

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2011

H. Wang, Ed.
Y. Shi, Ed.
Hangzhou H3C Tech. Co., Ltd.
T. Tsou
Huawei Technologies
October 18, 2010

EAP Extensions for EAP Early Authentication Protocol (EEP)
draft-hao-hokey-eep-00

Abstract

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

Based on the EAP Early Authentication Model defined by RFC5836, this document specifies the extensions of EAP to support both intra-AAA-realm and inter-AAA-realm handover.

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 April 21, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Terminology	3
2.1. Standards Language	3
2.2. Acronyms	3
3. Message Flow of EAP Early Authentication	4
3.1. Intra-AAA-Realm Handover	4
3.2. Inter-AAA-Realm Handovers	5
4. Problem Statement	6
5. Solution	8
6. Assumptions	8
7. Protocol Message Flow	9
7.1. Intra-AAA-Realm Handovers	9
7.2. Inter-AAA-Realm Handovers(Full trust relationship)	10
7.3. Inter-AAA-Realm Handovers(Semi trust relationship)	12
7.4. Release authentication session	14
8. EEP Key Hierarchy	16
8.1. Key Derivation	17
8.1.1. pRK Derivation	17
8.1.2. pIK Derivation	17
8.1.3. pMSK Derivation	17
9. Packet and TLV Extension	17
9.1. EAP Initiate/Re-auth-Start Packet Extension	18
9.2. EAP Initiate/Pre-Early-auth	19
9.3. EAP Finish/Pre-Early-auth	21
9.4. EAP Initiate/Post-Early-auth	24
9.5. EAP Finish/Post-Early-auth	25
9.6. EAP Initiate/Early-auth Action	27
9.7. EAP Finish/Early-auth Action	30
10. Lower Layer Considerations	33
11. AAA Transport Considerations	33
12. Security Considerations	33
13. IANA Considerations	33
14. Acknowledgements	34
15. References	34
15.1. Normative References	34
15.2. Informative References	34

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, the handover process often requires authentication and authorization for acquisition or modification of resources assigned to the mobile device. In most cases, these authentications and authorizations require interaction with a central authority in a realm. In some cases, the central authority may be distant from the mobile device. The delay introduced due to such an authentication and authorization procedure adds to the handover latency and consequently affects ongoing application sessions.

In the problem statement [RFC5836], it suggests that optimized solutions for secure inter-authenticator handovers can be seen either as security context transfer (e.g., using the EAP Extensions for EAP Re-authentication Protocol (ERP)) [RFC5296], or as EAP Early Authentication.

This document specifies EAP Extensions for Early Authentication Model. The protocol that uses these extensions itself is referred to as the EAP Early Authentication Protocol (EEP). A peer does EAP method-independent Early Authentication before it attaches to a CAP. The protocol and the key hierarchy required for EAP Early Authentication are described in this document.

Note that to support EEP, lower-layer specifications may need to be revised to allow carrying EAP messages that have a code value more than 4 and to accommodate the peer-initiated nature of EEP. Specifically, the IEEE802.1x specification must be revised and RFC 4306 must be updated to carry EEP messages.

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]

MH Mobile Host

SAP Serving Attachment Point [RFC5836]

3. Message Flow of EAP Early Authentication

Based on the functional elements of EAP Early Authentication [RFC5836], the following sections introduce the general message flow of Inter-AAA-Realm and Intra-AAA-Realm handovers. The figures below are to give an overview of EAP Early Authentication.

It is assumed that the MH has previously completed full EAP authentication with Home AAA.

3.1. Intra-AAA-Realm Handover

In intra-AAA-realm handover scenario, SAP and CAP belong to a same AAA realm.

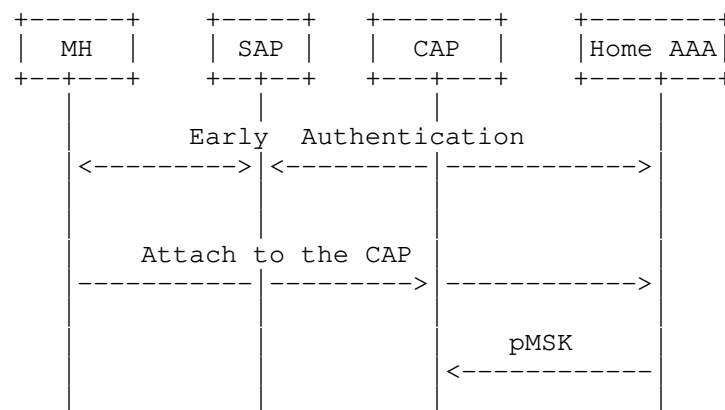


Figure 1: Intra-AAA-Realm Handover

Before MH (peer) performs handover from SAP to CAP, it does early authentication with Home AAA.

Since SAP and CAP belong to the same Home AAA, the complete EAP method exchange is not required in early authentication. The MH informs Home AAA of the NAS-id of CAPs and each CAP's sequence number. Home AAA will derive the pMSK from EMSK and sequence number.

Sequence number must be unique for each CAP to derive a unique pMSK.

After handover, MH attaches to the CAP. MH request to change from early authenticated state to fully authorized and authenticated state. Its Home AAA is not changed. And then Home AAA distribute the pMSK to CAP.

3.2. Inter-AAA-Realm Handovers

In inter-AAA-realm scenario, as the first step, Home AAA and CAP-AAA need to establish a trust relationship.

There are two cases for this step.

In first case, Home AAA and CAP-AAA belong to a same operator. In this case, a full trust relationship may be established. That means security context transfer between AAA servers is permitted.

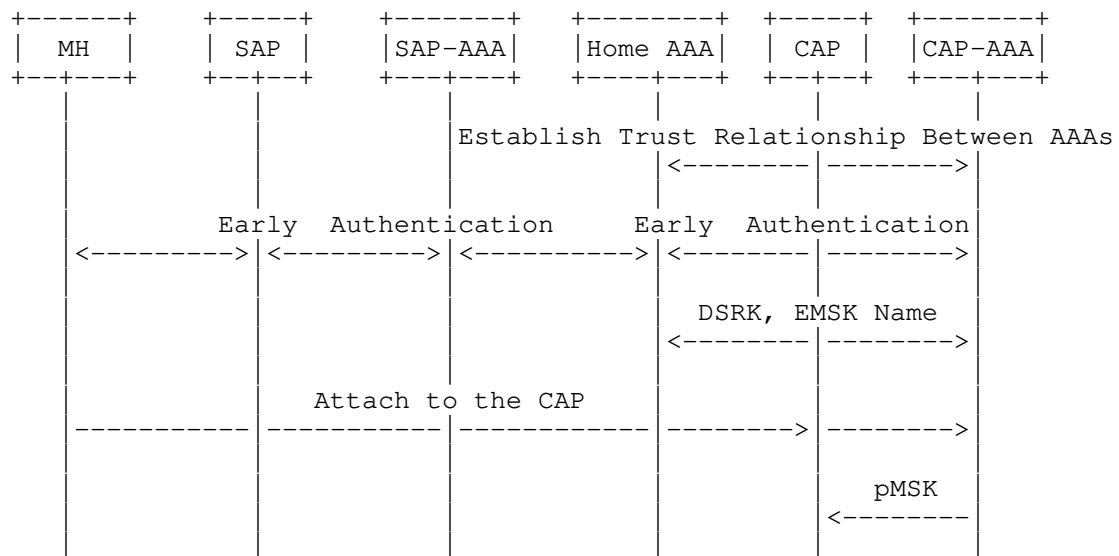


Figure 2: Inter-AAA-Realm Handovers(Full trust relationship)

Before MH (peer) performs handover from SAP to CAP, it does early authentication with CAP-AAA, and messages will be forwarded by SAP, SAP-AAA and Home AAA to CAP-AAA.

Since Home AAA and CAP-AAA belong to the same operator, the complete EAP method exchange is not required in early authentication. The

CAP-AAA will get DSRK and EMSK Name from Home AAA and derive pMSK from DSRK directly.

After handover, MH attaches to the CAP. Its Home AAA is not changed and CAP-AAA becomes the new local AAA server(SAP-AAA).

In second case, Home AAA and CAP-AAA belong to different operators. In this case, a semi trust relationship may be established. That means two AAA servers can recognize each other based on domain name and communicate each other. But the security context transfer is not permitted.

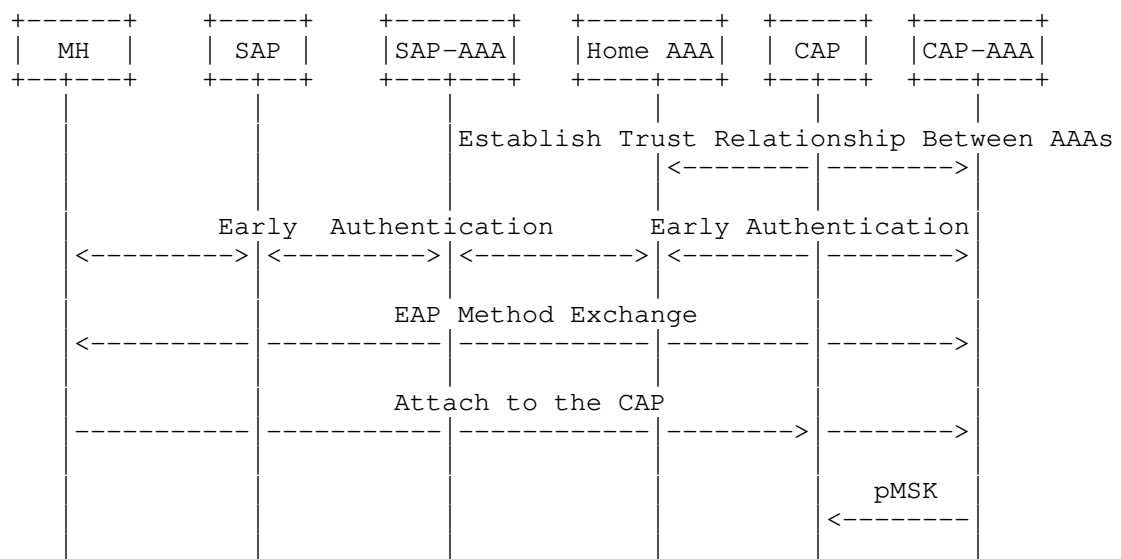


Figure 3: Inter-AAA-Realm Handovers (Semi trust relationship)

Since Home AAA and CAP-AAA belong to the different operators, usually, a complete EAP method exchange will be done in early authentication. MSK and EMSK will be derived in full EAP authentication. CAP-AAA will use the MSK as the pMSK.

After handover, MH attaches to the CAP, its Home AAA is changed and CAP-AAA acts as a new Home AAA.

4. Problem Statement

According to the general message flow of Intra-AAA-Realm and Inter-AAA-Realm handovers, the following problems need to be resolved for Early Authentication Model.

- 1) How to establish a trust relationship between Home AAA and CAP-AAA?

It is an important issue but the solution is out of the scope of this document.

- 2) How does MH knows whether a complete EAP method exchange is required?

A method is required for MH to negotiate this issue with CAP-AAA when it request to start the early authentication.

- 3) How does MH get CAP's status and capability information in advance?

CAPs are discovered through EAP Lower layer. But early authentication is done through EAP layer. MH needs to know whether the discovered CAPs can be early authenticated through Home AAA or not. If MH can't get such knowledge before the early authentication, it is evident that the handover experience will be inefficient.

- 4) How to forward the EEP message between MH and CAP-AAA?

Unlike normal EAP authentication, The SAP-AAA and Home AAA should forward EAP early authentication packets to CAP-AAA instead of processing them locally. So the SAP-AAA and Home AAA should know the domain name of CAP-AAA and when the early authentication is started.

- 5) How to handle the frequent MH handover?

AAA server needs to maintain early authentication sessions, while frequent MH handover may lead to redundant obsolete early authentication sessions on AAA servers. A mechanism is required to settle this situation.

- 6) How to ensure the information consistent between MH and CAP-AAA?

It is a high possibility of information inconsistency between MH and CAP-AAA. For example, after handover, MH starts to use pMSK for EAP lower layer key derivation. But the early authentication session on CAP-AAA has just been expired without notifying MH.

5. Solution

Similiar to ERP protocol, a trigger message is required by SAP to inform MH of its capability to support early authentication. To avoid redundant trigger message, EAP Initiate/Re-auth-Start [RFC5296] is reused and one E flag is added to indicate whether EEP is supported.

EAP Codes 5 (EAP Initiate) and 6 (EAP Finish) defined in the protocol of ERP [RFC5296] is reused.

New EAP Initiate/Pre-early-auth and EAP Finish/Pre-early-auth messages are defined to start the early authentication and negotiate whether full EAP authentication is required.

New EAP Initiate/Post-early-auth and EAP Finish/Post-early-auth messages are defined to confirm the early authentication information and change the state from early authenticated to fully authorized and authenticated.

Early auth action message is defined for below functionality.

- Probe whether the early authentication is supported for sepecified CAP.
- Release the early authentication session to avoid redudant resource assumption.
- Request to change from fully authenticated state to early authenticated state.

6. Assumptions

For the solution, it is assumed that:

- The trust relationship has been established between Home AAA server and CAP-AAA server.
- EEP server has co-located with the AAA server.
- The authenticator act as a pass-through entity for early authentication protocol in a manner similar to that of an EAP authenticator described in RFC3748.
- The entity which support EEP can also support ERP [RFC5296]. So MH can use ERP message to obtain the local domain name.
- MH has fully authenticated with Home AAA before handover.

7. Protocol Message Flow

Based on the Section 3 and Section 5, the below figures show the protocol message flow of EEP protocol.

7.1. Intra-AAA-Realm Handovers

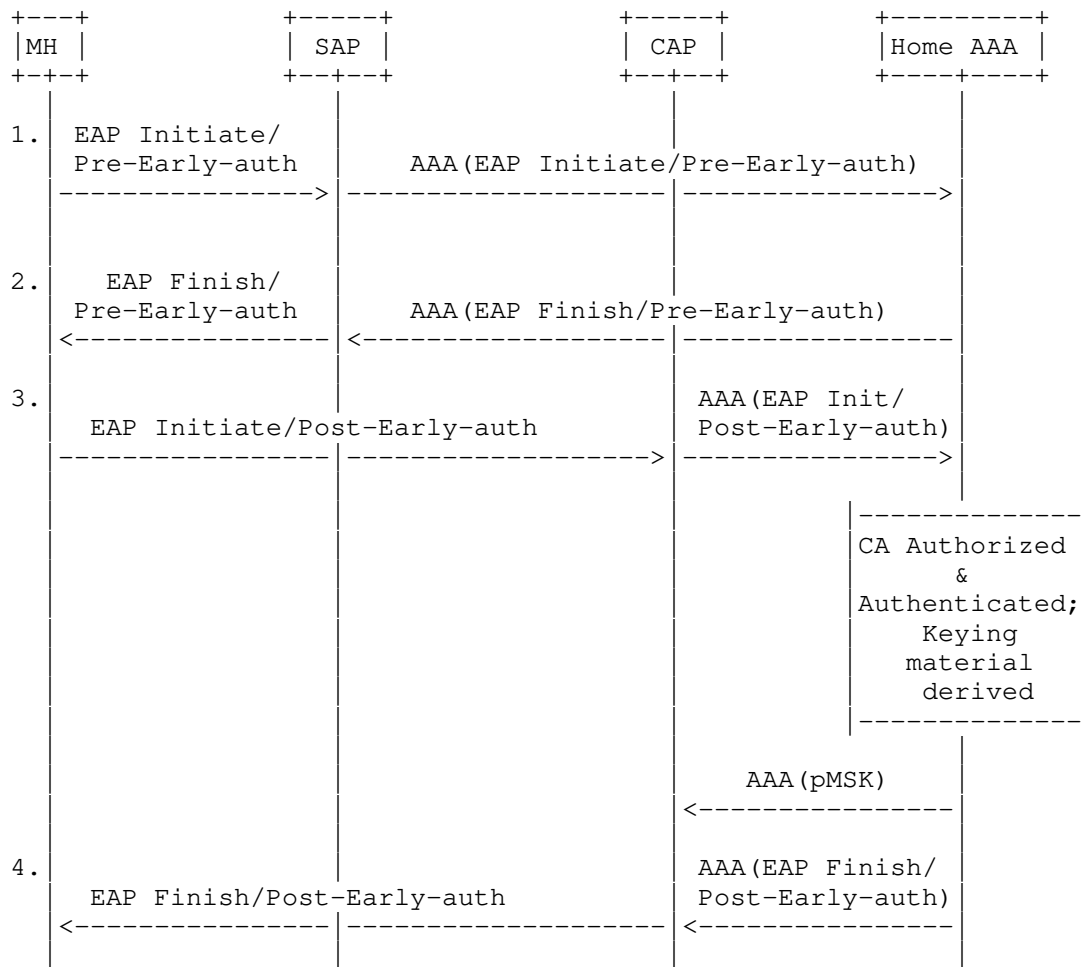


Figure 4: Intra-AAA-Realm Handovers

1) MH request to start the early authentication

MH starts the early authentication using EAP Initiate/Pre-Early-auth message. In Pre-Early-auth message, the NAS-id of CAP and sequence number is included. EAP Initiate/Pre-Early-auth is protected by pIK for middle man attack.

2) Home AAA respond with early authentication result

When Home AAA receive the request from MH, it verify the availability of CAP's NAS-id. And check whether EEP is supported by this CAP. Home AAA respond with early authentication result using EAP Finish/Pre-Early-auth message. pMSK will be derived from EMSK and sequence number and will be kept in early authentication session.

3) MH request to change its state

After handover, MH request to change its state from early authenticated state to fully authorized and authenticated state. In EAP Initiate/Post-Early-auth message, the NAS-id of CAP and EMSK name is included.

4) Home AAA confirm the state change

Home AAA confirm the NAS-id and key name, and then respond with state changing result using EAP Finish/Post-Early-auth message. Home AAA distribute the pMSK to the CAP.

7.2. Inter-AAA-Realm Handovers(Full trust relationship)

It is assumed that SAP-AAA act as the Home AAA server.

