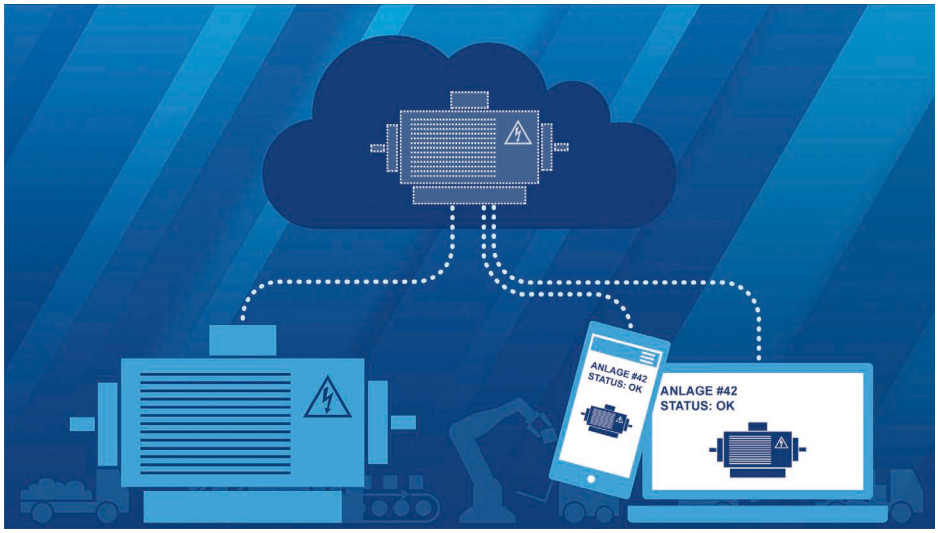
IoT Connectivity mit digitalen Zwillingen



Ein digitaler Zwilling ist nicht nur die virtuelle Instanz eines physischen Objekts, sondern auch eine universell einsetzbare IT-Applikation. Damit lassen sich Integrationsaufgaben lösen, die z. B. durch unterschiedliche Wireless Wide Area Network (WWAN)-Verbindungen zwischen Klimaanlagen und einer Service-Cloud verursacht werden.

Man stelle sich einfach einmal die folgende Aufgabenstellung vor: In den Schaltschränken dezentraler Energieanlagen wird eine relativ konstante Innentemperatur benötigt. Dafür wurden spezielle Klimaanlagen installiert, für die eine sehr hohe Verfügbarkeit benötigt wird. In diesen Geräten existiert ein Montageplatz für nachrüstbare Erweiterungskarten, um die jeweilige Anlage bei Bedarf mit dem ISDN-Telefon- oder GSM-Mobilfunknetz zu verbinden.

Diese Anbindung soll bestimmte Fernwartungsaufgaben ermöglichen. Dazu gehört auch eine Fernabfrage hinsichtlich verschiedener Anlagenzustände. Alternativ kann automatisch eine individuelle Telefonnummer angerufen werden, um eine ISDN- bzw. CSD-Datenverbindung aufzubauen und mit Hilfe einer konfigurierbaren Zeichenfolge die aktuellen Zustände sowie weitere Betriebsdaten zu übermitteln. Die für den Betrieb erforderlichen ISDN- und CSD-Dienste wurden bzw. werden inzwischen allerdings von praktisch allen Providern eingestellt.

Autor:
Klaus-Dieter Walter
CEO
SSV Software Systems GmbH
www.ssv-embedded.de

Insofern ist eine Alternative erforderlich, um bestehende Installationen um- und neue Klimaanlagen mit einer weltweit einsatzfähigen IoT-Kommunikationsbaugruppe auszurüsten. Bild 1 zeigt, dass die Kombination unterschiedlicher WWAN-Funktechnologien eine weltweite IoT-Funkabdeckung ermöglicht. In Ballungszentren und urbanen Umgebungen stehen Mobilfunknetze mit unterschiedlichen Bandbreiten zur Verfügung. Abgelegene Standorte lassen sich mit LEO-Satellitenverbindungen integrieren. Zur Zustandsüberwachung kritischer Infrastrukturen sind sogar zwei Technologien kombinierbar, um im Notfall einen Out-of-Band-Kanal nutzen zu können.

