

# Smart ConDev S&P 2014

## Workshop on Security and Privacy for Smart Connected Devices

<http://wls.orange-labs.fr/smartcondevsp2014/>

Institute of Mathematics and Computer Science Wroclaw University of Technology (Poland), 10-11 September 2014, co-located with ESORICS 2014: <http://esorics2014.pwr.wroc.pl>.

### Scope

The security and privacy of information and communications are nowadays major concerns in the development of smart devices based services, since they can represent a brake for a large scale deployment. It is then essential to find appropriate solutions, that are secure, privacy-preserving and, at the same time, efficient enough to be embedded into these devices that can be seen as too restricted to embed complex cryptographic algorithms.

The workshop aims at bringing together researchers and practitioners working in cryptography, security and privacy, from academia and industry, who are interested in achieving best practices for smart connected devices' based services.

One example may be developing security tools that can enable end users to securely access and operate contactless services in a privacy-preserving manner that is, without having to disclose their identity or any other unnecessary information related to personal data. Another example may be procedures to develop or improve the security of several smartphone and smartcard based services.

### Topics

The main topics of the workshop include, but are not limited to:

- Authentication and confidentiality
- Delegation of computation
- Efficient and secure implementations of cryptographic algorithms
- Low-power devices cryptography
- Mobile service-oriented architectures
- Outsourced storage/computation
- Privacy, anonymity, and untraceability
- Privacy for location-based services
- Privacy-preserving lightweight cryptography
- Security and privacy for smart services, NFC services, and/or smartcards

### Submissions

Any paper describing a new technical contribution or a position paper summarizing a provoking idea can be submitted to the workshop. Contributions will be selected by the program committee according to their novelty, relevance with the topics of the workshop and their potential for permitting exchanges among the participants.

The workshop will have no paper proceedings, but slides will be posted on the web page. Some of the presentations will be selected as best papers after the workshop by the Program Committee. The authors of the selected accepted papers will be invited to revise their work for publication in a special issue of the *International Journal of Applied Cryptography* (IJACT) – Inderscience (<http://www.inderscience.com/jhome.php?jcode=ijact>).

Submitted papers must not substantially overlap with papers that have been published or that have been simultaneously submitted to a journal or a conference. Submissions should begin with a title, authors' names and affiliations, a short abstract, and a list of keywords. They should be in standard PDF format, in one-column, using 11pt fonts, and less than 12 pages long, excluding the bibliography and well-marked appendices, with reasonable margins. All papers must be submitted electronically according to the instructions described at <https://smartcondevsp2014.di.ens.fr/>.

### Important Dates (tentative)

- Paper submission: 20th May 2014
- Notification to authors: 10th July 2014

### General Chairs

Sébastien Canard, Orange

Jacques Traoré, Orange

### Program Chairs

David Pointcheval, ENS

Kazue Sako, NEC

### Program Committee

*To be announced*