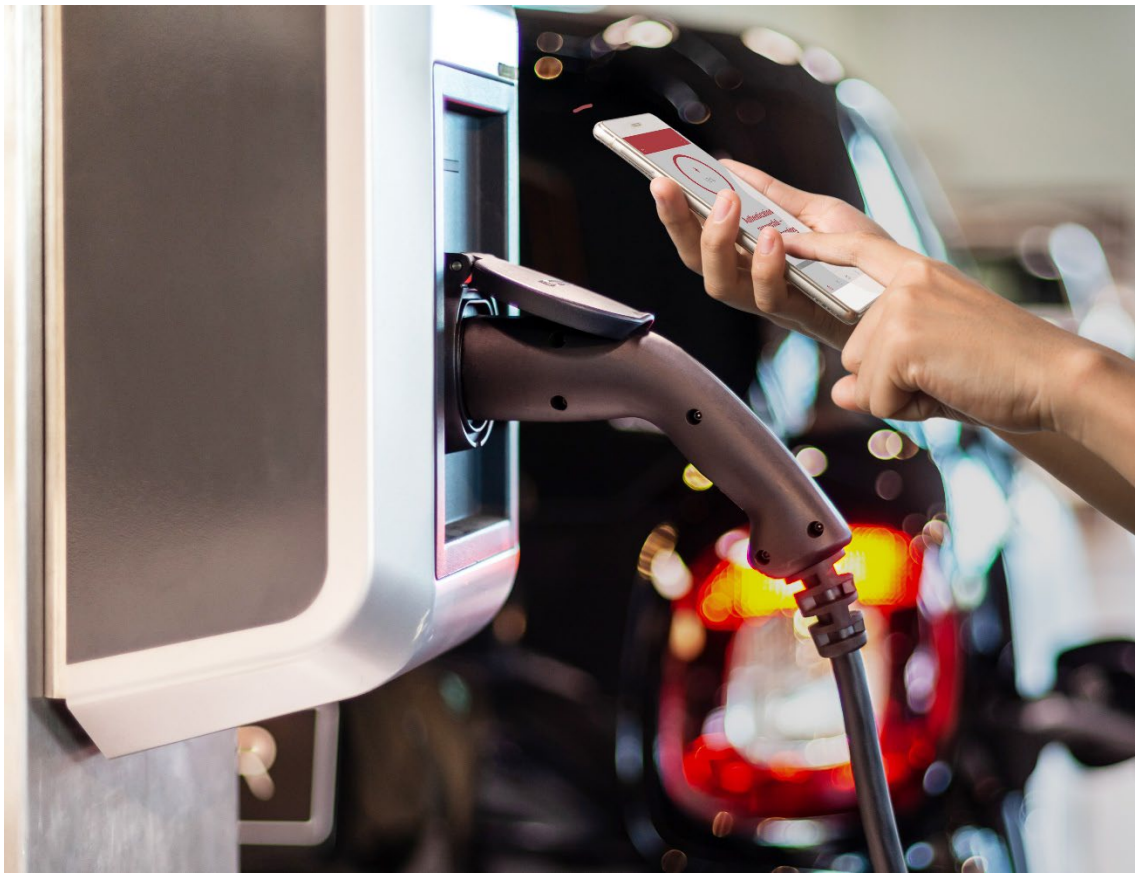
ELATEC
RFID Systems

THE FUTURE OF SECURE CHARGING

Modern authentication solution for EV charging



As the number of electric vehicles grows, so does the need for high-performance charging infrastructure—including a reliable authentication solution that can be used to manage both access to charging stations and billing simply and securely. RFID (Radio-Frequency Identification) and mobile technologies such as NFC (Near Field Communication) or BLE (Bluetooth® Low Energy) are particularly suitable for this purpose. But in a rapidly changing industry, the requirements for an authentication solution can change quickly. To ensure that their choice is sustainable and future-proof, operators and manufacturers of charging infrastructure must therefore consider important points.

The refueling of electric vehicles with electricity should function safely and conveniently. To ensure this, operators of charging stations—whether public or private—must consider a number of elements that depend on many individual circumstances. Who is allowed to use the charging facility? How is billing done? And how is the traceability of the charging process ensured?

User authentication, access restriction, and billing model requirements vary by application. Options range from membership programs to free offerings. For example, fleet vehicles can be charged using employee ID cards so that only authorized users have access to the charging options and a secure charging process is ensured. For internal billing purposes, it is necessary in this case to track who has used the charging column, when and for how long. Companies such as movie theaters or shopping malls that use charging stations as an additional source of revenue, as well as large network operators that offer charging options on expressways or highways, must offer their customers convenient access and transparent billing models that work via credit card or smartphone app.

Original equipment manufacturers (OEMs) must adapt their offerings to the requirements of operators and users. This is true not only in terms of the charging technology with which the charging station operates, but also in terms of the options for access control and user authentication.