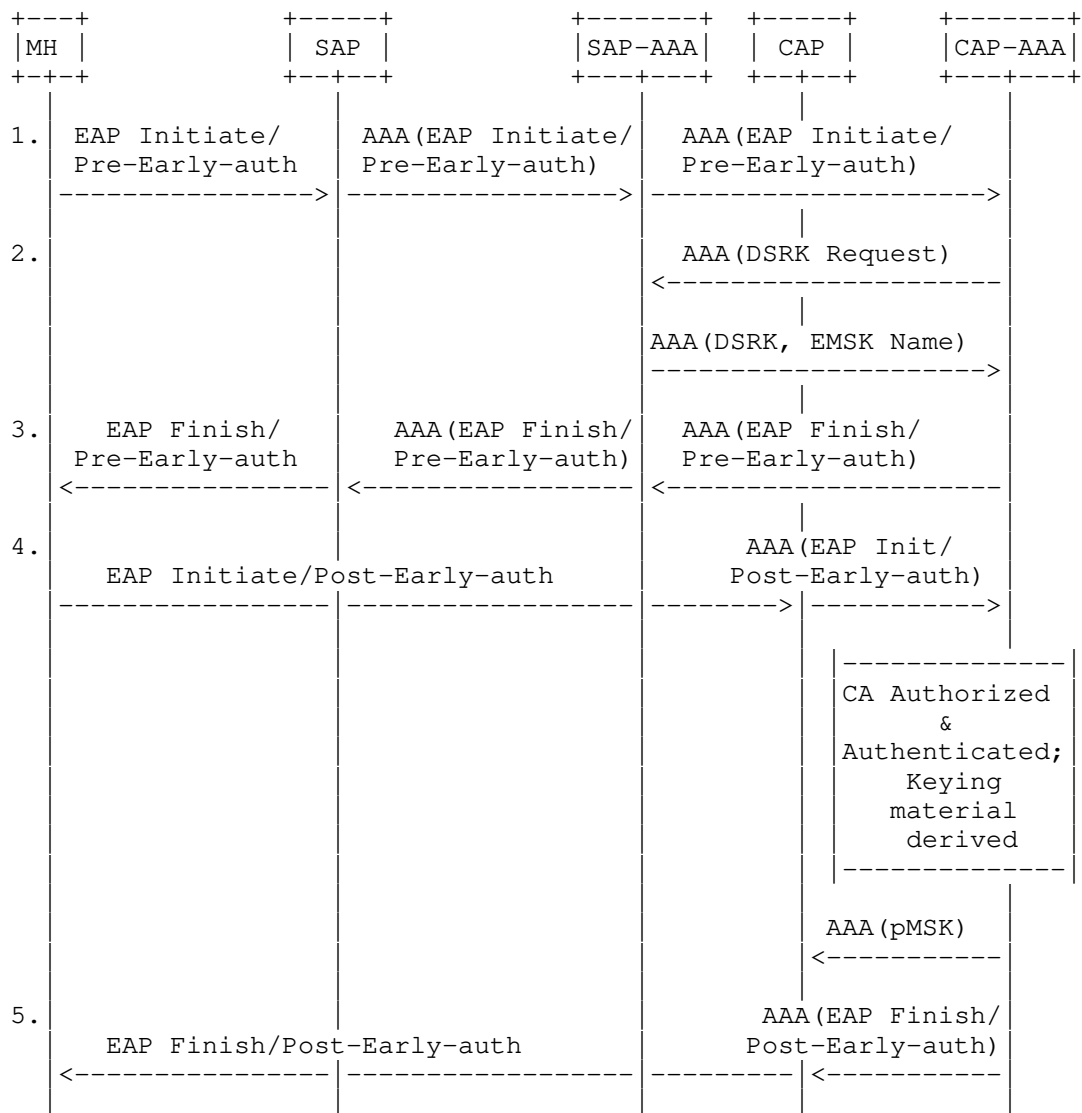


Figure 5: Intra-AAA-Realm Handovers(Full trust relationship)

1) MH request to start the early authentication

MH starts the early authentication using EAP Initiate/Pre-Early-auth message. In Pre-Early-auth message, the NAS-id-NAI of CAP and sequence number is included. Based on the realm part of NAS-id-NAI, the SAP-AAA will forward the Pre-Early-auth message

to the corresponding CAP-AAA. if the CAP-AAA can not be found or trust relationship has not been established, SAP-AAA will directly reject the early authentication request.

2) CAP-AAA request DSRK and EMSK Name from SAP-AAA

After receiving the early authentication request, CAP-AAA find that the full trust relationship has been established between SAP-AAA and CAP-AAA. So CAP-AAA request DSRK and EMSK name from SAP-AAA(Home AAA).

3) CAP-AAA respond with early authentication result

Home AAA respond with early authentication result using EAP Finish/Pre-Early-auth message. pMSK will be derived from DSRK and sequence number and will be kept in early authentication entry.

4) MH request to change its state

After handover, MH request to change its state from early authenticated state to fully authorized and authenticated state.

5) Home AAA confirm the state change

Home AAA respond with state changing result using EAP Finish/Post-Early-auth message. Home AAA distribute the pMSK to the CAP.

7.3. Inter-AAA-Realm Handovers(Semi trust relationship)

It is assumed that SAP-AAA act as the Home AAA server.

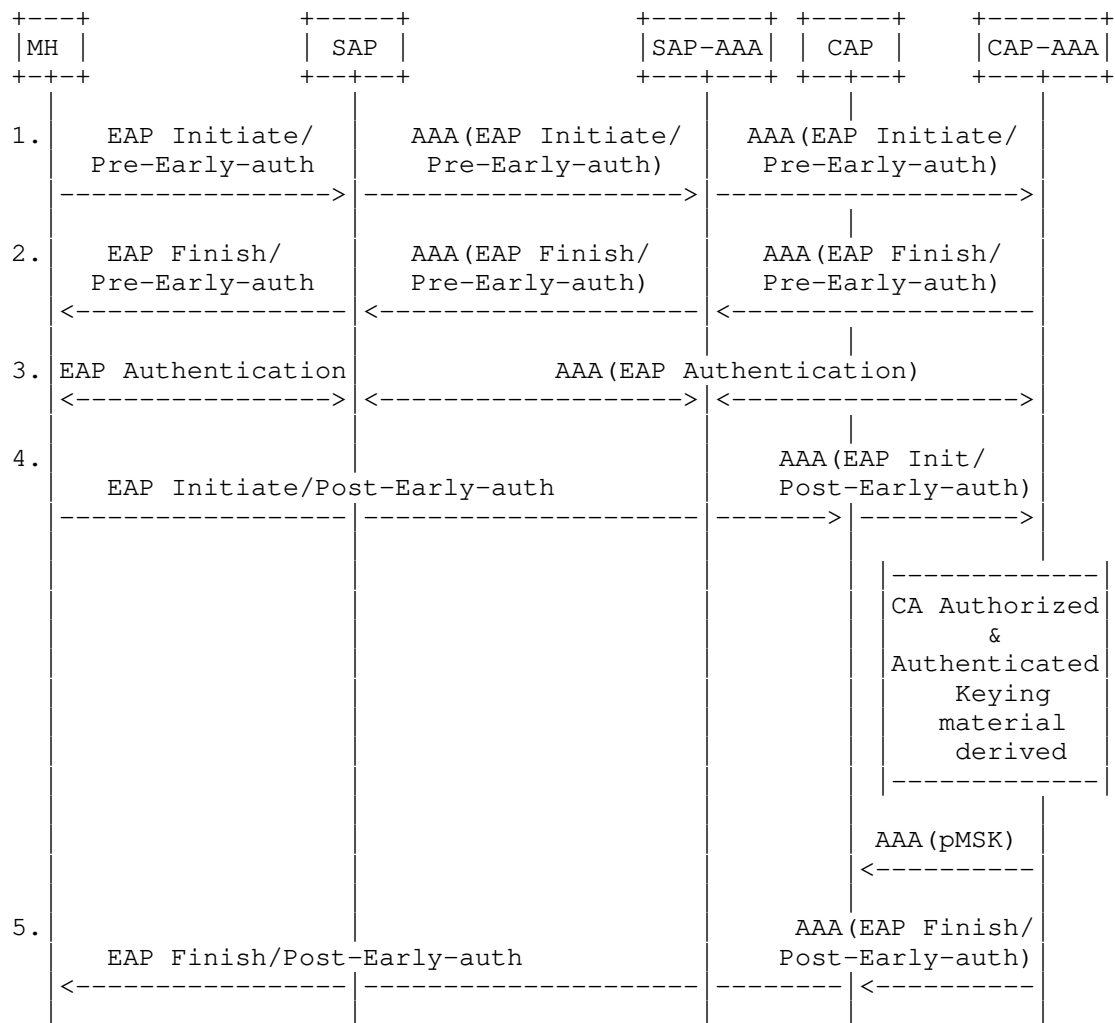


Figure 6: Inter-AAA-Realm Handovers (Semi trust relationship)

1) MH request to start the early authentication

MH starts the early authentication using EAP Initiate/Pre-Early-auth message. In Pre-Early-auth message, the NAS-id-NAI of CAP and sequence number is included. Based on the realm part of NAS-id-NAI, the SAP-AAA will forward the Pre-Early-auth message to the corresponding CAP-AAA. if the CAP-AAA can not be found or trust relationship has not been established, SAP-AAA will directly reject the early authentication request.

2) CAP-AAA respond with early authentication result

After receiving the early authentication request, CAP-AAA find that the semi trust relationship has been established between SAP-AAA and CAP-AAA. Home AAA respond with early authentication result using EAP Finish/Pre-Early-auth message. And in the message, Home AAA inform MH that full EAP authentication is required.

3) MH do full EAP authentication with CAP-AAA

MH do eap authentication with CAP-AAA with full authentication method exchange. SAP-AAA will forward the EAP authentication message to CAP-AAA and reponse message to MH.

4) MH request to change its state

After handover, MH request to change its state from early authenticated state to fully authorized and authenticated state.

5) Home AAA confirm the state change

Home AAA respond with state changing result using EAP Finish/Post-Early-auth message. Home AAA distribute the pMSK to the CAP.

7.4. Release authentication session

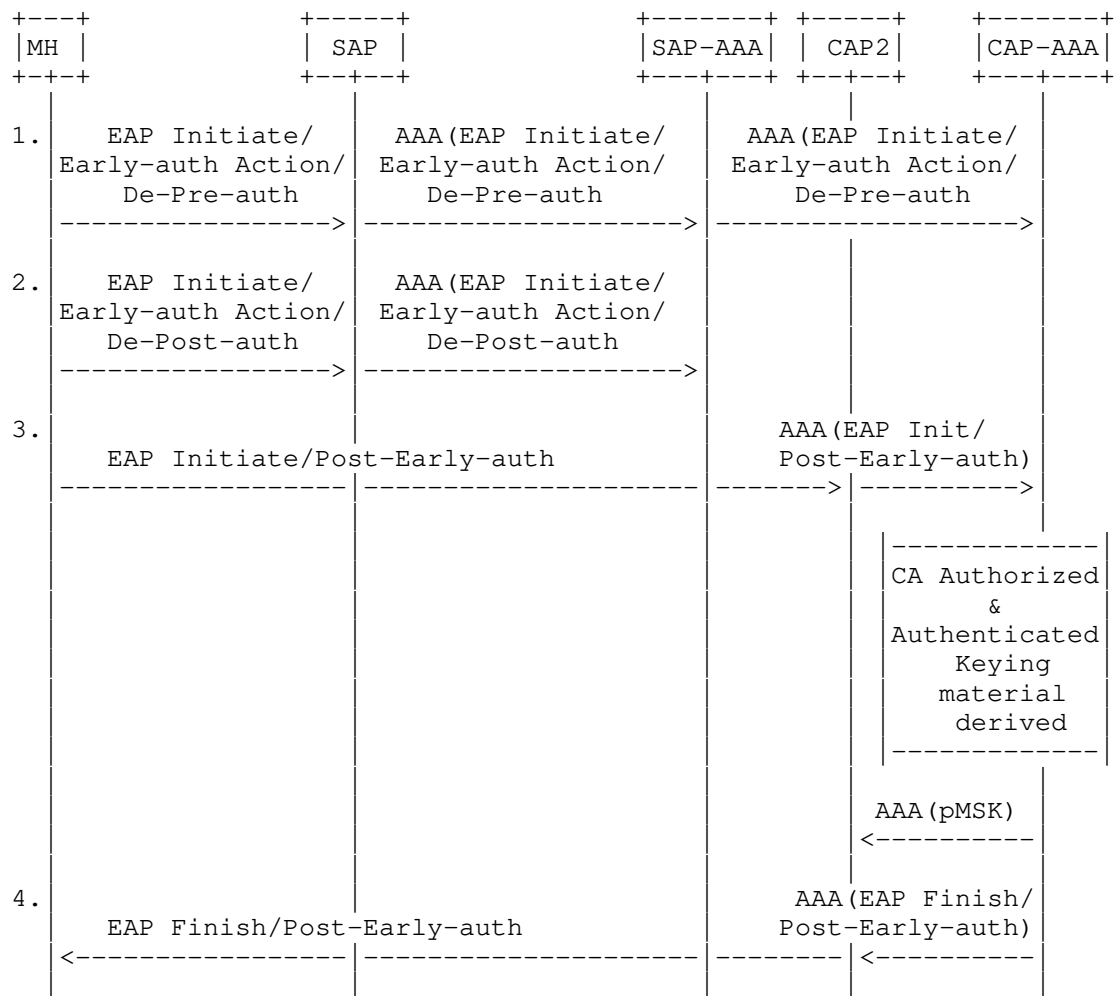


Figure 7

- 1) MH release the early authentication session with CAP1

MH sends EAP Initiate/Early-auth Action/De-Pre-auth to inform CAP-AAA release early authentication session for CAP1.

- 2) MH release the full authentication session with SAP

MH sends EAP Initiate/Early-auth Action/De-Post-auth to inform SAP-AAA to change its state from full authorized and authenticated state to early authenticated state.

3) MH request to change its state

After handover, MH request to change its state from early authenticated state to fully authorized and authenticated state.

4) Home AAA confirm the state change

Home AAA respond with state changing result using EAP Finish/Post-Early-auth message. Home AAA distribute the pMSK to the CAP2.

8. EEP Key Hierarchy

EEP uses key hierarchy similar to that of ERP [RFC5296]. The EMSK is used to derive the EEP pre-established Root Key (pRK). Similarly, the EEP pre-established Integrity Key (pIK) and the pre-established Master Session Key (pMSK) is 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 do post early authentication after handover. The hierarchy relationship is illustrated in Figure 8, below.

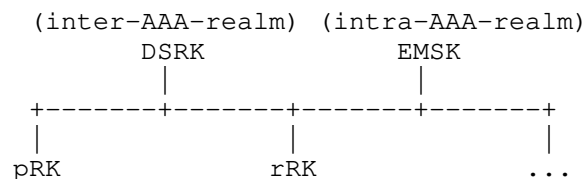


Figure 8

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 DSRK in case of the peer moving in the visited AAA realm. The DSRK is delivered from the EAP server to the EEP server as specified in [I-D.ietf-dime-local-keytran]. if the peer has previously authenticated by means of EEP, the DSRK SHOULD be directly re-used.

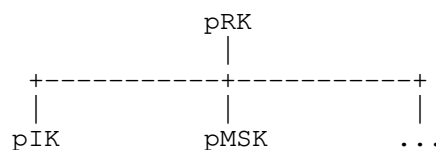


Figure 9

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).

8.1. Key Derivation

As specified in [I-D.ietf-hokey-erp-aak], the key derivation method is given below.

8.1.1. pRK Derivation

$pRK = KDF(K, S)$, where $K = EMSK$ or $DSRK$ and $S = pRK \text{ Label} \parallel "\backslash 0" \parallel \text{length}$

The pRK Label is an IANA-assigned 8-bit ASCII string:

Early authentication Root Key@ietf.org

8.1.2. pIK Derivation

$pIK = KDF(K, S)$, where $K = pRK$ and $S = pIK \text{ Label} \parallel "\backslash 0" \parallel \text{cryptosuite} \parallel \text{length}$

The pIK Label is the 8-bit ASCII string:

Early authentication Integrity Key@ietf.org

8.1.3. pMSK Derivation

$pMSK = KDF(K, S)$, where $K = pRK$ and $S = pMSK \text{ label} \parallel "\backslash 0" \parallel SEQ \parallel \text{length}$

The pMSK label is the 8-bit ASCII string:

Early authentication Master Session Key@ietf.org

9. Packet and TLV Extension

EEP reuse EAP Codes 5(EAP Initiate) and 6(EAP Finish) defined in the protocol of ERP [RFC5296]. The packet format for these messages follows the EAP packet format defined in RFC 3748.

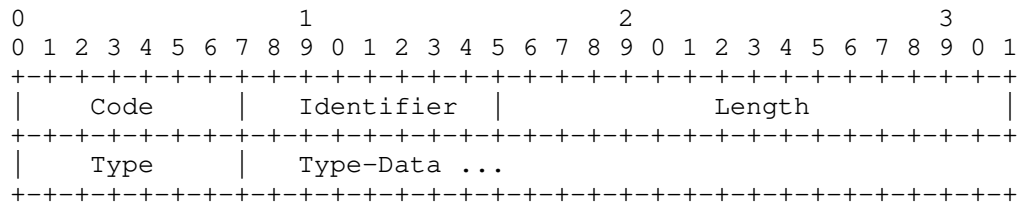


Figure 10: EAP Packet

Code

5 Initiate

6 Finish

Identifier

Refer to [RFC5296] Section 5.3

Type

This field indicates that this is an EEP exchange. Three new Type values are defined for the purpose of early authentication.

3 Pre-Early-auth

4 Post-Early-auth

5 Early-auth Action

Type-Data

The Type-Data field varies with the Type of early authentication packet.

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

One E flag bit is added in EAP Initiate/Re-auth-Start message.

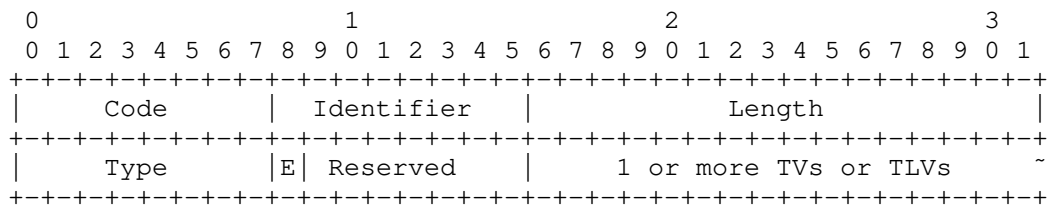


Figure 11: EAP Initiate/Re-auth-Start Packet

Code = 5(EAP Initiate)

Identifier

Refer to [RFC5296] Section 5.3

Type = 1(Re-auth-Start)

Flags

'E' - The E flag is used to indicate whether EEP is supported or not. If E Bit is set to 1, it indicate that EEP is supported by the authenticator and the MH can start the early authentication. If E Bit is set to 0, MH can not start early authentication using EEP.

Reserved: MUST be set to 0.

TVs or TLVs: refer to ERP [RFC5296].

To avoid redundant trigger message at the beginning, No new early authentication start message is defined.

9.2. EAP Initiate/Pre-Early-auth

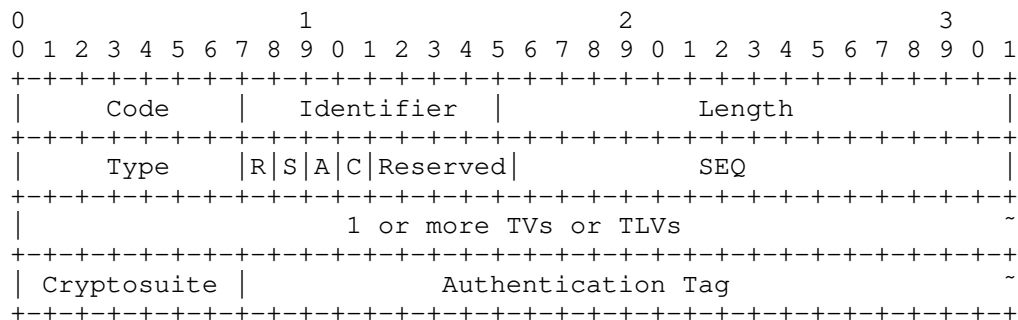


Figure 12: EAP Initiate/Pre-Early-auth Packet

Code = 5(EAP Initiate)

Identifier

Refer to [RFC5296] Section 5.3

Type = 3(Pre-Early-auth)

Flags

'R' - The value of result flag MUST be zero and ignored on reception.

'S' - The value of secure flag indicate whether cryptosuite and authentication tag is appended.

0 Cryptosuite and Authentication Tag are not appended.

1 Cryptosuite and Authentication Tag are appended at the end of message.

When the EAP Initiate/Early-auth action message is transferred between SAP-AAA and Home-AAA, S Bit = 0.

'A' - Authentication flag:

0 MH do not request to do full EAP authentication.

1 MH request to do full EAP authentication.

'C' - Continue flag:

0 This is a normal Pre-Early-auth message.

1 This message is used to extend the lifetime of Pre-Early-auth session.

SEQ

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

TVs and TLVs

NAS-Identifier: This is a TLV payload, type is 4. Exactly one NAS-Identifier or NAS-Identifier-NAI TLV SHOULD be included in the EAP Initiate/Pre-Early-auth message.

NAS-Identifier-NAI: This is a TLV payload, type is TBD. Exactly one NAS-Identifier or NAS-Identifier-NAI TLV SHOULD be included in the EAP Initiate/Pre-Early-auth message.

