Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 15, 2011

Z. Cao
H. Deng
China Mobile
Y. Wang
Q. Wu
Huawei Technologies Co., Ltd.
G. Zorn
Network Zen

March 14, 2011

EAP Re-authentication Protocol Extensions for Authenticated Anticipatory Keying (ERP/AAK)

draft-ietf-hokey-erp-aak-04

Abstract

The Extensible Authentication Protocol (EAP) is a generic framework supporting multiple of authentication methods.

The EAP Re-authentication Protocol (ERP) specifies extensions to EAP and the EAP keying hierarchy to support an EAP method-independent protocol for efficient re-authentication between the peer and an EAP re-authentication server through any authenticator.

Authenticated Anticipatory Keying (AAK) is a method by which cryptographic keying material may be established prior to handover upon one or more candidate attachment points (CAPs). AAK uses the AAA infrastructure for key transport.

This document specifies the extensions necessary to enable AAK support in ERP.

Status of This Memo

This Internet-Draft will expire on September 15, 2011.

Table of Contents

1. Introduction

The Extensible Authentication Protocol (EAP) [RFC3748] is a generic framework supporting multiple types of authentication methods. In systems where EAP is used for authentication, it is desirable to not repeat the entire EAP exchange with another authenticator. The EAP Re-authentication Protocol (ERP) [RFC5296] specifies extensions to EAP and the EAP keying hierarchy to support an EAP method-independent protocol for efficient re-authentication between the peer and an EAP re-authentication server through any authenticator. The re-authentication server may be in the home network or in the local network to which the peer is connecting.

Authenticated Anticipatory Keying (AAK) [RFC5836] is a method by which cryptographic keying material may be established prior to handover upon one or more candidate attachment points (CAPs). AAK utilizes the AAA infrastructure for key transport.

This document specifies the extensions necessary to enable AAK support in ERP.

2. Terminology

2.1. Standards 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 RFC 2119 [RFC2119].

2.2. Acronyms

The following acronyms are used in this document; see the references for more details.

AAA Authentication, Authorization and Accounting [RFC3588]

CAP Candidate Attachment Point [RFC5836]

EA Abbreviation for "ERP/AAK"; used in figures

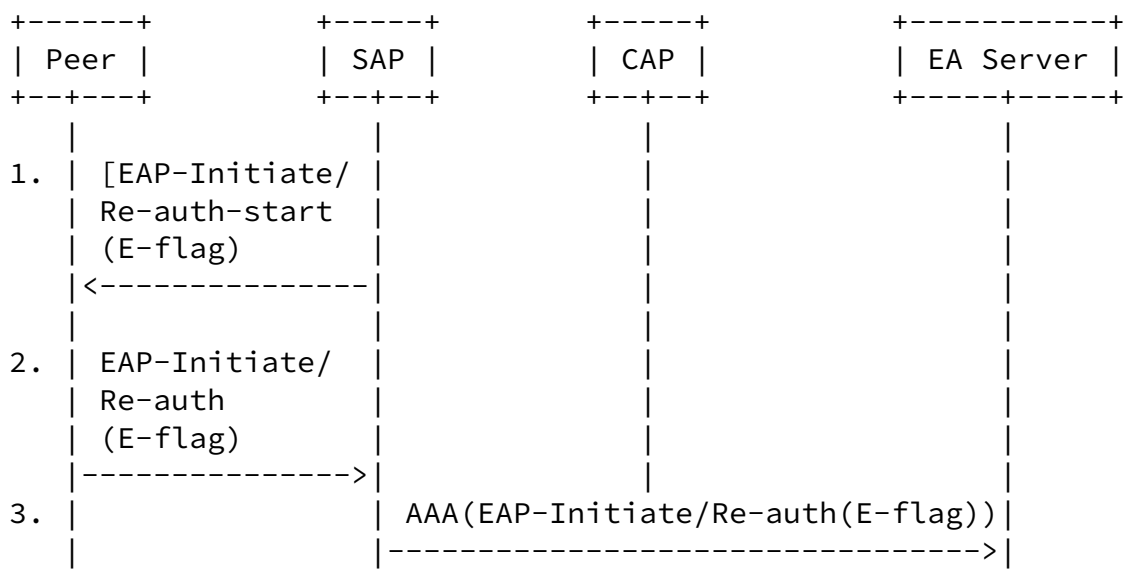
MH Mobile Host

SAP Serving Attachment Point [RFC5836]

3. ERP/AAK Overview

ERP/AAK is intended to allow the establishment of cryptographic keying materials on a single Candidate Attachment Points prior to the arrival of the MH at the Candidate Access Network (CAN). The document also specifies a method by which the SAP may send the identities of neighboring attachment points to the peer in the EAP-Initiate/Re-auth-Start message.

