WHITE PAPER

Die Integration mobiler Geräte in Zutrittskontrollsysteme

Sicherheit trifft Komfort - mobile Geräte in der Zutrittskontrolle

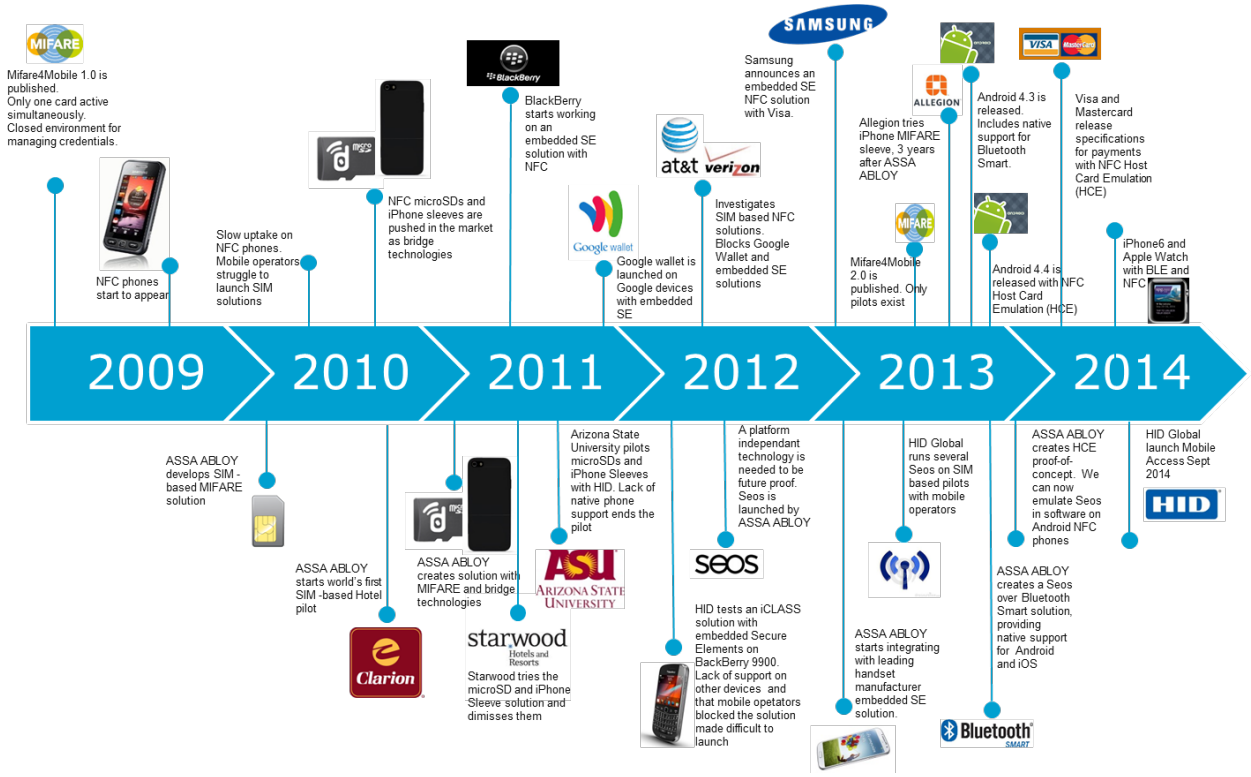
Mobile Zutrittskontrolle

Beim Konzept der Zutrittskontrolle mit Smartphones oder Tablets geht es nicht nur darum, den Zugang zu Gebäuden mit mobilen Geräten zu ermöglichen. Es geht vielmehr darum, die Zutrittskontrolle als solche zu verbessern, dem technologischen Fortschritt Rechnung zu tragen und unseren Umgang mit dem Zugang zu Gebäuden und Daten grundlegend zu verändern. Im Zeitalter von Mobilität und Cloud-Computing machen sich Unternehmen und Privatpersonen zunehmend Gedanken über die Sicherheit und den Schutz ihrer Umgebung. Wird die mobile Zutrittskontrolle korrekt implementiert, ist sie zukunftsweisend: Zum ersten Mal verügen wir über eine Lösung, die sowohl die Sicherheit als auch den Komfort verbessert.

Mobile Trends

Die Telekommunikationsbranche ist eine der innovativsten und schnelllebigsten. Sie hat sich in den letzten Jahren bemerkenswert entwickelt. Industrieforschungsinstitute gehen davon aus, dass die Anzahl der ausgelieferten mobilen Geräte im Jahr 2014 1,7 Milliarden erreichen wird. Mit diesem rasanten Wachstum entwickeln sich auch die Technologien und Standards der mobilen Geräte weiter. Immer mehr Menschen nutzen diese täglich, und so kommen laufend neue Anwendungen hinzu. Ein großer Teil der Technologie in aktuellen Geräten wird erst jetzt von der breiten Masse genutzt, obwohl diese bereits seit langem existieren. Bluetooth® wurde 1994 eingeführt und es dauerte 15 Jahre, bis es zum De-facto-Standard in mobilen Geräten wurde. Das Surfen im Internet mit mobilen Geräten ist seit Beginn der 2000er Jahre möglich, doch erst mit der Einführung des iPhone® im Jahr 2007 verbreitete sich die Nutzung von Smartphones als vernetzter Computer. NFC wurde 2006 im Nokia® 6131 eingeführt und wird inzwischen von den meisten Geräten unterstützt. Trotzdem hält sich die Anzahl der NFC-basierten Dienste in Grenzen.

Smartphones in der Zutrtittskontrolle – das ist keine neue Idee. Zu Beginn der 2000er Jahre wurde das Konzept bereits für bargeldlose Zahlungen, im öffentlichen Nahverkehr und in der Zutrittskonrolle getestet. Verschiedene Länder haben auch tatsächlich Lösungen für die Öffentlichkeit bereitgestellt. Das Interesse an kontaktlosen Diensten war schon immer groß – allerdings lag die Schwierigkeit darin, die Erwartungen von Anwendern in puncto Benutzerfreundlichkeit und Anwendungsmöglichkeiten zu erfüllen.



Für die mobile Zutrittskontrolle mit unterschiedlichen Technologien wie microSDs, zusätzliche Hüllen, MIFARE® Classic, NFC Peer-to Peer und Bluetooth Classic wurden viele verschiedene Ansätze verwendet, die alle mit besonderen Herausforderungen verbunden waren. Ergebnis der Entwicklung: Eine technologieunabhängige und anpassbare Architektur wie NFC oder Bluetooth Smart ist von zentraler Bedeutung.

Aktuelle Technologien für die mobile Zutrittskontrolle

Das Vertrauen in kontaktlose Anwendungen und Technologien wie NFC, Bluetooth, mobile Geldbörsen, iBeam™ und iBeacon™ wächst zunehmend. Auch die Kenntnis über verfügbare Technologien für die Zutrittskontrolle mit mobilen Geräten steigt stetig. Sicherheitsbeauftragte und IT-Verantwortliche müssen prüfen, welche Technologien in ihrem Fall am besten geeignet sind, um Mitarbeitern und Dienstleistern komfortabel Zutritt zu ihrem Betriebsgelände zu gewähren.

Near Field Communication (NFC)

NFC wurde entwickelt, um einen einheitlichen kontaktlosen Standards zu schaffen. Die Einführung in mobile Geräte verlief jedoch nicht reibungslos. Bis vor kurzem war die Emulation einer kontaktlosen Karte auf einem mobilen Gerät nur über ein Secure Element (SE) wie eine SIM-Karte möglich. Es musste ein System in Form von Trusted Service Managers (TSM) eingerichtet werden, um das SE-zentrische Modell zu unterstützen. Dies führte zu komplexen technischen Integrationen und Geschäftsmodellen, die die Einführung kontaktloser Anwendungen auf NFC-Basis erschwerten.

