PHD Student: Joel Höglund, RISE Computer System Lab, Kista Stockholm
<joel.hoglund@ri.se>

Supervisors: Thiemo Voigt, Uppsala universitet, Shahid Raza, RISE Cybersecurity

Title: Towards a PKI for IoT

Abstract:

Public Key Infrastructure is the state-of-the-art credential management solution on the Internet. Also resource constrained devices, forming the Internet of Things, can benefit from the proven PKI for key management. However, current PKI is formed out of a set of heavy-weight protocols that are neither employable nor a cost-effective solution for cheap resource-constrained IoT devices. This work presents ongoing efforts to bring Internet-scale PKI into resource-constrained, possibly battery-powered, IoT devices.

Two of the new building blocks for PKI are: A new fully-automated digital certificate enrollment protocol over CoAP that suits IoT constraints as well as speaks recent IoT standards. A lightweight X.509 certificate profile and its encoding using the Concise Binary Object Representation format.

Near future deployment scenarios include e-health as well as vehicle communication domain. In addition we are looking to extend and adapt our PKI solutions to relevant new application layer protocols.

To have potential for industrial impact the proposed solutions are developed in close alignment with ongoing standardisation efforts in the area.

This work is partly funded by the SFS PhD program for Research Institutes.