White Paper

Schutz für Interaktionen im Industrial Internet of Things (IIoT)

Autoren: Anthony Fitze, Carl Fenger, LEGIC Identsysteme AG

Das Vertrauen in IIoT-Daten beruht darauf, verifizierte Nutzer mit vertrauenswürdigen Sensoren und Objekten zu verbinden, damit ihre Interaktionen zuverlässig, transparent und nachvollziehbar sind.

Zusammenfassung

Abstract: Das IIoT verspricht, Prozesse zu optimieren, Kosten zu senken, Qualität, Sicherheit, Verantwortlichkeit (Nachvollziehbarkeit) und Serviceverfügbarkeit zu verbessern. Das Erreichen dieser Ziele hängt davon ab, ob eine IoT-Plattform die Verantwortlichkeit der Benutzer unterstützen kann, indem sie ihre Interaktionen mit Sensoren, Anlagen und Infrastrukturen absichert. Nur so können zuverlässige, transparente und überprüfbare Geschäftsprozesse erreicht werden. «Security by Design» schafft Vertrauen und kann durch Mobile Credentialing-, Managed Encryption- und Secure Element-Technologien realisiert werden.

Das Industrial Internet of Things absichern

In industriellen Umgebungen führen der massenhafte Einsatz von Sensoren und die Möglichkeit, Daten von festen und mobilen Anlagen zu erfassen und zu verarbeiten, zu einer erheblichen Effizienzsteigerung und letztendlich zu besseren geschäftlichen Entscheidungen. Damit werden die Optimierung von Prozessen, die Verringerung von Fehlern, die Unterstützung von Audits und die Durchsetzung von Qualitätskontrollen erleichtert, die andernfalls auf Ad-hoc- oder statistischer Stichprobenbasis durchgeführt würden.

Der gemeinsame Nenner: Vertrauen

Es reicht nicht aus, Sensoren einfach mit dem Internet zu verbinden. Die Funktionsfähigkeit der durch das «industrielle Internet der Dinge» verbesserten Prozesse hängt von einem gemeinsamen Nenner ab: Vertrauen. Wenn den Daten, Sensoren und den Menschen, die auf sie zugreifen, sie konfigurieren und warten, nicht vertraut werden kann, verlieren IIoT-Implementierungen ihre Wirksamkeit. Wenn kein Vertrauen in Benutzer, Sensoren/Objekte und ihre Interaktionen gesetzt werden kann, können die Ergebnisse irreführend, kostspielig und sogar katastrophal sein. Das gilt insbesondere in Umgebungen, in denen wertvolle oder unbeständige Güter und die Sicherheit von Menschen betroffen sind, was häufig der Fall ist.

Die drei Säulen des Vertrauens im industriellen IoT (IIoT)

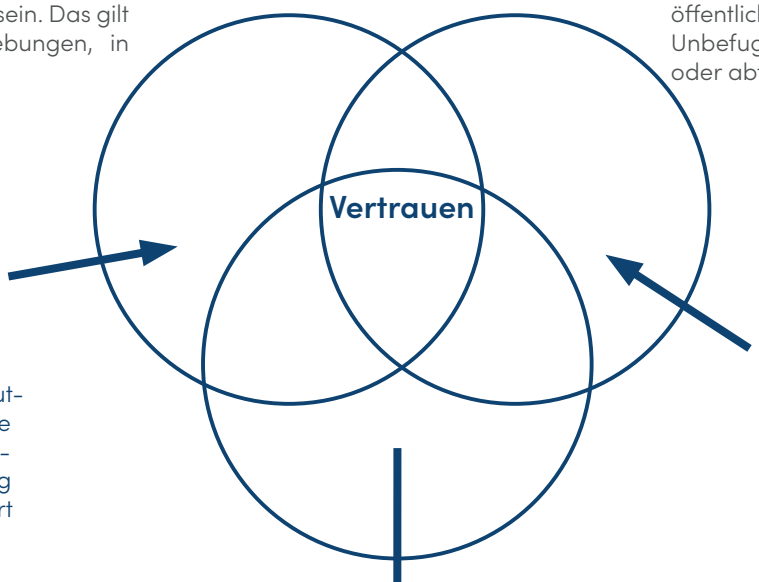
Das Vertrauen in IIoT-Daten beruht darauf, verifizierte Nutzer mit vertrauenswürdigen Sensoren und Objekten zu verbinden, damit ihre Interaktionen zuverlässig, transparent und nachvollziehbar sind. Die Verwirklichung dieses Ziels beruht auf den folgenden drei Grundsätzen:

