Expert Insights: Over-the-Air-Updates

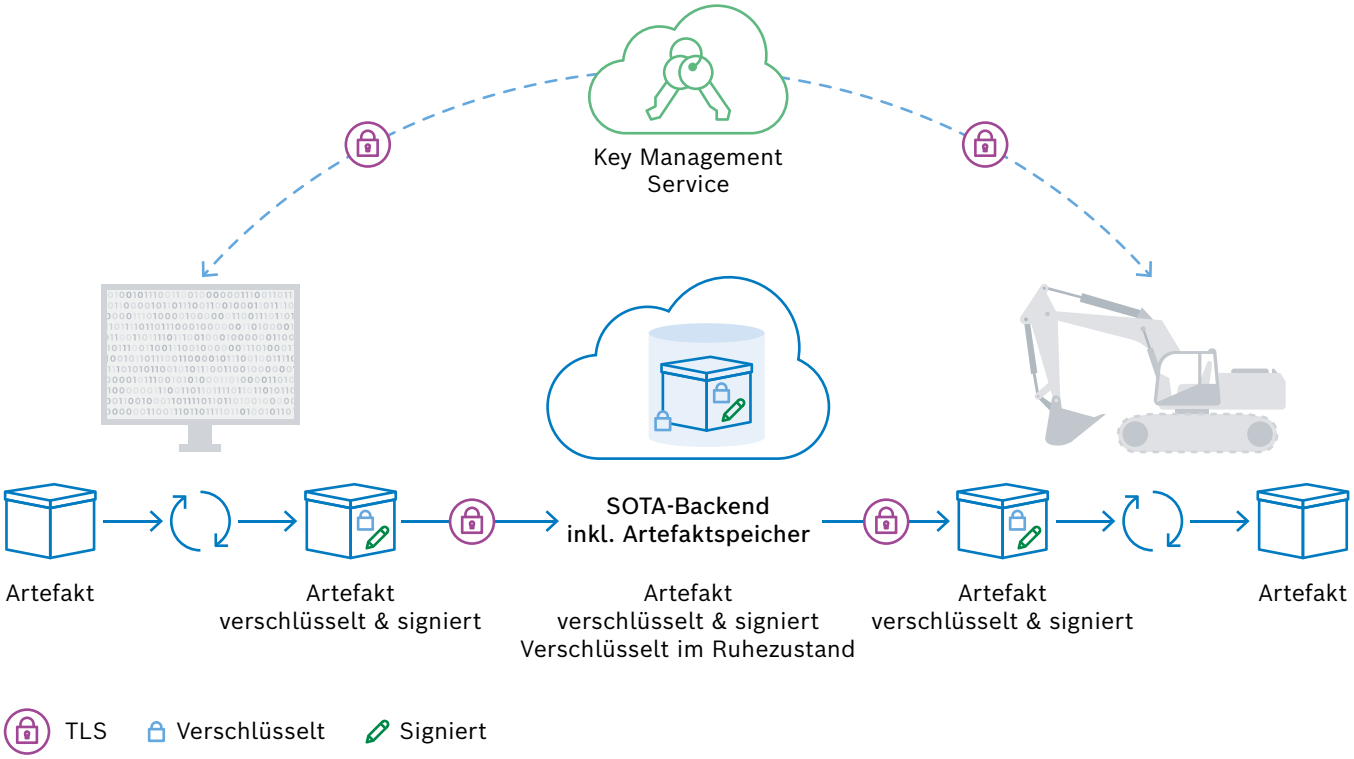
Zentrale Überlegungen für sichere Software-Updates

Durch das Bereitstellen von Updates auf Geräten können Unternehmen nicht nur Softwareprobleme rasch lösen, sie können Software-Updates auch nutzen, um neue Funktionen aufzuspielen und so den Produktlebenszyklus zu verlängern. Dies wiederum kann als Grundlage für völlig neue Geschäftsmodelle dienen.