2013 stellte Google® in Android™ 4.4 eine neue NFC-Funktion vor: „Host-based Card Emulation“ (HCE). Mit HCE kann eine kontaktlose Karte unabhängig von einem SE in einer App emuliert werden. Mit HCE ist es möglich, skalierbare und kosteneffektive NFC-Dienste anzubieten, solange eine standardbasierte Kartentechnologie verwendet wird.

Visa® und MasterCard® haben Spezifikationen wie Transaktionen vom Typ Visa payWave® und MasterCard PayPass™ eingeführt, die HCE verwenden, und HID Global® bietet eine mobile

Zutrittskontrolllösung mit HCE auf Seos-Basis an. Mit HCE wird NFC leichter zugänglich und vielseitiger, so dass Entwickler Dienste für die breite Masse auf den Markt bringen können und so die Verbreitung dieser Technologie fördern werden. Das iPhone allerdings unterstützt keine NFC Anwendungen. Zwar wächst die Anzahl der installierten Android 4.4 Geräte rasch, die fehlende NFC-Unterstützung beim iPhone 4 und iPhone 5, und auch beim iPhone 6 (NFC-Unterstützung gegenwärtig nur für Apple Pay™) bremst die Marktdurchdringung für HCE-basierte Lösungen.

NFC Host Card Emulation

- Standardbasierte kontaktlose Karten können durch eine App emuliert werden
- Funktioniert mit NFC-fähigen Lesegeräten, wenn eine standardbasierte Kartentechnologie verwendet wird
- Ideal für Tap-Funktionalität (kurze Lesereichweite, Antippen des Lesegeräts mit dem Smartphone notwendig)
- Wird vom iPhone nicht unterstützt

Mobile Betriebssysteme mit Unterstützung von NFC Host Card Emulation

- Android 4.4
- BlackBerry® 9 und 10

Bluetooth Smart

Bluetooth Smart wurde 2010 in den Bluetooth-Standard aufgenommen und hält jetzt, nachdem es sich im Gesundheitswesen bewährt hat, seinen Einzug in Zahlungsverkehr und Einzelhandel. Ein wichtiger Faktor für den Erfolg von Bluetooth Smart liegt darin, dass diese Technologie seit dem iPhone 4S auch von Apple unterstützt wird. Google führte Bluetooth Smart mit Android 4.3 ein und so ist Bluetooth Smart seit dem 31. Oktober 2013 die einzige kontaktlose Technologie, die von den beiden großen Betriebssystemen unterstützt wird – Android und iOS. Dank des geringen Stromverbrauchs ist kein Pairing erforderlich. Die große Lesereichweite macht Bluetooth Smart zu einer interessanten Option für die Zutrittskontrolle.

Bluetooth Smart

- Da Bluetooth Smart kein Pairing erfordert und wenig Strom verbraucht, ist es in Kombination mit einer standardbasierten kontaktlosen Kartentechnologie gut für Zutrittsanwendungen mit mobile Geräten geeignet
- Lesegeräte können versteckt oder außer Sichtweite angebracht werden
- Öffnet Türen aus großer Entfernung – ideal in Parkhäusern oder um die Haustür zu öffnen, wenn jemand geklingelt hat
- Konfigurieren von Lesegeräten einschließlich Firmware mit einem Bluetooth Smart-fähigen Gerät (wie ein Smartphone oder Tablet-PC)

Betriebssysteme, die Bluetooth Smart unterstützen

- iOS 7 und 8
- Android 4.4
- BlackBerry 10

- Windows Phone® 8.1

Da sich die Technologie rasant weiterentwickelt, raten wir dazu, den Anbieter der Zutrittskontrollanwendung nach einer Liste unterstützter mobiler Geräte zu fragen.