1. Verantwortlichkeit:

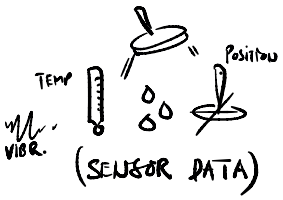
Benutzer in einer IIoT-Umgebung müssen identifizierbar und damit zur Verantwortung zu ziehen sein, bevor sie Zugang zu Sensoren oder Infrastrukturen erhalten. D.h. alle Aktionen müssen jederzeit nachvollziehbar sein. Die Zugriffsberechtigungen müssen dann zugewiesen werden auf der Grundlage der Rolle der Benutzer, ihrer Ausbildung und der damit verbundenen Berechtigung sowie kontextbezogener Kriterien wie Zeit, Standort, Umgebungsdaten und anderer Attribute, die zur Unterstützung und Sicherung des Betriebs erforderlich sind. Berechtigungen müssen autonom durchgesetzt werden, sowohl online als auch offline, um menschliche Fehler zu minimieren und einen zuverlässigen Betrieb rund um die Uhr zu unterstützen. Alle Nutzeraktivitäten müssen transparent, nachvollziehbar und überprüfbar sein..

2. Sicherheit: Die Konfiguration von Geräten darf nur durch befugte Benutzer möglich sein, und der Zugang darf nur diesen gestattet sein. Die Geräte müssen auch gegen Spoofing resistent sein. Da es sich bei Sensoren um die exponierteste und damit anfälligste Komponente eines IIoT-Systems handelt, muss die Sicherheit auf physischer Hardware-Ebene in Form eines integrierten Secure Elements für das Hosting von Verschlüsselungscodes und Benutzerberechtigungen implementiert werden.

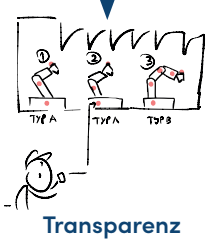
3. Transparenz: Die Interaktionen zwischen Nutzern und Geräten und die von ihnen erzeugten Daten müssen vertrauenswürdig und für validierte Nutzer transparent sein. Sie dürfen weder am Sensor noch in LANs, über Luftschnittstellen oder über das Netz, einschliesslich des öffentlich zugänglichen Internets, für Unbefugte sichtbar, manipulierbar oder abfangbar sein.



Nachvollziehbarkeit
Vertrauenswürdige Benutzer werden über mobile Credentials und biometrische Authentifizierung verifiziert und autorisiert



Sicherheit
Sensoren sind kryptografisch über ein Secure Element gesichert und der Zugriff ist auf vertrauenswürdige, berechtigte Benutzer beschränkt



Transparenz
Sensordaten und Nutzerinteraktionen sind vertrauenswürdig, transparent, zuverlässig und durch verwaltete End-to-End-Verschlüsselung geschützt

Säule 1: Verantwortlichkeit
Um Verantwortlichkeit zu erreichen, müssen alle, die ein IIoT-System nutzen, verifiziert werden. Das schafft Vertrauen. Die Zugriffsrechte auf Bereiche, Maschinen, Funktionen, Fahrzeuge, Informationen und Lager müssen auf der Grundlage der Credentials der vertrauenswürdigen Benutzer erteilt werden. Mit den Credentials kann festgelegt werden, wo und wann sich Benutzer aufhalten dürfen, welche Maschinen und deren Funktionen je nach Ausbildung und Funktion genutzt werden dürfen, welche Schliessfächer und Lagerbehälter geöffnet werden dürfen usw.

Die Benutzer wechseln regelmässig – täglich kommen und gehen Mitarbeitende, wechseln die Funktion oder absolvieren Trainings. Externe Mitarbeitende wie Auditoren oder Auftragnehmer benötigen zeitlich befristete Ad-hoc-Credentials. Berechtigungen müssen daher in Echtzeit und Over-the-Air erstellt und neu konfiguriert werden können. Das System für Berechtigungen muss sowohl im Online- als auch im Offline-Modus funktionieren, da Netzwerkverbindungen nicht immer verfügbar oder zuverlässig sind.

