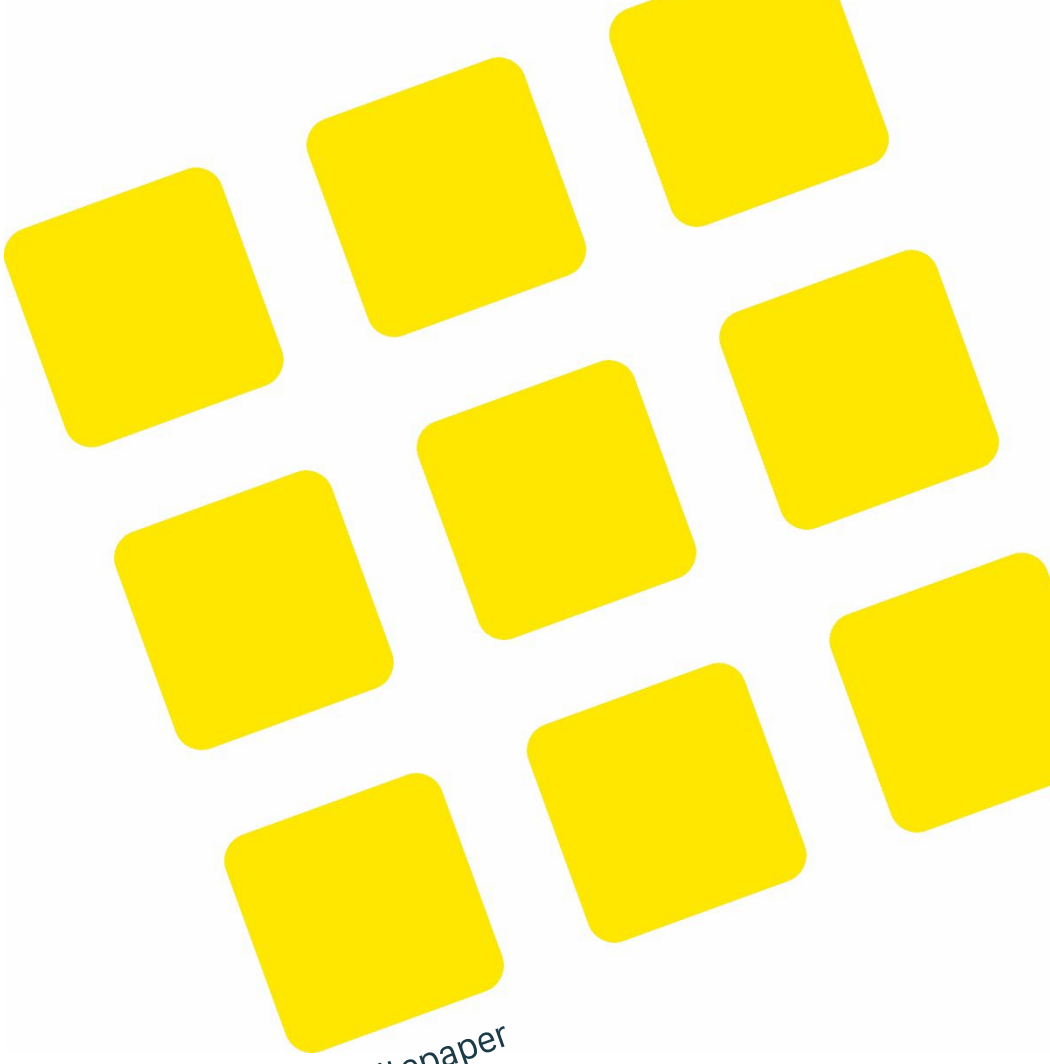

PKI – Schlüssel – Zertifikate

ECOS TrustManagementAppliance

- **Grundbausteine digitaler Sicherheit**
- **Herausforderungen in der Welt von IoT / OT**

ecos

Inhalt

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Einführung

Industrie 4.0 – Konvergenz von OT und IT

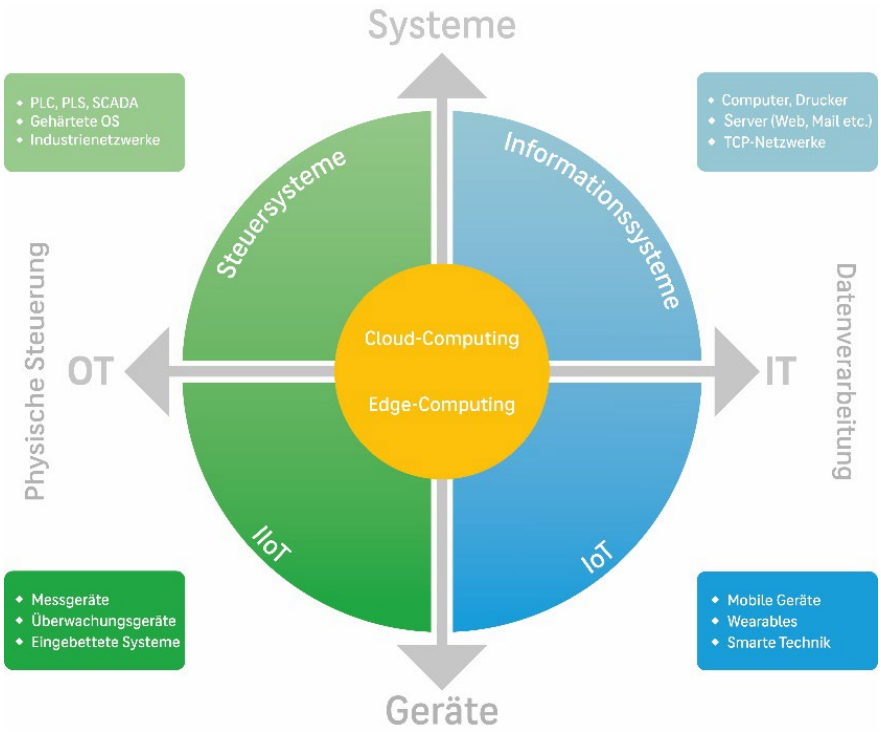

Abbildung 1: Unterschied OT & IT

Nicht nur die menschliche Welt wird durch Globalisierung und Digitalisierung immer vernetzter, mit dem Internet der Dinge (IoT) werden auch immer mehr physische Geräte in Netzwerke eingebunden. Das macht auch im Industriebereich nicht halt.
Lange Zeit war Operational Technology (OT) eine geschlossene Technologie, die abseits der Ethernet-basierten Information Technology (IT) abgeschottet in den Produktionsumgebungen der Industrie eingesetzt wurde. Die Instrumente zur Überwachung und Steuerung physischer Geräte waren mechanisch und diejenigen, die über digitale Steuerkomponenten verfügten, waren zwar miteinander vernetzt, nutzten aber eigene Kommunikationswege und Bussysteme, basierend auf proprietären Protokollen und Schnittstellen.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Das Internet der Dinge oder *Internet of Things (IoT)* ist ein Sammelbegriff für ein System von über das Internet miteinander vernetzten physischen Objekten, die über Sensoren, Verarbeitungsfähigkeiten, Software und andere Technologien verfügen, um Daten auszutauschen.

