                            DIAMETER
                         Secure Proxying

Status of this Memo

   This document is an individual contribution for consideration by the
   AAA Working Group of the Internet Engineering Task Force. Comments
   should be submitted to the diameter@ipass.com mailing list.

   Distribution of this memo is unlimited.

   This document is an Internet-Draft and is in full conformance with
   all provisions of Section 10 of RFC2026. Internet-Drafts are working
   documents of the Internet Engineering Task Force (IETF), its areas,
   and its working groups. Note that other groups may also distribute
   working documents as Internet-Drafts.

   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."

   The list of current Internet-Drafts can be accessed at:

      http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at:

      http://www.ietf.org/shadow.html.

Abstract

   The DIAMETER base protocol [2] allows for secure communication
   between two DIAMETER nodes, and introduces the concept of proxying
   through the Proxy-State AVP. However, the base protocol only allows
   for hop-by-hop security, and the work done in the ROAMOPS WG [8]
   shows that support for end-to-end security through proxies. This
   document describes the extensions necessary to provide for secure

communication through DIAMETER proxies.

Table of Contents

1.0 Introduction

   Many services, including ROAMOPS and MobileIP, have a requirement for
   DIAMETER Server to proxy a request to another DIAMETER Server. The
   concept of proxying AAA requests was introduced by RADIUS and has
   been in use for many years.

   The DIAMETER base protocol [2] does provide the basic capability for
   proxying, but only defines hop-by-hop security, which has some known
   security flaws. Specifically a fraudulent proxy server can modify
   some portions of an AAA request in order to make the next hop
   improperly believe that some services were rendered. For example, a
   DIAMETER Proxy Server could modify an accounting request, such as the
   number of bytes that a user transfered, and the end system would have
   no way of determining that this change occured.

This specification contains the extensions necessary to DIAMETER to
allow for end-to-end AVP integrity and privacy. The document also
describes a method that DIAMETER can provide referal services to
clients.

The Extension number for this draft is two (2). This value is used in
the Extension-Id AVP as defined in [2].

1.1 **Copyright Statement**

1.2 **Requirements language**

In this document, the key words "MAY", "MUST, "MUST NOT", "optional",
"recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as
described in [13].

1.3 **Changes in version -02**

The following changes were made in version 02 of the document:

  - New title

  - A good cleanup of the abstract and the introduction.

  - Fixed up text in section 3.2 that stated that all AVPs with the
  'P' disabled were protected. This should have stated enabled.

  - Added Section 2 which describes the extended AVP Header Format.

  - Moved the Proxy State AVP to the base protocol.

  - Changed the description of the Digital-Signature AVP.

  - The Next-Hop AVP now requires a preceeding Digital-Signature AVP
  instead of a Host-IP-Address AVP. This change was necessary since
  the base protocol does not explicitly state that the Host-IP-
  Address AVP may appear multiple times in a single message. Such a
  change would be a big departure from the current RADIUS model
  where the Host-IP-Address contains the IP address of the
  originator of the message, not the address of intermediate hops.

  - Fixed various references to sections that were incorrect.

- Added clarification about the use of ICV and Digital Signatures
  within a single message.

- Updated the AVP Header flags.

- Re-wrote a good portion of section 4.1 ...

- ... well, re-wrote a good portion of all everything in section
  4.

- Added a reference to RFC 2459 (x.509 certs)

- Added an IANA Considerations section.

1.3 Changes in version -03

The following changes were made in version 03 of the document:

- Removed the DDR and DDA Commands. The new base protocol defines
  an error message that allows a broker to return a redirect
  indication. This new method really simplifies the protocol.

- Changed the AVP Command Code for Next-Hop from 278 to 290.

2.0 Extended AVP Format

The DIAMETER Proxy specification introduces a new bit in the AVP
flags field of the AVP Header. The following AVP header is used when
proxy support is enabled.