Zu den wichtigen Systemanforderungen gehören Echtzeitaktualisierung von Credentials sowie das Hinzufügen und Entfernen von Mitarbeitenden per Knopfdruck. All dies kann durch eine Mobile App auf Geräten wie iOS-/ Android-Smartphones oder -Tablets unterstützt werden.

Säule 2: Sicherheit
Vertrauenswürdige Daten dürfen nur von vertrauenswürdigen Geräten

	Datenzugriff				Zugriff auf Infrastruktur								Gerätezugriff				
	Logistiksystem	Verwaltungsakten	Steuerung der Fertigungslinie	Abrechnungs-/Finanzsystem	Haupteingang des Werks	Produktionsbereiche	Fertigungsmaschinen	Logistik-/Lagerbereiche	Kantine	Verwaltungsbüro	Versorgungsraum	Serverraum	Produktionskontrolle	Logistikmaschinen	Überwachungsgeräte	Lager-/Versandbehälter	Heizung/Lüftung/Klimaanlagen
Betriebsleitung	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
CFO	x	x		x	x	(x)		x	x	x	x						
Bedienung	(x)		x		(x)	x	x		x	x			(x)	(x)	(x)		
Service/IT	x		(x)	(x)	x	(x)	(x)	(x)	x		(x)	x	(x)			(x)	x
Qualitätskontrolle	(x)		(x)		x	(x)	(x)	x	x		x	(x)	(x)	(x)	x		
Audits*	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)		(x)	(x)	(x)	(x)	(x)	(x)	
Reinigung*					(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)				(x)	(x)

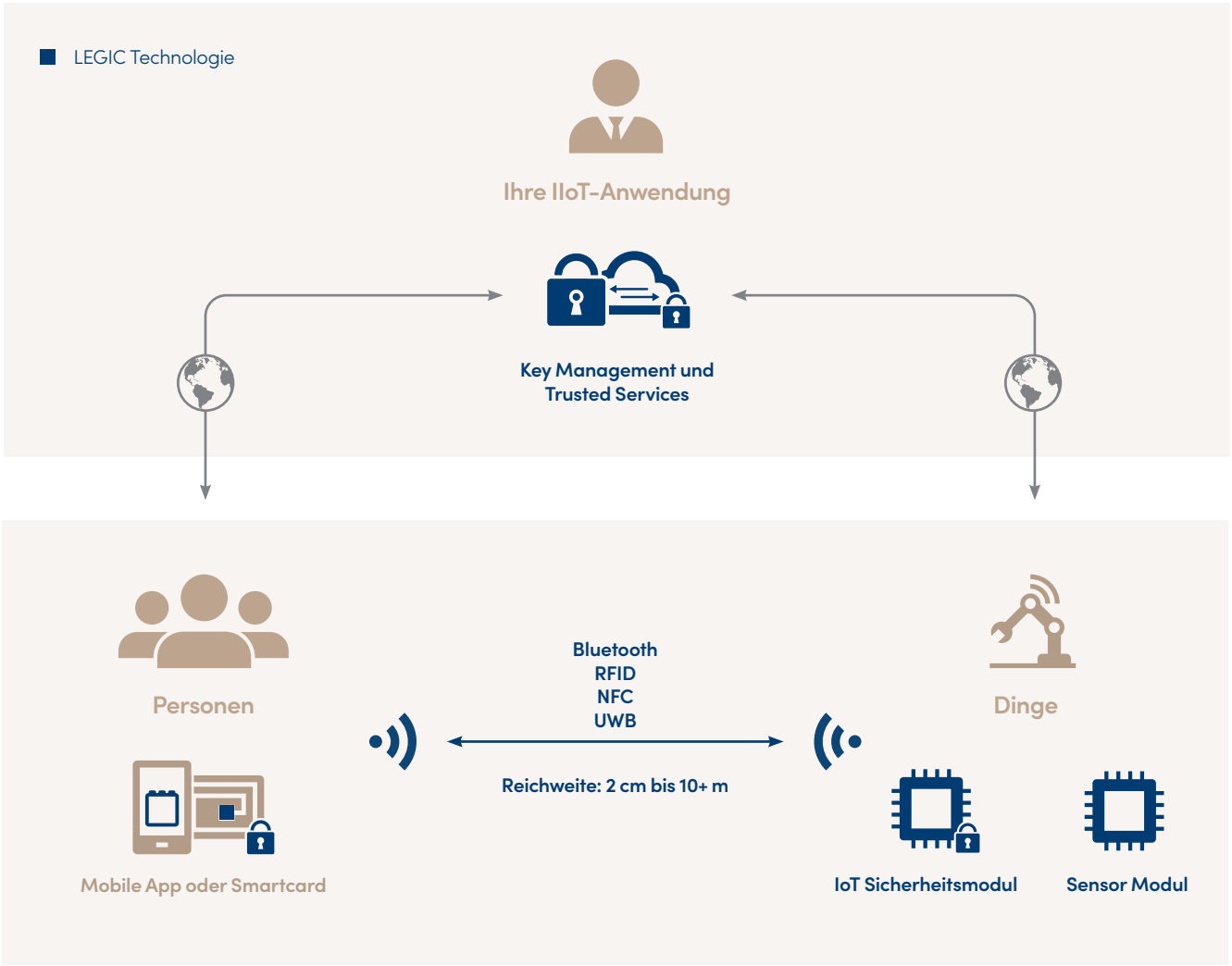
(x) = Bedingter Zugriff (z. B. abhängig von Tageszeit, verfügbarer Funktionalität)
* = Externe Dienstanbieter

