Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

L. Xue
D. Zhang
Huawei
B. Gao
China Telecom
D. Liu
China Mobile

July 4, 2014

RADIUS Extensions for Key Management in WLAN network
draft-xue-radext-key-management-03

Abstract

When a mobile device (referred to as Station (STA)) tries to connect to a Wireless Local Area Network (WLAN), it needs to first perform mutual authentication with the EAP server of the network. As a result of successful authentication, a Pairwise Master Key (PMK) will be generated, and distributed to the STA and the Authenticator of the network by the EAP server respectively. The PMK is used for securing the subsequent communications between the STA and the Wireless Termination Point (WTP) it attaches to. In practice, the authenticator may not be deployed on the WTP. In this case, an approach is required to help the WTP to obtain the PMK. This work tries to discuss the issues related with this topic and proposes a RADIUS extension to address the problem.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 5, 2015.

Table of Contents

1. Introduction

WLAN is now widely used by service operators as a complement of the cellular (2G/3G/LTE) networks, and Extensible Authentication Protocol (EAP)[RFC3748] is regarded as a widely preferred solution for STA authentication in WLAN. When a STA tries to connect to the WLAN, it needs to mutually authenticate with the EAP server of the network first.

According to the security requirements specified in [IEEE-802.11i], a successful EAP authentication procedure must result in a Pairwise Master Key (PMK) for the communication between the STA and the EAP server. In addition, the EAP server also distribute the PMK to the Authenticator.

In practice, the encryption/decryption operations on the STA traffics are carried out either on the WTP or the associated Access Controller

(AC) [RFC5416], and so they need to get the PMK to perform this job. In some deployment scenarios, the Authenticator may be deployed on a Gateway (GW) node rather than on the WTP or the AC. In this case, a solution needs to be provided in order to forward keys to the WTP/AC.

This document discribes the motivation scenario and further proposes a solution which extends RADIUS so as to enable an Authenticator to transfer PMKs to the associated WTPs or ACs.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Terminology

This document uses the same terminologies as found in [RFC5415] and[RFC5247]. Some of the terms defined in the document have been repeated in this section for the reader convenience, along with additional terminologies used by this document.

Access Controller (AC)

The network entity that provides WTP access to the network infrastructure in the data plane, control plane, management plane, or a combination therein.

Authenticator

The entity initiating EAP authentication.

Backend Authentication Server

A backend authentication server is an entity that provides an authentication service to an authenticator. When used, this server typically executes EAP methods for the authenticator. This terminology is also used in [IEEE-802.1X]

EAP Server

The entity that terminates the EAP authentication method with the supplicant. In the case where no backend authentication server is used, the EAP server is part of the authenticator. In the case where the authenticator operates in pass-through mode, the EAP server is located on the backend authentication server. In this work, the latter case is considered.

Gateway (GW)

A device in operator access network, who can charge the subscriber authentication and IP address management.

Station (STA)

A device that contains an interface to a wireless medium. User equipment (UE) with (U)SIM is one type of STA. In authentication procedure, STA is the Supplicant.

Pairwise Master Key (PMK)

PMK is a fresh symmetric key controlling STA’s and the encryption/ decryption node (WTP or AC) access to 802.11 channel during the session.

Pairwise Transient Key (PTK)

PTK is used to encrypt/decrypt unicast traffic for STA which is derived from the 4-way handshake [IEEE-802.11i].

Group Temporal Key (GTK)

GTK is used to encrypt/decrypt multicast/broadcast traffic for STA, which is derived from the 4-way handshake[IEEE-802.11i].

Wireless Termination Point (WTP)

The physical or logical network entity that contains an RF antenna and wireless physical layer (PHY) to transmit and receive station traffic for wireless access networks.

4. EAP in WLAN

In WLAN, EAP [RFC3748] messages are normally transported over RADIUS [RFC2865][RFC2866][RFC3579]. An example of end-to-end EAP authentication procedure in WLAN is illustrated in Figure 1.

