Sicherheit für vernetzte Automatisierungsumgebungen

EFFEKTIVES ZERTIFIKATSMANAGEMENT IN DER INDUSTRIE

In industriellen Automatisierungsumgebungen sind digitale Zertifikate von zentraler Bedeutung, um Authentifizierung, Integrität und Vertraulichkeit zu gewährleisten. Mit zunehmender Vernetzung und der Einführung von Technologien wie Industrie 4.0 und IoT stehen Betreiber vor der Herausforderung, verteilte Maschinen und Geräte sicher zu integrieren und zu verwalten. Unser Artikel beleuchtet die wichtigsten Sicherheitsaspekte und Herausforderungen bei der Einführung und Verwaltung von digitalen Zertifikaten in industriellen Umgebungen und stellt Lösungsansätze vor, die dazu im Forschungsprojekt Trustpoint erarbeitet werden.

Industrieanlagen werden zunehmend mit vernetzten Maschinen und Systemen ausgestattet, die auf Technologien wie Internet of Things (IoT) und Industrie 4.0 basieren. Dies schafft einerseits enorme Effizienzvorteile, vergrößert aber auch die Angriffsfläche für Cyberbedrohungen wie Ransomware, Sabotage oder Spionage. Jedes zusätzliche vernetzte Gerät stellt ein potenzielles Einfallstor dar. Hinzu kommt, dass viele industrielle Steuerungssysteme historisch bedingt nicht auf moderne Cyberangriffe vorbereitet sind, da sie ursprünglich in isolierten Netzwerken betrieben wurden. Die Transformation dieser Systeme in vernetzte Umgebungen ist eine erhebliche Herausforderung für die Sicherheit.

Ein zentrales Problem in diesem Zusammenhang ist das fehlende Gerätemanagement. In vielen industriellen Umgebungen gibt es kein zentrales System zur Überwachung und Verwaltung aller vernetzten Geräte. Dies führt dazu, dass unbekannte oder nicht verwaltete Geräte leicht in das Netzwerk gelangen können, ohne die notwendigen Sicherheitsupdates zu erhalten. Diese Geräte stellen ein erhebliches Risiko dar, da nicht ausgeschlossen werden kann, dass sie Schwachstellen aufweisen, die von Angreifern ausgenutzt werden können. Ohne ein zentrales Managementsystem können die betroffenen Geräte zudem nicht eindeutig identifiziert und authentifiziert werden, was das Risiko eines unberechtigten Zugriffs zusätzlich erhöht.

Ein weiteres Problemfeld ist die mangelnde Interoperabilität zwischen verschiedenen Her-

stellern und Betreibern industrieller Systeme. Oft sind Maschinen und Systeme unterschiedlicher Hersteller nicht ausreichend aufeinander abgestimmt, was die Integration erschwert und zu Sicherheitslücken führen kann. Zudem fehlen klare Standards, die die Bewertung und das Management der Sicherheit von Komponenten erleichtern würden. Diese Herausforderungen führen dazu, dass viele Betreiber Schwierigkeiten haben, die Sicherheit ihrer vernetzten Systeme zu gewährleisten.

Die begrenzte Konnektivität vieler Industrieanlagen stellt ebenfalls ein großes Hindernis dar. Viele Maschinen sind an Standorten mit eingeschränktem oder instabilem Netzwerkzugang installiert, was die regelmäßige Aktualisierung der erforderlichen Zertifikate erschwert. Abgelaufene Zertifikate und unsichere Verbindungen sind die Folge und machen die Systeme anfällig für Angriffe. Ohne eine stabile Verbindung können Sicherheitsverletzungen nicht sofort erkannt und behoben werden, was das Risiko weiter erhöht.

Abbildung 1: Anforderungen an das Zertifikatsmanagement im Überblick (Bild: Campus Schwarzwald gGmbH)

Die zunehmende Vernetzung von Industrieanlagen bietet also erhebliche Effizienzvorteile, führt jedoch auch zu signifikanten Herausforderungen in der Cybersicherheit. Die Ausweitung der Angriffsflächen erschwert den Schutz der Systeme. Um diese Bedrohungen zu minimieren, sind klare Standards und zuverlässige Sicherheitslösungen dringend erforderlich. Eine wichtige Komponente solcher Sicherheitslösungen ist ein effektives Zertifikatsmanagement.

