# Use Case: Secure, Contactless Access to Electric Vehicle Charging Services

To increase security, the closed-loop smartcards used by electric vehicle (EV) drivers to access EV charging services are upgrading to asymmetric cryptography. NXP's MIFARE DUOX IC combines asymmetric and symmetric cryptography on a single chip, enabling a cost-effective way to support secure authentication and offline signature validation for end-user authorization on EV charging terminals.

**Target Applications**

- Residential Charging (private home)
- Public Charging (along public roadway)
- EV Roaming (access to networks from different providers)
- Workplace Charging (on-site at company premises)

## Challenge

In today's infrastructure for EV charging, many charging stations support the use of contactless smartcards, also called RFID mediums, so drivers can stop and start the charging process, make payments, and register data about the charging session with a simple NFC-based tap.

Using smartcards at charging stations adds convenience to EV ownership and helps promote wider adoption of EVs. It also makes it easier for charging networks to provide individual drivers and fleet operators with data-driven insights that help monitor vehicle safety and manage power consumption for greater sustainability.

### Secure user authentication at the charging station

There are, however, concerns over security. In some cases, the charging station relies on the contactless smartcard's unique identifier (UID) for authentication, without adding any security measures, which is a practice that is vulnerable to fraud, including the use of cloned or fake smartcards. The UID of a contactless smartcard uniquely identifies the card, and is programmed into the smartcard chip during manufacturing. Essentially it is a serial number to uniquely identify the smartcard. Mentioned UID is required to ensure uniqueness and links the credential to an EV driver through the EV charging provider's backend system. The user's account is linked to the UID when the smartcard is issued and is used to look up the user account for every charging session. Since the UID can be easily retrieved in plaintext, relying solely on it for authentication poses a high security risk, as hackers can clone the credential, by simply copying the UID, and charge at another driver's expense. Copying a single credential may not yield significant damage for the Electro Mobility Service Provider (eMSP) or Charge Point Operator (CPO), but it can yield a major financial damage for the impacted user. The picture changes dramatically, when thousands of UIDs may be affected, as for example via UID guessing. Fraudsters who are in the possession of one valid UID which is accepted in the EV charging network, can try to guess other valid UIDs by simply brute forcing numbers close to the one valid UID. Once fraudsters have access to a higher number of valid UIDs, they can be abused for credential cloning by utilizing devices like RFID emulators, which are available quite inexpensive in the market. Some examples include devices like Flipper Zero, Chameleon Ultra, iCopy-X or Proxmark.

In other cases, to increase the security compared to the UID-only approach, there is an additional authentication step implemented between the EV charging station and the NFC smartcard. The authentication step uses symmetric cryptography, which is a step up in terms of protection, as symmetric encryption is robust, fast and efficient, but still subject to its own set of limitations and vulnerabilities within complex EV charging infrastructures. Symmetric key encryption is a method of encryption that uses the same key for both encryption and decryption. This means that both sender and receiver need to know the same key. All parties within the system must possess the same symmetric key to encrypt/decrypt data or perform valid authentication between the EV charging terminal and smartcard. Due to the requirement for all involved entities to use the same symmetric key, key management complexity increases, particularly when scaling to larger numbers.

A symmetric key should never be shared publicly and must be kept secure at all times. Effective key management is a crucial aspect of symmetric key handling, encompassing key generation, storage, distribution, rotation, and revocation in a secure and efficient way. The process becomes increasingly complex as more entities are involved. Symmetric key management is effective when there is a manageable number of parties who agree on a strong security framework. However, in scenarios involving a large number of entities, such as complex EV charging ecosystems where numerous companies collaborate for EV roaming and electricity sharing, the risk associated with key management and distribution increases. The entire system can be compromised if any entity mishandles the symmetric key, leading to potentially severe consequences.