The attribute format is shown below and MUST be sent in network byte
order.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AVP Code                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        AVP Length          | Cmd Flags |Reservd|P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Vendor ID (opt)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Tag (opt)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+-+-+-+
```

Command Flags

   All Command Codes defined in this spec MUST set all bits in this
   field to zero (0).

AVP Flags

   The AVP Flags field informs the DIAMETER host how each attribute
   must be handled.

   The 'P' bit, known as the protected AVP bit, is used to indicate
   whether the AVP is protected by a Digital Signature AVP. When set,
   the AVP is protected and the contents cannot be changed by a
   DIAMETER proxy server. An AVP MUST NOT have both the 'P' and the
   'H' bits set simultaneously, since the 'H' bit implies that the
   AVP will change on a hop-by-hop basis, and the 'P' requires that
   the AVP NOT change along a proxy chain.

   Note that unless noted, the 'P' bit can be set on any DIAMETER
   AVP. The Proxy-State AVP MUST not have the 'P' bit set since this
   AVP will be removed at each hop. Any other AVP that have similar
   properties (e.g. it will be removed or modified at each hop) MUST
   NOT have the 'P' bit enabled.

   When the 'E' bit is enabled it indicates that the AVP data is
   encrypted using end-to-end encryption.

   Note that the User-Name AVP [2] MUST NOT have the 'E' bit set
   since intermediate proxies require the domain information in order
   to determine the target proxy.

3.0 DIAMETER AVPs

   This section will define the mandatory AVPs which MUST be supported
   by all DIAMETER implementations claiming support for this
   specification.

   The following AVPs are defined in this document:

Attribute Name	Attribute Code	Definition in Section
Digital-Signature	260	3.1
X509-Certificate	264	3.2
X509-Certificate-URL	265	3.3
Next-Hop	290	3.4

3.1 Digital-Signature

  Description

    The Digital-Signature AVP is used to provide for authentication,
    integrity and non-repudiation of DIAMETER AVPs. A DIAMETER entity
    adding AVPs to a message that must be protected by the Digital
    Signature MUST ensure that they apprear prior to this AVP. Two are
    two exceptions to this rule. The Integrity-Check-Value AVP, which
    MUST appear after the Digital-Signature AVP, since it is stripped
    at each hop. Any AVP that has the 'H' bit set CANNOT be included
    in the Digital-Signature. Any other AVP that is stripped at each
    hop (e.g. Proxy-State AVP) also MUST NOT be protected by the
    Digital-Signature AVP. AVPs are marked as being protected by
    enabling their 'P' bit.

    A DIAMETER node adding a Digital-Signature to a message that
    already has such an AVP MUST sign all of the existing AVP that
    have the 'P' bit set in addition to the new protected AVPs added.

    It is imperative that Proxy servers NOT change the order of the
    AVPs with the 'P' bit set, otherwise the signature verification
    would fail. Proxy servers also MUST NOT remove, add, or change
    any AVP that has the 'P' bit set.

    The Digital Signature also includes the DIAMETER header. However,
    when computing the signature, it is necessary for the header's
    length, Ns and Nr fields to be set to zero (0). This is necessary
    since the message size and windowing information may change from
    one proxy server to another as AVPs are added and others are
    deleted.

    The Digital-Signature is generated in the method described in
    section 4.4.1.

    All DIAMETER implementations supporting this extension MUST
    support this AVP.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                AVP Header (AVP Code = 260)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Address                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Transform ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+-+-+-+
```

AVP Length
   The length of this attribute MUST be at least 17.

AVP Flags
   The 'M' bit MUST be set. The 'P', 'V', 'H' and 'T' bits MUST
   NOT be set.

Address
   The Address field contains the IP address of the DIAMETER host
   which generated the Digital-Signature.

Transform ID
   The Transform ID field contains a value that identifies the
   transform that was used to compute the signature. The following
   values are defined in this document:

      RSA [9]   1

Data
   The Data field contains the digital signature of the message up
   to this AVP.

3.2 X509-Certificate

  Description

   The X509-Certificate [12] is used in order to send a DIAMETER peer
   the local system's X.509 certificate chain, which is used in order
   to validate the Digital-Signature attribute.

