Peer-Review: 11.06.2024

Ende-zu-Ende gedacht

Industrielle Nutzung digitaler Identitäten

Rohit Bohara, asvin GmbH; Florian Handke, Alexander Harig, Campus Schwarzwald gGmbH; Dominik Isaak, achelos GmbH; Jan Pelzl, Hochschule Hamm-Lippstadt; Andreas Philipp, PrimeKey Labs GmbH; Claudia Priesterjahn, achelos GmbH; Christian Schwinne, Hochschule Hamm-Lippstadt

Die Anforderungen an die IT-Sicherheit von Maschinen und Anlagen werden fortlaufend komplexer. Dadurch wird die Verwendung von Maschinenidentitäten immer wichtiger. Sie spielen eine entscheidende Rolle beim Aufbau der IT-Sicherheit in industriellen Netzwerken. Maschinenidentitäten ermöglichen die Herstellung von Vertrauen zwischen Herstellern und Betreibern, z. B. durch den Nachweis der Herkunft von Komponenten und die Schaffung einer sicheren Rückverfolgbarkeit. Allerdings ist es aktuell noch schwierig, digitale Identitäten in industriellen Umgebungen einzuführen und zu verwalten. Die Inbetriebnahme, verbunden mit einer erstmaligen sicheren Integration der Geräte in das Netzwerk (Onboarding), ist dabei ein besonders kritischer Schritt. In diesem Artikel gehen wir auf die Bedeutung digitaler Identitäten für Komponenten ein, beschreiben notwendige Lösungsansätze wie das sichere Onboarding und geben mit unserem Forschungsprojekt Trustpoint ein Beispiel, wie eine sichere Verwaltung von digitalen Identitäten in der Industrie funktionieren kann.

#Industrielle Cybersicherheit #PKI #Digitale Identitäten #Onboarding

End-to-end considerations

Industrial utilization of digital identities

The IT security requirements for machines and systems are becoming increasingly complex. As a result, the use of machine identities is becoming increasingly important. They play a decisive role in establishing IT security in industrial networks. Machine identities enable the establishment of trust between manufacturers and operators, e.g. by proving the origin of components and creating secure traceability. However, digital identities are currently still difficult to introduce and manage in industrial environments. Commissioning - combined with the initial secure integration of devices into the network (onboarding) - is a particularly critical step. In this article, we look at the importance of digital identities for components and systems, describe necessary solutions such as secure onboarding and, with our Trustpoint research project, provide an example of how secure management of digital identities can work in industry.

#Industrial Security #PKI #Digital Identities #Onboarding

1. Bedeutung digitaler Identitäten für Maschinen

Die Industrie hat eine Transformation in Richtung hochautomatisierter, vernetzter und intelligenter Betriebsumgebungen erlebt. Das hat zu einem tiefgreifenden Wandel in den operativen Technologien und den industriellen Prozessen geführt. Durch die zunehmende Vernetzung und Automatisierung sind industrielle Umgebungen immer stärker durch Cyber-Angriffe bedroht. Dabei ist nicht nur die Produktion betroffen, sondern ganze Lieferketten. Als zusätzliche Rahmenbedingungen verpflichten u. a. der Cyber Resilience Act [1] und die NIS2-Direktive Hersteller zur Absicherung ihrer Komponenten, Systeme und Lieferketten. Auch Betreiber sind dazu verpflichtet, wenn sie z. B. nach IEC 62443 [2] vorgehen möchten. Deshalb gewinnt die IT-Sicherheit in dieser Domäne enorm an Bedeutung.

Infolge der industriellen Digitalisierung hat die Anzahl der Geräte mit Maschine-zu-Maschine-Kommunikation rapide zugenommen. Dieser Trend hat zu einem tiefgreifenden Wandel in den operativen Technologien (OT) und den industriellen Prozessen geführt. Betroffen sind nicht nur die Produktion, sondern auch die gesamte Lieferkette. Nach dem Cisco Annual Internet Report [3] wurden von 2018 bis 2023 ca. 10 Milliarden neue Geräte in Netzwerke eingebunden. Mit zunehmender Vernetzung und Automatisierung sind auch industrielle Umgebungen immer stärker von Cyber-Angriffen bedroht. Deshalb gewinnt die Gewährleistung der IT-Sicherheit enorm an Bedeutung.

Dabei ist die Basis für eine sichere Kommunikation mit solchen Geräten der Einsatz digitaler Identitäten und deren Verwendungsmöglichkeiten, wie sie in Standards wie OPC UA [4] und IEC 62443 beschrieben sind. Maschinenidentitäten spielen eine entscheidende Rolle beim Aufbau von Sicherheit und Integrität für Kommunikation und Daten in industriellen Netzwerken. Sie ermöglichen die Authentifizierung, die Validierung von Software, den Nachweis der Herkunft von Komponenten und die Schaffung einer sicheren Rückverfolgbarkeit. Damit ermöglichen digitale Identitäten die Herstellung von Vertrauen zwischen Herstellern und Betreibern.

1.1 Grundlagen digitaler Identitäten

Eine digitale Identität ist weit mehr als nur eine Geräte-ID oder Seriennummer. Eine digitale Identität stellt sicher, dass eine Komponente oder Anlage wirklich die ist, für die sie sich ausgibt – analog zu einem Ausweis für Personen. Eine digitale Maschinenidentität ist eindeutig und ermöglicht die Herstellung von Vertrauen zwischen Herstellern, Systemintegratoren und Betreibern. So ist z. B. der Nachweis der Herkunft von Komponenten und die Schaffung einer sicheren Rückverfolgbarkeit von Ereignissen im Lebenszyklus von Komponenten möglich. Die Echtheit einer digitalen Identität muss nachvollziehbar geprüft werden können und dient unter anderem der Autorisierung für den Zutritt zu Netzwerken oder weiteren Services wie vertraulicher Datenübertragung und digitalen Signaturen.

