Authentication, Authorization, and Accounting
Internet Draft
Document: draft-hiller-aaa-diamaka-00.txt
Category: Informational
February, 2001

Tom Hiller
Peter J. McCann
Lucent Technologies

DIAMETER Support for Authentication and Key Agreement (AKA)

Status of this Memo

1. Abstract

The Authentication and Key Agreement (AKA) protocol is a widely used mechanism for authenticating mobile nodes in wireless networks. This draft proposes new DIAMETER AVPs to carry AKA parameters, which will enable DIAMETER to serve as an inter-domain transport mechanism for AKA messages.

Because AKA was designed for a slightly different trust environment than that likely to be encountered in a DIAMETER-based network, we also discuss how AKA can be deployed in a DIAMETER environment to provide additional authenticity guarantees.

2. Conventions used in this document

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 [2].

3. Introduction

Authentication and Key Agreement (AKA) is a mutual authentication algorithm involving a set of message exchanges between mobile node (MN) and entities in the visited and home network. The basic Authentication and Key Agreement (AKA) protocol is described in the 3GPP document 3G TS 33.102 [3]. A by-product of AKA operation is the generation of integrity and encryption keys. Wireless SDOs such as 3GPP and 3GPP2 plan to support AKA as the primary means of authenticating mobile nodes. AKA extensions have already been proposed for SIP [4].

3GPP2 plans to support authentication and authorization via the use of DIAMETER. DIAMETER support is being considered in 3GPP. This contribution proposes extensions to DIAMETER that will allow it to serve as a transport for AKA parameters during the authentication procedure. For ease of reading, DIAMETER augmented with AKA extensions is simply referred to in this contribution as ôDIAMETER AKAö.

4. Overview of AKA

AKA is a 3-party protocol that takes place between a client, a service provider, and a home authentication center. For the explanation below, we assume that the service being used is basic network access as in todayÆs cellular network; that the service provider is a visited wireless carrier; and that the home authentication center is associated with a home network. In this case the client is a mobile node (MN), which will carry out AKA negotiation with a visited AAA server (VAAA), which will in turn communicate with a home AAA server (HAAA). However, the reader should keep in mind that AKA is a generic authentication and key agreement mechanism that could be used for other types of services, as outlined in later sections of this document. In this section we assume that the protocol used to carry AKA parameters between the client and service provider is some wireless link layer, but in other scenarios the particular protocol used may differ. For all scenarios, we assume that DIAMETER is the protocol of choice between VAAA and HAAA.

Initially, the MN is given an identity, which in cellular applications is the IMSI, and a secret K that it shares with HAAA. Upon connecting to the visited network, the MN transmits this identity to the VAAA. The VAAA uses the identity to locate the

HAAA and make an authentication data request, which returns a set of authentication vectors (AVs) from the home network.

Each AV contains a set of parameters (RAND, XRES, CK, IK, AUTN). RAND is a random number generated by the home network. XRES is

the expected response from the MN that would indicate a successful authentication. CK and IK are the Cipher Key and Integrity Key that should be used to protect the subsequent link layer data, assuming authentication was successful. The MN derives CK and IK by applying a key generating function to RAND, using the shared secret K known to the MN and HAAA. Finally, AUTN is itself another vector consisting of the elements (SQN+AK, AMF, MAC). Here SQN+AK is a monotonically increasing sequence number SQN XORed with an Anonymity Key AK, which is computed as a secure hash of RAND. AMF is a key management field that is used during re-synchronization procedures and for other purposes. Finally, MAC is a message authentication code computed over SQN, RAND, and AMF. All secure hashes (key generating and message authentication functions) are parameterized by the secret key K, so they are unique to a given mobile node.

