



Authentication Goes Mobile

Mobile Access Credentials from ELATEC GmbH

The potential of mobile authentication solutions is enormous. Many companies are already benefiting from the innovative application possibilities by adding mobile solutions to their access control systems.

At a rapid pace, companies are currently building a more modern working world in which employees can work flexibly both at home and in the office. Digitalization has never progressed as fast as it has in recent months. COVID-19 has accelerated this change in many areas. However, the development presents IT managers with new challenges. To protect sensitive company data, for example, they must ensure that the laptop is protected from unauthorized access at the user's home office. If users want to access their computers, access should not only be secure but also as uncomplicated as possible. This is where new technologies offer a wide range of possibilities. For example, employees can access the computer and data on

the company server using contactless authentication with their smartphone.

Even before Covid-19, providers of shared offices or coworking spaces increasingly relied on mobile solutions to control access to their premises. Before that, it was common practice to use keys or access cards, which are now often replaced by digital credentials. This approach is easy and convenient for the user, because the authorization process takes place directly via his or her smartphone.

The Technology Behind Mobile Access Control: Contactless and Lightning-fast

Mobile authentication solutions are mainly based on at least one of the following two technologies: Near Field Communication (NFC) and Bluetooth® Low Energy (BLE).

NFC is a high-frequency (13.56 MHz) international transmission standard that enables the contactless and secure exchange of data over a short distance. The transmission range of NFC is up to about ten centimeters, but the range depends heavily on the device used. If the smartphone is located near an RFID reader, the transaction is processed. Dr. Dominik Samson, the Director and CEO of Office and Business Development at ELATEC GmbH, a company based in Puchheim, Germany, adds: "Due to this short distance, in certain applications the establishment of a connection is interpreted as consent to a transaction. For example, when an employee—virtually in passing—holds his smartphone up to the reader in front of the turnstile of the office complex and gains access, or when contact data, pictures, videos and links are exchanged between smartphones and tablets."

Another advantage of Near-Field Communication, apart from its low energy consumption, is that it can be used immediately by the participants. There is no need for time-consuming authen-

ELATEC GmbH
Zeppelinstr. 1
82178 Puchheim
www.elatec.com



»» **Once implemented correctly and in line with requirements, user-friendliness is a major advantage, making BLE increasingly popular. After all, the user no longer needs to actively hold the smartphone up to the reader; it is sufficient to carry the device with him in his jacket pocket, for example.**

Dr. Dominik Samson, ELATEC GmbH



tication input or registration. The connection between two NFC-enabled end devices is also established in a fraction of a second. "Good NFC implementations behave almost exactly like RFID cards. This means there is no noticeable difference or latency when a cell phone is held in front of the reader," explains Dr. Samson.

According to Dr. Samson, NFC is suitable for several different types of use. "First, a great many of today's smartphones support this transmission standard and are therefore able to simulate contactless cards for authentication. In card emulation, the NFC device is used like a contactless identification medium and is held to an NFC-enabled RFID reader for authentication. Additionally, an NFC-capable device can simultaneously work as a reader and write to transponders. In this so-called read-write mode, the smartphone is in active mode and reads a passive NFC tag. The third application area is peer-to-peer communication, or P2P, between two active devices with NFC. Here, data is exchanged between two devices, for example a smartphone and a point-of-sale terminal."

These different types of use open up a wide range of possibilities for using the

technology in both the private and business sectors. With NFC, a multitude of applications for secure and convenient contactless authentication can be covered. Near-Field Communication is also becoming increasingly widespread in the area of payment and the exchange of multimedia files.

The NFC technology is used mainly for communication with Android devices; currently, iOS devices only support NFC to a limited extent. Even though Apple has supported writing on NFC tags since iOS11, a card emulation application is not yet generally available.

Here Bluetooth® Low Energy comes into play. BLE is a radio technology for distances up to ten meters in the frequency range of 2.4 GHz. The information carriers (BLE units) are active radio transmitters (beacons) that require power, for example from a battery. The beacons communicate with BLE-enabled cell phones and other readers without contact. Smartphones can also be used as radio transmitters. BLE is suitable for applications such as authentication at doors in emergency rooms, where a distance of several meters must be covered, and for secure authentication at shorter distances, for example for identification via smartphone. "Once implemented

correctly and in line with requirements, user-friendliness is a major advantage, making BLE increasingly popular. After all, the user no longer needs to actively hold the smartphone up to the reader; it is sufficient to carry the device with him in his jacket pocket, for example," explains Dr. Samson, adding: "But NFC also has many advantages and therefore a good chance of becoming more widely accepted."

In Practice: More Comfort, Lower Costs

A concrete area of application that clearly demonstrates the advantages of a smartphone as a means of identification is the location-independent issuing of mobile access authorizations in companies. The issuing and handover of physical ID cards is no longer necessary, which saves time and money. For example, a technician can easily and quickly obtain temporary access to certain branch offices of a company. The access authorization for the required areas is provided directly in the app on his smartphone. This way, he can easily obtain all necessary authorizations—for example, to pass the parking barrier, open the entrance door and authenticate himself at the IT room.



ELATEC App Offers Greater Flexibility

To integrate an access system, the appropriate technology must be purchased, and the infrastructure must be implemented. “The focus here is on the topic of security. But you should also make sure that the solutions provide maximum flexibility,” advises Dr. Samson. ELATEC solutions focus on these aspects. The products support mobile access systems with various contactless multi-frequency readers that use RFID, NFC and BLE for authentication and access control.

Another special feature is the ELATEC App. The ELATEC Mobile Badge BLE NFC App is an easy way to implement access authorization via mobile devices. The app enables iOS and Android devices to communicate directly with a reader—whether it is for access control, single sign-on in computer networks, secure printing or vending and ticketing. Customers can optimize the app for their particular application and system environment. All settings are made individually on each mobile device. Companies benefit from extending their system with a solution for identification, authentication and authorization. A unique ID is issued to each user, which cannot be changed by the user or by the

administrator. The ID is transferred to an ELATEC reader in encrypted form via BLE or NFC and transmitted to the company's back-end infrastructure. The ID can then be added to existing user management systems, for example by self-registration in a secure printing application. Dr. Samson summarizes: “This makes it very easy to extend existing classic RFID solutions with a mobile access system using smartphones.” On request, the design of the app can be customized to the corporate identity of the company. Users also benefit; all they need is a cell phone with the ELATEC app installed. “The app is quickly installed on the smartphone and immediately ready for use,” adds Dr. Samson.

There are two types of access authorization: managed and unmanaged. ELATEC offers both. The free ELATEC app is an unmanaged access authorization solution with essential basic functions. In addition, ELATEC also offers its customers various partner solutions with a more complex range of functions. These include KleverKey, for example. This solution for mobile access authorization simply adds the complete functionality of digital keys to ELATEC's TWN4 readers. For the administrator, the KleverKey portal offers a great deal of convenience, especially in terms of authoriza-

tion management. Safetrust Wallet is another partner solution of the same category. It also manages virtual identities completely securely and enables contactless access control to premises and resources. With end-to-end encryption and fast access, it offers ELATEC customers an optimal solution. This enables them to provide a convenient authentication process for their employees as well as their customers and visitors.

ident