

„Ulrich Jumar, Christian Diedrich (Hrsg.):
EKA 2024 - Entwurf komplexer Automatisierungssysteme, 18. Fachtagung“

Industrielle Sicherheit durch Zertifikatsmanagement-Konzepte im Lebenszyklus einer Produktions-Gray-Box

Marwin Madsen¹, Mike Barth²


Abstract: Die zunehmende IT/OT-Security-Bedrohung für Industrieanlagen führt zu neuen Regelungen wie dem EU Cyber Resilience Act. Gleichzeitig werden Innovationen wie modulare Produktionssysteme vorangetrieben, was zu Veränderungen der Automatisierungsarchitektur und damit auch zu bestehenden Angriffsvektoren führt. Bestehende Sicherheitskonzepte müssen für diese Entwicklungen überprüft werden, wobei die Verwendung von Zertifikaten und damit die Nutzung einer Public-Key-Infrastruktur für viele Sicherheitsmechanismen grundlegend ist. In diesem Artikel werden insbesondere neue Systemarchitekturen wie modulare Produktionszellen oder vernetzte Maschinenteile unter dem Aspekt der Sicherheit analysiert. Dazu werden verschiedene Architekturprinzipien wie Gray- und Black-Box als Grundlage herangezogen und in den Kontext des Zertifikatsmanagements gestellt.

Keywords: IT/OT-Security, PKI, Modularisierung

1 Einleitung

Während die Modularisierung in der diskreten Fertigungsindustrie bereits Stand der Technik ist, werden auch in der Prozessindustrie erste Ansätze verfolgt. Eines der Hauptziele von Modularisierungsstrategien ist es, ein Modul mit einem geringen Engineering-Aufwand hinsichtlich der notwendigen Integration oder Rekonfiguration bereitzustellen. In diesem Zusammenhang werden häufig Begriffe wie Gray- und Black-Box verwendet. Diese Konzepte dienen zwei Zwecken: erstens der Verringerung des Aufwands für den Betreiber und zweitens der Ermöglichung einer generischen Produktion für Hersteller ohne Offenlegung des geistigen Eigentums [Pr19]. Es ist jedoch wichtig, ein Gleichgewicht zwischen Flexibilität und Sicherheit zu finden und da die Sicherheit eines Systems nicht zu Gunsten seiner Flexibilität vernachlässigt werden darf, sind umfangreiche Zusatzkonzepte erforderlich. In diesem Beitrag wird Sicherheit in der Ausprägung IT/OT-Security thematisiert. Solche Zusatzkonzepte für die Sicherheit sind abgestimmt auf die Modularisierung lediglich vereinzelt veröffentlicht vorhanden [Ma23]. Dies steht jedoch im Widerspruch zu Konzepten wie „Security by Design“ und aufkommenden Regulierungen, beispielsweise in Form des European Cyber Resilience Act (CRA) [Ch23]. Darüber hinaus weisen jüngste Berichte auf zahlreiche Schwachstellen in klassischen Gerätefamilien und die kontinuierliche Entdeckung neuer Malware hin

¹ Karlsruher Institut für Technologie, Institut für Reglungs- und Steuersysteme, Fritz-Haber-Weg 1, 76131 Karlsruhe, marwin.madsen@kit.edu,  <https://orcid.org/0009-0006-9953-2382>

² Karlsruher Institut für Technologie, Institut für Reglungs- und Steuersysteme, Fritz-Haber-Weg 1, 76131 Karlsruhe, mike.barth@kit.edu,  <https://orcid.org/0000-0003-2337-063X>

[Gt23]. Die richtige Balance zwischen Flexibilität und Sicherheit zu finden, bleibt ein kritischer Aspekt moderner industrieller Prozesse.

Eine zentrale Komponente der Sicherheit in der OT ist die Verwendung von X.509-Zertifikaten für Aspekte wie Verschlüsselung, Authentizität und Integrität [Se23]. Diese Zertifikate erfordern sowohl eine Public-Key-Infrastruktur (PKI) als auch Mechanismen zur Verteilung der Zertifikate. Dies kann von manueller Interaktion bis hin zu vollautomatischen Zertifikatsmanagement (ZM) wie dem Certificate Management Protocol (CMP) [Ad05] reichen. Viele der in der OT verwendeten Technologien oder Protokolle erfordern für die Sicherheitsmechanismen entsprechend ausgerollte Zertifikate. Insbesondere die Standardisierungsorganisation PI (PROFIBUS\&PROFINET International), ODVA, Inc., OPC Foundation und FCG (FieldComm Group), die Protokolle wie PROFINET, Ethernet/IP, OPC UA und HART-IP spezifizieren, setzen auf diese als Schlüsselement [Wa22, Op23, Ni19]. Einige dieser Organisationen definieren auch ihre eigenen Spezifikationen für ZM. So beschreibt beispielsweise die OPC Foundation sowohl grundlegendes ZM in OPC UA Part 2 [Op23] als auch einen so genannten CertificateManager in OPC UA Part 12 [Op22a] sowie die Authentifizierung eines neuen Gerätes und das Ausrollen von Zertifikaten durch den Betreiber (Onboarding) in OPC UA Part 21 [Op22b]. Obwohl diese Ansätze für ihre jeweilige Industriedomäne bzw. die vorgesehene Anlagenarchitektur funktionieren, bleiben konzeptionelle Fragen im Hinblick auf eine generische und architekturunabhängige Forschungsperspektive bestehen. Die einzelnen Ansätze führen zu impliziten Architekturentscheidungen wie dem direkten Kontakt mit einem Registrar in OPC UA Part 21 oder einer PKI Management Entity in CMP.

Im Folgenden soll der Begriff "*Modul*" nicht auf ein unternehmens- oder domänenspezifisches Konzept oder ein entsprechendes Informationsmodell, wie z.B. das Module Type Package [Au20] aus der Prozessindustrie, bezogen werden. Um diese Unterscheidung zu betonen, wird im Folgenden anstelle des Begriffs Modul der Begriff Produktions-Gray-Box (PGB) verwendet. Die PGB ist eine Gerätekomposition mit mindestens einer dedizierten Modulschnittstelle (MS). Zusätzlich enthält diese Komposition weitere sogenannte modulinterne intelligente Einheiten (MIE). Intelligent bezieht sich in diesem Zusammenhang auf die zugehörige Kommunikation auf einer Ebene, die die Verwendung von Zertifikaten einschließt. Wenn diese untergeordneten MIE nach außen hin nicht offengelegt werden, ergeben sich aus Sicht des Lebenszyklus von Zertifikaten erhebliche Sicherheitsprobleme. Abb. 1 zeigt die Ausgangssituation beim Onboarding einer PGB. Der Hersteller ist für die funktionierende Kommunikation in der PGB verantwortlich und hat daher bereits entsprechende Zertifikate ausgerollt. Die einzige Kommunikationsmöglichkeit für die PKI des Betreibers ist über die MS, weshalb Zertifikate nicht direkt an die MIE verteilt werden können.

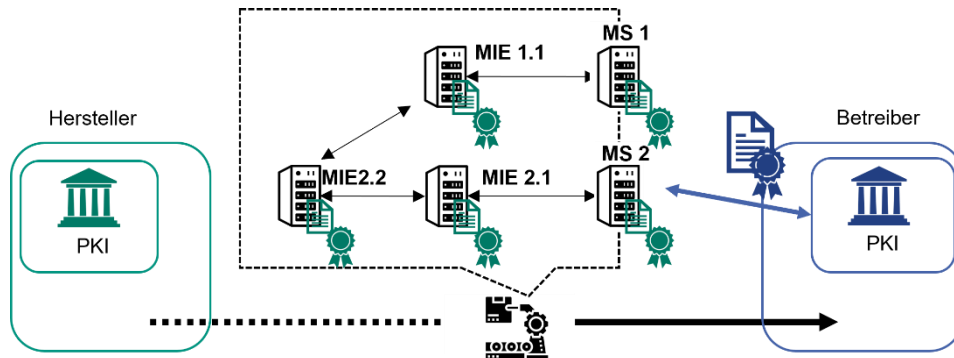


Abb. 1: Betrachtete modulare Architektur und Ausgangssituation während des Onboardings

