Elektromobilität durch Interoperable und Sichere Architekturen

Digitale Vernetzung und IoT-Fortschritte machen herkömmliche Vertrauenskonzepte überflüssig. Die steigende Nachfrage nach Smartphone-Zugang zu Fahrzeugen führt zu nicht interoperablen Apps. Der digitale Schlüssel des Car Connectivity Consortium (CCC) bietet eine universelle, sichere Lösung für die Speicherung und gemeinsame Nutzung digitaler Schlüssel. Diese standardisierte Technologie gewährleistet den Zugang zum Fahrzeug auch bei niedrigem Akkustand des Telefons und stellt Komfort, Sicherheit und Datenschutz in den Vordergrund. Im Bereich der Datensicherheit ist die Einrichtung einer Public-Key-Infrastruktur (PKI) für die sichere Kommunikation zwischen Fahrzeugen und Ladeinfrastruktur unter Einhaltung der ISO 15118-Normen von entscheidender Bedeutung. Um eine gleichberechtigte Teilnahme zwischen den Marktrollen zu gewährleisten, müssen Organisationen, die PKI anbieten, als vertrauenswürdige Zentren auf dem Markt fungieren.

Eckdaten

Kurztitel

ELISA

Forschungsschwerpunkt

Sustainable Production, Energy Technologies and Smart Materials

Laufzeit

01.07.2023 - 30.06.2026

Fördergeber

Bundesministerium für Wirtschaft und Klimaschutz

Projektträger

TÜV Rheinland Consulting GmbH

Ziele

Übergeordnetes Ziel für das Projekt ELISA ist es, den gestiegenen Anforderungen an die Cybersicherheit gerecht zu werden und einen Sicherheitsansatz für das Fahrzeugnetzwerk im Sinne einer Zero Trust Architecture (ZTA) zu entwickeln. Das dafür notwendige digitale Schlüsselmaterial wird durch ein im Fahrzeug integriertes Schlüsselmanagementsystem auf Basis eines Trusted Platform Module 2.0 (TPM) nach dem Standard (ISO/IEC11889) als Ausgangspunkt für vertrauenswürdige Anwendungen in den Bereichen Laden von E-Fahrzeugen nach IEC /ISO15118-20, Carsharing und Car Access verwaltet. Die genannten Anwendungen werden im Rahmen von ELISA im Detail betrachtet und in Form von konkreten Lösungen umgesetzt. Um eine solche Anwendung zu schützen, ist ein sicherer Bootvorgang der beteiligten Hardwarekomponenten erforderlich, der deren Authentizität und Integrität garantiert.

Finanziert von der Europäischen Union NextGenerationEU
Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages