IoT security Chip

Student Group

First Name	Surname	Matrikel Nr.

Table of Contents

IoT security Chip

NXP bietet mit dem IC A71CH einen Chip an, welcher intern ein public + private key Paar, sowie ein Zertifikat daraus, erzeugen kann. Weiterhin wird bei der Erzeugung der Zugriff auf den Speicher (z.B. über JTAG etc.) mittels Fuse blockiert. Die volle Doku und Application notes sind auf der NXP-Seite zu finden.