Beispiel für vertrauenswürdige Benutzer: Verwaltung des Zugangs zu Maschinen, Infrastruktur und Informationen auf der Grundlage von Benutzer-Credentials

Security by Design: LEGIC Connect, die mobile Credentialing-Plattform für IIoT-Systembenutzer

LEGIC Connect ist eine mobile Credentialing-Plattform, die mobile Berechtigungen oder andere Daten jederzeit, überall und sofort auf Knopfdruck sicher an registrierte Smartphones oder Tablets verteilt. Das System bietet einen weltweit verfügbaren, sicheren, durchgängigen mobilen Credentialing-Dienst. Er bildet die Grundlage für die Schaffung von Vertrauen und Verantwortlichkeit bei Interaktionen zwischen Benutzern, Geräten und Infrastruktur. Das System lässt sich problemlos in die bestehende industrielle Infrastruktur integrieren und gibt Betreibern von IIoT-Diensten die Möglichkeit, Benutzerberechtigungen zu verwalten sowie Daten sicher von Smartphones und Sensoren zu senden und auf ihnen zu empfangen.

LEGIC Connect schützt Infrastruktur, Daten und Credentials vor Manipulation, ermöglicht einen vollautomatischen Betrieb und bietet Transparenz durch transaktionsbasierte Daten, die von vertrauenswürdigen Benutzern, Geräten und Infrastruktur-Touchpoints gesammelt werden können. Details zur LEGIC Connect-Plattform für mobile Credentials finden Sie unter https://www.legic.com/de/sicherheitsplattform/legic-connect.



LEGIC IIoT Security Platform: auditierbare Transparenz via vertrauenswürdige Benutzer + vertrauenswürdige Sensoren

stammen, die gegen Manipulation abgesichert sind. Da bei typischen IIoT-Implementierungen tausende von Geräten involviert sein können, die über grosse Gebiete verteilt sind, stellen Implementierung und Konfiguration eine Herausforderung dar.

Die Verwaltung und das Lesen müssen einfach, schnell und kostengünstig sein. Ein einfaches Upgrade von Geräten ist ebenfalls wichtig, da viele bestehende Industrieanlagen schnell nachgerüstet werden müssen.

