ELATEC
RFID Systems

# SINGLE SIGN-ON APPLICATIONS FOR A NEW WORLD OF WORK

## Authentication solutions with RFID and mobile technologies

**Whether in companies, organizations or government agencies: the pandemic has permanently changed the way we work. When it comes to choosing a place to work, employees today can often make flexible decisions. But regardless of whether they are in the office or at home, data and networks must be protected against unauthorized access at all times and in all places. Single sign-on/PC logon systems that combine middleware with RFID (radio frequency identification) or smartphone-enabled technologies for user authentication can make an important contribution here.**

Many employees want to continue to benefit from the advantages of flexible, location-independent working in the future. According to a survey, 75% of participants would also like to have increased mobility in work in the future. Companies, organizations and even government agencies can seize their opportunity in the competition for the best minds by creating an attractive working environment. Simple, convenient processes that run just as smoothly in the office as they do when working on the move are a clear plus for employees. At the same time, access to data, networked devices and software systems must be protected in the best possible way at all times.

To simplify processes and reduce complexity for employees, single sign-on (SSO)/PC logon systems are a proven means. Single authentication allows employees to access all services, networks and files for which they are authorized. The benefits are obvious: single sign-on saves employees time and thus increases productivity. However, authentication in SSO/PC logon systems is often still done using passwords - with the familiar problems. For example, users often use particularly easy-to-remember passwords that can be easily guessed or compromised, or that fall into the hands of unauthorized individuals. It is true that the requirements for a secure, so-called "non-compromisable" password are clearly defined in the ISO 270001 standard for information security management systems. However, these are so comprehensive and complex that users can quickly develop a certain password fatigue. The common result: a makeshift solution where passwords are written down on a piece of paper and taped to the computer for all to see. However, the consequences of compromised or shared passwords can be severe, ranging from intellectual property theft and damage to an employer's image to fines for data privacy violations.

**Reliable and convenient authentication with SSO in combination with RFID and mobile technologies**

Alternatives to password authentication are available on the market. A secure and particularly convenient option for user authentication and access control is offered by an SSO solution that combines PC logon middleware with RFID or smartphone-based Bluetooth® Low Energy (BLE) or Near Field Communication (NFC) systems.

Here, 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.

Both options are easy for users to handle: RFID cards are already widely used for employee identification and building access control. The same cards can thus also be used for secure authentication as part of SSO/PC logon systems. The smartphone, always at hand, is also ideal for accessing corporate networks and resources. Whether card or smartphone, an SSO/PC logon solution of this kind works just as reliably in the office as it does when working on the move on a laptop. The simple authentication saves time during logon, reduces user password fatigue and thus increases security. Another positive effect is that it is always possible to track who has accessed which data and when.

However, it is not only users who benefit from switching to such an SSO/PC logon system. Companies in particular gain considerable advantages:

- Reduces the time spent on IT support due to forgotten passwords.
- The system contributes to the implementation of ISO 270001.
- The management of authentication systems can be centralized and thus simplified.
- Offers the possibility to secure all levels of access to systems without the need for multiple requests by the user.
- Access control information can be centralized for conformance testing to the various standards.
- Under certain conditions, companies can apply for government subsidies for the conversion to digital processes or digital transformation.

**Criteria for successful implementation**

When implementing an SSO/PC logon system that uses RFID, NFC or BLE for authentication, there are three aspects that require special attention to make the solution a sustainable success.

**1. 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. For companies and organizations, this means that employee badges with different technologies may be in use—especially if multiple locations are maintained worldwide. However, most readers are only capable of reading a few card technologies. One solution is offered by multi-frequency readers, which are compatible with up to 60 common transponder technologies worldwide and certified for use in up to 110 countries. The universal devices, which solution provider Elatec has in its portfolio, for example, use RFID for authentication and access as well as NFC or BLE. This means that mobile devices can also be integrated into the system, providing the greatest possible flexibility for users.

A modern authentication solution that uses multi-frequency readers allows seamless integration of different applications into an organization's existing systems. Thus, multiple applications such as SSO, access control or time-and-attendance can be integrated. This ensures unified and time-saving management as well as maximum user convenience.

**2. Reliable protection of networks and data**

The readers used must be equipped against both physical manipulation and hacker attacks and support advanced encryption for high-security applications. Only then is a secure authentication process a given. However, to effectively and holistically secure such an 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.

**3. Future-proofing in focus—thanks to remote updates and upgrades**

Requirements and IT infrastructures change over time. Only with a flexible system that provides for optimizations, adaptations and upgrades will organizations be on the safe side in the future. Readers should therefore have a robust open programming interface that makes them adaptable and thus future-proof. This makes it possible to program readers to provide key functionality for sophisticated PC logon middleware and to meet new requirements in the future that may be unknown at this point in time. Especially for SSO/PC logon applications, a central remote configuration option is essential and of decisive advantage. It allows all installed readers to be updated centrally and cost-effectively—regardless of their number and locations. This means that the same level of security can always be guaranteed when working on the move as on the computer in the office.

***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 from 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 nearfield 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
Vice President Secure Printing EMEA & Japan
ELATEC GmbH

In cooperation with:

IT-SICHERHEIT