## Solution

Concerns over security have, in recent years, led to various efforts to address security in smartcard-based EV charging. One of the most prominent and widely supported of these efforts is the VDE-AR-E 2532-100 application rule. Issued by VDE, a non-profit service organization concerned with the generation, distribution, and safe use of electricity, and the DKE German Commission for Electrical, Electronic & Information Technologies, the VDE-DKE guidelines aim to prevent unauthorized charging and fraud in the charging ecosystem by upgrading to asymmetric cryptography.

## High security with asymmetric cryptography

Asymmetric cryptography provides greater protection than the UID-only approach and more flexibility than symmetric cryptography on its own. With asymmetric cryptography, security is ensured by pairing a public key, which can be distributed openly without compromising security, with a private key that must be kept confidential. This keypair approach can enable stronger authentication of the smartcard and use of digital signatures for stronger protection of digital transactions.

Bringing a higher level of security to EV charging applications addresses concerns over fraud, counterfeiting, and data integrity. It also expands the opportunities for multi-application smartcard use, with support for functions beyond EV charging, such as micropayments, secure car access, parking access, and more.

The VDE-AR-E 2532-100 application rule is designed to be a simple, cost-effective upgrade for the manufacturers of charging systems. The upgrade involves an extension of the charging station's reader firmware, not hardware, so the charging equipment's bill of materials can remain the same. The software upgrade requires the EV charging station to be able to handle asymmetric cryptography, public keys and certificates, which is required for reading out the smartcard's dynamic signature and its validation. The upgrade can also be implemented in a "backward-compatible" mode, so the charging station can continue to accept existing cards, which have been issued earlier and still rely on reading out the UID only. Alternatively the software extension can be implemented in the EV charging backend system which means that no software upgrade at the NFC interface of the charging station's reader is required, making it even easier to roll out this solution.

What's more, the transition to VDE-AR-E 2531-100 can be gradual, so manufacturers can plan their rollouts in the way that makes the most sense for them, offering highest possible flexibility.

## Secure user authentication in compliance with EV charging regulations

To support easy implementation of VDE-AR-E 2531-100, NXP offers MIFARE DUOX, combining asymmetric and symmetric cryptography on a single chip, enabling simplified key management and fast asymmetric authentication for EV charging applications. MIFARE DUOX provides security for the NFC-based EV charging communication to ensure secure end-user authentication while enabling interoperability, ease of deployment and flexibility.

MIFARE DUOX for EV charging follows the VDE-AR-E 2532-100 specifications, with built-in support for end-user authentication and authorization in EV charging systems. Utilizing the asymmetric cryptography and public key infrastructure (PKI) capabilities of MIFARE DUOX enables interoperability between multiple CPOs and eMSPs. This provides substantial benefits to end-users, as a single smartcard can be utilized across various EV charging systems, offering maximum interoperability and optimal suitability for EV roaming scenarios.

MIFARE DUOX for EV charging is available as a ready-made product with a pre-configured card structure consisting of an on-chip application, keys, and certificate for EV charging applications, as specified by VDE-AR-E 2532-100.

Deploying cards based on MIFARE DUOX is made even easier as NXP pre-loads the required card layout, application structure, configuration settings, as well as the chip-unique asymmetric key pairs and security certificate. NXP acts as the Certificate Authority (CA) for the EV charging certificates and keys and, pre-loads certificates and keys unique to each chip into MIFAER DUOX ICs during manufacturing. The EV charging root certificate and public key can be retrieved freely from the NXP EV charging CA, and injected in all EV charging reader terminals which want to accept MIFARE DUOX smartcards. This ensures that MIFARE DUOX can work seamlessly in any EV charging infrastructure that supports VDE-AR-E 2532-100 and the related implementation for unilateral asymmetric authentication, which is based on a real-time dynamic card generated signature verification, on the reader terminal.

## Learn more

To dive deeper into the VDE-AR-E 2532-100 application rule for EV charging and how this concept can be realized with MIFARE DUOX, please have a look at our application note.

**nxp.com**