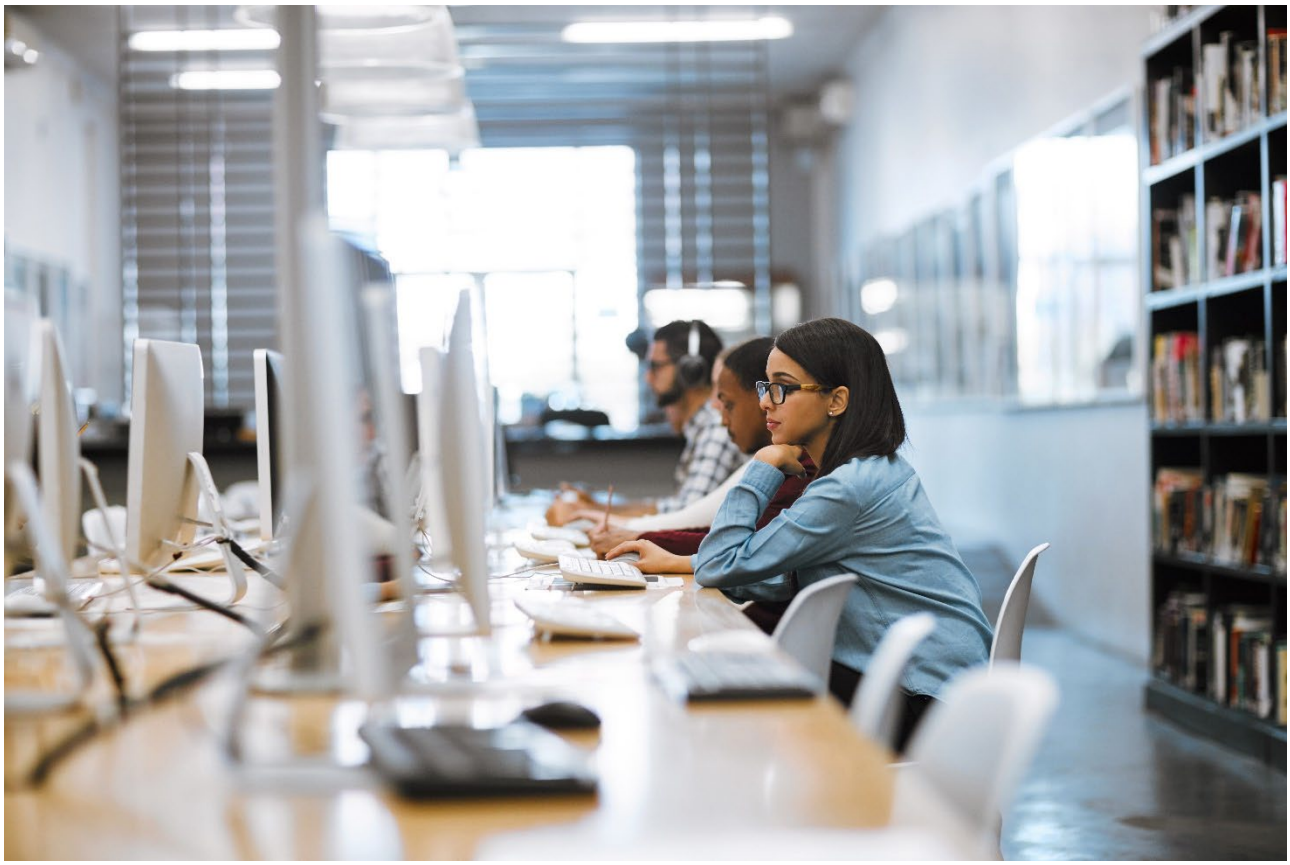
ELATEC
RFID Systems

BEST ACCESS TO EDUCATION

Modern authentication solutions for the smart campus



Universities are a living cosmos: thousands of students, faculty and staff learn, research, work and live in one place. A modern authentication solution based on radio frequency identification (RFID) and mobile technologies helps to provide all authorized persons with the required access and entry on campus. This ensures a smooth and secure day-to-day university life. To make sure that the implementation is a success, various aspects need to be taken into account.

The diverse groups of people at universities pose a challenge in terms of safety: there are numerous people moving around the campus, and they all go about different activities and have individual daily routines. Accordingly, they need access to various rooms and facilities on campus—from student dormitories to the library and offices. And this is best done via a contactless, and thus hygienic, solution. At the same time, the university itself deals with sensitive data such as research results or personal data such as grade transcripts, which may only be accessible to selected staff or faculty. In addition, the group of people on campus changes from semester to semester. To be able to map this complexity, technical support is necessary. This is provided by a modern, standardized access control system. It ensures that only authorized persons can enter rooms and gain access to services or sensitive information.

