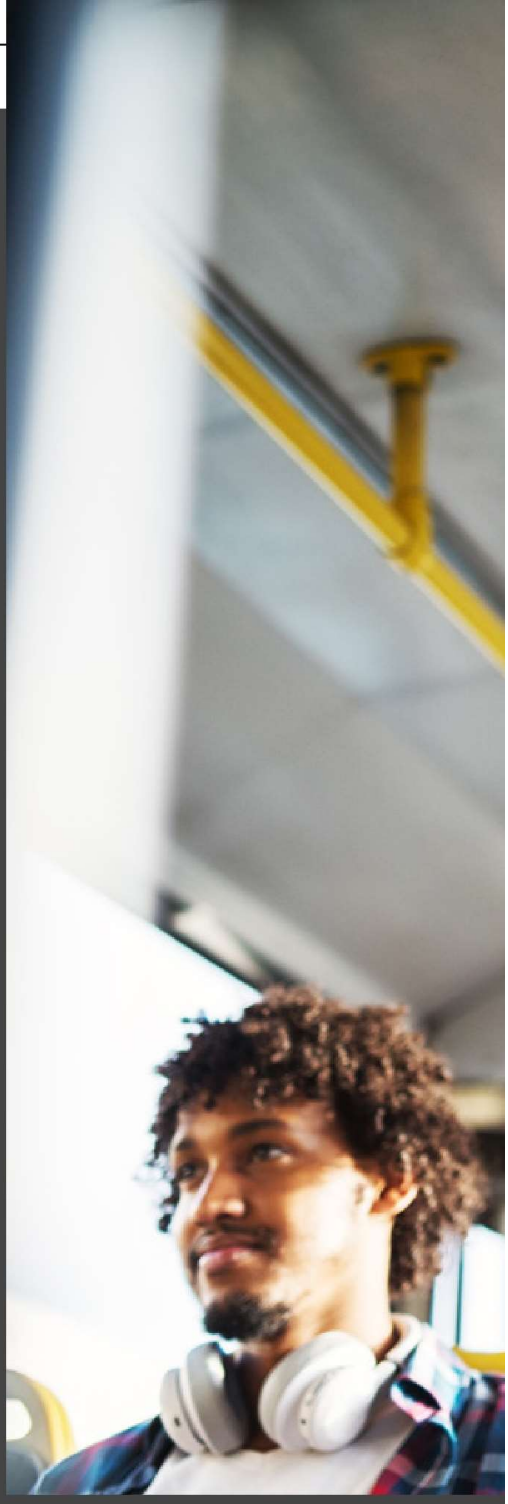
KNOWLEDGE PARTNER

THE EXCITING (NEAR) FUTURE OF MOBILE CREDENTIALS



Carl Fenger and Goran Stevanovic of LEGIC Identsystems investigate what happens when your smartphone knows what you want

Although mobile credentials as a concept is not well known, people use them on almost a daily basis. When opening your office door using your smartphone or entering a concert venue using a mobile e-ticket, you are presenting information relevant to you that is stored on your mobile device to gain access to areas that you are authorised to enter.

The infrastructure grants you rights based on digital information, or mobile credentials, stored on your mobile device such as smartphone or tablet.

Mobile credentials enable mobile devices to become a form of 'digital twin' that can store and selectively share data such as your identity, authorisations, preferences, credit card numbers, clothing size, shopping and location history etc. with any type of infrastructure, be it doors, public transportation, vehicles, shops, vending machines, parking garages, hotels and even your own living room. Mobile credentials are typically encrypted and can be as simple or content rich as an application requires.

When combined with metadata such as your location, time of day, weather, vicinity of friends and family, your personal calendar, applications that share mobile credentials with infrastructure make a great leap towards making your surrounding world more friendly, informative, customised and convenient.

Enabling powerful new apps

Three technologies are currently converging to enable a variety of service possibilities that will soon be commonplace.

