Diameter Maintanence and
Extensions (DIME)
Internet-Draft
Expires: September 7, 2006

H. Tschofenig
Siemens
T. Tsenov

G. Giaretta
TILab
J. Bournelle
GET/INT

March 6, 2006

Mobile IPv6 Bootstrapping using Diameter in the Split Scenario
draft-tschofenig-dime-mip6-split-01.txt

Status of this Memo

Copyright Notice

Abstract

In Mobile IPv6 deployment a need for an interaction between the Home Agent, the AAA infrastructure of the Mobile Service Provider (MSP) and the Mobility Service Authorizer (MSA) has been identified. This

document provides a description of the functionality that allows to meet the goals outlined in the MIPv6 AAA Goals document.

Table of Contents

1. Introduction

In Mobile IPv6 deployment, authentication, authorization and accounting issues in the protocol operations are approached by using the AAA infrastructure. The [8] document presents a number of bootstrapping scenarios using the HA-AAA interface and defines a list of requirements that this interface should cover. This document deals with the functional capabilities of the Diameter protocol as a AAA protocol applicable for the split scenario.

Currently, two Mobile IPv6 bootstrapping solutions exist. In the split scenario, only a HA-AAA interface is considered whereas in the integrated scenario both NAS-AAA and HA-AAA interface need to be addressed.

This document focuses only on the split scenario. A separate document describes a Diameter application for bootstrapping MIPv6 for the integrated scenario.

2. Motivation

Designed to cover network access requirements for AAA protocols [1], Diameter protocol provides a framework for applications offering AAA services. This design approach gives to the protocol extensibility, interoperability and flexibility in offering AAA solutions in comparison to other AAA protocols. Support of definition of new application Ids, commands and AVPs provides extensibility. Recommended re-use of commands and AVPs and careful consideration of the level of AVP's support provides interoperability. Usage of IPsec and TLS for transport hop-by-hop security, possible support for AVP integrity and confidentiality and usage of peer-to-peer model (any Diameter node can initiate a request message) provide flexibility of the Diameter AAA applications to fit to specific requirements.

In the following sections we try to specify by which means a possible Diameter application would cover the requirements for the HA-AAA interface specified in [8].

3. Bootstrapping Mobile IPv6 in the Split Scenario

In the split scenario for bootstrapping Mobile IPv6 [2], the MN discovers HA through DNS mechanism. Then it uses IKEv2 [3] to setup IPsec SAs. IKEv2 supports EAP to authenticate the Initiator and thus the MN. As such, the MN can use its credentials (obtained from the MSA) to be authenticated for the IPv6 mobility service. The HA MAY rely on a EAP server co-located on a AAA server for this purpose. In this case, a HA-AAA interface is needed. This interface MUST support transport of EAP packets.

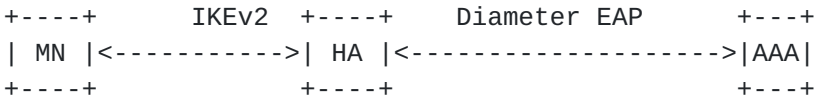

Figure 1: Diameter EAP as the HA-AAA interface in Split scenario

For this purpose, the HA can use Diameter EAP Application [4] (cf. Figure 1). As shown in the previous section, this protocol fulfill goals described in [8]

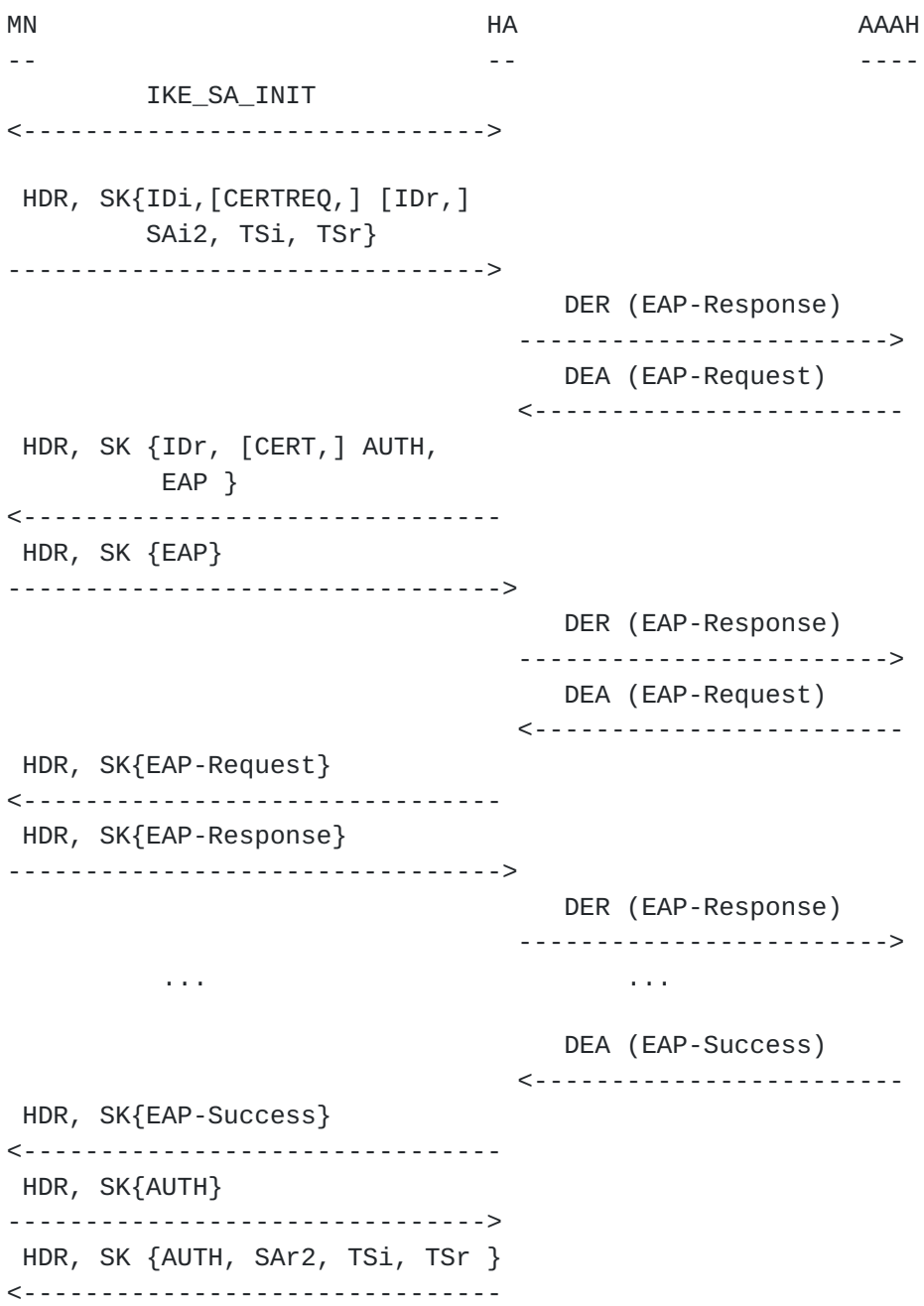

Figure 2: IKEv2 Diameter EAP

MN and HA start with an IKE_SA_INIT to setup the IKE SA. The MN indicates its desire to use EAP by not including the AUTH payload in the third message. However it indicates its identity (e.g. NAI) by using the IDi field. If the HA supports EAP for authentication, it forwards the identity to the AAAH by sending a Diameter-EAP-Request (DER) message containing the identity in the EAP-Payload AVP and in the User-Name AVP. Based on this identity, the AAAH chooses an

authentication method and sends the first EAP-Request in the Diameter-EAP-Answer message. During the EAP authentication phase, the HA relays EAP packets between the MN and the AAAH. If the authentication succeeds and if the MN is authorized to use Mobile IPv6 service, the AAAH sends a DEA message containing the EAP-success and the AAA-Key derived from the EAP authentication method . Note that EAP authentication methods that do not derive keys are not recommended. This key is used by both MN and HA to generate the AUTH payload. In the latter message, MN and HA finish to setup IPsec SAs for Mobile IPv6.

4. Goals

In presentation of the analysis of goals and possible design solutions by Diameter we follow the classification, labels and naming assigned in the document [8], where these goals are identified. Since several of the issues might be addressed in similar way or by similar Diameter functionality, we have grouped these issues and have given a general description of the groups.

4.1. General goals

4.1.1. G1.1 - G1.4 Security

As design goals for an AAA interface, G1.1 - G1.4 goals specify standard requirements for a AAA protocol - mutual authentication of the peers, integrity, replay protection and confidentiality. IPsec or TLS provide the hop-by-hop security. Combined, they SHOULD be able to provide the range of security services required for the HA-AAA interface.

4.1.2. Dead peer detection - the HA-AAA interface SHOULD support inactive peer detection.

Two possible approaches might be considered here:

- AAAH server and Home Agent establish a transport connection between each other. In this case Diameter heartbeat messages called Device-Watchdog-Request/Answer [1], which are exchanged over this connection to test for its aliveness, MAY be used to detect inactivity in any of the two Diameter peers.

- AAAH server and Home Agent do not have transport connection. In this case inactive peer detection functionality SHOULD be provided into the Diameter session - service stateless Diameter sessions might be established between the AAAH server and the range of MSP's Home Agents for detecting HAs availability.

4.2. Service Authorization

4.2.1. G2.1. The HA-AAA interface SHOULD allow the use of Network Access Identifier (NAI) to identify the mobile node.

Identification by User-Name AVP [1], which has a format consistent with the NAI specifications, is common for Diameter applications. Diameter provides functionality for routing of Diameter requests based on the information included in the User-Name AVP.

4.2.2. G2.2. The HA SHOULD be able to query the AAAH server to verify Mobile IPv6 service authorization for the mobile node.

Based on the peer-to-peer model, Diameter design gives the functionality that any Diameter node can initiate a request message. This, combined with the support of EAP, would provide flexible solutions for this issue. Currently several Diameter application standardized or under work-in-progress address different types of authorization - network access [5], credit control [9], quality of service [10]. This might allow re-use of present AVPs over the AAAH-HA interface.