Neue Retrofit-Lösung

Die zu entwickelnde neue Retrofit-Lösung soll auf der einen Seite ohne technische Änderungen an der Klimaanlagensteuerung direkt in den vorhandenen Montageplatz passen und je nach Anlagenstandort ein Mobilfunknetzwerk oder IoT-Satellitennetzwerk zur bidirektionalen Kommunikation nutzen. Datentechnisch soll von jeder Klimaanlage, die mit einer solchen Retrofit-Technik ausgestattet wird, täglich jeweils mindestens ein Datensatz an die IT eines Servicepartners übertragen werden. Weitere wichtige Anforderungen sind:

- **Minimale Investitionskosten** für Beschaffung und Nachrüsten der erforderlichen Kommunikationsbaugruppe im Montageplatz einer Klimaanlage.
- **Minimale Betriebskosten** für die tägliche Datenübertragung über eine WWAN-Funkverbindung.
- **Funktechnische Anpassungsfähigkeit** für den weltweiten Betrieb, die unterschiedlichen Standorte, Netzbetreiber sowie die damit verbundenen nationalen Zulassungen.
- **Flexibilität** hinsichtlich der datentechnischen Anpassung an die IT-Systeme verschiedener Servicepartner.

Bild 2 zeigt eine weltweit einsatzfähige Wireless-IoT-Kommunikationsbaugruppe, die in einem speziellen Montageplatz einer Klimaanlage montiert wird und im Rahmen der Retrofit-Aufgabe entwickelt wurde. Für die standortabhängigen Funkverbindungen zur Cloud wird ein miniPCIe-Steckmodul genutzt. Zur Integration einer Nahbereichsfunksensorik existiert ein Sub-Gigahertz IEEE 802.15.4-basiertes Interface für die drei Frequenzbereiche 700 MHz (China), 800 MHz (Europa) und 900 MHz (Nordamerika) und per 6LoWPAN unterstützt wird.

In unserem Beispiel kommuniziert eine Klimaanlagensteuerung über sogenannte „AT-Kommandos“ (erweiterter Hayes-Befehlssatz) mit der Modembaugruppe im Montageplatz für nachrüstbare Erweiterungskarten. Da diese Kommandos in der jeweiligen Steuerungssoftware hinterlegt sind und eine solche Software der Regel nicht verändert werden darf, muss die IoT-Retrofit-Baugruppe die erforderlichen AT-Befehle nachbilden und in die individuellen Kommunikationsaktionen für die jeweiligen Mobilfunk- oder IoT-Satellitennetzwerke umsetzen, um Klimaanlagendaten an eine IT-Infrastruktur zu übermitteln und ggf. weitere Aufgaben zu ermöglichen.

WWAN-Funkalternativen

Die große Herausforderung für diese Retrofit-Aufgabenstellung sind die völlig unterschiedlichen Anlagenstandorte, die damit verbundenen verschiedenartigen Mobilfunknetze und, falls überhaupt kein entsprechendes terrestrisches Netzwerk an einem bestimmten Standort existiert, die Verbindung zu IoT-Satelliten im Orbit mit einer LTE-ähnlichen Antennentechnik.

Ist eine 4G-Mobilfunkabdeckung vorhanden, lässt sich beispielsweise ein LTE-A-Modem (LTE+) einsetzen. Damit sind sogar Datenübertragungsraten von 500 Mbps und mehr möglich. Der LTE-A-Datendurchsatz eignet sich sowohl für den Livestream relativ hochauflösender Kamerabilder als auch für hochperformante Anlagenfernzugriffe, vergleichbar mit einem kabelgebundenen DSL-Zugang. An anderen Standorten gibt es aber vielleicht nur ein LTE-M-Funknetz mit einem Fall-back auf LTE Cat NB1 (NB-IoT). Das reicht zwar immer noch, um problemlos kleinere Datenmengen (z. B. zusammengefasste Zustands- bzw. Sensormessdaten) zu übertragen. Ein interaktiver Fernzugriff auf die Kommandozeilen- bzw. Remote-Desktop- (VNC-) oder webbasierte Benutzeroberfläche einer Anlagensteuerung ist allerdings nicht möglich.

IoT-Satellitennetzwerks mit LEO-Satelliten

Die anspruchsvollste Detailaufgabe wäre im Moment die Nutzung eines IoT-Satellitennetzwerks mit sogenannten LEO-Satelliten (LEO = Low Earth Orbit, Schwärme von Miniatursatelliten in Orbitalhöhen zwischen 200 und 2.000 km). Die Schnittstellen und der Providerspezifische Funktechnikeinsatz in diesem dynamischen Kommunikationsmarktsegment erfordern umfangreiches Expertenwissen (es existieren zurzeit keine Standards für die extraterrestrische IoT-Kommunikation). Weitere Herausforderungen sind das mögliche Datenvolumen pro Monat, von teilweise wenigen Kilobytes, der standortabhängige Zeitversatz zwischen den Sende- und Empfangszeitpunkten sowie die Datenintegration in IT-Anwendungen. Auf der Kostenseite zeigt der zunehmende Wettbewerb aber bereits Wirkung. Im schnellwachsenden Marktumfeld der LEO-Satellitenkommunikationsprovider sind die meisten Geschäftsmodelle gegenwärtig mehr oder weniger in der Positionierungsphase. Das hat Auswirkungen auf die etablierten Preismodelle für Datenverbindungen mit geostationären Satelliten, die bisher in erster Linie die High-end-M2M-Anwendungen adressierten. Insofern ist es nicht einfach, aussagefähige Betriebskostenvergleiche anzustellen, zumal auch die Details und Anzahl der Satelliten im Orbit und die dadurch bedingten unterschiedlichen Nachrichtenübertragungszeiten eine erhebliche Rolle spielen.

Anbieter

Man findet neue Anbieter, die für 5 US-Dollar (USD) pro Monat und IoT-Device bis zu 750 Nachrichten mit maximal 192 Bytes Nutzdaten ermöglichen. Als weitere Einschränkungen sind allerdings vorgegebene Tageslimits für die Anzahl der Uplink- und Downlink-Pakete bzw. ein Limit von insgesamt maximal 60 Downlink-Nachrichten pro Monat zu beachten (Beispiel: SpaceX-Tochter Swarm). Ein etablierter Mitbewerber fordert eine monatliche „Line Rental"-Gebühr von 15 USD je IoT-Device sowie 0,15 USD pro Datenpaket mit 50 Bytes Nutzdaten. Größere Pakete kosten das doppelte (Iridium Short Burst Data, Provider: Ground Control Communications). Auf das Jahr gerechnet ergeben sich da schon gravierende Unterschiede in den Betriebskosten.

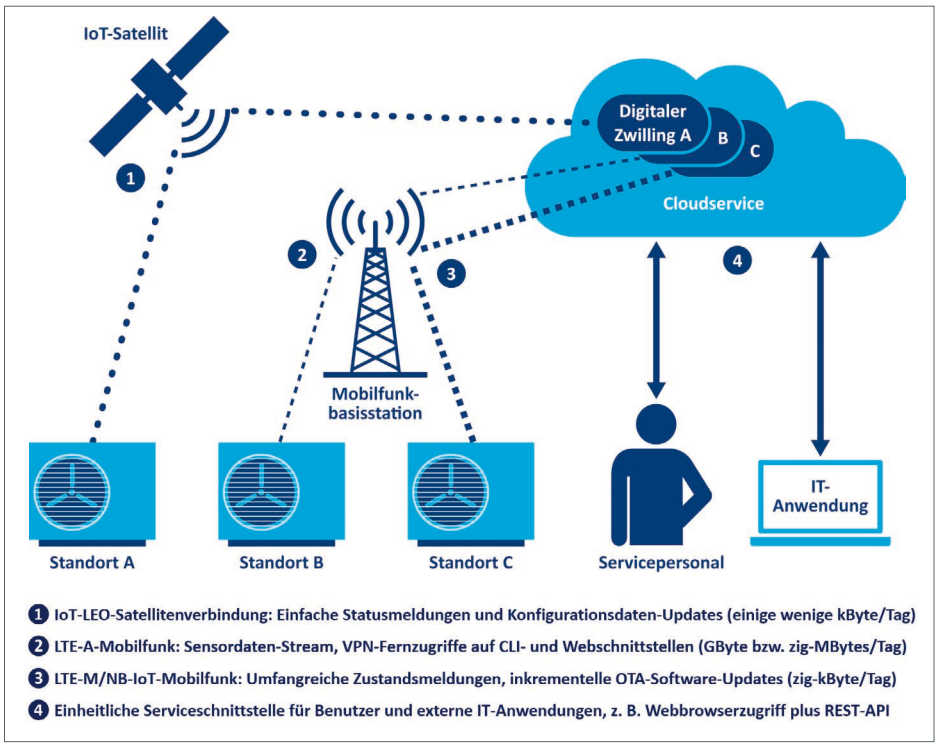


Bild 1: Die Kombination unterschiedlicher WWAN-Funktechnologien ermöglicht eine weltweite IoT-Funkabdeckung.