Upon receipt of the AV set, the VAAA chooses the next AV and transmits (RAND, AUTN) from the AV to the MN. Note that CK and IK are not transmitted to the MN. However, because the MN possesses the secret key K, it can derive the AK from RAND and hence can derive the SQN from the SQN+AK present in AUTN. This allows the MN to compute an expected value for MAC based on the inputs SQN, RAND, and AMF, and to compare this to the MAC received in AUTN. If the result matches, and if the sequence number SQN is in an acceptable range relative to the last authentication that was performed, the MN can verify that the VAAA did indeed get the AV from HAAA. This provides some assurance that the MN is communicating with a legitimate visited network.

Now the MN must prove its identity to the VAAA. It does so by computing RES, which is a simple message authentication function applied to RAND. It transmits this value to VAAA, which compares it to XRES. If the values match, the VAAA can assume that it is communicating with a legitimate MN that is in possession of the secret key K used to generate the AV. Also, it is now in agreement on CK and IK that are used to encrypt and authenticate data to and from the MN for the link layer session.

5. Trust Model Issues

The AKA protocol provides the proper guarantees for the environment in which it was designed to operate: that of a fairly small number of wireless operators communicating over a secure network, and with a large degree of trust among the various carriers. However, as we move to an all-IP wireless network, there are likely to be many more carriers supporting different types of access networks, and they will be interconnected by a network of brokers each of whom acts as a manager for many pair-wise trust relationships. As such, there may not be a direct

contractual or trust relationship between the VAAA and HAAA when a MN roams to a given visited network.

In particular, AKA allows the comparison of RES with XRES to be performed completely in the VAAA. This gives the HAAA no assurance that a legitimate MN was actually connected to VAAA. For this reason we propose that AKA authentication with DIAMETER proceed in two steps, one which retrieves AUTN but does not expose XRES to the VAAA, and a second round-trip where the home network can actually compare RES to XRES. Then the HAAA can return a DIAMETER Access-Accept or -Reject as appropriate to the VAAA. This would be in accordance with usual IETF AAA based authentication models.

This extra step introduces an additional round-trip through the AAA infrastructure. A potential remedy to this situation would be to alter AKA protocol such that the MN includes self-contained authentication credentials, based on a timestamp, sequence number, and random value. When this request is presented to the HAAA, the HAAA can immediately verify the identity of the MN and release a set of standard AKA AV (i.e., including XRES) to the VAAA. The VAAA then compares RES with XRES in the subsequent response from the MN. This solution would have improved latency, but it implies a change to the basic AKA protocol, which may not be possible in a legacy environment.

6. Application Scenarios

Figures 1-3 identify application scenarios for DIAMETER AKA in an all-IP wireless network.

Figure 1 shows a mobile using AKA for device level authentication. Note that in this scenario, the keys IK and CK could be used for over-the-air encryption and integrity protection of data and signaling traffic. This is because the HAAA provides CK and IK to the VAAA via the Authentication Vector (AV), which, in turn, passes the AV to the link layer access network element.

Figure 2 shows a legacy (circuit voice) mobile node connecting to a network that supports DIAMETER AKA. This network contains a VAAA that communicates with an HAAA via DIAMETER. The HAAA may gateway the AKA parameters to a legacy HLR-based authentication center to which the mobile node is homed.

Figure 3 shows a mobile with a SIP client being authenticated by a SIP server. The SIP registrations contain AKA extensions. The SIP server generates DIAMETER AKA messages directly. The SIP server could be in a wireless carrier network, private network, or the network of a third party provider. N.B. The 3GPP and 3GPP2 SDOs

place the authenticating SIP server only in the home network. In this case there might not be a need for an interdomain AAA protocol. However, we show this scenario to cover other relationships that might exist between a SIP server and the home network.

```
               +-------------+       +-------------+
               |             |       |             |
               |   VAAA      +-------+    HAAA
               |             |       |             |
               +------+------+       +-------------+
                      |
                      |
+----------+   +------+------+
|          |   | Radio       |
| Mobile   +---+ Access      |
| Station  |   | Network     |
+----------+   +-------------+
```

