energies

MDPI

Article

Secure Plug-in Electric Vehicle (PEV) Charging in a Smart Grid Network

Khaled Shuaib [1,*], Ezedin Barka [1], Juhar Ahmed Abdella [1], Farag Sallabi [1], Mohammed Abdel-Hafez [2] and Ala Al-Fuqaha [3]

[1] College of Information Technology, The United Arab Emirates University, Sheik Khalifa Bin Zayed Street P.O. Box 15551, Al Ain, UAE; ebarka@uaeu.ac.ae (E.B.); juhar.a@uaeu.ac.ae (J.A.A.); f.sallabi@uaeu.ac.ae (F.S.)

[2] College of Engineering, The United Arab Emirates University, Sheik Khalifa Bin Zayed Street P.O. Box 15551, Al Ain, UAE; mhafez@uaeu.ac.ae

[3] Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008, USA; ala.al-fuqaha@wmich.edu

* Correspondence: k.shuaib@uaeu.ac.ae; Tel.: +971-3-7135551

Received: 26 June 2017; Accepted: 13 July 2017; Published: 19 July 2017

Abstract: Charging of plug-in electric vehicles (PEVs) exposes smart grid systems and their users to different kinds of security and privacy attacks. Hence, a secure charging protocol is required for PEV charging. Existing PEV charging protocols are usually based on insufficiently represented and simplified charging models that do not consider the user's charging modes (charging at a private location, charging as a guest user, roaming within one's own supplier network or roaming within other suppliers' networks). However, the requirement for charging protocols depends greatly on the user's charging mode. Consequently, available solutions do not provide complete protocol specifications. Moreover, existing protocols do not support anonymous user authentication and payment simultaneously. In this paper, we propose a comprehensive end-to-end charging protocol that addresses the security and privacy issues in PEV charging. The proposed protocol uses nested signatures to protect users' privacy from external suppliers, their own suppliers and third parties. Our approach supports anonymous user authentication, anonymous payment, as well as anonymous message exchange between suppliers within a hierarchical smart grid architecture. We have verified our protocol using the AVISPA software verification tool and the results showed that our protocol is secure and works as desired.

Keywords: electric vehicles; information security protocols; smart grid; privacy; energy charging

1. Introduction

The current electrical power grid is a centrally controlled network distributed over a large geographic area with an enormous number of systems and devices, starting from the power generation plant all the way to the customer side. Smart grids (SGs), on the other hand, are a two-way communication-enabled power grid, in which electrical power generation is integrated with emerging technologies such as wireless communication, pervasive computing, and adaptive control to substantially improve the efficiency, reliability, and sustainability. Significant benefits can be achieved by adopting smart grid networks, including economic and environmental benefits. Deployment of plug-in electric vehicles (PEVs) can be easily integrated as part of a smart grid infrastructure. PEVs are gaining more popularity nowadays in an effort to reduce the air pollution (17% of global CO_2 emissions) caused by fuel operated vehicles and to save the vast amount of money spent on fuel [1]. The study in [2] indicates that CO_2 emissions could be reduced by 70% if PEVs were used instead of their fuel-operated counterparts. Various market research reports indicate that the electric vehicle market is projected to grow rapidly in the coming years. According to the report by Bloomberg [3], there was a 60 percent growth in electric vehicle sales globally in 2015. The report also forecasts that electric vehicles will account for 35 percent of new vehicle sales by 2040. As PEV usage increases, more sophisticated charging infrastructures will be built and users will be able to charge conveniently. However, just like any other appliance directly connected to the two-way communication system of the SG, PEV charging may expose the smart grid system and the users to different kinds of security and privacy problems. These include confidentiality, integrity, replay, DoS attacks and users' privacy breaches by various entities [4–8]. More importantly, there is a high chance of a user's privacy breach during roaming charging, i.e. outside the user's own supplier network. During roaming charging, there is a need for message exchange involving external untrusted entities. Thus, a user's sensitive information should be protected both from external electricity providers and other third parties. Besides users' privacy issues, there can be repudiation problems, unfair payments and misuse of electric vehicles if no proper user authentication mechanisms are deployed.

Our goal in this work is to allow for a ubiquitous secure PEV charging process based on various user and supplier attributes. The PEV user should be able to charge at various charging locations based on a particular charging mode when needed. A charging mode is defined by two variables: location and access privilege. Location refers to the relative location of the charging station as compared to the user's home supplier whereas the access privilege defines the user's privilege attributes at the charging location. We define a PEV user's access privilege as one of three: a privileged user, a guest user charging for free and a guest user paying for charging. Based on the charging mode, the user has to interact with different entities when charging which also can indicate the charging architecture (model). In addition, different requirements for privacy protection, authentication and payment are needed depending on the user's charging mode. We group charging modes into three general classes in the context of a charging procedure: a user charging at a private location as a privileged user, a user charging at a private location as a guest user (free or not) and a user charging at a commercial charging location. Examples of the first class include charging in one's own home or office as a privileged user. In this case, there is no need for frequent authentication between the user and the electricity provider. Once proper initialization is done, local authentication can be used thereafter. Charging at locations such as friend's house as a guest falls under the second class. Guests could be allowed to charge for free or by payment based on the willingness of the owner. The third class encompasses charging at any charging location built for commercial purposes; privately owned or publicly available. Table 1 shows the various possible charging modes.

Table 1. Classification of charging locations and charging modes.

Charging Location	Charging Mode	Charging Procedure/Method
Charging at one's own private location such as his home or office	Privileged user charging	Local authentication
Charging at a charging location which is not built for commercial purpose but allows guests to charge for free or by payment. e.g., friend's house.	Guest user charging	■ Local authentication if free ■ IRC protocol if charging is not free and the location is inside own supplier ■ ERC protocol if charging is not free and the location is outside own supplier
Charging at a charging location built for commercial purpose	Commercial charging	■ IRC protocol if the location is inside own supplier ■ ERC protocol if the location is outside own supplier

A PEV user is referred to as a roamer if he/she belongs to the second or third charging modes. Hence, a roaming charging protocol is required for these two cases, except when the user is allowed to charge as a guest for free. Furthermore, we define roaming charging into two categories: internal roaming charging (IRC) and external roaming charging (ERC). The user is said to be internally roaming if he is charging outside his private privileged location, but inside his own supplier network. For instance, a user can charge at a public charging station that belongs to the same supplier as his own supplier. In this case, even though the user is within the same supplier network, he or she has to be authenticated by the supplier as the user is unknown to the charging station. Moreover, since the user is connected to a charging point other than his private charging point, the user's privacy needs to be protected from charging stations, energy aggregators or secondary suppliers. The roaming is referred to as ERC when a user is charging at a charging location outside his home supplier's network (within an external supplier network). As will be discussed in detail in the related work section of this paper, considerable research has been conducted on PEV charging protocols [9–17], however, not all security issues have been thoroughly studied. In prior published research, authorization and payment mechanisms were not addressed well. Anonymous user authorization and payment were suggested to protect user's privacy from external entities during roaming charging. These two approaches were proposed by different researchers independently; anonymous authorization [10–12] and anonymous payment [16], however, they were not offered jointly. In addition, a payment transaction mechanism between suppliers has not been suggested by previous work and anonymous message exchange between suppliers was not supported during roaming which can further protect the privacy of the user. For instance, the roaming charging protocol suggested by [17] performs user authorization through direct communications between suppliers which allows the home supplier to compromise the roaming user's privacy by collecting information about the location of the user based on the location of the charging station/external supplier's charging points.

Moreover, existing works do not provide secure and privacy preserving protocols for all charging modes, i.e. earlier solutions do not clearly identify the different charging modes that may exist and propose solutions accordingly. The distinction between private charging, IRC and ERC was not well defined nor was modeled, which has led to insufficiently described charging models and incomplete specifications. In addition, despite the fact that a smart grid architecture is hierarchical, most previously proposed charging protocols were based on a simple charging architecture, where the only communicating entities are the user and a single electricity provider. For example, several studies conducted on charging models/architectures have asserted that the inclusion of an entity called aggregator in the charging architecture is inevitable [18–24]. According to these studies, aggregators act as intermediaries between the user and top level electricity providers such as primary and secondary suppliers, distribution grid operators and transmission grid operators. The function of aggregators is two-fold: First, during a grid to vehicle (G2V) mode, they optimize the charging process to protect the reliability of the power system, and second, during a vehicle to grid (V2G) mode, they accumulate the energy discharged from distributed electric vehicle batteries into a single load or source and provide it to the grid. The security aspect of coordinated and aggregated electric signals is considered an important component to ensure system reliability and integrity, however, it is beyond the scope of this paper and to be addressed as part of future work. Depending on their location, aggregators may sign contracts with other suppliers or buy energy directly from the energy market and provide charging/discharging services for end customers [18]. In the case of charging from one's private home, there can be no need for such an entity as its intended functionalities can be integrated as part of the used smart meter. The key contributions of this paper may be described as follows:

- An end to end charging protocol for PEV charging is being proposed in accordance with the various charging models which we have developed based on the different kinds of charging modes. More specifically, we provide a unified charging protocol for IRC and ERC scenarios and we suggest local charging methods for private privileged user charging and guest user charging.
- The proposed protocol incorporates nested signatures to protect user's privacy, not only from external suppliers, but also from their own contracted suppliers and involved third parties. Using nested signatures, the system can provide secure and privacy aware charging for all charging modes. We rely on cryptographic systems and adopt the concept of nested signatures (a dual signature in the case of IRC, and a triple signature in the case of ERC). In this nested signature approach, messages can be transported through a foreign network in such a way that each entity along the path can only see the part of the message pertained to it and not the other

parts. By utilizing nested signatures, a charging request message generated by the user can be divided into parts so that every participating entity in the charging process has access to only the information pertain to it. However, in the case of a dispute, the nested signature approach allows for the different parts of any request to be linked in order to resolve the dispute.

- The proposed approach not only allows the user to be authenticated and to make payments anonymously, but also supports anonymous message exchange between suppliers. In addition to the nested signature, we integrate a trusted third party as an intermediary entity to allow anonymous message exchange between suppliers. The anonymity feature allows suppliers to exchange authorization messages and also make payments to one another without revealing their identities to each other. To the best of our knowledge, our approach is the first to propose an anonymous authorization and payment transaction mechanism between energy suppliers.
- By applying nested signatures, our method supports secure and privacy-aware charging within a hierarchal smart grid architecture which may include primary and secondary suppliers. Aside from this, similar to the approach taken in [17], our method supports user-based authentication to avoid misuse of electric vehicles and implement fair payment.

In summary, our original contributions in this our work include: identifying the different charging modes and devising charging models (architectures) accordingly, a comprehensive end to end charging protocol and method that covers all charging modes (private charging, guest user charging, IRC and ERC), anonymous authentication and payment by the user and anonymous message exchange between suppliers for user authentication and payment transactions. Our work relies on the use of cryptographic hash functions and cryptography systems, both symmetric and asymmetric, to ensure confidentiality, integrity and to some extent anonymity. Symmetric key cryptography techniques utilize symmetric secret keys between any two communication entities where asymmetric (also known as a public key) cryptography systems utilize the use of public/private key pairs for secure communication and exchange of information. For more information on cryptography and hash functions, the reader is referred to [25].

The rest of this paper is organized as follows: Section 2 reviews related works. Section 3 introduces the various charging modes and their architectures. The proposed protocol for secure charging and payment transaction is discussed in Section 4. We present the formal verification of the proposed protocol in Section 5. Section 6 concludes the paper.

