**Thesis Title:** *Key management for the Internet of Things*

**Description of the Unit**

The Security Lab group at RISE SICS is among the largest cybersecurity research groups in Sweden. The current research focus is on IoT security, cloud security, software security, formal methods, cryptography, standardization, privacy (technical and social aspects), and virtualization. Currently, the lab is involved in multiple research projects, funded by EU H2020, VINNOVA, Eurostars, Celtic-Plus, ECSEL, EIT, SSF, VR, and Swedish industry.

**Thesis Description**

To realize the Internet of Things, with billions of connected devices, new and improved security solutions for IoT devices are crucial. Modern security solutions are based on public key cryptography, which works well for traditional Internet devices. To make these solutions work also for resource-constrained devices that lack traditional input such as keyboards, new lightweight solutions are being proposed. Still several issues remain to be solved. Specifically, regarding certificate management, new solutions for certificate revocation – how to invalidate existing security certificates marking the discontinuation of trust – are needed.

The security architecture on the Internet, with root Certificate Authorities (CAs), chains of delegation and often complex mechanisms for certificate revocation needs to be adapted to the constraints of IoT. This thesis will investigate how existing PKI standards and upcoming IoT security standards best can be used and modified, with the goal to propose a solution for certificate revocation for IoT devices.

RISE SICS will provide both background information and a certain amount of code libraries. The tasks of the Masters student for this thesis are:

- Study state-of-the-art PKI technologies and protocols, with focus on certificate revocation, and investigate their feasibility in resource-constrained IoT.
- Study related proposed IoT security standards.
- Specify and partially implement certificate revocation mechanisms, and evaluate them in an IoT testbed.
- Document the results as a thesis document.

**Competence**

We are looking for a bright MSc student with a background in cyber security, who has fulfilled the course requirements. Good programming skills are required, as is good spoken and written English.

**Application**

Applications should include a brief personal letter, CV, and recent grades. Candidates are encouraged to send in their application as soon as possible. Suitable applicants will be interviewed as applications are received.

**Start Time**

As soon as possible

**Location**

RISE SICS Kista, Stockholm

**Contact**

Dr. Shahid Raza  
Director Security Lab, RISE SICS  
[shahid.raza@ri.se](mailto:shahid.raza@ri.se)

Joel Höglund  
CSL, RISE SICS  
[joel.hoglund@ri.se](mailto:joel.hoglund@ri.se)