Es ist zu betonen, dass die hier betrachtete Architektur einer PGB eine entscheidende Voraussetzung ist und nicht in jedem Fall zutrifft. So kann beispielsweise eine PGB, die neben der MS intern nur mit Motoren oder Sensoren mittels 4-20 mA Stromstärke kommuniziert, keine Zertifikate nutzen. Moderne IoT-Konzepte tendieren jedoch zu immer komplexeren PGB mit zahlreichen MIE. Sobald ein Plug&Produce-Konzept angestrebt wird, ist die hierarchische Struktur aus Abb. 1 eine sinnvolle Annahme. Einfache Beispiele finden sich bereits in der Praxis [Si24], in Veröffentlichungen von Standardisierungsorganisationen wie NIST [St22] und wurden auch in Gesprächen mit Industriepartnern des Instituts für Regelungs- und Steuerungssysteme verifiziert. Im Maschinenbau ist es üblich, einen Motion Controller einzusetzen, der die Antriebe, Aktoren und Sensoren steuert. Der Maschinenbauer installiert den Motion Controller dann als Ethernet-basiertes Feldbusgerät unterhalb einer speicherprogrammierbaren Steuerung (SPS). Ein Beispiel für den Feldbus wäre PROFINET. Die Antriebe können in der Regel über eine geroutete Engineering-Kommunikation erreicht werden, um deren Zustand zu überwachen oder Änderungen an deren Konfiguration vorzunehmen. Diese Maschinenzelle wird dann in die Anlage des Betreibers integriert, wobei die SPS als Schnittstelle zur Maschine fungiert. Darüber hinaus sind die von der SPS vom Anlagennetzwerk abgekapselten Komponenten oft noch direkt mit einem mobilen Engineering-Gerät z.B. über eine USB-Schnittstelle erreichbar. Dies entspricht dem einfachsten Fall der in Abb. 1 betrachteten Architektur, in der es eine MS und eine MIE sowie eine große Anzahl weiterer, nicht im Fokus stehender Komponenten gibt.

2 Threat Modelling

Die Notwendigkeit von Zertifikaten im Allgemeinen lässt sich aus bestehenden Sicherheitskonzepten und deren Abhängigkeit von der Verwendung von Zertifikaten ableiten [Wa22, Ni19, Op23]. Allerdings muss die Bedrohungslage berücksichtigt werden, wenn Entitäten innerhalb einer PGB keinen Zugang zu Zertifikaten haben.

Eine sorgfältige Netzwerksegmentierung mit geeigneten Intrusion-Prevention-Systemen verhindert, dass ein Angriffsvektor in die PGB geschaffen wird, da die Kommunikation nur über die dedizierte MS möglich ist. Bestehende und bewährte ZM-Konzepte sind vollständig auf die MS anwendbar, da ein direkter Kontakt mit der PKI möglich ist. Allerdings ist zu bedenken, dass es zwar zunächst keinen Kommunikationskanal auf Softwareebene zu den MIE neben der MS gibt, aber ein physischer Zugriff möglich sein kann. Zu diesem Zweck wurde früher das Konzept der Sicherheit durch Abschottung verwendet, das heute jedoch als durchlässig gilt [Hu19]. Obwohl das Ziel darin besteht, so weit wie möglich eine Black-Box zu schaffen, ist dies nicht ganz zweckmäßig. So muss es beispielsweise möglich sein, defekte MIE auszutauschen, und in manchen Umgebungen kann eine bewusste Entscheidung gegen Remote-Updates getroffen werden, was bedeutet, dass ein lokaler Zugriff zur Installation dieser Updates möglich sein muss. Die MS kann auch durch sogenannte Zero-Day-Exploits (Angriffe am ersten Tag nach der Entwicklung eines neuen Angriffsvektors) kompromittiert werden, insbesondere wenn sie für die Kommunikation in der Cloud bestimmt ist. Eine Kompromittierung dieser würde sich bis in die PGB fortsetzen, da eine zentrale Instanz nicht wie bei Zertifikaten nach der Entdeckung eine Revokation vornehmen kann, sondern ein manueller Eingriff notwendig ist. Nach dem Defense-in-Depth-Konzept [KF06] sollte es mehrere Sicherheitsschichten geben. Bei automatisiertem ZM wäre es sinnvoll, die Vorteile der Zertifikate bis in die PGB hinein zu nutzen. Insbesondere wenn PGB durch die neuen Entwicklungen einen dynamischeren Kontext aufweisen als klassische Varianten, müssen Fallback-Mechanismen für mögliche Fehlerpotentiale berücksichtigt werden.