By leveraging mobile credentials with Ultra-Wideband (UWB) indoor positioning (a rapidly growing short-range radio technology that can identify your precise location even inside buildings) and Bluetooth advertising (the ability for any device within Bluetooth range to broadcast their availability, even while "asleep"), the connection between who you are, where

you are, and what's available around you is made. This can be illustrated in a variety of use cases:

Access control and indoor navigation

Guiding people as well as machines to their destination indoors as well as outside is the next evolutionary step for access control. Add in the growing demand for touchless entry due to COVID-19, the scenario already made famous by Star Trek over 50 years ago, is finally becoming reality: Doors that automatically open when authorised persons approach.

Due to the ability of UWB to recognise exactly where you are (in front of a door and not behind it) as well as in what direction you are moving and how fast, electronic doors can intelligently

> "Applications that share mobile credentials with infrastructure make a great leap towards making your surrounding world more friendly, informative, customised and convenient."

open and close as you freely walk through an office building, airport or campus.

Your mobile credentials make sure that only the right doors open and each door's Bluetooth advertising inform your smartphone app of its identity and presence.

Add into the mix the ability to support outdoor (via GPS/GNSS) and indoor navigation (via UWB) and visitors as well as robots can be precisely guided to their destinations, whether it be to a desired exhibit in a museum, hotel room or an industrial robot delivering a palette within a warehouse.

Shared mobility

With the popularity of shared vehicles and mobility services, the inconvenient step of registering in-person or repeatedly entering credit card details is bypassed with mobile credentials.

By simply approaching your selected mode of private transportation (with guidance provided by UWB navigation), your desired vehicle activates via Bluetooth wake-up, unlocks and even adjusts to your personal preferences such as seat position, climate control, destinations, preferred restaurants and POIs.

The same credentials can be wirelessly shared with parking facilities and fuelling/charging stations to provide a seamless driving experience where you never need to pull out keys, your wallet or purse.

Industrial IoT

In countless Industrial IoT (IIoT) deployments such as building management and logistics supply chains, millions of interactions take place per day between machines, infrastructure, containers, etc. and employees, contractors and partners.

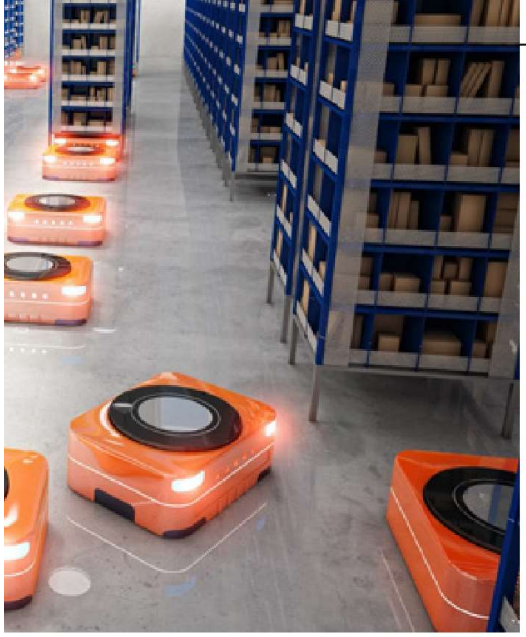
> "As theft of mobile credentials is a show-stopper for any possible business model, end-to-end encryption of credential data plus protection of encryption keys is a foremost requirement."

Ensuring that only authorised persons are interacting with industrial assets, and at the right time and place, requires the automated recognition of a person's (or robot's) mobile credentials. Only then can interactions be allowed to take place including logging of when and where it occurred.

An example is the shipping of pharmaceuticals which require a tightly controlled environment. Supply chains consist of multiple transport links provided by different parties from factory to warehouse to truck/train to container ship, and the reverse process, before reaching their destination.