Für die Sicherheit ist entscheidend, wie diese Identitäten erzeugt, gespeichert und verwendet werden. Dieser Prozess ist nicht trivial und wird in der Praxis noch häufig unterschätzt. Um eine digitale Identität eindeutig und fälschungssicher zu gestalten, bedient man sich der Methoden moderner Kryptografie. Digitale Identitäten werden heutzutage meistens durch digitale Zertifikate abgebildet, in welchen die Identität über einen zertifizierten, öffentlichen Schlüssel nachgewiesen wird. Ein solches Zertifikat beinhaltet neben dem öffentlichen Schlüssel maschinenbezogene Daten wie die Seriennummer, Herkunft und Softwarestand. Die Echtheit der Daten eines Zertifikates wird von einer vertrauenswürdigen Instanz, der Zertifizierungsstelle – auch Certification Authority (CA) genannt – attestiert. Das Ergebnis ist ein Zertifikat, das von anderen Maschinen oder Menschen geprüft werden kann. Die CA kann beispielsweise in der Hand des Komponentenherstellers oder des Betreibers liegen.

In der Praxis wird der private Schlüssel von Zertifikaten meist durch die Verwendung von sicheren Speichern vor unbefugter Vervielfältigung und Manipulation geschützt. So verfügt etwa der elektronische Personalausweis über einen Sicherheitschip, der praktisch nicht geknackt werden kann. Ob ein entsprechender Schutz auch bei Maschinenidentitäten notwendig ist oder ob niedrigere Sicherheitsmaßnahmen ausreichend sind, hängt von der Anwendung und den damit verbundenen Risiken ab und sollte sorgfältig geprüft werden.

Eine CA zu betreiben ist in der Praxis eine komplexe Aufgabe. Eine gängige Umsetzung für eine CA mit den erforderlichen Unterstützungsmechanismen ist Teil einer Public-Key-Infrastruktur (PKI). Zu den Unterstützungsmechanismen gehören unter anderem die sichere Identifizierung der Komponenten und Benutzer, für die ein Zertifikat ausgestellt werden soll, und natürlich das fälschungssichere Übertragen des öffentlichen Schlüssels der CA als Vertrauensanker. Die sichere Identifikation von Geräten ist Grundvoraussetzung für die Erstellung der Zertifikate und wird in diesem Beitrag beschrieben. Weitere praktische Herausforderungen ergeben sich durch die Existenz einer Vielzahl verschiedener CAs, wie im folgenden Abschnitt beschrieben wird. Auch das im Falle eines Sicherheitsvorfalls wichtige Widerrufen von Zertifikaten führt aus praktischer Sicht zu erhöhter Komplexität, da in den Geräten ein Prozess zur Überprüfung der Gültigkeit von Zertifikaten auf Basis von Online-Diensten oder Sperrlisten

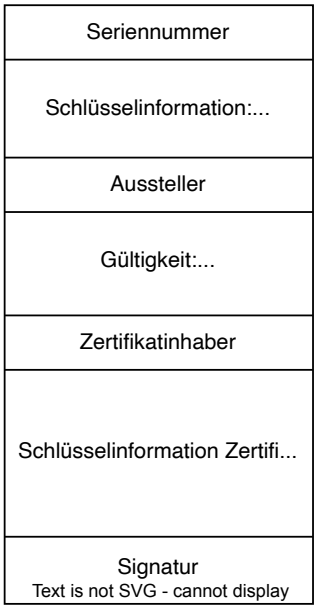

Abbildung 1: Beispielhafter Aufbau eines X.509 Zertifikates.

oder alternativ durch kurzlebige Zertifikate implementiert werden muss (vergl. [5]).

1.2 Digitale Identitäten nach dem X.509 Standard

Der dominante Standard für Zertifikate ist der X.509 Standard [6] und wird für die Authentisierung in Computernetzen weltweit genutzt. Entsprechend sind X.509-Zertifikate für industrielle Anwendungen sehr weit verbreitet. Im Folgenden betrachten wir die Struktur eines X.509-Zertifikates, wie in Abbildung 1 dargestellt:

- **Seriennummer:** Meist eine 8 bis max. 20 Byte lange Zufallszahl, die einmalig sein muss, um das Zertifikat eindeutig zu identifizieren [5]. Eine CA darf also kein zweites Zertifikat mit einer schon einmal ausgegebenen Seriennummer ausstellen.

- **Schlüsselinformation:** Spezifiziert, welcher asymmetrische kryptografische Algorithmus wie z. B. RSA oder ECC für die Signatur verwendet wird. Ebenso dessen Sicherheitsparameter wie etwa die Länge des Schlüssels spezifiziert.

- **Aussteller:** Angabe, wer der Aussteller des Zertifikats ist, in der Regel also die Seriennummer des CA-Zertifikats, das das vorliegende Zertifikat signiert hat.

- **Gültigkeit:** Zertifikate werden für einen bestimmten Zeitraum ausgestellt, bspw. für ein oder zwei Jahre. Grund hierfür ist, dass der private Schlüssel in dem Zertifikat möglicherweise kompromittiert werden kann. Durch das Ablaufdatum des Zertifikats hat ein Angreifer nur eine endliche Zeitspanne, in der er den kompromittierten Schlüssel nutzen kann.

- **Zertifikatinhaber:** Dieses Feld identifiziert die Maschine und kann z. B. die Seriennummer der Maschine oder den „common name“ (CN) eines X.509-Zertifikats enthalten.

Der CN beschreibt typischerweise den vollständig qualifizierten Domänennamen (FQDN) eines Servers oder den Namen des Zertifikatinhabers.

» **Schlüsselinformation Zertifikatinhaber:** Hier ist der öffentliche Schlüssel, der durch das Zertifikat geschützt wird, enthalten. Neben der Bitfolge des Schlüssels sind der Algorithmus und dessen Parameter gespeichert.

» **Signatur:** Eine digitale Signatur der CA über alle obenstehenden Felder. Die Signatur kann über den öffentlichen Schlüssel der CA geprüft werden

Im einfachsten Fall gäbe es genau eine CA, die Zertifikate für alle Maschinen weltweit ausstellt und der alle Menschen und zertifikatsprüfenden Anwendungen vertrauen. Leider ist die Situation in der Realität komplizierter. Es gibt üblicherweise viele verschiedene Zertifizierungsstellen für unterschiedliche Zwecke. So verfügen Hersteller beispielsweise heute schon über mehrere CAs für ihre Produktlinien und Anlagenbetreiber haben eigene CAs für ihre Anlagen und industriellen Netzwerke. Diese CAs sind meistens hierarchisch wie in Abbildung 2 gezeigt angelegt und den organisatorischen Rahmenbedingungen der Hersteller und Betreiber angepasst. Die oberste CA in einer Hierarchie wird hierbei Root CA genannt, die CAs für die Erstellung der Geräte-Zertifikate Issuing CAs. Aus organisatorischen Gründen werden die Issuing CAs häufig noch unter einer weiteren sogenannten Intermediate CA aufgehängt. Wie so eine Hierarchie aussehen kann, ist ein Abbildung 2 dargestellt. Damit Zertifikate von verschiedenen Herstellern und Betreibern untereinander akzeptiert werden, muss die Echtheit der Zertifikate entsprechend geprüft werden oder die Root CAs müssen sich gegenseitig vertrauen. Letzteres kann über eine Cross-Zertifizierung der CAs untereinander realisiert werden. Dabei stellen sich beide Root CAs gegenseitig Zertifikate aus, die den öffentlichen Schlüssel der jeweils anderen CA enthalten.