In der Praxis haben sich auf den jeweiligen Anwendungssektor bezogene Varianten herausgebildet, z.B. das *Internet of Industrial Things (IIoT)* für industrielle Anwendungen oder das *Internet of Medical Things (IoMT)* im Bereich der Medizin.

Dieses Whitepaper verwendet den Begriff IoT synonym für IIoT.

Auch die klassische IT arbeitete jahrzehntelang mit Systemen, die direkt am jeweiligen Unternehmensstandort betrieben wurden. Von der Außenwelt wurden diese Systeme mit Firewalls abgeschirmt, die im Laufe der Jahre weiterentwickelt wurden. Musste von außerhalb auf die Systeme zugegriffen werden, wurde dies i.d.R. durch eine VPN-Verbindung (Virtual Private Network) mithilfe eines entsprechenden Clients auf dem jeweiligen Endgerät ermöglicht.

Als *Operational Technology (OT)* werden Hard- und Software zur Überwachung und Steuerung von industriellen Anlagen, Maschinen, Geräten und ihrer Prozesse bezeichnet.

Im Gegensatz dazu bezeichnet *Information Technology (IT)* Hardware, Software, Kommunikationstechnologien und angeschlossene Dienste, die sich mit dem Verarbeiten, Speichern und Übertragen von Daten befassen.

Das rasante Wachstum des IoT, Trends wie Edge Computing, die (Vor-) Verarbeitung von Daten nahe am physischen Standort von IoT-Geräten, die zunehmende Verbreitung von Ethernet-basierten Vernetzungstechnologien im Industriebereich und die Integration von Cloud-Systemen in Unternehmensinfrastrukturen führen zu einer zunehmenden Konvergenz von OT und IT.

Cloud Computing bezeichnet die Bereitstellung von Computersystemressourcen und Rechenleistung über das Internet (Speicher, Server, Datenbanken, Netzwerke, Software etc.) ohne aktive Verwaltung durch den Nutzer. Daten werden nicht lokal gespeichert, sondern an einem beliebigen, anderen Ort.

Als *Edge Computing* wird die dezentrale Datenverarbeitung am Rand eines Netzwerks, der sogenannten Edge, bezeichnet. Die Daten werden lokal und in Echtzeit am physischen Standort von Geräten oder Maschinen verarbeitet, um Latenzzeiten gering zu halten.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Die Anforderungen an IoT-/OT-Anwendungen liegen in der Erfassung und Berechnung einer großen Menge an Echtzeitdaten am Netzwerkrand (Edge). Durch die zunehmende Verschmel-zung von OT und IT entstehen gleichzeitig neue Sicherheitsanforderungen, die in der OT auf-grund ihrer räumlichen Isolation unbekannt waren.

Zu diesen Anforderungen zählen:

- Authentifizierung von Verbindungen
- Sicherung der Datenübertragung
- Sicherstellung der operationellen Integrität

OT Security birgt spezifische Herausforderungen, die üblicherweise gar nicht mit der klassischen IT Security in Verbindung gebracht werden. So liegt es in der Natur des IoT, dass es sich über die Netzwerkgrenzen der klassischen IT hinaus in Umgebungen erstreckt, wie sie unterschiedlicher nicht sein könnten: Gebäudeautomation, robotergestützte Fertigung, automatisierte Verkehrssysteme, medizinisches und wissenschaftliches Equipment oder z.B. landwirtschaftliches Precision Farming.

Die größte Herausforderung liegt heute in der sicheren Datenverarbeitung und Kommunikation mit Geräten in unterschiedlichsten Umgebungen. Viele IoT-Geräte sind sehr klein und so vorteilhaft dies für die Mobilität ist, so begrenzt ist dadurch auch die Rechenleistung. Es müssen also einerseits durch Edge Computing riesige Mengen an Sensordaten dezentral und in Echtzeit in physischer Nähe der jeweiligen IoT-Geräte verarbeitet werden, um die Latenzzeiten möglichst gering zu halten, andererseits müssen die zur weiteren Auswertung vorverarbeiteten Daten an die Datenzentren der Unternehmen oder in die Cloud weitergereicht werden.

In der Folge bestehen IoT-/OT-Anwendungen aus einer immer komplexer werdenden Kombination aus Hardware, Software und Firmware, sodass es zunehmend schwieriger wird, das Vertrauen in Menschen und Maschinen in seinen Netzwerken zu gewährleisten.

Was ist Zero Trust?

Das frühere Sicherheitsmodell war schlicht: Innen vertrauenswürdig, außen gefährlich.
In den letzten Jahren geriet dieses Modell an seine Grenzen. Immer öfter erfolgen Angriffe von innen heraus, aus der Zone, der oft heute noch zu sehr vertraut wird. Auch wenn im Maschinenbereich, insbesondere im Bereich kritischer Infrastrukturen, das Thema Sicherheit langsam ankommt,

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

existieren immer noch viele Bereiche, in denen die IT-Sicherheit vernachlässigt wird.

Es kann nicht oft genug betont werden, dass durch die rasante Vernetzung die früheren physischen Grenzen zunehmend entfallen, während gleichzeitig die Systeme durch standardisierte Protokolle immer interoperabler werden. Unternehmen müssen daher eine Unzahl von Angriffsvektoren im Blick haben.

Potentielle Angreifer haben es demgegenüber vergleichsweise bequem: Sie müssen nur eine einzige Lücke finden, um in ein System zu gelangen. Dort können sie sich ungesehen, z.B. per Lateral Movement, vorantasten und den Aufbau des Systems erkunden, bis sie die nächste Sicherheitslücke gefunden und irgendwann ihr Ziel erreicht haben.