Zahlreiche Bedrohungsanalysen der letzten Jahre sind auf die hier betrachtete Architektur adaptierbar und behalten Gültigkeit in Ihrer Argumentation [NM22]. Darüber hinaus betonen sowohl Kommunikationstechnologien als auch Sicherheitsstandards die Bedeutung einer PKI [Wa22, Se23]. Insbesondere die Arbeiten im Bereich Ethernet-APL zeigen den Bedarf an Zertifikaten. Diese basieren auf einem konvergenten Netzwerk, also dass alle Komponenten einer Produktionszelle an das gleiche Netz angeschlossen sind und ein einheitliches Protokoll verwendet wird. Das heißt, die hierarchische Struktur klassischer Automatisierungssysteme wird aufgebrochen und alle Komponenten können alle anderen zumindest kommunikativ erreichen. So hätten beispielsweise Engineering- und Operator-Stationen direkten Zugriff auf Feldgeräte. Dies berücksichtigt jedoch nicht die Entwicklung flexibler Automatisierungsarchitekturen, in denen zwar ein konvergentes Netzwerk möglich ist, aber dennoch hierarchische Strukturen zwischen MS und einer Orchestrierungsebene bestehen. Wird dieses Merkmal in die Architektur der Bedrohungsanalyse integriert, bleibt die Notwendigkeit für den Einsatz von Zertifikaten bestehen: Die bisher verwendeten Protokolle zwischen Feld und Steuerung - nämlich PROFIBUS DP, PROFIBUS PA und HART - ermöglichten keine sichere Kommunikation. Angesichts der zunehmenden Verbreitung von IP-basierten Protokollen, die durch höhere Datenraten und eine vereinfachte Installation, Konfiguration und Wartung von Geräten und Automatisierungstechnik getrieben werden, wäre das einzige Gegenargument gegen den Einsatz ihrer Sicherheitsmechanismen, wenn ein unverhältnismäßig hoher Aufwand für deren Implementierung notwendig wäre [Se23].

3 Analyse bestehender Spezifikationen

Bestehende Spezifikationen gehen bereits umfassend auf das ZM während des gesamten Lebenszyklus eines Geräts ein. Insbesondere das Onboarding und die nachfolgenden Interaktionen mit dem Betreiber werden detailliert betrachtet. Das Ausrollen von Zertifikaten in die MS ist bereits ein üblicher Betrachtungspunkt, da sie direkt mit dem Netz des Betreibers kommuniziert, welches eine Komponente zur Anbindung an die PKI enthalten sollte. Im Folgenden soll geprüft werden, ob sich die beschriebene Architektur einer PGB nahtlos in die bestehende Landschaft einfügt, insbesondere wenn auch die MIE mit Zertifikaten versorgt werden sollen.

3.1 Certificate Management Protocol

Es gibt eine Vielzahl von ZM-Protokollen, die hier nicht behandelt werden können. Eines der umfassendsten Protokolle ist das CMP, das den größten Teil des Lebenszyklus eines Zertifikats abdeckt. Es ist zu beachten, dass der Schwerpunkt des Lebenszyklus auf dem Zertifikat und nicht auf dem Gerät liegt. Es basiert auf authentifizierten, in sich geschlossene Nachrichten und ist daher nicht auf spezielle Transportprotokolle wie TLS beschränkt. Stattdessen kann es auch in Umgebungen mit eingeschränkten Ressourcen verwendet werden. Für CMP werden in diesem Abschnitt sowohl der ursprüngliche Standard in RFC 4210 [Ad05] als auch der industriegetriebene Entwurf eines Lightweight CMP Profile [BOF23] analysiert. RFC 4210 klassifiziert PKI-Entitäten in End Entities (EE), Registration Authorities (RA) und Certification Authorities (CA). Die beiden letztgenannten Entitäten sind Teil des PKI-Managements, und wenn keine Notwendigkeit besteht, zwischen ihnen zu unterscheiden, werden sie als PKI-Management-Entität bezeichnet. Im RFC 4210 wird nicht explizit auf die Möglichkeit von Proxys zwischen der EE und einer PKI Management Entity eingegangen. RFC 6712 hingegen enthält eine Spezifikation von HTTP als Transportprotokoll für CMP und weist darauf hin, dass HTTP die Überwindung von Netzwerkgrenzen durch die Verwendung von allgegenwärtigen Proxys erleichtert [KP12]. CMP-Nachrichten enthalten zwar keine sensiblen Informationen, die die PKI-Sicherheit gefährden könnten, aber es besteht die Möglichkeit, dass vertrauliche technische oder geschäftskritische Informationen beobachtet werden. Daher wird die Verwendung von TLS oder VPNs empfohlen. Die MS genießt zwar aufgrund ihres Onboardings ein gewisses Vertrauen, doch sollte dieses nicht allumfassend sein. Stattdessen sollte es für die vorgesehenen Aufgaben nach dem Prinzip der geringsten Privilegien eingeschränkt werden. Dieser Ansatz stellt sicher, dass nur die notwendigen Berechtigungen erteilt werden und mindert das Risiko eines möglichen Missbrauchs der Proxy-Stellung. Ein zentraler Baustein einer PKI ist die Sperrung von Zertifikaten und der damit verbundene Zugriff auf Sperrlisten. In diesem Zusammenhang wäre ein solcher Zugriff jedoch nur über die MS möglich. Folglich würde sich jede Kompromittierung der MS direkt auf die gesamte PGB auswirken. Ein anderer Ansatz wäre die MS als RA für die PGB zu nutzen. Es wird sogar ausdrücklich betont, dass die Einrichtung von RAs ein Implementierungsproblem ist, und es lediglich vorausgesetzt wird, dass eine RA