- **Alle Daten, die von den Geräten kommen und an sie gehen, müssen geschützt werden.** Es muss die höchste kommerziell verfügbare Verschlüsselungsstufe wie AES (Advanced Encryption Standard) eingesetzt werden.
- **Die Verschlüsselungscodes müssen während der Initialisierung unsichtbar und während des Betriebs unzugänglich sein.** Da Daten zunehmend von Edge Devices generiert werden, die von Natur aus physisch anfällig für Manipulationen sind, müssen Schlüssel und andere sensible Daten in einem physisch und elektronisch unzugänglichen, in das Gerät integrierten Secure Element gespeichert werden. Während der Initialisierung des Geräts dürfen die Verschlüsselungscodes weder im Speicher noch bei der Übermittlung für Menschen lesbar sein.
- **Ein Spoofing der Infrastruktur muss unmöglich sein** (z. B. durch einen Sensor, der böswillig durch einen manipulierten Sensor ersetzt wurde). Ein einzigartiger, unsichtbarer Verschlüsselungscode, der in ein Secure Element im Sensor integriert ist, verhindert dies: Ohne diesen Schlüssel kann der Sensor weder auf externe Befehle reagieren noch fehlerhafte Daten melden.
- **Ein kontaktloser Zugang ist unerlässlich.** Da die Geräte oft in schwer zugänglichen Bereichen installiert sind, ist eine verschlüsselte Wireless-Konfiguration und Auslesung über RFID, Bluetooth Low Energy oder NFC per Smartphone erforderlich.
- **Firmware-Update Over-the-Air ist erforderlich.** Die Konfiguration und Aktualisierung der Geräte vor Ort, einschliesslich der Installation von Verschlüsselungscodes über das Netzwerk oder per Smartphone, muss möglich sein. Eine werksseitige Programmierung sollte vermieden werden, um die Implementierungs- und Logistikkosten niedrig zu halten. Da damit keine Fremdhersteller

Security by Design: Vertrauenswürdige Sensoren von LEGIC mit Secure Element

Das LEGIC XDK Secure Sensor Evaluation Kit stellt gewissermassen das «Schweizer Taschenmesser der IoT-Lösungen» dar. Es handelt sich um ein universelles, programmierbares Sensorgerät und eine Prototyping-Plattform für jeden denkbaren IoT-Anwendungsfall.

TextfeldAusgestattet mit einem Sicherheitsmodul mit integriertem Secure Element für die Speicherung von kryptografischen Schlüsseln/Whitelists und drahtloser Kommunikation, ermöglicht es das schnelle Prototyping von hochsicheren, berührungslosen, sensorbasierten Produkten und Anwendungen und bietet Entwicklern die Freiheit, schnell einfache bis hochentwickelte IoT-Lösungen zu erstellen.

- All-in-One-Sensor-Kit: keine Auswahl von Komponenten, kein Zusammenbau von Hardware und keine Implementierung eines Echtzeitbetriebssystems erforderlich
- Fertiglösungen für die Protokollierung Ihrer Daten
- Enthält Beschleunigungsmesser, Gyroskop, Magnetometer, Umgebungssensoren (Luftfeuchtigkeit, Temperatur, Luftdruck), Umgebungslicht und ein Mikrofon zur Geräuscherkennung sowie WLAN, Bluetooth® Low Energy und einen SD-Karten-Slot
- Softwarebeispiele und Entwicklungs-APIs enthalten

LEGIC XDK Secure Sensor Evaluation Kit with LEGIC Security Module and Secure Element

beteiligt sind, erhöht dies ausserdem die Sicherheit.

- **Die Geräte und der Zugang zu ihnen müssen sowohl online als auch offline funktionieren.** Das System muss auch dann funktionieren, wenn keine Netzwerkverbindung verfügbar ist, um einen soliden und zuverlässigen Betrieb sicherzustellen.

- **Die Geräte müssen modular sein, serienmässig zu produzieren und ohne Vorkonfiguration einfach zu implementieren sein.** Dadurch werden die Lieferketten für Geräte rationalisiert und die Möglichkeiten der Manipulation oder Verfälschung von Geräten während der Herstellung minimiert. Es ermöglicht auch einfachere anwendungs- oder kundenspezifische Konfigurationen vor Ort, während der Administrator der IoT-Implementierung unabhängig von den Gerätelieferanten agieren kann.

Säule 3: Transparenz
Wenn das Vertrauen in die Verantwortlichkeit der Benutzer und die Sicherheit der Geräte hergestellt ist, wird systemweite Transparenz erreicht, da verifizierte Benutzer sicher Daten von vertrauenswürdigen Geräten über ein verschlüsseltes Netzwerk zur Verarbeitung durch ein Managementsystem sammeln oder verwalten. IIoT-Implementierungen bestehen aus Geräten, die über ein weites geografisches Gebiet verteilt sind oder in mobilen Fahrzeugen oder Containern installiert sind, welche sich überall befinden können. So ist es von entscheidender Bedeutung, dass den Daten vertraut werden kann, während sie verschiedenste Mobilfunk- und lokale Netzwerkverbindungen durchlaufen.