ANFORDERUNGEN AN EIN EFFEKTIVES ZERTIFIKATSMANAGEMENT

In der industriellen Automatisierung ist die sichere Verwaltung digitaler Zertifikate unerlässlich, um die Authentifizierung und Integrität vernetzter Systeme zu gewährleisten. Angesichts der Komplexität und Heterogenität solcher Umgebungen muss eine Zertifikatsmanagementlösung flexibel, benutzerfreundlich und auf die spezifischen Anforderungen zugeschnitten sein. Diese Anforderungen stellen wir im Folgenden vor (siehe dazu auch Abbildung 1):

Einfache Zugänglichkeit der PKI: Eine Public Key Infrastructure (PKI) muss so gestaltet sein, dass sie auch von Service-Technikern und Instandhaltern ohne tiefere kryptografische Kenntnisse genutzt werden kann. Komplexe Aspekte wie Schlüssellängen oder Algorithmen sollten auf Basis bewährter Best Practices, etwa den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), automatisch angewendet werden. So kann der Anwender sicher sein, dass Zertifikate immer den aktuellen Sicherheitsstandards entsprechen, ohne sich in technische Details einarbeiten zu müssen.

Automatisierung der Zertifikatserstellung: In stark vernetzten Umgebungen ist es wichtig, den Prozess der Zertifikatserstellung zu automatisieren. Attribute, die in Zertifikaten festgehalten werden, sollten automatisch und fehlerfrei ausgefüllt werden, um den manuellen Aufwand zu reduzieren und potenzielle Fehlerquellen zu minimieren. Der gesamte Prozess sollte so gestaltet sein, dass er intuitiv und ohne tiefere technische Kenntnisse durchgeführt werden kann, was die Effizienz erheblich steigert.

Benutzerfreundliche Bedienung: Eine intuitive und klar strukturierte Benutzeroberfläche ist entscheidend, damit auch Anwender ohne tiefes technisches Hintergrundwissen den Zertifizierungsprozess sicher und korrekt durchführen können. Die Navigation sollte logisch aufgebaut und leicht verständlich sein, sodass der Benutzer problemlos durch den Zertifizierungsprozess geführt werden kann. Eine einfache Benutzerführung hilft, Fehler zu vermeiden und stellt sicher, dass Sicherheitsmaßnahmen konsequent umgesetzt werden.

Sicherheitsrisiken durch ältere Komponenten: In vielen industriellen Netzwerken sind noch ältere Geräte im Einsatz, die nur veraltete kryptografische Algorithmen wie RSA mit einer Schlüssellänge von 1024 Bits unterstützen. Die Zertifikatsmanagementlösung muss in der Lage sein, die mit diesen veralteten Algorithmen verbundenen Risiken zu identifizieren und geeignete Vorschläge zur Risikominimierung zu machen. Gleichzeitig sollte die Lösung sicherstellen, dass diese älteren Geräte weiterhin unterstützt werden können, um den reibungslosen Betrieb nicht zu gefährden.

Vereinfachung der Zertifikatserstellung: In der Praxis greifen viele Nutzer aus Bequemlichkeit auf selbstsignierte Zertifikate zurück, da diese einfach zu erstellen sind und oft mit einer langen Gültigkeit ausgestellt werden. Um die Verwendung von sicheren verwalteten Zertifikaten zu fördern, sollte die Lösung den Erstellungsprozess so weit vereinfachen, dass der Umstieg auf verwaltete Zertifikate attraktiv wird. Der gesamte Prozess muss so benutzerfreundlich sein, dass unsichere selbstsignierte Zertifikate nicht mehr benötigt werden. Verwaltete Zertifikate bieten im Gegensatz zu selbstsignierten Zertifikaten

ein höheres Maß an Sicherheit, da sie von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt und regelmäßig überprüft werden. Dies schützt vor gefälschten Identitäten und reduziert Sicherheitsrisiken, die bei selbstsignierten Zertifikaten auftreten können.

Unterstützung unterschiedlicher Protokolle: Industrielle Automatisierungsumgebungen bestehen oft aus einer Vielzahl von Geräten, die unterschiedliche Zertifikatsprotokolle wie das Certificate Management Protocol (CMP), Enrollment over Secure Transport (EST) oder das Simple Certificate Enrollment Protocol (SCEP) oder sogar herstellerspezifische Lösungen verwenden. Ein effektives Zertifikatsmanagement muss diese Vielfalt an Protokollen unterstützen, um eine nahtlose Integration in bestehende Systeme zu ermöglichen und die Verwaltung der Zertifikate für alle Geräte sicherzustellen.

