

Sichere Bereitstellung von Komponenten in beliebigen Datenplattformen

Mit der Softwarelösung KEYNOA wird ein automatischer Prozess zur sicheren Installation und Konfiguration von Geräten in beliebigen IoT-Clouds und On-Premises-Datenplattformen ermöglicht. Dafür nutzt das Startup DEVITY asymmetrische Public-Key-Kryptographie als Basis für eindeutige Geräteidentitäten und eine verschlüsselte Datenkommunikation.

Als Hochschulausgründung, die 2020 aus der Universität Paderborn entstanden ist, hat DEVITY eine Möglichkeit entwickelt, IIoT-Geräte mit eindeutigen Identitäten in IoT-Plattformen einzubinden. Dank eines Enrollment-Service kann deren Bereitstellung schnell, einfach und sicher vorgenommen werden, ohne dass bestehenden Entwicklungs- und Fertigungsprozesse gestört werden. Dadurch kann geistiges Eigentum geschützt und Prozesse können flexibel gesteuert werden.

Für ein produzierendes Unternehmen hat DEVITY zusammen mit der Janz Tec AG, einem Spezialisten für industrielle IoT-Lösungen, mit KEYNOA ein IoT-Gateway unter Beachtung der IEC 62443, einer internationalen Normenreihe über „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“, entwickelt.

Die Idee einer Kooperation mit Janz Tec entstand durch einen gemeinsamen Prototyp, der im Zuge eines universitären Kundenprojektes entwickelt wurde. „Durch die Bündelung von Kompetenzen im Bereich Hardware und der forschungsnahen IT-Sicherheit ergeben sich durch die Zusammenarbeit starke Synergien für Kunden in der industriellen Automatisierung“, erklärt Ulrich Lütke Entrup, Senior Key Account Manager bei Janz Tec.

Installation und Konfiguration als Herausforderung

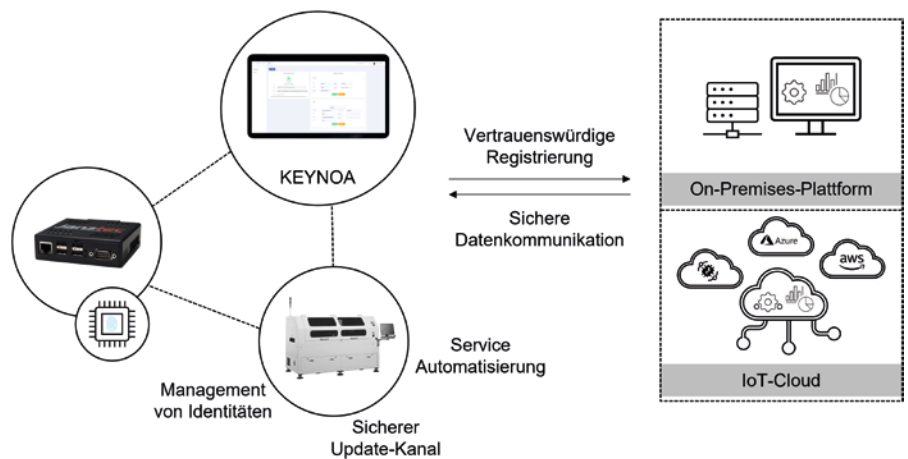
Um Sensoren, Steuerungen und Maschinen in Industrieanwendungen nutzen zu können, ist zunächst eine Bereitstellung erforderlich – das heißt, alle Komponenten müssen installiert und eingerichtet werden, um mit einer IoT-Datenplattform (Cloud oder On-Premises) kommunizieren zu können. Bislang erfolgt dieser Prozess in der Regel manuell durch einen Facharbeiter, was jedoch langsam, teuer und unsicher ist.

Alternativ können die Geräte vom Hersteller vorkonfiguriert werden, um Informationen mit einer Zieldatenplattform auszutauschen. Dafür müssen die Gerätehersteller allerdings bereits während der Produktion wissen, wer

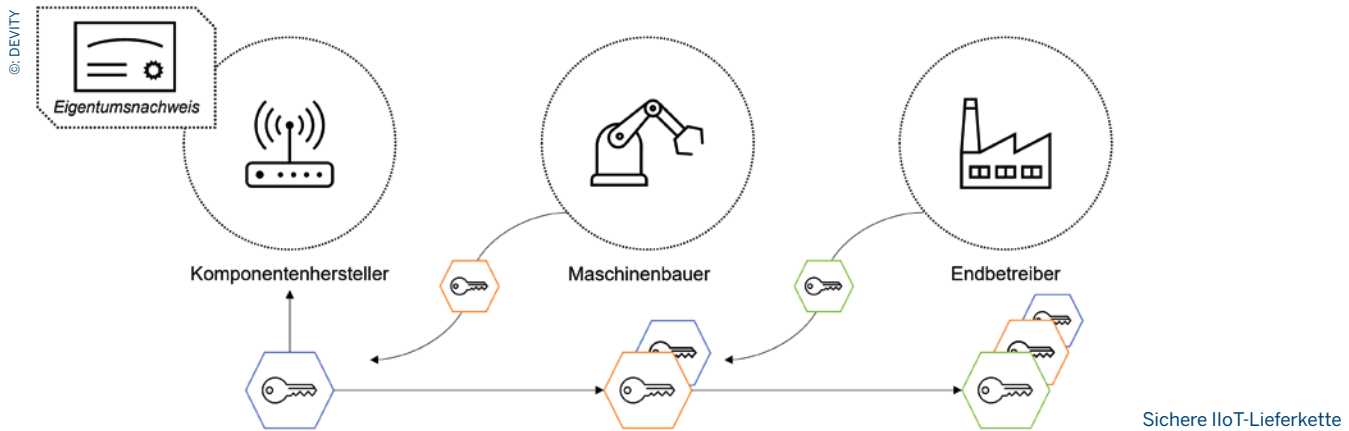
der Endbetreiber sein wird und mit welchen Systemen dieser arbeitet. Dieser Aufwand ist oftmals nur wirtschaftlich, wenn der Kunde große Mengen abnimmt, da gleichzeitig die Lieferkette komplexer wird. Zudem ergeben sich in der industriellen Lieferkette aufgrund einer fehlenden Standardisierung uneinheitliche Methoden für die IT-Sicherheit von Maschinen und Anlagen. Die IEC 62443 bietet im Industriebereich eine wichtige Grundlage für eine gemeinsame Richtlinie.

