TELEKOM AUSTRIA GROUP M2M

White Paper – M2M Security

Telekom Austria Group M2M und A1 Telekom Austria AG ermöglichen einen sicheren Betrieb und einfache Verwaltung Ihrer M2M Anwendungen.

In diesem Artikel werden eine professionelle Architektur für die M2M Kommunikation skizziert und allgemeine Empfehlungen für das Kommunikationsverhalten von verteilten M2M Anwendungen vorgeschlagen. Jede Kommunikationslösung hat neben Kosten- und Verfügbarkeitsaspekten auch Sicherheits- und Betriebsrisiken. Wir zeigen mögliche Szenarien auf, welche Services die Mobilfunktechnologie anbietet, um den Betrieb einer großen Anzahl von M2M Geräten zu ermöglichen und die Risiken zu minimieren.

IP überall

In den letzten Jahren hat sich der Einsatz des Internets grundlegend verändert. Statt des Internetkonsums am PC, wird das Internet zunehmend mobil genutzt. Smartphones mit ihren zahlreichen Apps dominieren in immer größerem Ausmaß den Markt für mobile Endgeräte. Günstige Datentarife erlauben es z.B. Fotos und Videos direkt vom mobilen Gerät ins Internet zu stellen und mit Freunden zu teilen. Doch nicht nur Menschen,auch Maschinen (z.B. Messgeräte, Kameras, Getränkeautomaten, sowie diverse Steuerungen) nutzen das Internet, um miteinander in Kontakt zu treten. Man spricht in diesem Fall von „Machine-to-Machine Communication“, kurz M2M genannt.

Die Welt der mobilen elektronischen Steuerungen war in den letzten Jahren einem noch größeren Wandel unterworfen als die Internetnutzung selbst. Vor wenigen Jahren war die Entwicklung z.B. eines mobilen Messgeräts kostspielig und zeitaufwändig und die Anbindung an ein Mobilfunknetz war Modem- und Telekommunikationsspezialisten vorbehalten. Günstige, energiesparende und trotzdem äußerst leistungsstarke Kleinstrechner (z.B. Arduino[1] oder Raspberry Pi[2]) ermöglichen, verschiedenste Steuerungen kostengünstig und rasch zu realisieren. Dazu reicht es aus, die Kleinstrechner mit einem Mobilfunkmodem zu verbinden und Daten mittels klassischer Internettechnologien zu übertragen. Software Technologien wie Python oder Java gehören mittlerweile auch bei mobilen Kleinstrechnern zum Standard und die Entwicklung von Anwendungen wird durch leistungsfähige (Open Source) Tools maßgeblich unterstützt.

Massenlösungen und Sonderlösungen von mobilen Mess- & Steuergeräten sind für viele Anwendungen erschwinglich geworden und motivieren somit viele Unternehmen zur Investition in die mobile Steuerung und Überwachung von Prozessen. Dementsprechend steigt die Anzahl der auf M2M Kommunikation zurückzuführenden Verbindungen ständig und wird - wie in Abbildung 1 ersichtlich - 2020 weltweit die Anzahl der Verbindungen von Mobiltelefonen und Datenkarten deutlich übertreffen.

[1] http://de.wikipedia.org/wiki/Arduino-Plattform
[2] http://de.wikipedia.org/wiki/Raspberry_Pi

Telekom Austria Group M2M GmbH, Obere Donaustraße 33, 1020 Wien
Tel.: +43 50664 45881, E-Mail: m2m.smartmetering@telekomaustria.com
Web: http://m2m.telekomaustria.com/smart-metering

Aufgabenstellung

Szenario 1: Das M2M Gerät als Webserver

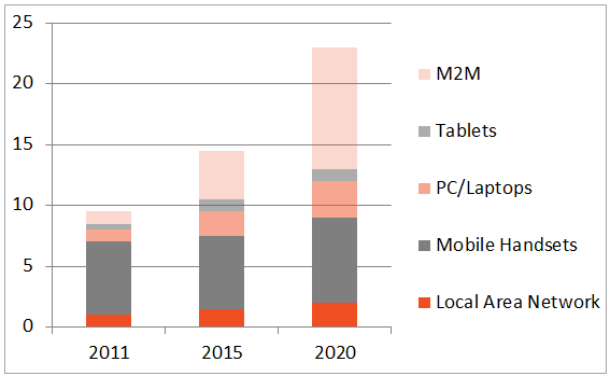

Abb.1: Geräte im Mobilfunk weltweit

Viele M2M Geräte auf dem Markt benutzen eine Internetanbindung. Das heißt, das mobile Endgerät wird mit einem Mobilfunkmodem zur Verbindung mit dem öffentlichen Internet ausgestattet. Damit dieses Gerät von beliebigen Internet PCs und Notebooks erreichbar ist, werden oftmals auch Dienste wie Dynamisches DNS verwendet. Somit ist das Gerät jederzeit über einen Internet Domainnamen, einen sogenannten URL, erreichbar. Die Abbildung 2 zeigt ein fiktives Beispiel mit einer fernbedienbaren Kamera, die mit der (frei erfundenen) URL http://meine--nummer-08-15.dyndns.org/ erreichbar sein könnte.

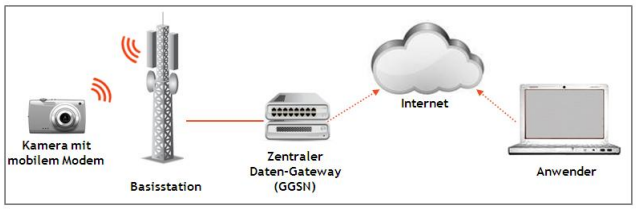

Abb. 2: Kamera als Webserver

Vorteile:

- Diese Art der Installation eines M2M Services ist einfach und rasch. Sie funktioniert mit den meisten SIM-Karten, wie sie in Smartphones und Datensticks verwendet werden.

Nachteile:

- Das M2M Gerät ist mit einer öffentlichen IP Adresse ausgestattet. Das bedeutet, dass dieses Gerät allen Sicherheitsrisiken des weltweiten Internets ausgesetzt ist. Deshalb muss es sicherheitstechnisch laufend und rasch gewartet werden.
- Das Management der Geräte ist dezentral und wird bei größeren Installationen ziemlich aufwändig.
- Der Zugriffschutz zum Gerät muss eingerichtet werden, oft bleiben Standard Kennworte bestehen und deren Existenz wird nach der ersten Inbetriebnahme vergessen.
- Es fehlen professionelle Schutzeinrichtungen, wie z.B. Firewalls oder Intrusion Detection/Prevention Systeme.
- http-Anwendungen übertragen die Daten unverschlüsselt im Internet. Schützenswerte Daten müssen verschlüsselt werden.
- Betrieblich ist das M2M Gerät selbst für das Management der Verbindung zum Internet und der Aktualisierung eines eventuell genutzten dynamischen DNS Dienstes verantwortlich.
- Es ist nicht klar, ob mehrere Benutzer gleichzeitig auf das M2M Gerät zugreifen dürfen. Falls mehrere Benutzer gleichzeitig zugreifen, muss das Videomaterial für jeden Benutzer gleichzeitig über das Mobilfunknetz übertragen werden. Das führt zu einem unnötig hohen Datenverkehr, der das Limit eines Mobilfunkteilnehmers in einer Funkzelle übersteigen kann, sodass die Kamera für einzelne oder alle Nutzer nicht mehr in der gewünschten Qualität erreichbar ist.

Szenario 2: Das M2M Gerät als Client

Um beim Beispiel der Kamera zu bleiben, wird in diesem Szenario, das in Abbildung 3 dargestellt ist, ein Server verwendet, der mit

einer Kamera verbunden ist und das entsprechende Bildmaterial regelmäßig hochlädt. Mehrere Benutzer können es vom zentralen Server abrufen.

Diese Variante hat wichtige Vorteile:

- Die Kamera muss aus dem Internet nicht mehr erreichbar sein. Somit sind Dienste wie Dynamic DNS nicht mehr notwendig.
- Das Datenmaterial wird nur einmal über das Mobilfunknetz übertragen.
- Die Verwaltung der Anwender geschieht im Server.
- Die Benutzer können das Bildmaterial rasch über einen Server abrufen. Der Server kann je nach Kapazität viele Benutzer gleichzeitig bedienen.
- Die Qualität und Verfügbarkeit der M2M Geräte kann vom Server gemessen, protokolliert und ausgewertet werden.

