In the last decade, wireless communications and electronic devices have experienced an impressive growth. The use of the air as a propagation medium has greatly attracted both users and industry due to the numerous advantages offered by this kind of communication. Nowadays, the use of our smart phone, tablet, or netbook is becoming a core part of our daily lives. Nevertheless, wireless communications capabilities are expected to be integrated in multiple types of products such as vehicles, electrical appliances, hospital devices, etc. Thus, in the days to come, we expect that wireless communications will become ubiquitous for the future computer systems. The feasibility of this scenario strongly relies on the existence of technologies enabling both mobility and security. Mobility is the cornerstone of wireless communications and an essential feature to enable the communication between devices anywhere, anytime. However, these communications need to be secured since, due to the wireless network’s nature, eavesdroppers are able to capture any communication happening near to its coverage area.

Standardization organizations, aware of this challenging issue in future communication systems, are producing a set of specifications to enable secure mobility in different scenarios. For example, the IEEE 802.21 group is developing standards to assist a secure handoff in future Next Generation Networks (NGNs). This work is complemented by the IETF where it can be found a wide number of working groups dealing with mobility management and security in future heterogeneous networks, an issue that is also being tackled by the ITU-T Y-Series recommendations. The ISO and ETSI organizations are also dealing with mobility and security in other communication scenarios. For instance, the technical committee ISO TC 204 is addressing the specific needs that appear in Intelligent Transport Systems (ITS). This topic is also addressed by ETSI, where different work programs are also producing standards for Machine-to-Machine communications and Smart Grids, paying special attention to the specific security requirements of these scenarios. These are just a few examples of the great effort being devoted by the standardization activity, which demonstrates the importance of the subject.

The objective of this Special Issue is to provide a comprehensive guide on solutions reached by the standardization organizations in the mobility and security fields. In particular, it will focus on either recently standardized solutions or proposals under discussion. We expect that the special issue will stimulate further related research and technology improvements in this significant subject.

All received submissions will be sent out for peer review by at least two experts in the field and evaluated with respect to relevance to the special issue, level of innovation, depth of contributions, and quality of presentation. Guest editors will make an initial assessment of the suitability and scope of all submissions. Contributions that either lack originality, clarity in presentation or fall outside the scope of the special issue will not be sent for review and the authors will be promptly informed in such cases. Submitted papers must not be under consideration by any other journal or publication.

**SCOPE**

This special issue is intended to collect existing standardization efforts on achieving secure mobility in future communication systems: Next Generation Networks (NGNs), Machine-to-Machine Communications (M2M), Intelligent Transport Systems (ITS), Smart Grid, Mesh Networks, etc. Suggested topics include but are not restricted to:

- Technologies enabling secure mobility
- Service access control solutions
- Key distribution and management schemes
- Privacy preserving mechanisms and anonymity
- Trust establishment, negotiation, and management
- Secure AAA infrastructures
Secure and privacy preserving handover mechanisms
Cryptographic protocols and lightweight cryptography
Secure and privacy preserving mobile location services
Cross Layer approach to security in respect to mobility
Secure and privacy preserving mobile applications and services

SCHEDULE

Manuscript submission deadline: Oct. 31, 2012
Authors to receive a 1st decision by: Jan. 31, 2013
Final notification of acceptance: Mar. 31, 2013
Publication of special issue: (Subject to CS&I schedule)

SUBMISSION PROCEDURE

Authors should follow the “Instructions to Authors” available at the journal’s homepage http://www.journals.elsevier.com/computer-standards-and-interfaces/. A copy of the manuscript should also be emailed to the corresponding guest editor (gkamb@aegean.gr) as pdf files. The submission must include the title, abstract of your paper, and the corresponding author’s name(s) and affiliation. Please mention “SMFCS special issue submission” in the subject line of your email.

GUEST EDITORS

<table>
<thead>
<tr>
<th>Dr. Georgios Kambourakis</th>
<th>Dr. Fernando Pereñíguez García</th>
<th>Dr. Peter Mueller</th>
<th>Dr. Tom Karygiannis</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of the Aegean, Greece</td>
<td>University of Murcia, Spain</td>
<td>IBM Zurich Research Laboratory, Switzerland</td>
<td>National Institute of Standards and Technology (NIST), USA</td>
</tr>
<tr>
<td>Email: <a href="mailto:gkamb@aegean.gr">gkamb@aegean.gr</a></td>
<td>Email: <a href="mailto:pereniguez@um.es">pereniguez@um.es</a></td>
<td>E-mail: <a href="mailto:pmu@zurich.ibm.com">pmu@zurich.ibm.com</a></td>
<td>Email: <a href="mailto:tom.karygiannis@nist.gov">tom.karygiannis@nist.gov</a></td>
</tr>
</tbody>
</table>