Security by Design

Schon bei der Produktion wurde auf einem industriellen IoT-Gerät, in diesem Fall einem Raspberry Pi3+ von Janz Tec, die Softwarelösung KEYNOA installiert. Die Software sorgt dafür, dass eine



DEVITY Lösungskonzept



eindeutige Identität erzeugt wird, die kryptografisch gebunden ist und dem Gerät eindeutig zuordenbar ist. Diese Identität attestiert die Integrität des Geräts innerhalb der Lieferkette und bietet die notwendige Grundlage für den automatischen Bereitstellungsprozess.

Um die Identität hardwarebasiert zu sichern, wurde ein Trusted Platform Module (TPM) eingebaut. Vor der Versendung wird außerhalb des Geräts ein digitaler Eigentumsnachweis erstellt. Mit diesem digitalen Dokument kann sich der Besitzer des Geräts später im Bereitstellungsprozess ausweisen. Den Eigentumsnachweis erhält der Besitzer über die KEYNOA beim Kauf der Hardwarelösung von Janz Tec. Anschließend kann der Kunde wichtige Konfigurationen für den Betrieb und die IoT-Datenplattform für die bestellten Geräte über KEYNOA definieren. Änderungen können auf der KEYNOA-Weboberfläche – auch ohne vorheriges Auspacken des Geräts – vorgenommen werden. Gleichzeitig können die Einstellungen für alle bestellten Geräte simultan als Flotte definiert werden, sodass der beschriebene Prozess nur einmal durchlaufen werden muss.

Ablauf der Bereitstellung der IoT-Geräte

Zu Beginn des Bereitstellungsprozesses verbinden sich die Geräte mit dem

Netzwerk. Die Geräte identifizieren sich gegenüber KEYNOA und die Software ordnet diese wiederum ihrer Zieldatenplattform zu. Im Gegenzug authentifiziert sich die Zieldatenplattform mit dem Eigentumsnachweis als Eigentümer der Geräte. So wird ein gesicherter, verschlüsselter Kanal zwischen dem Gerät und der Cloud bzw. On-Premises-Instanz etabliert, über den die benötigten Zugangsdaten oder Konfigurationen heruntergeladen werden können. Das lohnt sich vor allem, wenn viele Geräte installiert werden sollen und Endkunden unterschiedliche Plattformen für die Datenauswertung nutzen. Insbesondere die Kompatibilität zu Hyperscaler-Clouds (Azure, AWS) ist ein wichtiges Differenzierungsmerkmal für digitalisierte Maschinen- und Anlagenbauer.

Mit IEC 62443 konforme Lösung

KEYNOA reduziert die Komplexität drastisch, wenn es darum geht, starke Geräteidentitäten in vernetzte Architekturen einzubetten. Von der Verwaltung standardbasierter digitaler Identitäten über den Lebenszyklus des Geräts von der Herstellung über die Bereitstellung und Wartung bis hin zur Außerbetriebnahme liefert die Lösung einen mit IEC 62443 konformen Ansatz. Durch eine hohe Automatisierung und Benutzerführung wird die Handhabung von Identitäten für die Verschlüsselung

von Maschinendaten von der Produktion bis in die Cloud deutlich vereinfacht. Dadurch können digitale Mehrwertdienste sicher umgesetzt werden und Geräte werden auch ohne physischen Zugriff überwacht, konfiguriert und mit wichtigen Updates versorgt.

„Mit Janz Tec haben wir einen verlässlichen Partner mit viel Erfahrung im Bereich Industrial IoT gefunden. Die räumliche Nähe ist ein weiterer Vorteil“, sagt Christoph Milder, CEO von DEVITY, und ergänzt rückblickend auf die Zusammenarbeit: „Eine erfolgreiche Startup-Kooperation bedeutet für mich, die gegenseitigen Kernkompetenzen zu erkennen, um den besten Nutzen für den Kunden und das Produkt zu erzielen. Die Basis dafür bilden Vertrauen, Zielstrebigkeit und fachliches Know-how.“

Bis zum Ende des Jahres werden gemeinsam mit Janz Tec nun Lösungen für weitere Anwendungsfälle erarbeitet.

Kontakt

Sven Uthe
Chief Technology Officer
DEVITY
Paderborn
www.devity.eu