List of cryptosuites: This is a TLV payload, type is 5. Exactly one List of cryptosuites TLV SHOULD be included in the EAP Initiate/Pre-Early-auth message.

KeyName-NAI: This is a TLV payload. Type = 1. When the S Bit is set to 1, exactly one KeyName-NAI attribute SHOULD be present in an EAP

Initiate/Pre-Early-auth packet.

Sequence Number: It is carried in a TV payload. The Type is TBD (which is lower than 128). When the C flag is set to 1, exactly one sequence number SHOULD be present in an EAP Initiate/Pre-Early-auth packet.

Cryptosuite: This field indicates the integrity algorithm and the PRF used for EEP. Key lengths and output lengths are either indicated or 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 EEP packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

Authentication Tag is calculated using pIK derived from EMSK or DS-pIK derived from DSRK.

9.3. EAP Finish/Pre-Early-auth

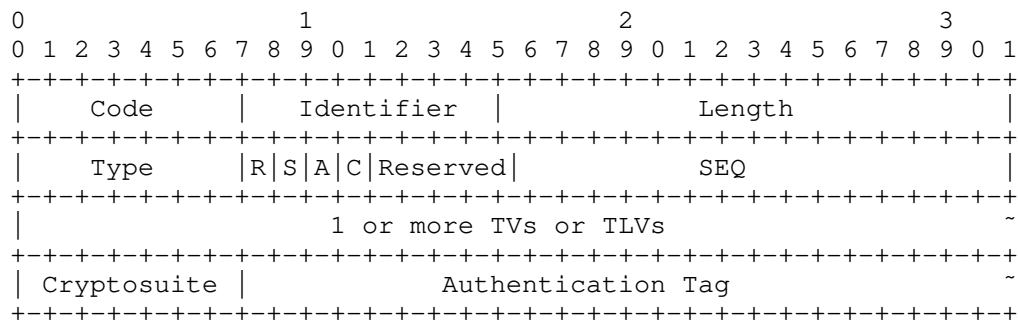


Figure 13: EAP Finish/Pre-Early-auth Packet

Code = 6(EAP Finish)

Identifier

Refer to [RFC5296] Section 5.3

Type = 3 (Pre-Early-auth)

Flags

'R' - Result flag, value 0 Indicate success, 1 Indicate failure.

'S' - The value of secure flag indicate whether cryptosuite and authentication tag is appended.

0 Cryptosuite and Authentication Tag are not appended.

1 Cryptosuite and Authentication Tag are appended at the end of message.

'A' - Authentication flag, value:

0 Full EAP authentication is not required.

1 Full EAP authentication is required.

If MH set A flag to 1 in EAP Initiate/Pre-Early-auth message, the AAA server either rejects the early authentication or set A flag to 1 in EAP Finish/Pre-Early-auth message.

'C' - Continue flag:

0 This is a normal Pre-Early-auth message.

1 This message is used to extend the lifetime of Pre-Early-auth session.

SEQ

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

TVs and TLVs

pMSK Lifetime: This is a TV payload. The value field is a 32-bit field and contains the lifetime of pMSK generated in early authentication.

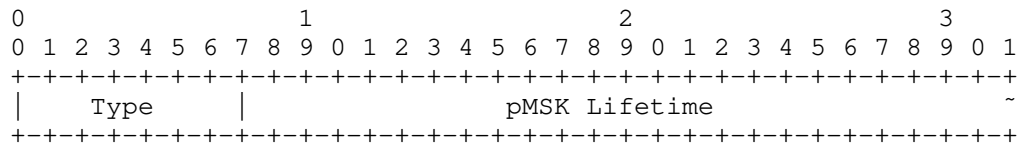


Figure 14: pMSK Lifetime

Type = TBD

The life time is calculated after the pMSK has been generated. That is to say, if full authentication is require, the life time is started after EAP authentication. If the pMSK life time expired, the MH should do Pre-Early-auth again and Post-Early-auth will be rejected.

pRK Lifetime: This is a TV payload. The value field is a 32-bit field and contains the lifetime of pRK generated in early authentication.

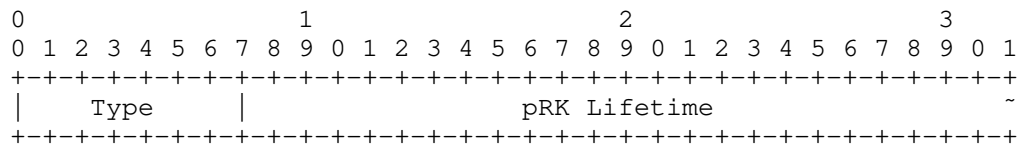


Figure 15: pRK Lifetime

Type = TBD

Result Code: When R flag is set to 1, this TV payload MAY be included in EAP Finish/Pre-Early-auth message.

List of cryptosuites: This is a TLV payload, type is 5. Exactly one List of cryptosuites TLV SHOULD be included in the EAP Finish/Pre-Early-auth message. It will help MH to select proper crypto suite to do key verification in Post-Early-auth phase.

KeyName-NAI: This is a TLV payload. Type = 1. When the S flag is set to 1, exactly one KeyName-NAI attribute SHOULD be present in an EAP Finish/Pre-Early-auth packet.

Cryptosuite: This field indicates the integrity algorithm and the PRF used for EEP. 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 EEP packet, excluding the authentication tag field itself. The

length of the field is indicated by the Cryptosuite.

Authentication Tag is calculated using pIK derived from EMSK or DS-pIK derived from DSRK.

9.4. EAP Initiate/Post-Early-auth

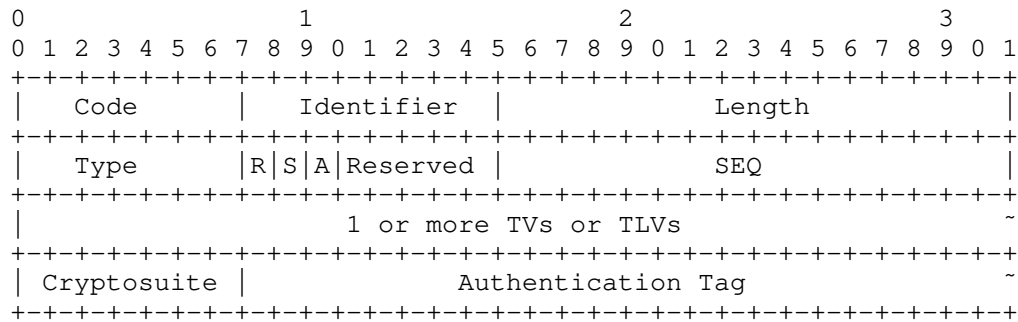


Figure 16: EAP Initiate/Post-Early-auth Packet

Code = 5 (EAP Initiate)

Identifier

Refer to [RFC5296] Section 5.3

Type = 4 (Post-Early-auth)

Flags

'R' - Result flag, Value MUST be zero and ignored on reception.

'S' - Secure flag, value MUST be 1 and Cryptosuite and Authentication Tag must be appended at the end of message.

'A' - Authentication flag, value MUST Be 0 and full EAP authentication is not required.

SEQ

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

TVs and TLVs

NAS-Identifier: This is a TLV payload, type is 4. Exactly one NAS-Identifier or NAS-Identifier-NAI TLV SHOULD be included in the EAP Initiate/Post-Early-auth message.

NAS-Identifier-NAI: This is a TLV payload, type is TBD. Exactly one NAS-Identifier or NAS-Identifier-NAI TLV SHOULD be included in the EAP Initiate/Post-Early-auth message.

KeyName-NAI: This is a TLV payload. Type = 1. Exactly one KeyName-NAI attribute MUST be present in an EAP Finish/Post-Early-auth packet.

Cryptosuite: This field indicates the integrity algorithm and the PRF used for EEP. 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 EEP packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

Authentication Tag is calculated using pIK derived from EMSK or DS-pIK derived from DSRK.

9.5. EAP Finish/Post-Early-auth

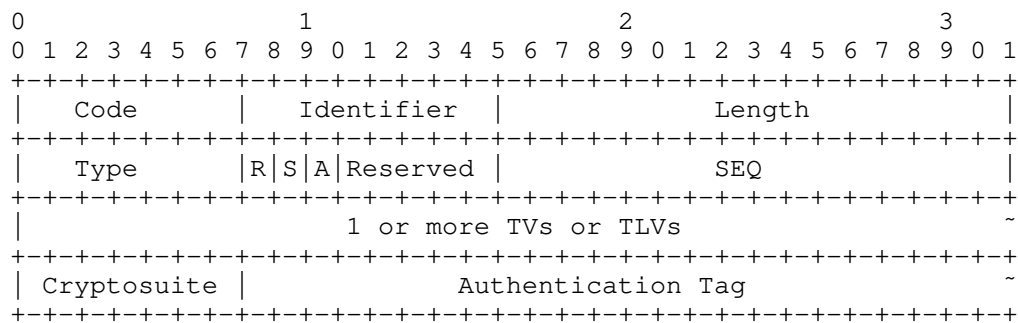


Figure 17: EAP Finish/Post-Early-auth Packet

Code = 6(EAP Finish)

Identifier

Refer to [RFC5296] Section 5.3

Type = 4(Post-Early-auth)

Flags

'R' - Result flag, value 0 Indicate success, 1 Indicate failure.

'S' - The value of secure flag indicate whether cryptosuite and

authentication tag is appended.

0 Cryptosuite and Authentication Tag are not appended.

1 Cryptosuite and Authentication Tag are appended at the end of message.

'A' - Authentication flag, value:

0 Full EAP authentication is not required.

1 Full EAP authentication is required.

If MH set A flag to 1 in EAP Initiate/Pre-Early-auth message, the AAA server either rejects the early authentication or set A flag to 1 in EAP Finish/Pre-Early-auth message.

SEQ

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

TVs and TLVs

Result Code: When R flag is set to 1, this TV payload MAY be included in EAP Finish/Post-Early-auth message.

List of cryptosuites: This is a TLV payload, type is 5. If the Result Code is 2 (crypto cipher suite is not supported). This TLV should be included in the EAP Finish/Post-Early-auth message.

KeyName-NAI: This is a TLV payload. Type = 1. If the Result Code is 3 (key is not found), the TLV should not be included in the EAP Finish/Post-Early-auth message and S Bit should be set to 0. When the S flag is set to 1, exactly one KeyName-NAI attribute SHOULD be present in an EAP Finish/Post-Early-auth packet.

Cryptosuite: This field indicates the integrity algorithm and the PRF used for EEP. 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 EEP packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

Authentication Tag is calculated using pIK derived from EMSK or DS-pIK derived from DSRK.

9.6. EAP Initiate/Early-auth Action

The functionality of message EAP Initiate/Early-auth Action message is based on its sub type. The detailed information refers to the description of sub type field.

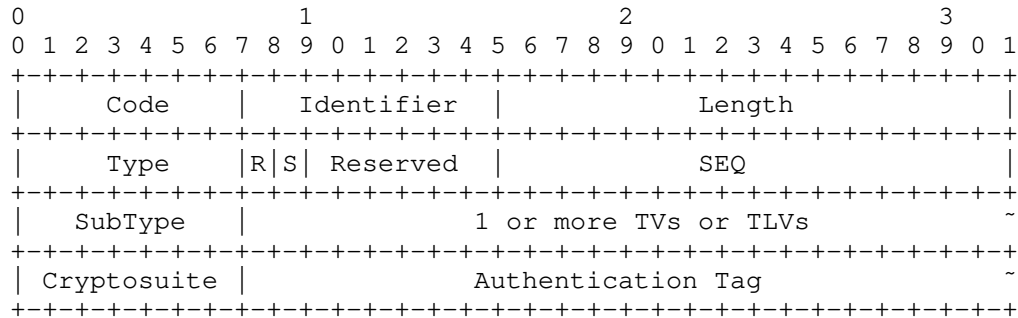


Figure 18: EAP Initiate/Early-auth Action Packet

Code = 5(EAP Initiate).

Identifier

Refer to [RFC5296] Section 5.3

Type = 5(Early-auth Action).

Flags

'R' - The value of result flag MUST be zero and ignored on reception.

'S' - The value of secure flag indicate whether cryptosuite and authentication tag is appended.

0 Cryptosuite and Authentication Tag are not appended.

1 Cryptosuite and Authentication Tag are appended at the end of message.

When the EAP Initiate/Early-auth action message is transferred between SAP-AAA and Home-AAA, S Bit = 0.

SEQ

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

Sub Type

1 Early authentication Probe message. The message is sent by MH to SAP to probe whether the early authentication for specified CAP is supported.

2 De-Pre-Early-auth message. The message is sent by MH to SAP to release the early authentication with specified CAP.

To avoid obsolete early authentication session, MH may release its established early authentication session before it disconnecting from the network.

3 De-Post-Early-auth message. The message is sent by MH to SAP to change the current fully authenticated state to early authenticated state.

This message is used to adapt to the situation where MH keep moving between 2 AAA realms.

TVs and TLVs

NAS-Identifier: As defined in [RFC5296], it is carried in a TLV payload. It is used to indicate the identifier of a CAP. One or more NAS-identifier MAY be included in EAP Initiate/Early-auth Action message sent by MH. The Local Domain is considered as the AAA realm for this CAP.

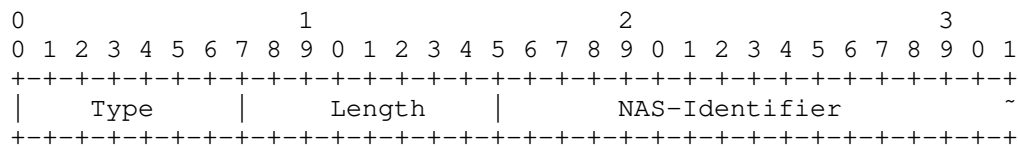


Figure 19: NAS-Identifier

Type = 4

Length >= 1

NAS-Identifier-NAI:

The NAI is variable in length, not exceeding 253 octets. The NAS-identifier is in the username part of the NAI. The realm part of the NAI is the visited domain name. One or more NAS-identifier-NAI MAY be included in EAP Initiate/Early-auth Action message sent by MH.

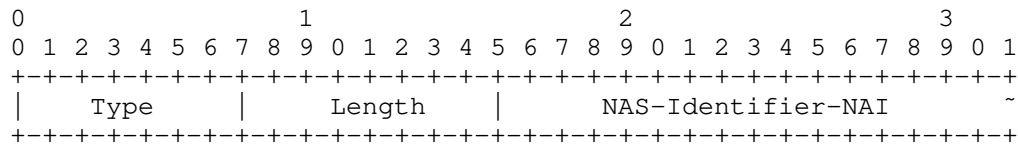


Figure 20: NAS-Identifier-NAI

Type = TBD

Length >= 1

KeyName-NAI: This is a TLV payload. The NAI is variable in length, not exceeding 253 octets. The EMSK name is in the username part of the NAI and is encoded in hexadecimal values. The EMSK name is 64 bits in length and so the username portion takes up 128 octets. The realm part of the NAI is the visited domain name. When the S Bit is set to 1, exactly one KeyName-NAI attribute SHOULD be present in an EAP Initiate/Early-auth Action packet.

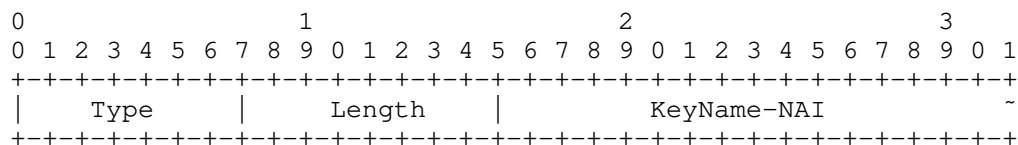


Figure 21: KeyName-NAI

Type = 1

Length >= 1

The authenticator uses the realm in the KeyName-NAI field to send the message to the appropriate EEP server.

Cryptosuite: This field indicates the integrity algorithm and the PRF used for EEP. 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 EEP packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

Authentication Tag is calculated using pIK derived from EMSK or DS-pIK derived from DSRK.

9.7. EAP Finish/Early-auth Action

EAP Finish/Early-auth Action is sent by SAP-AAA through SAP to inform MH the action results. For De-Pre-Early-auth and De-Post-Early-auth, reply message is not required. So corresponding sub type is not defined.

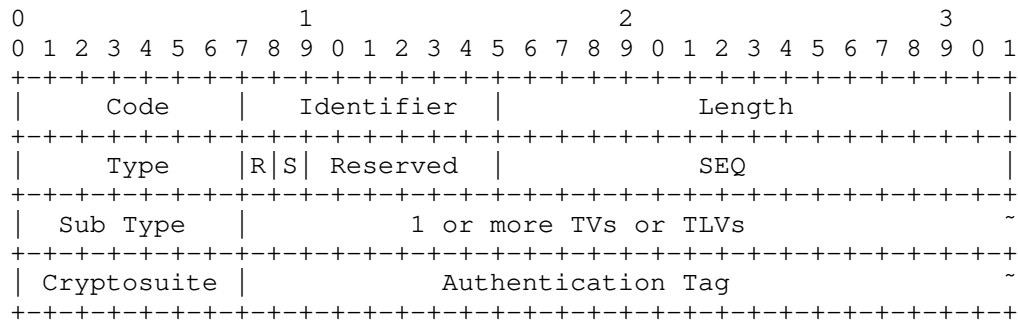


Figure 22: EAP Finish/Early-auth Action Packet

Code = 5(EAP Initiate)

Identifier

Refer to [RFC5296] Section 5.3

Type = 5(Early-auth Action)

Flags

'R' - Result flag, value 0 Indicate success, 1 Indicate failure.

'S' - The value of secure flag indicate whether cryptosuite and authentication tag is appended.

0 Cryptosuite and Authentication Tag are not appended.

1 Cryptosuite and Authentication Tag are appended at the end of message.

SEQ

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

Sub Type

1 Early authentication Probe message.

TVs and TLVs

Result Code: When R Bit is set to 1, this TV payload MAY be included in EAP Finish/Early-auth Action message.

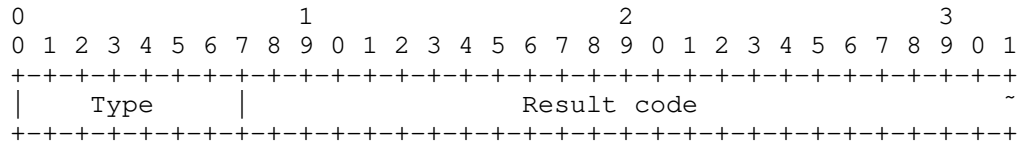


Figure 23: Result Code

Type = TBD

Result code

0 Success

1 Unspecified failure

2 Cryptosuite is not supported

3 Key is not found

4 Fail to verify the authentication tag

5~9 Reserved

10 Early authentication is not supported

11~20 Reserved

21 Early authentication session is not found for this CAP

Probe Result: This is TLV payload. If the Result Code is 0 (success), The number of Probe Results in EAP Finish/Early-auth action message should be identical to the number of NAS-ids and NAS-id-NAIs in EAP Initiate/Early-auth Action message.

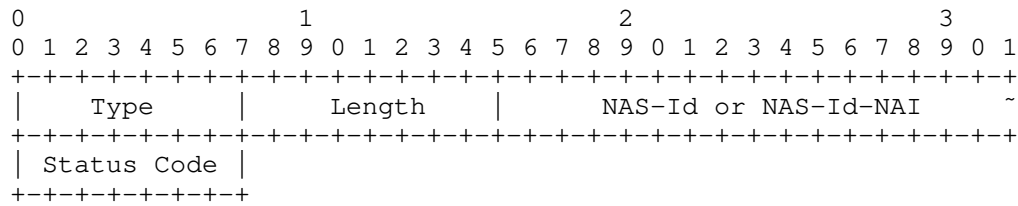


Figure 24: Probe Result

Type = TBD

Length >= 2

Status Code:

0 EEP is supported for this CAP

1 EEP is not supported for this CAP

List of cryptosuites: This is a TLV payload. If the Result Code is 2, crypto cipher suite is not supported. This TLV MAY be included in the EAP Finish/Early-auth Action message.

