



Conference Chair

Jörn-Marc Schmidt, *TU Graz, Austria*

Publicity Chair

Jean-Jacques Quisquater, *UCL, Belgium*

Program Chair

Stefan Mangard, *Infineon, Germany*

Program Committee

N. Asokan
Nokia Research Center, Finland

Gildas Avoine
UCL, Belgium

Chetali Boutheina
Trusted Labs, France

Josep Domingo Ferrer
Rovari i Virgili University, Catalonia

Hermann Drexler
Giesecke & Devrient, Germany

Martin Feldhofer
NXP, Austria

Berndt Gammel
Infineon, Germany

Tim Güneysu
Ruhr-University Bochum, Germany

Helena Handschuh
*Cryptography Research Inc., USA
and KU Leuven, Belgium*

Michael Hutter
TU Graz, Austria

Marc Joye
Technicolor, France

Ioannis Krontiris
Göthe Universität Frankfurt, Germany

Jean-Louis Lanet
University of Limoges, France

Konstantinos Markantonakis
Royal Holloway, UK

Andrew Martin
University of Oxford, UK

David Naccache
ENS, France

Elisabeth Oswald
University of Bristol, UK

Catuscia Palamidessi
INRIA, France

Eric Peeters
Texas Instruments, USA

Erik Poll
RU Nijmegen, Netherlands

Bart Preneel
KU Leuven, Belgium

Emmanuel Prouff
ANSSI, France

Matthieu Rivain
CryptoExperts, France

Pankaj Rohatgi
Cryptography Research, USA

Ahmad-Reza Sadeghi
TU Darmstadt, Germany

Jean-Pierre Seifert
TU Berlin, Germany

Sergei Skorobogatov
Cambridge University, UK

François-Xavier Standaert
UCL, Belgium

Frederic Stumpf
Fraunhofer AISEC, Germany

Marc Witteman
Riscure, Netherlands

CARDIS 2012 is supported by



Call For Papers

Eleventh Smart Card Research and Advanced Application Conference (CARDIS 2012)

Graz, Austria, 28 – 30 November 2012

<http://www.cardis.org>

Since 1994, CARDIS is the foremost international conference dedicated to smart card research and applications. Smart cards and secure elements are the basis for many secure systems and play a decisive role in ID management. Established computer science areas like hardware design, operating systems, system modeling, cryptography, verification and networking 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 and secure elements in secure platforms or systems.

The eleventh Smart Card Research and Advanced Application Conference, organized by the Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, will be held in the Weitzer Hotel, Graz, Austria.

The program committee is seeking original papers on all aspects of smart cards and secure elements. Submissions across a broad range of the development phases are encouraged, from exploratory research and proof-of-concept studies to practical applications and deployment of smart cards and related technologies. Topics of interest include, but are not limited to:

- Software for secure embedded systems (operating system, virtual machines, ...)*
- Hardware architectures for secure embedded systems*
- Security of RFID systems and sensor nodes*
- Security of mobile devices and applications*
- Efficient and secure implementations of cryptographic algorithms*
- Cryptographic protocols for embedded systems*
- Physical attacks and countermeasures*
- Secure applications for embedded systems*
- Embedded systems networking*
- Person representation in embedded systems*
- Formal modeling and formal proofs of security*
- Validation and certification of embedded systems and applications*
- Identity, privacy and trust issues*

Authors are invited to submit papers (PDF or PS format) with novel contributions electronically using the submission form available on the following web site: <http://www.easychair.org/conferences/?conf=cardis2012>. Submitted papers must be original, unpublished, anonymous and not submitted to journals or other conferences/workshops that have proceedings. Submissions must be written in English and should be at most 15 pages in total. Papers not meeting these guidelines risk rejection without consideration. All submissions will be blind-refereed.

Submission implies the willingness of at least one of the authors to register and present the paper. The proceedings will be published in the Springer Lecture Notes in Computer Science (LNCS) series. Accepted papers should follow the LNCS default author instructions at <http://www.springer.de/comp/lncs/authors.html>.

Important Dates

Submission of papers:	August 20, 2012, 23:59 CET
Notification of acceptance:	October 15, 2012
Pre-proceeding version:	November 7, 2012
Workshop date:	November 28 – 30, 2012
Final version:	December 17, 2012