Challenges of integrating an authentication solution for OEMs and operators

Whether employees, tenants or fleet drivers—operators of charging infrastructure need to know who is accessing their service, regulate access to charging infrastructure, and ensure that data security is maintained at all times. Operators depend on an authentication solution that ensures maximum security of sensitive, personal user data. This is especially true for authentication and access control solutions for metered charging stations; without encryption, there is a risk that signals exchanged between the card and the reader, such as account data, could be intercepted and misused.

If charging station manufacturers offer their products across regions or even countries, they must take into account that the market for charging infrastructure is highly fragmented: for example, in terms of technical specifications and data protection laws. Especially when integrating authentication and access control solutions, it is important that the chosen solution simplifies charging station management. If a large number of readers have to be updated on-site in a large-scale, possibly nationwide charging network, an update or reconfiguration can involve considerable time and financial effort.

Users of the charging infrastructure may also have different card or mobile technologies in use. This is because a large number of transponder technologies are available on the international market, each with its own data formats, communication frequencies and security functions. However, most readers are only capable of reading a few card technologies. This means OEMs looking to increase their market opportunities may need to stock different readers for different customers. It can also be a challenge for charging network providers that have stations in multiple regions or countries to find a reader that is certified for use in all target markets and supports all the technologies preferred in each location.

Last but not least, market requirements and legal regulations are also constantly changing. Smartphone-based solutions are becoming increasingly popular and are replacing the classic card in many areas and application scenarios. However, most readers can only be upgraded and adapted to current customer needs to a limited extent and would therefore have to be replaced at great expense as technologies and functionality requirements change.

The solution: authentication based on RFID and mobile technologies

A simple, convenient and secure option for user authentication and access control is provided by a modern authentication solution based on RFID and mobile technologies. At public and private charging stations, users can be uniquely identified with either an RFID card or a token. It is also possible to use digital credentials, also called mobile credentials. These are based on the NFC or BLE technologies with which a large proportion of all mobile devices such as smartphones are equipped. The use of such authentication protects charging stations from unauthorized access and ensures that sensitive information such as users' payment data does not fall into the wrong hands.

All users need to do is simply hold their credentials in the form of a card or smartphone up to the charging station. The integrated reader then enables secure, hygienic and contactless access to use the charging infrastructure—without the need for credit cards or passwords and PINs that are difficult to remember.

Make access control and user authentication sustainable and secure: This is what you need to consider

If operators and manufacturers want their charging infrastructure to be advanced, flexible and secure in the market, the authentication solution should meet the following criteria:

Security for infrastructure and data: An access control solution with authentication increases the level of security. It protects against misuse—both in terms of data and the valuable charging infrastructure. This is because only authorized users with their ID cards or smartphone credentials are given the opportunity to fill up with electricity. Their charging behavior can also be easily tracked. To increase data security, a reader should be programmable to support encryption technologies, including cryptographic methods that require high computing power. Appropriate devices allow manufacturers or operators to use customized encryption methods and other complex functions.

Flexibility and complexity reduction: The challenges posed by the highly fragmented market for charging infrastructure and the multitude of common transponder technologies can be met by operators and manufacturers with multi-frequency readers. Universal readers are available on the market that can process more than 60 common transponder technologies worldwide and are certified for use in up to 110 countries. These readers, which solution provider Elatec has in its portfolio, for example, are compatible with virtually every card technology and can also process mobile credentials. This makes them ideal for use in EV charging applications. Thus, with a single, easy-to-integrate device, they provide a solution that simplifies distribution and inventory management. For manufacturers, this means they only need to stock one version of their system for all potential customers. Complexity is significantly reduced with such a solution.

Future-proofing through remote updates and upgrades: Requirements and IT infrastructures change over time and make adjustments necessary. Only with a flexible system that provides for optimizations, adaptations, and upgrades will providers and operators of charging infrastructure be on the safe side in the future. The possibility of remote configuration of the readers is, therefore, a must in the field of charging infrastructure. This enables operators and OEMs to react quickly to changing IT infrastructures and requirements and to carry out optimizations, adaptations and upgrades without any problems. With remote updates and upgrades, all installed readers can also be updated easily and quickly, regardless of their location, without incurring high costs for technicians.

Conclusion

Not only large corporations and government agencies with their own fleets, but increasingly also small businesses and rental companies are expected to drive the expansion of the charging infrastructure in the coming years. Operators and OEMs that rely on a secure, scalable authentication solution that can be applied across markets have a clear advantage and a chance to make a decisive contribution to a stable charging infrastructure.

How RFID, NFC and BLE 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

A unique data record—for example, a number—is stored on each RFID card, which 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 an RFID reader, the reader sends out a radio signal to interrogate the tag. The radio signal activates the tag, which then uses the energy of the radio signal to communicate its unique ID to the reader.

- Both BLE and NFC 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 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.

Johannes Weil
Head of Industry Team Europe,
Elatec GmbH, Puchheim
info-rfid@elatec.com

In cooperation with:

Internationales Verkehrswesen