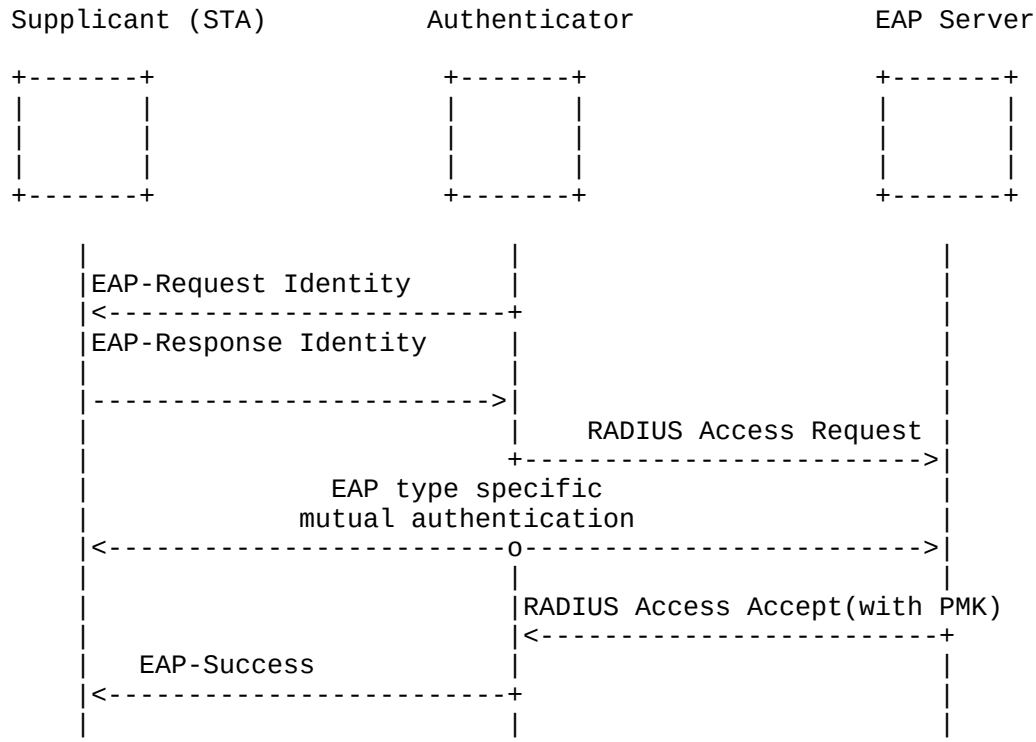

Figure 1. EAP Procedure

In the EAP authentication framework, there are three entities:

- Supplicant: The end of the link that responds to the Authenticator. In this work, a supplicant is actually a STA.
- Authenticator: An entity that facilitates authentication of other entities attached to the same LAN. In a WLAN, an Authenticator could be deployed on WTP, AC or GW according to the operator's requirements.
- EAP Server : An entity provides an authentication service to an authenticator. In this work, it is assumed that an EAP server is deployed on a backend device (e.g., AAA server).

5. Motivation Scenario

The architecture of a typical hotspot WLAN deployment [BBF-WT-321] is shown in Figure 2 .

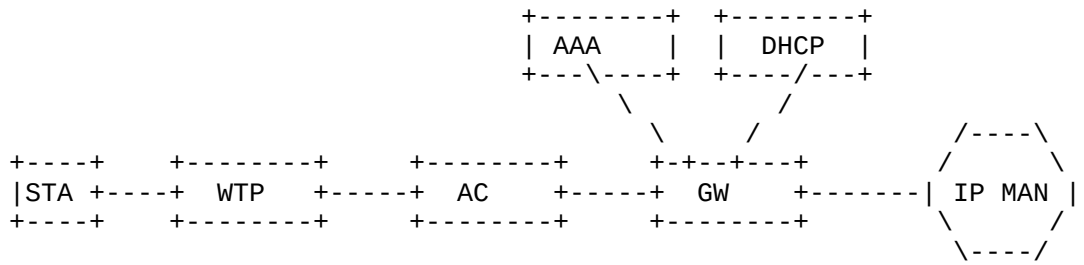

Figure 2 WLAN architecture

As illustrated in this diagram:

- o AC and GW are deployed separately.
- o AC is responsible for AP management as [RFC5415].
- o GW is responsible to provide IP address management and traffic management (e.g., QoS, Charging, Remark, etc) for each STA attached to it. When a STA attempts to access the WLAN, GW will assign an IPv4 address to the STA after the STA has been authenticated. In addition, based on the privileges associated with a STA, GW can decide whether to forward (maybe certain types of) STA traffics not.

Assuming a STA is attached to the WLAN. After a successful EAP session, the GW needs to obtain sufficient information about the STA (including authentication and authorization results) to provide IP address management and traffic management. There are two candidate solutions to achieve this.