2. Related Work

A number of studies have been conducted on the integration of electric vehicles in a smart grid environment. In particular, the security and privacy aspect of PEV charging has attracted researchers in recent years. The papers [4–7] analyzed the security and privacy issues that emanate from integrating PEVs with the smart grid and proposed their own mitigation techniques. A detailed survey of the various privacy issues and a review of the recent works on privacy preservation of PEV charging is provided in [8].

Researchers have also worked on various security protocols, many of which focused on authentication only. A batch authentication scheme was proposed by [9] to make authentication fast enough to meet V2G communication requirements. The studies in [10,11] presented an anonymous authentication scheme to preserve the privacy of PEV users. The work in [12] suggested a mutual batch authentication protocol to preserve the privacy of the PEV user both from home suppliers/aggregators and external suppliers/aggregators based on a bilinear pairing technique. Context-aware authentication (battery-aware and role-aware) scheme was used to preserve privacy for V2G communications in the SG [13]. Two kinds of authentication schemes were implemented by [14]. The first one was a mutual authentication mechanism between the PEV and a trusted SG server for the case when the only communicating entities are the PEV and the SG. The second scheme was a privacy-preserving authentication scheme between the PEV and the SG server when the two are communicating through a non-trusted third party. Battery status-aware authentication scheme was presented in [15] for V2G networks in SG to protect the privacy and security threats resulted from varying battery status. The paper in [16] came up with a two-way anonymous payment system between a user and a supplier that can be used both in the case of charging/discharging. However, [16] did not support roaming. The most relevant work to our approach is the one presented by [17]. However, significant differences exist between the two approaches. The study in [17] proposed a privacy preserving charging and billing protocol for roaming PEV. Their work is equivalent to our ERC case and does not consider the other cases such IRC and private charging cases. Also, their work does not support payment transaction mechanisms and anonymous authorization between suppliers. Moreover, like all others, their charging model is based on a simplified charging model where there is only one supplier.

Studies of security frameworks, models and architectures have also been made for PEV charging infrastructure. The authors in [26] evaluated the weaknesses and strengths of the NISTIR 7628 Cybersecurity standard for smart grid in the context of PEV charging and found two weaknesses (authentication and privacy issues). The authors in [27] proposed a unified security and privacy preserving framework (USaPP) to examine basic issues of smart grid security and privacy in an efficient and comprehensive way. The authors demonstrate their framework by taking the example of roaming PEV charging. A secure client-server based cybersecurity architecture for integrating the PEV with the smart grid is proposed in [28]. Their approach suggests the usage of four kinds of servers: Charge Management Server (CMS), Vehicle Management Server (VMS), Billing Management Server (BMS), and Grid Management Server (GMS). The PEV connects to the system through CMS. The VMS is considered a third party service supplier as it provides PEVs with various information about the charging station. The work in [29] presents a data management architecture which defines a data aggregation and publication procedure for the V2G mode to solve privacy preserving issues such as location and payment related information. A cyber insurance-based model for charging and discharging of PEVs in V2G systems is introduced in [30]. In their model, cyber risks originating from unreliable wireless communication between aggregator and PEVs are transferred to a third party known as cyber insurance company so that PEVs are secured from cyber-attacks and also compensated for any damage caused by attackers.

An attribute-based encryption was proposed in [31] to protect user privacy from aggregators in a V2G network that provides multi-quality charging services to its customers as the aggregators need to collect various information of the user to determine what level of charging service to offer. As per commercial implementation of systems for charging electric vehicles, the work done by "FleetCarma" [32] can be considered as an integration of electric vehicle charging infrastructure within a smart grid environment. The focus of their work is to provide smart charging platforms to better serve both the utility providers and owners of EVs. However, information security aspects are not fully integrated as part of such systems.

A summary of the comparison between existing works and our proposed system is presented in Table 2.

Table 2. Summary comparison of existing works with our proposed system.

Feature	Covered by
Charging mode (Private, Guest, IRC and ERC)	IRC (Guo et al. [9], Liu et al. [10], Chen et al. [11], Saxena et al. [12], Zhang et al. [13], Nicanfar et al. [14], Liu et al. [15], Au et al. [16]), ERC (Mustafa et al. [17]), all modes (Ours)
Anonymous user Authentication during IRC	Liu et al. [10], Chen et al. [11], Ours.
Anonymous user Payment during IRC	Ours
Anonymous user Authentication during ERC	Mustafa et al. [17], Ours
Payment Transaction Mechanism during ERC	Ours
Anonymous message exchange between suppliers	Ours
Authentication (User based, Batch, Mutual, Context-aware)	User-based (Mustafa et. al. [17], Ours), Batch (Guo et al. [9]), Mutual (Saxena et al. [12], Nicanfar et al. [14], Ours), Context aware (Zhang et al. [13], Liu et al. [15])

3. PEV Charging Modes and Architectures

PEV users are mobile and are assumed to be charging at different locations and might be using different access privileges based on one of the previously explained charging modes. The user may be connected to his/her own home charging point or to a charging point outside his home such as a friend's home, a public street charging point, a private charging station, a workplace charging point, etc. In some cases, the charging locations may belong to the same supplier as the user's home supplier. For example, a PEV user's home supplier can be the same as the supplier at his workplace/nearby charging station. In other cases, the charging location may be outside his home supplier's network. In addition, from the perspective of access privilege, the user could charge as a privileged user in a private location, as a guest user or as a commercial user.

The number of communicating entities participating in the charging process varies based on the charging mode. For example, when the user is charging at his own home, the only entities engaged are the user, home aggregator (HAG), if exists, and home supplier (HS). However, if the user is roaming within an external supplier network, the number of interacting entities include: user, external aggregator (EAG), external supplier (ES), trusted third party and home supplier. In the case of ERC, the home supplier and the trusted third party are also involved in the communication. This is due to user authentication being performed remotely between suppliers through a trusted third party. The existence of a trusted third party is necessary to make payment transactions between suppliers, to solve disputes and to protect the user from privacy breaches. Consequently, the charging model and the charging protocol used depends on the kind of charging mode as that mandates a different kind of security and privacy requirement owing to the difference in the number of entities taking part in the charging process.

Different previous charging models/architectures were introduced before by others. Examples of this include [5,13,16,18–20,28,30]. Although these charging models should have incorporated the different kinds of charging modes, the majority were simplified and did not fully represent the various charging cases. Of these, [5,9] formulated a relatively detailed conceptual model for the different charging modes (home, public charging on streets, and dedicated charging stations). Therefore, in this section, we first identify and group the different kinds of charging modes which will enable us to suggest different kinds of charging models, methods and protocols based on our own perspective on grouping. We can generally group the charging modes into three classes based on two attributes: charging location and access privilege. The charging modes are discussed in subsequent sections. Prior to that, we introduce the entities in our system. Some of these entities do not appear in all charging modes. For example, Broker (BR), Certificate Authority (CA), External Suppliers (ES) and External Aggregators come into the system only during the ERC case. Our proposed system entities are defined below:

User (U): is an electricity consumer who has contract with a supplier.

Electric Vehicle Supply Equipment (EVSE): This is an intelligent device that is used as a charging point connecting the PEV to the smart grid system.

Smart Meter (SM): a smart electronic device that continuously records electricity consumption and sends it to the supplier based defined time intervals.

Home Supplier (HS): A supplier is a company that sells electricity to customers. The home supplier is the supplier with whom the user has a contract.

Home Aggregator (HAG): Aggregators are responsible for optimizing charging/discharging processes. For home charging, this functionality can be integrated as part of the SM or a separate entity installed inside the house. However, in the presence of multiple renewable energy sources being used to inject energy into the grid a HAG as a separate entity can be used to optimize such a process.

Visiting Aggregator (VAG): During IRC, the user communicates with a different aggregator other than the home aggregator but within the home supplier network. We refer to this as visiting aggregator (VAG).

External Supplier (ES): An external supplier is a supplier other than the home supplier. The user communicates with an external supplier during ERC.

External Aggregator (EAG): External aggregators are those which belong to external supplier networks.

Certificate Authority (CA): A trusted third party that issues certificates for suppliers and Brokers.

Broker (BR): is a trusted third party that acts as a mediator between suppliers for authorization and payment transaction. This facilitates communication between suppliers without them revealing their real identities to each other.

3.1. Private-Privileged User Charging

This charging mode represents the situation when a user is charging at a private charging point with full privileges to charge at that location:

I. User's Home: A customer charging at his own home on his private charging point. Figure 1 below illustrates the home charging model. When the user charges at his own home, a specific protocol may not be required and a simple charging process can be implemented as follows:

    ■ Authentication is done locally on the EVSE. To be able to do so, before charging, information about authorized members who are allowed to charge a certain vehicle using the home charging point can be saved to the EVSE either by the users themselves or loaded automatically by the supplier. The information can be for example the hash of the user's smart card (SC) number and the vehicle ID.

    ■ When the user starts charging, the EVSE first checks whether the user's information is available locally or not. If the user's information is found locally on the EVSE, the EVSE immediately allows charging. However, for the purpose of fair payment, the EVSE has to prepare an electric consumption report (ECR) in the name of the current consuming user and send it to the supplier.

    ■ During charging, the authorized members use their smart card to sign the (ECR).

II. User's Office/Company: A company may provide a free or discounted charging service for its employees by installing charging infrastructure in the office parking area. In this case, we assume that the employees are not directly billed for the service. Instead the company will pay for them. Hence, the electricity provider will consider the company as the end customer. However, the company needs to register its users and also authenticate them using a local authentication server. Moreover, the company may need to keep a charging history for the purpose of internal auditing. The charging model of this mode is illustrated in Figure 2. The charging steps are:

    ■ The company authenticates employees locally on the authentication server.

    ■ Before charging, the company initially registers its employees and their vehicles. During charging, the EVSE first checks if the user is authentic by contacting the local authentication server. If the user is authenticated, the EVSE automatically allows charging. However, for the purpose of internal auditing, the EVSE has to prepare an electric consumption report (ECR) by the name of the consuming user and send it to the employer's server and if needed to the supplier.

During charging, the employees use their smart card to sign the (ECR).

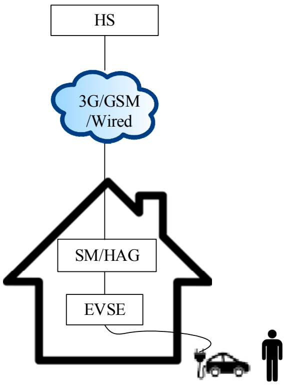


Figure 1. Charging Model for Home Charging.

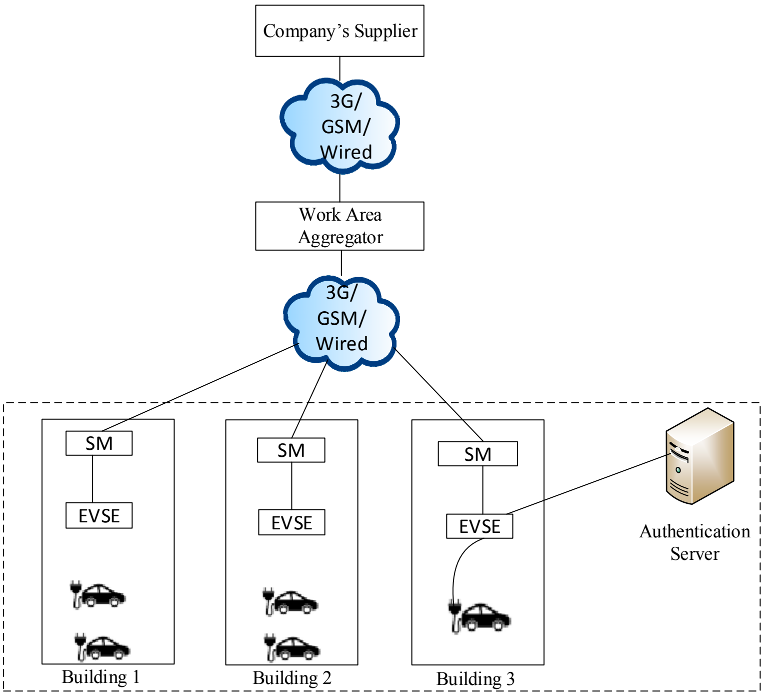


Figure 2. Charging Model for Office/Company Charging.