The handling of goods and exposure to ambient temperatures, humidity, vibration, shock and more takes place at multiple points along the way. By implementing an IIoT system that not only monitors environmental conditions and the location of shipments, but also requires mobile credentialing of personnel before containers will open and close, end-to-end accountability can be established to ensure that proper handling has been enforced throughout the delivery chain.

Should an error be encountered, for instance, a shipment of medicines that was exposed to too high temperatures, the exact point of failure including when, how long



and the responsible party can be instantly identified for auditing and insurance purposes.

On-the-fly access to services

Mobile credentials are commonly used for public transportation passes. Typically purchased on an annual basis, credentials can be shared with partners, for example, to provide bundled complementary services such as discounts for rental car, hotels and ski-passes.

Many services are required on-the-fly and on-demand and maybe even only one time. An example is an office visitor who needs a single-day access to your company printers, employee restaurant and coffee machines. In this case, the simplest kind of mobile credential can be provisioned to the visitor's phone via QR code or email deep link: A random token that is recognised by the back-end credentialing system as a valid one-day pass to use services in your office.

Smart self-service retail

Unmanned convenience stores are growing at a rapid pace worldwide to meet consumer demand for fast check-out, while reducing costs for retailers. This shopping trend leverages mobile credentials, a smartphone equivalent to current customer loyalty cards, with mobile wallets.

"Just walk out" stores such as Amazon Go implement AI with computer vision, sensors and RFID to detect items taken from the shelf. As there is no staff present, UWB navigation can further enhance the experience with indoor navigation to guide consumers to desired products and Bluetooth wake-up can advertise specials or new products as shoppers come within range.

This technology also facilitates "shop-in-shop" scenarios where mobile credentials are shared with temporary third party retailers who can also benefit from Bluetooth advertising and indoor navigation to announce their presence and guide shoppers to their area.

An end-to-end mobile credentialing platform

To enable all these scenarios, an end-to-end security platform is needed that facilitates creating, storing, modifying, distributing and protecting mobile credentials both in-transit and at rest, as they are distributed over the internet or broadcast via Bluetooth.

As theft of mobile credentials is a show-stopper for any possible business model, end-to-end encryption of credential data plus protection of encryption keys is a foremost requirement.

A key component for supporting mobile credentialing – LEGIC Security Modules

Especially for valuable infrastructure that is broadcasting its presence – be it electronic doors, mobility vehicle or shipping container – encryption keys must be stored in a Bluetooth reader device containing a secure element that is physically and electronically inaccessible.

This is accomplished via LEGIC 6000 series Security Modules which also enable devices and infrastructure to advertise their presence via Bluetooth, even while in a sleep-mode – important for battery powered devices. Security Modules are an integral part of LEGIC's end-to-end Security Platform which includes Trusted Services and Mobile SDK.

For more details about LEGIC's end-to-end Security Platform for mobile credentialing, visit: www.legic.com/connect

SECURITY BY DESIGN

LEGIC Connect is a mobile credentialing platform that securely distributes mobile credentials or other data to registered smartphones or tablets anytime, anywhere, instantly, automatically or at the touch of a button.

