eBook: The Foundation of Smart Cities? Smart Security.

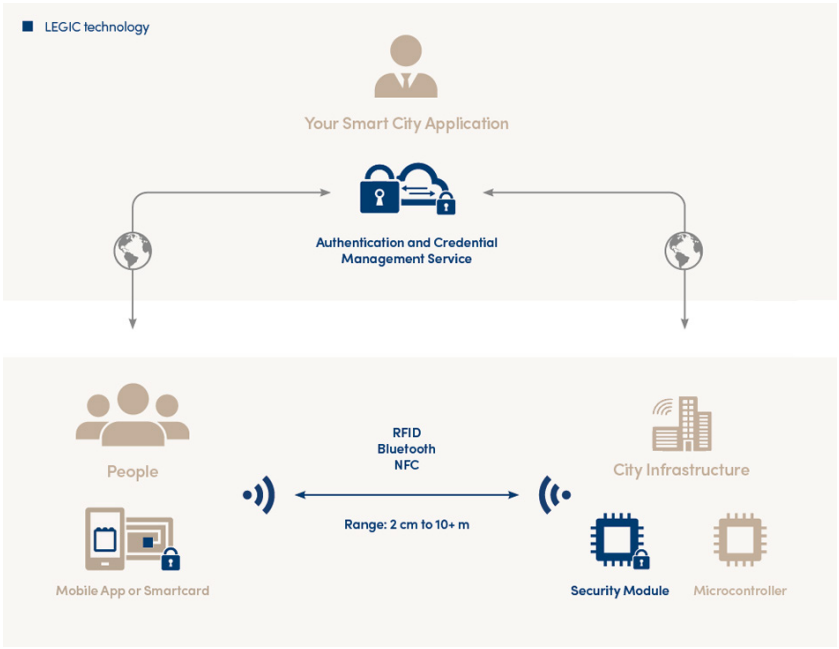
dormakaba

The era of "Smart Cities" is here and now includes more than just a traditional urban space. From public spaces to business to healthcare to college campuses to multifamily and residential properties, technology accomplishes what humans alone cannot: instantly and securely confirm the identity of a person and present dynamically and remotely provisioned credentials to infrastructure. This establishes what each individual prefers or is allowed to do, when and where. As dependence on "smart" grows, the need to assure maximum security of data also grows exponentially. Technology-driven credentials generate a lot of data. And, how that data is stored and used is fast becoming an important differentiator as properties make decisions about technology partners.

Smart City requires a secure platform approach

By 2050, 70% of the world's population will live in cities; over 50 megacities will contain over 10 million inhabitants. To sustain this massive urbanization, "Smart City" technology implementing secure cloud connectivity, authentication and personal credential management, and Bluetooth last-meter interaction is essential. Enabling this scenario requires an end-to-end platform approach.

Although to end-users the only visible part of Smart City technology is the smartphone or smartcard, a complete, end-to-end encrypted cloud service backend is required to support secure authentication of individuals and infrastructure, as well as to manage and dynamically update their credentials (i.e. what they prefer, can use and how). As the security of Smart City services has large ramifications on personal and public safety as well as on millions of e-payment transactions that take place in cities every day, state-of-art end-to-end encryption is a crucial feature of the platform.



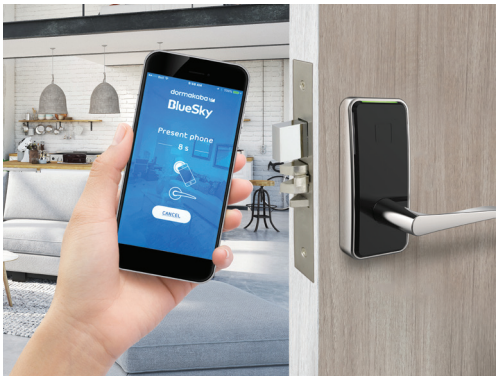
The figure above illustrates a Smart City application built on top of a security platform that authenticates users while managing their credentials. The three main components illustrated are the individual (via his or her Bluetooth enabled smartphone or NFC enabled smartcard), city infrastructure (e.g. a train, door, shared vehicle, shop, tourist services etc.), and cloud-hosted application (e.g. car-sharing application or e-ticketing for public transport) coupled with an authentication and credential management service.

Two links in this triangle are supported by the publicly available internet where TLS 2.0, a commonly deployed encryption protocol, is considered today as the minimal security level for most websites (https). As Smart City apps can be life or business critical, an additional level of security under the Smart City service provider's direct control is desirable, in particular end-to-end AES-128/256 encryption where keys are protected and managed by a Hardware Security Module together with Secure Element technology running in a trusted environment.

These well-established, industry-proven techniques provide the strongest protection against hacking, data interception or infrastructure manipulation. Short-range wireless communication between smartphone / smartcard and infrastructure is also protected by mutually held, session-dependent encryption keys.

Through this combination of technologies, the platform enables secure, managed and permissioned access to Smart City services and resources be it simply access control (who may open which doors and when), to mobility services (e.g. car sharing or e-scooter rental), to education (e.g. controlling student access to classrooms, libraries, and IT resources such as virtual PCs and printers).

Not all BLE is equal



Properties interested in incorporating BLE (Bluetooth Low Energy) technology into their environments need to conduct vigilant due diligence. The best smart technology providers own end-to-end encryption with no third-party interference, do not have hidden fees and are able to work across access solutions such as mobile, fob, or keycard with equal ease and security.

LEGIC Identsystems AG, the technology owned by dormakaba, provides system integrators with a cryptographically secure authentication and credential management platform used for contactless, permissioned access to devices, assets and infrastructure. Over 2 million digital keys have been deployed with dormakaba BLE locks on over 35,000 properties.

dormakaba's multifamily access control solutions allow for intuitive access management for residences, amenities, common areas and perimeters including integrated access management software for property management and BLE credential management through LEGIC. Streamlined smart access for multifamily properties further connects residents with Smart City technologies.

The following questions can guide BLE access research

- How many BLE/digital keys have you provided in the marketplace?
- How long have you provided BLE solutions?
- How far across one property can your BLE solution take the user? Does this technology seamlessly integrate with both property and amenity doors?
- Is your BLE solution truly authenticated and will it remain that way throughout its life? How frequently does it need to be re-authenticated?
- How has the security been tested? What kind of third-party testing is in place?
- Can you scale this solution across multiple access solutions such as mobile, fob and keycard with equal success?
- Do you own your BLE solution and end-to-end system deployment with a cryptographically secure authentication and credential management platform?

The technology to securely enable Smart Cities exists today, with proof of concept demonstrated each time we make a contactless credit or debit card transaction, enter our office building with our badge, or purchase a train e-ticket with our smartphone. Extending this proven technology to all aspects of our interactions with infrastructure and services within cities is without a doubt a smart idea!