Diameter Strong Security Extension

Status of this Memo

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:


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@diameter.org mailing list.

Distribution of this memo is unlimited.

Copyright   (C) The Internet Society 1999. All Rights Reserved.
Abstract

The Diameter base protocol defines message integrity and AVP encryption using symmetric transforms to secure the communication between two Diameter nodes. The base protocol also defines a Diameter proxy server, that forwards requests to other servers when it detects that a given request cannot be satisfied locally.

The ROAMOPS Working Group has defined a requirement that allows for the Diameter servers communicating through the proxy to be able to provide for end-to-end AVP integrity and confidentiality, making it difficult for the proxy to be able to modify, and/or be able to view sensitive information, within the message. The Mobile-IP and NASREQ Working Groups have stated that strong authentication is a requirement for AAA data, such as accounting records, for the purposes of non-repudiation.

This Diameter extension specifies how strong AVP authentication, integrity and encryption can be done using asymmetric transforms, by encapsulating Cryptographic Message Syntax (CMS) data into Diameter AVPs. The CMS data can also be used to carry X.509 certificates.

Table of Contents

1.0 Introduction
   1.1 Certificate Requirements
   1.2 Requirements language
2.0 Extended AVP Format
3.0 CMS-Data AVP
4.0 Result-Code AVP Values
   4.1 Permanent Failures
5.0 IANA Considerations
6.0 Security Considerations
7.0 References
8.0 Acknowledgements
9.0 Authors' Addresses
10.0 Full Copyright Statement
1.0 Introduction

The Diameter base protocol [1] defines message integrity and AVP encryption using symmetric transforms to secure the communication between two Diameter nodes. The base protocol also defines a Diameter proxy server, that forwards requests to other servers when it detects that a given request cannot be satisfied locally.

The ROAMOPS Working Group has defined a requirement in [10] that allows for the Diameter servers communicating through the proxy to be able to provide for end-to-end AVP integrity and confidentiality, making it difficult for the proxy to be able to modify and see sensitive information within the message. The Mobile-IP and NASREQ Working Groups have stated in [6, 7, 8] that non-repudiation is a requirement for AAA data, such as accounting records.

When a chain of proxies use hop-by-hop security, each node in the proxy chain MUST recompute the Integrity-Value-Check (ICV) [1], making it easy for a malicious proxy to modify information in a Diameter message. It is virtually impossible for the rest of the nodes in the proxy chain to know that the message was modified in mid-stream. Figure 1 shows an example of such a network, where DIA3 modifies the contents of "foo" in both the request and the response.

```
(Request)         (Request)         (Request)
[AVP(foo)=x]      [AVP(foo)=x]      [AVP(foo)=y]
+------>          +------>          +------>
|      |              |      |              |      |
| NASB +----------+ DIA2 +----------+ DIA3 +----------+ DIA1 |
|      |              |      |              |      |
+------>          +------>          +------>
(Answer)          (Answer)          (Answer)
[AVP(foo)=b]      [AVP(foo)=b]      [AVP(foo)=a]
```

Figure 1: Proxy Chain

This document describes how strong authentication and encryption can be provided in the Diameter protocol, by encapsulating CMS objects [3] in AVPs. The CMS object can also be used to carry X.509 certificates and revocation lists.

In the example provided in Figure 1, the originator of the request and response adds a digital signature that covers a set of AVPs within the message. The protected AVPs MUST NOT be changed by an intermediate proxy server (DIA2, DIA3), since the signature validation performed by the end server would fail.

The Diameter base protocol also allows a Diameter broker to provide redirect services, as shown in Figure 2. The Diameter broker MAY
return information to a requesting server that would allow the servers to interact directly, bypassing the broker. This optimized approach reduces the complexity associated with end-to-end security.

```
                      +------------------+
                      |     Diameter     |
                      |      Broker      |
                      +------------------+

  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Request    | Response +
  Local      | Redirect  | Home
  ISP        v

  ^
  ^
  abc.net   |xyz.net |
  Diameter  <----------> Diameter
  Server    | Server |

  +----------+    Direct    +----------+
  Communication
```

Figure 2: Diameter Broker Returning Redirect Indication

When redirect services are used, a network layer security protocol, such as IP Security, MAY be used to secure the traffic between the two Diameter servers. However, security at the application level may still be necessary in this network configuration, specifically the ability to authenticate a select set of AVPs. Brokers that operate in a redirect mode typically require that both Diameter servers sign accounting records. The accounting record, signed by both parties is then forwarded to the broker via the local Diameter server. This provides the broker with some assurances that both networks agreed on the accounting data, which it MAY use for settlement purposes. If the underlying security protocol provides confidentiality, strong encryption MAY not be necessary in the redirect case.

Given that asymmetric transform operations are expensive, Diameter servers MAY wish to use them only when dealing with inter-domain servers, as shown in Figure 3. This configuration is normally desirable since Diameter entities within a given administrative domain MAY inherently trust each other. Further, it is desirable to move this functionality to the edges, since NASes do not necessarily have the CPU power to perform expensive cryptographic operations.
The Extension number for this draft is two (2). This value is used in the Extension-Id AVP as defined in [1].

1.1 Certificate Requirements

Certificates used for the purposes of Diameter MUST conform to the PKIX profile [4], and MUST also include a Diameter node’s NAI, which is typically added in the Host-Name AVP [1], as one of the values of the subjectAltName extension of the Certificate. The NAI is to be encoded as an rfc822Name within the subjectAltName.

These names are used for two purposes:

1. Where a Diameter node is verifying a signature it needs to be able to compare the identity of the signer against the identity in the Host-Name AVP.

2. Where a Diameter node is encrypting AVPs, it needs to be able to ensure that it uses a public key for the intended recipient. This requires comparing the identity in a Certificate against the NAI of the intended recipient (which is assumed to be known).

In either case, the presence of the required NAI as an rfc822Name value in the subjectAltName extension of a verified public key certificate satisfies the matching requirement.

Note that there MAY also be other values in the subjectAltName extension, (either using rfc822Name or other elements of the CHOICE), these can be safely ignored, but implementations MUST be able to handle their presence.

Note also that the PKIX profile [4], section 4.1.2.6, specifies the
rules for the relationship between the subjectAltName extension and the subject field of public key certificates.

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].

2.0 Extended AVP Format

This specification introduces the 'P' bit in the AVP Header, which is defined in [1]. The 'P' bit, known as the protected AVP bit, is used to indicate whether the AVP is protected by a digital signature. When set, the AVP is protected and the contents cannot be changed by a Diameter proxy server without detection.

```
+------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AVP Code                            |
+------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          AVP Length           |     Reserved        |P|R|V|R|M|
+------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Vendor ID (opt)                        |
+------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...          |
```

Figure 4: Extended Diameter AVP Header

Note that unless stated otherwise, the 'P' bit can be set on any Diameter AVP. The Proxy-State and Integrity-Check-Value AVPs [1] MUST NOT have the 'P' bit set. The Encrypted-Payload AVP MAY have the 'P' bit set if there is no intermediate proxy server. Any additional AVPs that MUST be removed, or changed, at each hop in a proxy chain MUST NOT have the 'P' bit set.

3.0 CMS-Data AVP

The CMS-Data AVP (AVP Code 310) is of type OctetString and contains the Distinguished Encoding Rules (DER) encoding of a CMS object [3] of type ContentInfo. The profile of CMS algorithm and structure usage is as specified in the S/MIME v3 message specification [11]. This means that where a set of AVPs is protected using CMS, the set MUST first be encoded according to MIME encoding rules specified below.
This method of encapsulating AVPs allows existing S/MIME toolkits to be used without changes in order to produce strongly protected Diameter messages. The CMS object MAY contain any of the three methods; signed-only, enveloped-only and signed-and-enveloped. Optional certificates and CRLs MAY be present in all three methods.