It is assumed that the peer has previously completed full EAP authentication. Figure 1 shows the general protocol exchange by which the keying material is established on the CAP. This document only discusses the case of distributing the key to a single CAP.



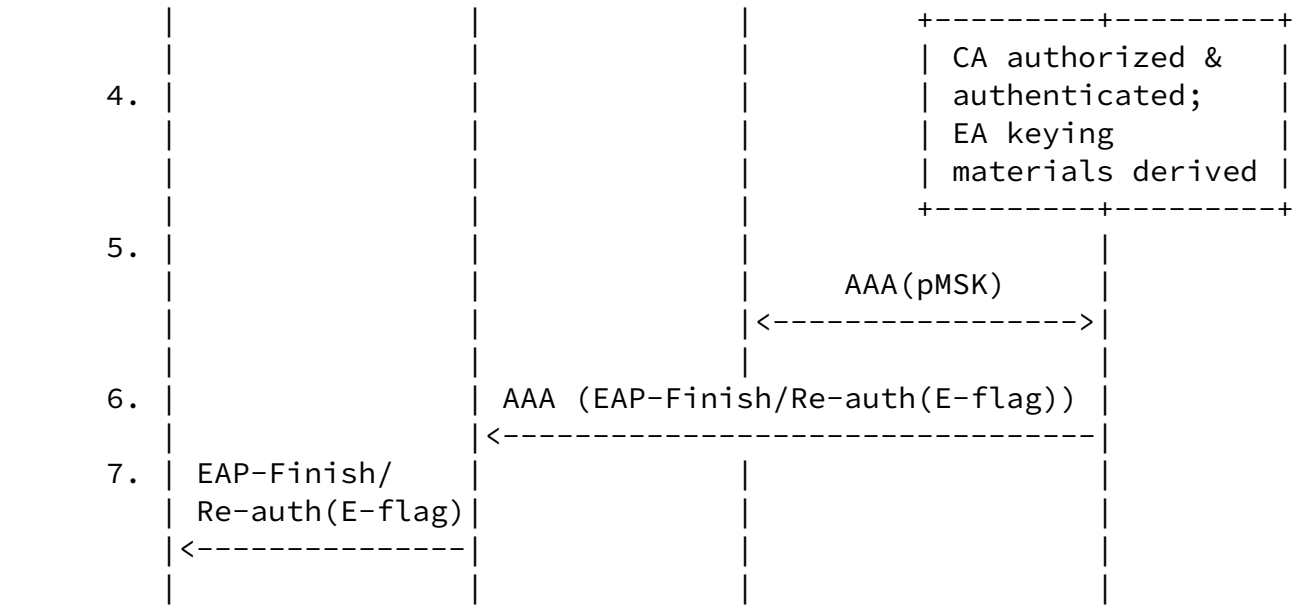


Figure 1: ERP/AAK Operation

ERP/AAK re-uses the packet format defined by ERP, but specifies a new flag to differentiate EAP early-authentication from EAP re-authentication. The peer initiates ERP/AAK itself, or does so in response to an EAP-Initiate/Re-Auth-Start message from the SAP. In this document, it is required that the SAP should support ERP/AAK. If either the peer or the SAP does not support ERP/AAK, it should fall back to full EAP authentication.

The peer sends an early-authentication request message (EAP-Initiate/Re-auth with the 'E' flag set) containing the keyName-NAI, the NAS-Identifier, rIK and sequence number. The realm in the keyName-NAI field is used to locate the peer's ERP/AAK server. The NAS-Identifier is used to identify the CAP. The rIK is used to protect the message. The sequence number is used for replay protection. To avoid the same pre-established Master Session Key (pMSK) being derived for multiple CAPs, the sequence number MUST be unique for each CAP.

The SAP encapsulates the early-authentication message into a AAA message and sends it to the peer's ERP/AAK server in the realm indicated in the keyName-NAI field.

Upon receiving the message, the ERP/AAK server first checks its integrity and freshness, then authenticates and authorizes the CAP presented in the NAS-Identifier TLV(s). After the CAP is authenticated and authorized successfully, the ERP/AAK server derives the pRK and the subsequent pMSK for the CAP.