Die Antwort auf dieses Ungleichgewicht ist die Zero-Trust-Strategie: Jedem wird misstraut, sowohl innerhalb als auch außerhalb des eigenen Netzwerks, egal ob Mensch oder Maschine. Aus dieser Strategie ergeben sich drei gemeinsame Ansätze für die Sicherheit von IT- und OT-Umgebungen:

- Ohne Authentifizierung erfolgt keine Verbindung oder Zugriff
- Der gesamte Netzverkehr muss überprüft werden
- Alle Daten müssen verschlüsselt werden

Eine Zero-Trust-Strategie ist das Gegenteil von in dubio pro reo: Niemand ist vertrauenswürdig, jeder ist verdächtig – bis zum digitalen Beweis des Gegenteils. Die digitale Beweisführung ist dabei nicht beliebig, sondern folgt klar definierten Schutzzielen:

Authentizität
Jede zum Handeln befugte Entität muss anhand einer eindeutig zugewiesenen Identität überprüfbar sein. Die Authentizität von Daten und Informationen gilt erst als sichergestellt, wenn die Entität, von der sie stammen, zweifelsfrei authentifiziert ist.

Vertraulichkeit
Daten dürfen nur von einer Entität gesendet oder abgerufen werden, die hierzu auch als berechtigt definiert wurde.

Integrität
Keine Entität soll Daten unbemerkt oder unerkannt verändern dürfen.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Zurechenbarkeit und Verbindlichkeit
Jede Handlung muss jederzeit der Entität zuordenbar sein, die sie ausgeführt hat. Dieser Entität darf es außerdem nicht möglich sein, ihre Handlung abzustreiten.

Für die Umsetzung eines Zero-Trust-Konzept ist es entscheidend, dass diese Schutzziele bereits in der Entwurfsphase von Anlagen eingeplant und implementiert werden. Alle digitalen Assets (Benutzer, Geräte, Systeme etc.) müssen systematisch erfasst und die benötigten Zugriffsrechte sorgfältig definiert werden.

Zero-Trust-Mechanismen und Security by Design ab der frühsten Planungsphase sind für die Sicherheit von IoT/OT-Infrastrukturen entscheidend.

Welche Rolle spielen Schlüssel und Zertifikate?

Für eine Zero-Trust-Strategie, in der jede Kommunikation zuverlässig authentifiziert werden kann, braucht es zunächst glaubwürdige Identitäten.

Zertifikate sind der Nachweis dieser Identität. Zertifikate erfüllen in der digitalen Welt Funktionen analog zum Personalausweis in der realen Welt. Während in der realen Welt nur natürliche Personen einen Personalausweis besitzen, ist es in der digitalen Welt irrelevant, ob ein Mensch, eine Maschine, ein Gerät oder ein Dienst ein Zertifikat besitzt. Das Zertifikat soll die Zurechenbarkeit der Handlung und die Vertraulichkeit von Daten sicherstellen.

So wie es in einem Haushalt Schlüssel für die Haustür oder das Auto gibt, gibt es auch kryptografische Schlüssel in der digitalen Welt. Wie in der physischen Welt werden Daten mit einem kryptografischen Schlüssel gesperrt (verschlüsselt) und können nur mit dem richtigen Schlüssel wieder entsperrt (entschlüsselt) werden.

Kryptosysteme sind Verschlüsselungsverfahren und lassen sich in Familien einteilen, die sich in der Handhabung unterscheiden. Hierzu zählen symmetrische und asymmetrische Kryptosysteme. Beide Varianten haben ihre spezifischen Vor- und Nachteile und eigenen sich deshalb für unterschiedliche Einsatzgebiete.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Symmetrische Schlüssel

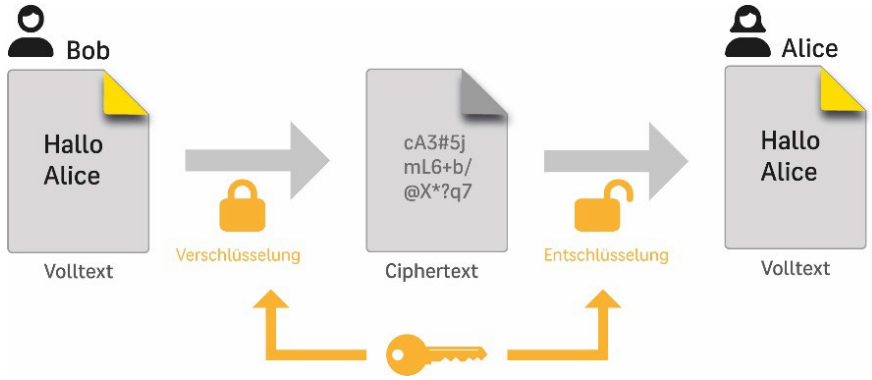

Abbildung 2: Symmetrische Verschlüsselung mit einem geheimen Schlüssel

Bei symmetrischen Kryptosystemen wird ein einziger Schlüssel für die Ver- und Entschlüsselung von Daten verwendet. Dieser Schlüssel wird als geheimer Schlüssel oder Shared Secret bezeichnet.

Der Vorteil von symmetrischen Schlüsseln ist, dass sie sehr schnell sind und sehr wenig Rechenleistung benötigen. Dadurch eignen sie sich n icht nur ideal zum Verschlüsseln sehr großer Datenmengen, sie sind auch ideal für IoT-Geräte mit wenig Rechenleistung oder für Geräte, die langfristig mit geringer Batterieleistung laufen müssen, etwa IoMT-Geräte, Verbrauchszähler oder Sensoren.

Ein symmetrischer Schlüssel ist eine Bitfolge von Nullen und Einsen, deren Reihenfolge zufällig und nicht vorhersagbar ist. Diese Bitfolge wird von einem kryptografischen Algorithmus verwendet, um Daten so zu ändern, dass sie zufällig erscheinen. Kryptografische Schlüssel sind also praktisch ein Haufen Zufall. Wer einen 128-Bit-Schlüssel generiert, generiert nichts Anderes als 128 Bit reinen Zufall. Zufall spielt technisch eine entscheidende Rolle, denn Schlüssel dürfen nicht zu erraten sein.

Werden symmetrische Schlüssel verwendet, müssen natürlich beide Seiten das Geheimnis kennen, damit der Empfänger die Daten auch wieder entschlüsseln kann. Bei entfernten Kommunikationspartnern ist dies ein Problem, denn ehe die verschlüsselten Daten transportiert werden können, muss der Schlüssel sicher transportiert werden, damit ihn niemand abfangen kann – es legt ja schließlich niemand seinen Haustürschlüssel unter die Fußmatte oder in den Blumentopf neben der Haustür, wo ihn jeder finden kann.