To package a set of AVPs as a MIME type, the AVPs are first concatenated in the order in which they occur in the Diameter message. The entire AVP MUST be input to the signing/encryption process, from the first byte of the AVP code to the last byte of the AVP data, including all other fields, length, reserved/flags, and optional vendor IDs, and padding. The AVP MUST be input to the signing/encryption process in network byte order. If AVPs are to be enciphered, then the encryptor is free to order AVPs whatever way it chooses. This value is then used as the value of a new MIME type application/x-diameter-avps, which MUST be prepared in accordance with the rules specified in section 3.1 of [11]. If a receiver detects that the contents of the CMS-Data AVP is invalid, it SHOULD return the new Result-Code AVP value defined in section 4.0.

Where signing only is performed, the signature is calculated over the canonical encoding of the application/x-diameter-avps MIME type, but the AVPs themselves are not carried within the CMS-Data AVP. Instead, the digest value within the SignedData structure contains the digest over the canonicalized encoding of application/x-diameter-avps. Multiple Diameter entities MAY add their signatures to an existing CMS-Data AVP using the countersignature attribute, defined in section 11.4 of [3]. The countersignature attribute requires that the signatures occur sequentially, meaning that each node’s signature covers the existing signatures in the CMS object.

Where encryption only is performed, the encryptedContent MUST contain the canonical encoding of the application/x-diameter-avps MIME type.

Where signing and encryption are both performed, signing MUST occur first, the resulting CMS object MUST then be MIME encoded producing an application/pkcs7-mime MIME type which is then used as the content of the EnvelopedData.

There is no need for an ‘outer’ MIME encoding when only signing, or only encryption is applied.

Where AVPs are encapsulated within a CMS-Data AVP, the eContentType of the EncapsulatedContentTypeInfo MUST be id-data [11].

The signing and encryption algorithms supported MUST be those specified in sections 2.2 and 2.3 of [11].
Conformant implementations MUST emit a CMS-Data AVP which contains only one application/x-diameter-avps MIME type. Implementations which receive any other MIME type MUST indicate an error.

Where a CMS-Data AVP contains a set of certificates then both public key certificates (Certificate) and attribute certificates (AttributeCertificate) are allowed by CMS (as well as one other legacy format which MUST NOT be used). Support for use of the Certificate structure is REQUIRED, implementations SHOULD support use of the AttributeCertificate structure as defined in the PKIX attribute certificate profile [12]. This allows Diameter implementations to include a certificate from a trusted party that they are authorized to emit the AVPs contained in the message.

When a SignedData object is present, the eContent field of the EncapsulatedContentInfo structure MUST be absent since the authentication covers data outside of the object. The signature is computed over all AVPs prior to the AVP that have the ‘P’ bit enabled. The order of the AVPs MUST be preserved and the computation begins with the first AVP immediately following the Diameter header. If the CMS-Data AVP is present in a Grouped-AVP, it covers all AVPs within the Grouped-AVP AVP that has the ‘P’ bit set. An Integrity-Check-Value (ICV) AVP MUST NOT preceed a CMS-Data AVP containing a SignedData object. If the signature cannot be verified correctly, a response with the Result-Code AVP set to Diameter_INVALID_AUTH [1] MUST be returned.

When an EnvelopedData object is present, the encryptedContentInfo field MUST contain the Host-Name AVP, containing the host name of the encryptor, and one or more additional AVPs.

When a conforming implementation receives a Diameter message which contains encrypted AVPs within a CMS EnvelopedData, then the recipient MUST check to see if it is on the list of recipients specified in the RecipientInfos of the EnvelopedData. If not, the recipient MAY choose to process the message or indicate an error. If the recipient is in the RecipientInfos and an error occurs during decryption, then the recipient MUST indicate an error.

A CMS-Data MAY also contain a certs-only CMS structure, which is a degenerate form of CMS structure containing only PKI related information (see section 3.6 of [11] for details of the CMS certs-only structure). This use of the CMS-Data AVP can be used to "push" public key and attribute certificates and CRLs using Diameter, which MAY be useful in environments where repositories (e.g. LDAP servers) are either not used or not available (e.g. due to crossing a domain boundary). Conforming implementations MUST be able to emit a certs-only CMS structure which contains relevant PKI related information.
and MUST be able to process a CMS-Data AVP which contains a certs-
only CMS structure. Of course, the recipient of such a certs-only CMS
structure SHOULD NOT use the PKI related information without first
verifying it, e.g.
by checking that issuer’s are trusted, signatures
verify etc.

When the CMS-Data AVP contains certificates in the certificates field
of the SignedData, a CRL [4] MAY also be provided in the crls field
of the SignedData, which MAY be used to assist in determining whether
a certificate has been revoked. Optionally, the Diameter server MAY
check the status of certificates using another mechanism, such as
Online Certificate Status Protocol (OCSP) [9].

This AVP MUST have the ‘M’ bit enabled. The ‘P’ and ‘V’ bits MUST NOT
be enabled.

The following is an example of a message that includes strong
security and hop-by-hop security:

Example-Command ::= < Diameter-Header: 9999999 >
[ AVP ]
{ CMS-Data }
* [ Proxy-State ]
* [ Route-Record ]
* [ Routing-Realm ]
0*1< Integrity-Check-Value >

4.0 Result-Code AVP Values

This section defines new Result-Code [1] values that MUST be
supported by all Diameter implementations that conform to this
specification.

4.1 Permanent Failures

Errors that fall within the permanent failures category are used to
inform the peer that the request failed, and should not be attempted
again.

Diameter_INVALID_CMS_DATA      5018
This error code is returned when a CMS-Data AVP is received
with an invalid ContentInfo object.

5.0 IANA Considerations
The CMD-Data AVP defined in Section 3 is a Diameter AVP whose identifier was allocated from the AVP numbering space [1], and extended in [13], [14] and [15]. IANA should assign a value of 310 to this AVP.

The Result-Code values defined in Section 4.0 are error codes as defined in [1] and extended in [13], [14] and [15]. They correspond to error values specific to the Strong Security extension. IANA should record the values as defined in Section 4.0.

6.0 Security Considerations

This document describes how strong security can be achieved in the Diameter protocol by allowing S/MIME Cryptographic Message Syntax [3] objects to be carried as a Diameter AVP.

Section 3.0 states that a certificate received in a CMS-Data AVP SHOULD NOT be used prior to cert verification. In most cases, the verification will be according to the rules specified in [4], however, some communities have indicated that they wish to be allowed to specify alternative certificate verification mechanisms, hence the "SHOULD NOT" rather than the more typical "MUST NOT". The authors do however strongly RECOMMEND that the verification procedures specified in [4] are always applied, regardless of whatever other verification mechanisms are in use.

7.0 References


8.0 Acknowledgements

The authors would also like to acknowledge the following people for their contribution in the development of the Diameter protocol:

9.0 Authors’ Addresses

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.
Building One, Suite 2000
4251 Plymouth Road
Ann Arbor, Michigan, 48105-2785
USA

Phone: +1 734-764-9993
Fax: +1 734-647-5185
E-mail: web@merit.edu

Stephen Farrell
Baltimore Technologies
61/62 Fitzwilliam Lane
Dublin 2,
IRELAND

Phone: +353-1-647-7300
Fax: +353-1-647-7499
E-Mail: stephen.farrell@baltimore.ie

10.0 Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

11.0 Expiration Date

This memo is filed as <draft-calhoun-diameter-strong-crypto-06.txt> and expires in July 2001.