The first solution is to deploy the Authenticator on the AC. In this case the GW can act as a RADIUS PROXY during EAP procedure to get the STA information, as shown in figure 3Figure 1. In this solution, both the GW and the AC MUST be involved with the EAP authentication procedure, and the STA related information needs to be redundantly maintained on both the GW and the AC. In addition, this solution will make ACs more complex. Especially, in the scenarios where there are large amount of WTPs, ACs MUST be deployed close to the WTPs because of normally a AC is only able to manage a limited number of WTPs. As a result, there will be a large amount of ACs in the network, which could be costly for operators and could introduce enormous management costs on both EAP servers and ACs. Moreover, the encryption of the communication between EAP server and ACs may damage the effectiveness of this solution.

The second solution is to deploy the Authenticator on the GW. This solution can largely avoid this issues occurred in the first solution. ACs do not have to support EAP procedures, and the number of GWs could be much less than the number of ACs in a WLAN. Especially, some operators prefer to forward the customer data packet to GW rather than AC in order to meet the scalability requirement [I-D.ietf-opsawg-capwap-alt-tunnel] . In this scenario, GW is preferred to be the Authenticator in order to achieve customer traffic management based on the customer authentication and authorization result. However, in the second solution, the GW needs to find a way to forward the PMK to the AC,which is the objective of this work.

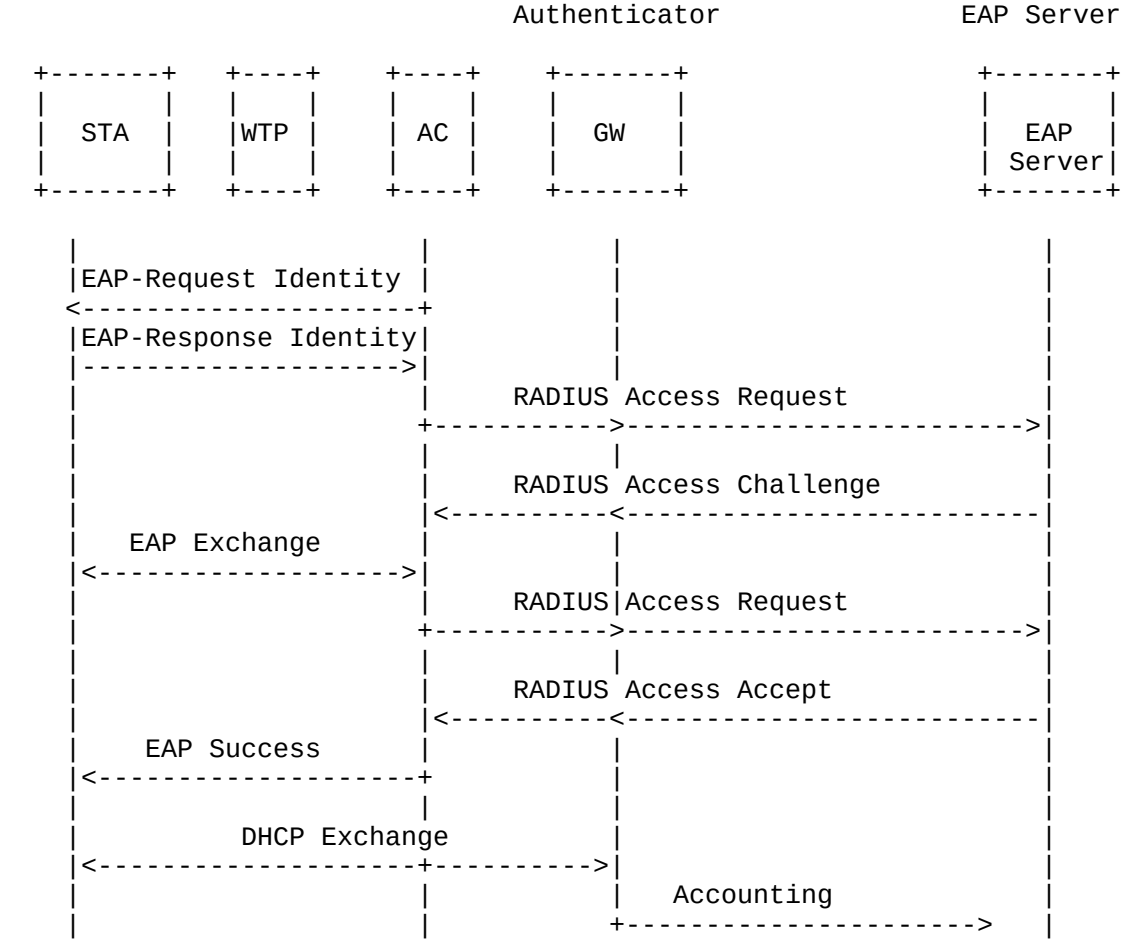

Figure 1: Figure 3 GW acts as RADIUS PROXY

6. Protocol overview

As introduced above, the encryption/decryption operations could be performed on either AC or WTP. If the AC is the encryption/ decryption node, the Authenticator then needs to send the PMK to AC. If the WTP is the encryption/decryption node, the Authenticator can also send the PMK to AC, and AC then forwards the PMK to WTP via protocol defined in [RFC4564]. Therefore, this work specifies three RADIUS commands and a set of attributes for PMK transportation from Authenticator(GW) to AC, i.e., Key-of-Announcement (KoA), KoA-ACK and KoA-NAK.

