Prevention of Unauthorized Unplugging of Unattended Recharging EVs

Raziq Yaqub[1], Azzam ul Asar[2], Fahad Butt[2] and Umair Ahmed Qazi[2]

[1]*CECOS University, Peshawar, Pakistan; and NIKSUN, Inc., Princeton, NJ, USA; e-mail: ryaqub@niksun.com*
[2]*CECOS University, Peshawar, Pakistan; e-mail: fahad_butt44@yahoo.com; umair.qazi123@hotmail.com*

Received 15 January 2013; Accepted 19 April 2013

Abstract

Charging time required by the charging nodes may be up to 5 hours. Due to long charging times, it is possible that drivers will leave their EVs unattended to run other errands while the vehicle is being charged. Unauthorized Unplugging of Unattended (UUU = Triple U, or 3U) vehicle is foreseen as a major issue. The 3U issue will not only result in stoppage of ongoing charging, but also cause frustration for the drivers, and concern for the law enforcer. This paper addresses this problem and presents a method that prevents unauthorized unplugging of EV.

Keywords: Automobile Recharging Nodes (ARN), Unauthorized Unplugging of Unattended Recharging (UUU), electric vehicle.

1 Introduction

Media predict that by 2015 the U.S. will have almost 1 million publicly accessible Electric Vehicle (EV) recharging nodes [1]. The charging time required by the commercial charging facilities may vary from 15 minutes to 5 hours [2] depending on the state of charge of the vehicle, and the Automobile Recharging Node's (ARN) capabilities. Due to long charging times,

it is possible that drivers will leave their EVs unattended to run other errands, or kill their time entertaining themselves while the vehicle is being charged. Unauthorized Unplugging of Unattended (UUU = Triple U, or 3U) vehicle is foreseen as a major issue. The 3U issue will not only result in stoppage of ongoing charging, but also cause frustration for the drivers, and concern for the law enforcer. 3U may be committed by misbehaved teens, or EV drivers who might be in a hurry. Such drivers may double park, unplug the charging connector to interrupt ongoing charging, and unethically plug in their own EV for charging. This paper addresses this problem and presents a method that prevents unauthorized unplugging of EV.

According to the method proposed in this paper, upon authentication of the EV driver (e.g. for billing purpose), the ARN will electronically lock the EV charging connector, and establish the security association between the proposed locking mechanism and the EV driver. The security association will result in generating a unique, encrypted, secure digital key (called triple U-Key or 3U-KEY) for the every charging event. The 3U-KEY would be delivered by the ARN to the EV driver upon starting the EV recharging, and would be required to unlock the EV charging connector. Without presentation of the 3U-KEY, the ARN will not unlock the EV charging connector. (The EV charging connector is simply called 'connector' hereinafter.)

The proposed solution will not only prevent Unauthorized Unplugging of Unattended recharging EVs, but also offer several other benefits, e.g. perfect coupling between Charge Coupler (connector and receptacle that connects the electric charging source to electric vehicle), guaranteed disconnection of electrical power supply before attempting to unplug the connector, that would eliminate electrical hazards, capability to unlock the connector by first respondents under potential hazardous or emergency situations even without providing the 3U-KEY, through interaction with the System Administrator.

2 Detailed Description

According to the method proposed here, the ARN is equipped with a mechanism of electronically locking and releasing the charge connector. The electronic lock may exist either in ARN (if the connector and cable is the part of EV, and Receptacle is in the ARN), or in the connector (if the connector and cable is the part of ARN, and Receptacle is in the EV). This mechanism locks the connector in a way that the connector release button either locks or becomes dysfunctional such that the connector cannot be released even on pressing the release connector button. Such locking mechanism locks the

connector at the time of charging and delivers an electronic key to the EV driver. The connector is unlocked only by the authorized person who holds the key. Failure in presenting the 3U-KEY to ARN will not unlock the connector.

Electronic key delivery to an EV driver is globally unique for each charging event. We refer to this key as the 3U-KEY. The 3U-KEY is generated by the proposed Unauthorized Unplugging of Unattended EV mechanism, and delivered as encrypted Bar Code, QR Code, or any state of the art secure encrypted code.

The proposed solution will not only prevent Unauthorized Unplugging of Unattended recharging but also offer several other benefits, e.g. (a) perfect coupling between mating parts engaged in high voltage connection, (b) guaranteed disconnection of electrical power supply before unlocking the connector to eliminate electrical hazards, (c) communication capability between system administrator and EV driver/emergency respondents to unlock the connector under hazardous or emergency situations while EV driver is away, or when the system does not accept 3U-KEY due to malfunctioning.

3 Functional Entities

Our method consists of several functional entities as shown in Figure 1. These entities essentially comprise of hardware and software capable of processing tasks pertinent to the present paper. The hardware of the data processing system may comprise of, e.g., lock mechanism, central processing unit (CPU), memory unit, liquid crystal display scanner/printer unit, internal interfaces/buses for wireless/wireline for short/long range communication as shown in Figure 1. The logical entities are discussed in Section 4 and shown in Figure 3.