   Section 4.6 contains more information about the use of
   certificates.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                  AVP Header (AVP Code = 264)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+-+-+-+-+
```

AVP Flags
    The 'M' bit MUST be set. The 'P' bits MAY be set if end to end
    message integrity is required. The 'V', 'H' and 'T' bits MUST
    NOT be set.

Data
    The Data field contains the X.509 Certificate Chain.

3.3 X509-Certificate-URL

  Description

    The X509-Certificate-URL is used in order to send a DIAMETER peer
    a URL to the local system's X.509 certificate chain [12], which is
    used in order to validate the Digital-Signature attribute.

    Section 4.6 contains more information about the use of
    certificates.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                  AVP Header (AVP Code = 265)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    String ...
+-+-+-+-+-+-+-+-+
```

AVP Flags
    The 'M' bit MUST be set. The 'P' bits MAY be set if end to end
    message integrity is required. The 'V', 'H' and 'T' bits MUST
    NOT be set.

String
    The String field contains the X.509 Certificate Chain URL.

3.4 Next-Hop

  Description

The Next-Hop AVP MUST preceed a Digital-Signature AVP and is used
to validate that a message traversed the proxy chain that was
intended. A DIAMETER message with the Next-Hop Address being
different than the address found in the preceeding Digital-
Signature AVP is considered invalid.

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                 AVP Header (AVP Code = 290)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Address                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

AVP Flags
   The 'M' bit and 'P' bits MUST be set. The 'V', 'H' and 'T'
   bits MUST NOT be set.

Address
   This field contains the IP Address of the next DIAMETER Server.
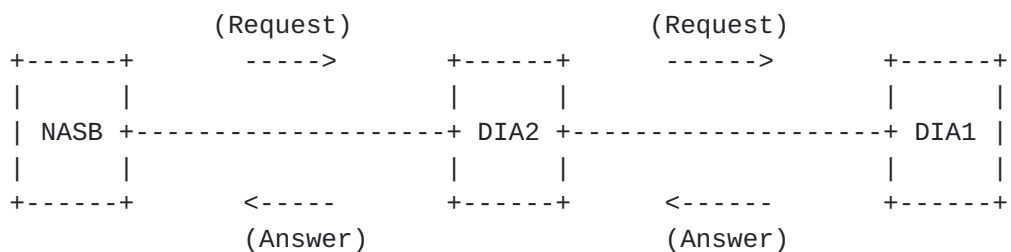

4.0 Protocol Definition

This section will describe how the base protocol works (or is at
least an attempt to).

4.1 Feature Advertisement/Discovery

As defined in [2], the Reboot-Ind and Device-Feature-Query messages
can be used to inform a peer about locally supported DIAMETER
Extensions. In order to advertise support of this extension, the
Extension-Id AVP must be transmitted with a value of two (2).

4.2 DIAMETER Secure Proxying

The ROAMOPS specification [11] discusses how RADIUS servers can be
arranged in a hierarchical manner, allowing message exchanges across
domain boundaries. The specification also describes some security
flaws encountered when RADIUS is used in a proxy environment. The
DIAMETER extension described in this document introduces end-to-end
security, which solves many of the problems encountered when RADIUS
is used.

```
                  (Request)                    (Request)
    +------+         ----->         +------+      ------>        +------+
    |      |                        |      |                     |      |
    | NASB +--------------------+ DIA2 +--------------------+ DIA1 |
    |      |                        |      |                     |      |
    +------+         <-----         +------+      <------        +------+
                  (Answer)                     (Answer)
```

In this example NASB generates a Request that is forwarded to DIA2.
The Request contains a Digital-Signature AVP which "protects" all
preceeding AVPs bit the 'P' bit set (known as protected AVPs) within
the request. All AVPs which may be modified, or removed by
intermediate DIAMETRE Proxies MUST NOT have the 'P' bit set. Such
AVPs include the Integrity-Check-Value, Proxy-State, etc. Once DIA2
receives the request, it MAY validate the signature in the request to
ensure that it was originated by NASB. Verification may not be
necessary if the signature was added by a DIAMETER node one hop away
since the Integrity-Check-Value (or any whatever security mechanism
used for hop-by-hop security) may be sufficient.