Unterbrechungsfreie Zertifikatsupdates: In der industriellen Produktion ist es entscheidend, dass Zertifikatsupdates und -erneuerungen ohne Unterbrechungen im laufenden Betrieb durchgeführt werden können. Der gesamte Prozess muss im Hintergrund ablaufen, damit Ausfallzeiten vermieden und Produktionsprozesse nicht gestört werden.

Offline- und Air-Gap-Unterstützung: Da viele industrielle Netzwerke aus Sicherheitsgründen air-gapped sind oder keine permanente Verbindung zum Internet haben, muss die Zertifikatsverwaltung in der Lage sein, auch ohne ständige Netzwerkanbindung zu funktionieren. Zertifikate müssen offline erstellt, verteilt und erneuert werden können, um die Sicherheit der Systeme auch in isolierten Netzwerken zu gewährleisten.

Verteilung von Truststores anderer CAs: Zusätzlich sollte die Zertifikatsverwaltung es ermöglichen, Truststores anderer Certificate Authorities (CAs) zu verteilen. Dies ermöglicht eine nahtlose Integration in bestehende PKI-Systeme und Vertrauensnetzwerke, wodurch die Verwaltung der Zertifikate über verschiedene Systeme hinweg vereinfacht wird.

TRUSTPOINT: OPEN-SOURCE FÜR ZERTIFIKATSMANAGEMENT

Im Projekt Trustpoint werden Lösungsansätze für die genannten Herausforderungen erarbeitet und in eine Open-Source-Software überführt. Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt hat das Ziel, eine einfache und effektive Verwaltung von Zertifikaten in OT-Netzwerken (Operational Technology, OT) zu ermöglichen. Trustpoint steht unter der MIT-Lizenz auf GitHub (https://github.com/TrustPoint-Project/trustpoint) zur Verfügung und bietet umfangreiche Funktionen für das Zertifikatsmanagement, die sich nahtlos in Automatisierungsumgebungen integrieren lassen.

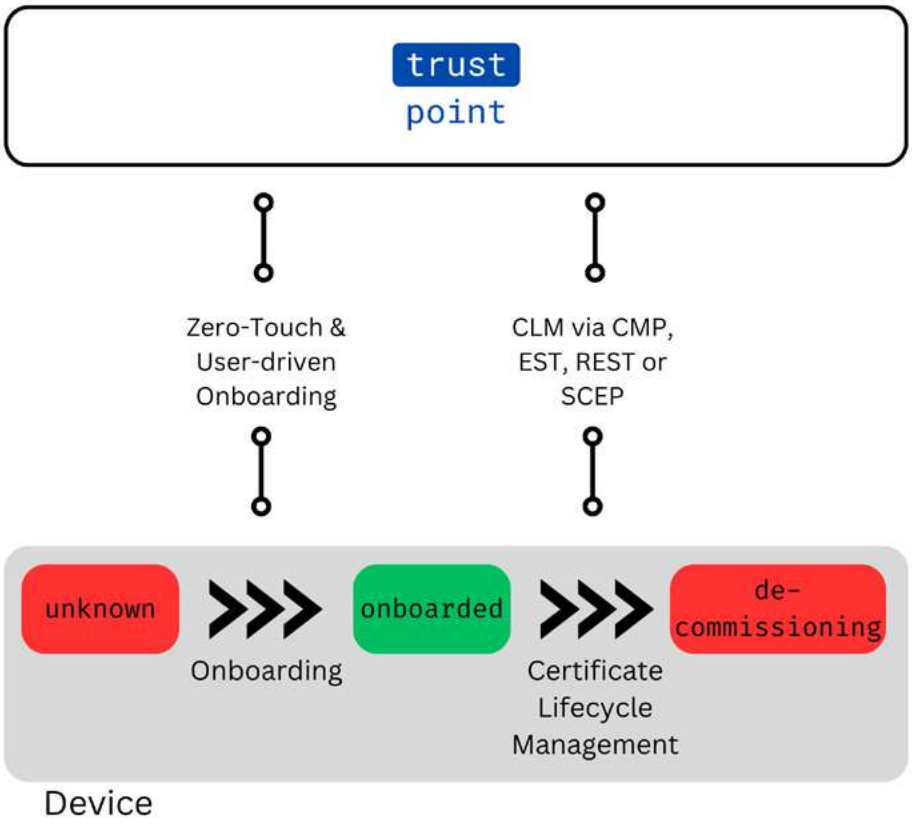

Abbildung 2: Der Onboarding-Prozess für neue Geräte (Bild: Campus Schwarzwald gGmbH)

Ein zentraler Aspekt von Trustpoint ist der Onboarding-Prozess für neue Geräte (siehe Abbildung 2). Dabei wird einem Gerät ein erstes Zertifikat zugewiesen, um es sicher in das Netzwerk zu integrieren. Dem Bedürfnis nach einem automatisierten und benutzerfreundlichen Zertifikatsmanagement trägt Trustpoint unter anderem durch verschiedene Onboarding-Verfahren Rechnung. Ein Zertifikat kann manuell heruntergeladen und auf das Gerät aufgebracht werden, alternativ lässt sich der Onboarding-Prozess auch über die Kommandozeile oder den Browser automatisieren. Trustpoint unterstützt zudem moderne Protokolle wie Bootstrapping Remote Secure Key Infrastructure (BRSKI), die eine vollständige Automatisierung des Onboarding-Prozesses ermöglichen und so den manuellen Aufwand und die Fehleranfälligkeit minimieren.

Ein weiteres wichtiges Feature von Trustpoint ist die Unterstützung einer breiten Palette von Public-Key-Infrastruktur-(PKI)-Protokollen, was besonders in heterogenen industriellen Netzwerken entscheidend ist. Da viele Geräte in industriellen Umgebungen keine oder unterschiedliche Zertifikatsmanagementprotokolle wie CMP, EST, SCEP oder herstellerspezifische Lösungen unterstützen, ist es wichtig, dass das System flexibel auf verschiedene Protokolle reagieren kann. Trustpoint erfüllt diese Anforderung, indem es alle gängigen Protokolle unterstützt und sowohl in Online- als auch in Offline-Umgebungen betrieben werden kann. Dies ermöglicht auch die Integration bestehender PKI-Systeme in Unternehmen, wobei Trustpoint die Anfragen von Geräten an externe PKIs weiterleiten kann (als sogenannte Registration Authority). Damit bietet Trustpoint auch in Air-Gap-Umgebungen oder Netzwerken ohne per-

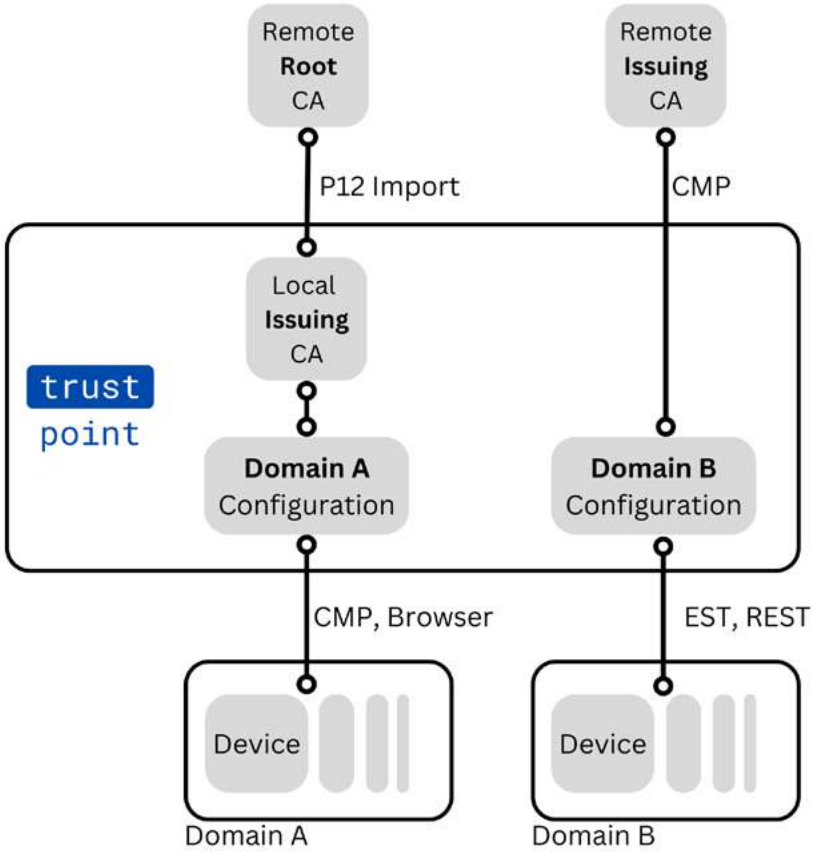

Abbildung 3: Die Architektur von Trustpoint (Bild: Campus Schwarzwald gGmbH)

