# Sicherheit bei mobilen Hotel-ID- und IoT-Lösungen

Wir alle leben in einer Zeit, in der nichts sicher zu sein scheint. Tagtäglich lesen wir von Hackerangriffen, Wirtschaftsspionage, Datendiebstahl und einiges mehr in der Geschäftswelt. Die weitläufig zitierte Phrase, es gäbe keine absolute Sicherheit, gilt auch für jegliche zu Sicherheitszwecken eingesetzte Technologie. Dennoch lässt sich das Risiko einer Sicherheitslücke durch die ordnungsgemässe Anwendung und Verbindung geeigneter Sicherheitsmassnahmen deutlich verringern.

Die Zahl der Einbrüche steigt von Jahr zu Jahr, die Magnetstreifen unserer EC-Karten werden geklont, Sicherheitsdienste spähen unsere E-Mails aus und Phishing-Mails wollen sich Zugriff auf unsere Konten verschaffen. Heutzutage muss man Dinge doppelt und dreifach sichern, regulieren, standardisieren und zertifizieren, damit man sich sicher und geschützt fühlt.

Im Dezember 2016 verkündete der Chaos Computer Club den Hack eines Türschlosses und des dazugehörigen Mobile Apps, welches mittels Bluetooth Low Energy (BLE) mit dem Schloss kommuniziert. Das könnte möglicherweise Konsequenzen für Hotels haben, in denen mobile Zimmerschlüssel für die Räume zum Einsatz kommen, da auch deren Türschlösser via BLE mit Smartphones kommunizieren und vertrauliche Informationen austauschen. LEGIC, ein Schweizer Sicherheitsunternehmen, ist auf end-to-end Lösungen spezialisiert, die ein Hacken solcher mobilen ID-Lösungen verhindern.

*Mit LEGIC lassen sich Hoteltüren per Smartphone öffnen.*

## MOBILE ZIMMERSCHLÜSSEL

Mittlerweile erweitern immer mehr Hotels ihre Apps um mobile Zimmerschlüssel, da das Gasterlebnis und die Gastbeteiligung durch eine App immer wichtiger werden. Mobile Zimmerschlüssel bieten zahlreiche Vorteile: Die Gäste müssen sich nicht an der Rezeption anmelden und auf ihre Zimmerkarten warten. Das Buchen des Lieblingszimmers im Voraus und der Erhalt des Zimmerschlüssels direkt aufs Smartphone oder das Verlängern des Aufenthalts, ohne sich nochmal in die Schlange an der Rezeption einreihen zu müssen, sind nur einige der erwähnenswerten Vorteile.

Auch wenn viele Hotelgäste die mobilen Zimmerschlüssel schätzen, muss die Verbindung zur Übertragung sensibler Daten geschützt werden. Würde das komplette mobile Schliesssystem eines Hotels gehackt werden, hätten die Hacker Zugriff auf jeden einzelnen Raum in dem Hotel. Schlimmstenfalls müsste das Hotel dann nicht nur die mobile Schlüsselfunktion einstellen, sondern auch jede einzelne Schlüsselkarte neu konfigurieren und die Hardware in allen Türschlössern aufrüsten. Daraus ergäbe sich ein Imageschaden für das Hotel und auch die Kosten wären exorbitant.

## SICHERHEIT IN DER WELT MOBILER IDENTITÄT

Um einen hohen Sicherheitsstandard zu erreichen, muss das gesamte System umfassend geprüft und eine Reihe von Sicherheitsmassnahmen in Erwägung gezogen werden. Das Mobilgerät, meistens ein Smartphone, verfügt über eine Internetverbindung – ein Risiko für ferngesteuerte Angriffe. Da die derzeitigen Apps keinen vollumfänglichen Zugriff auf die Sicherheitshardware auf dem Telefon haben, sind die Apps nur eingeschränkt in der Lage, ihre sensiblen Daten, beispielsweise Verschlüsselungscodes, Identitätsrechte oder kritische Programmcodes, zu schützen. Eine Lösung, welche die Datenverschlüsselungscodes nicht in potentiell gefährdeten Apps speichert, sondern die Daten in einer vertrauenswürdigen Cloud-Lösung für die Ausgabe mobiler Zimmerschlüssel verschlüsselt und Daten in der Hardware der Türschlösser entschlüsselt, ist daher sehr empfehlenswert. Solche Lösungen nutzen die sogenannte end-to-end Hardware-Sicherheitstechnik.

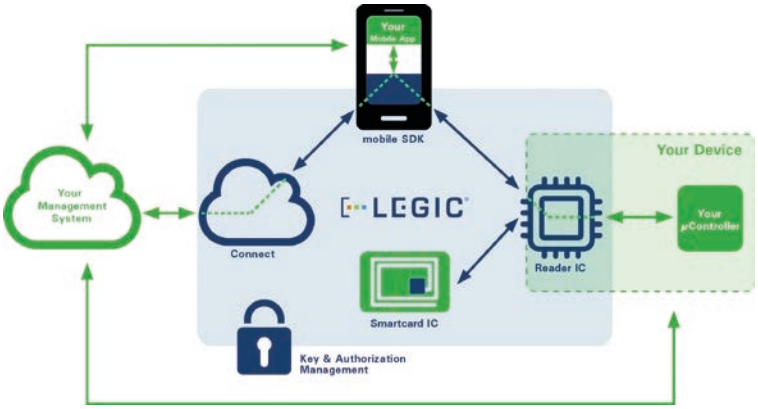
Die böswillige Übertragung von in einer Software gespeicherten Identitätsrechten auf ein anderes Mobilgerät mittels Klontechnik ist ein weiteres ernsthaftes

Problem. Die Sicherheitsrelevanz eines Mobilgeräts wird deutlich eingeschränkt, wenn es online und mit dem Verwaltungssystem verbunden ist, sobald mobile Identitätsrechte auf das Gerät übertragen werden müssen. In dieser Situation sollten die tatsächlichen Identitätsrechte im Verwaltungssystem gespeichert werden, während das Smartphone lediglich als Kommunikationsmedium dient. Eine Minderung des Schadens, den geklonte Smartphones anrichten, kann auch dadurch erreicht werden, dass das Verwaltungssystem eine Transaktionsautorisierung via SMS verschickt oder den Anwender dazu auffordert, ein Passwort, eine PIN oder einen Touch ID-Fingerabdruck einzugeben (sogenannte Zwei-Faktor-Authentisierung, die Dinge nutzt, die Sie besitzen, und die Sie wissen).

## AUGENMERK AUF SICHERHEIT

Das zunehmende Augenmerk von Hackerorganisationen auf Bluetooth-basierte Schlösser bedeutet, dass es für Hotels und andere Organisationen, die mobile Schlüssel einsetzen, wichtiger ist denn je, ein auf einer end-to-end Hardware-Sicherheit beruhendes mobiles Schliesssystem einzusetzen.

Das end-to-end Offering von LEGIC setzt Hardware-basierte Sicherheit ein, bei denen ein Leser-IC mit Bankenlevel (EAL 5+) zertifiziertem, manipulationssicherem Secure Element im Schloss und ein Hardware Security Module (HSM) im cloud-basierten Trusted Service LEGIC Connect zum Einsatz kommen. Das von LEGIC eingesetzte Secure Element (SE) bietet eine sichere Umgebung für das Speichern von Schlüsseln, kryptographischen Berechnungen und für die Speicherung essentieller Software für Sicherheit und Geschäftsbelange. Dieses SE ähnelt den Crypto Chips, die zur Sicherung von Zahlungsvorgängen in Kartenlesegeräten an Kassen verwendet werden, und ist somit sehr sicher. Außerdem werden mit LEGIC keine Datenverschlüsselungsschlüssel in potentiell gefährdeten Apps gespeichert, diese existieren nur im SE des Schlosses und den Trusted Service HSMs. Ein Hacken der App, wie vom Chaos Computer Club gezeigt, wird damit verhindert.




*Das LEGIC Offering mit der end-to-end Sicherheit zwischen LEGIC Connect und dem Leser-IC*

Seit 25 Jahren bietet LEGIC Sicherheitslösungen für höchste Ansprüche. Die offene Technologieplattform ist die beste Wahl für sichere Kommunikation und Identifikation. Die fünf Komponenten, bestehend aus LEGICs sicherem Trusted Service, dem Mobile SDK, Leser-ICs, Smartcard-ICs sowie dem Schlüssel- und Autorisierungsmanagement, bilden dank einer nahtlosen Zusammenarbeit eine leistungsstarke Technologieplattform für sichere mobile ID- und IoT-Anwendungen.

*Autor:*
*Sabrina Storrer,*
*Manager Product Marketing*
*LEGIC Identsystems AG*
*CH-8620 Wetzikon*
*Foto/Grafik: LEGIC*
*www.legic.com*