The DIA2 Server SHOULD add the Proxy-State AVP [2], which contains
opaque data that MUST be present in the response and is used to
identify state information related to the request or response. If a
Proxy-State AVP is found in the request, it SHOULD be replaced with a
locally generated Proxy-State AVP. This means that the Proxy-State
AVP cannot have the 'P' bit set. The Server MAY also add other new
AVPs to the request. All new AVPs that are protected by the new
Digital-Signature AVP MUST have the 'P' bit set, and MUST preceed the
Digital-Signature AVP. The message is then forwarded towards the DIA1
server.

The use of network level encryption, such as IPSec, cannot be used
for end-to-end AVP integrity between NASB and DIA1, since all
messages are processed by DIA2. What is needed is an application
level security mechanism, which is what the Digital-Signature AVP
provides. However, Digital-Signatures may not be necessary if the
messages do not traverse proxies, unless non-repudiation is required.

This mechanism now provides a method for DIA1 to be able to identify
that NAS was the initiator of the request, and that no "critial" AVPs
were modified mid-stream by intermediate proxies. Therefore, DIA2
cannot modify any protected AVPs (such as duration of a call, number
of bytes transfered, etc). This mechanism also provides the
application with the integrity, and non-repudiation, information it
may need should it deem it necessary to log such information.

This extension also provides for end-to-end AVP encryption, by using
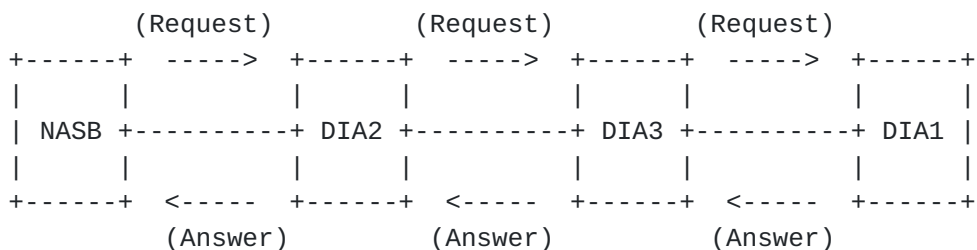the peer's public key. However, given that asymetric encryption is

very costly, it's use should be minimal.

An attack has been identified in this proposal which allows a
malicous man in the middle attack as shown in the following diagram.

```
        (Request)         (Request)          (Request)
  +------+  ----->  +------+  ----->  +------+  ----->  +------+
  |      |    |     |      |    |     |      |    |     |      |    |
  | NASB +----------+ DIA2 +----------+ DIA3 +----------+ DIA1 |
  |      |    |     |      |    |     |      |    |     |      |    |
  +------+  <-----  +------+  <-----  +------+  <-----  +------+
         (Answer)          (Answer)           (Answer)
```

In this example, DIA3 traps messages generated from DIA2 towards
DIA1, removes the AVPs added by DIA2 and inserts its own AVPs
(possibly by trying to convince DIA1 to pay DIA3 for the services).
This attack can be prevented by supporting a new Next-Hop AVP. In
this case when NASB prepares a request it inserts a protected Next-
Hop AVP which contains DIA2's identity. DIA2 also adds a Next-Hop
AVP with DIA1 as the next hop.

This mechanism ensures that a man in the middle cannot alter the
message by overriding the previous hop's additions and signature.
DIA1 could easily validate the message's path with the use of the
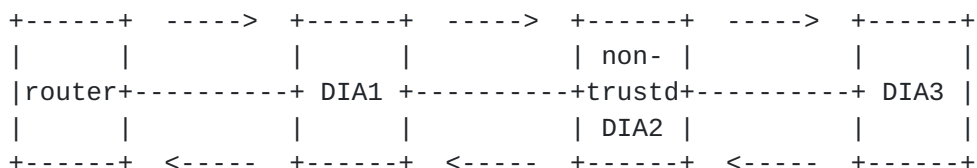Next-Hop AVPs.

4.3 Data Integrity

This section will describe how data integrity and non-repudiation is
achieved using the Digital-Signature AVP.

Note that the Timestamp and Nonce AVPs MUST be present in the message
PRIOR to the Digital-Signature AVPs discussed in this section. The
Timestamp AVP provides replay protection and the Nonce AVP provides
randomness.

