



CARDIS 2013

Call For Papers

General Chair

Jean-Pierre Siefert, *TU Berlin and Telekom Laboratories, DE*

Publicity Chair

Jean-Jacques Quisquater, *UCL, BE*

Program Chairs

Aurélien Francillon, *Eurecom, FR*

Pankaj Rohatgi, *Cryptography Research, USA*

Program Committee

Onur Aciicmez

Samsung, USA

N. Asokan

University of Helsinki, FI

Gildas Avoine

UCL, BE

Guillaume Barbu

Oberthur, FR

Christophe Clavier

University of Limoges, FR

Elke De Mulder

Cryptography Research, USA

Hermann Drexler

Giesecke & Devrient, DE

Martin Feldhofer

NXP, AT

Nathalie Feyt

Thales, FR

Berndt Gammel

Infineon, DE

Michael Hauspie

LIFL, FR

Michael Hutter

TU Graz, AT

Kari Kostianen

ETHZ, CH

Jean-Louis Lanet

University of Limoges, FR

Cedric Lauradoux

INRIA, FR

Stefan Mangard

Infineon Technologies, DE

David Naccache

ENS, FR

Svetla Nikova

K.U. Leuven, BE

Karsten Nohl

Security Research Labs, DE

David Oswald

Ruhr University Bochum, DE

Elisabeth Oswald

University of Bristol, UK

Eric Peeters

Texas Instruments, USA

Erik Poll

RU Nijmegen, NL

Axel Poschmann

Nanyang Tech. University, SG

Bart Preneel

K.U. Leuven, BE

Emmanuel Prouff

ANSSI, FR

Matthieu Rivain

CryptoExperts, FR

Jean-Marc Robert

ETS Montreal, CA

Thomas Roche

ANSSI, FR

Ahmad-Reza Sadeghi

TU Darmstadt, DE

Joern-Marc Schmidt

TU Graz, AT

Lex Schoonen

Brightsight, NL

Sergei Skorobogatov

Cambridge University, UK

François-Xavier Standaert

UCL, BE

Frederic Stumpf

Escrypt GmbH, DE

Marc Witteman

Riscure, NL

Twelfth Smart Card Research and Advanced Application Conference (CARDIS 2013)

Moevenpick Hotel

Berlin, Germany, 27 – 29 November 2013

<http://www.cardis.org>

CARDIS, first held in Lille, France in 1994, will turn 20 next year. Over these years, as smart cards have become a pervasive, foundational technology for bootstrapping trust in our society, CARDIS has become the foremost international academic conference dedicated to research on smart cards and their applications.

Smart cards are essential building blocks for many security critical applications and systems used in the payment, content protection, transportation, mobile and identification industries and are playing an increasing role in securing critical infrastructures. Established computer science disciplines such as hardware design, operating systems, system modeling, cryptography, verification and networking are adapting to support this ever evolving technology. Unlike events devoted to commercial and application aspects of smart cards, the CARDIS conference gathers researchers and technologists who focus on all aspects of smart cards development and deployment as well as applications of these security devices to secure platforms and systems.

The twelfth Smart Card Research and Advanced Application Conference is organized by the Chair for Security in Telecommunications (SecT), Technical University of Berlin and will be held in the Moevenpick Hotel, Berlin, Germany.

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:

- Applications for secure embedded systems*
- Virtualization and operating systems for secure embedded systems*
- Hardware architectures for secure embedded systems*
- Security of RFID systems, Internet of Things and Machine to Machine*
- Anti-cloning and anti-counterfeiting technologies*
- Security of mobile devices and applications of secure elements*
- Security of NFC based applications and payment systems*
- Trusted computing (mobile TPMs, TrustZone, Trusted Execution Environments, ...)*
- Efficient and secure implementations of cryptographic algorithms*
- Cryptographic protocols for embedded systems*
- Physical attacks and countermeasures*
- Secure networking for embedded systems*
- Security for access control, identification and transportation tokens*
- Secure embedded systems and architectures for critical infrastructure protection*
- Formal modeling and formal security proofs*
- Validation and certification of embedded systems and applications*
- Privacy and trust management for secure embedded systems and applications*
- Hardware Trojans implementation and detection*
- Design and performance evaluation of operating systems and execution environments for smart cards (e.g., Java Card)*

Submitted papers must be original, unpublished, anonymous and not simultaneously submitted to journals or other conferences/workshops with proceedings. Submissions must be formatted according to LNCS rules and should be at most 15 pages in total. Papers not meeting these guidelines risk rejection without consideration. Submissions must be anonymized and avoid obvious self-references, reviews will be double blind. Authors are invited to submit papers, in PDF format, using the dedicated submission site: <http://www.easychair.org/conferences/?conf=cardis2013> 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 after the conference, allowing to use the community feedback received during the conference for the final proceedings. All papers will also be available on the CARDIS website.

Important Dates

Submission of papers:	September 10, 2013, 23:59 GMT+02
Submission of papers:	September 17, 2013, 23:59 GMT+02 (EXTENDED)
Notification of acceptance:	October 31 November 4, 2013
Pre-proceeding version:	November 12, 2013
Workshop date:	November 27 – 29, 2013
Final version:	January 10, 2014
Proceedings:	March 2014

CARDIS 2013 is supported by