3.2. Guest User Charging

This mode covers the scenario where a user visits a charging location such as a friend's home and charges his PEV as a guest. When a guest user connects to a privately owned non-commercial charging point, the owner of the charging location will be notified via a pre-arranged notification method. For example, for a charging point that belongs to individuals, the supplier could contact the owner through a simple communication method such as an SMS. The owner will be asked to grant or deny the guest user the permission to charge at his charging location. Moreover, the owner can also be asked to choose from different payment options (e.g., the owner pays for the guest user or the visitor pays). Base on the response from the owner, one of two charging processes could be activated. If the owner allows the visitor to charge for free, the EVSE starts charging immediately and the payment is credited from the account of the owner. Otherwise, a roaming charging protocol will be activated. The protocol to be activated is either IRC or ERC, based on the location of the current charging point as compared to the location of the home supplier of the guest user. The charging models for IRC and ERC are illustrated in Figures 3 and 4, respectively.

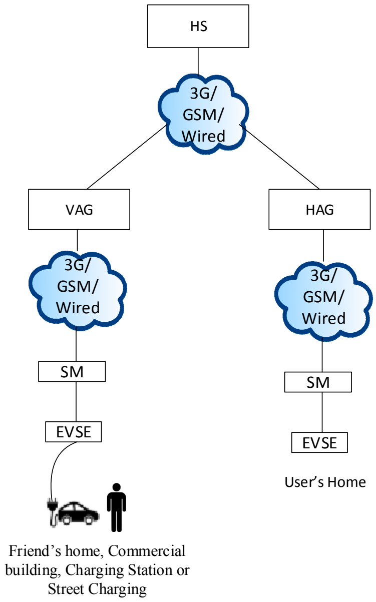


Figure 3. Internal Roaming Charging Model.

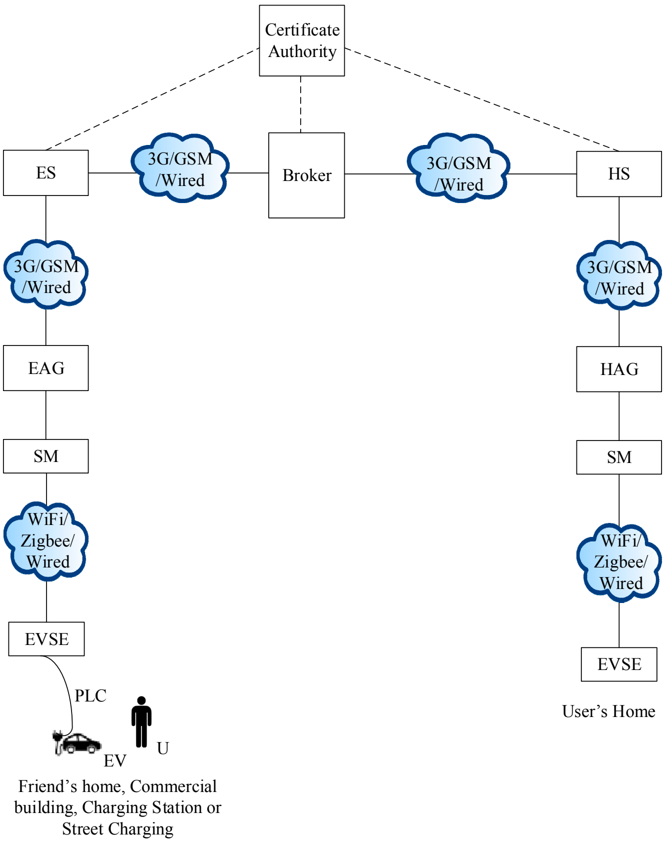


Figure 4. External Roaming Charging Model.

3.3. *Commercial Charging Location*

This kind of charging location is specifically built for commercial purposes and is publicly available to anyone to use. Such users are considered random users who have no specific privileges on the used charging location, and therefore the charging point does not need to implement local privileged/guest user charging procedures. In this case, the user and the PEV need to be authenticated/authorized before charging and billing will be managed through the user's respective supplier. In other words, either IRC or ERC protocol will be applied. We mention here three of such kind of charging locations:

- Charging station: A charging station with several charging points supporting different charging options, specifically fast charging modes.
- A commercial building: Several EV charging points can be installed at a commercial building parking area for use by clients.
- Street Charging: Public charging places on the streets, or at public parking areas etc.

4. Roaming Charging Protocol

In this section, we discuss the charging protocol for the following two cases: IRC protocol for users charging inside their own supplier network but outside their own home and the ERC protocol for users charging within an external supplier network. Our system dynamically decides which of the two protocols (IRC protocol or ERC protocol) to activate based on the initial information configured on the EVSE and the information configured on the smart card of the user. The user's SC is configured with the hash of the user's home supplier ID ($h(HS_{ID})$). When the user connects to the EVSE, one of the pieces of information the SC sends to the EVSE at the initial stage is the $h(HS_{ID})$. On the other hand, the EVSE also stores the hash of its own supplier ID. Therefore, upon receiving the $h(HS_{ID})$ from the SC, the EVSE can compare these two hash values and decide whether the user belongs to the same supplier or not. The content of the initial response message from the EVSE to the SC depends on the outcome of this comparison. The SC prepares a charging request message that matches the selected charging protocol based on the initial response message from the EVSE. For private charging points that belong to individuals/private companies, the EVSE performs two additional steps before it proceeds with deciding on which protocol (IRC and ERC protocol) to apply, as it has to also consider the other two cases (private user charging and guest user charging) as follows:

1. The EVSE checks whether the user is a privileged private user or not by comparing the user's information with the data saved locally on the EVSE or by contacting the authentication server.
2. If the result in step 1 indicates that the user is a visitor and not a privileged private user, it contacts the owner of the charging point for approval. The owner's response could be one of three: Deny charging, allow charging for free or allow charging for a fee. If the owner chooses to deny charging, the EVSE acts accordingly. If the response from the owner is "allow charging for free", the EVSE allows charging and bills the owner for the electricity consumed by the guest user. If the response from the owner is "allow charging for a fee", the EVSE initiates either the IRC or ERC protocol as per the procedure explained earlier.

System initialization is needed for proper operation of the protocol as will be discussed in the next section.

4.1. System Initialization

The following are the required system initializations/registrations required by the protocol:

Certificate Generation and Distribution: The certificate authority (CA) generates and distributes certificates for suppliers and the broker (BR). Moreover, each supplier publishes its public key to other suppliers and the broker.

Suppliers Register with Broker (BR): Suppliers register with the broker by presenting their credentials and their accounts are then created for billing purposes.

Aggregators sign a contract with suppliers: Aggregators establish an agreement with suppliers to provide charging/discharging service to end users. During the contract agreement, aggregators get certificates from suppliers. As needed, aggregators also get the list of public keys of the smart meters for the area they are going to provide service in.

User Registration: Users establish contracts with suppliers by registering their PEVs and the list of authorized individuals who are allowed to charge those PEVs. A unique user ID (U_{ID}) is assigned to each user during registration. Suppliers also provide users with smart cards which contain data about the user and the supplier itself. The information stored on the smart card include: the public/private key pairs of the user, the U_{ID} of the user, the public key of the supplier and the hash of the supplier ID (S_{ID}). However, the private key of the user is stored encrypted at the smart card and can only be retrieved when the user enters the correct PIN number configured during registration. We assume that each PEV is provided with a unique Vehicle ID (V_{ID}) during production and suppliers can uniquely identify any PEV using its ID. However, for privacy, the PEVs' real IDs are not used during charging, instead, suppliers generate a set of pseudonym IDs (P_{ID}) that map to the real vehicle's IDs to be used during charging. Suppliers keep the mapping between the real IDs and the corresponding pseudonym IDs in their database which can be expressed as:

$$V_{ID_1} = \{P_{ID_{1\text{-}1}}, P_{ID_{1\text{-}2}} \ldots P_{ID_{1\text{-}N}}\}, V_{ID_2} = \{P_{ID_{2\text{-}1}}, P_{ID_{2\text{-}2}} \ldots P_{ID_{2\text{-}N}}\} \ldots V_{ID_N} = \{P_{ID_{N\text{-}1}}, P_{ID_{N\text{-}2}} \ldots P_{ID_{N\text{-}N}}\}$$

The set of pseudonym IDs (P_{ID}) is also stored in the PEV's firmware such that at the time of charging, a PEV can pick one P_{ID} at random and use it to request charging. In addition to the real vehicle ID to pseudonym ID mapping, suppliers also keep the mapping between users and the list of vehicles they are allowed to use. This data is required to avoid misuse of PEVs and to enable fair payment. A mapping example can be represented as follows:

$$U_{ID_1} = \{V_{ID_1}, V_{ID_3}\}, U_{ID_2} = \{V_{ID_2}, V_{ID_3}, V_{ID_{10}}\} \ldots U_{ID_N} = \{V_{ID_4}\}$$

Initializing EVSE and SM: Suppliers prepare certificates for all SMs and EVSEs which belong to them and configure them with their respective public/private key pairs. Moreover, a ring of public keys (the public key of SM, the supplier and BR) and the hash of the supplier ID are stored in all EVSEs. On the other hand, the public keys of the aggregator and EVSE are also installed on the SMs.

Uploading User's Data to the Directory Service: Once all the other steps are accomplished, suppliers need to make the list of registered users available to the BR by uploading it to a directory service that is accessible by the BR. Moreover, suppliers should regularly push new data to the directory as new users register and existing users leave. The BR on the other hand should update its database by pulling fresh data periodically. Users' and suppliers' information available at the BR is shown in Table 3.

Table 3. Supplier and User data at Broker.

Supplier (S)	Supplier Billing Account (BA)	Supplier's Public Key	Registered Users
S_1	BA_{S_1}	KU_{S_1}	$\{U_{S_{1\text{-}1}}, U_{S_{1\text{-}2}} \ldots U_{S_{1\text{-}X}}\}$
S_2	BA_{S_2}	KU_{S_2}	$\{U_{S_{2\text{-}1}}, U_{S_{2\text{-}2}} \ldots U_{S_{2\text{-}X}}\}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_N	BA_{S_N}	KU_{S_N}	$\{U_{S_{N\text{-}1}}, U_{S_{N\text{-}2}} \ldots U_{S_{N\text{-}Z}}\}$

4.2. Internal Roaming Charging (IRC)

The IRC protocol is activated when the user charges for a fee at a charging point which resides inside his own supplier network but outside his private location. The IRC protocol utilizes dual signature and is performed in three steps: charging request, charging response and payment capture. These steps are discussed next in details.

1. Charging Request

   (a) A random user U is charging at a charging point which has a display screen where the user can see general information such as the available charging type (level 1, level 2, level 3, ...), charging rate (CR), the maximum available amount of electricity etc. The CR is the price information of electricity over a time range as it might vary over time-based on the change in supply/demand. Once the PEV is connected to the EVSE and the user has inserted its smart card (SC) into the card reader (CRD), the smart card prompts the user for a password/PIN before the user can start charging.