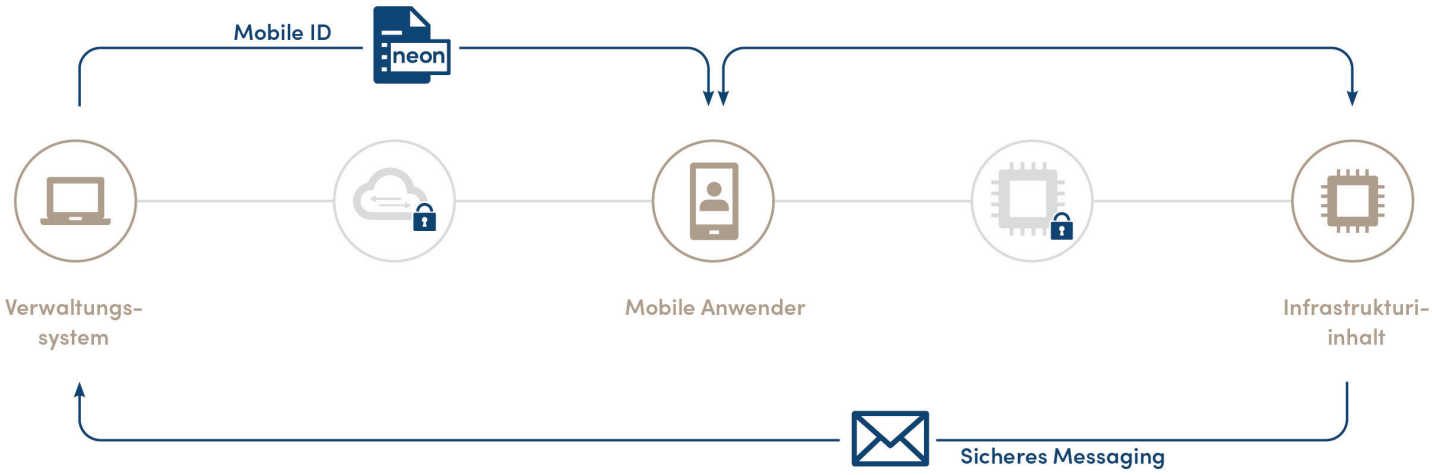
Da kein Netzwerk, weder ein privates noch ein öffentliches, zu 100% gegen das Abfangen von Daten geschützt werden kann, muss eine Ende-zu-Ende-Verschlüsselung eingesetzt werden. Die verwaltete AES-Verschlüsselung ist das leistungsfähigste, kommerziell erhältliche Verschlüsselungsprotokoll. Wird sie genutzt, ist Hacken nutzlos, selbst bei Netzwerken, die für das Abfangen von Daten anfällig sind. Die Nutzdaten in jedem Datenpaket können nämlich ohne den Verschlüsselungscode nicht gelesen werden. Die Schlüssel dürfen weder bei der Übermittlung noch im Speicher sichtbar sein.

Sicherer Gatekeeper am IIoT-Rand
Mit einer kryptografisch sicheren End-to-End-IIoT-Plattform, die auf Mobile Credentialing-, Managed Encryption- und Secure Element-Technologien basiert, lassen sich Verantwortlichkeit, Sicherheit und Transparenz erreichen. Dynamisch aktualisierbare Benutzer-Credentials können mit standort- und anderen kontextbezogenen Informationen wie Sensordaten kombiniert werden, um Aufgaben einfacher, effizienter und sicherer zu machen und gleichzeitig die Prozessqualität, Integrität, Verantwortlichkeit und den Komfort zu verbessern.

Einige spezifische Anwendungsfälle:

- **Automatisierung der Logistik:** Eine vertrauenswürdige IIoT-Plattform ermöglicht eine sichere und transparente Bewegung von Waren sowohl innerhalb von als auch zwischen Einrichtungen. Dazu sichert sie den Zugang und protokolliert Interaktionen und Zustände während des Transports. Für die Authentifizierung können Smartcard- oder Smartphone-Credentials verwendet werden. Der autorisierte Transport von Waren innerhalb einer Einrichtung wird durch Systeme für die Positionierung in Innenräumen weiter verbessert (siehe Anwendungsfall «Kombination eines UWB-RTLS (Real Time Locating System) mit sicherer Transporteur-Authentifizierung»).