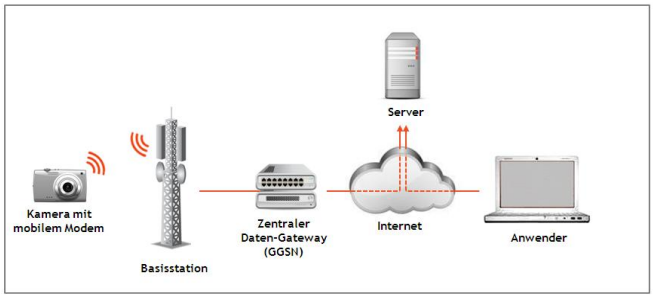

Abb. 3: Kamera als Client

Aber auch bei dieser Installation bleiben erhebliche Risiken bestehen

- Die Kamera wird weiterhin im öffentlichen Internet betrieben und bleibt den Gefahren im Internet ausgesetzt.
- Der Server muss sowohl seitens der Kamera als auch vom Benutzer aus dem öffentlichen Internet erreichbar sein und muss deshalb angemessen gesichert werden.
- Der manuelle Verwaltungsaufwand der SIM-Karten ist bei großen Installationen erheblich.

Lösungsvorschlag – Best Practice

Um zu verstehen, wie die Daten in einem Mobilfunknetz transportiert werden und welche Systemkomponenten besonders wichtig sind, wird der Aufbau und die Funktionsweise in diesem Abschnitt erklärt und anschließend ein Architekturvorschlag für ein sicheres M2M Service beschrieben.

Aufbau eines Mobilfunknetzes

Ein Mobilfunknetz wird zentral verwaltet: Sowohl Telefonie als auch der Datenverkehr werden über wenige leistungsstarke zentrale Elemente geführt. Abbildung 4 zeigt ein stark vereinfachtes Modell eines Mobilfunknetzes. Im Mittelpunkt stehen zentrale Elemente, wie z.B. eine Vermittlung (MSC – Mobile Switching Center), die Telefongespräche von Teilnehmern verbinden, oder der zentrale Daten-Gateway (GGSN – Gateway GPRS Support Node; GPRS – General Packet Radio Service), der die IP Pakete eines Teilnehmers an das öffentliche Internet oder in private Datennetze übergibt.

Mobile Geräte sind über Funk an einer Basisstation im Netz eingebucht. Mehrere regionale Kontrollstationen (RNC – Radio Network Controller) leiten den Datenverkehr zwischen den Basisstationen und den zentralen Elementen weiter. Eine zentrale Datenbank (HLR – Home Location Register) vermerkt, welche SIM-Karten im Netz einbuchen können und welche Services diese nutzen dürfen.

Mobiles Datennetzwerk

Für den Aufbau einer mobilen IP basierten Datenverbindung kontrolliert zunächst die zentrale Datenbank HLR, welche SIM-Karte für welche Datendienste berechtigt ist und teilt dies auf Anfrage dem zentralen Daten-Gateway GGSN mit. Wie bereits beschrieben, verbindet der GGSN das Mobilfunknetz mit externen Datennetzen. Im Gegensatz zu einem „herkömmlichen“ Internet Router erlaubt der GGSN die Festlegung verschiedener Übergangspunkte, die unterschiedlich be-

nannt werden (engl. Access Point Name = APN).

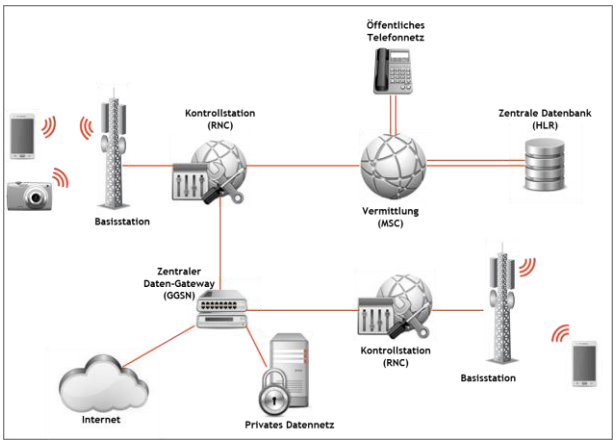

Abb. 4: Aufbau eines Mobilfunknetzes

Der GGSN bietet also die Möglichkeit, die mobilen IP Daten getrennt in verschiedene externe Netze weiterzuleiten. Im Falle von Smartphones und Datenkarten ist in der Regel ein APN für das öffentliche Internet vorkonfiguriert. Im A1 Netz heißt der Internet APN beispielsweise „a1.net“ und ist bei allen A1 Smartphones voreingestellt.