Das Problem des Schlüsselaustauschs kann z.B. mit einem zusätzlichen asymmetrischen Kryptosystem gelöst werden.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Asymmetrische Schlüssel

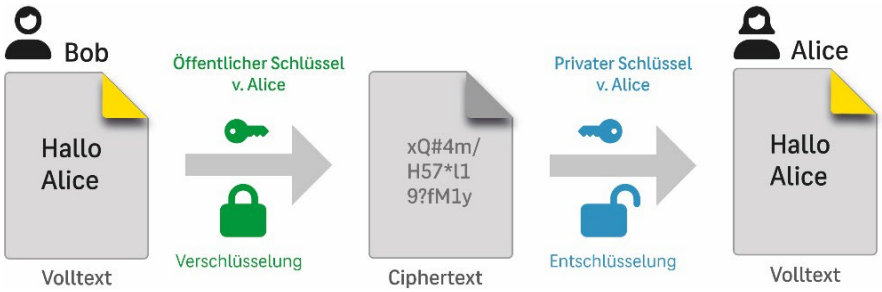

Abbildung 3: Asymmetrische Verschlüsselung mit Public/Private Key

Bei asymmetrischen Kryptosystemen wird ein Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel verwendet. Mit dem öffentlichen Schlüssel werden Daten verschlüsselt, mit dem privaten Schlüssel entschlüsselt oder auch umgedreht mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen entschlüsselt, jedoch niemals mit ein und demselben Schlüssel ver- und entschlüsselt. Mittels dieser Grundoperationen, kann das Schlüsselpaar auch zum Authentifizieren und zum Signieren genutzt werden, um die Authentizität und Manipulationsfreiheit von Daten sicherzustellen.

Beim RSA-Verfahren wird als Algorithmus eine modulare Potenzierung großer Primzahlen verwendet. Beim ECC-Verfahren werden mathematische Operationen mit Punktepaaren auf elliptischen Kurven verwendet. Da die Hardwareleistung immer besser wird, müssen auch die Schlüssellängen immer größer werden. Laut BSI müssen ab 2023 3072-Bit-RSA-Keys verwendet werden. Beim ECC-Verfahren werden kleinere Schlüssellängen verwendet, hier sind 50-Bit-Schlüssel das Äquivalent.

Der Vorteil bei asymmetrischen Kryptosystemen: Sie benötigen keinen Schlüsselaustausch. Der öffentliche Schlüssel ist, wie der Name schon sagt, öffentlich, er kann problemlos weitergegeben werden. Entscheidend ist, dass der Empfänger das Datenpaket nur mit dem zu seinem öffentlichen Schlüssel passenden privaten Schlüssel wieder entschlüsseln kann.

Zudem können mithilfe von asymmetrischen Kryptosystemen digitale Signaturen erstellt werden. Hierbei berechnet der Sender mit seinem privaten Schlüssel und einem Hashalgorithmus einen Wert zu einem Datenpaket. Dieser Wert ermöglicht es jedem, mithilfe des öffentlichen Schlüssels des Senders die Authentizität und Integrität der empfangenen Daten zu prüfen.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