The PMK transportation is trigged when the Authenticator receives a RADIUS Accept message in EAP session which indicates the authentication success.

6.1. RADIUS Commands for PMK Transportation

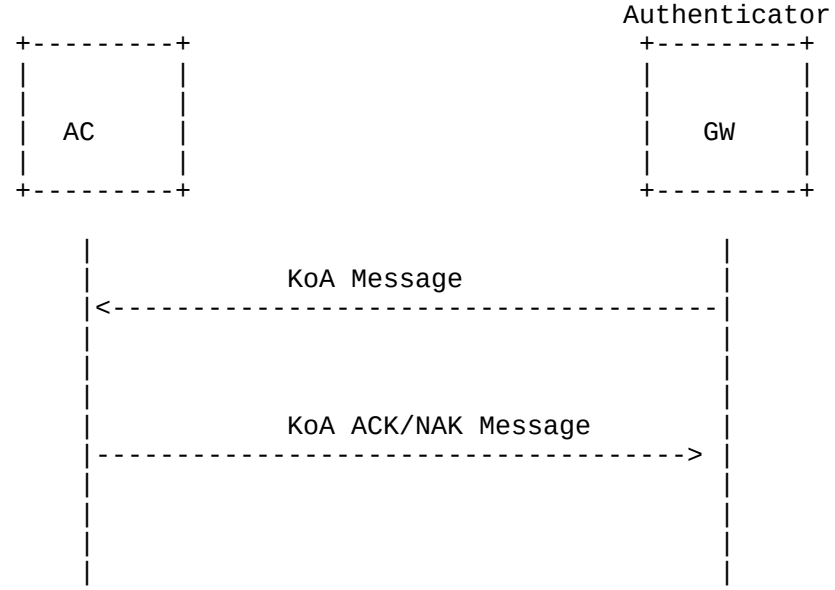

Figure 4 RADIUS Commands for PMK Transportation

As illustrated in the above figure, during the authentication procedure between a STA and a EAP server, the GW acts as an Authenticator. The GW constructs a KoA message and forwards the message to the AC when it obtains the PMK carried in the RADIUS Accept message from EAP server. The AC responds with a KoA-ACK message after successfully accept the PMK. Otherwise, the AC responds with a KoA-NAK.

The commands use the format of Change-of-Authorization Messages (CoA) [RFC5176], presented as follows

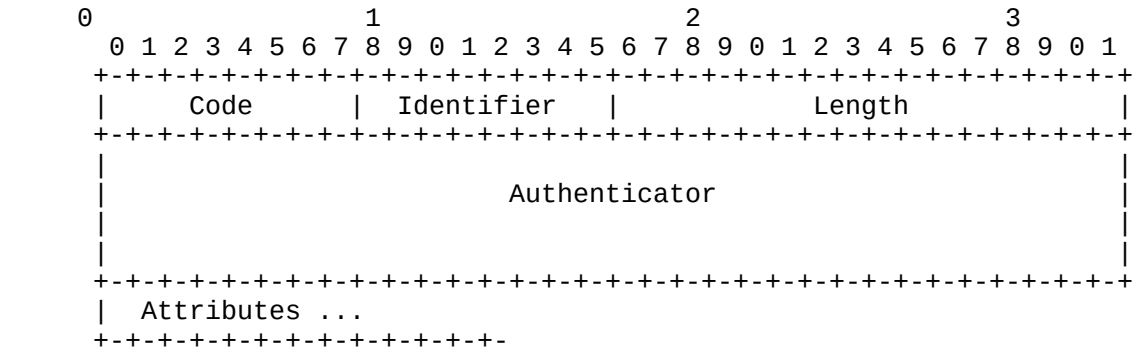

Figure 5 Packet Format

Code

The Code field is one octet, and identifies the type of RADIUS packet. Three new RADIUS codes are defined.

- 100 - Key-of-Announcement
- 101 - KoA-ACK
- 102 - KoA-NAK

Identifier

This field is one octet, and aids in matching requests and replies. This value is set by GW when GW sends the KoA message to the AC. It is used to identifier a pair of KoA and KoA-ACK/NAK message. The Identifier field must be changed by GW whenever a valid reply has been received for a previous request.