The value field contains a list of crypto suites, each of size 1 octet. The SAP-AAA include this attribute in the EAP Finish/Early-auth Action message to signal to the MH about its cryptographic algorithm capabilities. The Cryptosuite values are as specified:

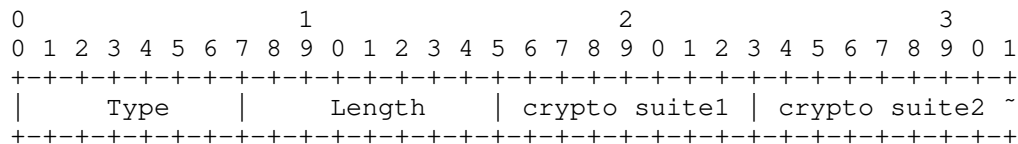


Figure 25: List of cryptosuites

Type = 5

Length >= 1

Crypto suite

0 RESERVED

1 HMAC-SHA256-64

2 HMAC-SHA256-128 (Mandatory to implement and should be enabled in

the default configuration)

3 HMAC-SHA256-256

KeyName-NAI: This is a TLV payload. Type = 1. If the S flag is set to 1, exactly one KeyName-NAI TLV should be included in EAP Finish/Early-auth Action message. If R flag is set to 1 and the Result Code is 3 (key is not found), the TLV should not be included in the EAP Finish/Early-auth Action message and S flag should be set to 0.

Cryptosuite: This field indicates the integrity algorithm and the PRF used for EEP. 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 EEP packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

Authentication Tag is calculated using pIK derived from EMSK or DS-pIK derived from DSRK.

10. Lower Layer Considerations

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

11. AAA Transport Considerations

AAA transport of EEP messages is the same as AAA transport of the ERP message [RFC5296]. In addition, the document requires AAA transport of the EEP keying materials delivered by the EEP server to the CAP. Hence, a new Diameter EEP application message should be specified to transport the keying materials.

12. Security Considerations

TBD.

13. IANA Considerations

New TLV types:

NAS-Identifier

Sequence number

NAS-Identifier-NAI

pMSK lifetime

pRK lifetime

Result code

Probe result

14. Acknowledgements

Thanks to Qin Wu for guiding some technique solution and helpful comments on this document.

15. References

15.1. 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.

15.2. 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.

[I-D.ietf-hokey-erp-aak] Cao, Z., Deng, H., Wang, Y., Wu, W., and G. Zorn, "EAP Re-authentication Protocol Extensions for Authenticated Anticipatory Keying (ERP/AAK)", draft-ietf-hokey-erp-aak-02 (work in progress), May 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.
- [RFC5836] Ohba, Y., Wu, Q., and G. Zorn, "Extensible Authentication Protocol (EAP) Early Authentication Problem Statement", RFC 5836, April 2010.

Authors' Addresses

Hao Wang (editor)
Hangzhou H3C Tech. Co., Ltd.
H3C, Digital Technology Plaza, Shangdi 9 Street, Haidian District
Beijing
China(100085)

Phone: +86 010 82774462
EMail: hwang@h3c.com

Yang Shi (editor)
Hangzhou H3C Tech. Co., Ltd.
H3C, Digital Technology Plaza, Shangdi 9 Street, Haidian District
Beijing
China(100085)

Phone: +86 010 82775276
EMail: young@h3c.com

Tina Tsou
Huawei Technologies
BHuaWei Technologies,
Bantian, Longgang District
Shenzhen
China(518129)

EMail: tena@huawei.com

Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 28, 2011

K. Hoeper
Motorola
S. Decugis
NICT
G. Zorn
Network Zen
Q. Wu
T. Taylor
Huawei
October 25, 2010

Handover Keying (HOKEY) Architecture Design
draft-ietf-hokey-arch-design-01

Abstract

The Handover Keying (HOKEY) Working Group seeks to minimize handover delay due to authentication when a peer moves from one point of attachment to another. Work has progressed on two different approaches to reduce handover delay: early authentication (so that authentication does not need to be performed during handover), and reuse of cryptographic material generated during an initial authentication to save time during re-authentication. A starting assumption is that the mobile host or "peer" is initially authenticated using the Extensible Authentication Protocol (EAP), executed between the peer and an EAP server as defined in RFC 3748.

This document documents the HOKEY architecture. Specifically, it describes design objectives, the functional environment within which handover keying operates, the functions to be performed by the HOKEY architecture itself, and the assignment of those functions to architectural components. It goes on to illustrate the operation of the architecture within various deployment scenarios that are described more fully in other documents produced by the HOKEY Working Group.

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 April 28, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	4
2. Terminology	6
3. Design Goals	6
3.1. Reducing Signalling Overhead	6
3.1.1. Minimized Communications with Home Servers	6
3.1.2. Integrated Local Domain Name (LDN) Discovery	7
3.2. Better Deployment Scalability	7
4. Functions That Must Be Supported	7
4.1. System Overview	7
4.2. Pre-Authentication Function (Direct or Indirect)	10
4.3. EAP Re-authentication Function	10
4.4. EAP Authentication Function	10
4.5. Authenticated Anticipatory Keying (AAK) Function	10
4.6. EAP-Based Handover Key Management	11
5. Components of the HOKEY Architecture	11
5.1. Functions of the Peer	12
5.2. Functions of the Serving Authenticator	12
5.3. Functions of the Candidate Authenticator	13
5.4. Functions of the EAP Server	14
5.5. Functions of the ER Server	15
6. Deployment Scenarios	16
7. AAA Consideration	16
7.1. Standalone HOKEY server	16
8. Security Considerations	17
9. IANA Considerations	17
10. Acknowledgments	17
11. Informative References	17
Authors' Addresses	18

1. Introduction

The Extensible Authentication Protocol (EAP) [RFC3748] is an authentication framework that supports different types of authentication methods. Originally designed for dial-up connections, EAP is now commonly used for authentication in wireless access networks.

When a host (or "peer", the term used from this point onward) changes its point of attachment to the network, it must be re-authenticated. If a full EAP authentication must be repeated, several message round-trips between the peer and the home EAP server may be involved. The resulting delay will result in degradation or in the worst case loss of any service session in progress if communication is suspended while re-authentication is carried out. The delay is worse if the new point of attachment is in a visited network rather than the peer's home network, because of the extra procedural steps involved as well as because of the probable increase in round-trip time.

[RFC5169] describes this problem more fully and establishes design goals for solutions to reduce re-authentication delay for transfers within a single administrative domain. [RFC5169] also suggests a number of ways to achieve a solution:

- o specification of a method-independent, efficient, re-authentication protocol;
- o reuse of keying material from the initial authentication;
- o deployment of re-authentication servers local to the peer to reduce round-trip delay; and
- o specification of the additional protocol needed to allow the EAP server to pass authentication information to the local re-authentication servers.

[RFC5295] tackles the problem of reuse of keying material by specifying how to derive a hierarchy of cryptographically independent purpose-specific keys from the results of the original EAP authentication. [RFC5296] specifies a method-independent re-authentication protocol (ERP) applicable to two specific deployment scenarios:

- o where the peer's home EAP server also performs re-authentication; and
- o where a local re-authentication server exists but is collocated with a AAA proxy within the domain.

Other work provides further pieces of the solution or insight into the problem. For the purpose of this draft, [RFC5749] provides an abstract mechanism for distribution of keying material from the EAP server to re-authentication servers. [RFC5836] contrasts the EAP re-authentication (ER) strategy provided by [RFC5296] with an alternative strategy called "early authentication". [RFC5836] defines EAP early authentication as the use of EAP by a mobile peer to establish authenticated keying material on a target attachment point prior to its arrival. Here, a full EAP execution occurs before the handover of the peer takes place. Hence, the goal of EAP early authentication is to complete all EAP-related communications, including AAA signaling, in preparation for the handover, before the mobile device actually moves. Early authentication includes direct and indirect pre-authentication as well as Authenticated Anticipatory Keying (AAK). All three mechanisms provide means to execute a full EAP authentication with a Candidate Access Point (CAP) while still being connected to the Serving Access Point (SAP) but vary in their respective system assumptions and communication paths. In particular, direct pre-authentication assumes that clients are capable of discovering candidate access points and all communications are routed through the serving access point. On the other hand, indirect pre-authentication assumes an existing relationship between SAP and CAP, whereas in AAK the client interacts with the AAA to discover and connect to CAPs.

Both EAP re-authentication and early authentication enable faster inter-authenticator handovers. However, it is currently unclear how the necessary handover infrastructure is deployed and can be integrated into existing EAP infrastructures. In particular, previous work has not described how ER servers that act as endpoints in the re-authentication process should be integrated into local and home domain networks. Furthermore, it is currently unspecified how EAP infrastructure can support the timely triggering of early authentications and aid with the selection of candidate access points.

This document proposes a general HOKEY architecture and demonstrates how it can be adapted to different deployment scenarios. To begin with, Section 3 recalls the design objectives for the HOKEY architecture. Section 4 reviews the functions that must be supported within the architecture. Section 5 describes the components of the HOKEY architecture. Finally, Section 6 describes the different deployment scenarios that the HOKEY Working Group has addressed and the information flows that must occur within those scenarios, by reference to the documents summarized above where possible and otherwise within this document itself.

2. Terminology

This document contains no normative language, hence [RFC2119] language does not apply.

This document reuses most of the terms defined in Section 2.2 of [RFC5836]. In addition, it defines the following:

EAP Early Authentication

The use of EAP by a mobile peer to establish authenticated keying material on a target attachment point prior to its arrival, see [RFC5836].

EAP Re-authentication (ER)

The use of keying material derived from an initial EAP authentication to enable single-roundtrip re-authentication of a mobile peer. For a detailed description of the keying material see Section 3 of [RFC5296].

ER Server

A component of the HOKEY architecture that terminates the EAP re-authentication exchange with the peer.

ER Key Management

An instantiation of the mechanism provided by [RFC5749] for creating and delivering root keys from an EAP server to an ER server.

3. Design Goals

This section investigates the design goals for the HOKEY architecture. These include reducing the signaling overhead for re-authentication and early authentication, integrating local domain name discovery, and improving deployment scalability. These goals supplement the discussion in [RFC5169].

3.1. Reducing Signalling Overhead

3.1.1. Minimized Communications with Home Servers

ERP requires only one round trip, however, this roundtrip may require communications between a peer and its home ER and/or home AAA server even if the peer is currently attached to a visited (local) network. As a result, even this one round trip may introduce long delays because home ER and home AAA servers may be distant from the peer. To lower the signaling overhead, communication with the home ER server and home AAA server should be minimized. Ideally, a peer

should only need to communicate with local servers and other local entities.

3.1.2. Integrated Local Domain Name (LDN) Discovery

ERP bootstrapping must occur before (implicit) or during (explicit) a handover to transport the necessary re-authentication root keys to the local ER server involved. Implicit bootstrapping is preferable because it does not require communication with the home ER server during handover (see previous section), but it requires the peer to know the domain name of the ER server in order to derive the necessary re-authentication keying material. [RFC5296] does not specify such a domain name discovery mechanism and suggests that the peer may learn the domain name through the EAP- Initiate/ Re-auth-Start message or via lower layer announcements. To allow more efficient handovers, a HOKEY architecture should support an efficient domain name discovery mechanism and allow its integration with ERP implicit bootstrapping. Even in the case of explicit bootstrapping, local domain name discovery should be optimized such that it does not require contacting the home AAA server, as is currently the case.

3.2. Better Deployment Scalability

To provide better deployment scalability, it should not be required that the HOKEY server and AAA servers or proxies are collocated. Separation of these entities may cause problems with routing, but allows flexibility in deployment and implementation.

4. Functions That Must Be Supported

4.1. System Overview

This section views the HOKEY architecture as the implementation of a subsystem providing authentication services to AAA. Not only does AAA depend on the authentication subsystem, but the latter also depends on AAA as a means for the routing and secure transport of messages internal to the operation of network access authentication.

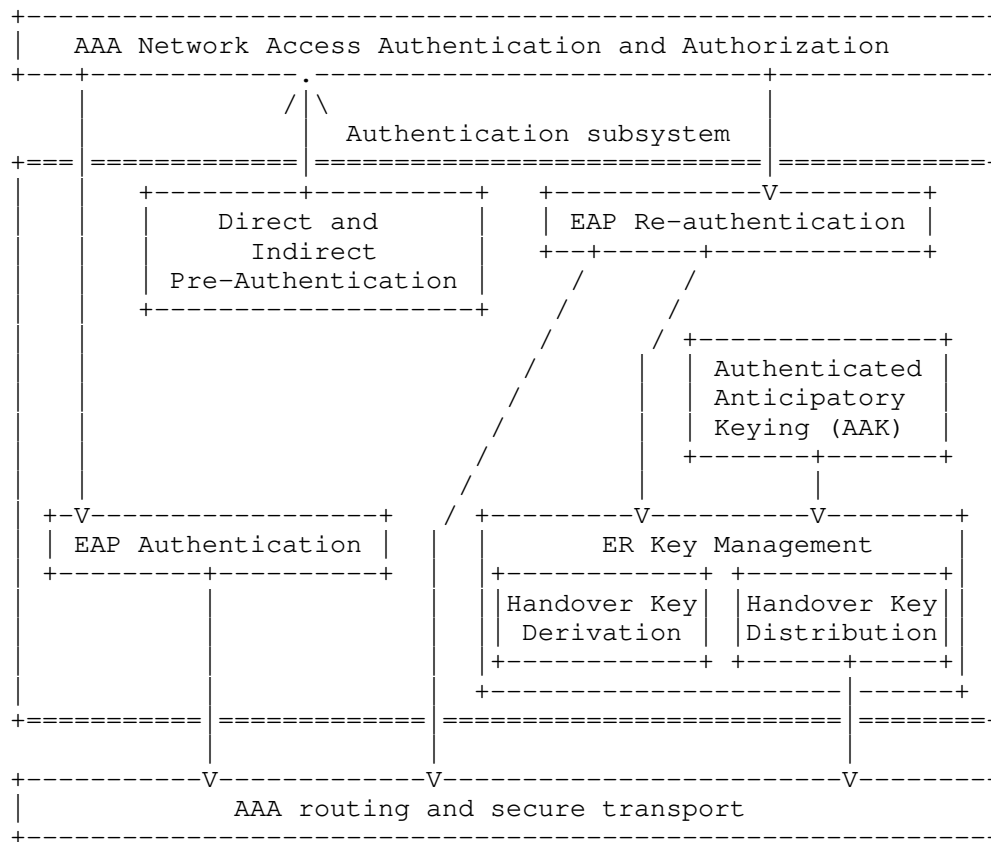
The operation of the authentication subsystem also depends on the availability of a number of discovery functions:

- o discovery of candidate access points, by the peer, by the serving attachment point, or by some other entity;
- o discovery of the authentication services supported at a given candidate access point;

- o discovery of the required server in the home domain when a candidate access point is not in the same domain as the serving attachment point, or no local server is available;
- o peer discovery of the local domain name (LDN) when EAP re-authentication is used with a local server.

It is assumed that these functions are provided by the environment within which the authentication subsystem operates, and are outside the scope of the authentication subsystem itself. Local domain name discovery is a possible exception.

Figure 1 shows the major functions comprising the authentication subsystem and their interdependencies. These functions are described below. [EDITOR'S NOTE: These probably need refinement. The relationship of pre-authentication to EAP authentication, for instance, is currently not totally correct, when one takes account of the roles described in Section 5. AAK also needs an extension of ER key management.]



Arrows show the direction of functional dependency.

Figure 1: Authentication Subsystem Functional Overview

Figure 1 shows the following dependencies:

- o When AAA is invoked to authenticate and authorize network access, it uses one of two services offered by the authentication subsystem: full EAP authentication, or EAP re-authentication.
- o Pre-authentication triggers AAA network access authentication and authorization at each candidate access point, which in turn causes full EAP authentication to be invoked.
- o EAP re-authentication invokes ER key management at the time of authentication to create and distribute keying material to ER servers.

- o Authenticated anticipatory keying (AAK) relies on ER key management to establish keying material on ER/AAK servers, but uses an extension to ER key management to derive and establish keying material on candidate authenticators.

EAP authentication, EAP re-authentication, and handover key distribution depend on the routing and secure transport service provided by AAA. Discovery functions and the function of authentication and authorization of network entities (access points, ER servers) are not shown. As stated above, these are external to the authentication subsystem.

4.2. Pre-Authentication Function (Direct or Indirect)

The pre-authentication function is responsible for discovery of candidate access points and completion of network access authentication and authorization at each candidate access point in advance of handover. The operation of this function is described in general terms in [RFC5836]. No document is yet available to describe the implementation of pre-authentication in terms of specific protocols. [RFC5873] could be part of the solution, but is Experimental rather than Standards Track.

4.3. EAP Re-authentication Function

The EAP re-authentication function is responsible for authenticating the peer at a specific access point using keying material derived from a prior full EAP authentication. [RFC5169] provides the design objectives for an implementation of this function. [RFC5296] describes a protocol to implement EAP re-authentication subject to the architectural restrictions noted above. Work is in progress to relax those restrictions.

4.4. EAP Authentication Function

The EAP authentication function is responsible for authenticating the peer at a specific access point using a full EAP exchange. [RFC3748] defines the associated protocol. [RFC5836] shows the use of EAP as part of pre-authentication. Note that the HOKEY Working Group has not specified the non-AAA protocol required to transport EAP frames over IP that is shown in Figures 3 and 5 of [RFC5836], although [RFC5873] is a candidate.

4.5. Authenticated Anticipatory Keying (AAK) Function

The authenticated anticipatory keying function is responsible for pre-placing keying material derived from an initial full EAP authentication on candidate access points. The operation is carried

out in two steps: ER key management (with trigger not currently specified) places root keys derived from initial EAP authentication onto an ER/AAK server associated with the peer. When requested by the peer, the ER/AAK server derives and pushes predefined master session keys to a list of candidate access points. The operation of the authenticated anticipatory keying function is described in very general terms in [RFC5836]. A protocol implementation is being specified in [I-D.ietf-hokey-erp-aak].

4.6. EAP-Based Handover Key Management

EAP-based handover key management consists of EAP method independent key derivation and distribution and comprises the following specific functions:

- o handover key derivation; and
- o handover key distribution.

The derivation of handover keys is specified in [RFC5295], and key distribution is specified in [RFC5749].

5. Components of the HOKEY Architecture

This section describes the components of the HOKEY architecture, in terms of the functions they perform. The components cooperate as described in this section to carry out the functions described in the previous section. Section 6 describes the different deployment scenarios that are possible using these functions.

The components of the HOKEY architecture are as follows:

- o the peer;
- o the authenticator, which is a part of the serving access point and candidate access points;
- o the EAP server; and
- o the ER server, either in the home domain or local to the authenticator.

[EDITOR'S NOTE: probably have to add the ER/AAK server named in [I-D.ietf-hokey-erp-aak] to this list.]

5.1. Functions of the Peer

The peer participates in the functions described in Section 4 as shown in Table 1.

Function	Peer Role
EAP authentication	Determines that full EAP authentication is needed based on context (e.g., initial authentication), prompting from the authenticator, or discovery that only EAP authentication is supported. Participates in the EAP exchange with the EAP server.
-	-
Direct pre-authentication	Discovers candidate access points. Initiates pre-authentication with each, followed by EAP authentication as above, but using IP rather than L2 transport for the EAP frames.
-	-
Indirect pre-authentication	Enters into a full EAP exchange when triggered, using either L2 or L3 transport for the frames.
-	-
EAP re-authentication	Determines that EAP re-authentication is possible based on discovery or authenticator prompting. Discovers ER server. Participates in ERP exchange with ER server.
-	-
Authenticated anticipatory keying	Determines that AAK is possible based on discovery or serving authenticator prompting. Discovers candidate access points. Sends request to serving authenticator to distribute keying material to the candidate access points.
-	-
ER key management	No role.