Software-Updates Over-the-Air (OTA) machen diesen Prozess wesentlich einfacher und effizienter. Für Geräteherstel-ler ist dies jedoch kein leichtes Unterfangen. Sie müssen eine ganze Reihe von Aspekten beachten: Updates müssen entsprechenden Geräten zugewiesen, groß angelegte Software-Rollouts sorgfältig abgewickelt und Update-Prozesse kontinuierlich überwacht werden. Ein Thema ist dabei besonders wichtig: Sicherheit.

Wie gewährleisten Unternehmen einen durchgängig sicheren Software-Rollout? Im Folgenden beschreiben wir drei zentrale Punkte, die es zu beachten gilt:

1. Sicherheit während des Artefaktlebenszyklus



Ob technische Probleme bei der Dateiübertragung oder böswillige Angriffe – ein Software-Artefakt kann auf verschiedene Weise beschädigt oder kompromit-tiert werden. Für Unternehmen ist es deshalb zentral, Software-Artefakte zu schützen und ihre Vertraulichkeit, Authentizität und Integrität über den gesamten Lebens-zyklus hinweg zu gewährleisten – von der Entwicklung bis zur Installation auf einem Gerät.

Dazu muss eine Vertrauensbeziehung zwischen der Stelle, die die Artefakte veröffentlicht, und den Geräten aufgebaut werden. Hier kommt der Einsatz von Verschlüs-selung und digitalen Signaturen ins Spiel. Diese Mecha-nismen sorgen für lückenlose Sicherheit, ganz gleich, ob sich das Artefakt im Ruhezustand befindet oder übertra-gen wird.

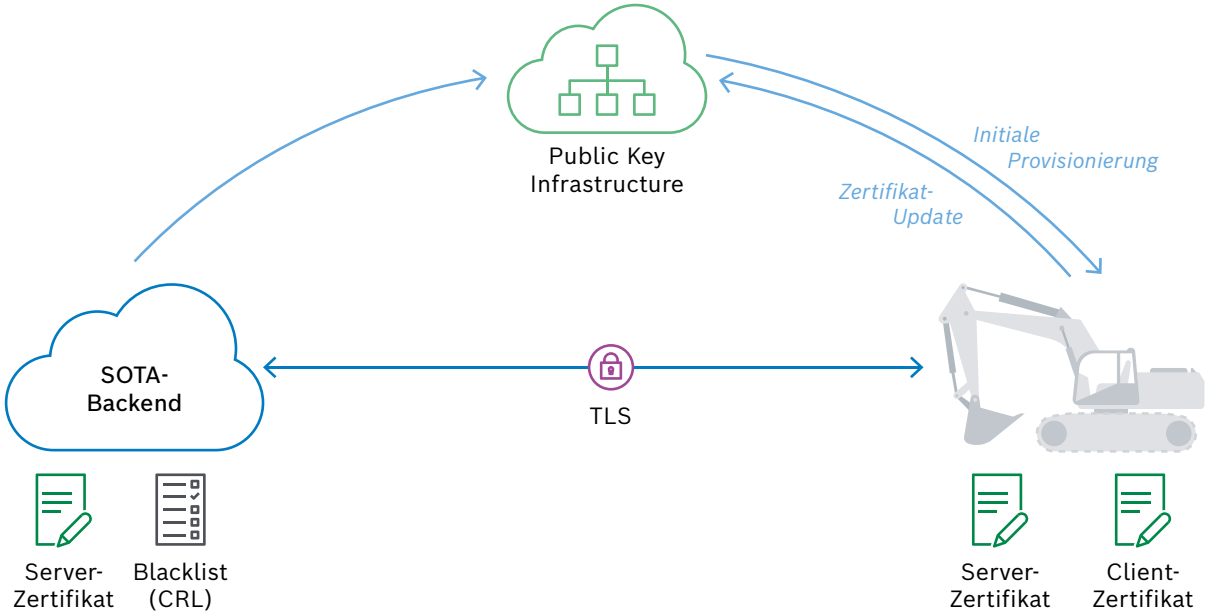
Verschlüsselung dient dazu, die **Vertraulichkeit der übermittelten Informationen** zu garantieren. Sie stellt sicher, dass die ausgetauschten Nachrichten nur vom Sender und vom vorgesehenen Empfänger gelesen werden können – nicht von Dritten.