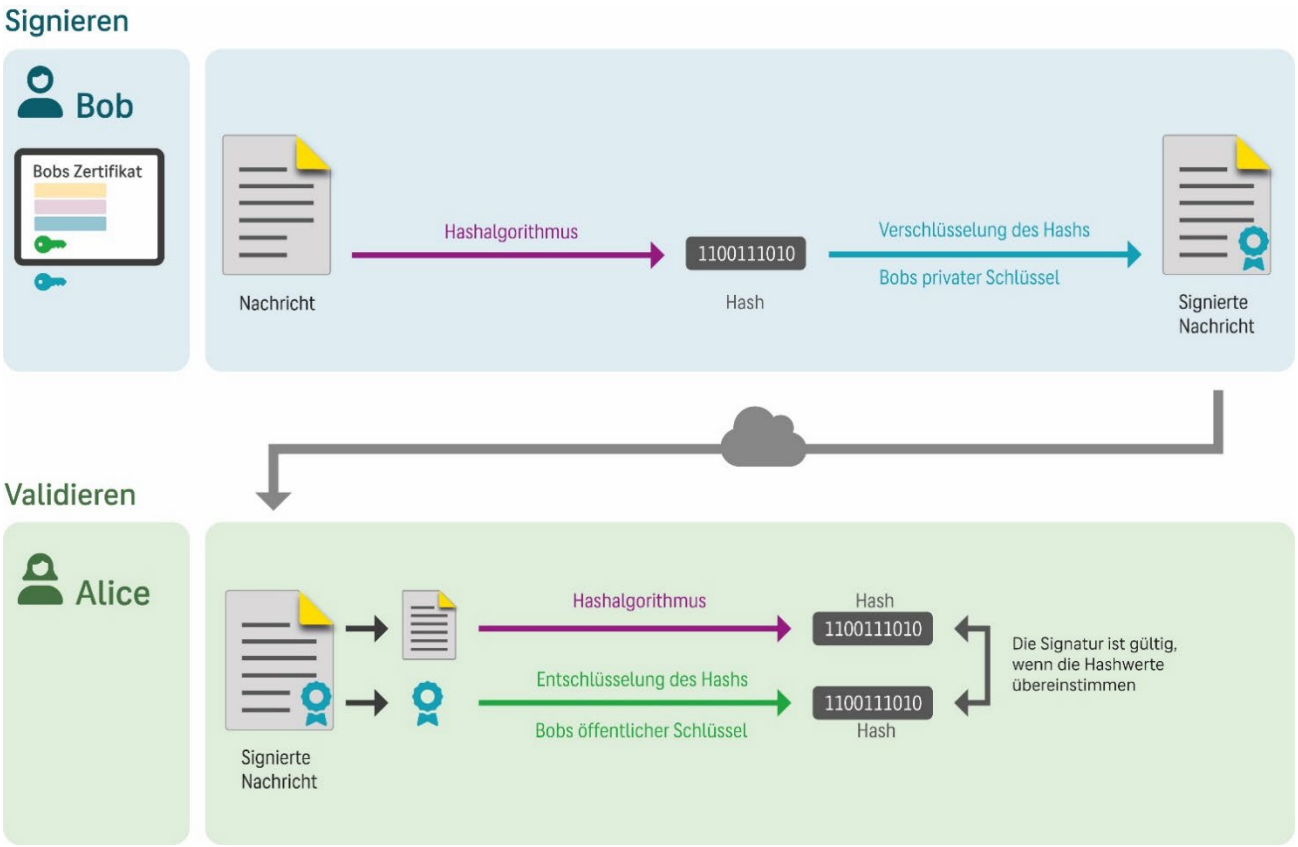

Abbildung 4: Signatur und Signaturprüfung

Asymmetrische Kryptosysteme lösen auch das Problem des Austauschs symmetrischer Schlüssel: Der Sender verschlüsselt die zu übertragenden Daten mit einem zufällig gewählten symmetrischen Sitzungsschlüssel (auch Session Key genannt). Der Sitzungsschlüssel wird anschließend mit dem öffentlichen Schlüssel des Empfä ngers verschlüsselt, der ihn mit seinem privaten Schlüssel wieder entschlüsseln kann, um dann mit dem Sitzungsschlüssel die eigentlichen Daten zu entschlüsseln. Dieses Hybridverschlüsselungsverfahren erhält den Geschwindigkeitsvorteil der symmetrischen Verschlüsselung und erlaubt trotzdem einen Schlüsselaustausch über eine unsichere Verbindung.

Der Nachteil asymmetrischer Kryptosysteme ist, dass sie aufwendiger sind und eine entsprechend hohe Rechenleistung erfordern.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Zertifikate und Certificate Authority

Wenn jeder seinen öffentlichen Schlüssel publik machen kann, muss technisch sichergestellt sein, dass Besitzer und Schlüssel – somit auch indirekt der private Schlüssel – tatsächlich zusammengehören.

Abbildung 5: Metainformationen eines X.509-Zertifikats

Dies ist die Aufgabe des Zertifikats: Als standardisierter Datensatz den öffentlichen Schlüssel um zusätzliche Metainformationen zur Identität des Besitzers, zu seiner Organisation, zur Gültigkeit und zum Aussteller zu ergänzen.

Technisch gesehen wird in den meisten Fällen der ITU-T-Standard X.509 für Public-Key-Infrastrukturen zum Erstellen digitaler Zertifikate verwendet, um die vertrauenswürdige Zuordnung von öffentlichen Schlüsseln zu ihren Besitzern zu ermöglichen. Dieser Standard ist im Request for Comments RFC 5280 der Internet Engineering Task Force beschrieben.

Dem Aussteller des Zertifikats kommt hierbei eine wichtige Aufgabe zu: Die Rolle einer vertrauenswürdigen Drittinstanz, die den legitimen Besitz des öffentlichen Schlüssels bezeugt. Das Prinzip ist vergleichbar mit einem Personalausweis, bei denen der Staat als Aussteller die Echtheit der enthaltenden Identitätsinformationen mit seinem hoheitlichen Stempel beglaubigt.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Bei digitalen Zertifikaten fungiert eine Zertifizierungsstelle, die sog. Certificate Authority (CA), als Aussteller und garantiert als übergeordnete, vertrauenswürdige Instanz die Echtheit eines Zertifikats, indem sie dessen Metainformationen mit ihrem privaten Schlüssel signiert. Anhand des öffentlichen Schlüssels der CA kann eine Entität die Echtheit der von dieser CA ausgestellten bzw. signierten Zertifikate überprüfen.

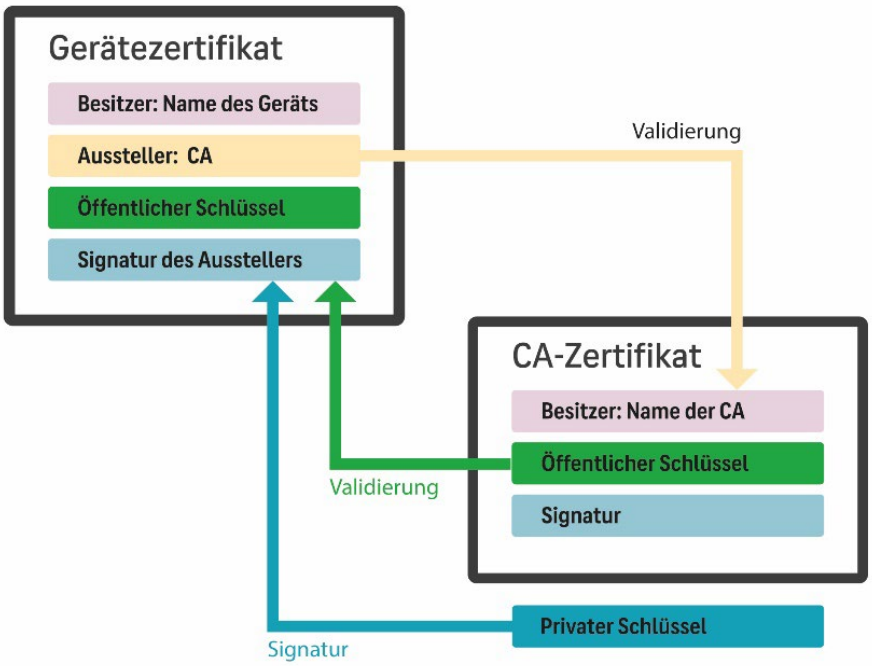

Abbildung 6: Signaturvalidierung

Die CA bündelt außerdem Sicherheitsrichtlinien und Verfahren zur zweckgemäßen Ausstellung digitaler Zertifikate, zur Validierung der Identitäten der Zertifikatempfänger und veröffentlicht Sperrlisten zurückgezogener bzw. widerrufener Zertifikate.