Connectivity-Integrationszwilling

Durch die völlig unterschiedlichen WWAN-Varianten existieren stark voneinander abweichende Datenübertragungsbandbreiten zwischen der Klimaanlagensteuerung auf der einen und einem Cloudservice auf der gegenüberliegenden Seite. Unter Berücksichtigung der Provider-bedingten Datenvolumen-Limits sowie der Besonderheiten von LEO-Satellitenorbits und der davon abhängigen Sichtbarkeitsbereiche (eine Datenübertragung ist je nach Standort nur zu bestimmten Zeitpunkten innerhalb eines variablen Zeitfenster möglich), führt das zu sehr unterschiedlichen Nutzdatenmengen pro Tag. Der große Vorteil einer solchen modularen Lösung ist allerdings, dass sich damit industrielle IoT-Anwendungen mit weltweiter Funkabdeckung zu akzeptablen Kosten realisieren lassen. Egal an welchem Standort die IoT-Retrofit-Baugruppe installiert wird, entweder gibt es einen LTE-Breitband- oder Schmalband-Netzzugang. Ansonsten wird eine IoT-Satellitenfunkverbindung als Alternative genutzt.

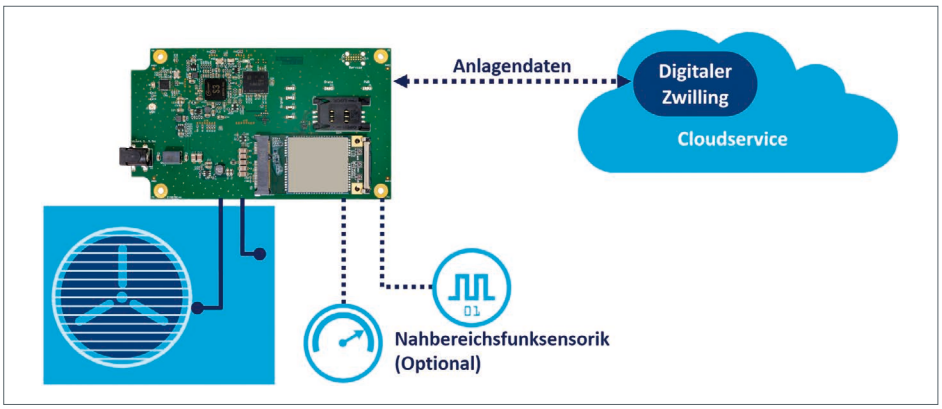


Bild 2: Im Rahmen einer Retrofit-Aufgabe wurde eine weltweit einsatzfähige Wireless-IoT-Kommunikationsbaugruppe entwickelt, die in einem speziellen Montageplatz einer Klimaanlage montiert wird.

Einheitliche Cloudschnittstelle

In der Praxis ist auf jeden Fall sicherzustellen, dass eine einheitliche Cloudschnittstelle für den Datenzugriff existiert. Mit anderen Worten: der Datennutzer muss sich keine Gedanken darüber machen, ob die Anlagendaten über einen Live-Datenstrom per LTE+, in stündlichen Intervallen per LTE-M oder durch einige wenige tägliche NB-IoT- bzw. Satellitendatenübertragungen übermittelt werden, die vor dem Versenden ggf. auch noch mit Hilfe spezieller Machine-Learning (ML)-Algorithmen vorverdichtet wurden. Er kann wie gewohnt per Webbrowser auf eine Webseite bzw. per VNC-Client auf einen Remote Desktop zugreifen, um sich das aktuelle Analgendatenbild bzw. Betriebszustände anzuschauen oder neue Konfigurationsdateneinstellungen vorzunehmen. Bei einer LTE-A- oder LTE-M-Verbindung könnte sich der dafür erforderliche Web- bzw. VNC-Server direkt in der Anlage befinden. Mit einem NB-IoT- oder LEO-Satellitenlink ist das latenzbedingt nicht sinnvoll.