(b) Once the user enters his PIN, he/she will be directed to a screen to select the charging information (CI) which contains the requested energy amount (REA) and the charging end time (CET). This will initiate a charging request between the user's SC (on behalf of the user) and the EVSE. An initial message (InMess) containing the P_{ID}, h(HS_{ID}) and the CI is sent from the user's SC to the EVSE. This can be represented as: U → EVSE := InMess where InMess = P_{ID} | | CI | | h(HS_{ID}) and CI = REA | | CET.

(c) Once the EVSE receives the initial message, it first checks whether U belongs to the same supplier as that of the EVSE by comparing h(HS_{ID}) with the hash value of the supplier ID stored in the EVSE. If the two hash values match, the IRC protocol will be applied, otherwise, the ERC protocol will be selected. In the case of IRC, the EVSE prepares an initial response message (InResMess) by concatenating the InMess with a unique transaction ID (TID), CR and maximum payment (MP). The MP is the approximate maximum payment that the user will be asked to pay for the requested electricity calculated at the price rate of CR. The MP is used for payment authorization purposes. The actual electricity usage and actual payment will be calculated after charging have been completed. This is because the user may decide to stop charging in the middle or before the maximum requested energy is reached. This is represented as: EVSE → U := InResMess where InResMess = P_{ID} | | CI | | CR | | MP | | TID.

(d) Upon receiving the initial response message, the SC prepares the charging request (CReQ) using a dual signature. The steps followed for preparing a charging request are:

I. SC first generates the needed dual signature as shown in Figure 5. The dual signature is comprised of the Charging Order Information (COI) and the Billing Information (BI) analogous to the Order Information (OI) and the Payment Information (PI) in the SET protocol:

Charging Order Information (COI): This consists of the P_{ID}, transaction ID, CI, CR and MP received during the initial response phase, where COI = P_{ID} | | TID | | CI | | CR | | MP.

Billing Information (BI): The BI contains the P_{ID}, TID, U_{ID} and MP, where BI = P_{ID} | | TID | | U_{ID} | |MP.

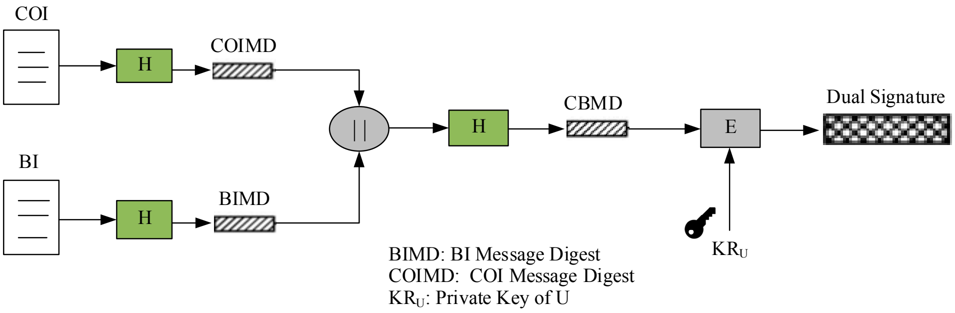


Figure 5. Dual signature generation.

II. SC then prepares the charging request (CReQ). The CReQ consists of two parts: the first part conveys the visiting aggregator (VAG) while the second part conveys the home supplier (HS). It encrypts the part of the message that is targeted to the HS using HS's public key. These two messages are represented as:

U to VAG, M (U → VAG) = COI | | DS | | BIMD | | $\mathrm{Cert_U}$ where $\mathrm{Cert_U}$ is the certificate of U.

U to HS, M (U → HS) = $\mathrm{E_{KU_{HS}}}$[BI | | DS | | COIMD].

The SC also attaches a time stamp T_1 to the CReQ message as: CReQ = M (U → VAG) | | M (U → HS) | | T_1 before it is sent to EVSE, U → EVSE := CReQ. The CReQ is then delivered from the EVSE to the SM and subsequently to the HS.

(e) Once the EVSE receives the CReQ message, it sends it to the SM by encrypting it using the public key of the SM and by signing it using its private key i.e., EVSE → SM := $\mathrm{E_{KR_{EVSE}}}$[$\mathrm{E_{KU_{SM}}}$[CReQ]] | | $\mathrm{E_{KU_{SM}}}$[CReQ].

(f) When the CReQ message reaches the SM, the SM verifies that the message is from the EVSE, not a replay and that the message is not changed in transit by using the public key of the EVSE. The SM then decrypts the message using its private key. It then encrypts it using the public key of the VAG, signs it and sends it to the VAG. This is shown as: CReQ = $\mathrm{D_{KR_{SM}}}$ [$\mathrm{E_{KU_{SM}}}$[CReQ]], SM → VAG : = $\mathrm{E_{KR_{SM}}}$[$\mathrm{E_{KU_{VAG}}}$[CReQ]] | | $\mathrm{E_{KU_{VAG}}}$[CReQ].

(g) Upon receiving the charging request message from the SM, the VAG first checks the integrity and freshness of the message and also verifies that the message is actually from SM using the public key of the SM. The VAG then decrypts the message using its private key to get the CReQ i.e., CReQ = $\mathrm{D_{KR_{VAG}}}$[$\mathrm{E_{KU_{VAG}}}$[CReQ]] = CReQ.

The VAG can verify the charging request message using the dual signature. The VAG then process the part of the message targeted to it and forwards the other part to the HS. The message that is sent from the VAG to the HS is signed by the VAG using its private key. A new time stamp is also attached to it as shown in: VAG → HS := $\mathrm{E_{KR_{VAG}}}$[M (U → HS) | | T_2] | | M (U → HS) | | T_2.

2. Charging response

(a) Upon CReQ message arrival from VAG, the HS verifies its origin authenticity and its integrity using the public key of VAG. The HS can also verify the charging request message using the dual signature. Once the message is verified, the HS decrypts the original message from U using its private key.

(b) After verifying that the charging request is generated from U, the HS authenticates the user and the authorization proceeds as follows:

I. The HS obtains the user ID of U ($\mathrm{U_{ID}}$) from the BI and checks whether $\mathrm{U_{ID}}$ is a registered user. If U is not a registered user, HS automatically returns a negative charging response (CharRes) message to the VAG. The charging response message takes the following format: CharRes = $\mathrm{P_{ID}}$ | | TID | | DEC, where DEC stands for a binary decision of two values: Allow as a positive response and Deny as a negative response. The charging response is encrypted using the public key of the VAG and signed by the HS. Hence in this case (the case of negative charging response), the response from the HS to the VAG is CharRes = $\mathrm{P_{ID}}$ | | TID | | Deny.

HS → VAG := $\mathrm{E_{KR_{HS}}}$[$\mathrm{E_{KU_{VAG}}}$[CharRes]] | | $\mathrm{E_{KU_{VAG}}}$[CharRes].

(c) If U is a registered user, the HS proceeds with the authorization check using two steps before returning a response to the VAG:

I. Finds the $\mathrm{V_{ID}}$ that corresponds to $\mathrm{P_{ID}}$ in its database and checks if U is allowed to use the vehicle with $\mathrm{V_{ID}}$.

II. The HS also checks if U has the needed credit to support the requested payment amount MP.

If both of the above pre-conditions are satisfied, the HS returns a positive charging response to the VAG expressed as:

CharRes = P_{ID} | | TID | | Allow, Otherwise, HS returns a negative response as CharRes = P_{ID} | | TID | | Deny.

HS → VAG := $E_{KR_{HS}}[E_{KU_{VAG}}[\text{CharRes}]]$ | | $E_{KU_{VAG}}[\text{CharRes}]$.

(d) The VAG verifies the origin of the received charging response from HS and its integrity by decrypting the message using its private key, then it encrypts it using the public key of the SM, signs it and sends it to the SM. The VAG also keeps a copy of the response for itself for later use.

CharRes = P_{ID} | | TID | | Allow or P_{ID} | | TID | | Deny and VAG → SM := $E_{KR_{VAG}}[E_{KU_{SM}}$ [CharRes]] | | $E_{KU_{SM}}[\text{CharRes}]$.

(e) Similarly, the SM processes the received message and sends it to the EVSE. SM → EVSE := $E_{KR_{SM}}[E_{KU_{EVSE}}[\text{CharRes}]]$ | | $E_{KU_{EVSE}}[\text{CharRes}]$.

(f) Upon receiving the message, the EVSE either allows charging or denies it based on the response. If the charging response is positive the PEV starts charging and the EVSE records the actual electricity usage (AEU) of the PEV and makes sure the AEU is not greater than the REA. EVSE stops charging if the AEU reaches the REA or if the PEV becomes fully charged.

3. Payment Capture

a. When charging is completed, the EVSE prepares an electric consumption report (ECR) and forwards it to the SC. The ECR contains the P_{ID}, TID, AEU and AP (actual payment). The EVSE calculates the AP needed to be paid by the user based on the AEU and the CR. The SC signs the ECR with the private key of the user and sends it back to the EVSE as: U → EVSE := ECR where ECR = $E_{KR_U}[P_{ID}$ | | TID | | AEU | | AP].

b. The ECR message is sent to the VAG in a similar way as explained before (encrypting it with the public key of the receiver and then signing it with the private key of the sender).

EVSE → SM = $E_{KR_{EVSE}}[E_{KU_{SM}}[\text{ECR}]]$ | | $E_{KU_{SM}}[\text{ECR}]$

SM → VAG = $E_{KR_{SM}}[E_{KU_{VAG}}[\text{ECR}]]$ | | $E_{KU_{VAG}}[\text{ECR}]$

When the ECR message reaches the VAG, it verifies the message using the public key of the SM. The VAG then decrypts the message using its private key to get the ECR. VAG also confirms that the message is generated from U by using U's public key. Next, the VAG forwards a copy of the ECR to the HS after signing it using its private key i.e., VAG → HS = $E_{KR_{VAG}}[E_{KU_{HS}}[\text{ECR}]]$ | | $E_{KU_{HS}}[\text{ECR}]$. Upon arrival of the ECR message from the VAG, the HS performs the following: Confirms that the message comes from VAG by using the VAG's public key, decrypts the message using its private key to get the ECR, verifies that the ECR is prepared by U by using U's public key and gets the actual payment (AP) from the ECR and bills U accordingly. The FSM diagram for IRC protocol is shown in Figure 6.

