Foto: shutterstock

Digitale Schlüsselverwaltung

Personenbezogene Daten müssen künftig sicher verschlüsselt werden – in sämtlichen Messsystemen und über den gesamten Lebenszyklus. Standardisierte Systeme für den Metering-Markt erleichtern das Management der digitalen Schlüssel.

Wenn eine wertvolle Fracht transportiert wird, sichert man üblicherweise nicht nur den Transportweg. Man sorgt auch dafür, dass sich die Wertsache selbst in einem gut geschützten Behältnis befindet. Diese einfache Wahrheit gewinnt mit dem Inkrafttreten der Europäischen Datenschutzgrundverordnung (EU-DSGVO) für den Metering Markt eine besondere Bedeutung. Denn wo Verbräuche ausgelesen, Anlagen oder Geräte geschaltet werden, sind zumeist personenbezogene Daten im Spiel. Diese werden – um im Bild zu bleiben – in Geräten „aufbewahrt", welche nach der neuen Rechtslage ebenso verlässlich gesichert werden müssen, wie der Austausch der Informationen in den unterschiedlichen Geschäftsprozessen. Die Hersteller digitaler Verbrauchszähler und anderer intelligenter Messgeräte sind dabei ebenso in der Pflicht wie Stadtwerke, Netz- und Messstellenbetreiber, die beispielsweise Submetering-Dienstleistungen erbringen möchten.

Aktuelle Verfahren nicht ausreichend

Bisher hat man sich bei der Übermittlung personenbezogener Daten auf gesicherte Verbindungen, sogenannte VPNs, verlassen. Damit sind die Daten zwar auf der Verbindungsstrecke geschützt, liegen jedoch unverschlüsselt auf den Messgeräten oder im Headend-System. Um dieses Problem zu lösen, gilt es somit, auch das Messgerät zu sichern. Dazu kommen in der Regel symmetrische Verschlüsselungsverfahren zum Einsatz. Tamer Kemeröz, Vorstand der MTG AG, eines auf IT-Sicherheit spezialisierten Software- und Beratungshauses, erläutert die Einzelheiten: „Hier wird gegenwärtig beispielsweise ein AES Schlüssel generiert und in eine bestimmte Produktionsserie von Zählern oder Messgeräten eingebaut. Der Kunde erhält den fraglichen Schlüssel und kann damit die Ende- zu-Ende verschlüsselten Daten bei Bedarf entschlüsseln." Das Problem: Kennt man den einen Schlüssel, hat man Zugang zu der gesamten Produktionsserie. Da nicht selten Produktionsserien an mehrere Kunden ausgeliefert werden, könnte theoretisch jeder Kunde die Daten der anderen entschlüsseln. Gleiches gilt, wenn solch ein „Zentralschlüssel" einer Produktionsserie in falsche Hände gerät. Tamer Kemeröz: „Von einem ‚angemessenen Schutzniveau' kann man hier unseres Erachtens nicht mehr sprechen."

Individuelle Geräteschlüssel erzeugen und verwalten

Hersteller von digitalen Zählern und Messgeräten müssen also künftig im Produktionsprozess individuelle und kryptografisch hochwertige Schlüssel generieren und diese dann einzelnen Geräten eindeutig zuordnen. Die Geräteschlüssel müssen dann sicher zum Anwender geliefert werden – idealerweise mit einem ebenfalls verschlüsselten elektronischen Lieferschein. Der Nutzer wiederum hat die Aufgabe, die verschlüsselten Geräte sicher in seinen Betriebs- und Kundenprozessen abzubilden. „Das wird mit einer Excel-Tabelle nicht mehr möglich sein – zumal es im Betrieb auch erforderlich sein kann, Schlüssel zu erneuern, etwa wenn das Schlüsselmaterial kryptographisch veraltet ist oder der Verdacht einer Kompromittierung vorliegt", gibt Tamer Kemeröz zu bedenken.

Alle Hersteller von digitalen Messgeräten, aber auch Unternehmen die sie einsetzen, werden also in Zukunft ein Key Management System (KMS) benötigen – eine IT-Lösung für die effiziente Verwaltung der digitalen Geräteschlüssel. Proprietäre Lösungen seien dabei mit Vorsicht zu genießen, wie der Technologieexperte betont, „es gibt immer mehr Gerätetypen und Anwendungen, die kryptografische Verfahren einsetzen. Wenn jeder Anbieter sein eigenes KMS liefert, entsteht beim Stadtwerk ein immenser Aufwand für Wartung und Betrieb der Systeme." Sinnvoll seien daher Lösungen, die oberhalb der einzelnen IT-Anwendungen aufgesetzt sind und zudem auf anerkannten Standards basieren: „Ein zentrales Key Management System befreit die Anwendung von den aufwändigen Security Aufgaben, vereinheitlicht die Prozesse und reduziert damit Kosten."

