INDUSTRY EXPERT

THE COMING OF AGE FOR MOBILE CREDENTIALS

People everywhere are increasingly using their smartphones to interact with the world, writes Carl Fenger, Technical Communications Manager, LEGIC Identsystems

Tasks such as opening doors, buying tickets, sharing or charging vehicles are convenient, easy and secure to do with your smartphone.

At the core of these many possibilities is the secure provisioning of mobile credentials – user specific digital information that is distributed to mobile devices over-the-air. Mobile credentials give end users permission to access, use, rent, purchase, control or monitor things based on a user's rights, time, place or any other information that is relevant to each service. Here are some examples of how mobile credentials are used.

eCharging

The electric car market in Europe will grow from 2.9 million vehicles in 2023 to over 5.5 million vehicles in 2027 (Statista). To service this expanding market, eCharging stations will experience even faster growth, reaching 56 billion dollars by 2029, an impressive CAGR of over 30% during 2022-29 (Businesswire).

To facilitate this market, eCharging stations are leveraging smartphone apps and mobile credentials to support customer authentication, secure ePayment and bi-directional communication with the service provider's cloud. They also foster customer loyalty by sharing mobile credentials with complementary services to apply discounts to eParking, mobility rental services, public transport, car wash, food and drink, etc. In this way, eCharging stations can deliver attractive service bundles that are all accessed via a single Android/iOS mobile app.

Industrial IoT

The viability of the advances within the "Industrial Internet of Things" strongly depends on a common denominator: Trust. If users, IoT sensors and their interactions cannot be trusted, the results can be costly, especially where valuable assets and human safety are involved.

The integration of mobile credentials combined with a smartphone's built-in biometric verification capabilities is a quick and easy way to establish trust in an Industrial IoT environment. This can effectively restrict access to industrial sensors, containers, machines and physical areas to authorised personnel only. Similarly, IIoT sensors can be configured with their own encrypted credential embedded in a Secure Element (SE) which uniquely identifies them to the host system; this prohibits malicious manipulation of sensor data or sensor spoofing.

When IoT users, sensor data and infrastructure can be trusted, then interactions can be monitored and audited. This is especially relevant for industrial processes and supply chains where goods, multiple parties and liability are involved.

Access control

Perhaps the most widely deployed example of mobile credentialing is in the access control markets. This is essentially the ability to open doors, lockers, vehicles, etc. using a smartphone app. By leveraging a smartphone's facial or fingerprint recognition capabilities with a unique mobile credential for each user, a wide range of options can be implemented. This includes amongst others time limited or temporary access for shared resources like vehicles, hotel rooms, trunk deliveries etc. with real time provisioning of access rights in all these scenarios.

Mobile access is an easy extension of all existing smartcard (badge)-based solutions. Here, mobile credentials can be sold just like a smartcard is sold today. This gives vendors of card-based access control systems the choice to easily add mobile credentialing in addition to, or as a replacement for, their smartcard-based systems based on the same business model as smartcards.

> "MOBILE CREDENTIALS NEED TO BE EASILY AND SECURELY PROVISIONED."

Integration with digital wallets

Major smartphone vendors are integrating mobile credentials into the digital wallets of both iOS and Android devices. This provides users with a trusted, passwordless digital identity that can be used for virtually any service that requires reliable verification of users and customers. This makes it easy to prove we are who we claim to be and access rights and services to which we are entitled, both online and in the physical world.

Examples include opening a bank account, storing of a digital driver's license, passport, loyalty cards or vaccination record, renting a car, opening and starting a vehicle, entering residential and office buildings, buying a coffee or a train ticket, etc., all aggregated onto a single digital wallet app.

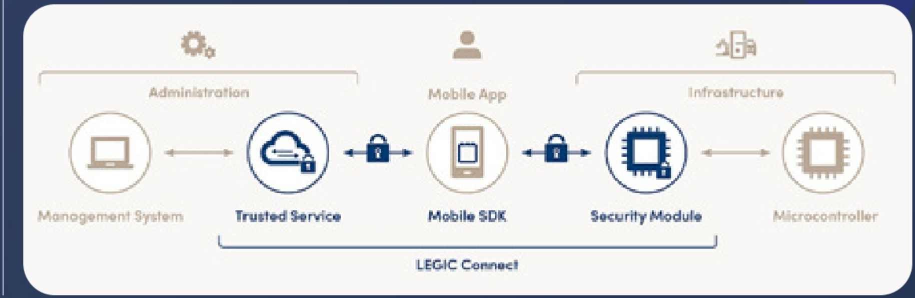
LEGIC Connect

Mobile credentials need to be easily and securely provisioned to users anytime and anywhere. LEGIC Connect offers exactly this and now provides end-to-end mobile credentialing services to over 14 million end users in over 200 countries and territories.. Provided as a trusted, cloud-based Software as a Service (SaaS), LEGIC Connect creates and securely deploys mobile credentials to Android and iOS smartphones anytime and anywhere in the world.

Users include large companies, international hotel chains, large campuses, governments and system integrators who leverage mobile credentials to create useful mobile-based products and services. LEGIC Connect comprises an OWASP-ASVS audited Trusted Service hosted on AWS, a Mobile SDK to jump-start development of branded mobile apps plus LEGIC Security Modules which include an RF transceiver and tamper-proof Secure Element (SM-6300, SM-6310). These modules are then embedded in infrastructure-devices such as electronic locks, eCharging stations or IoT sensors.

Together, these components establish a cryptographically secure, bidirectional channel from backend administration system to smartphone 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.

To find out more, visit: www.legic.com/connect ■


Administration
Mobile App
Infrastructure
Management System
Trusted Service
Mobile SDK
Security Module
Microcontroller
LEGIC Connect