ACCESS TO THE SMART OFFICE WORLD

How an authentication solution provides security and flexibility in future-oriented office environments

A flexible access system covers all applications needed in the office and can both improve usability and minimize security risks.

It is not only younger employees who long for flexibility in the workplace—especially since the Corona pandemic, preferences for working hours and location are becoming increasingly individualized. Companies must respond to this development with appropriate solutions to attract and retain employees. A modern office environment and the option for remote work are decisive factors in being perceived as an attractive employer. This new working world calls for a sophisticated authentication solution that combines convenience and security.

The modern office is the company's flagship and is more than just a physical location—it is a dynamic, technology-driven environment designed for efficiency, security and convenience. In this new working landscape, authentication and access control play a critical role. For example, the smart office requires a universal authentication solution that enables access to buildings and spaces, as well as access to devices and digital applications.

Seamless and secure authentication

In order to carry out their daily work in the smart office, employees are confronted with a multitude of authorizations: in addition to access to locations, they must be able to record their working hours, log on to the corporate network, book meeting rooms, securely receive print jobs and pay in the canteen. Then there is access to company vehicles and charging infrastructure for EVs. All of these applications are often accessed across multiple platforms and endpoints, requiring a variety of passwords, PINs, physical keys and authentication systems. This can lead to password fatigue, inefficient processes and increased security risk. Therefore, a seamless and secure authentication solution that reliably protects people, infrastructure and data is needed.

A system based on RFID that also supports mobile technologies provides an answer to these challenges. It covers all applications needed in the office and can both improve usability and minimize security risks. In addition, such a solution enables secure remote working. This is because access to data, networked devices and software systems must be particularly well protected, especially when used outside the office. For this purpose, a reader is connected to or integrated into the computer or workstation and connected to the PC logon middleware. Instead of entering a password to log on, users simply hold their ID card or smartphone with digital credentials up to the reader to gain access to networks, services and files.

> "Smart offices enhance the company's attractiveness to talented professionals and increase employee satisfaction."

Universal readers

Choosing the right technology is key to designing a unified access and entry system. Universal readers can recognize RFID signals from ID cards or key fobs as well as process mobile credentials via Bluetooth® Low Energy (BLE) or Near Field Communication (NFC). At the heart of such a solution are universal readers that are compatible with all popular RFID technologies and mobile credential systems. These versatile readers allow companies to standardize their access systems throughout the office and even across different locations without having to modify existing primary access and badging systems. If a different transponder technology is preferred in the future, adaptation is straightforward, as the readers can be easily reconfigured remotely. This provides companies with a flexible and future-proof system that can be easily adapted and scaled.

The combination of RFID and mobile credentials brings numerous advantages for companies.

- Ease of use: Many employees already carry RFID cards for identification and building access. These cards can be used not only for physical access, but also for digital applications across the enterprise.
- Security: A uniform system for access and entry ensures secure user identification for all areas of the office. This not only improves security, but also increases transparency. The likelihood of loss or theft of a badge or cell phone is lower than with traditional keys, passwords or PINs. Encrypted RFID or BLE/NFC credentials are highly resistant to copying or forgery.

- Reliability: RFID cards enable contactless identification and are characterized by their high reliability. Unlike magnetic stripe cards, which are susceptible to dirt and magnetic fields, RFID cards function reliably. This also applies in comparison to biometric technologies, which can exhibit errors under certain conditions.

The introduction of a unified authentication solution requires precise planning and integration into the existing office infrastructure. Seamless integration into existing security protocols and ensuring data privacy compliance are essential aspects. Data protection must be taken seriously, and appropriate safeguards must be implemented to ensure the confidentiality of the data collected.

Future-proof access solutions

Smart offices increase the attractiveness of the company for talented professionals and increase employee satisfaction. Implementing smart office technologies signals that the company is innovative and open to modern working methods. The prerequisite is a seamless, efficient and secure authentication solution that can accommodate such a working environment. RFID-based systems that also support mobile technologies provide an answer to these requirements. They improve the security, usability and efficiency of authentication processes in modern work environments. With careful planning, implementation and consideration of data protection aspects, this technology can make a significant contribution to shaping the working world of the future.

Author

ELATEC GmbH

Zeppelinstr. 1

82178 Puchheim, Germany,

Phone: +49 89 552 9961 0

E-mail: info-rfid@elatec.com

In cooperation with PROTECTOR