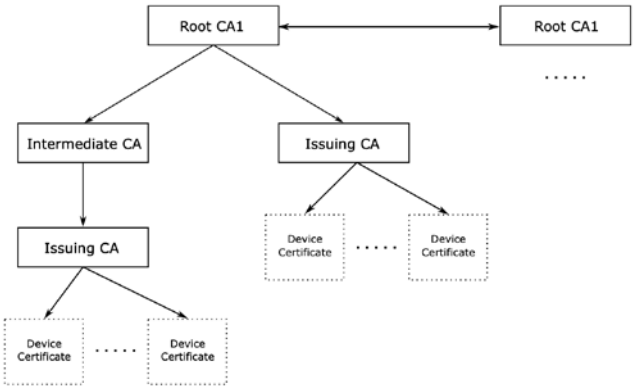

Abbildung 2: Beispiel für eine PKI mit zwei Cross-zertifizierten Root CAs und mehreren Issuing CAs.

1.3 Die Rolle von Zertifikaten in industriellen Netzwerken

Zertifikate spielen eine entscheidende Rolle bei der Sicherstellung der Sicherheit und Vertrauenswürdigkeit der Kommunikation in industriellen Netzwerken. Die Norm IEC 62443-4-2, welche die technischen Sicherheitsanforderungen für Komponenten industrieller Automatisierungssysteme festlegt, enthält spezifische Anforderungen zur Kommunikationsintegrität. Die Anforderung CR 3.1 bezieht sich auf die Fähigkeit der Komponenten, die Authentizität der empfangenen Informationen zu verifizieren. Dies schließt die Überprüfung ein, dass die Daten von einer vertrauenswürdigen Quelle stammen. Das gilt sowohl für den Client als auch für den Server, sodass beide ein entsprechendes Zertifikat benötigen. Zu den wichtigsten Bestandteilen in dieser Domäne gehören Truststores und TLS-Zertifikate, die je nach Einsatzbereich unterschiedliche Funktionen erfüllen.

Truststores enthalten Root-Zertifikate und Intermediate-Zertifikate, die zur Verifizierung der gesamten Zertifikatskette verwendet werden. Diese Root-Zertifikate dienen als Vertrauensanker, von denen alle anderen Zertifikate ihre Vertrauenswürdigkeit ableiten. Truststores werden genutzt, um digitale Signaturen zu verifizieren. So kann sichergestellt werden, dass die zertifizierte Software von einem vertrauenswürdigen Herausgeber stammt und nicht manipuliert wurde.

X.509-Zertifikate werden verwendet, um die Identität von Clients und Servern beim Aufbau einer TLS-Verbindung zu verifizieren. TLS steht für Transport Layer Security, ein Protokoll zur sicheren Datenübertragung [8]. Durch TLS wird Vertraulichkeit zwischen industriellen Geräten und Systemen hergestellt und die Integrität der ausgetauschten Daten sichergestellt. So wird garantiert, dass nur autorisierte Benutzer, Geräte und Anwendungen auf industrielle Systeme und Netzwerke zugreifen können. Zum Aufbau einer TLS-Verbindung authentifiziert sich der Server gegenüber dem Client durch ein Server-Zertifikat, das der Client anhand eines Truststores überprüft. Für beidseitige Authentisierung wird zusätzlich ein Client-Zertifikat verwendet, über das der Server den Client authentifiziert. TLS wird unter anderem auch zur sicheren Übertragung von Webseiten genutzt.

Die Einsatzmöglichkeiten von Zertifikaten in industriellen Netzwerken sind vielfältig. Im Folgenden sind exemplarisch drei mögliche Anwendungsfälle aufgeführt:

» **Sicherer Datenaustausch:** Der sichere Datenaustausch zwischen Maschinen (M2M) und Mensch-Maschine-Schnittstellen (HMI) wird zum Beispiel durch OPC UA ermöglicht. Das Protokoll verwendet X.509-Zertifikate zur Sicherstellung der Identität und Vertrauenswürdigkeit der Kommunikationspartner. Andere relevante Protokolle zur sicheren Kommunikation sind Modbus TCP [9] (mit TLS), das eine Erweiterung des Modbus-Protokolls zur Unterstützung von TLS-Verschlüsselung darstellt, und Profinet [10], das Sicherheitsmechanismen zur Authentifizierung und Datenverschlüsselung integriert.

» **Sichere Updates aus vertrauenswürdigen Quellen:** Firmware und Software in industriellen Netzwerken werden mit digitalen Signaturen versehen, um sicherzustellen, dass Updates von einer vertrauenswürdigen Quelle stammen und die Installation von manipulierten oder bösartigen Updates zu verhindern. Systeme überprüfen das Zertifikat des Updates vor der Installation und akzeptieren nur signierte und verifizierte Updates und stellen

damit sicher, dass das Update während der Übertragung nicht verändert wurde.

» **Sichere Fernwartung und Fernzugriff:** Zertifikate ermöglichen Technikern den sicheren Fernzugriff auf Maschinen und Systeme zur Diagnose und Wartung, wodurch Ausfallzeiten reduziert werden. Protokolle wie IPsec [11] (IP Security) und RDP [12] (Remote Desktop Protocol) nutzen zertifikatsbasierte Authentifizierung; VPN-Gateways sorgen für sichere und verschlüsselte Verbindungen zwischen entfernten Standorten und dem Firmennetzwerk.

1.4 Sicherheitsherausforderungen und Lösungsansätze

In industriellen Umgebungen stehen wir vor spezifischen Herausforderungen, die die Verwaltung von digitalen Zertifikaten und kryptographischen Schlüsseln erschweren. Dazu gehören stark segmentierte Netzwerke, eingeschränkte Konnektivität, begrenzte Hardware- und Software-Ressourcen, hohe Netzwerkdynamik und organisatorische Einschränkungen. Zudem müssen zukünftige Entwicklungen antizipiert werden, da die zu erwartende Lebensdauer von Komponenten in Maschinen deutlich länger ist als die herkömmlicher IT-Komponenten. Insbesondere stehen Hersteller und Betreiber vor der Herausforderung, Expertise im Bereich der Informationssicherheit aufzubauen und bestehende Sicherheitslösungen an die spezifischen Anforderungen und Einschränkungen von industriellen Anlagen anzupassen.

Nicht zuletzt aufgrund von menschlichen Fehlern bei der Verwaltung und Erneuerung von Zertifikaten bestehen Risiken für das System durch falsch ausgestellte, abgelaufene oder kompromittierte Zertifikate. Zusätzlich fehlen durch eingeschränkte Hard- und Softwareressourcen oft sichere Speichermöglichkeiten für kryptografisches Material. Sicherheitsfunktionen können fehlerhaft implementiert sein, insbesondere wenn die verwendete Software spezifisch für das Gerät ist, Sicherheitslücken selten oder nie durch Updates behoben werden und die Implementierung der Sicherheitsfunktion nicht unabhängig auf ihren Sicherheitswert überprüft wird.

Die Widerrufbarkeit von Zertifikaten ist ein wichtiger Faktor für den sicheren Einsatz digitaler Identitäten. Dabei werden häufig Sperrlisten (CRL) oder das Online Certificate Status Protocol (OCSP) verwendet. Allerdings sind diese Mechanismen in der Regel für industrielle Umgebungen zu ressourcenintensiv. Sowohl das Widerrufen von Zertifikaten als auch die Überprüfung, ob ein Zertifikat widerrufen wurde, können mit den praktischen Anforderungen an ein industrielles System kollidieren.

In solchen Umgebungen ist es von entscheidender Bedeutung, alternative Ansätze zu berücksichtigen, die weniger Ressourcen erfordern. Eine solche Alternative sind kurzlebige Zertifikate. Hierbei werden die Zertifikate in regelmäßigen Abständen ersetzt, um den Zeitraum zu minimieren, in dem ein kompromittiertes Zertifikat unrechtmäßig verwendet werden kann. Je nach spezifischen Anforderungen und Risiken der industriellen Umgebung wird entweder ein Mechanismus zur automatisierten Zertifikatserneuerung eingesetzt oder ein kurzlebiges Zertifikat zur Durchführung einer bestimmten Aktion ausgestellt, sofern die Verfügbare Rechenleistung ausreichend ist.

2. Sicheres Onboarding als Grundvoraussetzung für den sicheren Betrieb

Onboarding beschreibt den Prozess des erstmaligen Anschließens eines Geräts im Netzwerk sowie der Einbindung in die lokale Domäne, sodass das Gerät mit anderen Hosts im Netzwerk sicher kommunizieren kann. Technisch endet der Onboarding-Prozess zu dem Zeitpunkt, an dem das Gerät ein lokales, domänenspezifisches Gerätezertifikat erhalten, verifiziert und akzeptiert hat. Dabei ist ein Gerät, das an das Netzwerk angeschlossen wurde, erst in der Lage mit anderen Hosts im Netzwerk zu kommunizieren, wenn es das lokale Gerätezertifikat erhalten hat und damit gegenseitiges Vertrauen zwischen der Domäne und dem Gerät hergestellt wurde.

Daher ist sicheres Onboarding eine essenzielle Grundvoraussetzung für den sicheren Betrieb eines vernetzten Geräts. Fortschrittliche Sicherheitslösungen wie eine Ende-zu-Ende-Verschlüsselung und insbesondere der Aufbau einer Zero-Trust-Architektur, in der keinem Gerät allein durch dessen Verbindung zum internen Netzwerk vertraut wird, sind nur möglich, wenn sichere, digitale Identitäten in Form von Zertifikaten auf die Geräte aufgebracht werden.

Der Onboarding-Prozess ist, falls nicht mit Bedacht und ohne beidseitige Authentifizierung durchgeführt, äußerst anfällig für eine Vielzahl von Angriffen, welche im schlimmsten Fall zu einer vollen Kompromittierung des Geräts und des Netzwerks führen kann.

2.1 Grundlagen

Die Grundlage eines sicheren Onboardings ist immer die beidseitige Authentifizierung zwischen Netzwerk und Gerät, bevor ein lokales, domänenspezifisches Gerätezertifikat ausgestellt und einem neuen Gerät übergeben wird.

Zunächst ist es wichtig, nur vertrauenswürdige und vorgesehene Geräte in die Domäne zu integrieren, um zu verhindern das sich möglicherweise böswillige Geräte Zugang zum Netzwerk und zur Domäne verschaffen. Es muss also eine Authentifizierung des Gerätes durch das Netzwerk stattfinden. Dies ist umso wichtiger, umso mehr Personen physikalischen Zugang zum Netzwerk haben.

In industriellen Netzwerken ist es ebenso von Bedeutung, dass ein Gerät das Netzwerk authentifiziert, bevor es ein lokales Gerätezertifikat akzeptiert und den Hosts in der dazugehörigen Domäne vertraut. Dieser Prozess dient dazu, sicherzustellen, dass das Gerät nur mit vertrauenswürdigen Entitäten kommuniziert und potenzielle Sicherheitsrisiken minimiert werden. Durch die Authentifizierung des Geräts wird verhindert, dass ein Angreifer ein Zertifikat einer anderen, nicht vorgesehenen Domäne aufspielt. Ohne diese Sicherheitsmaßnahme könnte ein Angreifer das Gerät manipulieren und Man-in-the-Middle-Angriffe oder Denial-of-Service-Angriffe durchführen.

Der Onboarding-Prozess kann manuell oder automatisiert ablaufen. Besonders in automatisierten Onboarding-Prozessen, bei denen das Gerät selbständig nach einer Domäne sucht,

ist die Authentifizierung von entscheidender Bedeutung. Das Gerät muss sicherstellen, dass es sich nur mit vertrauenswürdigen Netzwerken verbindet. Durch die Authentifizierung und das Vertrauen in die Domäne kann das Gerät sicherstellen, dass es nur mit Hosts innerhalb der erwarteten Domäne kommuniziert.

2.2 Manueller Onboarding-Prozess

Beim manuellen Prozess des Onboardings beantragt ein Administrator eine neue lokale Maschinenidentität (Zertifikat und Schlüsselpaar) für ein neues Gerät in Bezug auf die vorgesehene Domäne. Dies kann bei einer Zertifizierungsstelle (CA) oder einem internen System erfolgen. Die Identität wird mit Informationen wie der Seriennummer, dem Gerätehersteller, dem Softwarestand usw. verknüpft. Anschließend wird das Zertifikat manuell auf das Gerät aufgebracht und konfiguriert.

Dieser manuelle Prozess ist kaum skalierbar und gerade in komplexeren Netzwerkumgebungen fehleranfällig. Zusätzlich muss der Administrator dabei sicherstellen, dass das Zertifikat auf das korrekte Gerät angewendet wird. Ist das Gerät nicht direkt mit einer Tastatur und Monitor verbunden, sondern findet auch die erste Verbindung über eine Remote-Verbindung, z. B. SSH statt, muss bedacht werden, dass das Gerät noch nicht authentifiziert werden kann, insofern noch kein Vertrauensverhältnis besteht. Hier besteht folglich die Gefahr eines Man-in-the-Middle Angriffs, insbesondere falls es sich um ein größeres und zugängliches Netzwerk handelt.

2.3 Automatisierter Onboarding-Prozess

Ein automatisierter Prozess, auch als Zero-Touch Onboarding bezeichnet, ermöglicht es einem neuen Gerät, sich einfach mit dem Netzwerk zu verbinden. Der Onboarding-Prozess startet nun vollautomatisch, ohne dass ein vertrauenswürdiger Administrator erforderlich ist. In aktuellen Protokollen und Standards, die ein Zero-Touch Onboarding erlauben, wie BRSKI [13] oder FIDO FDO [14], finden meist Maschinenidentitäten, die vom Hersteller aufgebracht wurden sowie sogenannte Vouchers [15] Anwendung. Vouchers sind vom Hersteller signierte Informationen bezüglich des Netzwerks und Domänen zu dem sich das Gerät onboarden darf. Diese werden im Moment des Onboardings an das Gerät übermittelt. Das Gerät kann nun über den Voucher verifizieren, ob die Domäne legitim und vertrauenswürdig ist. Die vom Hersteller eingebrachten Gerätezertifikate hingegen erlauben dem Betreiber, ein Gerät eindeutig zu identifizieren und dessen Identität kryptographisch zu überprüfen. Dieser Prozess ist im Gegensatz zur manuellen Variante skalierbar, wenig fehleranfällig und kann ein gewisses Sicherheitslevel garantieren. Allerdings müssen sowohl Gerätehersteller als auch Betreiber Infrastruktur und Dienste bereitstellen, um die beidseitige Authentifizierung und damit das Onboarding zu ermöglichen. Der Hersteller muss eine PKI (Public-Key-Infrastruktur) zur Ausstellung der Gerätezertifikate und einen Dienst zur Ausstellung und Verwaltung der Voucher bereitstellen. Der Betreiber benötigt eine Infrastruktur und Dienste, die den gesamten Onboarding-Prozess orchestrieren und die beidseitige Authentifizierung der Geräte realisieren.

2.4 Herausforderungen bei der Integration von Geräten

Das übergeordnete Ziel ist es, neue Geräte mit Hilfe eines Zero-Touch-Verfahrens skalierbar und vollautomatisch in eine Domäne zu integrieren und damit eine Zero-Trust-Architektur zu ermöglichen. Eine große Herausforderung dabei ist zum einen die Vielzahl an verschiedenen Geräten mit den unterschiedlichsten Fähigkeiten, Protokollunterstützungen und einer lange Nutzungsdauer in industriellen Umgebungen. Dies bedingt, dass auch zukünftig auf manuelles Onboarding zurückgegriffen werden muss, um Geräte, die kein Zero-Touch-Verfahren anbieten, sicher in die Domäne integrieren zu können. Zum anderen ist die oft starke Netzwerksegmentierung eine weitere Herausforderung. Dies kann den Geräten die Verbindung zum zentralen Registrar erschweren, der für die Orchestrierung des automatischen Onboarding-Prozesses zuständig ist. Der Registrar in BRSKI fungiert als vertrauenswürdige Instanz zwischen den neuen Geräten, dem Netzwerk und dem Hersteller und validiert deren Anmeldeinformationen und unterstützt bei der sicheren Inbetriebnahme und Konfiguration.

Aber auch bei einem manuellen Verfahren ergeben sich Probleme. Auf Grund der Vielzahl an unterschiedlichen Geräten mit unterschiedlichen Fähigkeiten spielt der Administrator hier eine besonders wichtige Rolle. Dieser muss über Expertenwissen in der IT-Sicherheit verfügen, sich in verschiedenen Betriebssystemen zurechtfinden und sicherstellen, dass Onboarding und Konfiguration der Geräte korrekt erfolgt. Allgemein ist dieser Prozess sehr fehleranfällig, sowohl durch falsche Konfiguration als auch durch potenzielle Angriffe.

3. Verschiedene Wege des Onboardings in industriellen Netzwerken am Beispiel des Projekts Trustpoint

Mit dem vom BMBF geförderten Forschungsprojekt Trustpoint entwickeln wir eine niederschwellige Lösung zur sicheren Orchestrierung und Verwaltung von digitalen Identitäten in industriellen Umgebungen. Trustpoint ermöglicht eine nahtlose und vertrauenswürdige Kommunikation zwischen verschiedenen Akteuren entlang der Wertschöpfungskette durch die Schaffung eines Vertrauensankers (Trustpoint). Das Ziel des Forschungsprojekts Trustpoint besteht darin, komplexe Prozesse und Mechanismen so zu abstrahieren, dass Hersteller und Betreiber Maschinen und Geräte sicher in ihre Netzwerke integrieren und betreiben können. Diese Lösung soll niederschwellig im Rahmen eines Open-Source-Softwarestacks angeboten werden.

Wie in Abbildung 3 dargestellt, bildet Trustpoint einen Vertrauensanker in Fabriken und Maschinen und verwaltet die im Netzwerk befindlichen Geräte. Dabei werden verschiedene Schnittstellen zu Vertrauensdiensten wie einer PKI sowie zu den jeweiligen Endgeräten angeboten.