zertifiziert ist und über einen privaten Schlüssel zum Signieren verfügt. Ein MS könnte daher nach dem Onboarding als RA betrachtet werden. Die CMP-Spezifikation RFC 4210 definiert jedoch mehrere obligatorische PKI-Funktionen (sowie weitere empfohlene und optionale Funktionen), die RAs bereitstellen müssen und die keinen sinnvollen Overhead für MS darstellen würden.

Zusätzlich zu den bestehenden Entitäten spezifiziert das Lightweight CMP Profile auch eine Local Registration Authority (LRA), die eine RA mit Nähe zur Endentität darstellt. Dies hebt zum einen hervor, dass Produktionssysteme hierarchisch aufgebaut sind und die meisten Entitäten keinen direkten Kontakt zu zentralen Instanzen haben und zum anderen, dass PKI-Verwaltungsinstanzen wie CAs in besonders abgeschotteten Umgebungen gesichert werden müssen. Anstatt Zertifikatsanfragen durch mehrere Netzwerke zu einer zentralen CA oder RA zu schleifen, kann eine LRA bereits innerhalb desselben Netzwerks wie die Entität Prüfungen durchführen. Allerdings wird auch in diesem Zusammenhang nicht diskutiert, ob sich eine LRA zwingend im gleichen Netz befinden muss oder ob CMP-Nachrichten ohne Sicherheitsbedenken über einen Proxy an die nächste PKI-Verwaltungsinstanz gesendet werden können. In der hier betrachteten Architektur ist jedoch genau dies der Fall. Die MS ist nämlich keine klassische LRA, sondern ein notwendiger Proxy. Wenn die MS an die Stelle einer LRA treten sollte, gibt es den Anwendungsfall "FwdKeep", bei dem die CMP-Nachricht ohne Änderungen weitergeleitet wird und somit de-facto als Proxy fungiert. Obwohl die MS diese Proxy-Funktionalität bereitstellen könnte, müssen LRAs auch mindestens "FwdAddS" ermöglichen, d. h. das Hinzufügen einer Schutzschicht zur bestehenden CMP-Nachricht vor deren Weiterleitung. Die ursprüngliche Authentifizierung wird also nicht verändert, während die LRA gemäß der Spezifikation die Anfrage erfolgreich validiert und genehmigt. Darüber hinaus sollte eine LRA auch weitere PKI-Verwaltungsfunktionen implementieren, einschließlich der Fähigkeit, Zertifikate im Namen von Endteilnehmern zu widerrufen.

Es bleibt unklar, ob bei der Kommunikation zwischen EE und LRA eine Berücksichtigung von Proxys vorgesehen ist oder wie eine LRA eingerichtet wird. Insbesondere da der Proxy kein vorheriger Bestandteil des Anlagennetzwerk des Betreibers wäre. Beide Ansätze sind jedoch gültig und sollten bewertet werden.

3.2 OPC UA

Als Kommunikationstechnologie verfügt OPC UA über eine umfassende Spezifikation für Zertifikate, einschließlich Part 2 [Op23], 12 [Op22a] und 21 [Op22b], die in Bezug auf die PGB-Architektur analysiert wurden. Teil 2 unterstreicht, dass Zertifikate die grundlegende Komponente zur Gewährleistung der Sicherheit in OPC UA sind. Der Lebenszyklus eines Geräts nach Part 21 verdeutlicht, dass Sicherheitskonzepte unter potenziell komplexen Lieferketten, mehreren beteiligten Akteuren und komplexen Architekturen berücksichtigt werden müssen. Wo es früher nur ein Gerät mit einer Herstellerzertifikate als Ausgangspunkt gab, gibt es jetzt ein zusammengesetztes Gerät