Die Kommunikation zwischen Geräten und der Backend-Anwendung wird meist asymmetrisch verschlüsselt. Dabei werden Nachrichten mit einem öffentlichen Schlüssel ver- und mit einem privaten Schlüssel entschlüsselt. Zugegeben, die symmetrische Verschlüsselung kommt mit allgemein kürzeren Schlüsseln aus und ist schneller, weniger aufwendig und unkomplizierter. Doch da bei diesem Verfahren der gemeinsame, geheime Schlüssel an beiden Enden der Kommunikation aufbewahrt werden muss, ist das Sicherheitsrisiko höher. Dies gilt insbesondere für Geräte, auf die ein Angreifer physisch zugreifen und so das Geheimnis auslesen kann.

Mit einer **digitalen Signatur** können Geräte die **Integrität der empfangenen Artefakte** verifizieren. Dazu wird das oben beschriebene Verschlüsselungsverfahren angewendet, um die Signatur zu valideren. Nach der erfolgreichen Validierung kann der Inhalt des Pakets entschlüsselt und ausgelesen werden.

Gerade bei groß angelegten Software-Rollouts werden Software-Artefakte nicht direkt vom Entwickler zum Gerät übertragen, sondern in einem Artefaktspeicher zwischengespeichert. Um die ruhenden Artefakte im Backend zu schützen, ist eine verschlüsselte Persistenz erforderlich. Dies erschwert es Dritten, Artefakte abzugreifen oder zu verändern. Zudem müssen der Upload in und Download aus dem Speicher abgesichert werden. Hier kommen Standardmechanismen wie **Transport Layer Security** (TLS) ins Spiel, die für Sicherheit bei der Übertragung sorgen.

2. Sichere Kommunikation und Authentifizierung zwischen Geräten und dem SOTA-Backend



Eine zentrale Aufgabe einer SOTA-Lösung besteht darin, eine sichere Kommunikation zwischen dem Backend und den Geräten zu gewährleisten sowie die Schlüsselverwaltung zu ermöglichen. Was sollten Unternehmen bei der technischen Umsetzung beachten?

Verschlüsselung: Public Key Infrastructure (PKI) und Key Management System (KMS)
Die Public Key Infrastructure ist ein hierarchisches System oder Konzept. Sie legt den Lebenszyklus von Zertifikaten fest und schafft einen Rahmen für die Verwaltung der privaten und öffentlichen Schlüssel. Darüber hinaus definiert sie die Prozesse, Protokolle und Richtlinien für deren Verteilung.

Die Public Key Infrastructure stellt öffentliche Schlüssel für die Verschlüsselung sowie hierarchische digitale Zertifikate bereit. Diese dienen der sicheren Datenübermittlung, meist in der Form von TLS, oder zur Geräteauthentifizierung im SOTA-Backend.

Mit den digitalen Zertifikaten begegnet die Public Key Infrastructure auch einer wesentlichen Problematik in Zusammenhang mit der asymmetrischen (und symmetrischen) Verschlüsselung: Wie lässt sich sicherstellen, dass der private Schlüssel zu der vorgesehenen Anwendung oder dem vorgesehenen Gerät gehört und nicht zu einem Man-in-the-Middle-Angreifer? Zertifikate weisen Geräte oder Backend-Anwendungen bestimmten Schlüsseln zu, um ihre Identität zu bestätigen.

Wie setzen Unternehmen das Konzept einer Public Key Infrastructure in die Praxis um? Hier kommt ein Key Management System ins Spiel. Als Teil der SOTA-Lösung verwaltet dieses System die Schlüssel, die vom Backend und Gerät gemeinsam verwendet werden.