The whole mechanism works together for authorized disconnection of connector. The 3U-KEY may be:

a. Delivered to the EV driver on a passive device (which does not require a battery, e.g. paper tag). Thus the proposed 3U method has the capability of printing and dispatching the 3U-KEY on a tag. The holder of the passive tag can only unlock and get the released by presenting the physical tag to the ARN. To unlock the connector, the physical possession of the passive tag and the physical presence of tag holder near ARN is required by the system.
b. Delivered to the EV driver on an active device (e.g. mobile device as soft key), thus 3U mechanism has the capability of delivering a 3U-KEY us-

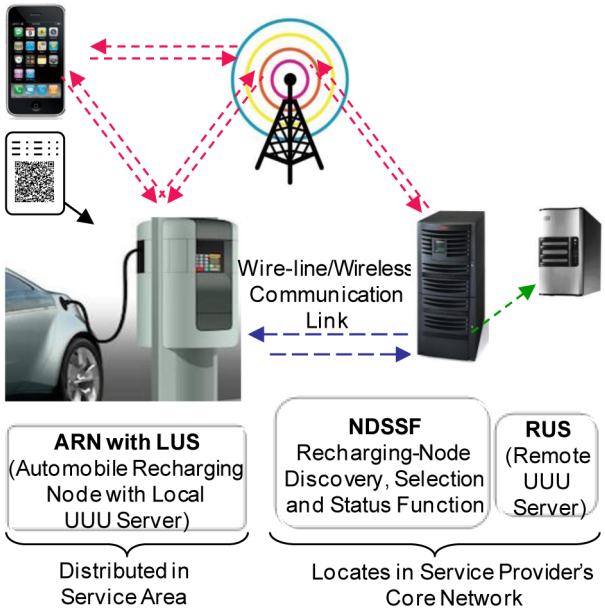

Figure 1 Authorized disconnection of connector.

ing any existing or evolved short range communication, e.g. Near Field Communication. To unlock the connector, the physical presence of the 3U-KEY holder near the ARN is not required.

c. Associated with the EV driver's biometrics. Thus the KGVF memorizes the 3U-KEY, at least until the EV charging event is over and/or the EV is delivered to its driver by presenting the same biometrics. Thus the proposed mechanism has the capability of scanning fingerprint, retina or face, and memorizing the images using any existing or evolved state of the art biometrics technologies. To unlock the connector, the physical presence of the 3U-KEY holder near the ARN is required.
d. Associated with the EV driver's card (e.g. credit card, pre-paid card, gift card, membership card, or any other card or coupon). Thus the KGVF memorizes the 3U-KEY, at least until the EV charging event is over and/or the EV is delivered to its driver by presenting/swiping the same card. Thus the proposed mechanism has the capability of reading cards and memorizing the information using existing or evolved state of the art Card Reading technologies. To unlock the connector, the physical

presence of the 3U-KEY holder near the ARN may or may not be required.

e. Delivered using a combination of the above noted schemes to enhance security.

The 3U-Key may also be based on the EV driver credentials, where the ARN may prompt the EV driver to enter his EV license plate number, and a password of his own choice to initiate charging and enters the same to retrieve the EV. This setting has been programmed by students of the CECOS University, Peshawar, Pakistan, and is shown in Figures 2a and 2b.

4 Logical Entities

4.1 Remote 3U Server (RUS)

The RUS is located in the service provider's network. It may be an independent server or a part of Customer Information Server [1]. (In contrast, the LUS is a part of the ARN [1], and is distributed throughout the service area.) RUS and LUS communicate logically through ARN and NDSSF [1] over any available state of the art communication systems, i.e. wireless (LTE, WiMAX), or wireline systems (Optical fiber, or Ethernet, BPL, etc.). Their ability to communicate provides several attractive features, for example:

- Remote recharging status query: The EV driver can send a "recharging status query" to the RUS geographically from anywhere by providing the 3U-KEY in the request message, and will get a response. This feature will be helpful to know the EV recharging status or any other relevant information without physically visiting the location.
- Remote EV claim: The EV driver can deactivate the locking mechanism by providing the 3U-KEY in the message from anywhere to release connector. This feature will be helpful to authorize the EV driver's proxy to claim the EV, without having the EV owner/driver physically visiting the location. Thus the EV may be dropped by one family member and picked up by the other, if authorized by the 3U-KEY holder remotely.

For the above features, the EV driver may send a message, either directly to the RUS only, or the LUS only, or to both, LUS or RUS. Each option has merits and demerits, e.g., the former option offers better security features and system control, whereas the latter reduces system signaling overhead, system messaging efficiency, and response delay, etc. In this paper we propose and support all the options.