Table 1: Functions of the Peer

5.2. Functions of the Serving Authenticator

The serving authenticator participates in the functions described in Section 4 as shown in Table 2.

Function	Serving Authenticator Role
EAP authentication	No role.
-	-
Direct pre-authentication	No role.
-	-
Indirect pre-authentication	Discovers candidate access points. Initiates an EAP exchange between the peer and the EAP server through each candidate authenticator. Mediates between L2 transport of EAP frames on the peer side and a non-AAA protocol over IP toward the candidate access point.
-	-
EAP re-authentication	No role.
-	-
Authenticated anticipatory keying	Mediates between L2 transport of AAK frames on the peer side and AAA transport toward the ER/AAK server.
-	-
ER key management	No role.

Table 2: Functions of the Serving Authenticator

5.3. Functions of the Candidate Authenticator

The candidate authenticator participates in the functions described in Section 4 as shown in Table 3.

Function	Candidate Authenticator Role
EAP authentication	Invokes AAA network access authentication and authorization upon handover/initial attachment. Mediates between L2 transport of EAP frames on the peer link and AAA transport toward the EAP server.
-	-
Direct pre-authentication	Invokes AAA network access authentication and authorization when the peer initiates authentication. Mediates between non-AAA L3 transport of EAP frames on the peer side and AAA transport toward the EAP server.
-	-
Indirect pre-authentication	Same as direct pre-authentication, except that it communicates with the serving authenticator rather than the peer.
-	-
EAP re-authentication	Invokes AAA network access authentication and authorization upon handover. Discovers or is configured with the address of the ER server. Mediates between L2 transport of a ERP frames on the peer side and AAA transport toward the ER server.
-	-
Authenticated anticipatory keying	Receives and saves pMSK.
-	-
ER key management	No role.

Table 3: Functions of the Candidate Authenticator

5.4. Functions of the EAP Server

The EAP server participates in the functions described in Section 4 as shown in Table 4.

Function	EAP Server Role
EAP authentication	Authenticates and authorizes the candidate access point to act as authenticator. Terminates EAP signalling between it and the peer via the candidate authenticator. Determines whether network access authentication succeeds or fails. Provides MSK to authenticator.
-	-
Direct pre-authentication	As for EAP authentication.
-	-
Indirect pre-authentication	As for EAP authentication.
-	-
EAP re-authentication	Mutually authenticates with the ER server and authorizes it for receiving keying material. Provides rRK or DSrRK to the ER server.
-	-
Authenticated anticipatory keying	As for EAP re-authentication.
-	-
ER key management	Creates rRK or DSrRK and distributes it to ER server requesting the information.

Table 4: Functions of the EAP Server

5.5. Functions of the ER Server

The ER server participates in the functions described in Section 4 as shown in Table 5. [EDITOR'S NOTE: Need discussion of respective roles of local and home ER server, or whether there should even be such a distinction.]

Function	ER Server Role
EAP authentication	No role.
-	-
Direct pre-authentication	No role.
-	-
Indirect pre-authentication	No role.
-	-
EAP re-authentication	Authenticates and authorizes the candidate access point to act as authenticator. Authenticates itself to the EAP server and acquires rRK or DSrRK as applicable when necessary. Terminates ERP signalling between it and the peer via the candidate authenticator. Determines whether network access authentication succeeds or fails. Provides MSK to authenticator.
-	-
Authenticated anticipatory keying	Authenticates itself to the EAP server and acquires rRK or DSrRK as applicable when necessary. Authenticates and authorizes the candidate access points to act as authenticator. Derives pMSKs and passes them to the candidate access points.
-	-
ER key management	Receives and saves rRK or DSrRK as applicable.

Table 5: Functions of the ER Server

6. Deployment Scenarios

The necessity for this section and its contents are TBD.

7. AAA Consideration

7.1. Standalone HOKEY server

TBD.

8. Security Considerations

TBD

9. IANA Considerations

This document has no actions for IANA.

10. Acknowledgments

The authors would like to thank Mark Jones and Zhen Cao for their reviews of previous versions of this draft.

11. Informative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
- [RFC5169] Clancy, T., Nakhjiri, M., Narayanan, V., and L. Dondeti, "Handover Key Management and Re-Authentication Problem Statement", RFC 5169, March 2008.
- [RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", RFC 5295, August 2008.
- [RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", RFC 5296, August 2008.
- [RFC5749] Hoeper, K., Nakhjiri, M., and Y. Ohba, "Distribution of EAP-Based Keys for Handover and Re-Authentication", RFC 5749, March 2010.
- [RFC5836] Ohba, Y., Wu, Q., and G. Zorn, "Extensible Authentication Protocol (EAP) Early Authentication Problem Statement", RFC 5836, April 2010.
- [RFC5873] Ohba, Y. and A. Yegin, "Pre-Authentication Support for the Protocol for Carrying Authentication for Network Access (PANA)", RFC 5873, May 2010.

[I-D.ietf-hokey-erp-aak]

Cao, Z., Deng, H., Wang, Y., Wu, Q., and G. Zorn, "EAP Re-authentication Protocol Extensions for Authenticated Anticipatory Keying (ERP/AAK)", Internet Draft draft-ietf-hokey-erp-aak-02, May 2010.

Authors' Addresses

Katrin Hoeper
Motorola, Inc.
1301 E. Algonquin Road
Schaumburg, IL 60196
USA

Email: khoeper@motorola.com

Sebastien Decugis
NICT
4-2-1 Nukui-Kitamachi
Tokyo, Koganei 184-8795
Japan

Email: sdecugis@nict.go.jp

Glen Zorn
Network Zen
1310 East Thomas Street
Seattle, Washington 98102
USA

Email: gwz@net-zen.net

Qin Wu
Huawei Technologies Co.,Ltd
Site B, Floor 12F, Huihong Mansion, No.91 Baixia Rd.
Nanjing, JiangSu 210001
China

Phone: +86-25-84565892
Email: sunseawq@huawei.com

Tom Taylor
Huawei Technologies Co., Ltd
Ottawa
Canada

Email: tom111.taylor@bell.net

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 4, 2011

G. Zorn
Network Zen
Q. Wu
Y. Wang
Huawei
October 1, 2010

The Local Domain Name DHCPv6 Option
draft-ietf-hokey-ldn-discovery-06

Abstract

In order to derive a Domain-Specific Root Key (DSRK) from the Extended Master Session Key (EMSK) generated as a side-effect of an Extensible Authentication Protocol (EAP) method, the EAP peer must discover the name of the domain to which it is attached.

This document specifies a Dynamic Host Configuration Protocol Version 6 (DHCPv6) option designed to allow a DHCPv6 server to inform clients of the name of the local domain..

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 April 4, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Terminology	3
3. Option Format	3
3.1. DHCPv6 Local Domain Name Option	3
4. Client Behavior	4
5. Relay Agent Behavior	4
6. Security Considerations	4
7. IANA considerations	4
8. References	4
8.1. Normative References	4
8.2. Informative References	5

1. Introduction

The EAP Re-authentication Protocol (ERP) [RFC5296] is designed to allow faster re-authentication of a mobile device which was previously authenticated by means of the Extensible Authentication Protocol [RFC3748]. Given that the local root key (e.g., DSRK RFC 5295 [RFC5295]) is generated using the local domain name (LDN), LDN discovery is an important part of re-authentication. As described in RFC 5296 [RFC5296], the local domain name can be learned by the mobile device through the ERP exchange or via a lower-layer mechanism. However, no lower-layer mechanisms for LDN discovery have yet been defined.

This document specifies an extension to DHCPv6 for local domain name discovery.

2. Terminology

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. Option Format

In DHCPv6-based local domain name discovery, the LDN option is used by the DHCPv6 client to obtain the local domain name from the DHCPv6 Server after full EAP authentication has taken place.

3.1. DHCPv6 Local Domain Name Option

The format of this option is:

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| OPTION_LOCAL_DOMAIN_NAME |          option-length          |
+-----+-----+-----+-----+-----+-----+-----+-----+
| local-domain-name...   |
+-----+-----+-----+-----+-----+-----+

```

option code

OPTION_LOCAL_DOMAIN_NAME (TBD)

option-length

Length of the local-domain-name field, in octets

local-domain-name

This field contains the name of the local domain and MUST be encoded as specified in Section 8 of RFC 3315 [RFC3315].

4. Client Behavior

If a DHCPv6 client doesn't know the local domain name and requires the DHCPv6 Server to provide the DHCPv6 LDN option, it MUST include an Option Request option requesting the DHCPv6 LDN option, as described in Section 22.7 of RFC 3315 [RFC3315].

When the DHCPv6 client receives a LDN option with the local domain name present in it, it MUST verify that the option length is no more than 256 octets (the maximum length of a single FQDN allowed by DNS), and that the local domain name is a properly encoded single FQDN, as specified in Section 8, "Representation and Use of Domain Names" of RFC3315 [RFC3315].

5. Relay Agent Behavior

If a DHCPv6 relay agent has pre-existing knowledge of the local domain name (for example, from a previous AAA exchange), it SHOULD include it in an instance of the DHCPv6 LDN option and forward to the DHCPv6 server as a suboption of the Relay-Supplied Options option [I-D.ietf-dhc-dhcpv6-relay-supplied-options].

6. Security Considerations

The communication between the DHCPv6 client and the DHCPv6 server for the exchange of local domain name information is security sensitive and requires authentication, integrity and replay protection. DHCPv6 security [RFC3315] can be used for this purpose.

7. IANA considerations

IANA is requested to assign one new option code from the registry of DHCP Option Codes maintained at <http://www.iana.org/assignments/dhcpv6-parameters>, referencing this document.

8. References

8.1. Normative References

[I-D.ietf-dhc-dhcpv6-relay-supplied-options] Lemon, T. and W. Wu, "Relay-Supplied DHCP Options", draft-ietf-dhc-dhcpv6-relay-

supplied-options-02
(work in progress),
September 2010.

[RFC2119]

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

[RFC3315]

Droms, R., Bound, J.,
Volz, B., Lemon, T.,
Perkins, C., and M.
Carney, "Dynamic Host
Configuration Protocol
for IPv6 (DHCPv6)",
RFC 3315, July 2003.

[RFC5295]

Salowey, J., Dondeti,
L., Narayanan, V., and
M. Nakhjiri,
"Specification for the
Derivation of Root Keys
from an Extended Master
Session Key (EMSK)",
RFC 5295, August 2008.

[RFC5296]

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

8.2. Informative References

[RFC3748]

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

Authors' Addresses

Glen Zorn
Network Zen
227/358 Thanon Sunpawut
Bang Na, Bangkok 10110
Thailand

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

Qin Wu
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 21001
China

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

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

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

Network Working Group
Internet-Draft
Obsoletes: 5296 (if approved)
Intended status: Standards Track
Expires: April 23, 2011

Q. Wu, Ed.
Huawei
Z. Cao
China Mobile
Y. Shi
H3C
B. He
CATR
October 20, 2010

EAP Extensions for EAP Re-authentication Protocol (ERP)
draft-ietf-hokey-rfc5296bis-01

Abstract

The Extensible Authentication Protocol (EAP) 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. This document 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.

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 April 23, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction	4
2. Terminology	5
3. ERP Description	6
3.1. ERP With the Home ER Server	9
3.2. ERP with a Local ER Server	10
4. ER Key Hierarchy	12
4.1. rRK Derivation	13
4.2. rRK Properties	14
4.3. rIK Derivation	14
4.4. rIK Properties	15
4.5. rIK Usage	15
4.6. rMSK Derivation	16
4.7. rMSK Properties	16
5. Protocol Details	17
5.1. ERP Bootstrapping	17
5.2. Steps in ERP	20
5.2.1. Multiple Simultaneous Runs of ERP	22
5.2.2. ERP Failure Handling	23
5.3. New EAP Packets	24
5.3.1. EAP-Initiate/Re-auth-Start Packet	25
5.3.1.1. Authenticator Operation	26
5.3.1.2. Peer Operation	26
5.3.2. EAP-Initiate/Re-auth Packet	26
5.3.3. EAP-Finish/Re-auth Packet	28
5.3.4. TV and TLV Attributes	31
5.4. Replay Protection	32
5.5. Channel Binding	32
6. Lower-Layer Considerations	33
7. Transport of ERP Messages	34
8. Security Considerations	35
9. IANA Considerations	39
10. References	39
10.1. Normative References	39
10.2. Informative References	40
Appendix A. Acknowledgments	41
A.1. RFC 5296	41
A.2. RFC 5296bis	41
Appendix B. Example ERP Exchange	42
Authors' Addresses	42

1. Introduction

The Extensible Authentication Protocol (EAP) is a an authentication framework that supports multiple authentication methods. The primary purpose is network access authentication, and a key-generating method is used when the lower layer wants to enforce access control. The EAP keying hierarchy defines two keys to be derived by all key-generating EAP methods: the Master Session Key (MSK) and the Extended MSK (EMSK). In the most common deployment scenario, an EAP peer and an EAP server authenticate each other through a third party known as the EAP authenticator. The EAP authenticator or an entity controlled by the EAP authenticator enforces access control. After successful authentication, the EAP server transports the MSK to the EAP authenticator; the EAP authenticator and the EAP peer establish transient session keys (TSKs) using the MSK as the authentication key, key derivation key, or a key transport key, and use the TSK for per-packet access enforcement.

When a peer moves from one authenticator to another, it is desirable to avoid a full EAP authentication to support fast handovers. The full EAP exchange with another run of the EAP method can take several round trips and significant time to complete, causing delays in handover times. Some EAP methods specify the use of state from the initial authentication to optimize re-authentications by reducing the computational overhead, but method-specific re-authentication takes at least 2 round trips with the original EAP server in most cases (e.g., [RFC4187]). It is also important to note that several methods do not offer support for re-authentication.

Key sharing across authenticators is sometimes used as a practical solution to lower handover times. In that case, compromise of an authenticator results in compromise of keying material established via other authenticators. Other solutions for fast re-authentication exist in the literature [MSKHierarchy].

In conclusion, to achieve low latency handovers, there is a need for a method-independent re-authentication protocol that completes in less than 2 round trips, preferably with a local server. The EAP re-authentication problem statement is described in detail in [RFC5169].

This document specifies EAP Re-authentication Extensions (ERXs) for efficient re-authentication using EAP. The protocol that uses these extensions is itself referred to as the EAP Re-authentication Protocol (ERP). It supports EAP method-independent re-authentication for a peer that has valid, unexpired key material from a previously performed EAP authentication. The protocol and the key hierarchy required for EAP re-authentication are described in this document.

Note that to support ERP, lower-layer specifications may need to be revised to allow carrying EAP messages that have a code value higher than 4 and to accommodate the peer-initiated nature of ERP. Specifically, the IEEE802.1x specification must be revised and RFC 4306 must be updated to carry ERP messages.

2. Terminology

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].

This document uses the basic EAP terminology [RFC3748] and EMSK keying hierarchy terminology [RFC5295]. In addition, this document uses the following terms:

ER Peer - An EAP peer that supports the EAP Re-authentication Protocol. All references to "peer" in this document imply an ER peer, unless specifically noted otherwise.

ER Authenticator - An entity that supports the authenticator functionality for EAP re-authentication described in this document. All references to "authenticator" in this document imply an ER authenticator, unless specifically noted otherwise.

ER Server - An entity that performs the server portion of ERP described here. This entity may or may not be an EAP server. All references to "server" in this document imply an ER server, unless specifically noted otherwise. An ER server is a logical entity; it may not necessarily be co-located with, or physically part of, a full EAP server.

ERX - EAP re-authentication extensions.

ERP - EAP Re-authentication Protocol that uses the re-authentication extensions.

rRK - re-authentication Root Key, derived from the EMSK or DSRK.

rIK - re-authentication Integrity Key, derived from the rRK.

rMSK - re-authentication MSK. This is a per-authenticator key, derived from the rRK.

keyName-NAI - ERP messages are integrity protected with the rIK or the DS-rIK. The use of rIK or DS-rIK for integrity protection of ERP messages is indicated by the EMSKname [RFC5295]; the protocol, which is ERP; and the realm, which indicates the domain name of the ER server. The EMSKname is copied into the username part of the NAI.

Domain - Refers to a "key management domain" as defined in [RFC5295]. For simplicity, it is referred to as "domain" in this document. The terms "home domain" and "local domain" are used to differentiate between the originating key management domain that performs the full EAP exchange with the peer and the local domain to which a peer may be attached at a given time.

3. ERP Description

ERP allows a peer and server to mutually verify proof of possession of keying material from an earlier EAP method run and to establish a security association between the peer and the authenticator. The authenticator acts as a pass-through entity for the Re-authentication Protocol in a manner similar to that of an EAP authenticator described in RFC 3748 [RFC3748]. ERP is a single round-trip exchange between the peer and the server; it is independent of the lower layer and the EAP method used during the full EAP exchange. The ER server may be in the home domain or in the same (visited) domain as the peer and the authenticator (i.e., local domain).

Figure 2 shows the protocol exchange. The first time the peer attaches to any network, it performs a full EAP exchange (shown in Figure 1) with the EAP server; as a result, an MSK is distributed to the EAP authenticator. The MSK is then used by the authenticator and the peer to establish TSKs as needed. At the time of the initial EAP exchange, the peer and the server also derive an EMSK, which is used to derive a re-authentication Root Key (rRK). More precisely, a re-authentication Root Key is derived from the EMSK or from a Domain-Specific Root Key (DSRK), which is itself derived from the EMSK. The rRK is only available to the peer and the ER server and is never handed out to any other entity. Further, a re-authentication Integrity Key (rIK) is derived from the rRK; the peer and the ER server use the rIK to provide proof of possession while performing an ERP exchange. The rIK is also never handed out to any entity and is only available to the peer and server.

EAP Peer =====	EAP Authenticator =====	EAP Server =====
<--- EAP-Request/ ----- Identity		
----- EAP Response/ ---> Identity	---AAA (EAP Response/Identity)-->	
<--- EAP Method -----> exchange	<----- AAA (EAP Method -----> exchange)	
	<----AAA (MSK, EAP-Success)-----	
<---EAP-Success-----		

Figure 1: EAP Authentication

Peer =====	ER Authenticator =====	ER Server =====
[<-- EAP-Initiate/ ----- Re-auth-Start]		
[<-- EAP-Request/ ----- Identity]		
----- EAP-Initiate/ -----> Re-auth/ [Bootstrap]	-----AAA (EAP-Initiate/ -----> Re-auth/ [Bootstrap])	
<--- EAP-Finish/ -----> Re-auth/ [Bootstrap]	<---AAA (rMSK, EAP-Finish/-----> Re-auth/ [Bootstrap])	

Note: [] brackets indicate optionality.

Figure 2: ERP Exchange

Two new EAP codes, EAP-Initiate and EAP-Finish, are specified in this document for the purpose of EAP re-authentication. When the peer identifies a target authenticator that supports EAP re-authentication, it performs an ERP exchange, as shown in Figure 2; the exchange itself may happen when the peer attaches to a new

authenticator supporting EAP re-authentication, or prior to attachment. The peer initiates ERP by itself; it may also do so in response to an EAP-Initiate/Re-auth-Start message from the new authenticator. The EAP-Initiate/Re-auth-Start message allows the authenticator to trigger the ERP exchange. The EAP-Finish message also can be used by the authenticator to announce local domain name.

It is plausible that the authenticator does not know whether the peer supports ERP and whether the peer has performed a full EAP authentication through another authenticator. The authenticator MAY initiate the ERP exchange by sending the EAP-Initiate/Re-auth-Start message, and if there is no response, it will send the EAP-Request/Identity message. Note that this avoids having two EAP messages in flight at the same time [RFC3748]. The authenticator may send the EAP-Initiate/Re-auth-Start message and wait for a short, locally configured amount of time. If the peer does not already know, this message indicates to the peer that the authenticator supports ERP. In response to this trigger from the authenticator, the peer can initiate the ERP exchange by sending an EAP-Initiate/Re-auth message. If there is no response from the peer after the necessary retransmissions (see Section 6), the authenticator MUST initiate EAP by sending an EAP-Request message, typically the EAP-Request/Identity message. Note that the authenticator may receive an EAP-Initiate/Re-auth message after it has sent an EAP-Request/Identity message. If the authenticator supports ERP, it MUST proceed with the ERP exchange. When the EAP-Request/Identity times out, the authenticator MUST NOT close the connection if an ERP exchange is in progress or has already succeeded in establishing a re-authentication MSK.

If the authenticator does not support ERP, it drops EAP-Initiate/Re-auth messages [RFC3748] as the EAP code of those packets is greater than 4. An ERP-capable peer will exhaust the EAP-Initiate/Re-auth message retransmissions and fall back to EAP authentication by responding to EAP Request/Identity messages from the authenticator. If the peer does not support ERP or if it does not have unexpired key material from a previous EAP authentication, it drops EAP-Initiate/Re-auth-Start messages. If there is no response to the EAP-Initiate/Re-auth-Start message, the authenticator SHALL send an EAP Request message (typically EAP Request/Identity) to start EAP authentication. From this stage onwards, RFC 3748 rules apply. Note that this may introduce some delay in starting EAP. In some lower layers, the delay can be minimized or even avoided by the peer initiating EAP by sending messages such as EAPoL-Start in the IEEE 802.1X specification [IEEE_802.1X].

The peer sends an EAP-Initiate/Re-auth message that contains the keyName-NAI to identify the ER server's domain and the rIK used to protect the message, and a sequence number for replay protection.

The EAP-Initiate/Re-auth message is integrity protected with the rIK. The authenticator uses the realm in the keyName-NAI [RFC4282] field to send the message to the appropriate ER server. The server uses the keyName to look up the rIK. The server, after verifying proof of possession of the rIK, and freshness of the message, derives a re-authentication MSK (rMSK) from the rRK using the sequence number as an input to the key derivation. The server updates the expected sequence number to the received sequence number plus one.

In response to the EAP-Initiate/Re-auth message, the server sends an EAP-Finish/Re-auth message; this message is integrity protected with the rIK. The server transports the rMSK along with this message to the authenticator. The rMSK is transported in a manner similar to that of the MSK along with the EAP-Success message in a full EAP exchange. Ongoing work in [RFC5749] describes an additional key distribution protocol that can be used to transport the rRK from an EAP server to one of many different ER servers that share a trust relationship with the EAP server.

The peer MAY request the server for the rMSK lifetime. If so, the ER server sends the rMSK lifetime in the EAP-Finish/Re-auth message.

In an ERP bootstrap exchange, the peer MAY request the server for the rRK lifetime. If so, the ER server sends the rRK lifetime in the EAP-Finish/Re-auth message.

The peer verifies the replay protection and the integrity of the message. It then uses the sequence number in the EAP-Finish/Re-auth message to compute the rMSK. The lower-layer security association protocol is ready to be triggered after this point.

When the ER server is in the home domain, the peer and the server use the rIK and rRK derived from the EMSK; and when the ER server is in the local domain, they use the DS-rIK and DS-rRK corresponding to the local domain. The domain of the ER server is identified by the realm portion of the keyname-NAI in ERP messages.

3.1. ERP With the Home ER Server

If the peer is in the home domain and does not know the domain name (did not receive the domain name through the EAP-Initiate/Re-auth-Start message or via the lower-layer announcement, due to a missed announcement or lack of support for domain name announcements in a specific lower layer) or there is no the local server in the same domain as the peer, it SHOULD initiate ERP bootstrap exchange with the home ER server to obtain the domain name.

The defined ER extensions allow executing the ERP with an ER server

in the home domain. The home ER server may be co-located with a home AAA server. The ERP with the Home ER Server is the similar as ERP exchange described in Figure 2.

Peer =====	ER Authenticator =====	Home ER Server =====
[<-- EAP-Initiate/ ----- Re-auth-Start]		
[<-- EAP-Request/ ----- Identity]		

EAP-Initiate/ ----->		----AAA(EAP-Initiate/ ----->
Re-auth/		Re-auth/
[Bootstrap]		[Bootstrap])
<----		<----AAA(rMSK,EAP-Finish/----->
EAP-Finish/ ----->		Re-auth/
Re-auth/		[Bootstrap])
[Bootstrap]		

Note: [] brackets indicate optionality.

Figure 3: ER ExplicitBootstrapping Exchange/ERP with the Home ER Sever

3.2. ERP with a Local ER Server

The defined ER extensions allow executing the ERP with an ER server in the local domain (access network) if the peer moves out of home domain. The local ER server may be co-located with a local AAA server. The peer may learn about the presence of a local ER server in the network and the local domain name (or ER server name) either via the lower layer or by means of ERP exchange. The peer uses the domain name and the EMSK to compute the DSRK and from that key, the DS-rRK; the peer also uses the domain name in the realm portion of the keyName-NAI for using ERP in the local domain. Figure 4 shows the ER Implicit bootstrapping exchange through local ER Server;Figure 5shows ERP with a local ER server.

Peer	EAP Authenticator /ER Authenticator	Local AAA Agent /Local ER Server	Home EAP Server
====	=====	=====	=====
<-- EAP-Request/ -- Identity			
-- EAP Response/--> Identity	--AAA (EAP Response/--> Identity, [domain name])	--AAA (EAP Response/ --> Identity, [DSRK Request, domain name])	
<----- EAP Method exchange----->			
		<---AAA (MSK, DSRK, ---- EMSKname, EAP-Success)	
	<--- AAA (MSK, ----- EAP-Success)		
<---EAP-Success-----			

Figure 4: Local ERP Exchange, Initial EAP Exchange

Peer	ER Authenticator	Local ER Server
====	=====	=====
[<-- EAP-Initiate/ ----- Re-auth-Start]		
[<-- EAP-Request/ ----- Identity]		
----- EAP-Initiate/ ----->	-----AAA (EAP-Initiate/ ----->	
Re-auth	Re-auth)	
<--- EAP-Finish/ -----	<---AAA (rMSK, EAP-Finish/-----	
Re-auth	Re-auth)	

Figure 5: Local ERP Exchange

As shown in Figure 4, the local ER server may be present in the path of the full EAP exchange (e.g., this may be one of the AAA entities, such as AAA proxies, in the path between the EAP authenticator and the home EAP server of the peer). In that case, the local ER server requests the DSRK by sending the domain name to the home EAP server through AAA message. In response, the home EAP server computes the DSRK by following the procedure specified in [RFC5295] and sends the DSRK and the key name, EMSKname, to the ER server in the claimed domain (i.e., local ER Server). The local domain is responsible for announcing that same domain name via the lower layer to the peer, e.g., DHCP based local domain name discovery specified in [I-D.ietf-hokey-ldn-discovery], or through the EAP-Initiate/Re-auth-Start message during subsequent ERP with local ER server.

After receiving the DSRK and the EMSKname, the local ER server computes the DS-rRK and the DS-rIK from the DSRK as defined in Sections 4.1 and 4.3 below. After receiving the domain name, the peer also derives the DSRK, the DS-rRK, and the DS-rIK. These keys are referred to by a keyName-NAI formed as follows: the username part of the NAI is the EMSKname, the realm portion of the NAI is the domain name. Both parties also maintain a sequence number (initialized to zero) corresponding to the specific keyName-NAI.

Subsequently, when the peer attaches to an authenticator within the local domain, it may perform an ERP exchange with the local ER server to obtain an rMSK for the new authenticator. The ERP with the local ER Server is the similar as ERP exchange described in Figure 2.

4. ER Key Hierarchy

Each time the peer re-authenticates to the network, the peer and the authenticator establish an rMSK. The rMSK serves the same purposes that an MSK, which is the result of full EAP authentication, serves. To prove possession of the rRK, we specify the derivation of another key, the rIK. These keys are derived from the rRK. Together they constitute the ER key hierarchy.

The rRK is derived from either the EMSK or a DSRK as specified in Section 4.1. For the purpose of rRK derivation, this document specifies derivation of a Usage-Specific Root Key (USRK) or a Domain-Specific USRK (DSUSRK) in accordance with [RFC5295] for re-authentication. The USRK designated for re-authentication is the re-authentication root key (rRK). A DSUSRK designated for re-authentication is the DS-rRK available to a local ER server in a particular domain. For simplicity, the keys are referred to without

the DS label in the rest of the document. However, the scope of the various keys is limited to just the respective domains they are derived for, in the case of the domain specific keys. Based on the ER server with which the peer performs the ERP exchange, it knows the corresponding keys that must be used.

The rRK is used to derive an rIK, and rMSKs for one or more authenticators. The figure below shows the key hierarchy with the rRK, rIK, and rMSKs.

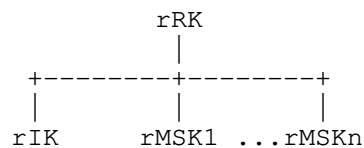


Figure 6: Re-authentication Key Hierarchy

The derivations in this document are according to [RFC5295]. Key derivations and field encodings, where unspecified, default to that document.

4.1. rRK Derivation

The rRK may be derived from the EMSK or DSRK. This section provides the relevant key derivations for that purpose.

The rRK is derived as specified in [RFC5295].

$rRK = KDF(K, S)$, where

$K = EMSK$ or $K = DSRK$ and

$S = rRK \text{ Label} \parallel "\backslash 0" \parallel \text{length}$

The rRK Label is an IANA-assigned 8-bit ASCII string:

EAP Re-authentication Root Key@ietf.org

assigned from the "USRK key labels" name space in accordance with [RFC5295].

The KDF and algorithm agility for the KDF are as defined in [RFC5295].

An rRK derived from the DSRK is referred to as a DS-rRK in the rest of the document. All the key derivation and properties specified in this section remain the same.

4.2. rRK Properties

The rRK has the following properties. These properties apply to the rRK regardless of the parent key used to derive it.

- o The length of the rRK MUST be equal to the length of the parent key used to derive it.
- o The rRK is to be used only as a root key for re-authentication and never used to directly protect any data.
- o The rRK is only used for derivation of rIK and rMSK as specified in this document.
- o The rRK MUST remain on the peer and the server that derived it and MUST NOT be transported to any other entity.
- o The lifetime of the rRK is never greater than that of its parent key. The rRK is expired when the parent key expires and MUST be removed from use at that time.

4.3. rIK Derivation

The re-authentication Integrity Key (rIK) is used for integrity protecting the ERP exchange. This serves as the proof of possession of valid keying material from a previous full EAP exchange by the peer to the server.

The rIK is derived as follows.

$\text{rIK} = \text{KDF}(\text{K}, \text{S})$, where

$\text{K} = \text{rRK}$ and

$\text{S} = \text{rIK Label} \parallel "\backslash 0" \parallel \text{cryptosuite} \parallel \text{length}$

The rIK Label is the 8-bit ASCII string:

Re-authentication Integrity Key@ietf.org

The length field refers to the length of the rIK in octets encoded as specified in [RFC5295].

The cryptosuite and length of the rIK are part of the input to the key derivation function to ensure cryptographic separation of keys if different rIKs of different lengths for use with different Message Authentication Code (MAC) algorithms are derived from the same rRK. The cryptosuite is encoded as an 8-bit number; see Section 5.3.2 for