- **Gebäudeverwaltung:** Die Verknüpfung von Personen



LEGIC Orbit: Sicheres Schlüssel- und Berechtigungsmanagement

Security by Design: LEGIC Orbit ermöglicht systemweite Datensicherheit und Transparenz

Basierend auf einer verwalteten End-to-End-AES-Verschlüsselung ermöglicht Ihnen LEGIC Orbit die sichere Konfiguration Ihrer IIoT-Lösungen. LEGIC Orbit sichert die Credentialing-Technologie von LEGIC, die das Herzstück Ihrer mobilen IIoT-Lösung darstellt. Es schützt auch das Messaging in umgekehrter Richtung: von Ihren Sensormodulen zu Ihrem IIoT-Managementsystem.

LEGIC Orbit: Secure key and authorization management

Einzelheiten zur sicheren Implementierung von Schlüsseln und Konfigurationsdaten für Sensoren und Infrastruktur finden Sie unter LEGIC Orbit: Schlüssel- und Berechtigungsmanagement.

mit einer verifizierten Identität ermöglicht eine vertrauenswürdige Überwachung von Gebäudeanlagen und Interaktionen zwischen Nutzern und Türen, HLK-Systemen (Heizung, Lüftung, Klima), Sicherheitssystemen, Feueralarmen, Indoor-Navigationssystemen usw. Standortgesteuerte automatisierte Prozesse können auf der Grundlage der Benutzeridentität implementiert und über zentralisierte, digital verteilte Zugriffsrechte und Berechtigungen verwaltet werden.

- **Industrieanlagen:**
  Die Verknüpfung von Personen mit einer verifizierten Identität, gefolgt von einer dynamischen Erteilung von Berechtigungen und dem Zugang zu Geräten sorgt für vertrauenswürdige Interaktionen und Verantwortlichkeit. Industrieanlagen können zuverlässig geortet, identifiziert und überwacht werden. Die protokollierten Daten zur Gerätenutzung lassen sich pro Benutzer erfassen. Die Erteilung und Einschränkung von Berechtigungen kann in Echtzeit und Over-the-Air erfolgen.

- **Hotelbranche:**
  Hotelzimmer buchen und einchecken per Smartphone. Die Gäste laden virtuelle Schlüssel herunter und haben keinen Zeitaufwand an der Rezeption mehr, sondern gehen direkt auf ihr Zimmer. Indoor-Navigation über UWB führt die Gäste an ihr Ziel. Mit dem Schlüssel werden digitale Credentials heruntergeladen. Auf der Grundlage der darin gespeicherten Präferenzen können massgeschneiderte Angebote auf das Smartphone der Gäste gesendet werden (siehe Anwendungsfall «Smartphone statt Schlüssel – Mobile Access zum Hotelzimmer bei Village Hotels UK»).

Die LEGIC IIoT-Sicherheitsplattform wird als vertrauenswürdige Sicherheitsplattform implementiert, die Verantwortlichkeit, Sicherheit und Transparenz bietet. Sie kann in jede Anwendung und in jede Infrastruktur integriert werden. Die Bereitstellung sicherer, verwalteter Kryptografie in Kombination mit Secure Element-Technologie, mobilem Credentialing und Bluetooth-, NFC-, WLAN- oder RFID-Funkkommunikation dürfte mit die sicherste Lösung mit bestmöglichem Schutz für lebenswichtige und geschäftskritische IIoT-Systeme darstellen.

Weitere Details zur Implementierung von vertrauensbasierten IIoT-Sensoren und -Systemen finden Sie unter www.legic.com/de/anwendungsbereiche/iot

Über LEGIC

Seit über 30 Jahren ermöglicht LEGIC Unternehmen aus aller Welt die Implementierung von Lösungen mit anspruchsvollen Sicherheitsanforderungen. Auf der Grundlage von Schlüsselverwaltung, Trusted Services und sicheren, kontaktlosen Halbleitern bietet die LEGIC-Sicherheitsplattform End-to-End-Sicherheit für Smartphone- und Smartcard-basierten Zugriff, Mobilität, gemeinsam genutzte Ressourcen und industrielle IoT-Anwendungen.

LEGIC

LEGIC Identsystems AG
Schweiz Telefon +41 44 933 64 64 info@legic.com www.legic.com

Januar 2022 Autoren: Anthony Fitze, Carl Fenger