ELATEC
RFID Systems

SYSTEMATIC SECURITY AND TRANSPARENCY

Contactless authentication solutions for laboratories and cleanroom environments

In laboratories and cleanrooms, controlling access is essential to protect people, machines and data. An authentication solution must meet the special requirements of this environment. Four criteria in particular must be taken into account.

Working in laboratories and cleanrooms requires special knowledge from employees—both in terms of handling expensive and sensitive equipment and potentially dangerous or toxic materials, and with regard to the strict hygiene regulations. Even external service providers such as cleaners must also comply with the rules that apply here. The higher the protection level or cleanroom class, the stricter the safety requirements. For operators, this means that where regulations require it, they must ensure that only authorized and trained persons are allowed access to the rooms, equipment and systems. Another key challenge is system security: machines, systems and peripherals, as well as sensitive and valuable data, must be effectively protected against unauthorized access.

Secure user authentication made easy

A modern user authentication and access control system based on RFID, which also allows the use of mobile authorization badges, is a simple and secure solution for protecting people, data and inventory. It also offers the possibility of documenting processes reliably and with little effort. This makes quality management and time-and-attendance recording, for example, much easier.

An equally straightforward and inexpensive option for implementing user authentication and access control is a badge equipped with an RFID tag—which most employees already carry with them in the form of an ID card or token. The use of wearables, for example in the form of wristbands, is also possible. When a physical badge of this type is held up to the reader, the identification process takes place automatically. The authorized person is immediately granted access to the laboratory rooms and can smoothly access computer systems or equipment. Authorization levels can be individually adapted depending on the employee's qualifications and permissions.

It is also possible to use digital credentials, also called mobile credentials. They are based on Near Field Communication (NFC) or Bluetooth® Low Energy (BLE) technologies, with which the majority of all mobile devices such as smartphones are equipped. The international transmission standard NFC allows the contactless and secure exchange of data over a short distance. The transaction is therefore processed when the smartphone is in the vicinity of a multi-frequency reader. With BLE radio technology, on the other hand, the cell phone doesn't necessarily have to be actively held up to the reader for the authentication process; depending on the distance specified in the system, authentication can happen from across the room. Both physical and digital credentials allow convenient, contactless and thus hygienic authentication.

In addition, if the work environment requires strong two-factor authentication, RFID can be used in conjunction with biometric or password systems.

Four criteria for choosing the right reader

Universal readers are at the heart of a modern access control system. Especially for use in laboratories and clean rooms, they must meet specific requirements to ensure that legal standards are met. The following aspects must be considered when making a selection.

Hygiene: The special requirements of GMP (Good Manufacturing Practice) environments are often neglected with regard to the readers used. Devices built into conventional plastic housings cannot be regularly treated with disinfectants or strong cleaning agents. This is because the housings are easily damaged by the use of aggressive substances and frequent cleaning cycles. In cleanrooms, this can even lead to an impairment of the work results, because a damaged housing bears the risk of releasing particles that could contaminate the environment. It is therefore advisable to use readers that are integrated into a housing made of stainless steel and glass, materials that are commonly used for GMP applications. They can withstand stringent cleaning and hygiene requirements. The housings should be designed without corners, edges or open connections and should comply with protection class IP65 (protection against low-pressure jets of water from all directions as well as against condensation and splash water).

