BlueID – das Smartphone

Die in Deutschland entwickelte BlueID-Technologie erlaubt die Integration von physischer Zugangsfunktion in beliebige Smartphone-Apps. ELV-Kunden genießen durch BlueID die exklusive Möglichkeit, ihre Wohnungstür zum Öffnen mit dem Smartphone einfach aufzurüsten.

Bild 1: Jede App kann durch das BlueID Software Development Kit (SDK) zum Steuern von Objekten mit dem Smartphone ausgerüstet werden.

als Schlüssel

Smartphones halten in großer Geschwindigkeit Einzug in unseren Alltag. Wer sich einmal an die Vielseitigkeit seines iPhones, BlackBerrys oder Android-Gerätes mit all seinen Apps gewöhnt hat, der möchte es nicht mehr missen. Kontinuierlich steigt die Funktionsvielfalt der Geräte: Wir können mit dem Telefon unsere E-Mails komfortabel abrufen, im Auto wird das Smartphone zum Navigationsgerät, und Anwendungen wie Mobile Banking sind mit den entsprechenden Apps ebenfalls möglich. Das Smartphone wird in unserem Alltag immer wertvoller und immer weniger gerne geben wir es aus der Hand – denn das Handy ist ein verhältnismäßig kleines, aber immens schlagkräftiges Werkzeug. Dieser Trend wird sich in Zukunft noch weiter verstärken.

BlueID-Technologie

Die BlueID-Technologie ist eine von baimos technologies in Deutschland entwickelte Technologie, die das Smartphone wortwörtlich zum Schlüssel macht. BlueID kann von App-Entwicklern in beliebige Apps integriert werden und erlaubt eine sichere Steuerung beliebiger physischer Objekte mit dem Smartphone (Bild 1). In der Praxis bedeutet dies, dass Zugangssystemanbieter durch ein Software Development Kit, das BlueID SDK, ihre Zugangssysteme zum Öffnen per Smartphone-App aufrüsten können. Parkraummanagement-Anbieter nutzen BlueID zum Öffnen von Parkschranken per Smartphone und Carsharing-Anbieter können durch BlueID sogar Autos per App öffnen und starten.

BlueID bietet den Vorteil, Zugangsberechtigungen sehr schnell über das Mobilfunknetz an Smartphones ausrollen zu können, genauso schnell können die ausgerollten digitalen Schlüssel auch wieder zurückgezogen werden. Das spart großen Unternehmen und Betreibern von Mobility Services jedes Jahr beträchtliche Summen beim Verwalten ihrer Zugangssysteme – denn alle Berechtigungen werden nur mehr digital ausgegeben und zurückgenommen. Gleichzeitig können die im Einsatz befindlichen Smartphone-Apps jederzeit einfach upgedated und mit neuen Features erweitert werden. Die Zugangsfunktionalität, welche einfach über die sogenannte BlueID Library in der App integriert ist, bleibt dabei unverändert und funktioniert zuverlässig.

Genauso einfach verhält es sich mit den Funktechnologien, die von BlueID unterstützt werden. Das mit zertifikatsbasierter Verschlüsselung gesicherte BlueID-Protokoll funktioniert einfach unabhängig vom Datenkanal. Es ist egal, ob das Kommando zum Öffnen einer Tür vom Smartphone per NFC, Bluetooth 4.0 Low Energy, Wi-Fi oder sogar weltweit über die mobile Internetverbindung des Smartphones gesendet wird. BlueID ist schnell in die App integriert und bietet durch seine Protokollunabhängigkeit auch Unterstützung für zukünftige Funktechnologien.

Im Bereich der Mobile Parking Apps nutzt zum Beispiel das international sehr bekannte Pango-Parksystem (www.mypango.com) die BlueID-Technologie, und führende europäische Carsharing-Anbieter setzen BlueID zum Öffnen ihrer Fahrzeuge ein (Bild 2).

Bild 2: Carsharing-Autos öffnen und starten per Smartphone-App – BlueID macht's möglich.

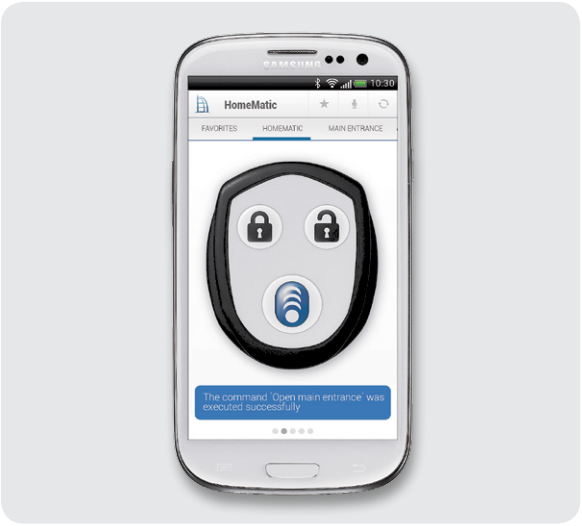

Bild 3: BlueID Access for HomeMatic erlaubt das Öffnen der Wohnungstür per App.