Die CA stellt einen vertrauenswürdigen Dritten dar. Dadurch, dass beide Kommunikationspartner der CA vertrauen, kann eine Vertrauensstellung zwischen ihnen hergestellt werden, ohne dass die Kommunikationspartner zur Herstellung dieses Vertrauens direkt miteinander in Kontakt treten müssen. Die CA stellt so das Vertrauen zwischen einander unbekannten Entitäten her und sorgt dafür, dass Menschen und Maschinen sicher miteinander kommunizieren können.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Einsatzmöglichkeiten von Zertifikaten und Schlüsseln

Zertifikate kommen dort zum Einsatz, wo die Identität eines Kommunikationspartners oder die Quelle einer Information zweifelsfrei festgestellt werden muss. Häufige Anwendungsbereiche sind:

- E-Mail und Dokumentenverschlüsselung
- Signieren von Software und Updates
- Authentifizierung von Knoten gegenüber WLANs
- Authentisierung von VPN-Verbindungen (Virtual Private Network)
- Verschlüsselung der Netzwerkkommunikation mit TLS
- HTTPS
- REST-APIs
- OPC UA

Für die Verschlüsselung der Netzwerkkommunikation kommt vor allem das Transport Layer Security (TLS)-Protokoll zum Einsatz. Eine praktische Anwendung ist z.B. die Verschlüsselung der Verbindung zwischen einem Webbrowser und einem Webserver über HTTPS. Hierbei werden die HTTP-Daten in TLS verpackt, also quasi nochmal eine Schale (Layer) außen herumgelegt. So soll zum einen die Identität des Kommunikationspartners, zum anderen die Vertraulichkeit der Daten sichergestellt werden.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

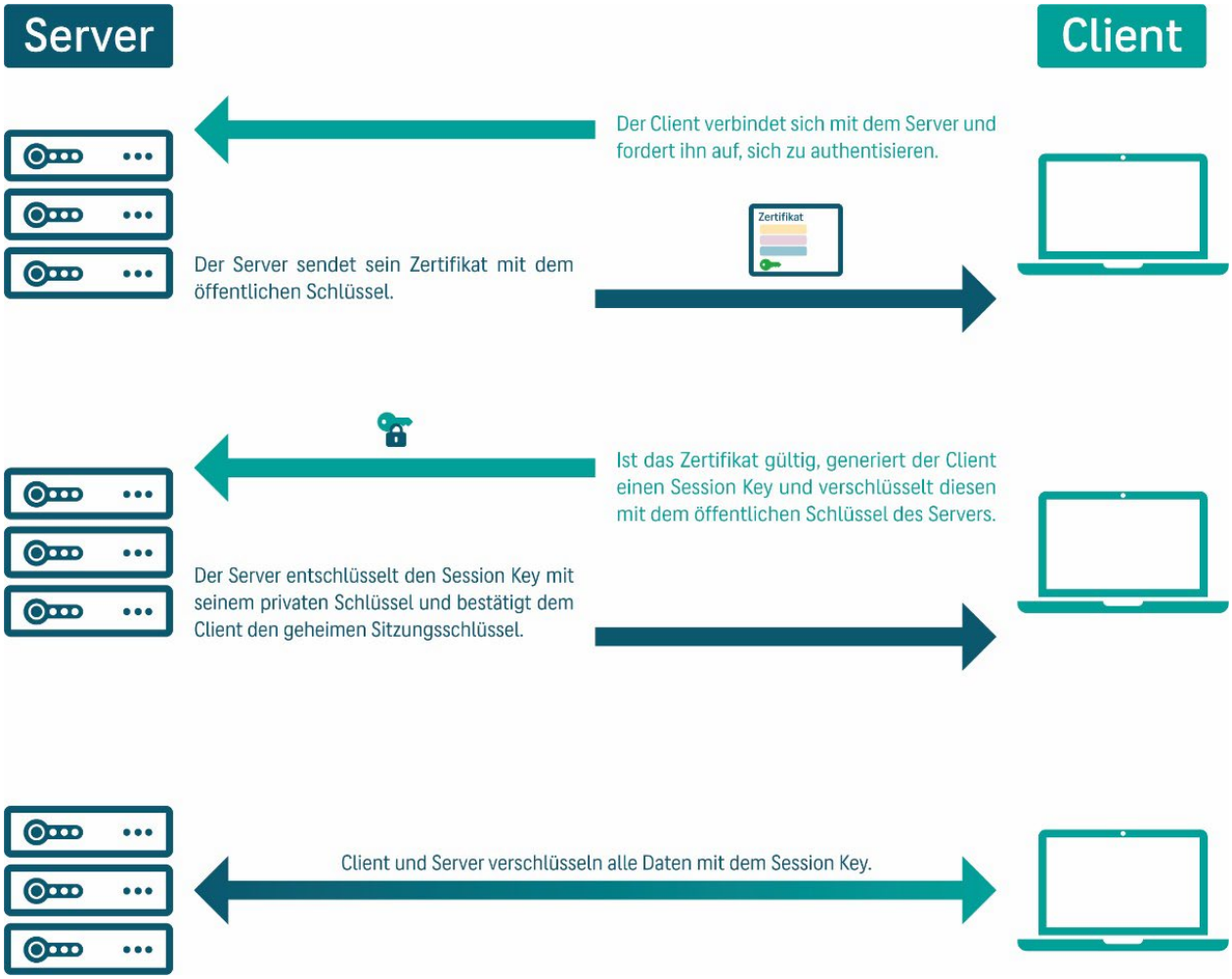

Abbildung 7: Beispiel für eine hybride Verschlüsselung mit TLS

Ein Anwendungsbeispiel hierfür ist das Homebanking. Der Server der Bank hat ein Zertifikat, mit dem er sich beim Webbrowser des Kontoinhabers ausweist. Das Betriebssystem auf dem Rechner des Kontoinhabers hat eine Liste aller offiziell vertrauenswürdigen CAs, die es auf der Welt gibt. Wurde ein Zertifikat von einer dieser CAs ausgestellt (technisch: signiert), dann sagt der Browser: Ja, das ist das richtige Zertifikat und das kleine Schloss in der Adresszeile des Browsers färbt sich grün.

Das Prinzip funktioniert natürlich auch in Gegenrichtung: Das Elster-Portal der Finanzämter stellt bei der Registrierung eines Kontos ein benutzerspezifisches Zertifikat zum Download bereit, mit dem sich der Benutzer künftig beim Login authentisieren muss.

Auch im IoT-Bereich kommen Zertifikate zum Einsatz, z.B. bei sehr vielen neu entworfenen Schnittstellen, bei denen über LAN/Ethernet HTTP zum Einsatz kommt, das in HTTPS gekapselt ist, also mit TLS verschlüsselt. So

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

kann auf sog. RESTful APIs zugegriffen werden, die mit HTTP funktionieren. Hier kann eine Entität nicht nur den Server überprüfen: die Gegenstelle, der Server, kann ebenso die Identität des Geräts überprüfen, das mit ihr kommuniziert – vorausgesetzt beide haben entsprechende Zertifikate und vertrauen der ausstellenden CA.

Alle neueren Protokolle in der IT und OT wie OPC UA, ein plattformübergreifender, quelloffener Standard für den Datenaustausch zwischen Sensoren und Cloud-Anwendungen, sind von Anfang an nach einem Security by Design-Konzept entworfen und verwenden Zertifikate mit entsprechenden Schlüsseln zur Authentisierung und Verschlüsselung.