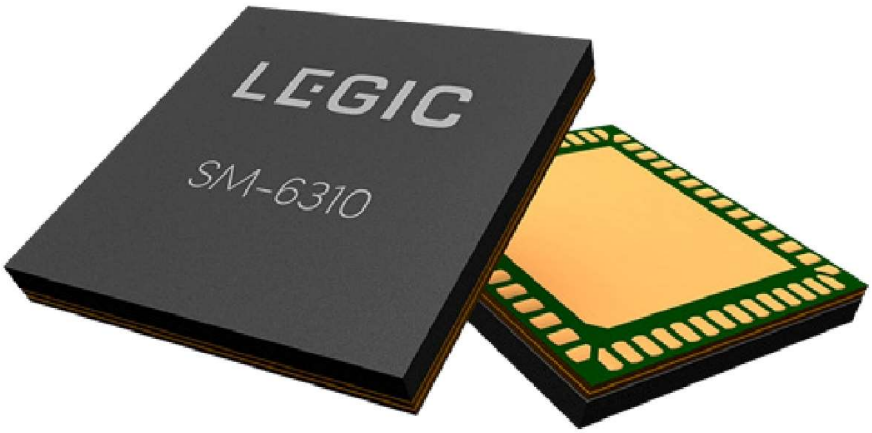
The system provides a globally available, secure, end-to-end mobile credentialing service that is the backbone of establishing trust and accountability in user/device /infrastructure interactions. The system can be easily integrated into existing infrastructures, giving service providers the ability to manage user credentials, permissions as well as send and receive data securely from smartphones and sensors. The system is fully compatible with UWB positioning systems and supports discovery of devices equipped with Bluetooth advertising.

LEGIC Connect protects infrastructure, data and credentials from manipulation, enables fully automated operation and provides transparency via transaction-based data that can be collected from trusted users, devices and infrastructure touchpoints. Android and iOS are supported, and a mobile SDK is provided for easy development of mobile apps that support any kind of service based on mobile credentialing.

LEGIC SECURITY PLATFORM RECEIVES MAJOR UPGRADES

Bluetooth Central Role for Smartphones and Bluetooth wake-up feature for the LEGIC 6000 series Security Modules opens a whole new world of applications

LEGIC is pleased to announce the addition of two new complementary, intelligent and power-saving features for the LEGIC 6000 series Security Modules: Bluetooth wake-up from sleep-mode via OS50 firmware update and Bluetooth Central Role for smartphone apps via an upgraded LEGIC Mobile SDK for iOS and Android.



Intelligent features

LEGIC, via its upgraded mobile SDK, now enables smartphone apps (or LEGIC Security Modules and third-party Bluetooth devices) to implement the Central Role in Bluetooth Low Energy communications. This can, for example, enable mobile devices to automatically search for, discover, filter, wake-up and connect to a specific Bluetooth-enabled peripheral device such as electronic door, locker, shared vehicle, etc.

To facilitate this new discovery feature, the firmware upgrade enables LEGIC 6000 series Security Modules embedded in readers, IoT devices and infrastructure to continuously broadcast a customer-defined designator and status via Bluetooth Low Energy, even while in sleep-mode.

Once discovered, woken up and connected to the mobile device, the selected LEGIC Security Module will allow the mobile app to explore and interact with the features and data that the peripheral device has to offer. This can, for example, allow a specific e-scooter parked amongst many to automatically wake-up from sleep-mode, flash lights and beep when the owner is within Bluetooth distance.

Lower power consumption for Bluetooth-based systems

A key USP of the LEGIC Security Platform is the support for battery-powered readers. To facilitate this, LEGIC 6000 series Security Modules come with a sleep-mode that can be activated by the host controller over the host command interface or via Custom Code, allowing a reader to power down its electronics. With this new upgrade, the Security Module continues to periodically advertise its presence including reader designator ID even while in sleep-mode. This signal can be read by other devices within Bluetooth range, for example a smartphone app.

Once the desired reader is discovered, the app can initiate the wake-up so that the reader can establish a connection via Bluetooth to the app. The app can then communicate with the peripheral based on its designator ID. This new Bluetooth wake-up feature is in addition to the previously available wake-up triggers Inductive or Capacitive Sensing, External I/O and Internal Timer.

These major upgrades deliver added value to customer applications. having the following characteristics:

- Environments with multiple Bluetooth reader devices in range
- Battery-powered Bluetooth reader devices that cannot rely on short-range, near-field sensing for wake-up
- LEGIC 6000 series Security Modules support virtually all possible wake-up mechanisms as well as Bluetooth Central and/or Peripheral Roles
- Each reader designator is customer-defined and encrypted so that it cannot be read by unauthorised devices