The ERP/AAK server transports the pMSK to the authenticated and authorized CAP(s) via AAA as described in Section 7.

Finally, the ERP/AAK server sends the early-authentication finish message (EAP-Finish/Re-auth with E-flag set) containing the determinated CAP to the peer via the SAP.

4. ERP/AAK Key Hierarchy

As an optimization of ERP, ERP/AAK uses key hierarchy similar to that of ERP. The EMSK is used to derive the ERP/AAK pre-established Root Key (pRK). Similarly, the ERP/AAK pre-established Integrity Key (pIK) and the pre-established Master Session Key (pMSK) are derived from the pRK. The pMSK is established for the CAP(s) when the peer early authenticates to the network. The pIK is established for the peer to re-authenticate the network after handover. The hierarchy relationship is illustrated in Figure 2, below.

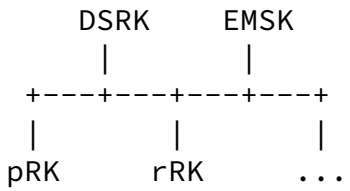


Figure 2

The EMSK and DSRK both can be used to derive the pRK. In general, the pRK is derived from the EMSK in case of the peer moving in the home AAA realm and derived from the DRSK in case of the peer moving in the visited AAA realm. The DSRK is delivered from the EAP server to the ERP/AAK server as specified in [I-D.ietf-dime-local-keytran]. If the peer has previously authenticated by means of ERP or ERP/AAK, the DSRK SHOULD be directly re-used.

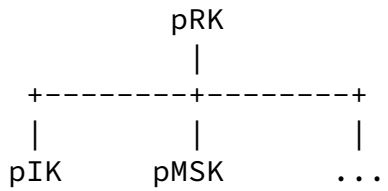


Figure 3

The pRK is used to derive the pIK and pMSK for the CAP(s). Different sequence numbers for each CAP MUST be used to derive the unique pMSK(s).

5. Packet and TLV Extension

This section describes the packet and TLV extensions for the ERP/AAK exchange.

5.1. EAP-Initiate/Re-auth-Start Packet Extension

Figure 4 shows the changed parameters contained in the EAP-Initiate/ Re-auth-Start packet defined in RFC 5296 [RFC5296].

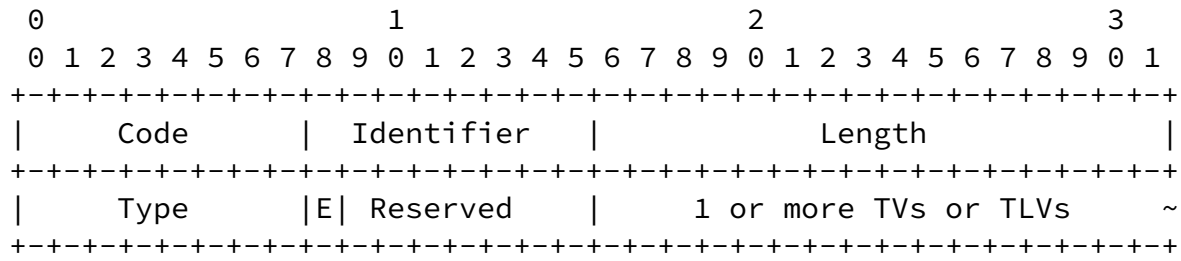


Figure 4

Flags

'E' - The E flag is used to indicate early-authentication.

Reserved: MUST be set to 0.

TVs and TLVs

NAS-Identifier: As defined in [RFC5296], it is carried in a TLV payload. It is used by the SAP to advertise the identifier(s) of CAP(s) to the peer. One or more NAS-Identifier TLVs MAY be included in the EAP-Initiate/Re-auth-Start packet if the SAP has performed CAP discovery.

If the EAP-Initiate/Re-auth-Start packet is not supported by the peer, it is discarded silently.

5.2. EAP-Initiate/Re-auth Packet Extension

Figure 5 illustrates the changed parameters contained in the EAP-Initiate/Re-auth packet defined in RFC 5296 [RFC5296].

