21 July 2021 Study · Web & Cloud · Digital Identity

Resource efficient DTLS Handshakes for IoT Sensors

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Version 2021-07-17
Source https://technology2.a-sit.at/en/publications/resource-efficient-dtls-handshakes-for-iot-sensors/

Every year, more and more smart sensors measure and influence many parts of our daily lives. Such sensors usually work on quite limited resources, as they have to be small and mobile. On the other hand, they are mostly part of the „Internet of Things“ (IoT): the sensors transmit their data to internet services that increasingly rely on cloud-oriented solutions. Thus, opposing characteristics meet: on the one hand, a need for resource efficiency and, on the other hand, the necessity for secure communication through the internet.

Traditional certificate-based authentication and key exchange can become a burden for such resource-limited devices. In this project report, we describe current research in this area and outline the design of our own delegation-based solution to the problem described.