Warum die Schlüsselverwaltung unternehmenskritisch ist

Jedes Mal, wenn eine CA ein X.509-Zertifikat ausstellt bzw. signiert, geschieht dies mit dem privaten Schlüssel der CA. Ein potentieller Angreifer kann sehr großen Schaden anrichten, wenn er Zugang zu einem privaten Schlüssel und dem entsprechenden Zertifikat hat. Er kann z.B. eine Phishing-Website mit dem Zertifikat des Unternehmens erstellen und/oder sich damit nach Belieben in Unternehmensnetzwerken authentifizieren, Daten signieren und Daten entschlüsseln – sprich: sich in die Kommunikation einklinken und auf geheime Daten zugreifen.

Es kann noch viel kritischer werden: Wenn das Unternehmen seine eigene Root-CA betreibt und ein Angreifer Zugang zum privaten Schlüssel dieser Root-CA erlangt, kann er sich selbst beliebig viele Zertifikate ausstellen. In einer kritischen Infrastruktur ist dies der größte anzunehmende Schadensfall.

Daher ist die sichere Schlüsselverwaltung das A und O für die Sicherheit einer Public-Key-Infrastruktur (PKI).

Administrative Herausforderungen von Zertifikaten

Es gibt viele downloadbare Tools, die Zertifikate erzeugen können, doch schon das Verwalten einzelner Zertifikate ist eine sehr arbeitsintensive Aufgabe. Eine stringente, geschweige denn automatisierte Zertifikatverwaltung ist mit diesen Tools nicht möglich.

Eine stringente Zertifikatverwaltung stellt folgende administrative Herausforderungen:

- *Flexibilität*
  Zertifikate müssen für Menschen und Maschinen ausstellbar sein

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

– je nach Unternehmens- bzw. Infrastrukturgröße auch in großen oder gar riesigen Mengen.

- *Verteilung*
  Zertifikate müssen über Schnittstellen automatisiert an die entsprechenden Systeme verteilt werden. Dies ist von enormer Bedeutung im IoT-Bereich, da hier unter Umständen abertausende Geräte mit Zertifikaten zu bestücken sind.
- *Gültigkeitsdauer*
  Zertifikate haben eine begrenzte Laufzeit und müssen dementsprechend rechtzeitig au-tomatisiert verlängert werden, damit z.B. die Produktion nicht stehen bleibt, weil ein Gerät kein gültiges Zertifikat mehr besitzt. Die Gültigkeit von Zertifikaten wird begrenzt, um sicherzustellen, dass essentielle Komponenten wie Schlüsselalgorithmen oder Schlüssellängen immer dem aktuellen Sicherheitsstandard entsprechen.
- *Zurückziehen*
  Zertifikate müssen jederzeit widerrufbar sein und der Gültigkeitsstatus jederzeit nachvollziehbar sein. Nicht zurückgezogene Zertifikate von ausgeschiedenen Mitarbeitern oder ausgemusterten Geräten sind beliebte Einfallstore für Angreifer, sowohl in der IT als auch im IoT.

Ein Unternehmen muss also jederzeit wissen, wer oder was Zertifikate und Schlüssel besitzt, welche Zertifikate gerade ablaufen und verlängert werden müssen oder welche Zertifikate zurück-gezogen werden müssen.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Beispiele für PKI-Implementierungen im IoT-Bereich

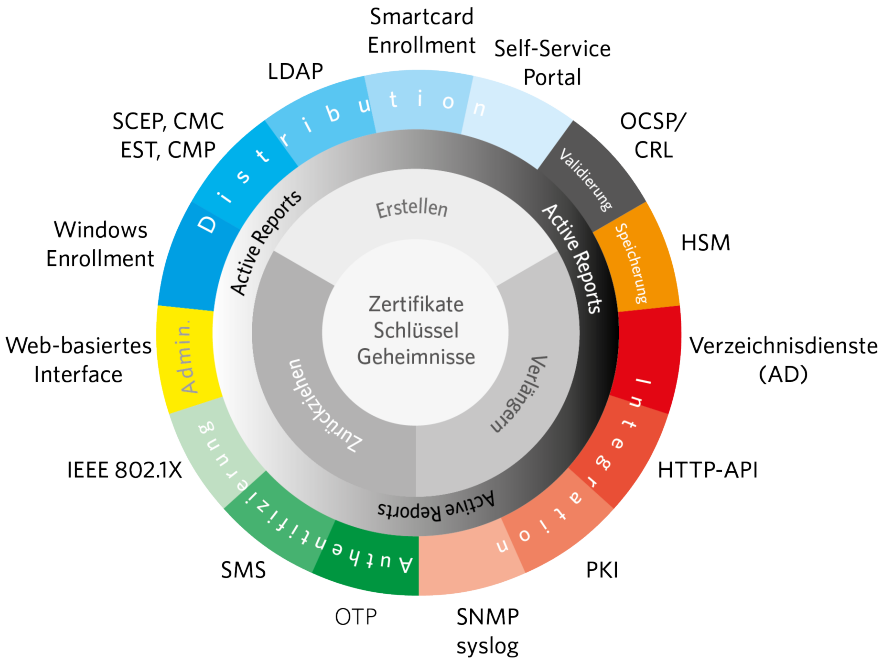

Abbildung 7: ECOS TrustManagementAppliance

ECOS Technology stellt mit der ECOS TrustManagementAppliance® eine PKI-Lösung im IoT-Bereich für ein zentrales und sicheres Management von Zertifikaten und Schlüsseln zur Verfügung – sowohl für den On-Premises-Betrieb als auch zum Betrieb in der Cloud.

Die Kernaufgabe der Trust Management Appliance (TMA), das Lifecycle-Management von Zertifikaten und Schlüsseln, ist als Dienstleistung für die eigentliche Aufgabe einer PKI zu verstehen: Geräte und Maschinen fernzusteuern, z.B. in der Produktion. Damit Zertifikate dorthin transportiert werden können, wo sie gebraucht werden, und damit Komponenten und Anwendungen reibungslos miteinander kommunizieren können, verfügt die TMA über eine große Anzahl an Schnittstellen in die verschiedensten Systeme und Umgebungen.

