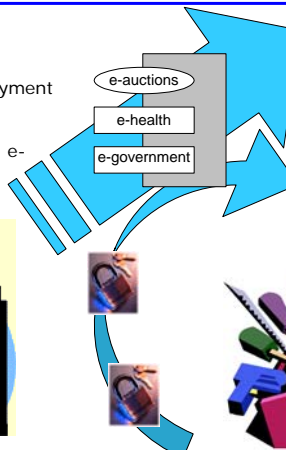
Duration: 3 years (January 2008 – December 2010)
Budget: € 4,7 Million Effort: 45 person years
Partners: 12 partners, 8 Universities, 2 SMEs and 1 Industry



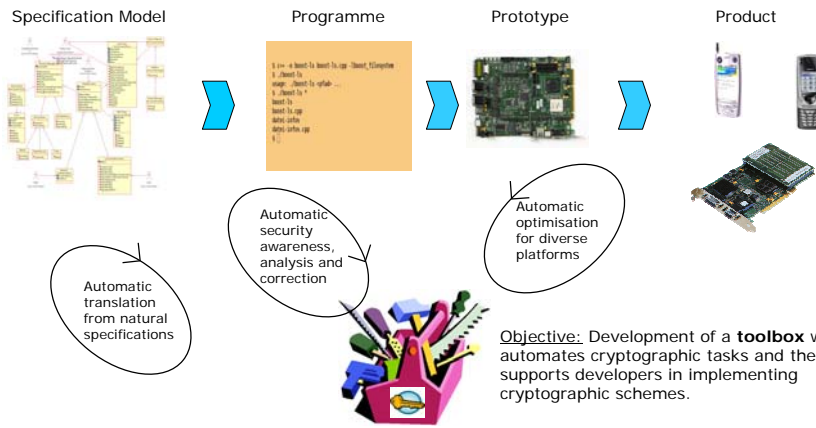
- TECHNIKON (AT) - Coordination
- Ruhr University Bochum (DE) – Technical Lead
- University of Bristol COMPSCI (GB)
- Eindhoven University of Technology (NL)
- University of Minho (PT)
- Bern University of Applied Sciences (CH)
- Aarhus University (DK)
- University of Haifa (IL)
- Sirrix security technologies AG (DE)
- Helsinki University of Technology (FI)
- Nokia (FI)
- Alexandra Institute (DK)



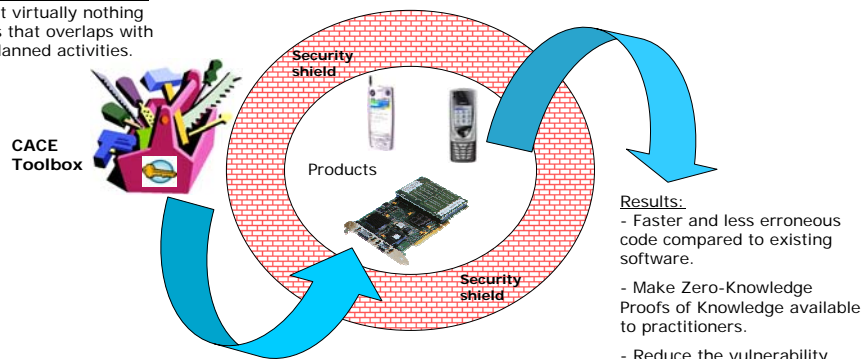
Modern applications processing sensitive data require the deployment of sophisticated cryptographic techniques. (e.g. for privacy preserving e-auctions, e-health, e-government,...)



Create a **toolbox** which makes high-quality **cryptographic** software available to non-expert developers.



Current state-of-the-art is that virtually nothing exists that overlaps with the planned activities.





Proposed work

Proposal to set up a pilot project with trusted computing client/server services & infrastructure.

Open for collaboration

Project duration: 1,5-2 years
Project volume: € 4-5 Million

If interested to cooperate, please contact

koch(at)technikon(dot)com

Proposed future work

The core topics are enabling and enhancing the development of new security technologies.

Open for collaboration

Project duration: 3-4 years

Project volume: € 15-20 Million

If interested to cooperate, please contact

koch(at)technikon(dot)com



State of the art

- ↳ Security functions are supported by Hardware/Software
- ↳ Assumption of trust in Hardware (Designers, Production steps)
- ↳ Security Hardware production is outsourced to low-cost sites

Technical issues to be addressed

- ↳ Efficient usage of physical properties of hardware for the purpose of authentication (anti-counterfeiting of products), secure secret key storage, e.g. by deploying the so-called Physical Unclonable Functions (PUFs);
 - ↳ Reconfigurable security processors (e.g. integrating security functionality (e.g. TPM) in CPU as Intel has already done;
 - ↳ Evaluation of security functions in hardware.
-



Goals of the proposed project are

- ↳ Explore various security hardware architectures for future generation of trusted devices
- ↳ Develop methodologies for evaluating their correctness and soundness as well as for identifying malicious and unspecified functionalities;
- ↳ Enable the detection of IC Trojans, IC trapdoors and unspecified functions in security hardware manufactured in un-trusted foundries; and to
- ↳ Monitor and audit the hardware after delivery by the manufacturer, e.g., to deter illegal redistribution through illegitimate overproduction or resell.



- Several European projects are on the way to create new security technology
- Projects create basic building blocks for the future internet and its infrastructure
 - ↳ Clients/Servers/Operating Systems (OpenTC)
 - ↳ Infrastructure/Embedded platforms (TECOM)
 - ↳ Cryptographic software engineering (CACE)
- Proposal to work collaborative on future Security Hardware common project
 - ↳ Trusted Computing Pilot
 - ↳ New Technology for Security Hardware



technikon Contact data
New Technology for Trust and Security

Dr. Klaus-Michael KOCH
Managing Director
TECHNIKON Forschungsgesellschaft mbH
Burgplatz 3A
A-9500 Villach
Tel.: +43 4242 23355
E-Mail: koch(at)technikon(dot)com



technikon



Klaus-Michael KOCH - June 10th 2008 - Brussels

29