oder, in der Bezeichnung dieser Arbeit, eine PGB, die ein oder mehrere MS und MIE hat. OPC UA Part 21 erkennt an, dass in der Industrie nicht nur isolierte Einheiten, sondern miteinander verbundene Systeme involviert sind. Diese Systeme bestehen aus Gerätenetzwerken, in denen PGB durch andere Maschinenbauer zu neuen PGB erweitert werden können. Es wird davon ausgegangen, dass PGB eine Abstraktion innerhalb eines Netzes sind und nur von einem oder mehreren nach außen sichtbaren Geräten, d. h. von ihren MS, physisch erreicht werden können. Es wird davon ausgegangen, dass die internen Interaktionen zwischen MIE vom Maschinenbauer konfiguriert werden.

Die entscheidende Divergenz zwischen Part 21 und der bestehenden Bedrohungsanalyse in Abschnitt 2 besteht darin, dass OPC UA allenfalls die Bereitstellung von Zertifikaten an die MS anerkennt. Dies spiegelt sich in der Definition der Composite Identity wider, in welchem bereits die Provisionierung der MS nur in die Kategorie „may“ eingeordnet wird und MIE nicht erwähnt werden. Außerdem wird das Composite-Konzept in erster Linie nur für den Authentifizierungsprozess verwendet, nicht aber für das anschließende Ausrollen der Zertifikate. Die Device Configuration Application (DCA) wird als zuständige Instanz für die Verwaltung der Zertifikate für die Anwendungen definiert und läuft auf Geräteebene. Aufgrund der Annahmen in der Composite Identity, dass höchstens MS, provisioniert werden, gibt es keine Spezifikationen des Zusammenspiels der DCA, die auf dem MS läuft, und den MIE. Dies setzt sich in Part 12 fort, wo, ähnlich wie bei den ZM-Protokollen, eine direkte Kommunikation zu einem CertificateManager gefordert wird, der die Form einer RA darstellt. Somit bietet OPC UA derzeit keine expliziten Mechanismen für die Provisionierung der MIE außer manuellen Methoden.

4 Ableitung von Forschungsfragen und Lösungsvektoren

Ein naheliegendes Konzept besteht darin, die MIE in das bestehende ZM zu integrieren. Hierbei können viele Betrachtungen aus klassischen Systemen adaptiert werden. Es bleibt zu klären, ob die MS das ZM für alle MIE gegenüber der PKI des Betreibers übernehmen kann, oder ob eine vollständige Implementierung bis hinunter zu jeder MIE notwendig ist. Typischerweise ist die Beantragung im Namen einer anderen Entität nur für besonders vertrauenswürdige Geräte zulässig, da sonst zusätzliche Angriffsvektoren geschaffen würden. Es ist daher notwendig, die Bedingungen für die sichere Einrichtung einer RA zu spezifizieren und dann zu prüfen, ob bestehende Onboarding-Prozesse der MS ein ausreichendes Sicherheitsniveau bieten können. Es ergibt sich die folgende Forschungsfrage:

R1. Was sind die Anforderungen an eine MS und einen Onboarding-Prozess um das ZM für MIE zu übernehmen?

Die Alternative wäre, dass die MIE das gleiche Onboarding durchlaufen wie die MS. MIE sind jedoch in der Regel nicht Teil desselben Netzes wie die PKI oder die RA. Folglich müssten sie die MS als Stellvertreter nutzen. Dies zwar theoretisch machbar, würde aber verfahrenstechnische Anpassungen des Onboardings erfordern. Beispielsweise spielt bei

OPC UA Part 21 ein Discovery-Service eine zentrale Rolle. Eine Anpassung könnte auch vorsehen, dass die PGB über die MS hinreichend authentifiziert werden, so dass die MIE nur noch in das Ausrollen der Zertifikate integriert werden müssten. So könnte die MS nach erfolgreichem Onboarding die MIE mit Daten über die PKI-Management-Entity versorgen. Anschließend könnten die MIE den Prozess der Zertifikatsbeantragung mit der MS als Proxy einleiten. Wie jedoch in Abschnitt 3 hervorgehoben wurde, fehlt in der derzeitigen Landschaft eine explizite Sicherheitsbetrachtung hinsichtlich der Verwendung von Proxys im ZM. Insbesondere die Revokation ist noch nicht hinreichend für diesen Fall betrachtet. Auch das Zusammenspiel zwischen MS und MIE müsste spezifiziert werden, da automatisierte Prozesse nur über standardisierte Schnittstellen möglich sind.

