ELATEC
RFID Systems

SYSTEMATIC SECURITY AND TRANSPARENCY

Contactless authentication solution for cleanroom environments

Reliable access control is essential in cleanrooms as well as in laboratories to protect people, machines and data. Last but not least, it helps to prevent contamination of the environment by preventing unauthorized persons from gaining access. To meet the high demands associated with a cleanroom environment in terms of security and hygiene, a contactless authentication solution based on RFID and mobile technologies is ideal. Five criteria in particular must be taken into account when selecting the right reader.

Working in cleanrooms requires special knowledge from employees. This applies with regard to the strict hygiene regulations as well as to the handling of expensive and delicate equipment and sensitive materials that may be hazardous to health. But that's not all: 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, it must be ensured that only authorized and trained persons are allowed access to the rooms and to equipment and systems. Another key challenge is system security: machines, systems and peripheral equipment, as well as sensitive and valuable data, must be effectively protected against unauthorized access.

Smooth and secure user authentication with RFID and mobile technologies

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. This allows efficient and reliable control of access to laboratories and clean rooms, as well as access to sensitive machinery, equipment, supplies and substances. Single sign-on (SSO) for computer systems, networks and printers, as well as electronic signature authentication for manufacturing execution systems (MES) or laboratory information management systems (LIMS), can also be implemented. Another advantage is that processes can be documented reliably and with little effort, which makes quality management or the recording of working hours much easier.

An equally straightforward and inexpensive option for implementing user authentication and access controls is a badge equipped with an RFID tag—which most employees already carry in the form of an ID card or token. The use of wearables, for example in the form of wristbands, is also possible. When such a physical badge is held up to the reader, the authentication process takes place automatically. The authorized person is immediately granted access to the laboratory rooms and can smoothly access all computer systems or equipment for which he or she is authorized. Depending on the employee's qualifications, the authorizations can be easily and individually adjusted.

Another option is the use of digital credentials, so-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 no longer necessarily has to be actively held up to the reader for the authentication process (depending on the distance specified in the system). Both physical and digital credentials allow convenient, contactless and thus hygienic authentication.

If the work environment also requires strong two-factor authentication, RFID can be used in conjunction with password systems. A combination with biometric systems is also possible. One example is wearables that are linked to an employee's digital identity. When the employee starts work, the band is put on, and the employee places his or her finger on a fingerprint scanner once, thus activating the band. Later in the day, the band is simply held up to a reader that works with NFC or Bluetooth. In this way, authentication can be carried out quickly and without contact.

Five criteria for choosing the right reader

Universal readers are at the heart of modern access control systems. Particularly for use in clean rooms and laboratories, special requirements must be met—not least to ensure that legal standards are adhered to. Therefore, the following five aspects in particular must be considered when selecting the right system.

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 used in high-security labs or production environments should therefore support advanced encryption technology. Encrypted RFID or BLE/NFC signals are harder to intercept or counterfeit. Readers that are compatible with biometric methods (e.g., wristband) for two-factor authentication provide additional security.

Last but not least, employees must be protected by means of access control. After all, many materials used in cleanrooms and laboratories can pose a significant health hazard if used improperly.

Hygiene: Since any unnecessary touch point should be avoided in a cleanroom environment, a contactless authentication solution is the right choice. This eliminates the need to enter passwords or codes on shared keypads for access control. However, the strict hygiene standards in cleanroom environments necessitate further considerations when choosing the right reader. For example, the special requirements of GMP (Good Manufacturing Practice) environments do not usually allow the use of conventional readers. Devices built into simple plastic housings cannot be regularly treated with disinfectants or strong cleaning agents, as the housings are quickly damaged when aggressive substances are used and frequent cleaning cycles are performed. Particularly in clean rooms, this can even impair the work results, because a damaged housing poses the risk of released particles contaminating 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 the 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).

Flexibility: Dozens of different 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. Within these categories, however, different manufacturers' cards have their own unique formats. Organizations with multiple locations or existing user authentication and access control systems, in particular, should look to universal readers that are certified for global use and support a variety of technologies. Multi-frequency readers allow all transponder technologies that may be used currently or in the future in the company to be processed and are also suitable for smartphone authentication with BLE or NFC technology. They thus offer companies an all-in-one solution that reduces complexity and helps save time and costs. Reader models from solution provider Elatec, for example, which can process up to 60 common transponder technologies, are a good choice.

Future-proofing: Changes to operating systems, the use of new transponder technologies, or emerging security threats may make it necessary to update or reconfigure readers. It is therefore 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. This not only saves time and money, but also has the advantage that the clean room does not have to be entered unnecessarily by service providers. Readers should also be programmable to enable specific functions for sophisticated PC logon software and support mobile access control technologies. In this way, readers meet the needs of cleanroom operators and users over a long period of time.

Ergonomics: Last but not least, the ergonomic suitability of the readers should not be disregarded in such a highly regulated industry where employees have to authenticate themselves several times a day. An ergonomically suitable solution for the corresponding workplace should always be guaranteed. It is therefore advisable to choose a reader that is ideally available in different versions and thus covers a wide range of spatial and ergonomic requirements.

How RFID, BLE AND NFC work

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

Each RFID card has a unique set of data stored on it—for example, a number—which is used to identify the card and thus also the person carrying it. When a card with an embedded RFID tag is near an RFID reader, the reader sends out a radio signal to interrogate this data set. The signal activates the tag, which then uses this energy to tell the reader its unique ID.

Both NFC and BLE are technologies for contactless data exchange. Their main difference to RFID is that the information carriers (e.g., smartphones) are active radio transmitters and require a power source.

- NFC is based on high-frequency RFID technology (13.56 MHz) and enables contactless data exchange in near-field communication (<10 cm)
- BLE is a short-range radio technology for distances of up to ten meters in the 2.4 GHz frequency range

When smartphones are used for user authentication and access control, they act as card emulators and send a unique user ID to the reader.

Author:

Burhan Gündüz, Global VP Secure Printing

ELATEC GmbH, Zeppelinstr. 1, 82178 Puchheim, Germany

Phone: +49 89 552 9961 0, E-Mail: info-rfid@elatec.com

In cooperattion with