Eighth Smart Card Research and Advanced Application Conference
CARDIS 2008 – Call for Papers
Royal Holloway, University of London, September 8-11, 2008
http://www.scc.rhul.ac.uk/CARDIS/

The eighth Smart Card Research and Advanced Application IFIP Conference, organized by IFIP Working Groups WG 8.8 and WG 11.2, will be held in Royal Holloway, University of London, Egham, Surrey, UK. Since 1994, CARDIS has been the foremost international conference dedicated to smart card research and applications. Every two years the scientific community congregates to present new ideas and to discuss recent developments. Also in 2008, forty years after Jürgen Dethloff and Helmut Grötrupp filled their idea of incorporating an integrated circuit in an identification card, CARDIS'08 will bring together leading researchers and practitioners in the development and deployment of state-of-the-art smart card technologies. The fast evolutionary process in the field of information security requires adequate means to represent humans in the process of human-machine interactions. Smart cards, or by extension smart devices with their processing power and their direct correlation to the user are considered to be the first choice. In rather young and new realms, such as pervasive computing, smart cards and devices face new challenges. Today, the capabilities of smart cards and devices with their highly advanced specialized security features reach a wide variety of applications. They are the basis for many secure systems and play a decisive role in ID management. Established computer science areas like hardware design, operating systems, modeling systems, cryptography or distributed systems got adapted to this fast growing technology and investigate emerging issues resulting from it. Unlike events devoted to commercial and application aspects of smart cards, CARDIS conferences gather researchers and technologists who focused on all aspects of the design, development, deployment, validation and application of smart cards or smart personal devices.

Conference Scope:

The program committee is seeking papers describing the design, development, application and validation of smart card technologies. Submissions across a broad range of smart card development phases are encouraged, from exploratory research and proof-of-concept studies to practical applications and deployment of smart card technology. As a response to the growing development of contactless applications and RFID systems, a special interest is also devoted to low cost cryptographic mechanisms and physical security of constrained devices.

Topics of interest include, but are not limited to:

- From smart cards to smart devices (hardware, form factor, display),
- Software environments for smart cards and devices (OS, VM, API),
- Smart cards and devices networking and high-level data models,
- Smart cards and devices applications, development and deployment,
- Person representation and biometrics using smart technologies,
- Identity, privacy and trust issues for smart technologies,
- High-speed, small-footprint implementations of cryptographic algorithms,
- Attacks and countermeasures in hardware and software,
- Cryptographic protocols for smart cards and devices,
- Biometrics and smart cards,
- Formal modeling of environments and applications,
- Interplay of TPMs and smart cards,
- Security of RFID systems.

Important Dates:

Submission: **Extended Deadline Feb. 23th, 2008**   Notification of acceptance: May 1st, 2008
Camera-ready version of papers: June 15th, 2008   Workshop date: September 8-11th, 2008

Paper submission and proceedings:

Submitted papers should present novel contributions related to the topics listed above. They must be original, unpublished, anonymous and not submitted to another conference or journal for consideration of publication. Papers must be written in English, they should not exceed 15 pages. Submissions not meeting these guidelines risk rejection without consideration of their merits. All submissions will be blind-refereed. Authors are invited to submit their manuscripts (PDF or PS format) by filling in the submission form available on the following web site: http://www.scc.rhul.ac.uk/submissions/. Submission implies the willingness of at least one author to register and present the paper. The proceedings will be published as a Springer LNCS volume.

Organizing committee co-chairs:

- Konstantinos Markantonakis, Royal Holloway University of London, UK
- Keith Mayes, Royal Holloway University of London, UK

Program co-chairs:

- Gilles Grimaud : University of Lille 1, France
- François-Xavier Standaert: UCL Crypto Group, Belgium

Program committee:

- Mehdi-Laurent Akkar, Barclays Capital, USA
- Gildas Avoine, MIT CSAIL, USA
- Boris Balacheff, Hewlett-Packard Laboratories, England
- Eduardo De Jong, Sun Microsystems, USA
- Josep Domingo-Ferrer, Universitat Rovira i Virgili, Spain
- Dieter Gollmann, TU Hamburg-Harburg, Germany
- Louis Goubin, Université de Versailles, France
- Pieter Hartel, University of Twente, the Netherlands
- Jaap-Henk Hoepman, TNO and Radbout University Nijmegen, the Netherlands
- Dirk Husemann, IBM Zurich Research Laboratories, Switzerland
- Marc Joye, Thomson Multimedia, France
- Jean-Louis Lanet, GemAlto, France
- Javier Lopez, University of Malaga, Spain
- Pierre Paradinas, INRIA, France
- Joachim Posegga, University of Hamburg, Germany
- Emmanuel Prouff, Oberthur Card Systems, France
- Damien Sauveron, University of Limoges, France
- Isabelle Simplot-Ryl, University of Lille, France
- Issa Taore, University of Victoria, Canada
- Mike Tunstall, University College Cork, Ireland
- Jean-Jacques Vandewalle, GemAlto, France
- Johannes Wolkerstorfer, IAIK/ Universisity of Graz, Austria