R2. Wie können neue Angriffsvektoren abgeschwächt werden, wenn die MS als Proxy für das ZM der MIE verwendet wird?

Eine weitere Konzeptvariante im Sinne der Modularisierung sieht die Entwicklung einer modulminimalistischen PKI vor. Diese PKI soll auf möglichst wenige Funktionalitäten reduziert werden, so dass sie ZM intern innerhalb eines PGB übernehmen kann. Ähnliche Ansätze werden bereits in anderen Domänen verwendet, z.B. in mobilen Umgebungen [TB08]. Der Grund dafür liegt darin, dass die MIE selbst nicht mit dem System des Betreibers interagiert. Sie benötigt lediglich Zertifikate für die interne Kommunikation. Es besteht daher keine zwingende Notwendigkeit, diese in die PKI des Betreibers zu integrieren. Allerdings bedeutet dieser Ansatz zunächst einen technologischen und prozessualen Mehraufwand für die PGB, der in späteren Arbeiten detailliert untersucht werden soll. Automatisierte Engineering-Methoden können diesen Prozess vereinfachen. Ermöglicht wird diese Konzeptvariante insbesondere durch die von dem CRA vorgeschriebenen Updates [Ch22]. Diese Updates ermöglichen eine kontinuierliche Anpassung der internen PKI an die laufende Evaluierung von kryptographischen Algorithmen. Von besonderem Interesse für eine solche modulminimalistische PKI sind Weiterentwicklungen von PKI-Ansätzen aus der Informatik. Während die Herausforderungen einer PKI in der OT - vor allem die Komplexität - und in der IT divergieren, bietet eine PGB ein relativ geschlossenes System und Anpassungspotential.

R3. Wie können bestehende ZM-Ansätze so angepasst oder erweitert werden, dass sie die autonome Natur der betrachteten Architektur nutzen können?

Die Analyse der bestehenden Spezifikationen zeigt einen weiteren Bedarf auf. So zielen beispielsweise Modularisierungsstrategien auf einen Plug&Produce-Prozess ab, bei dem Schnittstellen definiert werden und Konfigurationsparameter möglichst automatisch übernommen werden können. Die Verwendung von Zertifikaten allein bis hin zur MS, geschweige denn innerhalb der PGB, unterscheidet sich jedoch je nach PGB-Typ und der PKI-Unterstützung des Betreibers für das Onboarding und das nachfolgende ZM. Selbst wenn die PKI des Betreibers mehrere der zahlreichen Technologien unterstützt, gibt es keine Möglichkeit, dies in den bestehenden Informationsmodellen automatisch auszulesen. Selbst die viel diskutierte Asset Administration Shell bietet noch kein Submodell, das den Modularisierungsansatz auf die Sicherheit überträgt. Zwar ist ein

Teilmodell namens Security Engineering in der Entwicklung, doch liegt dessen Schwerpunkt eher auf der Ermöglichung strukturierter Sicherheitsentscheidungen durch die Hersteller [Re24]. Dies schließt natürlich die Anwendbarkeit auf die dargestellten Herausforderungen nicht aus, aber es ist offensichtlich, dass das Erreichen von Plug&Produce derzeit mit ZM nicht möglich ist, ganz zu schweigen von den verschiedenen anderen Sicherheitsmechanismen.

R4. Inwieweit ist das Ziel der Modularisierung, d.h. eine herstellerunabhängige, automatische Integration mit geringem Aufwand, für Sicherheitsmechanismen realisierbar und welche Modifikationen sind erforderlich?

5 Zusammenfassung & Ausblick

In dieser Arbeit wurde die Architektur einer PGB definiert und untersucht. Bei dieser Architektur könnte es sich zum Beispiel um eine Maschinenzelle mit mehreren internen Geräten und internen Kommunikationsprotokollen handeln, die auf X.509-Zertifikaten für die Sicherheit beruhen. Die PGB-Architektur wird in der Industrie bereits eingesetzt und dürfte sich aufgrund der fortschreitenden technologischen Entwicklung weiterverbreiten. Es wurde eine prägnante Bedrohungsanalyse speziell für diese Architektur durchgeführt, die auf das Rational bestehender Bedrohungsanalysen für Zertifikate in OT-Systemen zurückgreift. Die Ergebnisse zeigen, dass Zertifikate nicht nur für die PGB-Schnittstelle im Anlagennetzwerk, sondern auch für die internen Geräte erforderlich sind. Anschließend wurde die Anwendbarkeit bestehender und etablierter ZM-Protokolle und ZM aus Kommunikationstechnologien im Zusammenhang mit dieser Architektur bewertet. Es ergibt sich, dass diese bestehenden Ansätze nicht direkt auf die PGB-Architektur angewendet werden können, ohne dass zusätzliche Sicherheitsbewertungen oder eine explizite Berücksichtigung möglicher Probleme vorgenommen werden. Abschließend wurden mögliche Anpassungsansätze identifiziert und Forschungsfragen skizziert, die in zukünftigen Arbeiten beantwortet werden.

