Whitepaper

Secure User Identification and Authorization in EV Charging Applications

Introduction

As electric vehicle (EV) adoption accelerates, the pressure on charging infrastructure grows. Millions of new customers will rely on an expanding network of public and private charging stations, which are increasing in number and improving in technology. While fast, convenient and secure access to these charging stations is crucial, there remains a worrying issue with user authentication. Many systems are inadvertently using insecure practices, relying on smartcards' unique identifiers (UIDs) to authenticate users, which can leave drivers vulnerable to fraud and operators exposed to risk. This paper explores the critical need for secure user identification in EV charging and shows how new standards and technologies offer a safer, more scalable path forward.

Protecting your valuables is a natural instinct. Take your home as an example, you go to great lengths to ensure that it's safe and secure. At the very least, you take the most basic precaution of having a front door. So, let's say you choose a very robust door, with advanced security and multiple locks and levers. But when it's delivered, you choose to simply hang the door on the frame, leaving locks and alarms untouched and uninstalled. Anyone wanting to get into your house simply has to know the number on your door, then walk right in.

This extreme illustration isn't as far-fetched as you might think. Worryingly, it's not uncommon for businesses to adopt a tool for its security features, then only use a fraction of its protective potential. It's happening right now in user identification and payment capture for EV charging.

The market for electric vehicles continues to expand, driven by growing demand, environmental regulations and governmental incentives. In 2024, EV sales rose more than 25% year-over-year to more than 17 million vehicles, with total numbers expected to reach around 350 million by 2030. The International Energy Agency predicts that the global EV fleet is set to grow twelve-fold by 2035, by which time estimates indicate up to 60% of vehicles sold globally will be electric.

In parallel with this ongoing growth, there is an urgent need for an improved charging infrastructure to accommodate the expected millions of EV drivers. As battery technology continues to evolve, travel ranges will extend and new chargers will recharge batteries faster, further driving consumer interest in EVs. The European Automobile Manufacturers' Association (ACEA) estimates that 8.8 million charging stations will be needed by 2030, while the European Commission calculates 3.5 million public charging stations will be required to meet targets of 55% CO2 reduction for new cars. A recent ACEA report indicates a strong correlation between EV sales and the availability of public charging stations, namely that people are more likely to buy an EV when they feel adequately supported by charging opportunities. But there is ongoing concern from consumers about range anxiety and the lack of fast-charging stations, further feeding the need for an effective, efficient and trustworthy charging infrastructure.

Increasingly complex market with interwoven interests and players

The global EV charging infrastructure market was valued at USD $25.83 billion in 2023 and is projected to grow at a compound annual growth rate of 25.4% from 2024 to 2030. There are multiple players within this multi-billion-dollar EV charging ecosystem. Each stakeholder has their own priorities, concerns and perspectives, with few having the capacity or expertise to maintain a complete overview. From the EV OEMs with their own charging networks, to the oil and gas companies diversifying into this high opportunity market, to the equipment manufacturers, charging stations and network operators. Among the many challenges that they face, building enough chargers to serve consumers is just one. Companies are investing heavily into electrical grid development, focusing on smart energy management and distribution, time-of-use electricity tariffs, real-time electricity pricing, grid load monitoring and balancing. At the same time, they are creating individual apps, smartcards and tokens for charging, increasing complexity for drivers simply looking to charge their vehicle.

Charge Point Operators (CPOs): Responsible for the physical operation, maintenance and expansion of EV charging networks. They deploy and manage charging hardware and rely on back-end systems – Charge Point Management Software (CPMS) – for operational oversight, load management, and analytics.

eMobility Service Providers (eMSPs): Provide the front-end service layer, managing user subscriptions, payment, billing and customer support. The eMSPs often issue smartcards or mobile apps to EV drivers for authentication and payment at charging stations.

Original Equipment Manufacturers (OEMs): Many car manufacturers, including Tesla, VW, Mercedes, Ford, Renault and BMW, now act as both CPOs and eMSPs, bundling charging services with vehicle purchases.

Electric Vehicle Supply Equipment (EVSE) Manufacturers: Develop charging hardware and associated technology.

Roaming Network Operators (RNOs): Facilitate network interconnectivity between CPOs and eMSPs. This enables cross-network charging access, also known as EV Roaming, through interoperability agreements.

How smart charging is enhancing user experience

CPOs, eMSPs, EVSEs and RNOs are responsible for ensuring that visits to charging stations are smooth and convenient, delivering uninterrupted charging with reliable and secure payment. Thanks to a EU 2024 regulation called the Alternative Fuels Infrastructure Regulation (AFIR), operators of public charging stations are now obliged to implement smart charging, with links to a backend system. Most EV charging stations connect directly to the energy grid, from where they channel electricity directly into the vehicles that hook up to them. Smart chargers are the successors of the basic or standalone chargers seen in older or local systems. In smart charging, each charging station is remotely managed through a cloud-based system and Charge Point Management Software (CPMS). This gives the CPO a clear overview of all stations, their operational status and load, allowing remote management and load balancing. This ensures that the available electrical power is shared intelligently across multiple EVs, avoiding overload and maximizing charging efficiency.