4.3.1 Using Digital Signatures

In the case of a simple peer to peer relationship the use of IPSEC is
sufficient for data integrity and confidentiality. However there are
instances where a peer must communicate with another peer through the
use of a proxy server. IPSEC does not provide a mechanism to protect
traffic when two peers must use an intermediary node to communicate
at the application layer therefore the Digital-Signature AVP MUST be
used.

The following diagram shows an example of a router initiating a
DIAMETER message to DIA1. Once DIA1 has finished processing the
message it adds its signature and forwards the message to the non-
trusted DIA2 proxy server. If DIA2 needs to add any protected AVPs it
SHOULD add its digital signature before forwarding the message to
DIA3.

```
   +------+  ----->  +------+  ----->  +------+  ----->  +------+
   |      |          |      |          | non- |          |      |
   |router+----------+ DIA1 +----------+trustd+----------+ DIA3 |
   |      |          |      |          | DIA2 |          |      |
   +------+  <-----  +------+  <-----  +------+  <-----  +------+
```

Since intermediate DIAMETER proxies may add, or delete unprotected
AVPs "en route" towards the final DIAMETER destination, it is
necessary for the length, Ns and Nr in the header to be set to zero
(0) prior to the signature computation. The fields must be restored
once the computation is complete.

The following is an example of a message that include end-to-end
security:

```
    <DIAMETER Message> ::= <DIAMETER Header>
                           <Command AVP>
                           [<Additional AVPs>]
                           <Next-Hop AVP>
                           <Timestamp AVP>
                           <Nonce AVP>
                           <Digital-Signature AVP>
```

The AVP Header's 'P' bit is used to identify which AVPs are
considered protected when applying a digital signature to a DIAMETER
message. Protected AVPs cannot be changed "en route" since they are
protected by the Digital Signature AVP. All protected AVPs added by a
DIAMETER entity MUST appear prior to the new Digital Signature AVP.
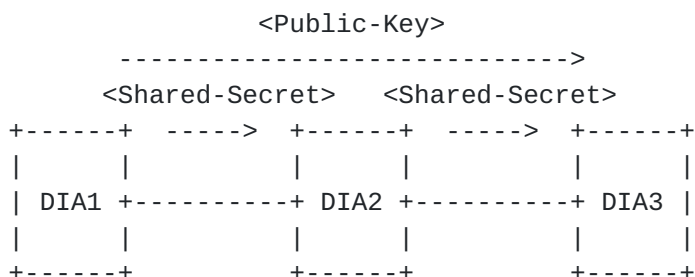
The Next-Hop AVP indicates the intended recipient of the DIAMETER
message. When a DIAMETER message is received with a Next-Hop AVP
that does not correspond with the address information with the
preceeding Digital-Signature AVP, the message MUST be considered
invalid and MUST be rejected. The Next-Hop AVP MUST be protected.

The Data field of the Digital-Signature AVP contains the RSA/MD5
signature algorithm as defined in [9].

4.3.2 Using Mixed Data Integrity AVPs

The previous sections described the Integrity-Check-Value and the
Digital-Signature AVP. Since the ICV offers hop-by-hop integrity and
the digital signature offers end to end integrity, it is possible to
use both AVPs within a single DIAMETER message. In fact, the use of
the ICV and the Digital-Signature is recommended to provide both
types of AVP integrity, which is necessary when messages are proxied.
In the event that two peers use an underlying integrity mechanism
(e.g. IPSec) for hop-by-hop AVP integrity, the ICV AVP is not
necessary and should not be used.