Beim Öffnen von Wohnungs- und Haustüren (Bild 3) haben die Kunden von ELV die Nase vorn: Auch sie haben die Möglichkeit, im privaten Bereich oder auch in kleinen Büros (Bild 4) kostengünstig Türen selbst zum Öffnen mit dem Smartphone auszurüsten. Das mächtige BlueID-Berechtigungsmanagement zum Verwalten der Berechtigungen ist dabei genau das Gleiche wie das im großen Stil von Betreiberunternehmen eingesetzte System. ELV-Kunden profitieren so von professionellem Berechtigungsmanagement zu einem Preis, der auch im Heimbereich leistbar ist.

Digitaler Schlüssel – Funktion und Sicherheit

Die Funktionsweise der digitalen Schlüsselvergabe und die Nutzung der digitalen Schlüssel lässt sich am besten anhand einer grafischen Darstellung erklären. In der Grafik (Bild 5) links oben ist der BlueID Ticket Manager zu sehen, welcher als Schnittstelle zur digitalen Schlüsselerstellung fungiert. Ein autorisierter Administrator, also zum Beispiel der Besitzer oder Mieter einer Wohnung, kann mithilfe des BlueID Ticket Managers über ein Webinterface auf das BlueID Trust Center zugreifen. Dieses ist die digitale Schlüsselfräse – unter der Verwendung von Zertifikaten werden die digitalen Schlüssel, sogenannte BlueID-Tickets, generiert. Jeder Schlüssel besitzt bestimmte Parameter: Er kann nur von einem bestimmten Benutzer unter Einsatz seines persönlichen Smartphones genutzt werden, um in einem exakt definierten Zeitraum ein bestimmtes gesichertes Objekt zu öffnen. Bei BlueID Access for HomeMatic, dem Smartphone-Zugang für das HomeMatic-System, sind gesicherte Objekte immer einzelne Türen wie Wohnungs- oder Bürotüren.

Der Zugriff des Administrators auf das Trust Center erfolgt über eine geschützte Verbindung mit SSL-Verschlüsselung. Das BlueID Trust Center selbst, als Kernstück der Technologie, wird in einem nach ISO/IEC 27001:2005 zertifizierten, bankensicheren Rechenzentrum in Deutschland betrieben. Die digitalen Schlüssel, also die Zugangsberechtigungen zu einzelnen Türen, werden mithilfe eines RSA/AES-verschlüsselten Kanals über die mobile Internetverbindung an das Smartphone des Zutrittsberechtigten übertragen. Der Nutzer lädt, bevor er seinen ersten digitalen Schlüssel empfängt, die App „BlueID – your digital key" auf sein Smartphone, damit das Telefon die verschlüsselten BlueID-Tickets empfangen und zum Öffnen von Türen nutzen kann.

Die App selbst kann eine beliebige Zahl an Zugangsberechtigungen in verschlüsselter Form tragen. Der digitale Schlüsselbund wird an die Hardwareeigenschaften des Smartphones gebunden und erfüllt durch seine Verschlüsselung nach Standardverfahren mit bis zu 4096 Bit Sicherheitsanforderungen, welche die herkömmlicher Identifikationsmedien wie Schlüssel oder Zugangskarten bei Weitem übertreffen.

An der Tür

Möchte der Benutzer nun mit seinem Smartphone das Öffnen oder Schließen einer Tür auslösen, so verwendet er dazu die App auf seinem Smartphone. Durch das Drücken eines Buttons in der App wird der Öffnungs- oder Schließvorgang ausgelöst. Die Kommuni-

Bild 4: Bürotüren öffnen sich dank BlueID Access for HomeMatic per Knopfdruck auf dem Smartphone.

Zusatzinfo

So rüsten Sie Ihre Wohnungstür zum Öffnen mit dem Smartphone auf

Der ELV-Versand bietet Ihnen die Möglichkeit, dass auch Sie die BlueID-Technologie nutzen können. Mit dem BlueID-Access-for-HomeMatic-Software-Upgrade können Sie Ihre Wohnungstür zum Öffnen mit dem Smartphone aufrüsten. Sie können die Berechtigung zum Öffnen auch flexibel und mit zeitlichen Beschränkungen an mehrere Smartphones ausrollen. So kann die ganze Familie die Haustür öffnen. Auch Angestellte in einem kleinen Büro erhalten so flexibel und einfach Zugang zu den Büroräumen. Dazu benötigen Sie folgende Komponenten: Eine HomeMatic-Zentrale CCU, den Schlüsselmotor KeyMatic sowie das BlueID-Access-for-HomeMatic-Software-Upgrade.
Die Komponenten sind online bestellbar unter: www.elv.de

