Scope
PRISMS' focus is the convergence of information and communication technology in mobile scenarios. This convergence is realised in intelligent mobile devices, accompanied by the increasing importance of heterogeneous access networks networks such as 3G, 4G, LTE, WiFi, PAN, NFC, etc. Privacy and security aspects need to be covered at all layers of mobile communication, from devices, over privacy-respecting credentials and mobile identity management, to machine-to-machine communications. In particular, mobile devices such as Smartphones and Internet Tablets have been very successful in commercialization. However, their security mechanisms are not always able to deal with the growing threat of attacks. As mobile communication and information processing becomes a commodity, economy and society require protection of this precious resource. Mobility and trust in networking go hand in hand for future generations of users, who need privacy and security at all layers of technology. In addition, the introduction of new data collection practices and data-flows (e.g. sensing data) from mobile devices makes it more difficult to understand the new security and privacy threats introduced. PRISMS strives to bring together the leading-edge of academia and industry in mobile systems security, as well as practitioners, standards developers and policymakers. Contributions may range from architecture designs and implementations to cryptographic solutions for mobile and resource-constrained devices.

Papers
Technical papers describing original, previously unpublished research, not currently under review by another conference or journal, are solicited. PRISMS solicits original, high-quality research contributions in the form of full papers. The focus is on the security of information and communication systems including mobile networks, devices and applications. Papers from other areas, e.g., formal methods, cryptography, database security, operating system security, will be considered if a clear connection to one of the topics below is demonstrated.

Topics of interest include, but are not limited to the following focus areas:

- **Privacy and Security in Emerging Mobile Applications and Services**
  - Privacy-respecting Authentication
  - Mobile Identity Management
  - Privacy in the Internet of Things
  - Mobile Wallets, Mobile Payments
  - Location-based Services and Mobile Sensing

- **Machine-to-Machine Security**
  - Device Identities and Authentication
  - M2M Security Architectures and Standardization
  - Remote Security Management, Verification, and Remediation of M2M Devices
  - Societal Impact of M2M Communication Security Issues

- **User Device Security and Privacy**
  - Advanced Security & Privacy Mechanisms
  - Trusted Execution Environments (TEE) and their applications
  - Mobile Application Detection and Protection
  - Secure Elements and Tokens
  - Forensic Analysis

Proposals for panels/demos/workshops/tutorials are solicited. Potential organisers are welcome to submit a proposal to one of the general chairs.

Papers must be formatted as PDF files and be submitted only through the EasyChair conference management system (https://www.easychair.org/conferences/?conf=prisms2013). Papers must not exceed the limit of 8 pages, or 4 pages for short papers, including text, figures and references. The font size must be at least 10 points.

It is strongly recommended to use the standard IEEE templates for preparing your manuscripts. Standard IEEE templates for Microsoft Word or LaTeX formats can be found at http://www.ieee.org/conferences_events/conferences/publishing/templates.html. Accepted papers will be published in the PRISMS Conference Proceedings and IEEE XPLORE.

Selected high-quality papers will be invited to a Special Issue in the Journal, *Security and Communication Networks* (SCN, Wiley; to be confirmed)