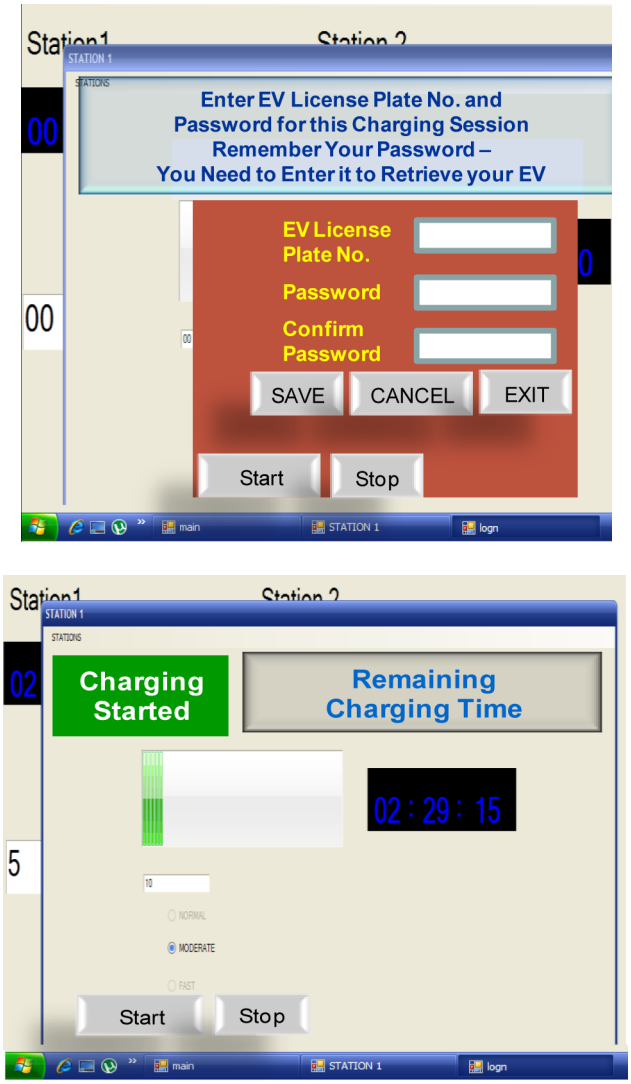

Figure 2 (a) ARN prompts to initiate charging. (b) ARN starts charging.

As shown in Figure 3, the RUS interfaces with a System Administrative. The System Administrative may be a human being or a Voice Activated/Speech Recognition intelligent system. It provides the communication capability between, e.g., Emergency Respondents, or the EV driver and the

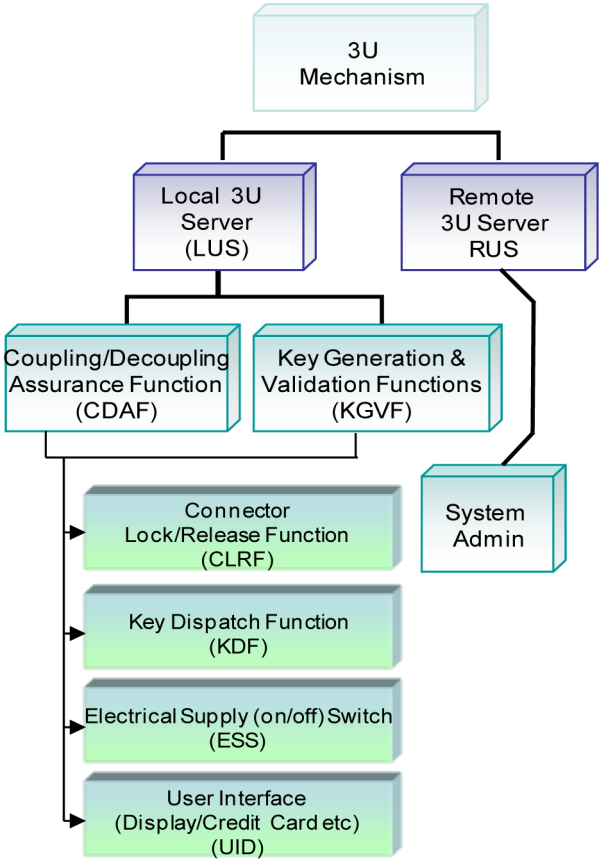

Figure 3 Functional entities of the 3U mechanism.

System Administrator. This feature is useful for several emergency scenarios, for example:

a. the legitimate EV driver lost the 3U-KEY and wants to unlock the connector, or
b. there is potential hazard in the surrounding environment (e.g. a fire) while the EV driver is away and law enforcement agencies need immediate removal of the connector/EV, or
c. the system malfunctions and denies to accept the 3U-KEY, or
d. any other unforeseen reason that mandates to unlock the connector without presenting the 3U-KEY to the system.

4.2 Local 3U Server (LUS)

The LUS is located in the ARN [1]. Upon authentication of the EV driver's credentials (for billing purpose), the LUS will electronically lock the connector. The connector can be unlocked only by presenting the same credentials. Thus the LUS will prevent unauthorized unplugging of unattended EV already being charged.

More specifically according to the method proposed in this paper, upon authentication of the EV driver's credentials the LUS (housed in the ARN) will electronically lock the connector, and establish the security association between the ARN locking mechanism and the EV driver's credentials. The security association will result in generating a unique, encrypted, secure digital key (which we call 3U-KEY) for the every charging event. The 3U-KEY would be delivered by the LUS to the EV driver before starting the EV recharging. The LUS will require the same 3U-Key to unlock the EV charging connector. Without presentation of 3U-KEY, the LUS will not unlock the EV charging connector.

Following the four sub-functional entities assist the LUS in performing its functions. These entities comprise of hardware and, software to perform the tasks pertinent to the present paper. The hardware may, for example, comprise of central processing unit (CPU), memory unit, scanner/printing unit, connector locking mechanism, liquid crystal display (LCD), bus(es) for internal communication, wireless or wireline channels for external communication, and relays/switches, etc. The software may comprise of programs, algorithm and protocols, and so on These functional entities work in coordination:

a. to electronically lock the connector,
b. to establish the security association between the EV driver's credentials and the connector locking mechanism,
c. to generate the 3U-KEY,
d. to deliver the 3U-KEY to the EV driver,
e. to demand the same 3U-KEY to unlock and relinquish the connector, and
f. to unlock the connector on successful presentation and validation of the 3U-KEY.

Unlocking of the connector can be triggered either (a) by the EV driver at any time during or upon completion of the recharging process, or (b) by the LUS upon 100% completion of the charging.

The 3U-KEY may be generated in the form of encrypted Bar Code, QR Code, or any state of the art secure encrypted security Code. The delivery

of 3U-KEY to the EV driver may take any one or any combination of the following:

a. Deliver to the EV driver on a passive device (e.g. a tangible/paper tag that does not require a battery). Thus the 3U mechanism has the capability of printing and dispatching the 3U-KEY on a tag using any existing or evolved state of the art mechanisms. The holder of the passive tag can only activate the unlocking mechanism and get the connector released by presenting the physical tag to ARN. Physical possession of the passive tag and physical presence of tag holder near ARN is required by the system.
b. Deliver to the EV driver on an active device (this requires a battery, e.g. mobile communication device as soft key). Thus the 3U mechanism has the capability of delivering a 3U-KEY using any existing or evolved state of the art short range communication, e.g. Near Field Communication (NFC). If the 3U-KEY is delivered to the EV driver's mobile communication device over NFC, the holder of the 3U-KEY can deactivate the lock and get the connector released by presenting the 3U-KEY to ARN in the following two ways:
    i. Presenting the 3U-KEY to the ARN over NFC. NFC is a short-range wireless technology, typically requiring a distance of 4 cm or less. NFC operates at 13.56 MHz and at rates ranging from 106 to 848 kbit/s. NFC always involves an initiator (mobile device in this case) and a target (ARN in this case). Physical possession of the active device and physical presence of the 3U-KEY holder is required to claim the EV.
    ii. Presenting the 3U-KEY to the ARN over a local or wide area network (WLAN, WiMAX, LTE, wireline, or any state of the art network). Physical possession of the active device is required but physical presence of the 3U-KEY holder is not required. Thus the owner of EV may authorize his driver or proxy to claim the vehicle, from the location for which the unlocking step was performed by the owner from remote location.

    The EV driver's mobile device may also generate an RF field to read and download the 3U-KEY from a passive tag and deactivate the lock using his mobile device as noted in (a) and (i) above. However, in such a scenario (i.e. LUS issued 3U-KEY on a passive device, and receives 3U-KEY from an active device), additional security measures are built in,

e.g. the system may require drivers' license number upon relinquishing the EV.

c. Associate with the EV driver's biometrics. Thus KGVF memorizes the 3U-KEY, at least till the EV charging event is over and/or EV is delivered to its driver by presenting the same biometrics. Thus the proposed mechanism has the capability of scanning fingerprint, retina or face, and memorizing the images using any existing or evolved state of the art biometrics technologies. If the 3U-KEY is associated with the EV driver's Biometrics (based on fingerprint scan, retina scan, or face scan or combination of these) memorized by the ARN, physical presence is required to claim the EV by presenting the same combination of biometrics. (In case of biometrics, it is encouraged implementing combination and or scan of state issued ID card. It would discourage the possibility of dodging the system by using contact lens, gloves, or any other masking means, etc.)
d. Associate with the EV driver's card (e.g. credit card, pre-paid card, gift card, membership card, license, or any other card). Thus KGVF memorizes the 3U-KEY, at least till the EV charging event is over and/or the EV is delivered to its driver by presenting the same card. Thus the proposed mechanism has the capability of reading cards and memorizing the information using existing or evolved state of the art card reading technologies. If the 3U-KEY is associated with the EV driver's Credit Card, memorized by the ARN, physical swipe of the same card is required to claim the EV.

In a charge-status query mode, the 3U-KEY may be presented over local or wide area network (WLAN, WiMAX, LTE, wireline, or any state of the art network) to enquire the status of charging. LUS or RUS, in response, will send the charging status (such as for example fully (100%) charged at time HH:MM:SS on date MM/DD/YYYY, or half (50%) charged at time HH:MM:SS on date MM/DD/YYYY, or any other format most meaningful for the EV driver. (Deactivation of lock from remote may require confirmation to avoid accidental deactivation of the lock, e.g. the user did not intend to unlock the vehicle but just wanted to know the recharging status).