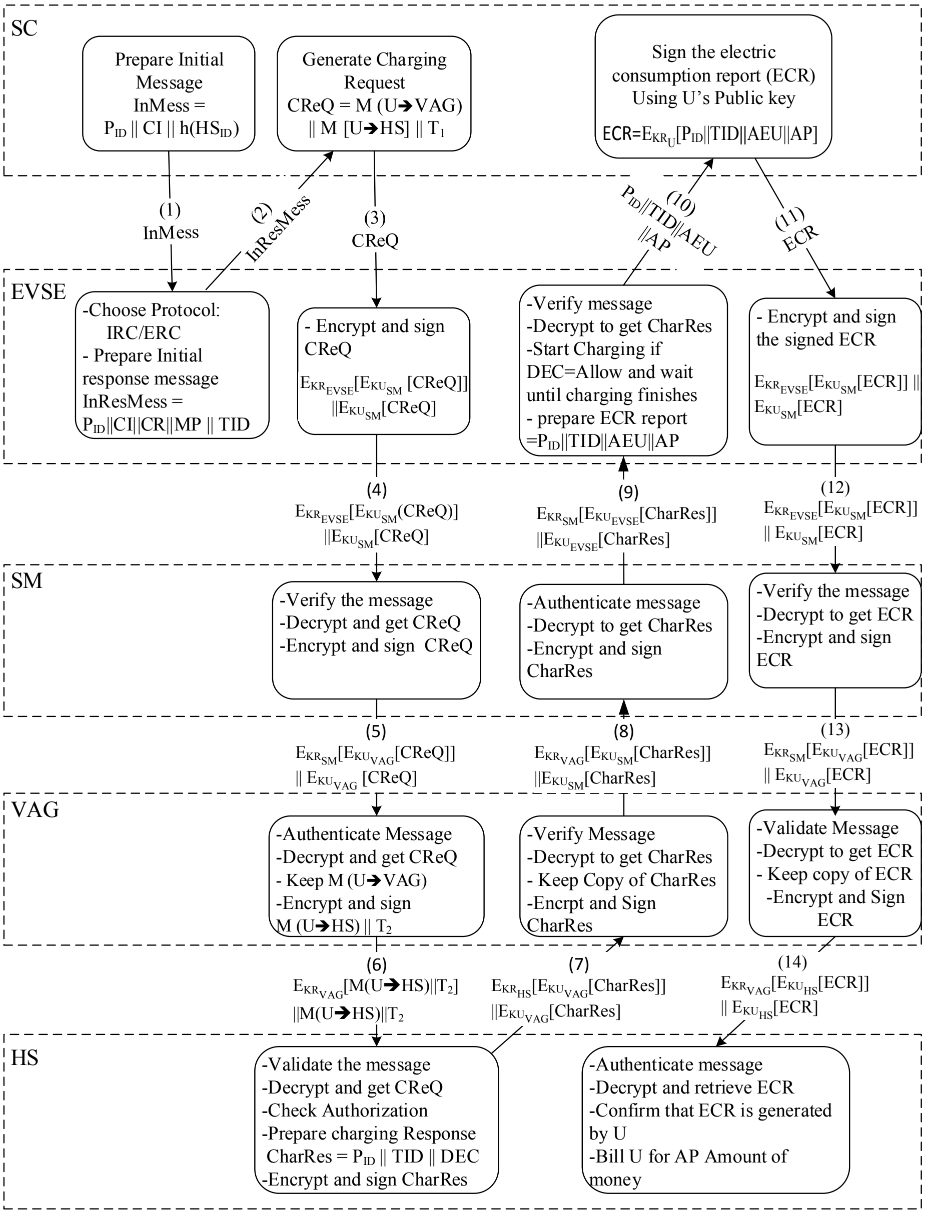

SC
Prepare Initial Message InMess = P_{ID} || CI || h(HS_{ID})
Generate Charging Request CReQ = M (U→VAG) || M [U→HS] || T_1
Sign the electric consumption report (ECR) Using U's Public key
ECR=E_{KR_U}[P_{ID}||TID||AEU||AP]
(1) InMess
(2) InResMess
(3) CReQ
(10) P_{ID}||TID||AEU ||AP
(11) ECR
EVSE
-Choose Protocol: IRC/ERC
- Prepare Initial response message InResMess = P_{ID}||CI||CR||MP || TID
- Encrypt and sign CReQ
$E_{KR_{EVSE}}$[$E_{KU_{SM}}$ [CReQ]] ||$E_{KU_{SM}}$[CReQ]
-Verify message
-Decrypt to get CharRes
-Start Charging if DEC=Allow and wait until charging finishes
- prepare ECR report =P_{ID}||TID||AEU||AP
- Encrypt and sign the signed ECR
$E_{KR_{EVSE}}$[$E_{KU_{SM}}$[ECR]] || $E_{KU_{SM}}$[ECR]
(4) $E_{KR_{EVSE}}$[$E_{KU_{SM}}$(CReQ)] ||$E_{KU_{SM}}$[CReQ]
(9) $E_{KR_{SM}}$[$E_{KU_{EVSE}}$[CharRes]] ||$E_{KU_{EVSE}}$[CharRes]
(12) $E_{KR_{EVSE}}$[$E_{KU_{SM}}$[ECR]] || $E_{KU_{SM}}$[ECR]
SM
-Verify the message
-Decrypt and get CReQ
-Encrypt and sign CReQ
-Authenticate message
-Decrypt to get CharRes
-Encrypt and sign CharRes
-Verify the message
-Decrypt to get ECR
-Encrypt and sign ECR
(5) $E_{KR_{SM}}$[$E_{KU_{VAG}}$[CReQ]] || $E_{KU_{VAG}}$ [CReQ]
(8) $E_{KR_{VAG}}$[$E_{KU_{SM}}$[CharRes]] ||$E_{KU_{SM}}$[CharRes]
(13) $E_{KR_{SM}}$[$E_{KU_{VAG}}$[ECR]] || $E_{KU_{VAG}}$[ECR]
VAG
-Authenticate Message
-Decrypt and get CReQ
- Keep M (U→VAG)
-Encrypt and sign M (U→HS) || T_2
-Verify Message
-Decrypt to get CharRes
- Keep Copy of CharRes
-Encrpt and Sign CharRes
-Validate Message
-Decrypt to get ECR
- Keep copy of ECR
-Encrypt and Sign ECR
(6) $E_{KR_{VAG}}$[M(U→HS)||T_2] ||M(U→HS)||T_2
(7) $E_{KR_{HS}}$[$E_{KU_{VAG}}$[CharRes]] ||$E_{KU_{VAG}}$[CharRes]
(14) $E_{KR_{VAG}}$[$E_{KU_{HS}}$[ECR]] || $E_{KU_{HS}}$[ECR]
HS
-Validate the message
-Decrypt and get CReQ
-Check Authorization
-Prepare charging Response CharRes = P_{ID} || TID || DEC
-Encrypt and sign CharRes
-Authenticate message
-Decrypt and retrieve ECR
-Confirm that ECR is generated by U
-Bill U for AP Amount of money

Figure 6. FSM diagram for IRC protocol.

4.3. External Roaming Charging (ERC)

The ERC protocol is initiated when a PEV user charges at a charging location situated outside his supplier's network. The ERC protocol employs triple signature to protect the user from various privacy breaches. The following section describes the four steps performed by this protocol similar to what was done for the IRC protocol.

1. Charging Request

   a. A visitor user U whose home supplier is HS would like to charge at one of the charging stations of an external supplier ES. In this case, steps a and b of the IRC will be repeated here as well. Starting from step c, a different process is followed. The initial response message (InResMess) sent back to SC in step c of the IRC protocol will contain the public keys of BR and ES and can be shown as: EVSE → U_B := InResMess where InResMess = P_{ID} | | CI | | CR | | MP | | TID | | PK_{BR} | | PK_{ES}.

b. Upon receiving the initial response message, the SC prepares a charging request (CReQ) using a triple signature using a two-step process as follows:

I. The SC first generates the needed triple signature (TS) as shown in Figure 7. The triple signature is prepared from the hash of three parts: Charging order information (COI), Authorization information (AI) and Billing Information (BI). External aggregators/suppliers can only see the COI. AI contains the information required for authorization by the BR. The BR can see the content of the AI but not the COI and the BI. The BI on the other hand is allowed to be seen only by the home supplier. The content of each part is given as:

COI: Consists of the pseudonym ID (P_{ID}), transaction ID (TID), charging information (CI), charging rate (CR) and maximum payment (MP) and can be represented as:

$COI = P_{ID} || TID || CI || CR || MP.$

AI: Contains the pseudonym ID (P_{ID}), transaction ID (TID), home supplier ID (HS_{ID}) and maximum payment (MP) and can be expressed as: $AI = P_{ID} || TID || HS_{ID} || MP$.

BI: Contains the pseudonym ID (P_{ID}), transaction ID (TID), User ID (UID_B) and maximum payment (MP) and can be presented as: $BI = P_{ID} || TID || U_{ID} || MP$.

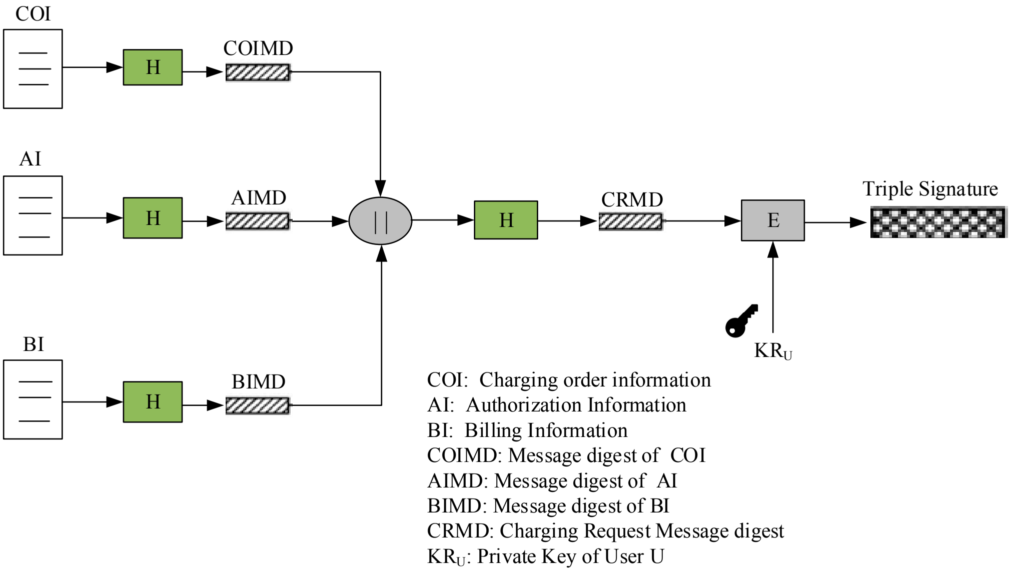
II. The SC then prepares the charging request (CReQ) which contains three parts: Message to External Supplier (MtoES), Message to Broker (MtoBR) and Message to Home Supplier (MtoHS). The parts of the messages for the BR and the HS are encrypted with shared secret keys K_1 and K_2 as shown below:

$MtoES = COI || TS || MDAI || MDBI || Cert_U$ where $Cert_U$ is certificate of user U.

$MtoBR = E_{KU_{BR}}[K_1] || E_{K_1}[AI || TS || MDCOI || MDBI || Cert_U].$

$MtoHS = E_{KU_{HS}}[K_2] || E_{K_2}[BI || TS || MDCOI || MDAI].$

$CReQ = MtoES || MtoBR || MtoHS || T_1$ where T_1 is time stamp.



COI: Charging order information
AI: Authorization Information
BI: Billing Information
COIMD: Message digest of COI
AIMD: Message digest of AI
BIMD: Message digest of BI
CRMD: Charging Request Message digest
KR_U: Private Key of User U

Figure 7. Triple signature generation.

c. When the EVSE receives the CReQ message, it sends it to the SM by encrypting it using the public key of the SM and by signing it using its own private key as: EVSE → SM := $E_{KR_{EVSE}}[E_{KU_{SM}}[CReQ]]\ ||\ E_{KU_{SM}}[CReQ]$.

d. Once the CReQ message is received by the SM, it verifies its origin and integrity using the public key of the EVSE. The SM then decrypts the message using its private key, encrypts it using the public key of the EAG, signs it and sends it to the EAG. This can be represented as: $CReQ = D_{KR_{SM}}[E_{KU_{SM}}[CReQ]]$ and SM → EAG := $E_{KR_{SM}}[E_{KU_{EAG}}[CReQ]]\ ||\ E_{KU_{EAG}}[CReQ]$.

e. Upon receiving the charging request message from SM, EAG first checks the integrity and freshness of the message and also verifies that the message is from SM by using the public key of SM. EAG then decrypts the message by using its private key and gets the CReQ i.e., $CReQ = D_{KR_{EAG}}[E_{KU_{EAG}}[CReQ]]$.