Benutzerfreundlichkeit in der Anwendung

Wir haben unser Telefon stets griffbereit und verlieren es höchst selten: Smartphones zählen heute zu den beliebtesten Technologiegeräten. Die Nutzung von mobilen Geräten in der Zutrittskontrolle ist daher nur folgerichtig, denn sie ist nicht nur bequem, sondern auch hoch sicher. Die große Lesereichweite mit Bluetooth Smart eröffnet ganz neue Möglichkeiten zum Öffnen von Türen und Anbringen von Lesegeräten. Für den schnellen und reibungslosen Zutritt zum Gebäude kann man eine Tür schon entriegeln während man auf sie zuläuft. Bluetooth Smart-fähige Lesegeräte sind in Parkhäusern sehr beliebt. Anstatt das Fenster herunterzukurbeln und genau im richtigen Abstand an der Parksäule anzuhalten um die Karte am Lesegerät zu präsentieren, öffnet sich jetzt einfach die Schranke, wenn man auf sie zufährt. Für manche Türen, beispielsweise in Bereichen mit Konferenzräumen und mehreren Lesegeräten dicht beieinander, könnte eine geringere Reichweite und das Antippen der Geräte mit einer Karte besser geeignet sein, damit sich auch nur die gewünschte Tür öffnet.

Mit den neuen Möglichkeiten ist der Kreativität von Architekten keine Grenze mehr gesetzt: Die Platzierung der Lesegeräte kann ganz neu geplant werden, beispielsweise für Büroräume mit Glastüren oder -wänden. Außerhalb angebrachte Lesegeräte können außerdem Ziel von Vandalismus werden. Die größere Lesereichweite von Bluetooth Smart mit einer Richtantenne schafft also nicht nur gestalterischen Freiraum, sondern verbessert zusätzlich die Sicherheit, indem Lesegeräte an der Tür-Innenseite und außer Sichtweite angebracht werden.

Die Lesereichweite unterliegt naturbedingt äußeren Einflüssen. In einem Aufzug kann sie durch die umgebende Metallkonstruktion wesentlich größer sein. Auch der Typ des verwendeten Smartphones kann die Lesereichweite beeinflussen. Für eine gut durchdachte mobile Zutrittskontrolllösung ist es wichtig, dass die Lesegeräte geeignet konfiguriert werden können (Öffnen aus der Entfernung oder mit Tap-Funktion) und eine Feinanpassung der optimalen Lesereichweite möglich ist.

Der Eindruck der Nutzer ist bei der Einführung neuer Lösungen enorm wichtig. Der erste Eindruck ist entscheidend und eine neue Lösung wird schnell abgelehnt, wenn sie den Erwartungen der Anwender nicht gerecht wird. Das Öffnen von Türen muss unkompliziert, intuitiv und bequem erfolgen – alles in einem Schritt. Verlang man von Anwendern, dass diese erst ihr Gerät entriegeln, dann eine App starten, schließlich eine Mobile ID auswählen und letzlich ihr Gerät am Lesegerät vorzeigen müssen, werden sie vermutlich ihre alten Ausweiskarten vorziehen. Wichtig ist auch, dass der Nutzer denselben reibungslosen Ablauf auf unterschiedlichen Mobilplattformen erlebt. Eventuelle Unterschiede in der Anwendung von Android und iOS wirken auf Mitarbeiter verwirrend, der Schulungsaufwand wird erhöht und die Support-Fälle häufen sich.

Auswirkungen auf die Verwaltung

Die Verwaltung von Ausweiskarten kann zeitaufwendig sein. Das Verwaltungspersonal an Universitäten und Hochschulen kennt die Probleme, wenn zu Beginn des Semesters Tausende von Studenten innerhalb kurzer Zeit ihre Ausweise abholen möchten. Bestellung, Druck, Ausgabe und die Erstellung von Ersatzkarten nach Verlust nehmen wertvolle Zeit in Anspruch – sowohl für das Sicherheitspersonal als auch für Mitarbeiter und Studenten.

