33rd Electric Vehicle Symposium (EVS33)
Portland, Oregon, June 14 - 17, 2020

NEMA EVSE 1 A Charging Network Interoperability Standard - A Contactless RFID Credential for Authentication

Steve Griffith, Industry Director, PMP

National Electrical Manufacturers Association (NEMA), 1300 North 17th Street, Arlington, VA 22209,
Steve.Griffith@nema.org

Summary

This NEMA standard describes a protocol for authenticating EV charging service requests using contactless proximity Radio Frequency Identification (RFID)–type credentials. Authentication provides assurance to the Electric Vehicle (EV) charging network that the EV driver is the correct authorized party incurring a financial or other obligation for the services to be rendered. Similarly, the EV driver can have confidence that transactions have not been authenticated using forged or fraudulent credentials.

Keywords: electric vehicle (EV), charging, infrastructure, interoperability, standardization, authentication, radio frequency identification (RFID)

1 Scope

This standard describes a protocol for authenticating EV charging service requests using ISO/IEC 14443 contactless proximity Radio Frequency Identification (RFID)–type credentials. Authentication provides assurance to the Electric Vehicle (EV) charging network that the EV driver is the correct authorized party incurring a financial or other obligation for the services to be rendered. Similarly, the EV driver can have confidence that transactions have not been authenticated using forged or fraudulent credentials. Authentication is also an important prerequisite in making access control decisions when other policy considerations need to be applied. The protocol specified in this standard enables secure and trustable EV charging service transactions to take place for both the service provider and the service consumer.

The method of EV driver authentication involves the use of an ISO/IEC 7816-4/5/8–based challenge-response application layer protocol and ISO/IEC 14443 contactless communication. EV drivers (also referred to as users) can hold the contactless authentication credentials in proximity to EV charging stations to authenticate, authorize, and receive EV charging services. The authentication credentials can be implemented in wallet-sized cards, mobile phones, key-fob tokens, or other physical form factors. Contactless authentication devices compliant with this standard on EV charging stations interact with authentication credentials to obtain unique and verifiable challenge-response data ascribing to the authenticity of the credentials. The challenge-response data are then sent to and validated by the credential authenticators in an online manner to confirm that the authentication credentials have not been impersonated (or otherwise compromised) and that the authentication credentials are in good standing (i.e., not declared lost or the associated account overdrawn).

The authentication credential and protocol defined by this standard applies to intra-network operation, as well as operation across inter-networked, multi-operator EV charging networks—with the principal difference in the latter case that authentication takes place at the foreign EV charging network responsible for issuing the credential, rather than at the local network. It is expected that participating networks will issue credentials compliant with this standard to enable their users to receive on-network and off-network EV charging services. By defining an industry standard authentication credential, service interoperability and roaming is made possible enabling EV drivers to receive charging and other services among compatible equipment and participating networks.

In subsequent sections of this document, the data objects and messages exchanged between the authentication credential, the authentication device, and the credential authenticator are described. These sections give the syntax and semantics of the data objects, along with the sequence of command and response message exchanges using ISO/IEC 7816-4/5/8 Application Protocol Data Units (APDUs). The challenge-response protocol is described, and a method of authentication data validation with the credential authenticator is also given.

2 Background

EV charging networks have evolved independently using different and incompatible authentication credentials. These incompatibilities have caused significant inconvenience to EV drivers and have required them to hold multiple authentication credentials – typically, one for each EV charging network. This has also forced EV drivers to hold multiple service relationships with different access, registration, account balance, and payment methods. To address these issues, and to support open access, the EV charging industry and stakeholders are developing a common authentication credential and protocol for EV driver authentication. This standard is a result of this work among EV charging industry participants, end users, government bodies, and other stakeholders.

The authentication credential and protocol specified here does not dictate specific user service and payment models, and the issuer of the credential is free to implement models that it believes is in the best interest of the EV driver through market choice. Prepaid, post-paid, aggregated-usage, contract-based, and other models are possible using this credential. Anonymous and non-anonymous EV drivers are also possible, as the credential and protocol do not impose a relationship between the credential issuer and the EV driver. The primary requirement is network connectivity between the point where authentication takes place and the credential issuer and authenticator to confirm the validity and status of the credential.

This standard does not define exclusively the only authentication and activation methods for requesting services at Electric Vehicle Charging Stations (EVCSs). Many EVCSs support multiple methods, including point-of-sale credit/debit/other payments; remote network charging start method; and SMS- or telephone-initiated service. This standard presents one method among possibly several that can be used to enable EV charging services. The use of the authentication credential and protocol described here facilitates service roaming, and it reflects the need for a convenient, fast, and easy-to-use multi-network authentication method. Other methods, such as the remote network charging start method, do not require the authentication credential described here and support service roaming scenarios.