the cryptosuite specification.

The rIK is referred to by EMSKname-NAI within the context of ERP messages. The username part of EMSKname-NAI is the EMSKname; the realm is the domain name of the ER server. In case of ERP with the home ER server, the peer uses the realm from its original NAI; in case of a local ER server, the peer uses the domain name received at the lower layer or through an ERP bootstrapping exchange.

An rIK derived from a DS-rRK is referred to as a DS-rIK in the rest of the document. All the key derivation and properties specified in this section remain the same.

4.4. rIK Properties

The rIK has the following properties.

- o The length of the rIK MUST be equal to the length of the rRK.
- o The rIK is only used for authentication of the ERP exchange as specified in this document.
- o The rIK MUST NOT be used to derive any other keys.
- o The rIK must remain on the peer and the server and MUST NOT be transported to any other entity.
- o The rIK is cryptographically separate from any other keys derived from the rRK.
- o The lifetime of the rIK is never greater than that of its parent key. The rIK MUST be expired when the EMSK expires and MUST be removed from use at that time.

4.5. rIK Usage

The rIK is the key whose possession is demonstrated by the peer and the ERP server to the other party. The peer demonstrates possession of the rIK by computing the integrity checksum over the EAP-Initiate/Re-auth message. When the peer uses the rIK for the first time, it can choose the integrity algorithm to use with the rIK. The peer and the server MUST use the same integrity algorithm with a given rIK for all ERP messages protected with that key. The peer and the server store the algorithm information after the first use, and they employ the same algorithm for all subsequent uses of that rIK.

If the server's policy does not allow the use of the cryptosuite selected by the peer, the server SHALL reject the EAP-Initiate/

Re-auth message and SHOULD send a list of acceptable cryptosuites in the EAP-Finish/Re-auth message.

The rIK length may be different from the key length required by an integrity algorithm. In case of hash-based MAC algorithms, the key is first hashed to the required key length as specified in [RFC2104]. In case of cipher-based MAC algorithms, if the required key length is less than 32 octets, the rIK is hashed using HMAC-SHA256 and the first k octets of the output are used, where k is the key length required by the algorithm. If the required key length is more than 32 octets, the first k octets of the rIK are used by the cipher-based MAC algorithm.

4.6. rMSK Derivation

The rMSK is derived at the peer and server and delivered to the authenticator. The rMSK is derived following an EAP Re-auth Protocol exchange.

The rMSK is derived as follows.

$\text{rMSK} = \text{KDF}(\text{K}, \text{S})$, where

$\text{K} = \text{rRK}$ and

$\text{S} = \text{rMSK label} \parallel "\backslash 0" \parallel \text{SEQ} \parallel \text{length}$

The rMSK label is the 8-bit ASCII string:

Re-authentication Master Session Key@ietf.org

The length field refers to the length of the rMSK in octets. The length field is encoded as specified in [RFC5295].

SEQ is the sequence number sent by the peer in the EAP-Initiate/Re-auth message. This field is encoded as a 16-bit number in network byte order (see Section 5.3.2).

An rMSK derived from a DS-rRK is referred to as a DS-rIK in the rest of the document. All the key derivation and properties specified in this section remain the same.

4.7. rMSK Properties

The rMSK has the following properties:

- o The length of the rMSK MUST be equal to the length of the rRK.

- o The rMSK is delivered to the authenticator and is used for the same purposes that an MSK is used at an authenticator.
- o The rMSK is cryptographically separate from any other keys derived from the rRK.
- o The lifetime of the rMSK is less than or equal to that of the rRK. It MUST NOT be greater than the lifetime of the rRK.
- o If a new rRK is derived, subsequent rMSKs MUST be derived from the new rRK. Previously delivered rMSKs MAY still be used until the expiry of the lifetime.
- o A given rMSK MUST NOT be shared by multiple authenticators.

5. Protocol Details

5.1. ERP Bootstrapping

We identify two types of bootstrapping for ERP: explicit and implicit bootstrapping. In implicit bootstrapping, the local AAA client or agent supporting EAP re-authentication SHOULD include its domain name and SHOULD request the DSRK from the home AAA server during the initial EAP exchange, in the AAA message encapsulating the first EAP Response message sent by the peer. If such EAP exchange is successful, the home EAP server sends the DSRK for the specified local AAA client or agent (derived using the EMSK and the domain name as specified in [RFC5295]), EMSKname, and DSRK lifetime along with the EAP-Success message. The local AAA client or agent MUST extract the DSRK, EMSKname, and DSRK lifetime (if present) before forwarding the EAP-Success message to the peer, as specified in [I-D.ietf-dime-erp]. Note that the MSK (also present along with the EAP Success message) is extracted by the EAP authenticator as usual. The peer learns the domain name through the EAP-Initiate/Re-auth-Start message, lower-layer announcements [I-D.ietf-hokey-ldn-discovery] or via ER Explicit bootstrapping exchange. When the domain name is available to the peer during or after the full EAP authentication, it attempts to use ERP when it associates with a new authenticator.

If the peer does not know the domain name (did not receive the domain name through the EAP-Initiate/Re-auth-Start message or via the lower-layer announcement, due to a missed announcement or lack of support for domain name announcements in a specific lower layer), it SHOULD initiate Explicit ER bootstrap exchange (ERP exchange with the bootstrap flag turned on) with the ER server in the same (visited) domain as the peer to obtain the local domain name. The peer MAY

also initiate bootstrapping to fetch information such as the rRK lifetime from the AAA server.

The following steps describe the ERP explicit bootstrapping process:

- o The peer sends the EAP-Initiate/Re-auth message with the bootstrapping flag turned on. The bootstrap message is always sent to the ER server, and the keyname-NAI attribute in the bootstrap message is constructed as follows: the username portion of the NAI contains the EMSKname, and the realm portion contains the home domain name.
- o In addition, the message MUST contain a sequence number for replay protection, a cryptosuite, and an integrity checksum. The cryptosuite indicates the authentication algorithm. The integrity checksum indicates that the message originated at the claimed entity, the peer indicated by the Peer-ID, or the rIKname.
- o The peer MAY additionally set the lifetime flag to request the key lifetimes.
- o When an ERP-capable authenticator receives the EAP-Initiate/Re-auth message from a peer, it copies the contents of the keyName-NAI into the User-Name attribute of RADIUS [RFC2865]. The rest of the process is similar to that described in [RFC3579].
- o Upon receipt of an EAP-Initiate/Re-auth message, the server verifies whether the message is fresh or is a replay by evaluating whether the received sequence number is equal to or greater than the expected sequence number for that rIK. The server then verifies to ensure that the cryptosuite used by the peer is acceptable. Next, it verifies the origin authentication of the message by looking up the rIK. If any of the checks fail, the server sends an EAP-Finish/Re-auth message with the Result flag set to '1'. Please refer to Section 5.2.2 for details on failure handling. This error MUST NOT have any correlation to any EAP-Success message that may have been received by the EAP authenticator and the peer earlier. If the EAP-Initiate/Re-auth message is well-formed and valid, the server prepares the EAP-Finish/Re-auth message. The bootstrap flag MUST be set to indicate that this is a bootstrapping exchange. The message contains the following fields:
 - * A sequence number for replay protection.
 - * The same keyName-NAI as in the EAP-Initiate/Re-auth message.

- * If the lifetime flag was set in the EAP-Initiate/Re-auth message, the ER server SHOULD include the rRK lifetime and the rMSK lifetime in the EAP-Finish/Re-auth message. The server may have a local policy for the network to maintain and enforce lifetime unilaterally. In such cases, the server need not respond to the peer's request for the lifetime.
 - * If the bootstrap flag is set, the ER server MUST include the domain name to which the DSRK is being sent along with the EAP-Finish/Re-auth message.
 - * If the ER server verifies the authorization of a local domain server, it MAY include the Authorization Indication TLV to indicate to the peer that the server (that received the DSRK and that is advertising the domain included in the domain name TLV) is authorized.
 - * An authentication tag MUST be included to prove that the EAP-Finish/Re-auth message originates at a server that possesses the rIK corresponding to the EMSKname-NAI.
- o If the ERP exchange is successful, the ER server SHOULD request the DSRK from the home EAP server during the initial EAP exchange as specified in [I-D.ietf-dime-local-keytran], the home EAP server MUST include the DSRK for the local ER server (derived using the EMSK and the domain name as specified in [RFC5295]), EMSKname, and DSRK lifetime along with the EAP-Finish/Re-auth message.
 - o In addition, the rMSK is sent along with the EAP-Finish/Re-auth message, in a AAA attribute [I-D.ietf-dime-erp].
 - o The ER server MUST extract the DSRK, EMSKname, and DSRK lifetime (if present) before forwarding the EAP-Success message to the peer, as specified in [I-D.ietf-dime-erp].
 - o The authenticator receives the rMSK.
 - o When the peer receives an EAP-Finish/Re-auth message with the bootstrap flag set, if a local domain name is present, it MUST use that to derive the appropriate DSRK, DS-rRK, DS-rIK, and keyName-NAI, and initialize the replay counter for the DS-rIK. If not, the peer SHOULD derive the domain-specific keys using the domain name it learned via the lower layer or from the EAP-Initiate/Re-auth-Start message. If the peer does not know the domain name, it must assume that there is no local ER server available.
 - o The peer MAY also verify the Authorization Indication TLV.

- o The procedures for encapsulating the ERP and obtaining relevant keys using Diameter are specified in [I-D.ietf-dime-erp].

Since the ER bootstrapping exchange is typically done immediately following the full EAP exchange, it is feasible that the process is completed through the same entity that served as the EAP authenticator for the full EAP exchange. In this case, the lower layer may already have established TSKs based on the MSK received earlier. The lower layer may then choose to ignore the rMSK that was received with the ER bootstrapping exchange. Alternatively, the lower layer may choose to establish a new TSK using the rMSK. In either case, the authenticator and the peer know which key is used based on whether or not a TSK establishment exchange is initiated. The bootstrapping exchange may also be carried out via a new authenticator, in which case, the rMSK received SHOULD trigger a lower layer TSK establishment exchange.

5.2. Steps in ERP

When a peer that has an active rRK and rIK associates with a new authenticator that supports ERP, it may perform an ERP exchange with that authenticator. ERP is typically a peer-initiated exchange, consisting of an EAP-Initiate/Re-auth and an EAP-Finish/Re-auth message. The ERP exchange may be performed with a local ER server (when one is present) or with the original EAP server.

It is plausible for the network to trigger the EAP re-authentication process, however. An ERP-capable authenticator SHOULD send an EAP-Initiate/Re-auth-Start message to indicate support for ERP. The peer may or may not wait for these messages to arrive to initiate the EAP-Initiate/Re-auth message.

The EAP-Initiate/Re-auth-Start message SHOULD be sent by an ERP-capable authenticator. The authenticator may retransmit it a few times until it receives an EAP-Initiate/Re-auth message in response from the peer. The EAP-Initiate/Re-auth message from the peer may have originated before the peer receives either an EAP-Request/Identity or an EAP-Initiate/Re-auth-Start message from the authenticator. Hence, the Identifier value in the EAP-Initiate/Re-auth message is independent of the Identifier value in the EAP-Initiate/Re-auth-Start or the EAP-Request/Identity messages.

Operational Considerations at the Peer:

ERP requires that the peer maintain retransmission timers for reliable transport of EAP re-authentication messages. The reliability considerations of Section 4.3 of RFC 3748 apply with the peer as the retransmitting entity.

The EAP Re-auth Protocol has the following steps:

The peer sends an EAP-Initiate/Re-auth message. At a minimum, the message SHALL include the following fields:

- a 16-bit sequence number for replay protection

- keyName-NAI as a TLV attribute to identify the rIK used to integrity protect the message.

- cryptosuite to indicate the authentication algorithm used to compute the integrity checksum.

- authentication tag over the message.

When the peer is performing ERP with a local ER server, it MUST use the corresponding DS-rIK it shares with the local ER server. The peer SHOULD set the lifetime flag to request the key lifetimes from the server. The peer can use the rRK lifetime to know when to trigger an EAP method exchange and the rMSK lifetime to know when to trigger another ERP exchange.

The authenticator copies the contents of the value field of the keyName-NAI TLV into the User-Name RADIUS attribute in the AAA message to the ER server.

The server uses the keyName-NAI to look up the rIK. It MUST first verify whether the sequence number is equal to or greater than the expected sequence number. If the server supports a sequence number window size greater than 1, it MUST verify whether the sequence number falls within the window and has not been received before. The server MUST then verify to ensure that the cryptosuite used by the peer is acceptable. The server then proceeds to verify the integrity of the message using the rIK, thereby verifying proof of possession of that key by the peer. If any of these verifications fail, the server MUST send an EAP-Finish/Re-auth message with the Result flag set to '1' (Failure). Please refer to Section 5.2.2 for details on failure handling. Otherwise, it MUST compute an rMSK from the rRK using the sequence number as the additional input to the key derivation.

In response to a well-formed EAP Re-auth/Initiate message, the server MUST send an EAP-Finish/Re-auth message with the following considerations:

- a 16-bit sequence number for replay protection, which MUST be the same as the received sequence number. The local copy of the sequence number MUST be incremented by 1. If the server

supports multiple simultaneous ERP exchanges, it MUST instead update the sequence number window.

keyName-NAI as a TLV attribute to identify the rIK used to integrity protect the message.

cryptosuite to indicate the authentication algorithm used to compute the integrity checksum.

authentication tag over the message.

If the lifetime flag was set in the EAP-Initiate/Re-auth message, the ER server SHOULD include the rRK lifetime and the rMSK lifetime.

The server transports the rMSK along with this message to the authenticator. The rMSK is transported in a manner similar to the MSK transport along with the EAP-Success message in a regular EAP exchange.

The peer looks up the sequence number to verify whether it is expecting an EAP-Finish/Re-auth message with that sequence number protected by the keyName-NAI. It then verifies the integrity of the message. If the verifications fail, the peer logs an error and stops the process; otherwise, it proceeds to the next step.

The peer uses the sequence number to compute the rMSK.

The lower-layer security association protocol can be triggered at this point.

5.2.1. Multiple Simultaneous Runs of ERP

When a peer is within the range of multiple authenticators, it may choose to run ERP via all of them simultaneously to the same ER server. In that case, it is plausible that the ERP messages may arrive out of order, resulting in the ER server rejecting legitimate EAP-Initiate/Re-auth messages.

To facilitate such operation, an ER server MAY allow multiple simultaneous ERP exchanges by accepting all EAP-Initiate/Re-auth messages with SEQ number values within a window of allowed values. Recall that the SEQ number allows replay protection. Replay window maintenance mechanisms are a local matter.

5.2.2. ERP Failure Handling

If the processing of the EAP-Initiate/Re-auth message results in a failure, the ER server MUST send an EAP-Finish Re-auth message with the Result flag set to '1'. If the server has a valid rIK for the peer, it MUST integrity protect the EAP-Finish/Re-auth failure message. If the failure is due to an unacceptable cryptosuite, the server SHOULD send a list of acceptable cryptosuites (in a TLV of Type 5) along with the EAP-Finish/Re-auth message. In this case, the server MUST indicate the cryptosuite used to protect the EAP-Finish/Re-auth message in the cryptosuite. The rIK used with the EAP-Finish/Re-auth message in this case MUST be computed as specified in Section 4.3 using the new cryptosuite. If the server does not have a valid rIK for the peer, the EAP-Finish/Re-auth message indicating a failure will be unauthenticated; the server MAY include a list of acceptable cryptosuites in the message.

The peer, upon receiving an EAP-Finish/Re-auth message with the Result flag set to '1', MUST verify the sequence number and the Authentication Tag to determine the validity of the message. If the peer supports the cryptosuite, it MUST verify the integrity of the received EAP-Finish/Re-auth message. If the EAP-Finish message contains a TLV of Type 5, the peer SHOULD retry the ERP exchange with a cryptosuite picked from the list included by the server. The peer MUST use the appropriate rIK for the subsequent ERP exchange, by computing it with the corresponding cryptosuite, as specified in Section 4.3. If the PRF in the chosen cryptosuite is different from the PRF originally used by the peer, it MUST derive a new DSRK (if required), rRK, and rIK before proceeding with the subsequent ERP exchange.

If the peer cannot verify the integrity of the received message, it MAY choose to retry the ERP exchange with one of the cryptosuites in the TLV of Type 5, after a failure has been clearly determined following the procedure in the next paragraph.

If the replay or integrity checks fail, the failure message may have been sent by an attacker. It may also imply that the server and peer do not support the same cryptosuites; however, the peer cannot determine if that is the case. Hence, the peer SHOULD continue the ERP exchange per the retransmission timers before declaring a failure.

When the peer runs explicit bootstrapping (ERP with the bootstrapping flag on), there may not be a local ER server available to send a DSRK Request and the domain name. In that case, the server cannot send the DSRK and MUST NOT include the domain name TLV. When the peer receives a response in the bootstrapping exchange without a domain

name TLV, it assumes that there is no local ER server. The home ER server sends an rMSK to the ER authenticator, however, and the peer SHALL run the TSK establishment protocol as usual.

5.3. New EAP Packets

Two new EAP Codes are defined for the purpose of ERP: EAP-Initiate and EAP-Finish. The packet format for these messages follows the EAP packet format defined in RFC 3748 [RFC3748].

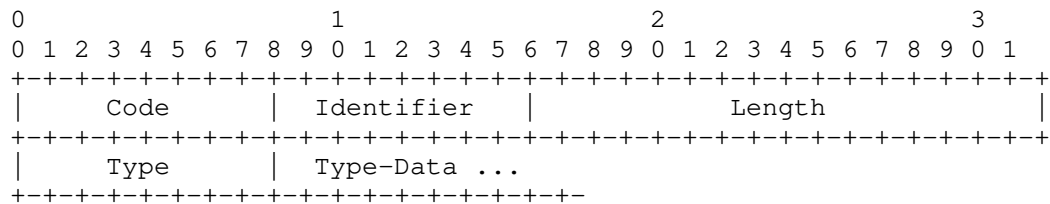


Figure 7: EAP Packet

Code

5 Initiate

6 Finish

Two new code values are defined for the purpose of ERP.

Identifier

The Identifier field is one octet. The Identifier field MUST be the same if an EAP-Initiate packet is retransmitted due to a timeout while waiting for a Finish message. Any new (non-retransmission) Initiate message MUST use a new Identifier field.

The Identifier field of the Finish message MUST match that of the currently outstanding Initiate message. A peer or authenticator receiving a Finish message whose Identifier value does not match that of the currently outstanding Initiate message MUST silently discard the packet.

In order to avoid confusion between new EAP-Initiate messages and retransmissions, the peer must choose an Identifier value that is different from the previous EAP-Initiate message, especially if that exchange has not finished. It is RECOMMENDED that the authenticator clear EAP Re-auth state after 300 seconds.

Type

This field indicates that this is an ERP exchange. Two type values are defined in this document for this purpose -- Re-auth-Start (assigned Type 1) and Re-auth (assigned Type 2).

Type-Data

The Type-Data field varies with the Type of re-authentication packet.

5.3.1. EAP-Initiate/Re-auth-Start Packet

The EAP-Initiate/Re-auth-Start packet contains the parameters shown in Figure 8.

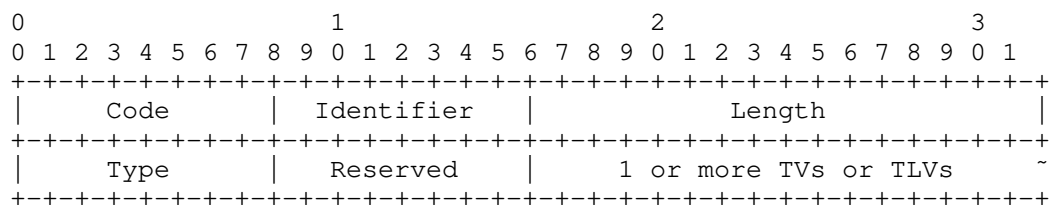


Figure 8: EAP-Initiate/Re-auth-Start Packet

Type = 1.

Reserved, MUST be zero. Set to zero on transmission and ignored on reception.

One or more TVs or TLVs are used to convey information to the peer; for instance, the authenticator may send the domain name to the peer.

TVs or TLVs: In the TV payloads, there is a 1-octet type payload and a value with type-specific length. In the TLV payloads, there is a 1-octet type payload and a 1-octet length payload. The length field indicates the length of the value expressed in number of octets.

Domain-Name: This is a TLV payload. The Type is 4. The domain name is to be used as the realm in an NAI [RFC4282]. The Domain-Name attribute SHOULD be present in an EAP-Initiate/Re-auth-Start message.

In addition, channel binding information MAY be included; see Section 5.5 for discussion. See Figure 12 for parameter specification.

5.3.1.1. Authenticator Operation

The authenticator MAY send the EAP-Initiate/Re-auth-Start message to indicate support for ERP to the peer and to initiate ERP if the peer has already performed full EAP authentication and has unexpired key material. The authenticator SHOULD include the domain name TLV to allow the peer to learn it without lower-layer support or the ERP bootstrapping exchange.

The authenticator MAY include channel binding information so that the peer can send the information to the server in the EAP-Initiate/Re-auth message so that the server can verify whether the authenticator is claiming the same identity to both parties.

The authenticator MAY re-transmit the EAP-Initiate/Re-auth-Start message a few times for reliable transport.

5.3.1.2. Peer Operation

The peer SHOULD send the EAP-Initiate/Re-auth message in response to the EAP-Initiate/Re-auth-Start message from the authenticator. If the peer does not recognize the Initiate code value, it silently discards the message. If the peer has already sent the EAP-Initiate/Re-auth message to begin the ERP exchange, it silently discards the message.

If the EAP-Initiate/Re-auth-Start message contains the domain name, and if the peer does not already have the domain information, the peer SHOULD use the domain name to compute the DSRK and use the corresponding DS-rIK to send an EAP-Initiate/Re-auth message to start an ERP exchange with the local ER server. If there are the local ER server between the peer and the home ER server and the peer has already initiated an ERP exchange with the local ER server, it SHOULD choose to not start an ERP exchange with the home ER server.

5.3.2. EAP-Initiate/Re-auth Packet

The EAP-Initiate/Re-auth packet contains the parameters shown in Figure 9.

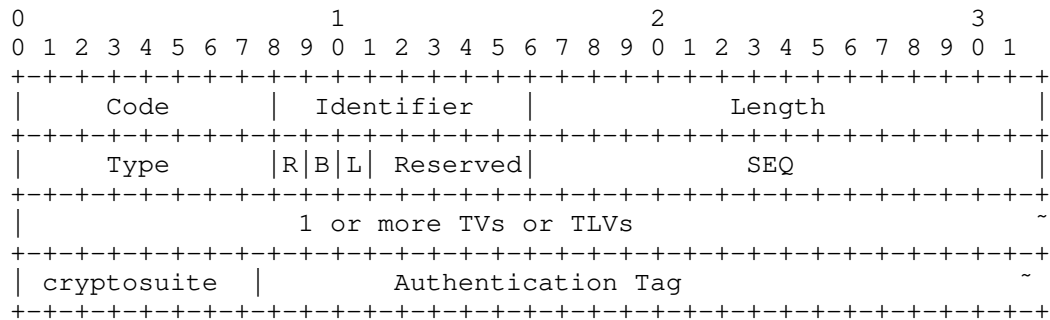


Figure 9: EAP-Initiate/Re-auth Packet

Type = 2.

Flags

'R' - The R flag is set to 0 and ignored upon reception.

'B' - The B flag is used as the bootstrapping flag. If the flag is turned on, the message is a bootstrap message.

'L' - The L flag is used to request the key lifetimes from the server.

The rest of the 5 bits are set to 0 and ignored on reception.

SEQ: A 16-bit sequence number is used for replay protection. The SEQ number field is initialized to 0 every time a new rRK is derived.

TVs or TLVs: In the TV payloads, there is a 1-octet type payload and a value with type-specific length. In the TLV payloads, there is a 1-octet type payload and a 1-octet length payload. The length field indicates the length of the value expressed in number of octets.

keyName-NAI: This is carried in a TLV payload. The Type is 1. The NAI is variable in length, not exceeding 253 octets. The EMSKname is in the username part of the NAI and is encoded in hexadecimal values. The EMSKname is 64 bits in length and so the username portion takes up 128 octets. If the rIK is derived from the EMSK, the realm part of the NAI is the home domain name, and if the rIK is derived from a DSRK, the realm part of the NAI is the domain name used in the derivation of the DSRK. The NAI syntax follows [RFC4282]. Exactly one keyName-NAI attribute SHALL be present in an EAP-Initiate/

Re-auth packet.

In addition, channel binding information MAY be included; see Section 5.5 for discussion. See Figure 12 for parameter specification.

