BUSINESS UPDATE

REVOLUTIONIZING PHYSICAL IDENTITY AND ACCESS MANAGEMENT

Patrick Wimmer, Joey Yanire and Carl Fenger, at LEGIC Identsystems, explain how smartphone wallets can unlock new potential in access management

In today's digital landscape, smartphones have evolved into essential multifunctional tools, serving as central hubs for everyday tasks such as payment, identification, health monitoring and communication. The integration of access management with smartphones represents a pioneering breakthrough in the realm of physical identity and access management (PIAM), transcending the constraints associated with conventional mechanical keys and plastic keycards, which are frequently lost, misplaced, forgotten, copied or stolen.

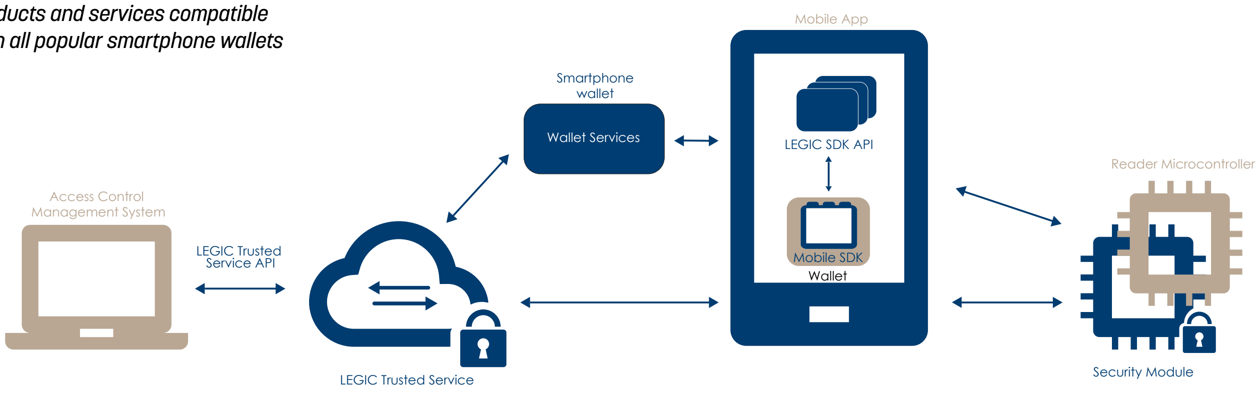
Here are two compelling approaches to achieve PIAM integration:

1. **Wallet integration:** by seamlessly merging the LEGIC Connect trusted service with popular digital wallets, your smartphone wallet can now assume the role of a universal key for your office, home, hotel room and much more. Initially designed for storing digital credit, debit and loyalty cards, smartphone wallets have expanded their functionality to encompass transit passes, ID cards, employee badges and now hotel room keys and office/ residential door access

2. **Dedicated app:** utilizing the LEGIC Security Platform and mobile software development kit (SDK), building operators and hospitality service providers can create their own branded apps for access control, along with in-house payment solutions for vending machines, restaurants, parking facilities, EV charging stations and other amenities within their company, campus or hotel. These apps can be tailored to specific use cases, combining as well as bundling access with multiple adjunct services to enhance the user experience

LEGIC can help make your Physical Identity and Access Management products and services compatible with all popular smartphone wallets

LEGIC "Wallet Program"



The key advantage of smartphone wallets is their status as a native application integrated into the pre-installed mobile operating system. This ensures automatic maintenance and updates by the mobile OS provider, streamlining setup and the addition of room, office and home keys with just a few simple steps. This frees the service provider from having to create, maintain, update and deploy a dedicated app.

Providing a keycard-like experience

Based on NFC access, smartphone wallets deliver a convenient user experience akin to using a traditional smartcard – they can function without the need to unlock the phone or establish a network connection. Users can simply present their locked phone to a reader terminal, eliminating the hassle of finding and launching an app that requires both hands – a significant improvement over dedicated applications.

Furthermore, users can enhance security by activating biometric verification such as facial recognition within their wallet. Additionally, digital wallets function as a centralized repository for multiple virtual cards and keys, simplifying their use across a variety of applications provided by multiple unrelated service providers.

Low battery operation adds safety and peace of mind

Digital wallets can operate even when the smartphone's battery is critically low, unlike dedicated apps that cease to function. This feature is particularly valuable for access control scenarios where the ability to enter an office, hotel room or residence when the phone battery appears dead provides both convenience and peace of mind.

> "DIGITAL WALLETS CAN OPERATE EVEN WHEN THE SMARTPHONE'S BATTERY IS CRITICALLY LOW."

Integrate mobile wallet access with the LEGIC Security Platform

As part of the LEGIC Security Platform dedicated to supporting secure mobile services, LEGIC Connect comprises an OWASP-ASVS audited Trusted Service hosted on AWS, a Mobile SDK plus LEGIC Security Modules which include an RF transceiver (Bluetooth, NFC, RFID) and tamper-proof Secure Element (SM-6300 and the programmable SM-6310). These modules are embedded in infrastructure-devices such as electronic locks, mobility vehicles or IoT sensors.

Together, these components establish a cryptographically secure, bidirectional channel from backend administration system, to smartphone app or wallet, to infrastructure. In addition to credentials, any data needing secure distribution to end devices such as firmware, cryptographic keys, whitelists or certificates can be transported via LEGIC Connect.

The LEGIC Wallet Program

For comprehensive information on how to make your LEGIC-based products and services compatible with smartphone wallets, please visit the Wallet Program webpage: www.legic.com/wallet.

Discover how to elevate your PIAM systems by embracing wallet integration on the LEGIC Security Platform and propel your access control products and services into a new realm of security, efficiency and user satisfaction.

Visit LEGIC at ISC East, 15-16 Nov. 2023 at the Jarvis Center in NYC, Booth 847.

About LEGIC Identsystems

For over 30 years, Swiss-based LEGIC Identsystems has enabled companies from around the world to deploy solutions with demanding security requirements. Based on key management, trusted services and secure, contactless semiconductors, the LEGIC Security Platform provides end-to-end security for smartphone and smartcard-based access, mobility, shared resource and industrial IoT applications. www.legic.com