The following diagram provides an example where DIAMETER Server 1
(DIA1) communicates with DIA3 using Digital-Signatures through DIA2.
In this example ICVs are used between DIA1 and DIA2 as well as
between DIA2 and DIA3.

```
                     <Public-Key>
            ----------------------------->
          <Shared-Secret>    <Shared-Secret>
     +------+  ----->  +------+  ----->  +------+
     |      |          |      |          |      |
     | DIA1 +----------+ DIA2 +----------+ DIA3 |
     |      |          |      |          |      |
     +------+          +------+          +------+
```

Using the previous diagram, the following message would be sent
between DIA1 and DIA2:

```
    <DIAMETER Message> ::= <DIAMETER Header>
                           <Command AVP>
                           [<Additional AVPs>]
                           <Timestamp AVP>
                           <Nonce AVP>
                           <Digital-Signature AVP>
                           <Integrity-Check-Value AVP (DIA1->DIA2)>
```

The following message would be sent between DIA2 and DIA3:

```
    <DIAMETER Message> ::= <DIAMETER Header>
                           <Command AVP>
                           [<Additional AVPs>]
                           <Timestamp AVP>
                           <Nonce AVP>
                           <Digital-Signature AVP>
                           <Timestamp AVP>
                           <Nonce AVP>
                           <Integrity-Check-Value AVP (DIA2->DIA3)>
```
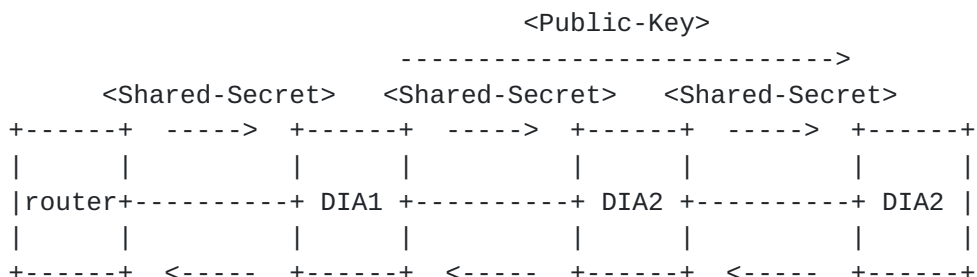
Note that in the above example messages the ICV AVP appear after the

Digital-Signature AVP. This is necessary since DIA2 above removes the
ICV AVP (DIA1->DIA2) and adds its own ICV AVP (DIA2->DIA3). The ICVs
provide hop-by-hop security while the Digital-Signature provides
integrity of the message between DIA1 and DIA3.

```
                                 <Public-Key>
                       ---------------------------->
            <Shared-Secret>    <Shared-Secret>    <Shared-Secret>
      +------+  ----->  +------+  ----->  +------+  ----->  +------+
      |      |   |      |      |   |      |      |   |      |      |
      |router+----------+ DIA1 +----------+ DIA2 +----------+ DIA2 |
      |      |   |      |      |   |      |      |   |      |      |
      +------+  <-----  +------+  <-----  +------+  <-----  +------+
```

There are cases, such as in remote access, where the device
initiating the DIAMETER request does not have the processing power to
generate Digital-Signatures as required by the protocol. In such an
arrangement, there normally exists a first hop DIAMETER Server (DIA1)
which acts as a proxy to relay the request to the final
authenticating DIAMETER server (DIA2). It is valid for the first hop
server to remove the Integrity-Check-Value AVP inserted by the router
and replace it with a Digital-Signature AVP.

4.4 AVP Encryption with Public Keys

AVP encryption using public keys is much more complex than the
previously decribed method, yet it is desirable to use it in cases
where the DIAMETER message will be processed by an untrusted
intermediate node (proxy).

Public Key encryption SHOULD be supported, however it is permissible
for a low powered device initiating the DIAMETER message to use
shared secret encryption with the first hop (proxy) DIAMETER server,
which would decrypt and encrypt using the Public Key method.

The PK-Encrypted-Data bit MUST only be set if the final DIAMETER host
is aware of the sender's public key. This information can be relayed
in three different methods as described in section 4.6.

The AVP is encrypted in the method described in [9].

4.5 Public Key Cryptography Support

A DIAMETER peer's public key is required in order to validate a
message which includes the the Digital-Signature AVP. There are three
possibilities on retrieving public keys:

4.5.1 X509-Certificate

A message which includes a Digital-Signature MAY include the X509-
Certificate AVP. Given the size of a typical certificate, this is
very wasteful and in most cases DIAMETER peers would cache such
information in order to minimize per message processing overhead.