Da M2M Geräte auf Grund der beschränkten Ressourcen und schwierigeren Wartung in der Regel nicht direkt mit dem öffentlichen Internet verbunden werden sollten, bietet es sich geradezu an, zusätzliche APNs speziell für M2M zu definieren. IP Daten, die an diese M2M APNs gesendet werden, leitet der GGSN in dazugehörige private Netze weiter.

Für unser fiktives Beispiel bedeutet das, dass ein exklusiver APN mit dem Namen „kameras.m2m“ definiert und eine direkte Datenleitung (oder ein VPN Tunnel) zwischen dem GGSN und dem Serversystem für diese Kameras errichtet wird. Somit befinden sich die Kameras und der dazugehörige Server in einem vom Internet abgeschirmten privaten Netz.

Das mobile Endgerät startet die mobile Datenverbindung, indem es dem Funknetz bekannt gibt, mit welchem APN es verbunden werden soll (z.B. „kameras.m2m“). Das Mobilfunknetz prüft mittels HLR Abfrage, ob die verwendete SIM-Karte für diesen APN berechtigt ist und vergibt eine IP Adresse an das mobile Endgerät. Von nun an leitet das Datengateway GGSN alle IP Pakete vom mobilen Endgerät automatisch in das zuvor eingerichtete private Datennetz weiter.

Das mobile Endgerät benötigt keinen VPN Client. Allein die Konfiguration des privaten APNs im Mobilfunkmodem reicht aus, um die Daten korrekt und sicher in das jeweilige private Firmennetz zu leiten.

Architektur für ein sicheres M2M Service

Unter Verwendung eines privaten APNs lässt sich nun beispielhaft eine sichere Architektur für einen M2M Dienst, wie in Abbildung 5 dargestellt, ableiten.

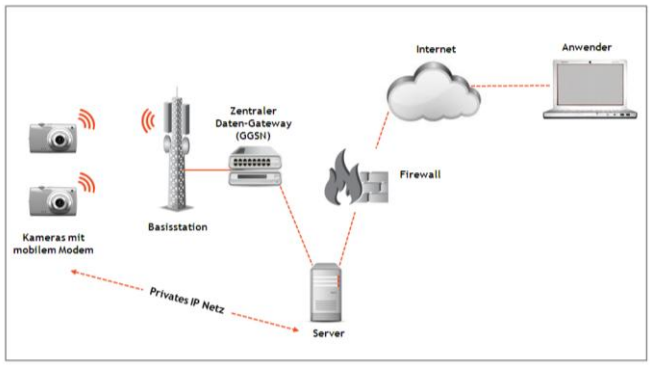

Abb. 5: Architektur für sicheres M2M Service

Der Provider definiert gemeinsam mit dem Kunden einen privaten APN, z.B. „kameras.m2m“ und aktiviert entsprechend die SIM-Karten für diese geschlossene Benutzergruppe. Diese Konfiguration garantiert, dass der IP Datenverkehr isoliert vom öffentlichen Internet über das Mobilfunknetz übertragen wird. Vom zentralen Daten-Gateway GGSN wird der private IP Datenverkehr direkt (oder über einen geschützten VPN Tunnel) zum Server des Kamera Systems weitergeleitet. Dieser befindet sich ebenfalls im gesicherten Bereich eines Rechenzentrums. Der Server kann vom Internet für alle berechtigten Anwender erreichbar sein, doch er wird entsprechend dem Stand der Technik mit Sicherheitssystemen, wie z.B. Firewalls und Intrusion Detec-

tion/Prevention Systemen, geschützt. IT Profis eines IKT Dienstleisters sorgen für den sicheren und zuverlässigen Betrieb dieser Architektur.

Diese Architektur bietet entscheidende Vorteile:

- Die einzelnen M2M Geräte sind nicht mit dem öffentlichen Internet verbunden. Somit sind die Risiken und der Wartungsaufwand der mobilen Geräte deutlich niedriger.
- Die Applikationsserver befinden sich in einem gesicherten und privaten Bereich eines Rechenzentrums. Ein professionelles IKT Dienstleistungsunternehmen administriert und überwacht den Betrieb, sowie den Netzwerkverkehr zu und von den M2M Geräten.
- Die M2M Geräte können mit fixen, privaten IP Adressen ausgestattet werden und somit ist sowohl ein Client als auch ein Serverbetrieb der M2M Geräte möglich.
- Der Provider sorgt dafür, dass der Zugang zum privaten Netz über den privaten APN ausschließlich mit berechtigten SIM-Karten möglich ist.
- Der Provider entzieht den SIM-Karten den APN für die Verbindung zum öffentlichen Internet. Sogar bei Fehlkonfiguration eines M2M Gerätes kann in diesem Fall keine Verbindung zum öffentlichen Internet hergestellt werden.

