ELATEC
RFID Systems

AUTHENTICATION SOLUTIONS FOR REMOTE WORK

Mobile Badge BLE+
Authentication successful
(Please wait a few seconds until next connection)
Can Advertise : ✓

The option of being able to freely decide where to work is a decisive factor for many employees when choosing a job today. If employers want to attract skilled workers, they must therefore create the conditions for convenient remote access and at the same time take measures to ensure the security of data and networks. Single sign-on (SSO)/PC logon systems that combine middleware with RFID (radio frequency identification) or mobile technologies for user authentication can make an important contribution here.

Better work-life balance is one of the benefits of remote work that helps companies create happier employees. But the fact that employees are not physically present in the office brings challenges in terms of cybersecurity. For example, when working on the go, it is not clear from the outset who is sitting in front of the computer. Therefore, checking the identity of employees—i.e., authentication—is particularly important in this case. Otherwise, there is an increased risk that unauthorized persons can access company data and networks.

SSO/PC logon systems are a proven measure to improve security by giving employees access to all services, networks and files for which they are authorized after one-time authentication. However, authentication is often still done via passwords, with known problems: users often use combinations of letters and numbers that are easy to guess.

Authentication with SSO in combination with RFID and mobile technologies

A secure and convenient alternative 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.

A reader is connected to or integrated into the computer or workstation and connected to the PC logon middleware. To gain access to networks, services and files, the user simply has to hold his or her ID card or smartphone, on which a digital credential is stored, up to the reader.

Both options are easy for users to manage. RFID cards are already widely used for employee identification and access control. The same cards can also be used for authentication as part of SSO/PC logon systems. The smartphone is also suitable as an identification medium, as it is always at hand. Such an SSO/PC logon solution works just as reliably in the office as it does when working on a laptop while on the move. The simple authentication also saves time during logon, reduces user password fatigue, and thus increases security.

In addition to the convenient handling for users, companies benefit from a conversion to such an SSO/PC logon system in other ways.

- It reduces the time spent on IT support due to forgotten passwords.
- The solution contributes to the implementation of an information security management system according to ISO 270001.
- The management of authentication systems can be centralized and thus simplified.
- It provides the ability 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.

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:

1. Flexibility through universal readers

A wide range of card technologies is available on the international market, each with its own data formats, communication frequencies and security functions—accordingly, employee ID cards with different technologies may be in use within a company. It is therefore advisable to use multifrequency readers that are compatible with up to 60 transponder technologies commonly used worldwide and certified for use in up to 110 countries. The universal devices, which the solution provider Elatec, for example, has in its portfolio, also offer the option of integrating mobile devices into the system. This provides the greatest possible flexibility in the selection of transponder media, in that future needs and requirements can also be mapped.

An authentication solution that uses multi-frequency readers allows seamless integration of different applications into an organization's existing systems. Thus, multiple applications such as access control, kiosk systems or secure printing 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. To effectively and holistically secure such an authentication solution, it is necessary to include not only the readers, but the complete system in the company's security concepts.

3. Focus on future security
Only with a flexible system that provides for optimization, adaptations and upgrades are companies on the safe side when the requirements for the IT infrastructure change. 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 important functions for sophisticated PC logon middleware and to meet new requirements in the future. Especially for SSO/PC logon applications, a centralized remote configuration option is essential. It allows all installed readers to be updated centrally and cost-effectively—regardless of their number and location.

Author

ELATEC GmbH

Zeppelinstr. 1

82178 Puchheim, Germany, Phone: +49 89 552 9961 0, E-mail: info-rfid@elatec.com

In cooperation with

IT-SICHERHEIT
Magazin für Informationssicherheit und Datenschutz