The EAG and the ES have the same access level to the user's information. Therefore, the EAG takes a copy of the part of the message targeted to the ES. EAG then forwards the CReQ to the ES encrypted using the public key of the ES and signed by EAG using its private key i.e., EAG → ES := $E_{KR_{EAG}}[E_{KU_{ES}}\ [CReQ]]\ ||\ E_{KU_{ES}}[CReQ]$.

f. Once the message is received by the ES, it first checks the origin, integrity and freshness of the message using the public key of EAG. This is shown as: ES := $D_{KU_{EAG}}[E_{KR_{EAG}}[E_{KU_{ES}}[CReQ]]] = E_{KU_{ES}}[CReQ]$.

ES then decrypts the message by using its private key and gets the CReQ i.e., CReQ= $D_{KR_{ES}}\ [E_{KU_{ES}}\ [CReQ]]$. The ES then divides the CReQ message into two parts to capture the part of the message targeted to it (MtoES) and forwards the rest to the Broker. The part of the message sent from ES to the Broker is signed by ES using its private key. A new timestamp, T_2, is also attached to the message. This is shown by: ES → BR := $E_{KR_{ES}}[E_{KU_{BR}}\ [MtoBR||MtoHS||T_2]]\ ||\ E_{KU_{BR}}[MtoBR||MtoHS||T_2]$.

2. Authorization

a. Once the BR receives the message from the ES, it verifies its origin, integrity and freshness using the public key of the ES. This can be shown as: $D_{KU_{ES}}[E_{KR_{ES}}[MtoBR\ ||\ MtoHS\ ||\ T_2]] = MtoBR\ ||\ MtoHS\ ||\ T_2$.

b. Once the message is verified, the BR captures its intended part (MtoBR) and decrypts the digital envelope sent by U using its private key to get the shared key, K_1 which is then used to decrypt the message. Next, the BR checks the authenticity of the user as follows:

I. The BR first gets the user ID (U_{ID}) and checks whether the user is a registered user with one of the suppliers. If the user is not a registered user, the BR automatically returns a negative authorization response (AuthReS) message to the ES. The authorization response message is structured as follows:

AuthReS = P_{ID} || TID || MP || DEC where DEC represents a binary decision of two values. Allow for a positive response and Deny for a negative response. The authorization response is encrypted using the public key of the ES and signed by the BR's private key. In this case, the response from the BR to the ES can be shown as: BR → ES := $E_{KR_{BR}}[E_{KU_{ES}}[AuthReS]]\ ||\ E_{KU_{ES}}[AuthReS]$ where AuthReS = P_{ID} || TID || MP || Deny.

II. If the user is a registered user with one of the suppliers, the BR finds the supplier ID for the user from its database (HS_{ID} in this case). The BR then sends the message received from the user (MtoHS || T_2) to the home supplier after encrypting it with the public key of HS and signing it with its private key. A copy of the message is also kept at the BR for future use in case of any disputes. This message is described as: BR → HS := $E_{KR_{BR}}[E_{KU_{HS}}[MtoHS\ ||\ T_2]]\ ||\ E_{KU_{HS}}[MtoHS\ ||\ T_2]$.

c. Upon receiving the message, the HS verifies the integrity and origin of the message. Then checks the following two conditions before returning an authorization response to the BR:

   I. Find the real ID (V_{ID}) of the vehicle corresponding to P_{ID} in its database and checks if the user is allowed to use the vehicle.
   II. Check if the user has enough credit to support the requested payment amount MP.

   If both of the above two conditions are satisfied, the HS returns a positive authorization response to the BR as: AuthReS = P_{ID} | | TID | | MP | | Allow, otherwise, it returns a negative authorization response as:

   AuthReS = P_{ID} | | TID | | MP | | Deny.

   HS → BR = $E_{KR_{HS}}[E_{KU_{BR}}[\text{AuthReS}]]$ | | $E_{KU_{BR}}[\text{AuthReS}]$.

d. When the BR receives an authorization response from the HS, it verifies its origin and integrity. The BR decrypts the message using its private key. Then encrypts it using the public key of the ES, signs it and sends it to the ES. The BR also keeps a copy of the response for future use. This can be depicted as:

   AuthReS = P_{ID} | | TID | | MP | | Allow or AuthReS = P_{ID} | | TID | | MP | | Deny.

   BR → ES := $E_{KR_{BR}}[E_{KU_{ES}}[\text{AuthReS}]]$ | | $E_{KU_{ES}}[\text{AuthReS}]$.

3. Charging Response

   a. When the ES receives the authorization response from the BR, it verifies that the message integrity is preserved and that the message comes from the BR by using the public key of BR. It then decrypts the authorization response using its private key, $KR_{ES,}$ and prepares a charging response (CharRes) message to be sent to the EVSE. The charging response is encrypted using the EAG's public key and signed by the private key of the ES. This is expressed as:

   CharRes = P_{ID} | | TID | | Allow or CharRes = P_{ID} | | TID | | Deny.

   ES → EAG :=$E_{KR_{ES}}[E_{KU_{EAG}}[\text{CharRes}]]$ | | $E_{KU_{EAG}}[\text{CharRes}]$.

   b. Upon receiving the charging response from the ES, the EAG verifies that the response comes from the ES and that the message is not changed in transit. The EAG decrypts the message using its private key. Then the EAG sends the message to the SM after encrypting it using the public key of the SM and signing it using its private key. The EAG also keeps a copy of the response for future use. This is described as:

   CharRes = P_{ID} | | TID | | Allow or P_{ID} | | TID | | Deny.

   EAG → SM := $E_{KR_{EAG}}[E_{KU_{SM}}[\text{CharRes}]]$ | | $E_{KU_{SM}}[\text{CharRes}]$.

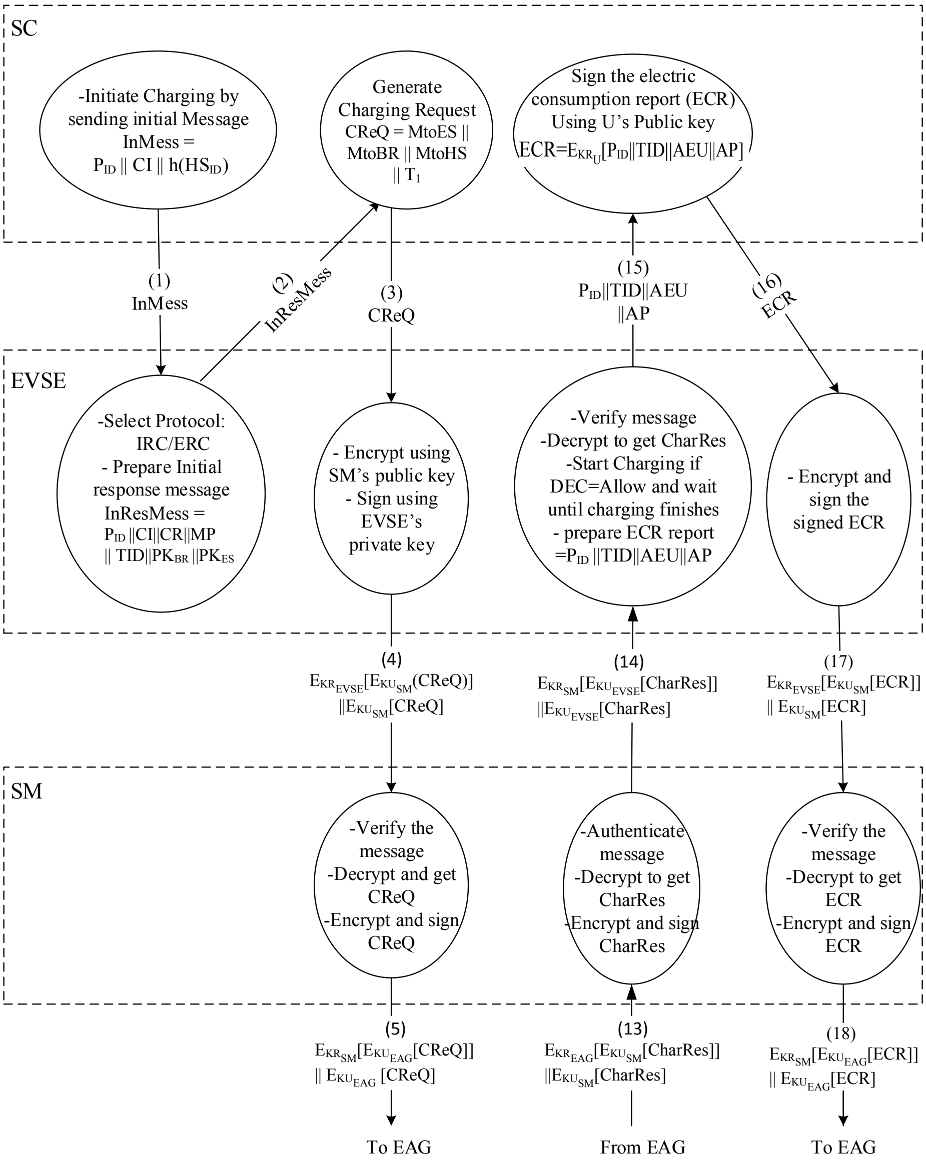
   c. The SM sends the message to the EVSE in a similar way as was done by the EAG: SM → EVSE := $E_{KR_{SM}}[E_{KU_{EVSE}}[\text{CharRes}]]$ | | $E_{KU_{EVSE}}[\text{CharRes}]$.

   d. When the charging response message is received by the EVSE, it either allows charging or denies it based on the response. If the charging response is positive, the PEV starts charging. While charging, the EVSE records the actual electricity usage (AEU) of the PEV and makes sure that it does not exceed the REA. The EVSE stops the charging process if the AEU reaches the REA or the PEV is fully charged.

4. Payment Capture

   a. The payment capture procedure starts immediately after the charging is complete. Similar to the IRC case, the EVSE prepares an ECR and forwards it to the SC. The SC signs the ECR with the private key of the user and sends it back to the EVSE as: U → EVSE := ECR where ECR = $E_{KR_{UB}}[P_{ID} \mid\mid TID \mid\mid AEU \mid\mid AP]$.

The ECR message is then sent to the SM, forwarded by the SM to the EAG which sends it to ES and the BR in a similar way as was explained before (encrypting with the public key of the receiver and signing with the private key of the sender). Both the EAG and the ES maintain a copy of the ECR before forwarding it to the next receiver. As soon as the BR receives the ECR message from the ES, it performs the following steps: Verifies that the ERC message is generated by U by using U's public key received earlier during the authorization stage, the BR forwards a copy of the ECR to the HS, the BR finds the actual payment (AP) from the ECR, deposits AP amount of money into the ES's account and subtracts the same amount from the account of the HS. The HS on the other hand upon receiving the ECR message from the BR it verifies that the ECR is prepared by U by decrypting it using U's public key and bills user U for the AP amount. The ERC protocol is illustrated by the FSM diagrams in Figures 8 and 9.