The LUS consists of a Coupling/Decoupling Assurance Function (CDAF) and Key Generation and Validation Functions (KGVF). These are shown in Figure 4.

4.3 Coupling/Decoupling Assurance Function (CDAF)

The CDAF is a major part of LUS and is housed in ARN. It communicates with the RUS (located in the service providers' network), as well as local entities (located with in the ARN), to perform and assure connector lock/release related tasks. Communication with RUS may be over any state of the art long distance wireless or wireline communication system, whereas the communication with local entities may be over any short range communication system (such as wireless personal area networks, wireless local area networks, or any other state of the local wireless or wireline communication link). Before the mechanism unlocks the connector, CDAF makes sure that all the electrical circuits are completely disconnected and high level of shielding and sealing is in place. This offers hazard free disconnect.

4.4 Key (3U-KEY) Generation and Validation Function (KGVF)

KGVF is another major part of LUS and is housed in ARN. It communicates with the RUS (located in the service provider's network) as well as local entities (located with in the ARN) to perform connector lock/release related tasks. The communication with RUS may be over any state of the art long distance wireless or wireline communication system, whereas the communication with local entities may be over any short range communication system (such as wireline or wireless personal area networks, wireless local area networks, or any other state of the communication link).

KGVF is responsible for establishing a security association between the EV driver's credentials and the locking mechanism for any charging event, and consequently generating a 3U-KEY. The 3U-KEY may be generated based on time stamp, recharging node's civic address/GPS coordinates, IP address, ARN identity number, a random key generator, user's credentials (from credit card/membership card, biometrics), any other parameters, and/or any state of the art security key generation algorithm, that ensure a strong security association. (The ARN IP address may be either encrypted or clear text depending on the service provider's business model and security requirements.)

The 3U-KEY can be successfully decoded by any LUS to provide information that may be useful for the EV driver. For example if the EV driver parked the EV for recharging at location "X" and presents the 3U-KEY at location "Y". In such an event, the KGVF may take two actions:

a. Search its own log/database and informs the EV driver that the 3U-KEY was not issued from this location, and
b. Take an additional step i.e. send a query to RUS and get the correct location (civic address) from where the 3U-KEY was issued. This would be beneficial if the EV driver forgot where he parked his car for recharging. However, it may raise security concern, i.e. a stolen/lost-found 3U-KEY may be used to find the EV driver's car, which may not be desirable. Thus this feature may be optionally turned on or off.
c. Take an additional step, i.e. send a query to RUS and get the updated information (e.g. EV is at xx location and yy% charge, or EV had already been claimed at HH:MM:SS on MM/DD/YYYY.

Following local entities assist CDFA and KGVF to achieve the 3U objectives:

- User Interface and Display (UID);
- Connector Lock/Release Function (CLRF);
- Key Dispatch Function (KDF);
- Electrical Supply (On/Off) Switch (ESS).

The functions of CDAF, KGVF, UID, CLRF, KDF and ESS can be easily understood by considering the scenarios presented in Figures 4, 5 and 6.

4.5 3U-KEY Issuance and Recharging Start Event

Figure 4 (with the following description) shows the steps involved in 3U-KEY Issuance and Recharging Start Event:

a = CRR informs CDAF that the connector is coupled
b = UID gets user credentials (e.g. credit card) through user interface and feeds to DKGF. (In this step it also gets user's preference for delivery of the encrypted 3U-KEY, e.g. tag, mobile device, biometrics, card, etc., and activates the related mechanism, e.g. in case of the biometrics option, it activates the scanner for fingerprint/retina/face scan)
c = DKGF authenticates the user with RUS for billing purpose
d = DKGF informs CDAF if the authentication is successful (unsuccessful auth. is informed to UID)
e = CDAF sends message to CLRF to lock the connector
f = CLRF locks the connector and acknowledges back to CDAF
g = CDAF advices On/Off switch to turn on electric supply for EV recharging
h = On/Off switch turns the connection ON and send acknowledgement to CDAF