Access and entry: simple and under control

An entry and access control system must meet a number of requirements to address the complex needs of higher education institutions.

User convenience: The authentication process should be as simple as it is convenient for users. It should also minimize touch points—an aspect that has become significantly more important in recent years as a result of the pandemic. Ideally, a solution should cover all the applications that the various user groups need in everyday university life. For example, students can use lockers and printers, book workstations in the library that comply with distance rules, or visit university-owned sports facilities. Staff and faculty are given more extensive permissions, depending on their roles. These can allow them to use parking spaces, work in the lab, and log on to the university network via single sign-on with an individual authorization level—to name just a few options.

Security and flexibility: While "convenience" is the decisive keyword for users, other important aspects count for university management and campus IT when it comes to access control. The main focus here is on the security of people, buildings and facilities, and the protection of data. The system must also be flexible and future-proof. It should be compatible with existing solutions on the site, allow adaptations to changing requirements and legal regulations, and be able to process future technologies. In addition, the management of authorizations, from issuing to blocking, must be as simple as possible to implement.

Card, smartphone or both: everything is possible

A modern authentication solution works on the basis of RFID and digital credentials. The mobile credentials use the technologies NFC (Near Field Communication) or BLE (Bluetooth® Low Energy), with which a majority of all mobile devices are equipped. This means that both an RFID card and a smartphone can serve as contactless identification media—simply hold them up to the reader, and the way is clear for authorized persons.

Before implementing a uniform campus solution, however, the question of which technology should be used for authentication must first be clarified. This is because both RFID cards and mobile access authorizations offer advantages for use in the university environment. For example, ID cards in the form of student and employee IDs are already in use at many universities and can be used for applications of an access control system. As drivers of innovation, however, universities should also take advantage of the opportunities offered by digital transformation—not only in teaching, but also on campus. In this environment, smartphones are an optimal identification medium. On the one hand, the cell phone is a constant companion for students and teachers in everyday life, so that they always have credentials on their smartphone at hand—and, unlike student IDs, generally do not pass them on. On the other hand, the central and simple administration of mobile authorizations saves resources for campus IT. Maximum flexibility is offered by a hybrid solution that allows the parallel use of cards and smartphones for authentication. This means that the decision for an identification medium can be made individually for each application and person and can be easily adapted as needed.

Tips for successful implementation

To ensure that the introduction of an authentication solution based on RFID, NFC and BLE is a success, the following aspects must be given special attention during implementation.

Flexibility through universal readers

A variety of card technologies are available on the international market, each with its own data formats, communication frequencies and security functions. Within a university, therefore, student and employee ID cards with different technologies may be in use—especially if faculties are located at different sites. The ID cards are used, for example, for applications such as paying in the dining hall or checking out books. However, most readers are only capable of reading a few card technologies. A solution is offered by multi-frequency readers that are compatible with up to 60 transponder technologies commonly used worldwide. The universal devices, which the solution provider Elatec has in its portfolio, for example, use both RFID and the NFC or BLE technologies for authentication and access. This makes it possible to integrate mobile devices into the system, providing the greatest possible flexibility.

A modern authentication solution using multi-frequency readers allows seamless integration of different applications into the existing systems on campus. Examples include single sign-on for computers or the use of laboratory facilities. This simultaneously ensures uniform and time-saving administration as well as maximum user convenience.

Reliable protection of people and data

To ensure reliable protection of people, buildings, facilities, and data, the readers must be equipped to withstand physical manipulation as well as hacker attacks and support advanced encryption. Only then will they provide the level of security required for the authentication process. However, to effectively and holistically secure an RFID-based authentication solution, it is not enough to look at the reader alone. It is necessary to include the complete system in the company's security concepts.

Future-proof thanks to central remote maintenance

Requirements and IT infrastructures change over time and make adjustments necessary. Only with a flexible system that provides for optimizations, adaptations and upgrades will universities be on the safe side in the future. This is because there are hundreds of readers on a campus, distributed across the often sprawling campus or even different locations. Normally, updates would have to be laboriously applied by a technician to each individual device directly on site. If remote updates are possible, however, all installed readers can be updated easily and quickly from a central location, regardless of their location.

Author:

Burhan Gündüz
Vice President Secure Printing EMEA & Japan
ELATEC GmbH

In cooperation with: