The interworking between IKEv2 and PMIPv6

draft-zhu-netext-ikev2-interworking-pmip-00.txt

Abstract

During the network operation, there is a scenario where the IKEv2 is used between MN and MAG while the PMIPv6 is used between MAG and LMA. Hence, the interworking between IKEv2 and PMIPv6 need to be considered in this scenario.

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 October 8, 2011.

Copyright Notice

Copyright (c) 2011 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. Motivation ................................................. 3
2. Protocol Overview ...................................... 4
3. New Mobility Option-IKEv2 Container ...................... 6
4. MAG Operation ........................................... 7
5. LMA Operation ........................................... 8
6. Security Considerations .................................. 9
7. IANA Considerations .................................... 10
8. Normative References ................................... 11
Authors’ Addresses .......................................... 12
1. Motivation

Non-transparent access is supported in UMTS since Release 99 and in Rel-8 it was naturally extended to the EPS with 3GPP access. In both UMTS and EPS, the credentials for PAP or CHAP authentication with the private Packet Data Network (PDN) are carried transparently between the UE and the GGSN/PGW inside the Protocol Configuration Options (PCO) information element. In I-WLAN it is possible to access a private PDN via a Packet Data Gateway (PDG) as defined in 3GPP TS 29.161. The approach specified in 3GPP TS 29.161 relies on multiple IKEv2 authentication exchanges, based on rfc4739.

However, access to private PDNs is still not possible via untrusted non-3GPP IP access, e.g. WLAN access with PMIPv6-based interface. Since the ePDG (i.e. MAG, contrary to the PDG in I-WLAN) has no RADIUS or Diameter interface with the AAA server in the private network, even according to rfc4739 the ePDG is not able to contact the AAA Server for the external authentication and authorization after receiving the credentials.

This document attempts to figure out the issue described above via extending PMIPv6 to achieve external authentication and authorization between UE and the AAA server.
2. Protocol Overview

It is proposed to define a new mobility option as a container (IKEv2 container) in Proxy Binding Update and Proxy Binding Acknowledge, which can be used to convey the information from IKEv2 and the result of external authentication and authorization.

The following steps is performed during the external authentication and authorization as described in Figure 1.

```
+-------+       +---------+                 +--------+      +-----------+
|  MN   |       |   MAG   |                 |  LMA   |      | External  |
+-------+       +---------+                 +--------+      | AAA Server |
                  |                         |          +-----------+
|                  |                         |                 |
|                  |                         |                 |
|                  |<-4.PBA(IKEv2 Container)-|                 |
|                  |                         |                 |
|                  |                  |3.Access-Req/Resp|
|                  |                  |<---------------->|
|                  |                  |                 |
|                  |                  |<-4.PBA(IKEv2 Container)-|
|                  |                  |                 |
|                  |                  |                 |
|                  |                  |                 |
|                  |                  |                 |
Figure 1: Authentication and authorization for the Private network access

The steps of the procedure in Figure 1 are as following.

1. The mobile node performs additional authentication and authorization with an external AAA Server as specified in rfc4739

2. The MAG constructs the IKEv2 container (e.g. PCO) in the Proxy Binding Update, copies the information from IKEv2 (e.g. User ID and password) into the IKEv2 container and sends the PBU to the LMA.
3. The LMA uses the authentication credentials provided in the IKEv2 container to perform an additional authentication and authorisation with an external AAA server.

4. Upon receiving the access response from external AAA server the LMA copies the results from the response message to the IKEv2 container which is included in the Proxy Binding Acknowledge.

5. Upon receiving credentials in the Proxy Binding Acknowledge the MAG performs the procedure as described in rfc4739 to complete the external Authentication/Authorization.
3. New Mobility Option-IKEv2 Container

TBD
4. MAG Operation

TBD
5. LMA Operation

TBD
6. Security Considerations

TBD
7. IANA Considerations

TBD
8. Normative References

Authors’ Addresses

Chunhui Zhu
ZTE Corporation
No.50 Ruanjiandadao Rd,Yuhuatai District
Nanjing
China
Email: zhu.chunhui@zte.com.cn

Xingyue Zhou
ZTE Corporation
No.50 Ruanjiandadao Rd,Yuhuatai District
Nanjing
China
Phone: +86-25-8801-4634
Email: zhou.xingyue@zte.com.cn