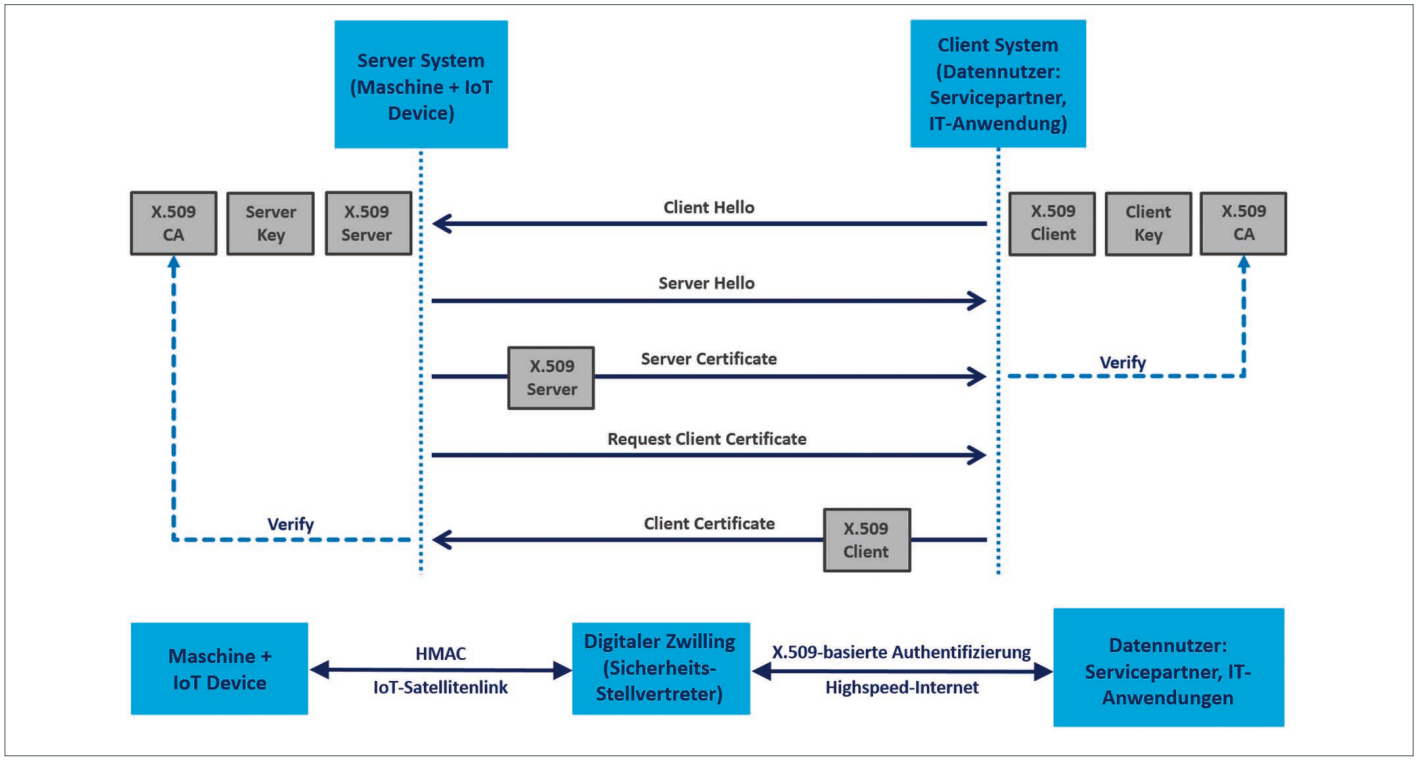


Bild 3: Um die Authentizität und Integrität von IoT-Daten zu gewährleisten, eigenen sich Ende-zu-Ende-PKI-Lösungen mit beidseitiger Authentifizierung.

Digitaler Zwilling

Diese Problematik lässt sich hervorragend mit einem digitalen Zwilling lösen: Webserver und Webseiten bzw. VNC-Server nebst Remote Desktop befinden sich grundsätzlich in der Zwillingsinstanz innerhalb einer Cloudservice-Plattform. Die eigentliche Datenverbindung zur Anlagensteuerung wird von einem Agenten abgewickelt, der bei der Instanziierung des digitalen Zwillings in Bezug auf den benutzten Verbindungstyp (LTE, NB-IoT oder Satellit) konfiguriert wird. In einer solchen Lösung sollte der digitale Zwilling allerdings einen geeigneten „Datenqualitätsindikator" hinzufügen, der den Datennutzer informiert, ob die dargestellten Anlagedaten per Live-Stream, Intervall-basierter Übertragung, Zeitreihendateninterpolation bzw. eventuell sogar durch den Einsatz spezieller ML-Klassifizierungsalgorithmen zu Stande gekommen sind (mit einer LTE-Verbindung > CAT 9 kann man hochauflösende Kamerabilder in Echtzeit übertragen. Werden NB-IoT oder ein IoT-Satelliten-Link genutzt, sollte man die Bilddaten direkt im Sensor analysieren und nur das Ergebnis übertragen).