SC
-Initiate Charging by sending initial Message InMess = P_{ID} || CI || h(HS_{ID})
Generate Charging Request CReQ = MtoES || MtoBR || MtoHS || T_1
Sign the electric consumption report (ECR) Using U's Public key ECR=$E_{KR_U}[P_{ID}||TID||AEU||AP]$
(1) InMess
(2) InResMess
(3) CReQ
(15) P_{ID}||TID||AEU ||AP
(16) ECR
EVSE
-Select Protocol: IRC/ERC - Prepare Initial response message InResMess = P_{ID} ||CI||CR||MP || TID||PK_{BR} ||PK_{ES}
- Encrypt using SM's public key - Sign using EVSE's private key
-Verify message -Decrypt to get CharRes -Start Charging if DEC=Allow and wait until charging finishes - prepare ECR report =P_{ID} ||TID||AEU||AP
- Encrypt and sign the signed ECR
(4) $E_{KR_{EVSE}}[E_{KU_{SM}}(CReQ)]$ ||$E_{KU_{SM}}$[CReQ]
(14) $E_{KR_{SM}}[E_{KU_{EVSE}}[CharRes]]$ ||$E_{KU_{EVSE}}$[CharRes]
(17) $E_{KR_{EVSE}}[E_{KU_{SM}}[ECR]]$ || $E_{KU_{SM}}$[ECR]
SM
-Verify the message -Decrypt and get CReQ -Encrypt and sign CReQ
-Authenticate message -Decrypt to get CharRes -Encrypt and sign CharRes
-Verify the message -Decrypt to get ECR -Encrypt and sign ECR
(5) $E_{KR_{SM}}[E_{KU_{EAG}}[CReQ]]$ || $E_{KU_{EAG}}$ [CReQ]
(13) $E_{KR_{EAG}}[E_{KU_{SM}}[CharRes]]$ ||$E_{KU_{SM}}$[CharRes]
(18) $E_{KR_{SM}}[E_{KU_{EAG}}[ECR]]$ || $E_{KU_{EAG}}$[ECR]
To EAG
From EAG
To EAG

Figure 8. FSM diagram for ERC protocol.

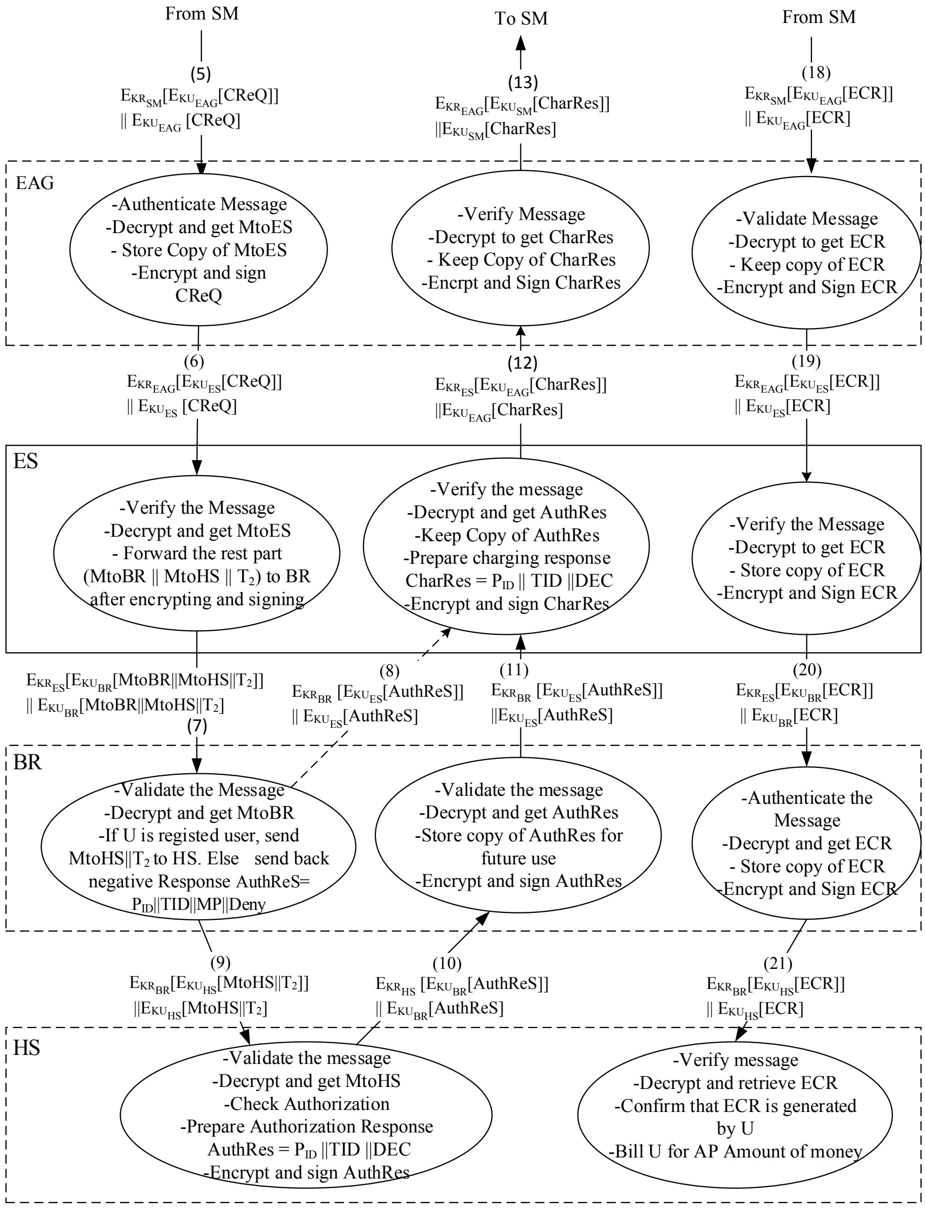
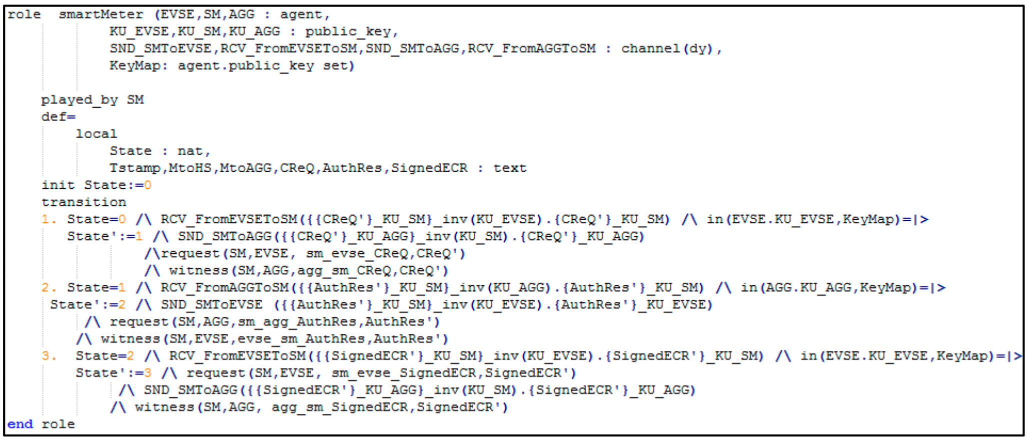

From SM
To SM
From SM
(5)
$E_{KR_{SM}}[E_{KU_{EAG}}[CReQ]]$
$\| E_{KU_{EAG}}[CReQ]$
(13)
$E_{KR_{EAG}}[E_{KU_{SM}}[CharRes]]$
$\|E_{KU_{SM}}[CharRes]$
(18)
$E_{KR_{SM}}[E_{KU_{EAG}}[ECR]]$
$\| E_{KU_{EAG}}[ECR]$
EAG
-Authenticate Message
-Decrypt and get MtoES
- Store Copy of MtoES
-Encrypt and sign
CReQ
-Verify Message
-Decrypt to get CharRes
- Keep Copy of CharRes
-Encrpt and Sign CharRes
-Validate Message
-Decrypt to get ECR
- Keep copy of ECR
-Encrypt and Sign ECR
(6)
$E_{KR_{EAG}}[E_{KU_{ES}}[CReQ]]$
$\| E_{KU_{ES}}[CReQ]$
(12)
$E_{KR_{ES}}[E_{KU_{EAG}}[CharRes]]$
$\|E_{KU_{EAG}}[CharRes]$
(19)
$E_{KR_{EAG}}[E_{KU_{ES}}[ECR]]$
$\| E_{KU_{ES}}[ECR]$
ES
-Verify the Message
-Decrypt and get MtoES
- Forward the rest part
(MtoBR || MtoHS || T_2) to BR
after encrypting and signing
-Verify the message
-Decrypt and get AuthRes
-Keep Copy of AuthRes
-Prepare charging response
CharRes = P_{ID} || TID ||DEC
-Encrypt and sign CharRes
-Verify the Message
-Decrypt to get ECR
- Store copy of ECR
-Encrypt and Sign ECR
$E_{KR_{ES}}[E_{KU_{BR}}[MtoBR\|MtoHS\|T_2]]$
$\| E_{KU_{BR}}[MtoBR\|MtoHS\|T_2]$
(7)
(8)
$E_{KR_{BR}}[E_{KU_{ES}}[AuthReS]]$
$\| E_{KU_{ES}}[AuthReS]$
(11)
$E_{KR_{BR}}[E_{KU_{ES}}[AuthReS]]$
$\|E_{KU_{ES}}[AuthReS]$
(20)
$E_{KR_{ES}}[E_{KU_{BR}}[ECR]]$
$\| E_{KU_{BR}}[ECR]$
BR
-Validate the Message
-Decrypt and get MtoBR
-If U is registed user, send
MtoHS||T_2 to HS. Else send back
negative Response AuthReS=
P_{ID}||TID||MP||Deny
-Validate the message
-Decrypt and get AuthRes
-Store copy of AuthRes for
future use
-Encrypt and sign AuthRes
-Authenticate the
Message
-Decrypt and get ECR
- Store copy of ECR
-Encrypt and Sign ECR
(9)
$E_{KR_{BR}}[E_{KU_{HS}}[MtoHS\|T_2]]$
$\|E_{KU_{HS}}[MtoHS\|T_2]$
(10)
$E_{KR_{HS}}[E_{KU_{BR}}[AuthReS]]$
$\| E_{KU_{BR}}[AuthReS]$
(21)
$E_{KR_{BR}}[E_{KU_{HS}}[ECR]]$
$\| E_{KU_{HS}}[ECR]$
HS
-Validate the message
-Decrypt and get MtoHS
-Check Authorization
-Prepare Authorization Response
AuthRes = P_{ID} ||TID ||DEC
-Encrypt and sign AuthRes
-Verify message
-Decrypt and retrieve ECR
-Confirm that ECR is generated
by U
-Bill U for AP Amount of money

Figure 9. FSM diagram for ERC protocol (continued from Figure 8).

5. Formal Verification of the Proposed Protocol

We used a software verification tool called AVISPA [33] to evaluate the security features of our charging protocol. AVISPA is considered a trusted verification tool by the research community nowadays. AVISPA stands for automatic verification and analysis of Internet security protocols. It consists of four back-ends: The On-the-fly Model-Checker OFMC, the Constraint-Logic-based Attack Searcher CL-AtSe, the SAT-based Model-Checker SATMC, and the Tree-Automata-based Protocol Analyzer (TA4SP protocol analyzer. All the backends work under the assumption that communications over the channel is according to the Dolev Yao model [34]. According to this model, the intruder has full control over the communication channel. To analyze a protocol using AVISPA, the protocol has to be expressed in High-Level Protocols Specification Language (HLPSL) [35].