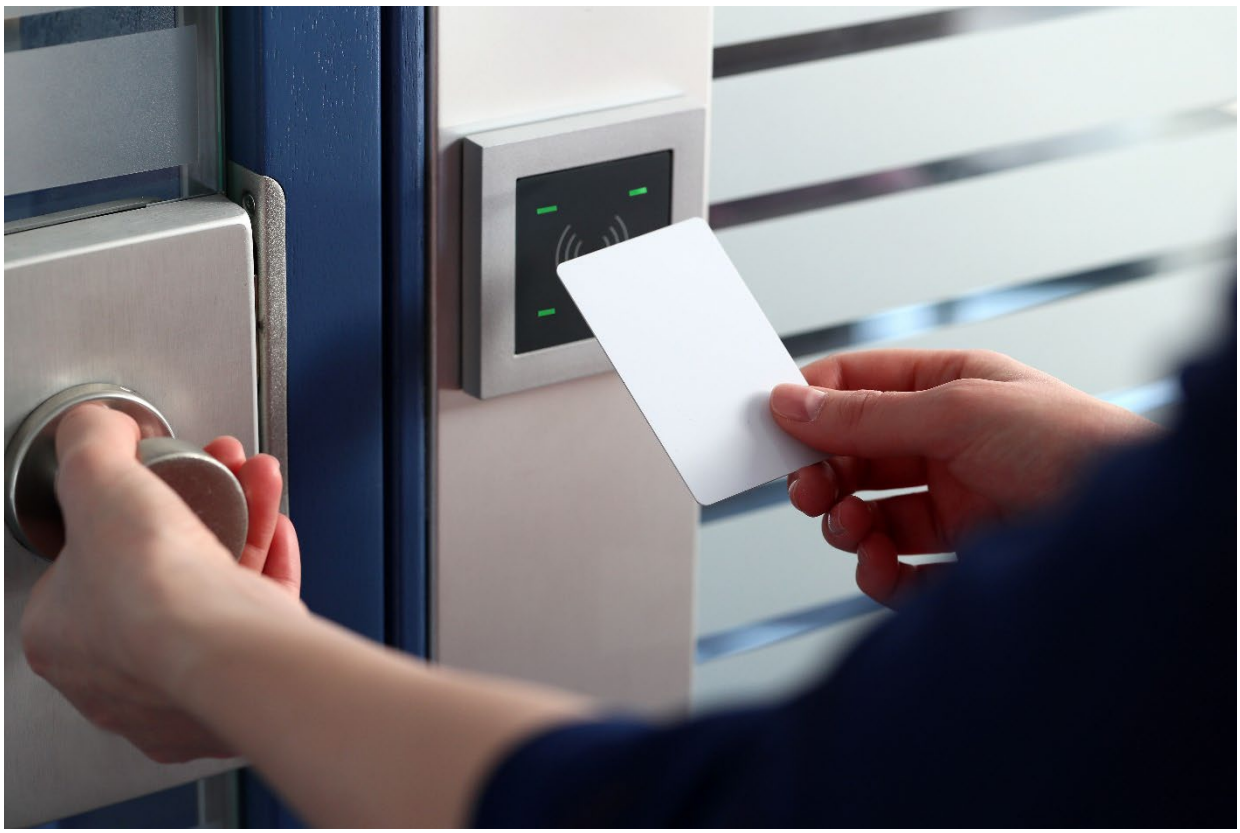
Security of data, systems and people: When it comes to accessing premises and computer networks and software systems, laboratory and cleanroom environments require a high level of security. This means that the readers used must be resistant to

both physical tampering and hacker attacks. Readers suitable for high-security labs or manufacturing environments should support advanced encryption technology. Encrypted RFID or BLE/NFC signals are harder to intercept or forge. For added security, readers that are compatible with biometrics (e.g., wristband biometric system) for two-factor authentication.

Last but not least, employees must be protected by access control. After all, laboratories and cleanrooms work with materials that can pose a considerable health hazard if used improperly.

Flexibility: Dozens of RFID card technologies are in use around the world, each with its own data formats, communication frequencies and security features. Cards can be broadly categorized as high frequency (HF) and low frequency (LF), depending on the frequency range they use for communication. However, within these categories, cards from different manufacturers have their own unique formats. Organizations with multiple locations or existing user authentication and access control systems should look to universal readers that are certified for global use and support a variety of technologies. They offer organizations an all-in-one solution that reduces complexity, helping to save time and money. Reader models from solution provider Elatec, for example, which can process up to 60 common transponder technologies, are a good choice. Multi-frequency readers make it possible to process all transponder technologies currently used in the company and those that will be used in the future; they are also suitable for smartphone authentication with BLE or NFC technology.

Future-proofing: Changes to operating systems, the use of new transponder technologies, or emerging security threats may require readers to be updated or reconfigured. It is advisable to implement readers that have an open programming interface. This ensures maximum adaptability and future-proofing of the devices as requirements change, because updates and upgrades can be carried out at any time. It is important that these can be carried out via remote maintenance. This avoids the need for technicians to laboriously remove, adjust and reinstall each individual device. Readers should also be programmable to enable specific functions for sophisticated PC login software and support mobile access control technologies. In this way, readers meet the needs of lab operators and users over a long period of time.



How RFID works

RFID cards have an embedded chip (or tag) that consists of two main components:

- an integrated unit that can store and process information
- an antenna for transmitting or receiving a signal

A unique data record—for example, a number—is stored on each RFID card and is used to identify the card and thus also the person carrying it. When a card with an embedded RFID tag is in the vicinity of a reader, the reader sends out a radio signal to query this data record. This activates the tag, which then uses the energy of the radio signal to communicate its unique ID to the reader.

Burhan Gündüz, Global VP Secure Printing, ELATEC GmbH

In cooperation with:

LABOR PRAXIS