Die Zutrittskontrolle mit Smartphones birgt nicht nur Vorteile in puncto Benutzerfreundlichkeit: Mobile Geräte bringen neue Möglichkeiten für die echtzeit-Verwaltung von mobilen Identitäten. Ein

cloud-basiertes Portal für eine zentrale Identititätsverwaltung erspart dem Personal viel Zeit, die heute mit der Verwaltung von Ausweiskarten verbracht wird.

Die Effizienz von Sicherheitsverantwortlichen steigt deutlich, wenn die mobilen Identitäten von Mitarbeitern oder Studenten über ein zentrales System verwaltet werden. Ein wichtiger Aspekt bei der Implementierung von Zutrittskontrollsystemen mit Smartphones ist der Aufnahmeprozess neuer Mitarbeiter in das System sowie die Ausgabe der mobilen ID. Das Hinzufügen von Name und E-Mail Adresse des Nutzers reicht schon aus: Er erhält sofort automatisch eine E-Mail mit Installationsanweisungen für die App. Sobald die App installiert und konfiguriert ist, wird die korrekte mobile Identität auf dem mobilen Gerät bereitgestellt und der Systemadministrator wird über die erfolgreiche Installation informiert. Bei großen Unternehmen erfolgt das Hochladen vieler Nutzerdaten über einen Massen-Upload in einer Datei. Die verwendete Plattform für diese mobilen Identitäten muss alle Daten validieren und für jeden einzelnen Nutzer den gesamten Prozess durchgehen (Senden der E-Mail, Ausgabe der mobilen Identität und Benachrichtigung des Sicherheitsadministrators über die erfolgreiche Ausgabe eines digitalen Schlüssels).

Vereinfachter Ausgabeprozess

Mobile Identitäten müssen einzigartig sein und sollten automatisch für die individuellen Anwendungen im Unternehmen konfiguriert werden. Die Ausgabe einer mobilen Identität an einen Mitarbeiter oder Studenten sollte lediglich erfordern, dass man den Nutzer und die korrekte mobile Identität auswählt. Die manuelle Eingabe von Nummern für Zutrittskontrollsysteme und Codes für Einrichtungen ist so fehleranfällig und zeitaufwendig, dass wir davon abraten.

Viele Unternehmen haben Zweigstellen und Büros mit unterschiedlichen Zutrittskontrollsystemen und -technologien in verschiedenen Teilen der Welt. Mitarbeiter benötigen für den Zutritt zu einer anderen Zweigstelle häufig einen Besucherausweis. Mit einer Zutrittskontrolllösung, die mobile Geräte unterstützt, können glelichzeitig mehrere digitale Identitäten auf demselben Gerät gespeichert werden. So kann man dem Mitarbeiter vor dem Verlassen seines Büros oder bei Ankunft am besuchten Büro eine zusätzliche mobile Identität zuschicken. Da private iPads® und Tablets immer häufiger am Arbeitsplatz genutzt werden, wird die Anbindung von Mitarbeitern mit unterschiedlichen mobilen Geräten zu einem weiteren wichtigen Aspekt.

Wir erleben derzeit einen klaren Trend hin zur Nutzung von mobilen Geräten als Authentifizierungsmittel für den Zugang zu Daten oder für die Anmeldung zu online Diensten. Viele Unternehmen haben die Vorteile erkannt, wenn Zutritt und Datenzugang miteinander verschmelzen: Die Kombination beider Systeme spart Kosten und erhöht die Sicherheit deutlich. Denn eine gemeinsame Plattform für digitale Identitäten erleichtert Sicherheitsadministratoren die Verwaltung von Zutritts- und Zugriffsrechten und Mitarbeitern die Authentifizierung an verschiedenen Diensten.Ein Sicherheitsadministrator kann Identitäten nach Bedarf an einen einzelnen Mitarbeiter oder eine Mitarbeitergruppe versenden. Diese Identitäten können dann für

den Zugang zu Diensten wie VPN und E-Mail mit starker Authentifizierung verwendet werden, wobei die gesamte Verwaltung auf derselben mobilen Identitätsplattform erfolgt.