It is however valid for a DIAMETER host to provide its X509-
Certificate in certain cases, such as when issuing the Device-
Reboot-Indication, or in the Domain-Discovery messages. It is
envisioned that the peer would validate and cache the certificate at
that time.

4.5.2 X509-Certificate-URL

The X509-Certificate-URL is a method for a DIAMETER host sending a
message that includes the Digital-Signature to provide a pointer to
its certificate.

Upon receiving such a message a DIAMETER host MAY choose to retrieve
the certificate if it is not locally cached. Of course the process of
retrieving and validating a certificate is lengthy and will require
the initiator of the message to retransmit the request. However once
cached the certificate can be used until it expires.

4.5.3 Static Public Key Configuration

Given that using certificates requires a PKI infrastructure which is
very costly, it is also possible to use this technology by locally
configuring DIAMETER peers' public keys.

Note that in a network involving many DIAMETER proxies this may not
scale well.

5.0 IANA Considerations

The numbers for the Command Code AVPs (section 3) is taken from the
numbering space defined for Command Codes in [2]. The numbers for the
various AVPs defined in section 4 were taken from the AVP numbering
space defined in [2]. The numbering for the AVP and Command Codes
MUST NOT conflict with values specified in [2] and other DIAMETER
related Internet Drafts.

This document also introduces two new bits to the AVP Header, which
MUST NOT conflict with the base protocol [2] and any other DIAMETER

extension.

6.0 References

[1] Rigney, et alia, "RADIUS", RFC-2138, April 1997
[2] Calhoun, Rubens, "DIAMETER Base Protocol", Internet-Draft,
    draft-calhoun-diameter-08.txt, August 1999.
[3] Rivest, Dusse, "The MD5 Message-Digest Algorithm",
    RFC 1321, April 1992.
[4] Kaufman, Perlman, Speciner, "Network Security: Private
    Communications in a Public World", Prentice Hall,
    March 1995, ISBN 0-13-061466-1.
[5] Krawczyk, Bellare, Canetti, "HMAC: Keyed-Hashing for Message
    Authentication", RFC 2104, January 1997.
[6] Calhoun, Bulley, "DIAMETER User Authentication Extensions",
    draft-calhoun-diameter-authen-06.txt, August 1999.
[7] Aboba, Beadles "The Network Access Identifier." RFC 2486.
    January 1999.
[8] Aboba, Zorn, "Criteria for Evaluating Roaming Protocols",
    RFC 2477, January 1999.
[9] Kaliski, "PKCS #1: RSA Encryption Version 1.5", Internet-
    Draft, draft-hoffman-pkcs-rsa-encrypt-03.txt, October 1997.
[10] Calhoun, Zorn, Pan, "DIAMETER Framework",
    draft-calhoun-diameter-framework-02.txt, Work in Progress,
    December 1998.
[11] Aboba, Vollbrecht, "Proxy Chaining and Policy Implementation in
    Roaming", RFC 2607, June 1999.
[12] Housley, Ford, Polk, Solo, "Internet X.509 Public Key
    Infrastructure Certificate and CRL Profile", RFC 2459,
    January 1999.
[13] S. Bradner, "Key words for use in RFCs to Indicate
    Requirement Levels", BCP 14, RFC 2119, March 1997.

7.0 Acknowledgements

The Authors would like to acknowledge the following people for their
contribution in the development of the DIAMETER protocol:

Bernard Aboba, Jari Arkko, Daniel C. Fox, Lol Grant, Nancy Greene,
Peter Heitman, Ryan Moats, Victor Muslin, Kenneth Peirce, Allan
Rubens, Sumit Vakil, John R. Vollbrecht, Jeff Weisberg and Glen Zorn

8.0 Author's Address

Questions about this memo can be directed to:

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, California, 94025
USA

 Phone: 1-650-786-7733
   Fax: 1-650-786-6445
E-mail: pcalhoun@eng.sun.com

William Bulley
Merit Network, Inc.
4251 Plymouth Road, Suite C
Ann Arbor, Michigan, 48105-2785
USA

 Phone: 1-734-764-9993
   Fax: 1-734-647-3185
E-mail: web@merit.edu

9.0 Full Copyright Statement