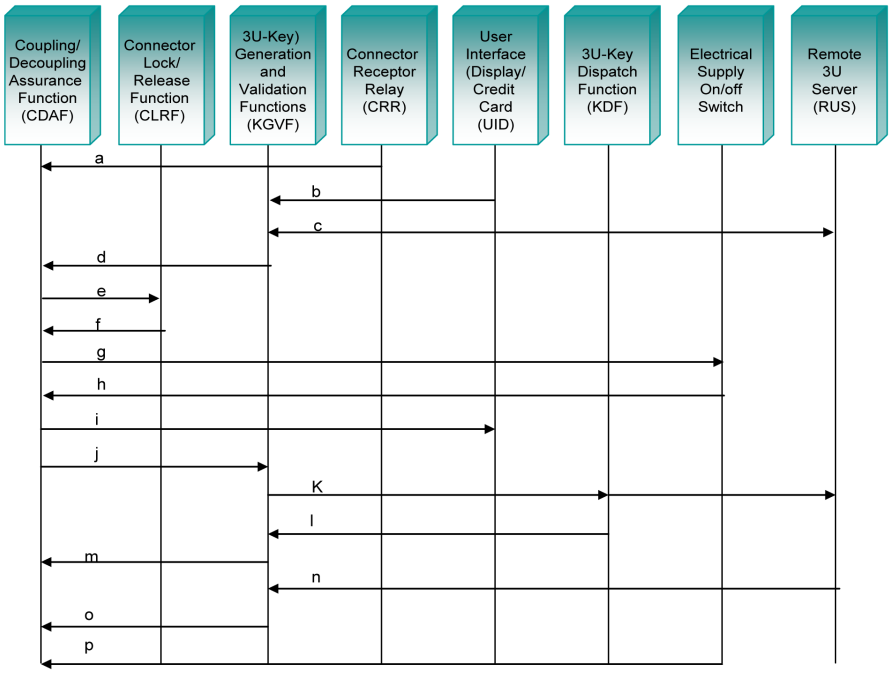

Figure 4 3U-Key Issuance and Recharging Start Event.

i = CDAF informs the user that EV charging started and 3U-KEY generation is in progress
j = CDAF advices DKGF to deliver the 3U-KEY to KDF
k = DKGF delivers the 3U-KEY to KDF (for dispatch to user) and to RUS (for provisioning of value added services and log/record keeping). (KDF delivers the 3U-KEY to the EV driver on the device of his choice, e.g. in case of paper tag, it activates the printer, in case of mobile device, it activates the communication circuitry (e.g. NFC, etc), in case of biometrics or card association, it saves the key in its own internal memory, till the EV charging event is over and driver had claimed the EV by presenting the same card or biometrics)
l = DKGF receives an acknowledgement from KDF
m = CDAF receives Acknowledgement from DKGF
n = DKGF receives an acknowledgement from the RUS
o = CDAF receives acknowledgement from DKGF

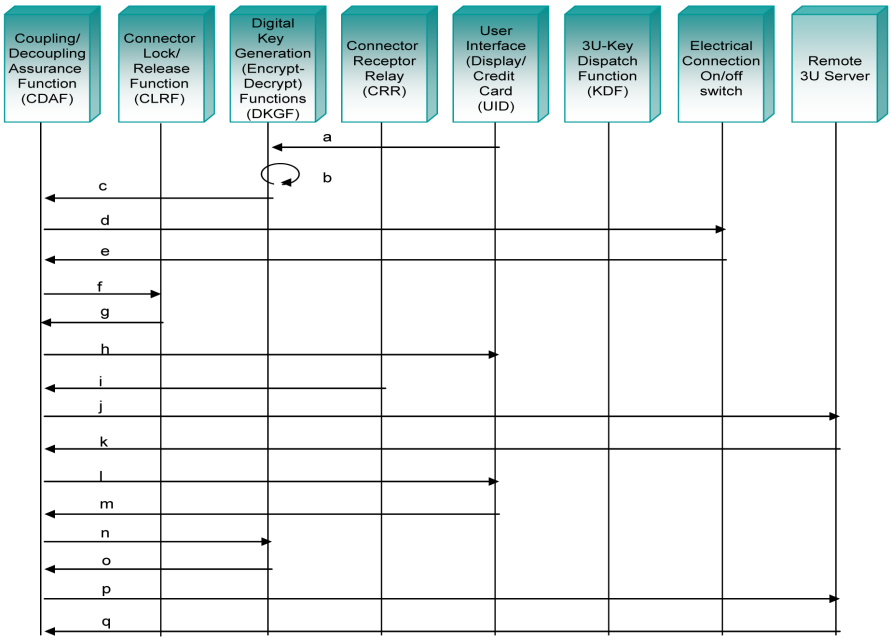

Figure 5 3U-Key Retrieval and Charging Stop Event initiated by the user.

p = ON/Off Switch continuous to measure the status of the battery charging every x seconds and sent to CDAF

If the RUS sends a query to CDAF (e.g. to find recharging status), the CDAF sends a response accordingly (not shown in figure).

4.6 3U-KEY Retrieval and Charging Stop Event Initiated by User

Figure 5 shows the steps involved in a 3U-KEY Retrieval and Charging Stop Event Initiated by the user.

