

STIP

Secured Trustworthy IoT Platform

Programm / Ausschreibung	COIN, Kooperation und Netzwerke, COIN Netzwerke 10. Ausschreibung	Status	abgeschlossen
Projektstart	01.10.2018	Projektende	31.12.2020
Zeitraum	2018 - 2020	Projektlaufzeit	27 Monate
Keywords	Security, Privacy, Trust, Identification, NFC		

Projektbeschreibung

“Secured Trustworthy IoT Platform” (STIP) adressiert den Aufbau eines offenen Technologieframeworks für IoT-Lösungen um den Einsatz neuer Anwendungen und Services zu ermöglichen, welche durch Technologiebarrieren wie unzureichende Sicherheit in der Kommunikation und Datenzugriff, komplexes Privacy Management, oder mangelnde Interoperabilität durch eine Vielzahl von Standards erschwert wird. Durch Fokussierung auf Hardware Security, sichere Nutzeridentifikation, Skalierbarkeit und ein offenes Framework behandelt STIP alle Ebenen einer IoT-Lösung von sicherer Hardware, dem Embedded Controller, der FW/SW bis zur Applikationsschicht. Ein „Open Innovation Ansatz“ wird ein Netzwerk von rund 100 Partnern aus Forschung, KMU’s und Industrieunternehmen einbinden um neue Produkte, Verfahren und Dienstleistungen auf Basis der STIP Plattform zu ermöglichen, und wird ebenso die Vernetzung innerhalb der Wertschöpfungskette verbessern.

Sichere Hardware (NXP, TUG): Bei IoT-Geräten sind auf dem Gerät gespeicherte Geheimschlüssel die Basis für abhörsichere Kommunikation zwischen Sensoren, Gateways und einem Cloud-System. Für kryptographische Operationen werden Secure Elements auf dem Chip als „Root-of-Trust“ verwendet. Um möglichst viele unterschiedliche Anwendungen zu unterstützen, ist ein flexibles System erforderlich, das die benötigten Daten erzeugt. STIP untersucht Methoden, die zur Erstellung komplexer Produktkonfigurationen auf Basis von Applikationsanforderungen eingesetzt werden.

Embedded Controller, FW/SW (CISC, TUG): Hohe Verfügbarkeit und einfache Wartbarkeit sind zentrale Anforderungen an IoT Lösungen. STIP wird Methoden entwickeln, um Verfügbarkeit, Vertraulichkeit und Integrität für eine sichere Kommunikation zwischen Embedded Controller und heterogenen Clouds zu gewährleisten. Auf Applikationsebene ist ein neuartiges Integrity-Management-Konzept nötig, um das Zusammenspiel von Service Provider über Unternehmensgrenzen und Anwendungsgebiete hinweg sicher zu stellen. Dieses generische Konzept ermöglicht dem Benutzer Zugriff auf Services, Dienstleistungen oder Berechtigungen, die von verschiedensten Anbietern mit derselben Technologie bereitgestellt werden können.

Anwendungsebene (IOT40, trinitec): Für eine sichere preventive Fernwartung zur rechtzeitigen Erkennung kritischer Situationen, wird die Cloud-Lösung die gesammelte Sensordaten analysieren um entsprechende Steuerungsaktionen von

Smart Services bis zum Eingriff in das System automatisch auszulösen. Basierend auf den gesammelten und aggregierten Sensordaten werden ausgewählte Data-Mining-Algorithmen angewendet, um die intrinsischen Informationen in (mobile) Bedien- und Managementsysteme zu extrahieren.

Open Innovation (SAC): Eine zielgerichtete „go-to-market“ Strategie realisiert durch frühe Ausrichtung auf konkrete Anwenderbedürfnisse wird mit Veröffentlichungen, Lead-User Informationsevents oder CoCreation-Workshops innerhalb des SAC Partnernetzwerks (ca. 100 Partner) umgesetzt.

Projektkoordinator

- CISC Semiconductor GmbH

Projektpartner

- NXP Semiconductors Austria GmbH & Co KG
- IoT40 Systems GmbH
- Silicon Alps Cluster GmbH
- Technische Universität Graz
- trinitec IT Solutions & Consulting GmbH