Cryptosuite: This field indicates the integrity algorithm used for ERP. 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 packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

5.3.3. EAP-Finish/Re-auth Packet

The EAP-Finish/Re-auth packet contains the parameters shown in Figure 10.

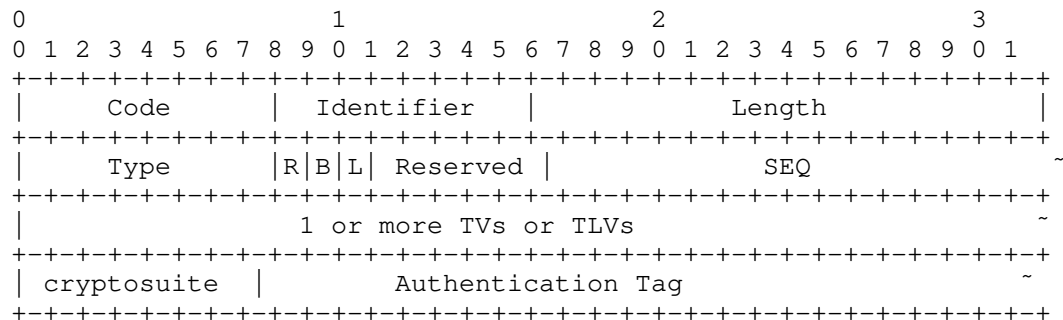


Figure 10: EAP-Finish/Re-auth Packet

Type = 2.

Flags

'R' - The R flag is used as the Result flag. When set to 0, it indicates success, and when set to '1', it indicates a failure.

'B' - The B flag is used as the bootstrapping flag. If the flag is turned on, the message is a bootstrap message.

'L' - The L flag is used to indicate the presence of the rRK lifetime TLV.

The rest of the 5 bits are set to 0 and ignored on reception.

SEQ: A 16-bit sequence number is used for replay protection. The SEQ number field is initialized to 0 every time a new rRK is derived.

TVs or TLVs: In the TV payloads, there is a 1-octet type payload and a value with type-specific length. In the TLV payloads, there is a 1-octet type payload and a 1-octet length payload. The length field indicates the length of the value expressed in number of octets.

keyName-NAI: This is carried in a TLV payload. The Type is 1. The NAI is variable in length, not exceeding 253 octets. EMSKname is in the username part of the NAI and is encoded in hexadecimal values. The EMSKname is 64 bits in length and so the username portion takes up 16 octets. If the rIK is derived from the EMSK, the realm part of the NAI is the home domain name, and if the rIK is derived from a DSRK, the realm part of the NAI is the domain name used in the derivation of the DSRK. The NAI syntax follows [RFC4282]. Exactly one instance of the keyName-NAI attribute SHALL be present in an EAP-Finish/Re-auth message.

rRK Lifetime: This is a TV payload. The Type is 2. The value field is a 32-bit field and contains the lifetime of the rRK in seconds. If the 'L' flag is set, the rRK Lifetime attribute SHOULD be present.

rMSK Lifetime: This is a TV payload. The Type is 3. The value field is a 32-bit field and contains the lifetime of the rMSK in seconds. If the 'L' flag is set, the rMSK Lifetime attribute SHOULD be present.

Domain-Name: This is a TLV payload. The Type is 4. The domain name is to be used as the realm in an NAI [RFC4282]. Domain-Name attribute MUST be present in an EAP-Finish/Re-auth message if the bootstrapping flag is set and if the local ER server sent a DSRK request.

List of cryptosuites: This is a TLV payload. The Type is 5. The value field contains a list of cryptosuites, each of size 1 octet. The cryptosuite values are as specified in Figure 9. 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.

Authorization Indication: This is a TLV payload. The Type is 6. This attribute MAY be included in the EAP-Finish/Re-auth message when a DSRK is delivered to a local ER server and if the home EAP server can verify the authorization of the local ER server to advertise the domain name included in the domain TLV in the same message. The value field in the TLV contains an authentication tag computed over the entire packet, starting from the first bit of the code field to the last bit of the cryptosuite field, with the value field of the Authorization Indication TLV filled with all 0s for the computation. The key used for the computation MUST be derived from the EMSK with key label "DSRK Delivery Authorized Key@ietf.org" and optional data containing an ASCII string representing the key management domain that the DSRK is being derived for.

In addition, channel binding information MAY be included: see Section 5.5 for discussion. See Figure 12 for parameter specification. The server sends this information so that the peer can verify the information seen at the lower layer, if channel binding is to be supported.

Cryptosuite: This field indicates the integrity algorithm and the PRF used for ERP. 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 packet, excluding the authentication tag field itself. The length of the field is indicated by the Cryptosuite.

5.3.4. TV and TLV Attributes

The TV attributes that may be present in the EAP-Initiate or EAP-Finish messages are of the following format:

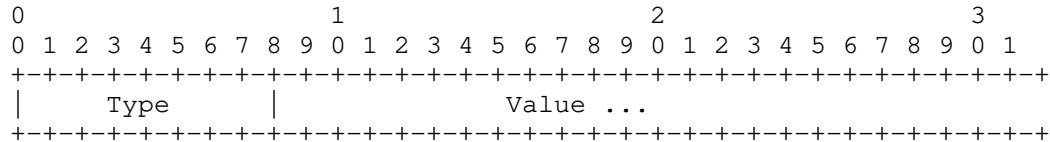


Figure 11: TV Attribute Format

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

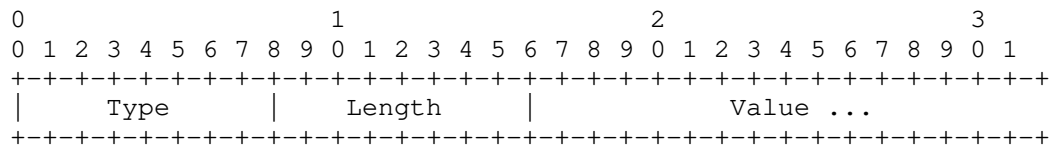


Figure 12: TLV Attribute Format

The following Types are defined in this document:

- '1' - keyName-NAI: This is a TLV payload.
- '2' - rRK Lifetime: This is a TV payload.
- '3' - rMSK Lifetime: This is a TV payload.
- '4' - domain name: This is a TLV payload.
- '5' - cryptosuite list: This is a TLV payload.
- '6' - Authorization Indication: This is a TLV payload.

The TLV type range of 128-191 is reserved to carry channel binding information in the EAP-Initiate and Finish/Re-auth messages. Below are the current assignments (all of them are TLVs):

- '128' - Called-Station-Id [RFC2865]
- '129' - Calling-Station-Id [RFC2865]

- '130' - NAS-Identifier [RFC2865]
- '131' - NAS-IP-Address [RFC2865]
- '132' - NAS-IPv6-Address [RFC3162]

The length field indicates the length of the value part of the attribute in octets.

5.4. Replay Protection

For replay protection, ERP uses sequence numbers. The sequence number is maintained per rIK and is initialized to zero in both directions. In the first EAP-Initiate/Re-auth message, the peer uses the sequence number zero or higher. Note that when the sequence number rotates, the rIK MUST be changed by running EAP authentication. The server expects a sequence number of zero or higher. When the server receives an EAP-Initiate/Re-auth message, it uses the same sequence number in the EAP-Finish/Re-auth message. The server then sets the expected sequence number to the received sequence number plus 1. The server accepts sequence numbers greater than or equal to the expected sequence number.

If the peer sends an EAP-Initiate/Re-auth message, but does not receive a response, it retransmits the request (with no changes to the message itself) a pre-configured number of times before giving up. However, it is plausible that the server itself may have responded to the message and it was lost in transit. Thus, the peer MUST increment the sequence number and use the new sequence number to send subsequent EAP re-authentication messages. The peer SHOULD increment the sequence number by 1; however, it may choose to increment by a larger number. When the sequence number rotates, the peer MUST run full EAP authentication.

5.5. Channel Binding

ERP provides a protected facility to carry channel binding (CB) information, according to the guidelines in Section 7.15 of [RFC3748]. The TLV type range of 128-191 is reserved to carry CB information in the EAP-Initiate/Re-auth and EAP-Finish/Re-auth messages. Called-Station-Id, Calling-Station-Id, NAS-Identifier, NAS-IP-Address, and NAS-IPv6-Address are some examples of channel binding information listed in RFC 3748, and they are assigned values 128-132. Additional values are IANA managed based on IETF Consensus [RFC5226].

The authenticator MAY provide CB information to the peer via the EAP-Initiate/Re-auth-Start message. The peer sends the information to

the server in the EAP-Initiate/Re-auth message; the server verifies whether the authenticator identity available via AAA attributes is the same as the identity provided to the peer.

If the peer does not include the CB information in the EAP-Initiate/Re-auth message, and if the local ER server's policy requires channel binding support, it SHALL send the CB attributes for the peer's verification. The peer attempts to verify the CB information if the authenticator has sent the CB parameters, and it proceeds with the lower-layer security association establishment if the attributes match. Otherwise, the peer SHALL NOT proceed with the lower-layer security association establishment.

6. Lower-Layer Considerations

The authenticator is responsible for retransmission of EAP-Initiate/Re-auth-Start messages. The authenticator MAY retransmit the message a few times or until it receives an EAP-Initiate/Re-auth message from the peer. The authenticator may not know whether the peer supports ERP; in those cases, the peer may be silently dropping the EAP-Initiate/Re-auth-Start packets. Thus, retransmission of these packets should be kept to a minimum. The exact number is up to each lower layer.

The Identifier value in the EAP-Initiate/Re-auth packet is independent of the Identifier value in the EAP-Initiate/Re-auth-Start packet.

The peer is responsible for retransmission of EAP-Initiate/Re-auth messages.

Retransmitted packets MUST be sent with the same Identifier value in order to distinguish them from new packets. By default, where the EAP-Initiate message is sent over an unreliable lower layer, the retransmission timer SHOULD be dynamically estimated. A maximum of 3-5 retransmissions is suggested (this is based on the recommendation of [RFC3748]). Where the EAP-Initiate message is sent over a reliable lower layer, the retransmission timer SHOULD be set to an infinite value, so that retransmissions do not occur at the EAP layer. Please refer to RFC 3748 [RFC3748] for additional guidance on setting timers.

The Identifier value in the EAP-Finish/Re-auth packet is the same as the Identifier value in the EAP-Initiate/Re-auth packet.

If an authenticator receives a valid duplicate EAP-Initiate/Re-auth message for which it has already sent an EAP-Finish/Re-auth message,

it MUST resend the EAP-Finish/Re-auth message without reprocessing the EAP-Initiate/Re-auth message. To facilitate this, the authenticator SHALL store a copy of the EAP-Finish/Re-auth message for a finite amount of time. The actual value of time is a local matter; this specification recommends a value of 100 milliseconds.

The lower layer may provide facilities for exchanging information between the peer and the authenticator about support for ERP, for the authenticator to send the domain name information and channel binding information to the peer

Note that to support ERP, lower-layer specifications may need to be revised. Specifically, the IEEE802.1x specification must be revised to allow carrying EAP messages of the new codes defined in this document in order to support ERP. Similarly, RFC 4306 must be updated to include EAP code values higher than 4 in order to use ERP with Internet Key Exchange Protocol version 2 (IKEv2). IKEv2 may also be updated to support peer-initiated ERP for optimized operation. Other lower layers may need similar revisions.

Our analysis indicates that some EAP implementations are not RFC 3748 compliant in that instead of silently dropping EAP packets with code values higher than 4, they may consider it an error. To accommodate such non-compliant EAP implementations, additional guidance has been provided below. Furthermore, it may not be easy to upgrade all the peers in some cases. In such cases, authenticators may be configured to not send EAP-Initiate/Re-auth-Start; peers may learn whether an authenticator supports ERP via configuration, from advertisements at the lower layer.

In order to accommodate implementations that are not compliant to RFC 3748, such lower layers SHOULD ensure that both parties support ERP; this is trivial for an instance when using a lower layer that is known to always support ERP. For lower layers where ERP support is not guaranteed, ERP support may be indicated through signaling (e.g., piggy-backed on a beacon) or through negotiation. Alternatively, clients may recognize environments where ERP is available based on pre-configuration. Other similar mechanisms may also be used. When ERP support cannot be verified, lower layers may mandate falling back to full EAP authentication to accommodate EAP implementations that are not compliant to RFC 3748.

7. Transport of ERP Messages

AAA Transport of ERP messages is specified in [RFC5749] and [I-D.ietf-dime-erp].

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

The EAP Re-auth Protocol satisfies this requirement. The algorithm chosen by the peer for the MAC generation 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. Algorithm agility for the KDF is specified in [RFC5295]. Only when the algorithms used are acceptable, the server proceeds with derivation of keys and verification of the proof of possession of relevant keying material by the peer. A full-blown negotiation of algorithms cannot be provided in a single round trip protocol. Hence, while the protocol provides algorithm agility, it does not provide true negotiation.

Strong, fresh session keys

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

Limit key scope

The scope of all the keys derived by ERP is well defined. The rRK and rIK are never shared with any entity and always remain on the peer and the server. The rMSK is provided only to the authenticator through which the peer performs the ERP exchange. No other authenticator is authorized to use that rMSK.

Replay detection mechanism

For replay protection of ERP messages, a sequence number associated with the rIK is used. The sequence number is maintained by the peer and the server, and initialized to zero when the rIK is generated. The peer increments the sequence number by one after it sends an ERP message. The server sets the expected sequence number to the received sequence number plus one after verifying the validity of the received message and responds to the message.

Authenticate all parties

The EAP Re-auth Protocol provides mutual authentication of the peer and the server. Both parties need to possess the keying material that resulted from a previous EAP exchange in order to successfully derive the required keys. Also, both the EAP re-authentication Response and the EAP re-authentication Information messages are integrity protected so that the peer and the server can verify each other. When the ERP exchange is executed with a local ER server, the peer and the local server mutually authenticate each other via that exchange in the same manner. The peer and the authenticator authenticate each other in the secure association protocol executed by the lower layer, just as in the case of a regular EAP exchange.

Peer and authenticator authorization

The peer and authenticator demonstrate possession of the same key material without disclosing it, as part of the lower-layer secure association protocol. Channel binding with ERP may be used to verify consistency of the identities exchanged, when the identities used in the lower layer differ from that exchanged within the AAA protocol.

Keying material confidentiality

The peer and the server derive the keys independently using parameters known to each entity. The AAA server sends the DSRK of a domain to the corresponding local ER server via the AAA protocol. Likewise, the ER server sends the rMSK to the authenticator via the AAA protocol.

Note that compromise of the DSRK results in compromise of all keys derived from it. Moreover, there is no forward secrecy within ERP. Thus, compromise of an DSRK retroactively compromises all ERP keys.

It is RECOMMENDED that the AAA protocol be protected using IPsec or TLS so that the keys are protected in transit. Note, however, that keys may be exposed to AAA proxies along the way and compromise of any of those proxies may result in compromise of keys being transported through them.

The home EAP server MUST NOT hand out a given DSRK to a local domain server more than once, unless it can verify that the entity receiving the DSRK after the first time is the same as that received the DSRK originally. If the home EAP server verifies authorization of a local domain server, it MAY hand

out the DSRK to that domain more than once. In this case, the home EAP server includes the Authorization Indication TLV to assure the peer that DSRK delivery is secure.

Confirm cryptosuite selection

Crypto algorithms for integrity and key derivation in the context of ERP MAY be the same as that used by the EAP method. In that case, the EAP method is responsible for confirming the cryptosuite selection. Furthermore, the cryptosuite is included in the ERP exchange by the peer and confirmed by the server. The protocol allows the server to reject the cryptosuite selected by the peer and provide alternatives. When a suitable rIK is not available for the peer, the alternatives may be sent in an unprotected fashion. The peer is allowed to retry the exchange using one of the allowed cryptosuites. However, in this case, any en route modifications to the list sent by the server will go undetected. If the server does have an rIK available for the peer, the list will be provided in a protected manner and this issue does not apply.

Uniquely named keys

All keys produced within the ERP context can be referred to uniquely as specified in this document. Also, the key names do not reveal any part of the keying material.

Prevent the domino effect

The compromise of one peer does not result in the compromise of keying material held by any other peer in the system. Also, the rMSK is meant for a single authenticator and is not shared with any other authenticator. Hence, the compromise of one authenticator does not lead to the compromise of sessions or keys held by any other authenticator in the system. Hence, the EAP Re-auth Protocol allows prevention of the domino effect by appropriately defining key scope.

However, if keys are transported using hop-by-hop protection, compromise of a proxy may result in compromise of key material, i.e., the DSRK being sent to a local ER server.

Bind key to its context

All the keys derived for ERP are bound to the appropriate context using appropriate key labels. Lifetime of a child key is less than or equal to that of its parent key as specified in

RFC 4962 [RFC4962]. The key usage, lifetime and the parties that have access to the keys are specified.

Confidentiality of identity

Deployments where privacy is a concern may find the use of rIKname-NAI to route ERP messages serves their privacy requirements. Note that it is plausible to associate multiple runs of ERP messages since the rIKname is not changed as part of the ERP protocol. There was no consensus for that requirement at the time of development of this specification. If the rIKname is not used and the Peer-ID is used instead, the ERP exchange will reveal the Peer-ID over the wire.

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. All the keys specified in this document are meant for use in ERP only. Any other restrictions of session keys may be imposed by the specific lower layer and are out of scope for this specification.

A denial-of-service (DoS) attack on the peer may be possible when using the EAP Initiate/Re-auth message. An attacker may send a bogus EAP-Initiate/Re-auth message, which may be carried by the authenticator in a RADIUS-Access-Request to the server; in response, the server may send an EAP-Finish/Re-auth with Failure indication in a RADIUS Access-Reject message. Note that such attacks may be plausible with the EAPoL-Start capability of IEEE 802.11 and other similar facilities in other link layers and where the peer can initiate EAP authentication. An attacker may use such messages to start an EAP method run, which fails and may result in the server sending a RADIUS Access-Reject message, thus resulting in the link-layer connections being terminated.

To prevent such DoS attacks, an ERP failure should not result in deletion of any authorization state established by a full EAP exchange. Alternatively, the lower layers and AAA protocols may define mechanisms to allow two link-layer security associations (SAs) derived from different EAP keying materials for the same peer to exist so that smooth migration from the current link layer SA to the new one is possible during rekey. These mechanisms prevent the link layer connections from being terminated when a re-authentication procedure fails due to the bogus EAP-Initiate/Re-auth message.

When a DSRK is sent from a home EAP server to a local domain server

or when a rMSK is sent from an ER server to an authenticator, in the absence of end-to-end security between the entity that is sending the key and the entity receiving the key, it is plausible for other entities to get access to keys being sent to an ER server in another domain. This mode of key transport is similar to that of MSK transport in the context of EAP authentication. We further observe that ERP is for access authentication and does not support end-to-end data security. In typical implementations, the traffic is in the clear beyond the access control enforcement point (the authenticator or an entity delegated by the authenticator for access control enforcement). The model works as long as entities in the middle of the network do not use keys intended for other parties to steal service from an access network. If that is not achievable, key delivery must be protected in an end-to-end manner.

9. IANA Considerations

This document has no IANA actions; all values referenced in this document were previously assigned in RFC 5296 [RFC5296].

10. References

10.1. Normative References

- [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
- [RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.
- [RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", RFC 5295, August 2008.

10.2. Informative References

- [I-D.ietf-dime-erp]
Bournelle, J., Morand, L., Wu, W., and G. Zorn, "Diameter Support for the EAP Re-authentication Protocol (ERP)", draft-ietf-dime-erp-04 (work in progress), September 2010.
- [I-D.ietf-dime-local-keytran]
, Q. and G. , "Diameter Attribute-Value Pairs for Cryptographic Key Transport", draft-ietf-dime-local-keytran-07 (work in progress), July 2010.
- [I-D.ietf-hokey-ldn-discovery]
Zorn, G., Wu, Q., and Y. Wang, "The Local Domain Name DHCPv6 Option", draft-ietf-hokey-ldn-discovery-05 (work in progress), September 2010.
- [IEEE_802.1X]
Institute of Electrical and Electronics Engineers, "IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004", December 2004.
- [MSKHierarchy]
Lopez, R., Skarmeta, A., Bournelle, J., Laurent-Maknavicus, M., and J. Combes, "Improved EAP keying framework for a secure mobility access service", IWCMC '06, Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, New York, NY, USA, 2006.
- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
- [RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.
- [RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.
- [RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.
- [RFC4962] Housley, R. and B. Aboba, "Guidance for Authentication,

Authorization, and Accounting (AAA) Key Management",
BCP 132, RFC 4962, July 2007.

- [RFC5169] Clancy, T., Nakhjiri, M., Narayanan, V., and L. Dondeti, "Handover Key Management and Re-Authentication Problem Statement", RFC 5169, March 2008.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
- [RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", RFC 5296, August 2008.
- [RFC5749] Hoeper, K., Nakhjiri, M., and Y. Ohba, "Distribution of EAP-Based Keys for Handover and Re-Authentication", RFC 5749, March 2010.

Appendix A. Acknowledgments

A.1. RFC 5296

In writing this document, we benefited from discussing the problem space and the protocol itself with a number of folks including Bernard Aboba, Jari Arkko, Sam Hartman, Russ Housley, Joe Salowey, Jesse Walker, Charles Clancy, Michaela Vanderveen, Kedar Gaonkar, Parag Agashe, Dinesh Dharmaraju, Pasi Eronen, Dan Harkins, Yoshi Ohba, Glen Zorn, Alan DeKok, Katrin Hoeper, and other participants of the HOKEY working group. The credit for the idea to use EAP-Initiate/Re-auth-Start goes to Charles Clancy, and the multiple link-layer SAs idea to mitigate the DoS attack goes to Yoshi Ohba. Katrin Hoeper suggested the use of the windowing technique to handle multiple simultaneous ER exchanges. Many thanks to Pasi Eronen for the suggestion to use hexadecimal encoding for rIKname when sent as part of keyName-NAI field. Thanks to Bernard Aboba for suggestions in clarifying the EAP lock-step operation, and Joe Salowey and Glen Zorn for help in specifying AAA transport of ERP messages. Thanks to Sam Hartman for the DSRK Authorization Indication mechanism.

A.2. RFC 5296bis

Glen Zorn wrote the initial draft for this document and provided useful reviews. Many thanks to him.

Appendix B. Example ERP Exchange

- 0. Authenticator --> Peer: [EAP-Initiate/Re-auth-Start]
 - 1. Peer --> Authenticator: EAP Initiate/Re-auth (SEQ, keyName-NAI, cryptosuite, Auth-tag*)
 - 1a. Authenticator --> Re-auth-Server: AAA-Request{Authenticator-Id, EAP Initiate/Re-auth (SEQ, keyName-NAI, cryptosuite, Auth-tag*)}
 - 2. ER-Server --> Authenticator: AAA-Response{rMSK, EAP-Finish/Re-auth (SEQ, keyName-NAI, cryptosuite, [CB-Info], Auth-tag*)}
 - 2b. Authenticator --> Peer: EAP-Finish/Re-auth (SEQ, keyName-NAI, cryptosuite, [CB-Info], Auth-tag*)
- * Auth-tag computation is over the entire EAP Initiate/Finish message; the code values for Initiate and Finish are different and thus reflection attacks are mitigated.

Authors' Addresses

Qin Wu (editor)
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, JiangSu 210012
China

Email: Sunseawq@huawei.com

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

Email: caozhen@chinamobile.com

Yang Shi
H3C Tech. Co., Ltd
Digital Technology Plaza, NO.9 Shangdi 9th Street, Haidian District
Beijing 100085
China

Email: young@h3c.com

Baohong He
China

Email: hebaohong@catr.cn