- *Distribution*
  Die Verteilung der Zertifikate an Geräte oder Maschinen und die reibungslose Interaktion zwischen PKI und Anwendungen wird mithilfe von Standardprotokollen wie SCEP, EST o-der Windows Enrollment gewährleistet. Eine Schnittstelle für Smartcard-Enrollment sorgt für die Verteilung von Zertifikaten auf Smartcards, wo der private Schlüssel sicher in der Hardware verwahrt wird.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

- *Validierung*
  Certificate Revocation Lists (CRL) und Online Certificate Status Protokoll (OCSP) dienen da-zu, abgelaufene oder zurückgezogene Zertifikate an zentraler Stelle öffentlich bekannt zu machen – in Form einer Sperrliste der ausstellenden CA, per direktem Real-Time-Access bei einem Validierungsdienst oder beides zusammen.
- *Integration*
  Weitere Schnittstellen erlauben die Synchronisation mit Verzeichnisdiensten wie Micro-soft AD für den Wartungs- und/oder Officebereich, die Fernsteuerung von Maschinen über HTTP-API sowie eine zentrale Überwachung und Steuerung von Netzwerkkomponenten.
- *Authentifizierung*
  Mit dem IEEE 802.1X-Standard kann gesteuert werden, dass sich (IoT-)Geräte in kabelgebundenen oder drahtlosen Netzwerken authentisieren müssen, ehe sie Zugriff erhalten. Es stehen zusätzlich Schnittstellen für eine Authentisierung per SMS oder OTP bereit.
- *Speicherung*
  Für die besonders sichere Anbindung steht eine Schnittstelle für ein Hardware-Security-Modul (HSM) bereit, um die privaten CA-Schlüssel sicher in vergossener Hardware zu speichern und alle kryptografischen Operationen dort durchzuführen.

Das Reporting- und automatische Benachrichtigungssystem sorgt dafür, dass man immer den Überblick über alle Zertifikate behält und abgelaufene Zertifikate, an die niemand denkt, der Vergangenheit angehören.

TMA im Einsatz bei Techem Energy Services

Techem betreibt europaweit ca. 39 Millionen Masterdatensammler als Teil des Techem Smart System. Masterdatensammler dienen dazu, die von den einzelnen Funkzählern übermittelten Verbrauchswerte und Gerätestatusinformationen gebäudezentral zu speichern und an die IoT-Cloud und das Rechenzentrum weiterzuleiten.

Mit der ECOS TrustManagementAppliance (TMA) sichert Techem den Datenverkehr von den Masterdatensammlern an die IoT-Cloud und von dort weiter an das Backend des Rechenzentrums ab.

Die verschlüsselte Übertragung der Verbrauchswerte ist für Techem aus mehreren Gründen essentiell: Zum einen sind diese Verbrauchswerte personenbezogene Daten gem. DSGVO, zum anderen muss der

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Energiedienstleister dafür Sorge tragen, dass Dritte keine Möglichkeit erhalten, die Funkprotokolle und sonstigen Daten mitzuschneiden oder zu manipulieren – denn hierdurch könnten theoretisch Bewegungsprofile erstellt oder Ablesewerte manipuliert werden.

Die Hauptaufgabe der Trust Management Appliance ist die Erzeugung von X.509-Zertifikaten für die von Techem eingesetzten Masterdatensammler. Mittels der Zertifikate wird dann die Kommunikation abgesichert. Die Zertifikate werden in sog. Batches gepackt, verschlüsselt und an die jeweiligen Hersteller versandt. Pro Batch handelt es sich dabei um ca. 50.000 Zertifikate, die vom jeweiligen Hersteller im Produktionsprozess auf die Masterdatensammler aufgespielt werden.

Im Produktionsprozess melden die Hersteller zurück, welches Zertifikat auf welchem Gerät aufgespielt wurde. Durch die Zuordnung von Gerätemetadaten zu den jeweiligen Zertifikaten weiß die TMA jederzeit, welches Gerät welches Zertifikat besitzt. Im Falle eines Anbieterwechsels, bei technisch defekten oder bereits in der Qualitätsprüfung aussortierten Masterdatensammlern können die Zertifikate jederzeit zurückgezogen werden. Die Zertifikate werden in der IoT-Cloud gegen die Certificate Revocation Lists (CRL) der CAs validiert.

Die turnusmäßige Verlängerung der Zertifikate ist bei Techem über eine eigene Certificate Policy geregelt. So ist sichergestellt, dass die Schlüsselalgorithmen und Schlüssellängen immer auf Höhe der Zeit bleiben und nicht technisch veralten, ehe ein Zertifikat regulär abläuft.

Zweites Beispiel

Im zweiten Praxisbeispiel geht es um die Produktion in einem deutschen Unternehmen. Hier fordert die Produktionsstraße über die HTTP-API die benötigten Zertifikate und Schlüssel direkt bei der Trust Management Appliance an. Der Zugriff ist von vornherein beschränkt: Nur die Produktionsstraße selbst darf Zertifikate anfordern, der menschliche Bediener aber nicht.

Die TMA erzeugt die Zertifikate und die Produktionsstraße meldet Seriennummer, Gerätetyp und weitere Metadaten zurück. Die Zertifikate selbst werden zunächst als temporär ungültig erzeugt. So können sie bereits auf die Geräte aufgespielt, aber in der IoT-Cloud nicht gegen die Certificate Revocation List der jeweiligen CA validiert werden. Erst wenn ein Gerät die Qualitätsprüfung bestanden hat und an seinem Bestimmungsort in Betrieb genommen wird, wird das Zertifikat freigeschaltet.

Da die privaten Schlüssel besonders kritische Komponenten sind, dürfen sie natürlich nicht in die IoT-Cloud geladen werden. In Kooperation mit dem

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Hersteller wurde daher ein System entwickelt, bei dem die Schlüssel von der TMA sicher verwahrt werden und alle Daten durch die TMA geschleust werden. Ähnlich wie bei einem Hardware-Security-Modul werden alle kryptografischen Operationen auf der TMA selbst durchgeführt.

Da die TMA über eine entsprechende Schnittstelle verfügt, kann sie für Produktionsstandorte im Ausland an eine weitere TMA gekoppelt werden. In diesem Fall können Schlüssel selektiv und temporär gesperrt an diese TMA transferiert werden. Erst wenn das jeweilige Gerät einsatzbereit ist, wird der Schlüssel entsperrt. So kann die Angriffsfläche deutlich minimiert werden.

Als plattformunabhängige All-In-One-PKI bietet die ECOS TrustManagementAppliance® die erforderlichen Funktionen und Schnittstellen für ein zentrales Management von Zertifikaten, Schlüsseln und sonstigen Geheimnissen zur Absicherung von IoT-Geräten.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333