Extending availability with EV Roaming

Smart chargers and the remote CPMS used to manage them, give clear oversight of the network for CPOs. More importantly for drivers, this also offers real-time visibility of available charging points. Thanks to agreements between partners in the charging ecosystem, this visibility can extend outside drivers' home region and usual supplier. With EV Roaming, drivers enjoy a much broader availability, expanding their charging options across regions and providers.

EV Roaming is made possible by protocols including the Open Charge Point Protocol (OCPP) and the Open Charge Point Interface (OCPI). It allows EV drivers to access and use charging stations operated by other networks, with one NFC-based smartcard for authentication and payment. It should also reduce drivers' need for multiple charging cards, apps and subscriptions, although current methods of identification, authentication and authorization are not without problems.

While the technologies behind user authentication and payment processing are relatively long-established, their implementation within the EV charging ecosystem has revealed some security gaps. EV drivers need charging convenience, speed and availability, combined with payment ease and security. With multiple CPOs and eMSPs issuing proprietary cards and apps, drivers face the prospect of juggling many cards and swiping through too many apps to find the correct one. Each card and app holds sensitive information, with customer identification on the smartcard linking to subscription and payment details on the backend. Unfortunately, the inconvenience of dealing with multiple cards and apps is compounded by the way legacy smartcards are being used, often with unsecured NFC communication between the charging station and smartcard.

Payment methods for EV charging services

Payment with contactless smartcards: There are three common methods of user authentication and payment for EV charging: contactless smartcards, bank/credit cards and smartphone apps. Each method has its draws and drawbacks, with the most popular choice being contactless smartcards. These are generally Radio Frequency Identification (RFID) cards issued by eMSPs, linked to a user account in the eMSP backend system. This is connected to the customer's preferred payment method, credit card or bank details. The eMSP user account will track usage, subscription details and any service bundles the driver has activated. As verified registered customers of the eMSP, drivers can benefit from discounts and special loyalty deals such as discounted rates. These are tracked through their account with the eMSP, accessed using their smartcard. Each card holds an NFC/RFID chip, so drivers can simply tap the card against the reader at the charging station to initiate the authentication process. After they are identified as a registered customer of the eMSP, the charging session can be authorized and charging begins.

The technology in this card makes it possible to securely encrypt the information exchanged between smartcard and reader, though this functionality is not always implemented. In addition, since the NFC/RFID chip is a passive unpowered device, the card can never run out of power, unlike a smartphone. And unlike a smartphone app, this chip does not need internet connectivity to function.

Payment with debit/credit cards: Europay/Mastercard/VISA (EMV) is another payment method accepted by many charging stations. Drivers can use EMV cards to access charging stations without a subscription to an eMSP, but this means that they have no access to the reductions, loyalty schemes and vouchers often associated with eMSP subscriptions. As a result, costs of EMV charging can be higher.

Payment with smartphone apps: Increasingly offered as a convenient and flexible payment option, smartphone apps give the driver a seamless overview of charging stations availability, navigation, charge history and cost. As with contactless smartcard payment, the app is linked to a user account. Charging can be initiated via NFC with a tap on the charging station, via a QR code or through the app. A caveat of this method is its reliance on a working internet connection and sufficient power in the phone to both start and stop the charging session.

The threats of smartcard UID misuse, a universal problem in EV charging

Most public EV charging systems today rely on contactless smartcards to identify users and authorize charging sessions. However, in the main, these cards are used in a very basic (and incorrect) way, with the system relying only on the card's unique identifier (UID). This number is a fixed value embedded into the chip at point of manufacture and was only ever intended to serve as a differentiator between cards. Tapping a card to a reader initiates an 'anti-collision protocol' as part of international standard ISO/IEC 14443-3. This establishes a communication line between card and reader, preventing chaos when two cards are tapped simultaneously. This was the only purpose of the UID, to function as a differentiator, a serial number.

Unfortunately, lax or uninformed practices have led to the common use of UIDs as the single means of user identification in EV charging systems. This is made more unfortunate by the fact that these NFC chips typically have dedicated data fields reserved in memory specifically for the purpose of user identification. In addition, those reserved data fields can be further protected by layers of secondary security such as cryptographic encryption.

The fact that only the very simplest aspect of the chip, its most basic identifier, is being used as a sole method of user identification, is cause for concern. In essence, this is the same as choosing a new door for your house, installing a robust model with advanced security, then leaving the door open with locks and alarms untouched and inactivated. The only requirement for intruders to access your house is knowing the number on your new front door.

Today, attackers can easily retrieve the UID of an NFC chip as plain text using simple tools. They can then clone this number to a blank RFID card and use that cloned card to initiate charging sessions at another driver's expense.