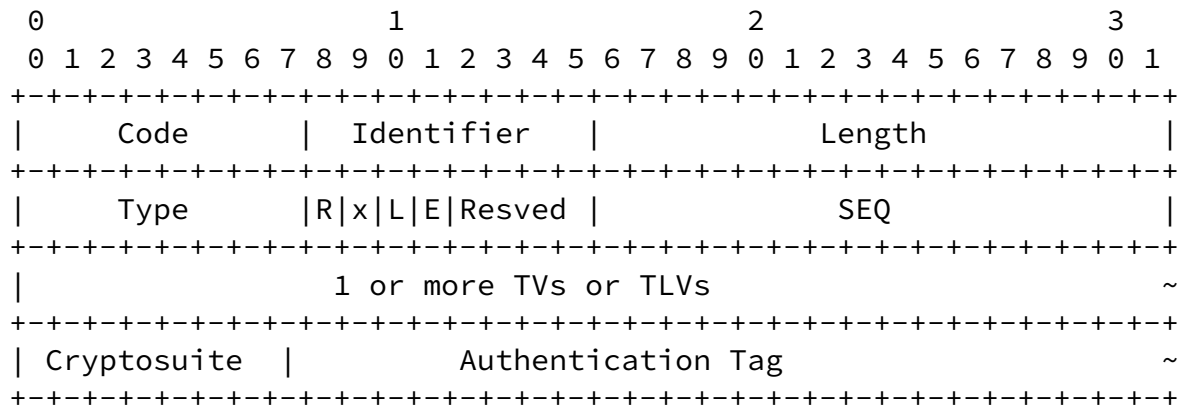


Figure 5

Flags

'x' - The x flag is reserved. It MUST be set to 0.

'E' - The E flag is used to indicate early-authentication.

The rest of the 4 bits (Resved) MUST be set to 0 and ignored on reception.

SEQ

A 16-bit sequence number is used for replay protection.

TVs and TLVs

keyName-NAI: As defined in RFC 5296 [RFC5296], this is carried in a TLV payload. The Type is 1. The NAI is variable in length, not exceeding 253 octets. The username part of the NAI is the EMSKname used identify the peer. The realm part of the NAI is the peer's home domain name or the domain to which the peer is currently attached. Exactly one keyName-NAI attribute SHALL be present in an EAP-Initiate/Re-auth packet.

NAS-Identifier: As defined in RFC 5296 [RFC5296], it is carried in a TLV payload. It is used to indicate the identifier of a CAP. Though this document only introduces the case of a single CAP, two or more NAS-Identifier may be included in the EAP-Initiate/Re-auth packet to identify multiple CAPs.

Sequence number: It is carried in a TV payload. The Type is TBD (which is lower than 128). It is used in the derivation of the pMSK for each CAP to avoid multiple CAP using the same pMSK. Each NAS-Identifier in the packet MUST be associated with a unique sequence number.

Cryptosuite

This field indicates the integrity algorithm used for ERP/AAK. Key lengths and output lengths are either indicated or are obvious from the cryptosuite name. We specify some cryptosuites below:

0 RESERVED

1 HMAC-SHA256-64

2 HMAC-SHA256-128

3 HMAC-SHA256-256

HMAC-SHA256-128 is mandatory to implement and should be enabled in the default configuration.

Authentication Tag

This field contains the integrity checksum over the ERP/AAK packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

If the EAP-Initiate/Re-auth packet is not supported by the SAP, it is discarded silently.

5.3. EAP-Finish/Re-auth extension

Figure 6 shows the changed parameters contained in the EAP-Finish/ Re-auth packet defined in [RFC5296].

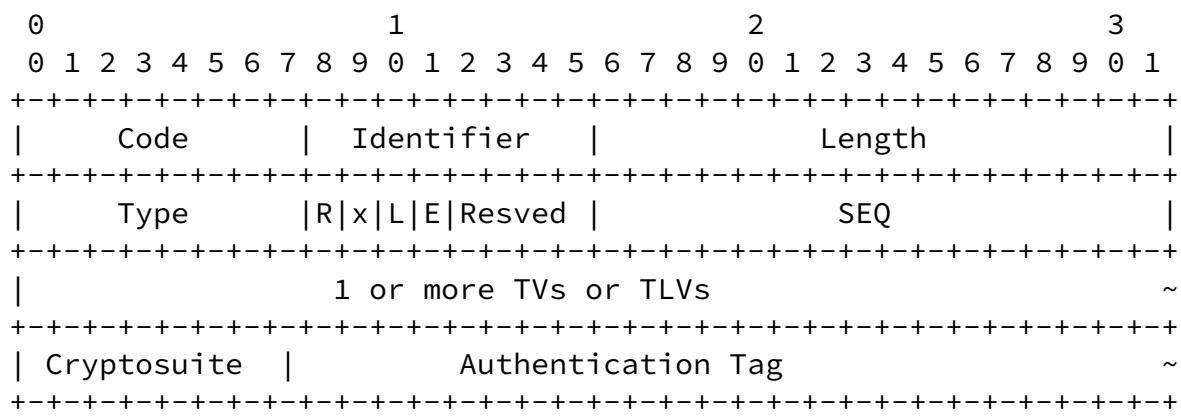


Figure 6

Flags

'x' - The x flag is reserved. It MUST be set to 0.