The steps involved in 3U-KEY retrieval and charging stop event initiated by user (per Figure 5) are the following:

a = DKGF receives user's 3U-KEY (e.g. tag, credit card, mobile device) through local UID, (or RUS)
b = DKGF verifies association (decrypts the 3U-KEY) locally and/or with RUS
c = DKGF informs CDAF if the association is verified (unsuccessful verification is informed to UID)

d = CDAF sends message to On/Off Switch to turn off electric supply for EV recharging
e = On/Off switch turns the connection OFF and sends acknowledgement to CDAF with energy consumed
f = CDAF sends message to CLRF to unlock the connector
g = CLRF unlocks the connector and acknowledges back to CDAF
h = CDAF informs UID that EV charging is stopped, connector is unlocked and be removed to stop billing
i = CRR informs CDAF that connector is removed
j = CDAF sends RUS the EV charging duration (connector insertion to removal) and energy consumed
k = RUS sends bill (based on charging duration plus energy consumed) to CDAF
l = CDAF sends command to UID to print the receipt
m = UID delivers the receipt to the customer and acknowledges the delivery of receipt to CDAF
n = CDAF advices DKGF to delete the association (RUS retains the information for some predetermined time)
o = DKGF deletes the 3U-KEY Association and send acknowledgement to CDAF
p = CDAF updates RUS the complete log of charging event
q = RUS sends acknowledgement to DKGF (RUS treats the information as specified by the operator)

4.7 3U-KEY Retrieval and Charging Stop Event Initiated by 3U System

Figure 6 shows the steps involved in 3U-KEY Retrieval and Charging Stop Event Initiated by the 3U System.

The steps involved in a 3U-KEY Retrieval and Ccharging Stop Event initiated by the 3U System (per Figure 6) are the following:

a = On/Off Switch turns the connection OFF on 100% charging and sends acknowledgement to CDAF with energy consumed
b = CDAF informs RUS about the 100% completion status
c = RUS sends a text message to the EV driver
d = DKGF receives user's 3U-KEY (e.g. tag, credit card, mobile device) through local UID, or RUS
e = DKGF verifies association (decrypts the 3U-KEY) locally and/or with RUS

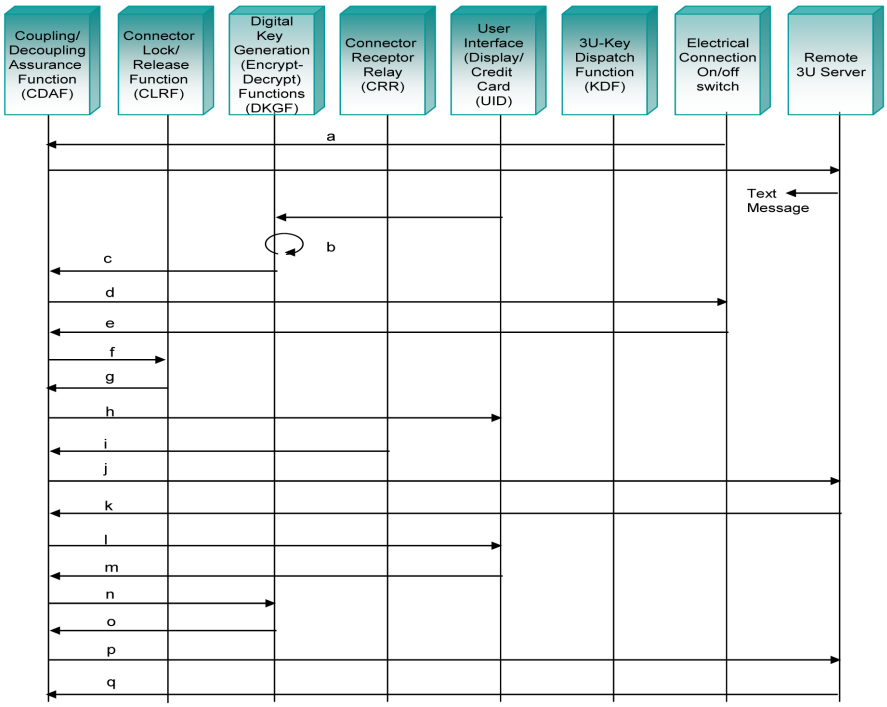

Figure 6 3U-Key Retrieval and Charging Stop Event initiated by 3U System.

f = DKGF informs CDAF if the association is verified (unsuccessful verification is informed to UID)
g = CDAF sends message to CLRF to unlock the connector
h = CLRF unlocks the connector and acknowledges back to CDAF
i = CDAF informs the user (UID) that EV charging was stopped at hh:mm:ss connector is unlocked and must be removed to stop billing
j = CRR informs CDAF that connector is removed
k = CDAF sends RUS the EV charging duration (between connector insertion and removal) and energy consumed
l = RUS sends bill (based on charging duration plus energy consumed) to CDAF
m = CDAF sends command to UID to print the receipt
n = UID acknowledges the delivery of receipt
o = CDAF advices DKGF to delete the association
p = DKGF deletes the 3U-KEY Association and sends acknowledgement

to CDAF
q = CDAF advices RUS that charging session is over
r = RUS sends acknowledgment (RUS treats the information as specified by the operator)

The information about any recharging session may be retained by the above noted several components for short term or long term, and may be deleted after some specified time. It may be is application, implementation, or business model specific.