Sichere Kommunikation: Transport Layer Security (TLS)
Beim Aufbau einer verschlüsselten Verbindung über TLS authentifiziert sich das SOTA-Backend über ein Zertifikat gegenüber dem IoT-Gerät. Das Zertifikat enthält einen öffentlichen Schlüssel vom Backend-Server, über den ein gemeinsames Geheimnis für die verschlüsselte Kommunikation generiert wird.

Ein Gerät muss sicherstellen, dass es dem Backend-Zertifikat vertrauen kann. Nur so weiß es, dass es auch mit dem erwarteten Server kommuniziert und nicht beispielsweise mit einem Man-in-the-Middle-Angreifer. Zu diesem Zweck muss eine Zertifizierungsstelle (CA) das Serverzertifikat signieren. Das Gerät prüft dann, ob der Hostname des Zertifikats mit dem SOTA-Backend übereinstimmt, ob das Zertifikat noch gültig ist und ob es von einer vertrauenswürdigen CA signiert wurde.

Vertrauenswürdige Server: Certificate Pinning
Das sogenannte Certificate Pinning erschwert es böswilligen Akteuren, Zertifikate für Angriffe oder Spoofing einzusetzen. Es reduziert unter anderem auch das Risiko einer kompromittierten CA oder von Man-in-the-Middle-Angriffen. Darüber hinaus erfordern Sicherheitsstandards wie OWASP Mobile Application Security Verification für eine Level-2-Zertifizierung von Geräten, die sensible Daten wie Krankenakten handhaben, eine geräteseitige Zertifikatsvalidierung.

Mit Certificate Pinning schränken IoT-Geräte den Kreis der SOTA-Backend-Zertifikate ein, die gültig und vertrauenswürdig sind. Ein Gerät kann dann die Verbindung mit einem Server ablehnen, wenn dieser das betreffende Zertifikat nicht verwendet. So müssen Geräte keinen Trust Store für Root-Zertifikate verwenden.

Wie funktioniert das? Das TLS-Zertifikat, über das der Server verfügen sollte, wird während der Entwicklung auf dem Gerät hinterlegt. Statt die Verwendung eines beliebigen vertrauenswürdigen Zertifikatsausstellers, öffentliche Schlüssel oder gar Anwenderzertifikate. Clients, die sich mit dem betreffenden Server verbinden, behandeln alle anderen Zertifikate als ungültig und verweigern den Aufbau einer HTTPS-Verbindung.

Beim Pinning gibt es verschiedene Möglichkeiten, abhängig vom Anwendungsfall, Zertifikat oder öffentlichen Schlüssel. Ein IoT-Gerät kann das Anwenderzertifikat oder die Hash-Funktion eines öffentlichen Schlüssels als einzige vertrauenswürdige Quelle festlegen. Das bedeutet, dass Verbindungen mit diesem Schlüssel exklusiv aufgebaut werden. Dies kann zu Problemen führen, wenn Serverzertifikate ablaufen, ausgetauscht oder widerrufen werden. Das Gerät kann sich dann nicht mehr mit dem SOTA-Backend verbinden.

Weniger fehleranfällig ist es daher, die Zertifizierungsstelle und nicht nur das Serverzertifikat zu pinnen. Dazu werden innerhalb der Zertifikatskette Zwischen- oder Root-Zertifikate gepinnt. So lassen sich Zertifikatsänderungen wesentlich einfacher bewältigen. Das Verfahren ist dennoch sicher, da nur eine vertrauenswürdige Zertifizierungsstelle Zertifikate ausstellt.

Vertrauenswürdige Clients: Geräteauthentifizierung
X.509-Zertifikate stellen sicher, dass sich nur berechtigte Geräte mit dem SOTA-Backend verbinden. Um sich zu authentifizieren, sendet ein Gerät zusammen mit der Anfrage eine vollständige (in sich geschlossene) Zertifikatskette an das Backend, wo sie validiert wird. Die Zertifikatskette kann mehrere Zertifikate beinhalten, zum Beispiel ein Geräte-spezifisches Client-Zertifikat, ein Zwischenzertifikat und ein Root-Zertifikat.

Kommunikation mit einem Content Delivery Network
Für eine effizientere Paketverfügbarkeit und -verteilung können Unternehmen anstelle eines zentralen Artefaktspeichers ein Content Delivery Network (CDN) nutzen. In diesem Fall empfiehlt sich der Einsatz signierter URLs. Diese haben meist eine kryptische Form, um Angriffe auf Grundlage ihres Namensschemas zu unterbinden. Signierte URLs machen eine Authentifizierung im CDN überflüssig, da sie die Authentifizierungsinformationen in ihren Abfrage-Strings enthalten. So können Geräte ohne Anmeldedaten den Download ausführen. Eine signierte URL bietet zudem eingeschränkte Zugriffsrechte und läuft nach einer gewissen Zeit ab.

3. Zugangsmanagement mit rollenbasierter Zugangskontrolle

Um eine SOTA-Lösung vor unbefugtem Zugriff zu schützen, ist es von zentraler Bedeutung, Zugriffe auf das Backend zu verwalten. Dies dient der Prävention von:

- Diebstahl oder unerlaubter Datenlöschung
- Missbrauch der Software
- unsachgemäßer Änderung oder Weitergabe von Informationen

Die rollenbasierte Zugangskontrolle vereinfacht darüber hinaus die Benutzerverwaltung und hilft dabei, klare Verantwortlichkeiten festzulegen. Sie befasst sich mit Fragen wie: Wer hat Zugang zum SOTA-Backend? Welche Berechtigungen haben bestimmte Nutzer? Zu welchen Bereichen haben sie Zugang?

Dank eines detaillierten Rollenkonzepts können System-Administratoren die Zugangsrechte von Nutzern verwalten und festlegen, wie sie mit den verschiedenen Funktionen einer SOTA-Lösung interagieren. Administratoren können spezifische Rollen für folgende Aufgaben einrichten:

- Verwalten von Update-Zielen (z. B. durch einen Deployment-Administrator)
- Erstellen und Hochladen von Software-Artefakten (z. B. durch einen Repository-Administrator)
- Definieren und Durchführen von Update-Kampagnen (z. B. durch einen Rollout-Administrator)
- Anzeigen von Berichten, Prüfen von Kundensupport-Anfragen sowie Untersuchen und Beheben von Problemen bei fehlgeschlagenen Updates (z. B. durch einen Support-Administrator)

Die Aufteilung der Verantwortlichkeiten auf verschiedene Rollen erleichtert es zudem, Genehmigungsprozesse zu implementieren – von der Entwicklung der Artefakte über die Kampagnendefinition, bis hin zur Bereitstellung der Software auf den IoT-Geräten.

Fazit

Sicherheit ist eine vielschichtige Thematik in der Welt des IoT. Unternehmen müssen ganzheitlich denken, um einen durchgängig sicheren Software-Rollout zu gewährleisten. Die oben beschriebenen Aspekte helfen Unternehmen dabei, dieser Komplexität gerecht werden und Sicherheitsrisiken zu minimieren. So beugen sie unautorisierten Zugriffen auf Daten oder Datenlecks vor.

Die Bosch IoT Suite ist unsere IoT-Plattform, die all diese Punkte abdeckt. Ergänzende Ansätze setzen wir in enger Zusammenarbeit mit der Bosch-Tochtergesellschaft Escrypt, einem Anbieter von Security-Lösungen, um.

Mit Ihnen gemeinsam finden wir die richtige Lösung, die den jeweiligen Sicherheitsanforderungen Ihres Anwendungsfalls gerecht wird. Von Standardimplementierungen zu maßgeschneiderten Lösungen – bei uns bekommen Sie alles aus einer Hand.

Möchten Sie mit uns über Ihren Anwendungsfall sprechen?
Kontaktieren Sie unsere SOTA- und IoT-Experten

Mehr über uns

Folgen Sie Bosch_IO auf Twitter

Folgen Sie Bosch.IO auf LinkedIn