manente Internetverbindung eine zuverlässige Lösung für die Zertifikatsverwaltung. Durch die verschiedenen Möglichkeiten der Ausstellung von Zertifikaten ist auch eine Unterstützung von Komponenten älterer Baujahre möglich.

FLEXIBLE ZERTIFIKATS-VERWALTUNG FÜR KOMPLEXE NETZWERKE

In komplexen industriellen Automatisierungsumgebungen ist es häufig notwendig, mehrere Domains mit unterschiedlichen Anforderungen zu betreiben, zum Beispiel Domain A und Domain B. In Domain A fungiert die Issuing CA A als zentrale Zertifizierungsstelle. Diese CA wird direkt auf Trustpoint betrieben und ist in der Lage, alle notwendigen Zertifikate für Geräte innerhalb dieser Domain zu erstellen und zu verwalten, ohne dass eine externe PKI benötigt wird. Dies ist besonders vorteilhaft für Offline-Umgebungen, da die Geräte unabhängig vom externen Netzwerk operieren können. Trustpoint unterstützt den gesamten Zertifikatslebenszyklus, von der Ausstellung bis zur Erneuerung und Sperrung von Zertifikaten, was die automatisierten Zertifikatsupdates ohne Betriebsunterbrechung ermöglicht.

Im Gegensatz dazu wird in Domain B die Issuing CA B als Registration Authority (RA) konfiguriert. In dieser Konstellation übernimmt Trustpoint die Rolle des Vermittlers zwischen den Geräten in Domain B und einer externen PKI. Geräte in Domain B senden ihre Zertifikatsanfragen an die RA, die diese Anfragen entgegennimmt und sie gegebenenfalls in das Certificate Management Protocol (CMP) überführt. Anschließend leitet die RA die Anfrage an die externe PKI weiter, die letztlich das Zertifikat ausstellt. Diese Flexibilität in der Architektur erfüllt die Anforderung, verschiedene Protokolle und Netzwerkkonfigurationen zu unterstützen und sicherzustellen, dass Zertifikate auch in komplexen Netzwerken effizient verwaltet werden können.

Trustpoint bietet zudem vorkonfigurierte Vorlagen für Anwendungszertifikate, die für verschiedene industrielle Protokolle wie Transport Layer Security (TLS), Message Queuing Telemetry Transport (MQTT) oder OPC Unified Architecture (OPC UA) optimiert sind. Dies vereinfacht die Erstellung von Zertifikaten erheblich und reduziert den Bedarf an tiefgehenden kryptografischen Kenntnissen seitens der Administratoren. Der Trustpoint-Client ermöglicht zudem die Beantragung und Verwaltung dieser Zertifikate per API oder Kommandozeilenbefehl, was eine zusätzliche Vereinfachung für die Benutzer bedeutet. Weiterhin kann Trustpoint auch verschiedene Truststores zentral verwalten und auf Endgeräte verteilen.

FAZIT

Die Verwaltung digitaler Zertifikate ist eine der zentralen Herausforderungen in modernen industriellen Umgebungen. Um Sicherheitslücken zu vermeiden, sind Automatisierung, Benutzerfreundlichkeit und die Unterstützung verschiedener Protokolle entscheidend. Trustpoint als Open-Source-Lösung bietet hier einen flexiblen Ansatz, um die Komplexität zu reduzieren und ein sicheres Zertifikatsmanagement auch in komplexen OT-Netzwerken zu gewährleisten. ■

FLORIAN HANDKE
ist Leiter Industrial Security der Campus Schwarzwald gGmbH.

ALEXANDER HARIG
ist Industrial Security Engineer bei der Campus Schwarzwald gGmbH.

DR. CLAUDIA PRIESTERJAHN
ist Team Lead eHealth Development and Consulting bei der achelos GmbH.