Authenticator

The same as defined in [RFC5176].

The following attributes should be included in KoA, KoA-ACK and KoA-NAK messages.

- Calling-Station-Id. This attribution is used to take the STA identifier, for example MAC address. It can be used to bind the PMK to a special STA. This attribute may include within KoA, KoA-ACK and KoA-NAK messages. The values are shown below.

Type

31 as defined in [RFC5176].

Length

8

Value

The Value field is 6 octets, containing the STA MAC address.

o Keying-Material. This attribute is used by GW to transport the PMK to the AC. This attribute may include within KoA, KoA-ACK and KoA-NAK messages. The format and the values are shown below.

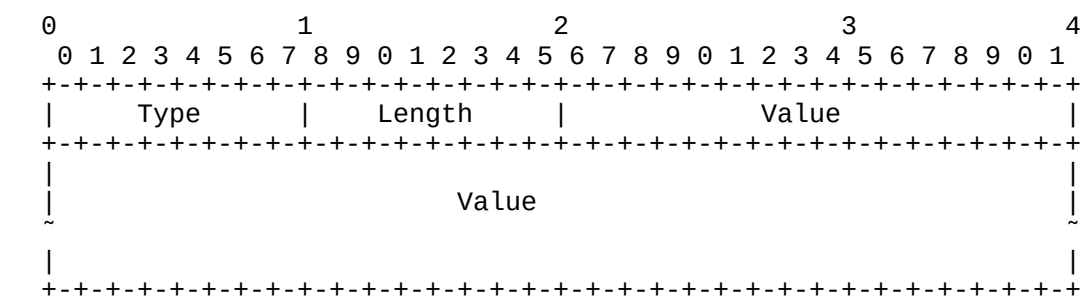

Figure 6 Keying-Material Attribute Format

Type

The type could be an unassigned type right now. In this specification, type 17 is recommended.

Length

34

Value

The Value field is 32 octets, containing the PMK information.

o KoA-Feedback. It is responsible to provide the feedback when AC receives the KoA command from GW. This attribute may include within KoA-ACK/NAK messages. The format is shown below.

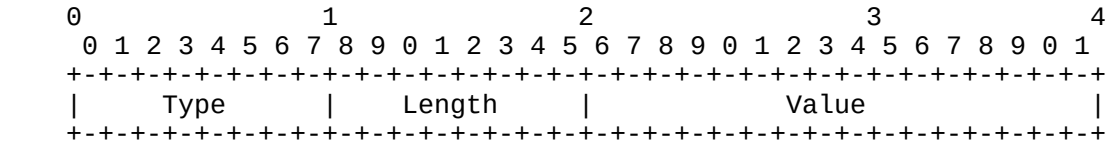

Figure 7 KoA-Feedback Attribute Format

Type

The type could be an unassigned type right now. In this specification, type 21 is recommended. Considering the compatibility, the type 18 can also be used referenced in[RFC2865].

Length

4

Value

The Value field is 2 octets, containing the feedback from the AC when received the KoA message. It could be reasons for PMK transportation fails.

7. IANA Considerations

TBD

8. Security Considerations

TBD

9. References

9.1. Normative References

[BBF-WT-321]
"Public Wi-Fi Access in Multi-service Broadband Networks", January 2014.

[IEEE-802.11i]
"Institute of Electrical and Electronics Engineers, "Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements -Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security" "", September 2004.

[IEEE-802.1X]
"Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control"", September 2001.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4564] Govindan, S., Cheng, H., Yao, ZH., Zhou, WH., and L. Yang, "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4564, July 2006.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

[RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, August 2008.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, March 2009.

9.2. Informative References

[I-D.ietf-opsawg-capwap-alt-tunnel]
Zhang, R., Cao, Z., Deng, H., Pazhyannur, R., Gundavelli, S., and L. Xue, "Alternate Tunnel Encapsulation for Data Frames in CAPWAP", draft-ietf-opsawg-capwap-alt-tunnel-00 (work in progress), May 2014.

Authors' Addresses

Li Xue
Huawei
No.156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan,
Beijing, HaiDian District 100095
China

Email: xueli@huawei.com

Dacheng Zhang
Huawei
Beijing
China

Email: zhangdacheng@huawei.com

Bo Gao
China Telecom
No. 1835, South Pudong Road
Shanghai 200122
China

Email: gaobo@sttri.com.cn

Dapeng Liu
China Mobile
Unit 2, 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
China

Email: liudapeng@chinamobile.com