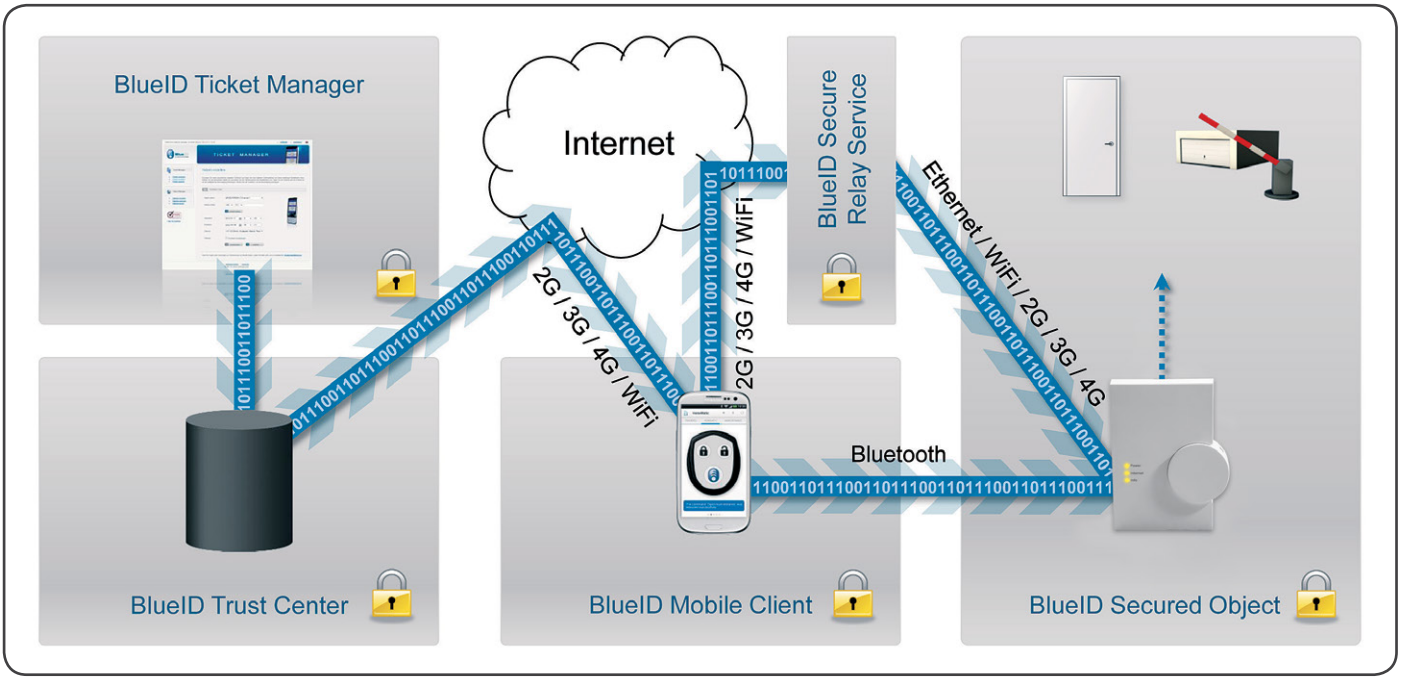

Bild 5: BlueID: Funktionsweise des digitalen Schlüssels auf dem Smartphone

kation des Smartphones mit dem digitalen BlueID-Sicherheitsmodul in der HomeMatic CCU (Bild 6) wird über zwei verschiedene Wege realisiert. Entweder das Smartphone kommuniziert zum Beispiel über Bluetooth direkt mit dem gesicherten Objekt oder indirekt über eine 2G/3G/4G/Wi-Fi-Datenverbindung. In beiden Fällen erfolgt die Berechtigungsübertragung RSA/AES-verschlüsselt, beim Senden des digitalen Schlüssels über das Internet wird auf einen Secure-Relay-Service zurückgegriffen.

Das digitale BlueID-Sicherheitsmodul in der HomeMatic CCU überprüft selbstständig die Gültigkeit und Authentizität des vom Smartphone empfangenen Schlüssels. Bei positiver Prüfung öffnet das Sicherheitsmodul mithilfe eines KeyMatic-Schlüsselmotors dann die Tür. Jeder Zugriff wird zudem protokolliert und kann vom Administrator eingesehen werden. Gerade in Situationen, in denen man zum Beispiel Nachbarn während des Urlaubs zum Blumengießen temporär einen digitalen Schlüssel zum Öffnen der Tür mit dem Smartphone ausstellt, kann dies von Nutzen sein. ELV

Zusatzinfo

Was passiert, wenn ich mein Smartphone verliere?
Im Gegensatz zum Verlust von Wohnungsschlüsseln können die digitalen Schlüssel auf dem Smartphone jederzeit in Sekundenschnelle per Webinterface im BlueID Trust Center gesperrt werden. Das gibt das beruhigende Gefühl der Sicherheit, nie wieder wegen verlorener Schlüssel ein Schloss tauschen zu müssen.

Bild 6: Das Smartphone steuert die HomeMatic-Zentrale mit BlueID.

Autor: David Schmidl
Alle Bilder: baimos technologies gmbh

Weitere Infos

Link zur BlueID-Technologie:
http://oem.BlueID.de