In HLPSL, the action of each agent participating in the protocol is represented by a module similar to methods in programming languages called roles. Roles describe the initial parameters the participant can use, its initial state, and the sequence of actions performed by the agent. For instance, the HLPSL code in Figure 10 shows the role representing the SM in our protocol. As we can see from the figure, the role takes initial parameters such as a set of public keys (the public key of EVSE, aggregator and its own public key), the agents that will be communicating with it, the channel over which it communicates . . . etc. The set of actions performed by a role and the transitions it makes are also specified. In our HLPSL code, we defined roles for each of the entities such as User, EVSE, SM, Aggregators, Broker and Suppliers. However, due to space constraint, they are not shown here. After defining each basic role, we need to describe a composed role that specifies how roles interact with one another to form sessions of the protocol.



```
role  smartMeter (EVSE,SM,AGG : agent,
            KU_EVSE,KU_SM,KU_AGG : public_key,
            SND_SMToEVSE,RCV_FromEVSEToSM,SND_SMToAGG,RCV_FromAGGToSM : channel(dy),
            KeyMap: agent.public_key set)

    played_by SM
    def=
        local
            State : nat,
            Tstamp,MtoHS,MtoAGG,CReQ,AuthRes,SignedECR : text
    init State:=0
    transition
    1. State=0 /\ RCV_FromEVSEToSM({{CReQ'}_KU_SM}_inv(KU_EVSE).{CReQ'}_KU_SM) /\ in(EVSE.KU_EVSE,KeyMap)=|>
       State':=1 /\ SND_SMToAGG({{CReQ'}_KU_AGG}_inv(KU_SM).{CReQ'}_KU_AGG)
                /\request(SM,EVSE, sm_evse_CReQ,CReQ')
                /\ witness(SM,AGG,agg_sm_CReQ,CReQ')
    2. State=1 /\ RCV_FromAGGToSM({{AuthRes'}_KU_SM}_inv(KU_AGG).{AuthRes'}_KU_SM) /\ in(AGG.KU_AGG,KeyMap)=|>
     State':=2 /\ SND_SMToEVSE ({{AuthRes'}_KU_SM}_inv(KU_EVSE).{AuthRes'}_KU_EVSE)
         /\ request(SM,AGG,sm_agg_AuthRes,AuthRes')
        /\ witness(SM,EVSE,evse_sm_AuthRes,AuthRes')
    3.  State=2 /\ RCV_FromEVSEToSM({{SignedECR'}_KU_SM}_inv(KU_EVSE).{SignedECR'}_KU_SM) /\ in(EVSE.KU_EVSE,KeyMap)=|>
        State':=3 /\ request(SM,EVSE, sm_evse_SignedECR,SignedECR')
             /\ SND_SMToAGG({{SignedECR'}_KU_AGG}_inv(KU_SM).{SignedECR'}_KU_AGG)
            /\ witness(SM,AGG, agg_sm_SignedECR,SignedECR')
end role
```

Figure 10. Role for SM in HLPSL.

Moreover, a top-level role, called Environmental, is also defined which describes a session where the intruder also plays a role. In our model, we assumed that the intruder has knowledge of all the other agents, their public keys, hash functions and its own public/private key pair. The AVISPA tool analyzes the protocol based on the security goals specified by the user which describe the security requirements the protocol should fulfill. We analyzed our protocol using two of the back ends (OFMC and CL-AtSe) and it was found to be secure from various attacks as shown in Table 4.

Table 4. Attacks tested for using AVISPA.

Attack Type	Safe
Message confidentiality	✔
Message integrity	✔
Impersonation	✔
Replay attacks	✔
Repudiation	✔

6. Conclusions

In this paper, we have presented a comprehensive charging protocol and methods that allow secure and privacy-aware charging under various charging conditions. A PEV user can charge in different charging locations and under various access privileges known as charging modes. The security and privacy requirement for charging protocols is highly dependent on the user's charging mode. Thus, we first classified the user's charging modes into four main groups: private privileged user charging, guest user charging, internal roaming charging (IRC) and external roaming charging (ERC). Based on the charging mode, we propose local authentication methods for a private and guest user charging, in addition to the IRC and ERC protocols. This is based on using nested signatures, to protect users' privacy from external suppliers, their own suppliers and any third parties. Dual signatures are used for IRC and triple signatures for ERC. In addition, our approach supports anonymity for user authentication, for payment and for communication between suppliers to protect users' privacy. We have verified the protocol using the AVISPA software verification tool and the output indicates that our protocol is secure and working as expected under various possible attacks such as message modification, message content release and replay, repudiation and masquerading.

Acknowledgments: This research is funded by the United Arab Emirates University (UAEU) research grant number 31T060.

Author Contributions: The paper was a collaborative effort among the authors. The authors contributed collectively to the theoretical analysis, protocol and framework design, verification, and manuscript preparation.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Hwang, R. Future of Electric Vehicles is Bright. Available online: https://www.nrdc.org/experts/roland-hwang/future-electric-vehicles-bright/ (accessed on 23 January 2017).
2. Ismail, M.; Serpedin, E.; Qaraqe, K. PEV charging in the future smart grid. In Proceedings of the 2015 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 9–10 July 2015; pp. 1–4.
3. Randall, T. Here is How Electric Cars Will Cause the Next Oil Crisis. Available online: http://www.bloomberg.com/features/2016-ev-oil-crisis/ (accessed on 23 January 2017).
4. Chaudhry, H.; Bohn, T. Security concerns of a plug-in vehicle. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; pp. 1–6.
5. Mustafa, M.A.; Zhang, N.; Kalogridis, G.; Fan, Z. Smart electric vehicle charging: Security analysis. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
6. Carryl, C.; Ilyas, M.; Mahgoub, I.; Rathod, M. The PEV security challenges to the smart grid: Analysis of threats and mitigation strategies. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 300–305.
7. Aloul, F.; Al-Ali, A.R.; Al-Dalky, R.; Al-Mardini, M.; El-Hajj, W. Smart Grid Security: Threats, Vulnerabilities and Solutions. *Int. J. Smart Grid Clean Energy* **2012**. [CrossRef]
8. Han, W.; Xiao, Y. Privacy preservation for V2G networks in smart grid: A survey. *Comput. Commun.* **2016**, *91–92*, 17–28. [CrossRef]
9. Guo, H.; Wu, Y.; Bao, F.; Chen, H.; Ma, M. UBAPV2G: A Unique Batch Authentication Protocol for Vehicle-to-Grid Communications. *IEEE Trans. Smart Grid* **2011**, *2*, 707–714. [CrossRef]
10. Liu, H.; Ning, H.; Zhang, Y.; Xiong, Q.; Yang, L.T. Role-Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 208–220. [CrossRef]
11. Chen, J.; Zhang, Y.; Su, W. An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks. *China Commun.* **2015**, *12*, 9–19. [CrossRef]
12. Saxena, N.; Choi, B.J. Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1438–1452. [CrossRef]
13. Zhang, Y.; Gjessing, S.; Liu, H.; Ning, H.; Yang, L.T.; Guizani, M. Securing vehicle-to-grid communications in the smart grid. *IEEE Wirel. Commun.* **2013**, *20*, 66–73. [CrossRef]
14. Nicanfar, H.; Fard, P.T.; Hosseininezhad, S.; Leung, V.C.M.; Damm, M. Security and privacy of electric vehicles in the smart grid context: Problem and solution. In Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Barcelona, Spain, 3–8 November 2013; ACM: New York, NY, USA; pp. 45–54.
15. Liu, H.; Ning, H.; Zhang, Y.; Guizani, M. Battery status-aware authentication scheme for V2G networks in smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 99–110. [CrossRef]
16. Au, M.H.; Liu, J.K.; Fang, J.; Jiang, Z.L.; Susilo, W.; Zhou, J. A New Payment System for Enhancing Location Privacy of Electric Vehicles. *IEEE Trans Veh. Technol.* **2014**, *63*, 3–18. [CrossRef]
17. Mustafa, M.A.; Zhang, N.; Kalogridis, G.; Fan, Z. Roaming electric vehicle charging and billing: An anonymous multi-user protocol. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 939–945.

18. García-Villalobos, J.; Zamora, I.; Martín, J.I.S.; Asensio, F.J.; Aperribay, V. Plug-in electric vehicles in electric distribution networks: A review of smart charging approaches. *Renew. Sustain. Energy Rev.* **2014**, *38*, 717–731. [CrossRef]
19. Román, T.G.S.; Momber, I.; Abbad, M.R.; Miralles, Á.S. Regulatory framework and business models for charging plug-in electric vehicles: Infrastructure, agents, and commercial relationships. *Energy Policy* **2011**, *39*, 6360–6375. [CrossRef]
20. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38. [CrossRef]
21. Bessa, R.J.; Matos, M.A. Economic and technical management of an aggregation agent for electric vehicles: A literature survey. *Int. Trans. Electr. Energy Syst.* **2012**, *22*, 334–350. [CrossRef]
22. Lopes, J.A.P.; Soares, F.J.; Almeida, P.M.R. Integration of electric vehicles in the electric power system. *Proc. IEEE* **2011**, *99*, 168–183. [CrossRef]
23. Guille, C.; Gross, G. Design of a conceptual framework for the V2G implementation. In Proceedings of the 2008 IEEE Energy 2030 Conference, Atlanta, GA, USA, 17–18 November 2008; pp. 1–3.
24. Bessa, R.J.; Matos, M.A. The role of an aggregator agent for EV in the electricity market. In Proceedings of the 7th Mediterranean Conference and Exhibition on Power Generation, Transmission, Distribution and Energy Conversion (MedPower 2010), Agia Napa, Cyprus, 7–10 November 2010; pp. 123–131.
25. Stalling, W. *Cryptography and Network Security: Principles and Practice*, 6th ed.; Prentice Hall, Inc.: Upper Saddle River, NJ, USA, 2014.
26. Chan, A.C.; Zhou, J. On smart grid cybersecurity standardization: Issues of designing with nistir 7628. *IEEE Commun. Mag.* **2013**, *51*, 58–65. [CrossRef]
27. Kalogridis, G.; Sooriyabandara, M.; Fan, Z.; Mustafa, M.A. Toward Unified Security and Privacy Protection for Smart Meter Networks. *IEEE Syst. J.* **2014**, *8*, 641–654. [CrossRef]
28. Chan, A.C.F.; Zhou, J. A Secure, Intelligent Electric Vehicle Ecosystem for Safe Integration with the Smart Grid. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 3367–3376. [CrossRef]
29. Han, W.; Xiao, Y. IP2DM for V2G networks in Smart Grid. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 782–787.
30. Hoang, D.T.; Wang, P.; Niyato, D.; Hossain, E. Charging and Discharging of Plug-In Electric Vehicles (PEVs) in Vehicle-to-Grid (V2G) Systems: A Cyber Insurance-Based Model. *IEEE Access* **2017**, *5*, 732–754. [CrossRef]
31. He, M.; Zhang, K.; Shen, X. PMQC: A privacy-preserving multi-quality charging scheme in V2G network. In Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM'14), Austin, TX, USA, 8–12 December 2014.
32. Smart Charge Rewards. Available online: http://www.fleetcarma.com/ (accessed on 10 July 2017).
33. Avispa—Automated Validation of Internet Security Protocols and Applications, 2006. Available online: http://www.avispa-project.org/ (accessed on 23 January 2017).
34. Dolev, D.; Yao, A. On the Security of Public-Key Protocols. *IEEE Trans. Inf. Theory* **1983**, *2*, 198–208. [CrossRef]
35. AVISPA. Deliverable 2.1: The High-Level Protocol Specification Language, 2003. Available online: http://www.avispa-project.org/ (accessed on 23 January 2017).