Industrielle Umgebungen erfordern innovative Ansätze, um digitale Identitäten von Maschinen und Komponenten sicher zu verwalten. Vor diesem Hintergrund bietet Trustpoint ein skalierbares Konzept, das sowohl ein benutzergesteuertes, manuelles Onboarding als auch automatisiertes Zero-Touch-Onboarding umfasst. Dieses Konzept soll es Herstellern und Betreibern einfacher machen, den Herausforderungen der

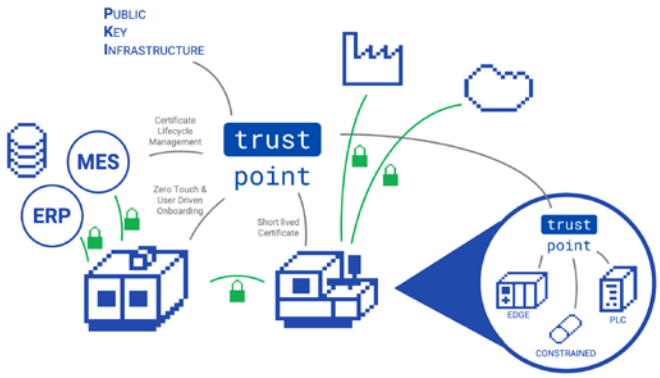

Abbildung 3: Trustpoint als Vertrauensanker im Anlagenbau.

dynamischen Industrielandschaft gerecht zu werden und eine flexible Lösung für die Integration von Geräten in komplexe Netzwerke bieten.
Das Projekt Trustpoint bietet auch eine Client-Software an, die den benutzergesteuerten Onboarding-Prozess erleichtert. Diese kann z. B. auf dem Steuergerät einer ins Netzwerk einzubindenden Maschine installiert werden. Die Software fungiert als Wrapper um PKI- und Krypto-Protokolle und ermöglicht die komfortable Durchführung von Onboarding-Aufgaben sowie die Verwaltung von Zertifikaten auf dem Gerät.

3.1 Zero-Touch Onboarding

Ein wesentlicher Aspekt des Trustpoint-Projekts ist die Integration von Zero-Touch Onboarding- und Bootstrapping-Verfahren, die in Standards wie BRSKI (Bootstrapping Remote Secure Key Infrastructure) [13], OPC UA Part 21 [4], FIDO FDO (Fast Identity Online Device Onboarding) [14] und sZTP (secure Zero-Touch Provisioning) [16] beschrieben sind. Zero-Touch bedeutet, dass bei der Inbetriebnahme keine manuellen Schritte zum Vertrauensaufbau notwendig sind und automatisiert ein idealerweise gegenseitiges Vertrauensverhältnis zwischen Gerät und Betreibernetzwerk aufgebaut wird. Trustpoint legt einen besonderen Fokus auf die Untersuchung der Prinzipien von BRSKI, um ein sicheres Onboarding von Geräten in Netzwerke zu gewährleisten. Dieser Prozess ermöglicht es, Maschinen und Komponenten sicher und effizient in ein Netzwerk zu integrieren, indem sichergestellt wird, dass sie über die notwendigen Identitäten und Schlüssel verfügen, um sich zu authentifizieren und sicher zu kommunizieren. Diese Integration erleichtert den Aufbau von Vertrauen zwischen den Geräten und dem Netzwerk.

3.2 User-Driven Onboarding

Eine ausschließliche Konzentration auf die Unterstützung von Zero-Touch-Onboarding-Protokollen wird in der Praxis aus verschiedenen Gründen als wenig praktikabel erachtet. Fabrikbetreiber, die Trustpoint nutzen, sehen sich der Herausforderung gegenüber, dass in ihren Umgebungen sowohl ältere als auch neuere Geräte betrieben werden. Einige dieser Geräte unterstützen teilweise nicht die notwendigen Komponenten und Protokolle oder werden als unsicher betrachtet, da sie aktuelle Cipher-Suiten nicht unterstützen. Ein weiterer Aspekt ist, dass derzeit kein Hersteller Zero-Touch Onboarding mit BRSKI oder OPC UA Part 21 unterstützt. Selbst wenn einzelne Vorreiter in den kommenden Jahren auftauchen sollten, werden diese sich wahrscheinlich auf geschlossene Systeme konzentrieren, bei denen nahezu ausschließlich auf Komponenten von einem Hersteller zurückgegriffen wird. Dies steht im Widerspruch zu vielen industriellen Umgebungen, in denen die in Maschinen verbauten Komponenten oft von verschiedenen Herstellern stammen. Falls ein Hersteller diese Mechanismen nicht unterstützt, sind Sonderlösungen notwendig, um BRSKI vollumfänglich nutzen zu können.
Obwohl Zero-Touch Onboarding hochautomatisierte Mechanismen bietet, ist es aus verschiedenen Gründen oft nicht möglich oder gewollt. Eine der Hauptursachen ist die Abhängigkeit von bestimmten Protokollen. Zum Beispiel erfordert BRSKI einen Online-Service des Geräteherstellers. In anderen Umgebungen sind nur Offline-Systeme verfügbar, entweder aus technischen Gründen oder aufgrund von Sicherheitsbedenken des Betreibers.
Das Konzept des benutzergesteuerten Onboardings ist daher ebenfalls ein zentraler Bestandteil von Trustpoint.

3.3 Beispiel für User-driven Onboarding auf Basis von Trustpoint

Das in Trustpoint integrierte Onboarding-Modul ermöglicht Administratoren über eine grafische Benutzeroberfläche (GUI) die Konfiguration und Durchführung von benutzergesteuerten Onboarding-Prozessen und fungiert als zentraler Verwalter für die Durchführung und Überwachung dieser. Für Geräte, die die Trustpoint-Client-Software installieren können, wird ein geführter Onboarding-Prozess angeboten. Die Client-Software kann flexibel entweder vom Trustpoint selbst oder aus verschiedenen Repositories bezogen werden. In Situationen, in denen die Installation der Trustpoint-Client-Software nicht möglich ist, bietet Trustpoint ein manuelles Onboarding über eine Kommandozeilenschnittstelle mittels gängiger Linux-Bordmittel, ohne zusätzliche Software zu installieren. Für eine höhere Nutzerfreundlichkeit generiert Trustpoint dabei die notwendigen Befehle und stellt sie in der Trustpoint-GUI dar. Wenn das Gerät SSH unterstützt, können die Befehle auch automatisiert darüber übertragen werden.
Zu Beginn besteht kein Vertrauen. Abbildung 4 zeigt den mehrstufigen Prozess des Onboardings bzw. der Vertrauensbildung:

» **Schritt 1:** Das öffentliche TLS-Zertifikat des Trustpoints wird als Truststore über einen vertrauenswürdigen Kanal auf das Gerät geladen. Hierfür können verschiedene Mechanismen verwendet werden. Der Truststore kann direkt zusammen mit dem Trustpoint-Client auf das Gerät übertragen werden. Dies bietet sich an, wenn die Client-Software über einen sicheren Kanal direkt vom Trustpoint bezogen wird. Alternativ kann er auch von einem USB-Speicher eingelesen werden. Ohne zusätzliche Hardware ist es möglich, den Truststore direkt per HTTP vom (angeblichen) Trustpoint herunterzuladen und dessen Integrität mittels einer Hashfunktion wie SHA2 sicherzustellen. Um die Sicherheit zu erhöhen und um zu vermeiden, dass der gesamte Hash abgeglichen werden muss, kann das PBKDF2-HMAC-Schema [17] verwendet werden. Dadurch wird ein vom Trustpoint generiertes

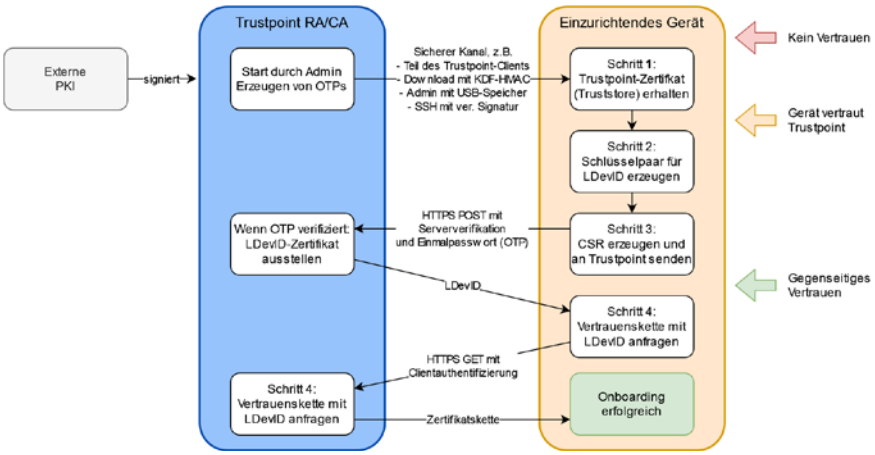

Abbildung 4: Ablaufschema eines User-driven-Onboarding.

Einmalpasswort erforderlich, um den Truststore zu signieren und zu überprüfen. Dieses Passwort muss manuell vom Administrator in das Gerät eingegeben werden.

» **Schritt 2:** Erzeugung eines asymmetrischen Schlüsselpaars auf dem einzubindenden Gerät.

» **Schritt 3:** Erzeugung einer Zertifikatssignierungsanfrage (CSR). Dabei wird das zuvor heruntergeladene Serverzertifikat verifiziert. Diese Anfrage wird im dritten Schritt über eine HTTPS-POST-Anfrage an Trustpoint oder die in die Software integrierte Registrierungsstelle (RA) gesendet. Das Gerät authentifiziert sich gegenüber dem Server über HTTP Basic Auth mithilfe eines Einmalpassworts (One-time-password, OTP), das zuvor über einen sicheren Kanal übertragen wurde. Wenn die Verifikation erfolgreich ist, stellt die in Trustpoint integrierte oder bei Bedarf auch externe ausstellende Zertifizierungsstelle (CA) ein Zertifikat für das Gerät aus. Zu diesem Zeitpunkt wurde das gegenseitige Vertrauensverhältnis zwischen dem Gerät und Trustpoint hergestellt.

» **Schritt 4:** Das Gerät ruft die vollständige Vertrauenskette des Zertifikats ab. Hierfür wird eine HTTPS-GET-Anfrage genutzt, bei der der Server bereits verifiziert ist. Zur Authentifizierung des Geräts gegenüber dem Trustpoint wird das soeben erhaltene Zertifikat im Rahmen der TLS-Clientverifizierung verwendet.

Dieses grundlegende Onboarding-Schema wird zukünftig u. a. noch um Mechanismen zur automatischen Zertifikatserneuerung erweitert.

4. Zusammenfassung und Ausblick

Digitale Identitäten spielen eine entscheidende Rolle beim Aufbau der IT-Sicherheit in industriellen Netzwerken. Zukünftig werden sich Hersteller, Integratoren und Betreiber noch intensiver um das Management von digitalen Identitäten kümmern und besonders in kritischen Umgebungen die Sicherheit einer Lösung nachweisen müssen. Dieser Fokus auf Sicherheit ist besonders relevant angesichts der zunehmenden Bedrohungen im Bereich der IT/OT-Security für Industrieanlagen und der Notwendigkeit, sich an neue Regelungen wie den EU Cyber Resilience Act anzupassen.
Die Einführung und Verwaltung von digitalen Identitäten im industriellen Umfeld sind anspruchsvoll, da spezielle Rahmenbedingungen besondere Mechanismen erfordern, um die Sicherheit dieser Identitäten und damit der gesamten industriellen Anlage zu gewährleisten. Um die Sicherheit digitaler Identitäten in industriellen Umgebungen zu gewährleisten, sind spezifische Maßnahmen erforderlich, die den besonderen Anforderungen dieser Umgebungen gerecht werden.
In diesem Artikel haben wir notwendige Lösungsansätze wie das sichere Onboarding beschrieben und haben mit unserem Forschungsprojekt Trustpoint ein Beispiel vorgestellt, wie eine sichere Verwaltung von digitalen Identitäten in der Industrie funktionieren kann. Trustpoint kann hierbei als quelloffene Umsetzung relevanter Anwendungsfälle eine gute Basis für die Umsetzung in Unternehmen bieten und bietet eine Referenz für aktuelle Standards zum sicheren Onboarding von Geräten. Trustpoint wird zukünftig an weitere industrielle Anforderungen angepasst und unter anderem mit Fokus auf Lifecycle Management weiterentwickelt.