MTG-KMS

MTG hat erstmals ein speziell auf die Anforderungen des Metering Marktes abgestimmtes KMS entwickelt. Das mandantenfähige System kann sowohl beim Gerätehersteller als auch im Stadtwerk eingesetzt werden. In beiden Anwendungsfällen arbeitet das MTG-KMS als zentraler Security-Baustein, an den man spezifische Anwendungen, also Produktionssysteme, Geräteverwaltung, Messdaten- oder Workforce-Management andocken kann. „Damit das schnell und einfach geht, haben wir einen internationalen Key-Management-Standard implementiert, den sogenannten OASIS KMIP-Standard (KeyManagement-Interoperability-Protocol). Das ist ist ein bewährter Standard, der bereits von vielen großen Unternehmen im internationalen IoT-Umfeld eingesetzt wird", erläutert der MTG-Vorstand.

Auch für den elektronischen Lieferschein bietet MTG alle erforderlichen „Krypto-Funktionalitäten" an und setzt dabei ebenfalls auf gängige Standards wie OMS-XKE (OMS XML Key-Exchange der Open Metering System Group) und FNN eLS 2.1. Die Anwendung für den elektronischen Lieferschein braucht dann nur noch angebunden zu werden, um die notwendigen Verschlüsselungsaufgaben zu erfüllen. Aufgrund der verwendeten Standards kann die MTG-Lösung zudem mit Key Management-Systemen anderer Anbieter zusammenarbeiten, wenn die Übergabe des Schlüsselmaterials ebenfalls in einem Standardformat geregelt ist.

Wie Tamer Kemeröz betont, wird bereits heute der gesamte Lebenszyklus von Schlüsseln im MTG-KMS unterstützt. Eingesetzte Verschlüsselungs- und Kryptografie-Verfahren werden zudem ständig weiterentwickelt und aktualisiert. „Selbst wenn zum Beispiel Post-Quantum-Kryptographie eines Tages erforderlich ist, muss lediglich ein einziges, zentrales System aktualisiert werden, ohne dass sich auf der Anwendungsseite wesentliche Prozesse ändern", so Kemeröz.

Einsatz im Bereich der BSI TR 03109

Das MTG-KMS unterstützt symmetrische und asymmetrische Verschlüsselungsverfahren inklusive des Zertifikatsmanagements. Für Basiszähler sind individuelle (symmetrische) Schlüssel vorgeschrieben. Hersteller benötigen damit in der Produktion ein System, das solche individuellen Schlüssel erzeugt, den Geräten zuordnet, diese verwaltet und dann verschlüsselt mittels eines elektronischen Lieferscheins weitergibt. „Diese Vorgaben entsprechen im Prinzip den Anforderungen, die sich durch die DSGVO für alle Hersteller digitaler Zähler oder Messgeräte ergeben und sind durch das MTG-KSM abgedeckt", erklärt Tamer Kemeröz.

Bei der Herstellung von Smart Meter Gateways kommen asymmetrische Verschlüsselungsverfahren und Zertifikate aus der Smart Meter PKI zum Einsatz. Dafür wurde der MTG-CryptoController entwickelt, der auf genau diese Anforderungen ausgelegt ist und bereits von einigen namhaften Gateway-Herstellern genutzt wird.

Bei CLS-Geräten und -Anlagen wird es noch komplizierter: Auch hier müssen Zertifikate aus einer PKI zum Einsatz kommen, welche jedoch nicht die Smart Meter PKI gemäß BSI TR 03109 sein darf. „Externe Marktteilnehmer und Gateway Administratoren werden also mit Zertifikaten aus mehreren fremden PKI umgehen müssen. Das wird noch eine hochkomplexe Aufgabe, was heute nur wenigen bewusst sein dürfte," ist der MTG-Vorstand überzeugt. Das MTG-KMS unterstützt auch solche Anwendungsfälle – bis hin zur automatischen Ausstellung der erforderlichen Zertifikate.

MTG Key Management System

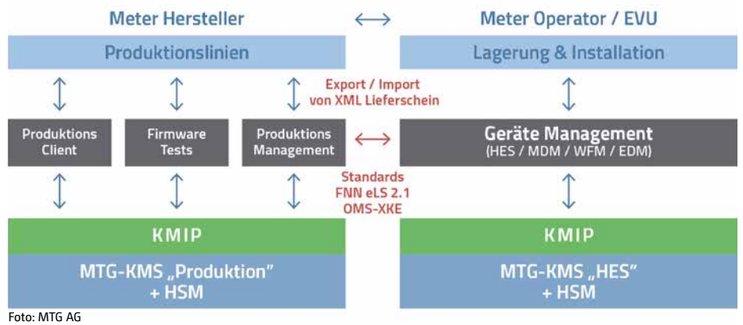

Foto: MTG AG

Kontakt: MTG AG, Tamer Kemeröz, 64293 Darmstadt, Tel.: +49 6151 8193-0, tkemeroez@mtg.de