'E' - The E flag is used to indicate early-authentication.

The rest of the 4 bits (Resved) MUST be set to 0 and ignored on reception.

SEQ

A 16-bit sequence number is used for replay protection.

TVs and TLVs

keyName-NAI: As defined in[RFC5296], this is carried in a TLV payload. The Type is 1. The NAI is variable in length, not exceeding 253 octets. The realm part of the NAI is the home domain name. Exactly one keyName-NAI attribute SHALL be present in an EAP-Finish/Re-auth packet.

ERP/AAK-Key: It is carried in a TLV payload for the key container. The type is TBD. One or more than one ERP/AAK-key may be present in an EAP-Finish/Re-auth packet.

```
ERP/AAK-Key ::=
     { sub-TLV: NAS-Identifier }
```

```
        { sub-TLV: pMSK-lifetime }
        { sub-TLV: pRK-lifetime }
```



```
        { sub-TLV: Cryptosuites }
```

NAS-Identifier: It is carried in a sub-TLV payload. It is used to indicate the identifier of candidate authenticator. There exactly one instance of the NAS-Identifier TLV MUST be present in the ERP/AAK-Key TLV.

pMSK-lifetime: It is carried in a sub-TLV payload. The Type is TBD. The value field is a 32-bit field and contains the lifetime of the pMSK in seconds. If the 'L' flag is set, the pMSK Lifetime attribute SHOULD be present.

pRK-lifetime: It is carried in a sub-TLV payload. The Type is TBD. The value field is a 32-bit field and contains the lifetime of the pRK in seconds. If the 'L' flag is set, the pRK Lifetime attribute SHOULD be present.

List of Cryptosuites: This is a sub-TLV payload. The Type is TBD. The value field contains a list of cryptosuites, each 1 octet in length. The allowed cryptosuite values are as specified in Section 5.2, above. The server SHOULD include this attribute if the cryptosuite used in the EAP-Initiate/Re-auth message was not acceptable and the message is being rejected. The server MAY include this attribute in other cases. The server MAY use this attribute to signal to the peer about its cryptographic algorithm capabilities.

Cryptosuite

This field indicates the integrity algorithm and PRF used for ERP/AAK. Key lengths and output lengths are either indicated or are obvious from the cryptosuite name.

Authentication Tag

This field contains the integrity checksum over the ERP/AAK packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

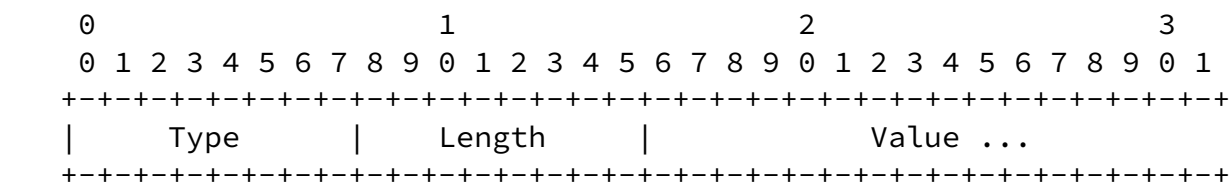
5.4. TV/TLV and sub-TLV Attributes

The TV and TLV attributes are the same specified as section 5.3.4 of [RFC5296]. In this document, some new TLV(s) which may be present in the EAP-Initiate or EAP-Finish messages are defined as below:

Sequence number - This is a TV payload. The type is TBD.

ERP/AAK-Key - This is a TLV payload. The type is TBD.

The format of sub-TLV attributes that may be present in the EAP-Initiate or EAP-Finish messages is:



The following types are defined in this document:

pRK Lifetime: This is a TV payload. The type of this sub-TLV is TBD.

pMSK Lifetime: This is a TV payload. The type of this sub-TLV is TBD.

List of Cryptosuites: This is a TLV payload. The type of this sub-TLV is TBD.

6. Lower Layer Considerations

Similar to ERP, some lower layer specifications may need to be revised to support ERP/AAK; refer to section 6 of [RFC5296] for additional guidance.