Referenzen

[1] Europäische Kommission. (2022). *Cyber Resilience Act*. Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0454

[2] IEC 62443. (2020). Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme. IEC: www.iec.ch

[3] Cisco. (2020). *Cisco Annual Internet Report (2018–2023) White Paper*. Abgerufen von: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[4] OPC Foundation. (2022). *OPC 10000-21: UA Part 21: Device Onboarding*. Abgerufen von: https://reference.opcfoundation.org/Onboarding/v105/docs/

[5] Paar, C., Pelzl, J., Güneysu, T. (2024). *Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms* (pp. 1-543). Springer.

[6] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W. (2008). *Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile* (No. rfc5280).

[7] Internet Engineering Task Force (IETF). (2008). *RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)*

Profile, Section 4.1.2.2. Abgerufen von: https://datatracker.ietf.org/doc/html/rfc5280

[8] Internet Engineering Task Force (IETF). (2018). *RFC 8446, The Transport Layer Security (TLS), Internet Engineering Task Force (IETF)*. Abgerufen von: https://datatracker.ietf.org/doc/html/rfc8446

[9] Modbus Organization. (2006). MODBUS Messaging in TCP/IP Implementation Guide V1.0b, Modbus Organization. Abgerufen von: https://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[10] PROFIBUS Nutzerorganisation e.V. (2018). Profinet (Process Field Network). Abgerufen von: https://de.profibus.com/downloads/profinet-field-devices

[11] Internet Engineering Task Force (IETF). (2011). RFC 6071, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, Internet Engineering Task Force (IETF). Abgerufen von: https://datatracker.ietf.org/doc/html/rfc6071

[12] Microsoft. (2020). *Microsoft-Remotedesktop Protocol (RDP)*. Abgerufen von: https://learn.microsoft.com/en-us/windows/win32/termserv/remote-desktop-protocol

[13] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., Watsen, K. (2021). Bootstrapping remote secure key infrastructures (BRSKI). *RFC 8995*.

[14] Cooper, G., Behm, B., Chakraborty, A., Kommalapati, H., Mandyam, G., ARM, H. T., & Bartsch, W. (2021). Fido device onboard specification 1.1. *FIDO Device Onboard Specification, 1*.

[15] Internet Engineering Task Force (IETF). (2018). RFC 8366, A Voucher Artifact for Bootstrapping Protocols, Internet Engineering Task Force (IETF). Abgerufen von: https://datatracker.ietf.org/doc/rfc8366/

[16] Internet Engineering Task Force (IETF). (2019). RFC 8572, Secure Zero Touch Provisioning (SZTP), Internet Engineering Task Force (IETF). Abgerufen von: https://datatracker.ietf.org/doc/html/rfc8572

[17] Internet Engineering Task Force (IETF). (2000). RFC 2898, PKCS #5: Password-Based Cryptography Specification Version 2.0, Internet Engineering Task Force (IETF). Abgerufen von: https://datatracker.ietf.org/doc/html/rfc2898

AUTOR:INNEN

Rohit Bohara, Chief Technology Officer bei der asvin GmbH, hat umfangreiche Erfahrung mit eingebetteten Systemen. Er begann seine berufliche Laufbahn bei LG Soft India, Bangalore im Jahr 2013 und wechselte 2015 zu AMD als Firmware-Ingenieur. 2016 zog er nach Stuttgart, um seinen Master in Embedded Systems zu machen. Die Sicherheit von IoT-Geräten unter Verwendung neuer Methoden und Technologien wie Blockchain, KI und IPFS ist sein Spezialgebiet. Seit 2018 ist er als CTO der asvin GmbH für die technologische Exzellenz verantwortlich.

Rohit Bohara
Chief Technology Officer
asvin GmbH
Eichwiesenring 1/1
70567 Stuttgart
✆ +49 711 2 20 40 93 80
@ rohit.bohara@asvin.io

Florian Handke ist Leiter Industrial Security am Campus Schwarzwald, einem Cluster von Unternehmen aus dem Maschinenbau und der produzierenden Industrie. Ursprünglich mit einem Abschluss in Produktionstechnik (MSc.), umfasst sein Aufgabengebiet die sichere Gestaltung von industriellen Maschinen und Komponenten.

Alexander Harig ist seit über sechs Jahren als Software-Engineer und -Architekt im Bereich der PKI und IAM tätig. Dabei liegt ein Fokus insbesondere auf OT-Umgebungen und deren Besonderheiten.

Dominik Isaak verfügt nach dem erfolgreichen Abschluss seines Wirtschaftsinformatikstudiums mit Schwerpunkt auf Cyber-Sicherheit über umfassende Kenntnisse in Wirtschaftsinformatik und IT-Sicherheit. Seit Ende 2020 ist er bei der achelos GmbH in Paderborn tätig, zunächst als dualer Student und inzwischen als Security Consultant im Bereich Public Key Infrastructure. In dieser Rolle konzentriert er sich auf die Entwicklung und Implementierung kryptografischer Lösungen für sicherheitskritische Anwendungen.

Prof. Dr.-Ing. Jan Pelzl arbeitet seit 1994 arbeitet im Gebiet der IT-Sicherheit und hat seit dem 1. Januar 2015 hat die Professur für Computer Security an der Hochschule Hamm-Lippstadt inne. Darüber hinaus gibt erKurse der Datensicherheit und Einführung in die Kryptographie für die Industrie, z. B. an der TÜV-Akademie Rheinland, International School for IT Security und Ruhr-Universität Bochum. Prof. Pelzl ist Autor von „Understanding Cryptography“, eines der führenden Lehrbücher für Kryptographie, das an über 250 Universitäten und Hochschulen in Lehre und Forschung eingesetzt wird.

Andreas Philipp ist Business Development Manager bei Primekey und zuständig für die Bereiche Industrial IoT-Lösungen.

Claudia Priesterjahn hat als promovierte Informatikerin mehr als 15 Jahre Erfahrung im Software-Engineering und der IT-Security sowohl in der angewandten Forschung als auch der Industrie. Seit 2018 ist sie bei der achelos GmbH in Paderborn tätig, einem Systemhaus für Cybersicherheit und digitales Identitätsmanagement, und seit 2023 Team Lead für den Bereich eHealth Development & Consulting. Als Expertin konzentriert sie sich auf kryptografische und technische Lösungen für sicherheitskritische Anwendungsbereiche und ist verantwortlich für die Forschungsprojekte der achelos.

Christian Schwinne ist Wissenschaftlicher Mitarbeiter im Projekt Trustpoint und entwickelt privat die Open Source Software "WLED". Im Masterstudium Business and Systems Engineering an der HSHL, abgeschlossener B. Eng. in Intelligent Systems Design.