3 Field of Application

The field of application for this standard is typically shared, multi-user EVCSs where access to charging services needs to be controlled. Access to charging services might be controlled for a variety of reasons, including payment for services rendered, compliance with usage policies, or other administrative reasons. The types of EVCSs for which the authentication might apply include public, commercial, workplace, and multi-tenant EV charging scenarios.

This standard is intended for public, commercial, workplace, and multi-tenant dwelling EV charging applications, where charging services are provided by a party different than the driver of the EV, and where there is need to account for (and/or assign usage costs to) the user of the services. These types of multi-party EV charging applications are differentiated from single-party, residential EV charging, where EV charging is typically included as part of EV drivers' residential electricity service bills and where identification of the service user is not necessary. These single-party, residential EV charging applications are not the immediate focus of this standard.

The scope of this standard was developed with multi-operator interoperability as a requirement. In heterogeneous multi-operator environments, it is vital that cryptographic keys for user authentication be protected securely within each credential-issuing network and not disclosed to competitors or other untrusted parties. Inadvertent disclosure of cryptographic keys by any party can render many or all credentials un-trustable (hence, unusable), thereby causing wholesale service disruption and credential replacement. Challenge-response based protocols have been used in a wide variety of applications and have the desirable property of not requiring distribution of cryptographic keys to foreign organizations or the use of cryptographic keys at the contactless reader. Cryptographic keys are known only within the network issuing and authenticating the credentials and are not needed at foreign network devices.

This standard facilitates service roaming in inter-connected, multi-operator EV charging networks by defining an industry-standard contactless credential for authentication. The EVCSs are connected to communications networks to support authentication of users in much the same manner as many credit/debit card processing networks are "online" connected networks. Each operator network is also connected via the protocols in this series of standards.

Figure 1 gives a high-level pictorial view of the environment in which the credential authentication process operates. In this figure, the EV driver (credential holder) requests charging services from an EVCS on a foreign network, i.e., a network different than the issuer of the contactless authentication credential. The credential user will have previously established an account on his/her EV charging network and will have received and activated the credential (shown as step 1 in the figure).

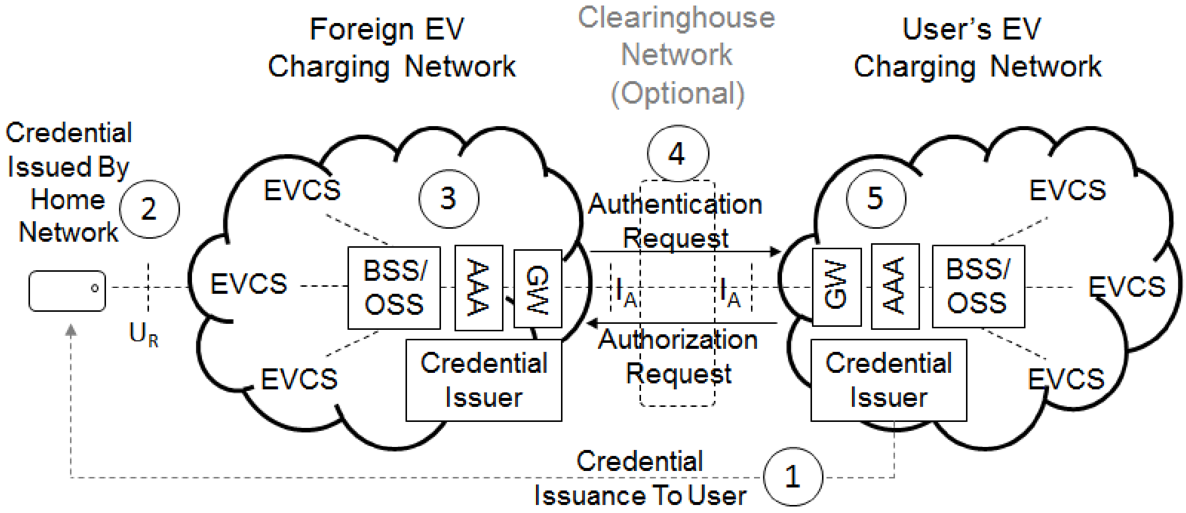

Figure 1
Credential Authentication in Multi-Operator EV Charging Networks

When the credential is presented to the foreign EVCS, the foreign EVCS (via its associated contactless reader) reads data from the credential and initiates a challenge-response operation to authenticate the credential (step 2). The challenge data along with data returned by the credential are passed from the EVCS to the foreign network's Authentication, Authorization, and Accounting (AAA) system for further processing and routing (step 3). Since the credential is from a network different than itself, the foreign network's gateway initiates an authentication request using an internetwork authentication exchange protocol (depicted as I_A) to the credential user's EV charging network gateway and its AAA system (step 4). An implementation of I_A is depicted between the foreign serving and user's EV charging networks (possibly via a clearinghouse network which might be used to facilitate neutral-party interconnection to multiple EV charging networks and provide message routing and forward functions) to transport the authentication data. As the user's EV charging network contains the same cryptographic key as the credential, it can compute the same operation on the challenge data and compare the result against the response from the credential (step 5). Note that the foreign network is unable to validate the credential, since it was not involved in seeding the cryptographic key into the credential (step 1) nor does it have access to the cryptographic key.

The result of the authentication validation is returned to the foreign EV charging network. This is followed by an authorization request (again via I_A) wherein the user's EV charging network issues a commitment to reimburse the foreign EV charging network for services rendered on behalf of its user—subject to the terms and conditions specified in the authorization request. Upon completion, the transaction is recorded on the user's account, and the user is billed for the EV charging service (and potentially a roaming fee).

While this standard is intended for use in networked EV charging applications, this U_R protocol can also be used in non-networked, non-roaming, standalone EVCS deployments where authentication is performed locally within the system. The use of common industry standard authentication credentials might prove useful when EV charging stations from multiple manufacturers are deployed and a common interoperable credential is needed across the standalone stations. Note that the processes and protocols for transferring authentication and authorization data securely to each standalone system are beyond the scope of this standard.

4 Relationship to ISO 15118

The U_R authentication method described in this standard is a form of “External Identification Means” (EIM) and can be used in parallel with the ISO 15118 and other related standards. Some EVCSs support only contactless authentication; others support the ISO 15118 standard. If both are available (and if the EV also supports ISO 15118), the service user can choose which method to use, including possibly selecting some other identification and payment means such as payment credit/debit cards, or generic NFC payment methods. In general, the service user will have the freedom to choose any authentication and activation method based up their EV communication capabilities, the EVCS features, their EV charging network affiliation, and their preferred choice of accounting or payment method.

5 Next Steps

Now that the EVSE 1 Standard is published NEMA is looking at ways to further promogulate and harmonize it through the following venues.

5.1 American National Standards Institute (ANSI)

NEMA is a recognized ANSI Standards Development Organization (SDO). All American National Standards are considered “open” standards. They are developed in such a way that all interested and affected parties are given a chance to be part of their creation. The standard process is collaborative, balanced, and uses a consensus-based approval process. An ANSI Canvass body will be formed to govern the process to convert NEMA EVSE 1 into an ANSI/NEMA Standard. Interested stakeholders are invited to participate.

5.2 International Electrotechnical Commission (IEC)

Elements of the NEMA EVSE 1 Standard are being discussed in the IEC TC 69 Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks. The scope of TC 69 focuses on preparing publications on electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks drawing current from a rechargeable energy storage system. The publications can cover but are not limited to topics such as: general requirements, functional requirements, communication between the EV and the EV supply equipment, electrical power/energy transfer between EV ad supply network, and management of the corresponding infrastructures in view of the associated value-added services.

Specific conversations are already taking place within (2) separate working groups in TC 69. WG 9 Electric Vehicle charging roaming service and JWG 11 Management of Electric Vehicles charging and discharging infrastructure. WG 9 is currently working on the revision of IEC 63119-2 Information exchange for Electric Vehicle charging roaming service- Part 2: Use Cases. Future work projects include the revision of IEC 63119-3- Part 3: Message Structure and IEC 63119-4- Part 4: Cybersecurity and Information Privacy. JWG 11 is currently working on the revision of IEC 63110-1 Protocol for Management of Electric Vehicles charging and discharging infrastructures- Part 1: Basic Definitions, Use Cases and architectures. Future work projects include IEC 63110-2- Part 2: Technical protocols specifications and requirements and IEC 63110-3- Part 3: Requirements for conformance tests.

Author

Steve Griffith is an Industry Director for NEMA's Transportation Systems Division. He manages sections within this division in such areas as Intelligent Transportation Systems (ITS), Electric Vehicle Supply Equipment, and Industrial Imaging & Communications. He is also the principle NEMA staff liaison for NEMA's Internet of Things (IoT) and Cybersecurity activities, leading and defining common approaches to standardization, guidelines, and architecture development while enabling connectivity, defining and simplifying interoperability, and safeguarding privacy and cybersecurity in electrotechnical and medical imaging products.

Steve holds a B.S in Chemical Engineering and a Project Management Professional (PMP) Certification