Weitere Tipps

Die folgenden Tipps helfen, eine mobile M2M-Anwendung möglichst effizient und effektiv zu gestalten, um dadurch die Voraussetzungen für beste M2M-Qualität zu schaffen.

Sparsamkeit

Nur jene **Daten**, die **unbedingt erforderlich** sind, sollen **übertragen** werden. Es macht zum Beispiel bei einer Kamera keinen Sinn ständig ein Foto zu übertragen, dessen Inhalt sich nicht ändert. Komprimierungsalgorithmen tragen zur Effizienz bei, z.B.ist es wesentlich effizienter, ein komprimiertes Foto zu übertragen, als die gesamte Datenmenge des Pixel-Rohformats eines CCD-chips.

Nicht jede Änderung eines Messwertes muss sofort übertragen werden (z.B.: die Temperatur eines Badesees). Je nach Bedeutung der Daten und Anwendungszweck macht es Sinn, weniger oft eine Datenverbindung aufzunehmen und dabei eine Datensammlung zu übertragen, anstatt jede Datenänderung mit einer eigenen Datenverbindung sofort mitzuteilen.

Push oder Pull?

Je nach Anwendung wird ein M2M Gerät entweder bei Eintreten definierter Ereignisse (z.B.: ein Bewegungssensor spricht an, ein Schwellwert wird überschritten) oder in periodischen Abständen (z.B. regelmäßiger Messwert) Daten an den Server liefern. In diesem Fall spricht man von einem „Push“ – Verfahren. Die **M2M Geräte werden selbst aktiv**, wenn es Daten zu liefern gibt oder Updates vom Server erwartet werden. Nach der Datenübertragung könnten die M2M Geräte ihre Datenverbindung abbauen und so Ressourcen sparen.

Bei einem „Pull“-Verfahren **fragt der Server beim M2M Gerät** nach, ob und welche Daten es zu liefern hätte oder neue Daten in das M2M Gerät zu übertragen sind. Der Vorteil dieses Verfahrens liegt in der zentralen Taktung der Datenübertragung aller dazugehörigen M2M Geräte. Beim Pull-„Verfahren“ müssen die **M2M Geräte empfangsbereit** für Befehle des Servers sein. Ob eine ständige Empfangsbereitschaft aller M2M Geräte für Datenanfragen zweckmäßig ist, hängt von der jeweiligen Anwendung ab.

Wenn eine M2M-Anwendung eine kleine Anzahl von Geräten umfasst, so hat das „Pull“-Verfahren wegen der unmittelbaren Erreichbarkeit der Geräte einen Vorteil. Gehören zu einer M2M-Anwendung jedoch sehr viele Geräte, so bleiben beim „Pull“-Verfahren dem zentralen Server, der die Geräte der Reihe

nach abfragt und dabei etwaige Fehlerfälle berücksichtigen muss, zu wenig Zeit pro Gerät. Bei einer sehr großen Zahl von M2M Geräten müssen Hierarchien von Servern und/oder parallele Verfahren eingesetzt werden, um viele Geräte in einer vorgegebenen Zeit bedienen zu können.

Vom Standpunkt der Sicherheit aus betrachtet, sind Geräte mit **„Push"-Verfahren** über das Netzwerk **schwerer anzugreifen** als Geräte mit „Pull"-Verfahren, weil die beim „Pull"-Verfahren notwendige Empfangsbereitschaft auch eine Angriffsmöglichkeit für gefälschte Serverbefehle bietet.

Wie könnten M2M Geräte, die ausschließlich im Push-Verfahren arbeiten, dennoch zentral erreicht werden? Hierbei bietet der Mobilfunk einen besonderen Vorteil: Ein M2M Gerät, das keine Datenverbindung aufgebaut hat, kann durch eine anwendungsspezifische SMS dazu veranlasst werden, diese aufzubauen.

