Dateiname: MA091_Fricke_H

Titel:
Entwurf eines Softwarekonzepts für die Sicherheitsarchitektur von Smart Meter Gateways nach BSI TR-03109

Bearbeiter:

Hendrik Fricke

Text der Kurzfassung:

Die Verteilung der Energie an die Stellen, an denen sie gebraucht wird, ist ein zentrales Thema der sog. Energiewende, welches über den Aufbau eines Smart Grids gelöst werden soll. Im Smart Grid sind Verteilnetze, Verbraucher und Erzeuger kommunikationstechnisch vernetzt und tauschen regelmäßig Zustandsdaten aus.

Die Datensicherheit des Verbrauches spielt dabei eine entscheidende Rolle, so dass das Bundesamt für Sicherheit in der Informationstechnik frühzeitig technische Richtlinien herausgebracht hat, die Mindestanforderungen an das Smart Meter Gateway beschreiben, welches im Privathaushalt Verbrauchs- und Erzeugerdaten zentral sammelt und verarbeitet. Die Datensicherheit soll durch verschiedenste Maßnahmen sichergestellt werden.

Diese Arbeit beschäftigt sich mit den grundlegenden Maßnahmen zur Realisierung der Datensicherheit eines Smart Meter Gateways und beschreibt die Umsetzung in der technischen Richtlinie. Ein besonderer Fokus wird auf die Transportsicherheit auf der Weitverkehrsnetz-Schnittstelle gelegt, welche durch TLS 1.2 unter Einsatz einer eigenen Smart-Metering-Public-Key-Infrastruktur realisiert werden soll.

Außer einer Beschreibung der speziellen Anforderungen der technischen Richtlinie an TLS, Zertifikate, Public-Key-Infrastruktur und zum Einsatz kommender Algorithmen und Cipher Suites wird auch auf das Zusammenspiel zwischen TLS-Verbindungsaufbau und Sicherheitsmodul eingegangen. Ausgehend von einem Softwarekonzept für die praktische Umsetzung der Sicherheitsarchitektur auf der Transportschicht, wird gezeigt, wie mit Open-Source-Komponenten erste Experimente und prototypische Umsetzungen einzelner Aspekte der Transportschichtsicherheit realisiert werden können und wie eine vorhandene TLS-Funktionsbibliothek an die speziellen Anforderungen der technischen Richtlinie angepasst werden kann.