Sicherheits-Stellvertreter

Neben der WWAN-Datenintegration zur Realisierung einer einheitlichen Serviceschnittstelle existiert für den digitalen Zwilling noch eine zweite Aufgabenstellung als Sicherheits-Stellvertreter. Der Bedarf dafür ergibt sich aus den unterschiedlichen Bandbreiten, um über die LTE-, NB-IoT- und LEO-Satellitenlink-Funkalternativen eine Ende-zu-Ende-Sicherheitslösung auf der Basis von X.509-Zertifikaten zu realisieren. Das dabei zum Einsatz kommende TLS- bzw. DTLS-Protokoll lässt sich zwar problemlos mit einer IP-basierten LTE-Verbindung nutzen, aber schon beim NB-IoT-Einsatz ergeben sich in der Regel die ersten Hürden durch das zusätzlich verursachte Datenvolumen und die monatlichen Kosten des Datenplans. Da die LEO-Satellitenkommunikation überwiegend nicht einmal IP als Netzwerkprotokoll einsetzt, sondern stattdessen an die technisch bedingten Limitierungen angepasste Spezialprotokolle verwendet, ist der TLS/DTLS-Einsatz hier nicht möglich. Innerhalb einer Applikation mit derart unterschiedlichen WWAN-Technologien lässt sich daher kein einheitlich hohes X.509-Zertifikat-basiertes Cybersicherheitsniveau realisieren. Um den im ersten Beispiel angesprochenen Datennutzern für die Webbrowser- und VNC-Remote-Desktop-Fernzugriffe auf Anlagendaten eine einheitliche TLS-basierte Ende-zu-Ende-Security zu bieten, dient im Falle einer LEO-Satellitenverbindung der digitale Zwilling und nicht die Klimaanlage als Endpunkt für eine beidseitige Authentifizierung (Mutual Authentication) mit X.509-Zertifikaten.

Bild 3 illustriert diese Zusammenhänge: Um die Authentizität und Integrität von IoT-Daten zu gewährleisten, eigenen sich Ende-zu-Ende-PKI-Lösungen mit beidseitiger Authentifizierung. Für eine LEO-Satellitenverbindung zwischen einer IoT-Device in einer Maschine bzw. Anlage und dem Datennutzer ist ein PKI-Einsatz mit X.509-Zertifikaten nicht ohne weiteres möglich. Die Lösung ist z. B. ein hybrides Konzept, in dem der digitale Zwilling als „Sicherheits-Stellvertreter" den PKI-Endpunkt bildet. Die Datenverbindung zur IoT Device wird hingegen mit einem HMAC abgesichert.

Mutual Authentication

Bei einer Mutual Authentication haben beide Kommunikationspartner jeweils ein eigenes X.509-Zertifkat mit dem dazugehörenden privaten Schlüssel (Server Key und Client Key in der Abbildung). Darüber hinaus existiert auf beiden Seiten mindestens ein CA-Zertifikat (X.509 CA), um andere Zertifikate prüfen zu können.

Der gesamte beidseitige Authentifizierungsprozess läuft in fünf Schritten ab. Es beginnt mit einem „Client Hallo", das durch ein „Server Hello" beantwortet wird. Gleichzeitig sendet der Server sein X.509-Zertifikat und fordert das Client-Zertifikat an. Der Client prüft die digitale Unterschrift des Server-Zertifikats mit Hilfe des X.509 CA. Verläuft diese Prüfung positiv, antwortet der Client mit seinem Zertifikat. Bei einer negativen Prüfung bricht der Client die Verbindung ab. Abschließend erfolgt die Server-seitige Prüfung des Client-Zertifikats. Nur bei einem ebenfalls positiven Prüfergebnis erfolgt anschließend die Nutzdatenübertragungsphase, ansonsten ein Verbindungsabbruch. Im Falle einer LTE-Verbindung lässt sich die Mutual Authentication direkt zwischen dem Rechnersystem des Datennutzers und dem IoT-Klimaanlagenmodem als Server vor Ort durchführen – das sicherheitstechnische Optimum.

Beim Einsatz eines LEO-Satellitenlinks bildet hingegen der digitale Zwilling den Server-Endpunkt. Die Datenauthentizität und Integrität sind also relativ unsicher. Verbessern lässt sicher dieser Zustand durch den Einsatz eines Message Authentication Codes (z. B. ein HMAC-Verfahren) für die Satellitenverbindung zum digitalen Zwilling. ◄