Next-level access control

Mobile authentication solutions from ELATEC

Modern access control systems are much more than simple door openers. This is especially true when it comes to mobile authentication solutions. If they are perfectly tailored to the requirements of a company, they have the potential to make everyday tasks considerably more convenient and secure. At the same time, they can reduce costs. However, companies are often hesitant to introduce such a future-proof solution—especially if a wide variety of technologies are already in use. But with the right expertise, successful integration of RFID and mobile access solutions is possible.

In the area of access control, mobile credentials are steadily gaining importance. The digital credentials on smartphones, tablets or wearables are always at hand and are thus an ideal supplement to conventional ID cards or keyfobs. It is possible to use mobile credentials based on NFC (Near Field Communication) or BLE (Bluetooth Low Energy) technologies, which the majority of mobile devices are equipped with. The international transmission standard NFC allows the contactless and secure exchange of data over a short distance. The transaction is thus processed when the smartphone is in the vicinity of a multi-frequency RFID (Radio Frequency Identification) reader. With the particularly user-friendly BLE radio technology, on the other hand, the smartphone no longer has to be actively held up to the reader for the authentication process. Companies benefit in several respects if they add mobile authentication solutions in the course of advancing digitalization in Physical Access Control, or PAC for short. On the one hand, the effort and costs involved in managing credentials are reduced. At the same time, the convenient handling saves employees time and increases their productivity.

Customized solutions through holistic consulting

The example illustrates the advantages and possible applications of a modern access control system that integrates mobile authentication solutions in addition to conventional transponders such as cards. However, successful implementation is a challenge. This is especially true if different technologies and credentials have already been introduced over the years. Customized solutions are needed here. After all, a medium-sized company with affiliated production facilities must solve different challenges with an access system than a multinational corporation with properties in several countries.

To ensure that the introduction of an access control system is a success, companies should pay particular atten-

You can find more information at

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

tion to the future-proofing and flexibility of the solution as well as the security of the overall system. Above all, however, it is advisable for companies to first seek the advice of experts who have experience in authentication processes before making an investment decision. Comprehensive pre-sales consulting from appropriate solution providers includes an analysis of the current situation and requirements as well as documentation of the results. Optimal consulting also includes a feasibility study, proof-of-concept, and a project and rollout plan. During the implementation phase, solution providers handle hardware and software integration, application development, configuration, and all customizations, as well as testing and protocol verification. During the transition to an access control system that also supports mobile authentication solutions, companies do not have to sacrifice the functionality of their access and access control: multi-frequency readers allow a smooth migration as they support RFID as well as NFC and BLE. This ensures that all transponders can be used continuously, from the mobile end device to the card ID to the keyfob.

Future-proof from initial integration

Requirements and IT infrastructures change over time—and so does the overall system. Companies should therefore ensure that technical support does not end with the initial integration. Only a flexible system that provides for optimization, adaptation and upgrades is future-proof. Companies should therefore ensure that solution providers offer their customers software development kits in addition to expert support. With these, the products delivered in standard configuration can be easily adapted, either by the company itself or by the solution provider—even remotely.

Flexibility for internationally operating companies

The integration of access control systems is particularly complex in an international context. Companies with subsidiaries in several countries or even on different continents often use different transponder technologies from location to location. In order to nevertheless enable simple and fast access for the company's own employees, but also for temporary visitors, a flexible solution is required. Readers are available on the market that use RFID, NFC and BLE for authentication and access control and are also suitable for international use. The readers from solution provider ELATEC, for example, are compatible with up to 60 transponder technologies and certified for sale in up to 110 countries worldwide. A uniform solution pays off particularly well for companies that operate internationally. On the one hand, conventional transponders such as cards or keyfobs can be used universally at all locations. On the other hand, central remote maintenance of digital credentials involves little effort. They are implemented directly on the user's smartphone and can be easily blocked in the event of loss or theft and reinstated when the phone is replaced.

> **To ensure that the introduction of an access control system is a success, companies should pay particular attention to the future-proofing and flexibility of the solution as well as the security of the overall system.**

Security: a question of the overall system

Access control systems serve to protect people and assets. To ensure this, the systems themselves must be secured against manipulation. This is because security gaps pose an enormous risk—especially in the age of digital transformation. When selecting a reader as a central component of an access solution, care must be taken to ensure that it supports the credentials and encryption algorithms appropriate for the application's security level. In addition, the physical security of the reader must be considered to prevent tampering. In this context, solution providers such as ELATEC not only offer the appropriate products, but also comprehensive consulting services that go beyond the reader itself. The experts cooperate closely with system integrators and support them by identifying the optimal authentication solution. The system integrators can thus concentrate on their core business.

However, in order to effectively and holistically secure an RFID-based system such as an access control system,

it is not sufficient to consider the reader alone. It is necessary to include the entire system in the company's security concepts in advance. This is a complex process that, in brief, proceeds as follows: based on a real existing or feared threat scenario, a protection concept is developed, which forms the basis for the implementation of the specific protection. This can be achieved by a technical element as well as a procedure or process. In any case, the following applies: security must always be related to the overall system.

Conclusion

First and foremost, access control systems are essential for corporate security. They are designed to ensure that only authorized persons are granted access to sensitive areas. But especially in combination with smartphone-based badge solutions, they can do more: they provide considerable relief for employees and thus increase their productivity and satisfaction. The decision in favor of a modern access control system can have a positive effect in the company that goes far beyond the aspects of security and reduction of costs and administrative effort.

ident

Convenience through smartphone-based ID solutions: an example

For Julia F., who works as an engineer in an international company, the company smartphone is an indispensable companion: it functions as a universal identification medium for access, entry, time recording or access authorization to the IT infrastructure, among other things. This is made possible by an app that implements the corresponding authorizations on her smartphone. The app allows iOS and Android devices to communicate directly with multifrequency RFID readers.

In the morning, the engineer uses her company smartphone to open the barrier to the underground parking garage. She then charges her e-car in the garage; user authentication at the charging station is also done with the smartphone. Thanks to the access authorization stored in her smartphone, the elevator takes her directly to the right floor. Once in the office, she uses her phone to log in to her PC and, using single sign-on, has immediate access to all of the computers and services for which she is authorized. Forgotten or insecure passwords are no longer an issue. Julia F. prints out confidential documents for the upcoming meeting with a customer. Secure Printing guarantees that they don't fall into the wrong hands: only when her company smartphone is physically near the printer is the print job triggered.

The engineer booked the room for the meeting in advance via her online booking system. Check-in is fast, contactless and hygienic—the smartphone communicates with the RFID reader installed at the entrance of the meeting room. And customer visits are also unproblematic, because the temporary access authorization on the customer's smartphone eliminates the often-tedious registration process at the reception desk.

But mobile credentials not only prove their advantages in the immediate context of work. They make paying in the cafeteria just as convenient as going to the company gym. In a few days, Julia F. will be going on a business trip to the company's location in the US. And she can already be sure that, thanks to a standardized company-wide solution, her smartphone has the appropriate authorizations to enable her to work productively right away.