6 Literaturverzeichnis

- [Pr19] Process Industry 4.0: The Age of Modular Production - On the Doorstep to Market Launch. ZVEI – Zentralverband Elektrotechnik und Elektronikindustrie e. V., 2019.
- [Ma23] Madsen, M.; Palmin, A.; Stutz, A.; Barth, M.: Security Analysis of the Module Type Package Concept. In: 21st IEEE International Conference on Industrial Informatics. S. 1-8, 2023.
- [Ch23] Chiara, P.G.: The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements. In: Int. Cybersecur. Law Rev. 3, S. 255–272, 2022.

-
- [Gt23] Ginter, A.; Hale, G.; Machtemes, R.; Molina, J.; Wallhof, M.; Schneider, C.: OT Cyber Threats Report, Waterfall Security Solutions, 2023.
- [Se23] Security for Industrial Automation and Control Systems. International Electrotechnical Commission (IEC), IEC 62443, 2009–2020.
- [Ad05] Adams, C.; Farrell, S.; Kause, T.; Mononen, T.: Certificate Management Protocol (CMP). Network Working Group, RFC 4210, 2005.
- [Wa22] Walz, A.; Berndt, D.; Visoky, J.; Koppers, J.; Wiberg, J.; Armstrong, R.; Vincent, S.; Merklin, S.: FAQ on Industrial Ethernet Security Concepts. Industrial Ethernet Security Harmonization Group, 2022.
- [Ni19] Niemann, K.-H.: IT security extensions for PROFINET.: In IEEE 17th International Conference on Industrial Informatics (INDIN). S. 407-412, 2019.
- [Op23] OPC 10000-2: UA Part 2: Security. OPC Foundation, 2023.
- [Op22a] OPC 10000-12: UA Part 12: Discovery and Global Services. OPC Foundation, 2022.
- [Op22b] OPC 10000-21: UA Part 21: Device Onboarding. OPC Foundation, 2022.
- [Au20] Automatisierungstechnisches Engineering modularer Anlagen in der Prozessindustrie - Allgemeines Konzept und Schnittstellen. Gesellschaft Mess- und Automatisierungstechnik, VDI/VDE/NAMUR 2658, 2013/2020.
- [Si24] SIMOTION D - Drive-based, Siemens AG, mall.industry.siemens.com/mall/de/WW/Catalog/Products/10014179, Stand: 30.04.2024.
- [St22] Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S.: Guide to Operational Technology (OT) Security. National Institute of Standards and Technology, NIST SP 800-82 Rev. 3, 2022.
- [Hu19] Hunt, T.; Jia, Z.; Miller, V.; Rossbach, C. J.; Witchel, E.: Isolation and Beyond: Challenges for System Security. In: Proceedings of the Workshop on Hot Topics in Operating Systems. S. 96-104, 2019.
- [KF06] Kuipers, S.; Fabro, M.: Control Systems Cyber Security: Defense-in-Depth Strategies. Idaho National Lab. (INL), 2006.
- [NM22] Niemann, K.-H.; Merklin, S.: OT security requirements for Ethernet-APL field devices. atp Magazin, 5/2022, 2022.
- [BOF23] Brockhaus, H.; von Oheimb, S.; Fries, S.: Lightweight Certificate Management Protocol (CMP) Profile. Internet Engineering Task Force (IETF), RFC 9483, 2023.
- [KP12] Kause, T.; Peylo, M.: HTTP Transfer for the Certificate Management Protocol (CMP). Internet Engineering Task Force (IETF), RFC 6712, 2012.
- [TB08] Toorani, M.; Beheshti, A.: LPKI - A Lightweight Public Key Infrastructure for the Mobile Environments. In: 11th IEEE Singapore International Conference on Communication Systems. S. 162-166, 2008.
- [Re24] Registered AAS Submodel Templates, Industrial Digital Twin Association e.V., <https://industrialdigitaltwin.org/content-hub/teilm Modelle>, Stand: 30.04.2024.