LEGIC

White paper

Enabling Smarter Cities

Felix Pütz, Dariusz Kafka, Carl Fenger
LEGIC Identsystems AG

Employing technology to increase efficiency, save costs and resources, and increase quality of life

Summary

The technology to securely enable Smart Cities exists today, with proof of concept demonstrated each time we make a 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!

Enabling secure interactions between people and infrastructure

The term "Smart City" was coined by IBM in 2009 to describe technology applied to help cities run more efficiently, save costs and resources, and increase the quality of life of its inhabitants. The term today is like many industry buzzwords and means different things to different cities, companies and people.

In order to come to a general definition, technology applied to solve city problems needs to address common-denominator elements that most affect cities and their inhabitants:

- **Infrastructure:** government services, educational facilities, sport and entertainment venues, lighting, security, utilities, hospitals, libraries, hotels, parking, roads
- **Transportation:** trains, buses, trams, micromobility, connected and shared cars, autonomous vehicles
- **Commerce:** shops, markets, malls, restaurants, services

What all these elements of a city have in common is that they are things that people in cities interact with, but each in a different way.

These interactions can be complex: things need to react differently to individuals depending on a person's identity, preferences, location and even time-of-day, for example, a first-class public transportation ticket that is valid only for the purchaser and only for specific areas during a specific time period. Similarly, a "Smart Retail" solution determines how shops and brands could react differently to mobile consumers via ads or special offers depending on individual preferences, location, time-of-day, purchase history or even the weather!

In Smart City scenarios, technology accomplishes what humans alone cannot: instantly and securely confirm the identity of a person and present dynamically and remotely provisioned credentials to city infrastructure. This establishes what each individual prefers or is allowed to do, when and where.

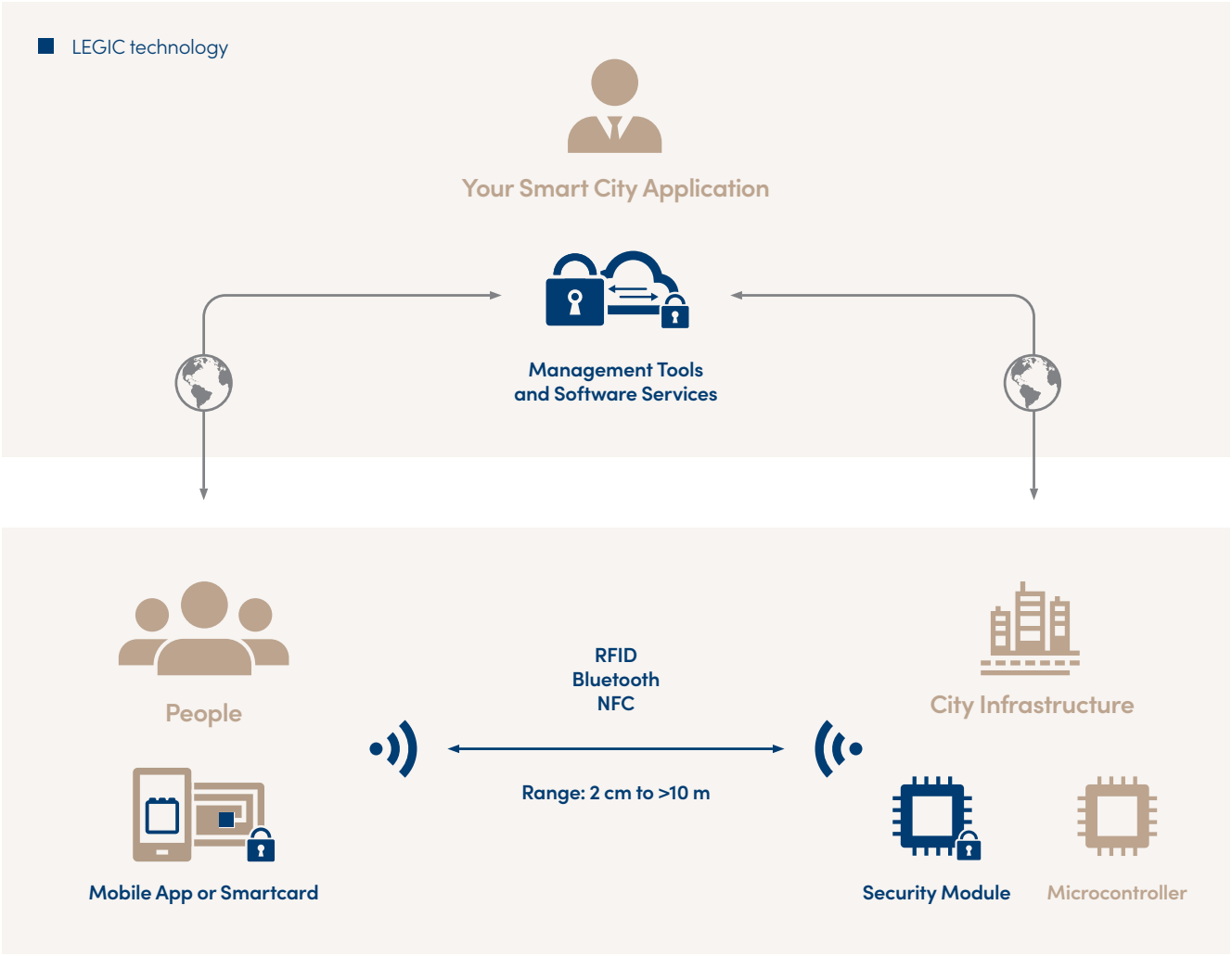
In the absence of surgically-implanted ID chips, a dystopian scenario best suited to science fiction films, the next best thing available to enable Smart City applications is the common smartphone or smartcard – most people are already in possession of one or the other.