In another embodiment (if the receptacle is in ARN and connector cable is a part of the EV vehicle), the ARN may unlock and automatically release the connector only in the event when 100% charging has been accomplished. This may be an optional provision in the ARN that may be activated or deactivated based on business model. In such a provision the EV manufacturers are proposed to build cable retract feature, i.e. when the ARN releases the connector cable, the EV retracts the cable automatically, and informs the EV driver on the dashboard indicator, or hand held device. This feature would be appreciated by those EV drivers who may prefer to stay inside the car (especially motor-home) during charging, i.e. when the ARN releases the charging cable, the EV retracts the cable automatically, and informs the EV driver. In case of automatic cable retraction provision, the EV manufacturers are proposed to install the cable stow away housing where retracing action does not damage the car body/paint.

The ARN is proposed to include a built-in communication system (comprising microphone, speaker, wired or wires channels, and all the components a modern communication system requires for dealing emergency situations). The built-in communication system would be useful in case of emergencies, such as loss of the 3U-KEY, or any other hazardous conditions wherein it becomes crucial to unplug the EV in the presence or absence of EV driver by law enforcement officer (fire fighter, policeman). Thus the proposed built-in communication system (or independent communication system) will allow the interaction with a System Administrator. The System Administrator would be able to unlock the connector remotely. The System Administrator may use several means (e.g. license number, date of birth, social security number, or any other parameter to verify the communicating person and keep the record).

The user interface utilizes the LCD to interact with the user or to display messages to the user. For example, the LCD may initially display a message, such as “Please insert connector”, “How would you like the get the 3U-KEY

(printed tag, or over mobile device)", "EV is xx percent charged", "Authentication successful", "Access denied, please try again" or "Please contact the System Administrator", or any other routine messages, error messages, informative message and/or system generated/related message. The display may also have diagnostic capabilities. This feature may be used diagnose the EV's battery health and advertise new battery or auto accessories.

To gain competitive edge, additional services may also be provided by the ARN. The additional services may cover wide range varying from completely technical services (e.g. automobile diagnostic, assessment, etc. and reporting to the EV driver and/or the dealer), to non technical services (e.g. entertainment, or any other service that provides most effective utilization of time while the automobile is being charged. The ARN may also be installed with Automated License Plate Readers (ALPR). This might be appreciated by law enforcement agencies to enhance security and safety of the residents.

References

[1] US Department of Energy. Plug-In Electric Vehicle Handbook for Public Charging Station Hosts. http://www.afdc.energy.gov/pdfs/51227.pdf.

[2] U.S. Department of Energy. Vehicle Technologies Program - Advanced Vehicle Testing Activity Plug-in Hybrid Electric Vehicle Charging Infrastructure Review, Final Report Battelle Energy Alliance Contract No. 58517. http://avt.inl.gov/pdf/phev/phevInfrastructureReport08.pdf.

Biographies

Raziq Yaqub earned a Ph.D. in Wireless Communication from Keio University, Japan, and MBA in Marketing from Fairleigh Dickenson University, USA. He is ere one of the pioneers of LTE/4G, and an inventor of numerous technologies of 4th Generation Wireless Communication, as well as Smart Grid. He received "Innovators Award" from the Governor of the State of New Jersey, USA, through New Jersey Inventors Hall of Fame, for making extra ordinary contributions to the advancement of knowledge and technology.

Dr. Yaqub remained an Executive Director of Toshiba America Research, Inc., from 2001 to 2009, Senior Consultant to the State of New Jersey for 700 MHz LTE Public Safety Network, a spokesperson in 3GPP on behalf of Department of Homeland Security for "Govt. Emergency Telecomm Service", Associate Professor of University of Tennessee in Chattanooga, Adjunct Professor in Stevens Institute of Technology, and now he is Director

of Technical Training in NIKSUN, Princeton, USA.

Azzam ul Asar received his Ph.D. and M.Sc. from the University of Strathclyde Glasgow, U.K. He completed his post-doctoral studies from New Jersey Institute of Technology, USA. His research areas include power system, smart grid, microgrid, and intelligent system. He has supervised a number of research projects on energy systems. He is an organizer/session chair of international and national conferences. He has over 100 publications in international journals and conference proceedings. Dr. Asar held several administrative positions during his service including Dean, Chairman, and Director graduate program. Currently, he is full Professor in the Department of Electrical Engineering, CECOS University, Peshawar, Pakistan. He is currently Chair, IEEE Peshawar Subsection, Chair IEEE PES/PEL Joint Society Chapter working under Islamabad Section and an Executive member of IEEE Islamabad Section.

Fahad Butt has done his bachelors degree from University of Engineering and Technology Peshawar in Electrical Power Engineering and his final year project was on control in Smart Grid. Currently he is working in National Engineering Services Pakistan. He is also enrolled in the Masters Programme in CECOS University Peshawar.

Umair Ahmed Qazi did his bachelors from University of Engineering and Technology, UET Peshawar in Electrical Power Engineering and worked in his final year project on power flow control in Smart Grid station. He is presently enrolled in masters program in CECOS University. Currently he is working in a private-sector company named Multinet.