Bewertung der Sicherheit

Angriffe können aus vielen Richtungen kommen und sich zahlreicher Mittel bedienen. Um alle Verbindungen innerhalb einer mobilen Zutrittslösung zu schützen und sicherzustellen, dass es zwischen Lesegeräten, mobilen Geräten und Backend-Sicherheitssystemen keine einzige Schwachstelle gibt, ist ein mehrschichtiges Sicherheitsmodell erforderlich. Sollte es Eindringlingen doch einmal gelingen, eine Sicherheitsebene zu durchbrechen, bleiben die Türen dahinter weiterhin geschlossen.

Die Verwaltung digitaler Schlüssel auf mobilen Geräten erfordert eine ganzheitliche Sicht auf die End-to-End-Sicherheit: Wie werden die digitalen Schlüssel erstellt? Wie werden sie über ihre gesamte Lebensdauer hinweg verwaltet und wie werden sie in Mobiltelefonen gespeichert? Die Sicherheit muss an erster Stelle stehen. Mobile Identitäten und Benutzerdaten sollten in einem sicheren Tresor mit Hardware-Sicherheitsmodulen geschützt werden, in denen alle Verschlüsselungscodes gespeichert und für kryptographischen Operationen verwendet werden.

Moderne Smartphone-Betriebssysteme wie Android und iOS verfügen über ein hohes Sicherheitsniveau. Eine App für den mobilen Zutritt sollte so erstellt werden, das sie diese Sicherheitsfunktionen voll ausschöpft. Die App sollte separat laufen, damit keine anderen Apps auf ihre Daten zugreifen oder diese modifizieren können. Sensible Daten und Schlüssel müssen durch ein Device Keychain geschützt werden – einen Bereich auf mobilen Geräten, in dem sensible Daten gespeichert werden. Zusätzlich zur Sicherheit des mobilen Betriebssystems müssen mobile Identitäten signiert und verschlüsselt werden, um Manipulationen auszuschließen.

Wie bei Karten wird die endgültige Entscheidung, wer das Gebäude betreten darf, durch das örtliche Zutrittskontrollsystem getroffen. Wenn ein mobiles Gerät verloren geht, gestohlen oder kompromittiert wird, können die Zutrittsberechtigungen für das entsprechende digitale Credential im Zutrittskontrollsystem gesperrt werden, um unerwünschten Zutritt zu verhindern. Im seltenen Fall eines kompromittierten mobilen Gerätes muss sich der Angriff auf die im Gerät installierten mobilen Identitäten begrenzen lassen, da jeder digitale Schlüssel nur einmal vorhanden sein soll. Außerdem wird ein Mitarbeiter den Verlust eines mobilen Gerätes viel eher bemerken als eine verlorene Ausweiskarte.

Mobile Geräte haben gegenüber Karten auch den Vorteil, dass sie online sind. Wenn der Sicherheitsadministrator einen digitalen Schlüssel von einem Gerät entfernen will, kann der digitale Ausweis kabellos storniert werden, solange das Gerät mit dem Wireless-Netzwerk verbunden ist. Wenn ein Mitarbeiter den Verlust eines Gerätes meldet, können die mobilen Identitäten annulliert werden, bevor das Gerät in falsche Hände gelangt.

Um die Folgen eines Diebstahls weiter zu entschärfen, können mobile Identitäten so konfiguriert werden, dass sie nur dann mit Lesegeräten zusammenarbeiten, wenn das mobile Gerät entsperrt ist. Das bedeutet, dass ein unberechtigter Nutzer zusätzlich die Geräte-PIN, Gesichtserkennung oder Fingerabdrucksicherung umgehen müsste, um sich mit dem Gerät Zutritt zu verschaffen.