1.1.1 Asynchronität

Beim Entwurf einer M2M-Anwendung, die periodisch bestimmte Aktivitäten durchführen soll, ist darauf zu achten, dass hunderttausende Geräte **nicht zum gleichen Zeitpunkt** kommunizieren. So etwas kann leicht passieren, wenn z.B. ein Anwendungsprogrammierer festlegt, dass gesammelte Daten immer zur vollen Stunde an den Server übertragen werden. Sollten wirklich hunderttausende Geräte gleichzeitig zum Server übertragen wollen - vorausgesetzt deren Uhren sind synchronisiert - so erzeugt dies einerseits eine **Spitzenlast im Mobilfunknetz** und andererseits wird ein gewöhnlicher Server unter einer so großen Anzahl gleichzeitiger Verbindungen zusammenbrechen. Datenverbindungen werden abbrechen und die M2M Geräte werden die Verbindungsversuche gleichzeitig wiederholen, was wiederum eine Lastspitze erzeugt.

Kommunikationsnetze sind für Millionen Anwender so entworfen, dass sie die üblichen Verkehrslasten und Verkehrsspitzen bewältigen können. Ein wichtiger Grundsatz ist, dass die Kommunikationsbedürfnisse **zufällig** und **voneinander unabhängig** entstehen und **statistisch verteilt** sind. **Gleichzeitigkeit führt zu Überlast.** Wie es vergleichsweise unmöglich ist, dass alle KFZ Lenker gleichzeitig auf die Autobahn auffahren, so ist es unmöglich, dass alle Teilnehmer eines Mobilfunknetzes gleichzeitig telefonieren können.

Der Architekt einer M2M-Anwendung muss deshalb die mögliche Gleichzeitigkeit der Kommunikation aller M2M Geräte berücksichtigen und Algorithmen einsetzen, die das vermeiden. Bei periodischen Aktivitäten einer sehr großen Zahl von M2M Geräten sollen deshalb variable Zufallsgrößen und/oder individuelle Gerätemerkmale (z.B. Seriennummern) den Zeitpunkt der Datenübertragung so beeinflussen, dass die Anzahl gleichzeitig kommunizierender Geräte minimiert wird.

Leistungen eines M2M Service Providers

Telekom Austria Group M2M bietet als Spezialist für M2M eine Vielzahl von Services an und kann dabei auf die Unternehmen der Telekom Austria Group, deren Technologie und Erfahrung mit dem Betrieb und dem Management von sicheren Dateninfrastrukturen zurückgreifen. Im Folgenden werden einzelne Punkte hervorgehoben, die zwar auf die Datenverbindung selbst nur indirekten Einfluss haben, jedoch erhebliche Vorteile für die effiziente Verwaltung und den wirtschaftlichen Betrieb von großen M2M Installationen bringen.

SIM-Karten Management

Die SIM-Karte speichert mit Hilfe von hochsicherer Smartcard Technologie die geheimen Schlüssel für den Zugang zum Mobilfunknetz. Das Mobilfunknetz wiederum speichert und verwaltet zentral die Berechtigungen für diese Karte. Diese Berechtigungen umfassen unter anderem:

- Zugang zu APNs
- Senden und Empfangen von SMS

- Sprachtelefonie
- Roaming

In vielen Einsatzgebieten von M2M sind die Anforderungen an SIM-Karten deutlich höher als bei Smartphones:

- Extreme **Temperaturschwankungen**
- **Mechanische Belastungen** (z.B. Zugverkehr bei Verkaufsautomaten auf einem Bahnsteig)
- **Austauschen** der SIM-Karte bei installierten Geräten ist nur **schwer** bis überhaupt nicht **möglich**
- **Sehr lange Lebensdauer** notwendig (z.B. Stromzähler)
- **Korrosionsbeständigkeit** (Kontakte zwischen SIM-Karte und SIM-Kartenhalter)

Aufgrund dieser Anforderungen bietet die Mobilfunkindustrie eine Vielzahl verschiedener Formfaktoren für SIM-Karten an. Besondere Bedeutung haben dabei sogenannte **embedded SIM-Karten**. Diese werden als Chips direkt in die Fabrik der M2M Geräte geliefert und werden, wie alle anderen elektronischen Bauteile **auf die Platine gelötet**. So benötigen die SIM-Karten erheblich weniger Platz, sind mechanisch stabiler und aufgrund der Direktverlötung korrosionsbeständiger. Nebenbei werden die Kosten für den SIM-Kartenhalter eingespart.

Voraussetzung für die Verwendung von embedded SIM-Karten ist die Integration der SIM-Karten-Bestellprozesse in den Fertigungs- und Testprozess der M2M Geräte. Beispielsweise muss **mitprotokolliert** werden, welche SIM-Karte in welches Gerät gelötet wurde. In Abbildung 6 sind die Prozessschritte dieses Beispiels abgebildet. Jeder Prozessschritt benötigt auch eine Dokumentation und Administration.

Um die Verwaltung von M2M SIM-Karten zu erleichtern, bietet Telekom Austria Group M2M spezielle **Webservices** an, die das automatische Aktivieren, Deaktivieren und Steuern einzelner SIM-Karten durch den Auftraggeber der M2M-Anwendung erlauben. Somit kann das Management der SIM-Karten vollautomatisch in den Lebenszyklus des M2M Geräts integriert werden.

M2M Security – mit "SIMplify" - die Telekom Austria Group SIM Management Lösung

Ein wichtiges Service ist die webbasierte SIM-Karten Managementplattform **SIMplify**, die es Kunden ermöglicht SIM-Karten selbständig zu aktivieren, deaktivieren und zu steuern.
SIMplify bietet eine Reihe von Sicherheitsfeatures:

- **Privater APN** mit dezidierten Login Credentials für jeden Kunden und jede Anwendung
- State of the Art Login-**Passwort Richtlinien** & Brute Force Attacken Detektion
- **VPN Tunnelung** (IPSec verschlüsselt)
- **Paarung** der **SIM**-Karte mit dem **Endgerät** (via IMEI) und automatische Blockade der Geräte, sollte sich eine SIM-Karte mit einer anderen IMEI einbuchen
- **Limitierung** der adressierbaren **IP Adressen** (white- und blacklisting)
- **Alarmierung** bei erhöhtem **Datenverbrauch**
- **Alarmierung** wenn das M2M Gerät das **Land verlässt**
- **Alarmierung** bei **unüblichem Geräteverhalten** (z.B. außergewöhnliche Anzahl an Verbindungen, oder Dauer einzelner Verbindungen)
- **Quarantäne Profile** für SIM-Karten mit verdächtigem Verhalten
- **Nicht gewünschte Services** (SMS, Daten, Roaming, etc.) können **deaktiviert** werden

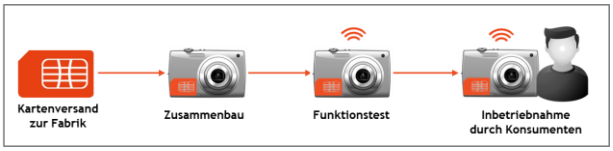

Abb.6: Zyklus der SIM-Karte bis zum Konsumenten

Roaming

Viele M2M Anwendungen machen nicht vor nationalen Grenzen halt. Beispielsweise benötigen viele Logistikfirmen M2M-Lösungen, die sowohl national als auch international mit dem gleichen Qualitätsstandard wie im Inland funktionieren. Die Roaming-Technologie erlaubt die **Verwendung** von **privat definierten APNs** in **ausländischen Netzen** genauso wie im Inland. Das heißt, die IP Pakete werden über gesicherte Tunnels vom ausländischen Mobilfunknetz an den GGSN in Österreich übergeben und hier in das zuvor definierte private Datennetz weitergeleitet. Somit ist auch im Roamingfall garantiert, dass die **Daten getrennt vom öffentlichen Internet** den Weg in das private Firmennetz finden.

Zusätzlich bietet die Telekom Austria Group M2M spezielle SIM-Karten an, die für alle nationalen Mobilfunknetze freigeschalten sind. Somit kann eine besonders hohe Mobilfunkverfügbarkeit selbst in schwierigen Versorgungslagen (Keller, Stahlbetongebäude, usw.) angeboten werden. Die Datenübertragung gelingt, wenn **irgendein Mobilfunknetz** am Ort des M2M Geräts verfügbar ist.

Kostenkontrolle

Da M2M Geräte autark und automatisch Datenverbindungen aufbauen, ist eine Steuerung und Überwachung der Kosten eine besondere Herausforderung. M2M Betreiber bieten dazu Tarife und Systeme an, die ein laufendes Reporting über den Datenverbrauch der einzelnen Geräte ermöglichen. Zusätzlich können für jede M2M SIM-Karte **individuelle Berechtigungen** vergeben werden, um beispielsweise die Berechtigung zum Roamen, oder den Datenverbrauch bis zu einem speziellen Limit im konkreten Fall anpassen zu können.

Weitere Dienstleistungen

Rund um den Lebenszyklus von M2M Geräten gibt es viele Prozesse, die von Telekom Austria Group M2M unterstützt werden können. Dazu gehören z.B.:

- **Hilfestellung** bei der Auswahl von M2M Geräten
- **Testen** von Geräten
- **Roll-out und Installation** vor Ort
- Betriebsüberwachung
- Entstörung und Wartung
- Diverse IT-Dienstleistungen

Wichtig ist die Tatsache, dass die Qualität, Zuverlässigkeit und Sicherheit einer M2M-Anwendung nicht nur von der mobilen Datenübertragung selbst, sondern auch von all diesen Prozessen und der Gesamtarchitektur der M2M-Anwendung abhängig ist.

Datenschutz beim Hosting

Im Zusammenhang mit M2M gibt es auch viele Anwendungen, die auf das Hosting von Services und Datenbanken zurückgreifen. Security ist dabei natürlich eine wesentliche Voraussetzung, um Betriebsrisiken zu minimieren. Darüber hinaus ist bei allen persönlichen und sensiblen Daten auch der **Datenschutz** von **höchster Wichtigkeit**. Die gesetzlichen Vorgaben sind dazu eindeutig. Werden im Rahmen von Hosting datenschutzrechtlich relevante Kundendaten verarbeitet, so handelt es sich im Sinne des Datenschutzgesetzes dabei um eine „Überlassung“ von Daten. Dabei werden Daten einem Dienstleister mit dem Auftrag übergeben, sie in einer bestimmten Weise für den Auftraggeber zu verarbeiten. Gemäß §§ 10 ff DSG ist neben dem eigentlichen IT-Dienstleistungsvertrag ein datenschutzrechtlicher Dienstleistungsvertrag mit dem Dienstleister abzuschließen, in welchem dem Dienstleister bestimmte Verpflichtungen bezgl. Datensicherheit auferlegt werden. „Herr der Daten“ bleibt jedenfalls nach wie

vor der Dienstgeber. Er entscheidet allein, WAS der Dienstleister WIE mit diesen Daten machen darf.

Zusammenfassung

Die Übertragungstechnik mit Internetprotokollen ist weit verbreitet und wird in zunehmendem Ausmaß für etliche Anwendung benutzt. Die Mobilfunknetze sind gut ausgebaut, verlässlich und günstig. Datenanwendungen, die auf IP Technik und Mobilfunk beruhen, sind zukunftssicher und bilden eine besonders gute Basis für die **Kommunikation von Maschine zu Maschine (M2M)**.
In diesem Artikel wurde eine Architektur für M2M Kommunikation entworfen und allgemeine Empfehlungen für das Kommunikationsverhalten von verteilten M2M Anwendungen vorgeschlagen.

Je größer die Zahl an M2M Geräten für eine bestimmte Anwendung ist, desto sorgfältiger muss diese geplant werden. Dieser allgemeine Artikel kann nicht alle Aspekte und Herausforderungen einer konkreten Anwendung abdecken. Als kompetenter Partner unterstützt Telekom Austria Group M2M gerne Ihr individuelles M2M Projekt.

Telekom Austria Group M2M ist ein 100%iges Tochterunternehmen der Telekom Austria Group, der führende Telekommunikationsanbieter in Mittel-und Osteuropa mit mehr als 22 Millionen Kunden in acht Märkten. Mit kostengünstigen Dienstleistungen und maßgeschneiderten Lösungen unterstützt Telekom Austria Group ihre Kunden bei der Entwicklung neuer M2M Geschäftsmodelle. Daraus ergeben sich signifikante Kosteneinsparungen, Prozessoptimierungen und eine effiziente Nutzung der natürlichen Ressourcen. Zusammen mit einem großen internationalen Netzwerk von strategischen Partnern bieten Telekom Austria Group und ihre Betriebsgesellschaften paneuropäische und globale Dienstleistungen rund um die Welt.

TELEKOM AUSTRIA GROUP M2M

Telekom Austria Group M2M GmbH, Obere Donaustraße 33, 1020 Wien
Tel.: +43 50664 45881, E-Mail: m2m.smartmetering@telekomaustria.com
Web: http://m2m.telekomaustria.com/smart-metering