4.2.3. G2.3. The AAAH server SHOULD be able to enforce explicit operational limitations and authorization restrictions on the HA.(e.g. packet filters, QoS parameters).

Several present Diameter applications, standardized or under work-in-progress address an operation and authorization control over specific services and have defined appropriate AVPs. NAS-Filter-Rule AVP, defined by Diameter NASREQ application [5], provides IP packet filter description. QoS-Filter-Rule AVP defined by Diameter NASREQ application and QSPEC AVP defined by Diameter QoS Authorization [10] provide QoS parameter description. Credit Control application [9] provides cost control over requested services. AVPs MAY be re-used for providing required functionality over the AAAH-HA interface. This, combined with the possibility that any node can initiate request message, gives control to the AAAH server over HA's functionality.

4.2.4. G2.4 - G2.6. Issues addressing the maintenance of a Mobile IPv6 session by the AAAH server, e.g. authorization lifetime,

extension of the authorization lifetime and explicit session termination by the AAAH server side.

Diameter base protocol provides a powerful set of commands and AVPs for management of the authorization and accounting sessions. A number of AVPs (Auth-Lifetime-AVP, Grace-Period-AVP, Session-Timeout-AVP) handle the duration (in time) of an authorization session [1]. Additional AVPs for measuring the authorization duration in units different that time are specified too [9]. Exchanging of application specific authorization request/answer messages provides extension of the authorization session. Initiation of the re-authorization by both sides could be supported. Both sides could initiate session termination, by using Diameter Session Termination and Abort Session messages.

All these are applied to the Diameter session used for authorization of a Mobile IPv6 session and need to be applied appropriately to this

Mobile IPv6 session too.

4.3. Accounting - G3.1. The HA-AAA interface MUST support the transfer of accounting records needed for service control and charging

Diameter accounting protocol provides a variety of options - real-time accounting, event/session-type accounting records, fault resilience, correlation of accounting records. Requirements for the accounting services over AAAH-HA interface are standard. Definition or re-used of AVPs for the specific accounting records combined with the functionality of the Diameter accounting protocol SHOULD provide desired accounting services.

4.4. Mobile Node Authentication (G4.1.)

These issues require the functionality of AAAH server working as a back-end authentication server and HA working as NAS and EAP authenticator in pass-through mode for providing a mobile node authentication. These functionalities are provided by Diameter NASREQ and EAP applications, and might be re-used at the AAAH-AH interface.[5], [4]

4.5. Provisioning of Configuration Parameters

Several AVPs could be re-used for carrying the home address of the NM to the AAAH server. Framed-IPv6-Prefix AVP in conjunction with Framed-Interface-Id AVP, Framed-IPv6-Route AVP or Login-IPv6-Host AVP defined by NASREQ might be used for home address communication to the AAAH [4].

Even if not explicitly mentioned as goal the AAAH server needs in some cases the FQDN from the MN if he should do an DNS update of his behalf. The MN FQDN could be delivered during the IKEv2 exchange between the HA and the MN (in the IDii field in IKE_AUTH). This FQDN must, if not already known by the AAAH delivered to it. [Editor's Note: An appropriate AVP for carrying the FQDN has not yet been found.]

5. Security Considerations

[Editor's Note: Since the document is not complete it is necessary to state that the security consideration section is incomplete as well. Hence, it is only possible to refer to the security issues raised in the Mobile IPv6 and Diameter protocol related documents mentioned here, such as [11], [8] and [1].]

6. IANA Considerations

No new message formats or command codes are defined in this document.

7. Acknowledgements

We would like to thank the MIPv6 Bootstrapping Design Team for their comments. Additionally, we would like to thank Junghoon Jee and Florian Kohlmayer for their input.

Parts of this document are a byproduct of the ENABLE Project, partially funded by the European Commission under its Sixth Framework Programme. It is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ENABLE Project or the European Commission.

8. References

8.1. Normative References

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

[2] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-01 (work in progress), October 2005.

[3] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

[4] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[5] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[6] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping via DHCPv6 for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-00 (work in progress), October 2005.

[7] Hamilton, M. and R. Wright, "Use of DNS Aliases for Network Services", BCP 17, RFC 2219, October 1997.

8.2. Informative References

[8] Giaretta, G., "Goals for AAA-HA interface", draft-ietf-mip6-aaa-ha-goals-01 (work in progress), January 2006.

[9] Mattila, L., Koskinen, J., Stura, M., Loughney, J., and H. Hakala, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-06 (work in progress), August 2004.

[10] Alfano, F., "Diameter Quality of Service Application", draft-alfano-aaa-qosprot-05 (work in progress), October 2005.

[11] Giaretta, G., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), October 2004.

Authors' Addresses

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com

Tseno Tsenov
Sofia,
Bulgaria

Email: tseno.tsenov@mytum.de

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Email: gerardo.giaretta@tilab.com

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: julien.bournelle@int-evry.fr

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.