Why aren't there security measures in place to prevent this? There are. Unfortunately, they are not commonly used, and with continued EV market growth, this could become an even greater security risk, exposing consumers to fraud and risking the reputation and trustworthiness of underprepared eMSPs and CPOs.

Robust solutions leveraging secure cryptography

The primary purpose of smartcards is to leverage the technology for storing and processing data securely, protecting end users' information confidentially and with

integrity. Current methods are not making full use of this functionality, due in large part to the mistaken belief that the UID is a security feature rather than a serial number. The solution lies in the implementation of cryptography as an additional authentication step.

Symmetric cryptography: Symmetric cryptography can be used to establish mutual authentication between the EV charger and the smartcard. One method involves a three-pass protocol using AES-128 or AES-256 encryption. Here, the card and reader prove possession of the same secret key by sharing encrypted versions of random numbers. The only way to show the same result is if both parties have the same symmetric key. In this way, the key itself is never transmitted, a method which prevents eavesdropping and replay attacks. Once authentication is successful, user-specific data can be securely exchanged over an encrypted channel and the charging session authorized. With symmetric cryptography of this type, the same key must be known by all authorized parties in the chain. CPOs, eMSPs and RNOs all have the same key and must handle it securely at all times, from key generation to storage, distribution to rotation and revocation. As the number of authorized parties grows, complexities increase and risks follow, since one leak from anywhere in the chain compromises the entire operation.

Asymmetric cryptography: As an alternative, asymmetric cryptography introduces greater flexibility. It uses a keypair (one public, one private) so that the public key can be freely distributed, while the private key remains securely stored in the card. In a card-unilateral asymmetric authentication, the reader sends random data, the card signs it using its private key and the reader verifies it with the public key. This real-time, dynamic signature verification ensures card originality and user authenticity and prevents cloning, spying or replay attacks. Once validated, user data can be securely exchanged.

VDE-AR-E 2532-100 enhances EV charging with asymmetric cryptography: VDE is a nonprofit German organization devoted to the generation, distribution and safe use of electricity. Its recent application guide VDE-AR-E 2532-100 is widely supported as a simple and cost-effective upgrade to introduce asymmetric cryptography to EV charging. By verifying the authenticity of each card using secure digital signatures, a system using VDE-AR-E 2532-100 can detect fraudulent credentials and block them from starting a charging session. The guideline outlines secure, interoperable authentication using RFID/NFC-based smartcards for new and existing charging stations. For existing charging stations, upgrades to asymmetric cryptography can be implemented using software in a straightforward manner. In both cases, VDE-AR-E 2532-100 guidelines open the way to secure EV charging and EV Roaming, with compatibility across different systems and networks. Finally, drivers will be able to use a single secure card to access multiple networks and providers, with no risk of card cloning or vulnerabilities seen in current systems.

Secure and compliant single-chip solution for EV charging: NXP offers a contactless NFC chip that is fully aligned with the VDE-AR-E 2532-100 guideline. The MIFARE DUOX smartcard IC combines both symmetric and asymmetric cryptography on a single chip, in a standards-compliant solution that is tailored to meet the needs of the EV charging market. MIFARE DUOX for EV charging enables secure end-user authentication and authorization, using asymmetric key pairs and real-time digital signature verification.

Each chip is pre-configured with a unique EV charging application, keys and certificate, in accordance with the VDE-AR-E 2532-100 specification, simplifying rollout and ensuring interoperability across multiple networks. By using public-key infrastructure, MIFARE DUOX avoids the complexities of symmetric key sharing, thus accelerating and simplifying secure deployment for CPOs and eMSPs.

To minimize disruption and optimize rollout, MIFARE DUOX can be incorporated into the EV charging system with no hardware changes to the charging station or reader. Support for the functionality specified in VDE-AR-E 2532-100 can be implemented through a software update, either at the charging station or backend service. At the charging station reader, a firmware upgrade can introduce support for the necessary cryptographic functions and NFC commands. Or this can be implemented through the connected backend service. MIFARE DUOX is also compatible with systems still relying on UID-only identification. This allows manufacturers and stakeholders further flexibility to plan their path to more secure user authentication.

Addressing concerns with a ready-made solution

Taking steps to increase the security of user authentication and payment in EV charging applications will address the growing concerns about fraud, counterfeiting and data integrity. MIFARE DUOX brings security, symmetric and asymmetric cryptography to both future and legacy systems, as part of a single smartcard that can be accepted across multiple networks. Bringing EV drivers the flexibility, simplicity and security they need, improving user experience, while adding a robustly secure and future-proof foundation for EV charging operators.

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.

For more information please visit:
nxp.com/products/MIFARE-DUOX

[1] Global EV Outlook 2024, iea.org/reports/global-ev-outlook-2024, pp 104.

nxp.com/MIFARE