Die Implementierung von mobiler Zutrittskontrolle

Bei der Implementierung von mobiler Zutrittskontrolle müssen mehrere Faktoren betrachtet werden, bevor man sich für ein bestimmtes Lesegerät entscheidet. Der Bestand an verwendeten mobilen Geräten kann die Wahl der Technologie beeinflussen, da iPhones 5s und früher NFC nicht unterstützen. In Unternehmen mit einem großen Bestand an iPhones stellt Bluetooth Smart die einzige Möglichkeit dar. Man sollte auch erwägen, welche Türen mit mobilen Geräten geöffnet werden sollen. Für Parkhäuser, Haupteingangstüren und Aufzüge ist eine größere Lesereichweite

vorteilhaft, da sie für die Mitarbeiter komfortabel ist. Wenn viele Lesegeräte auf engem Raum installiert sind, kann mit der Tap-Funktion verhindert werden, dass die falsche Tür geöffnet wird. Tap kann sowohl von NFC- als auch Bluetooth Smart-fähigen Lesegeräten unterstützt werden.

Viele Unternehmen verwenden eine MDM-Plattform (Mobile Device Management), auf der unternehmensspezifische Apps herausgegeben werden, die auf dem mobilen Gerät in einem separaten Container laufen. Für Interoperabilität der mobilen Zutrittslösung mit der MDM-Plattform zu sorgen, ist besonders dann sinnvoll, wenn die MDM-Plattform Sicherheitseinstellungen steuert.

Es sollte auch in Betracht gezogen werden, bestehende Kartenbestände und Lesegeräte weiter zu nutzen. Auch wenn die mobile Zutrittskontrolle den Komfort erhöht, kann es für manche Unternehmen sinnvoll sein, wenn die Mitarbeiter ihre Ausweiskarten als Backup behalten solange die Migration zu mehr Sicherheit und Mobilität noch nicht abgeschlossen ist.

Zusammenfassung

Unternehmen kombinieren Sicherheit und Benutzerfreundlichkeit an der Tür durch die Möglichkeit, Smartphones und andere mobile Geräte als zuverlässige und einfach zu verwendende digitale Identifikationsmittel einzusetzen und damit Schlüssel und Smartcards zu ersetzen. Bei der Auswahl einer mobilen Zutrittslösung gilt es jedoch einiges zu beachten. Um sicher zu sein, dass die Lösung mit den neuesten Smartphone-Technologien funktioniert und mit der Entwicklung der Telekommunikationsbranche Schritt halten kann, sollte sie auf einer standardbasierten Kartentechnologie beruhen, die auf zahlreichen Mobiltelefonen, Tablets und Wearables emuliert werden kann. Damit die Lösung von Mitarbeitern und Studenten akzeptiert wird, muss sie ebenso benutzerfreundlich sein wie die gewohnten Karten.

Der erste Eindruck ist entscheidend. Das Öffnen von Türen muss unkompliziert, intuitiv und komfortabel vor sich gehen, ohne dass der Nutzer viele verschiedene Schritte ausführen muss. Ein interessanter Faktor des Zutritts mit mobile Geräten besteht in der Möglichkeit, mobile Identitäten echtzeitnah ausgeben und annullieren zu können. Außerdem muss bei der Gestaltung der mobilen Identitätsplattform an eine benutzerfreundliche und effiziente Verwaltung gedacht werden. Die mobile Zutrittskontrolle weist neue Wege zum Öffnen von Türen sowie für die Interaktion mit unserer Umgebung und liefert bei korrekter Implementierung zukunftsfähige Lösungen.

2014-11-24-hid-mobile-access-best-practices-wp-de PLT-02173