Rikard Höglund

## Key Update for the IoT Security Standard OSCORE

The Constrained Application Protocol (CoAP) is a lightweight web-transfer protocol that follows the REST paradigm and is specifically suited for constrained devices and the Internet-of-Things. Object Security for Constrained RESTful Environments (OSCORE) is a lightweight security protocol that provides end-to-end protection of CoAP messages. Several methods exist for handling the establishment and update of OSCORE keying material. This work provides a detailed comparison of such methods, taking into account their features, limitations, and security properties. Additionally, it places special focus on the novel key update protocol KUDOS, for which it provides a more extended discussion about features and mechanics, as well as performing a formal verification of its security properties.