The beauty of these devices is their ability to (wirelessly via Bluetooth or NFC) serve a multitude of purposes simultaneously: from a metro ticket, to a e-payment card, to a contactless car key, city or event pass, ID or driver's license.

Convenience as enabler of adoption

Smartphones and smartcards as enablers for Smart City applications is accelerating primarily because they are convenient, wireless, and most people already have one in their pocket. Mobility solutions such as car sharing are already largely smartphone based, while smartcards (e.g. credit, debit or metro cards) are deployed worldwide for e-payment and public transportation.

This is only the beginning. As both smartphone and smartcards can easily support numerous applications simultaneously, it is only a matter of time before a wide range of services for Smart Retail, Smart Tourism, and Smart Living are added to these devices. Employing smartphones or smartcards to authenticate users to city infrastructure and services while applying each user's credential to determine what he or she may use, prefer, or have access to, is the common denominator.



Intelligent security and contactless interaction for connected infrastructure

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 connectivity, authentication and personal credential management is essential. Enabling this scenario requires and 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 smartphone or smartcard), city infrastructure (e.g. a train, door, shared vehicle, shop, 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 such as 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 spoofing.

Bluetooth and NFC wireless communication between smartphone / smartcard and infrastructure is also protected by mutually held, session-dependent encryption keys as well as biometric authentication data (e.g. fingerprint, facial, or Iris patterns) stored in a hardware Secure Element.

Through this combination of technologies, the platform enables secure, managed and permissioned access to Smart City services and resources.

Typical applications include employee and visitor 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).

The technology to securely enable Smart Cities exists today, with proof of concept demonstrated each time we make a 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!

About LEGIC

LEGIC Identsystems AG provides system integrators with a cryptographically secure authentication and credential management platform used for contactless, permissioned access to devices, assets and infrastructure. Consisting of software services and semiconductors based on a Root-of-Trust security anchor, the platform is used worldwide for smartphone and smartcard-based access, Smart City and IoT applications.

LEGIC

LEGIC Identsystems AG
Switzerland Phone +41 44 933 64 64 info@legic.com www.legic.com

April 2020 Author: Felix Pütz, Dariusz Kafka, Carl Fenger