7. AAA Transport Considerations

AAA transport of ERP/AAK messages is the same as AAA transport of the ERP message [RFC5296]. In addition, the document requires AAA

transport of the ERP/AAK keying materials delivered by the ERP/AAK server to the CAP. Hence, a new Diameter ERP/AAK application message should be specified to transport the keying materials.

8. Security Considerations

This section provides an analysis of the protocol in accordance with the AAA key management requirements specified in [RFC4962]

- Cryptographic algorithm independence: ERP-AAK satisfies this requirement. The algorithm chosen by the peer is indicated in the EAP-Initiate/Re-auth message. If the chosen algorithm is unacceptable, the EAP server returns an EAP- Finish/Re-auth message with Failure indication

- Strong, fresh session keys: ERP-AAK results in the derivation of strong, fresh keys that are unique for the given CAP. An pMSK is always derived on-demand when the peer requires a key with a new CAP. The derivation ensures that the compromise of one pMSK does not result in the compromise of a different pMSK at any time.

- Limit key scope: The scope of all the keys derived by ERP-AAK is well defined. The pRK is used to derive the pIK and pMSK for the CAP. Different sequence numbers for each CAP MUST be used to derive the unique pMSK.

- Replay detection mechanism: For replay protection of ERP-AAK messages, a sequence number associated with the pMSK is used.

- Authenticate all parties: The EAP Re-auth Protocol provides mutual authentication of the peer and the server. The peer and SAP are authenticated via ERP. The CAP is authenticated and trusted by the SAP.

- Peer and authenticator authorization: The sequence number is maintained by the peer and the server, and incremented by them synchronously.

- Keying material confidentiality: The peer and the server derive the keys independently using parameters known to each entity.

- Uniquely named keys: All keys produced within the ERP context can be referred to uniquely as specified in this document.

- Prevent the domino effect: Different sequence numbers for each CAP MUST be used to derive the unique pMSK. So the compromise of one pMSK does not hurt any other CAP.

- Bind key to its context: the pMSK are binded to the context where the sequence numbers are transmitted.

- Confidentiality of identity: this is the same with ERP protocol as analyzed in [RFC5296].

- Authorization restriction: All the keys derived are limited in lifetime by that of the parent key or by server policy. Any domain-specific keys are further restricted for use only in the domain for which the keys are derived. Any other restrictions of session keys may be imposed by the specific lower layer and are out of scope for this specification.

9. IANA Considerations

New TLV types:

Sequence number

ERP/AAK-Key

New sub-TLV types:

pRK Lifetime

pMSK Lifetime

10. Acknowledgement

In writing this document, we have received reviews from many experts in IETF, including Tom Taylor, Tena Zou, Tim Polk. We apologize if

we miss some names that have helped us.

11. References

11.1. Normative References

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

[RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", RFC 5296, August 2008.

11.2. Informative References

[I-D.ietf-dime-local-keytran] Zorn, G., Wu, W., and V. Cakulev, "Diameter Attribute-Value Pairs for Cryptographic Key Transport", draft-ietf-dime-local-keytran-08 (work in progress), October 2010.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

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

[RFC4962] Housley, R. and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management", BCP 132, RFC 4962, July 2007.

[RFC5836] Ohba, Y., Wu, Q., and G. Zorn, "Extensible Authentication Protocol (EAP) Early Authentication Problem

Statement", RFC 5836, April 2010.

Authors' Addresses

Zhen Cao
China Mobile
53A Xibianmennei Ave., Xuanwu District
Beijing, Beijing 100053
P.R. China

EMail: zehn.cao@gmail.com

Hui Deng
China Mobile
53A Xibianmennei Ave., Xuanwu District
Beijing, Beijing 100053
P.R. China

EMail: denghui02@gmail.com

Yungui Wang
Huawei Technologies Co., Ltd.
Floor 10, HuiHong Mansion, No.91 BaiXia Rd.
Nanjing, Jiangsu 210001
P.R. China

Phone: +86 25 84565893
EMail: w52006@huawei.com

Qin Wu
Huawei Technologies Co., Ltd.
Floor 12, HuiHong Mansion, No.91 BaiXia Rd.
Nanjing, Jiangsu 210001

P.R. China

Phone: +86 25 84565892
EMail: sunseawq@huawei.com

Glen Zorn
Network Zen
227/358 Thanon Sanphawut
Bang Na, Bangkok 10260
Thailand

Phone: +66 (0) 87-040-4617
EMail: gwz@net-zen.net