Figure 1: Network Access using DIAMETER-AKA

```
               +-------------+       +-------------+
               |             |       |             |
               |   VAAA      +--------|HAAA/Gateway |
               |             |       |             |
               +-----+-------+       +-------\-----+
                     |                        \
                     |                  +------\------+
+----------+  +------+------+           |             |
| Mobile   |  | Radio Access|           |     HLR     |
| Station  +--+ Network     |           |             |
|          |  |             |           +-------------+
+----------+  +-------------+
```

Figure 2: Network Access using Legacy HLR

```
                           +-------------+       +-------------+
                           |             |       |             |
                           |   VAAA      +-------+    HAAA
                           |             |       |             |
                           +-----+-------+       +-------------+
                                 |
                                 |
            +----------+  +------+------+
            | Mobile   |  | SIP         |
            | Station  +--+ Server      |
            |          |  |             |
            +----------+  +-------------+
```

Figure 3: Application-layer (SIP) access using DIAMETER AKA.

In all cases, the following statements apply:

- The mobile and network entity or entities involved mutually authenticate each other.

- The mobile and some participating entity in the network may use keys derived from AKA message exchanges (i.e., the AV) for integrity or encryption purposes. This could apply to data link layer or application layer protection mechanisms.

7. Protocol Extensions

Section 5 outlined two approaches. The first approach requires two traversals and places the RES and XRES comparison in the HAAA (i.e. the HAAA does not send the XRES in the AV to the VAAA). The second approach requires only one traversal but relies on a challenge from the VAAA followed by a corresponding response from the MN.

The AKA Request AVP is given in Figure 4. It is an optional AVP for use only when the MN supports the response to a global challenge in its initial request for service. If not then only the NAI AVP is present in the Access Request, which may require the HAAA to withhold XRES in its response, forcing a two round trip authentication procedure.

The AKA Response AVP is given in Figure 5. It is used to supply the VAAA with the random challenge plus authentication information to be sent to the MN.

The AKA Keys AVP is given in Figure 6. It is used to supply encryption and integrity keys to the VAAA after the HAAA has verified the identity of the MN. It may be included in the first response if the AKA Request AVP was included in the initial request from the VAAA. Otherwise it should only be included in a second response to the VAAA after the HAAA has compared RES with XRES.

The AKA Request Result AVP is given in Figure 7. This is used during the two-round AKA protocol to communicate the MN's response to the HAAA.

```
 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                    |Reserved             |P|R|V|R|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                           G-RAND                              +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                           AUTHR                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: AKA Request 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 Code                                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | AVP Length                    |Reserved             |P|R|V|R|M|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                                                               |
   +                           RAND                                +
   |                                                               |
   +                                                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +       SQN+AK                  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                               |          AMF                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                                                               |
   +                            MAC                                +
   |                                                               |
   +                                                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: AKA Response 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 Code                                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | AVP Length                    |Reserved             |P|R|V|R|M|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                                                               |
   +                            XRES                               +
   |                                                               |
   +                                                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                                                               |
   +                             CK                                +
   |                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                             IK                                +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: AKA Key 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 Code                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| AVP Length                    |Reserved             |P|R|V|R|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                             RES                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: AKA Request Result AVP

8. Security Considerations

This draft provides a basic transport function for the parameters of AKA, which is itself a protocol designed to authenticate the identity of a mobile node and to distribute keying material to a service provider. However, we rely on the DIAMETER infrastructure itself to guarantee that keying material is not exposed or tampered with between the VAAA and the HAAA. If one or more intervening brokers are present on the path between VAAA and HAAA, then mechanisms for end-to-end security in DIAMETER (which are outside the scope of this draft) should be applied. In any case we assume that any two peer DIAMETER servers will make use of IP Security mechanisms to protect data in transit.

8. References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

3 3G TS 33.102 version 3.4.0 Release 99; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspecs; 3G Security

4 UMTS AKA in SIP; S3-000456; 3GPP TSG SA WG3 Security; S3#14; August 2-4 2000

9. Acknowledgments

Semyon Mizikovsky provided valuable review and feedback on this draft.

10. Author's Addresses

Peter J. McCann
Lucent Technologies
Rm 2Z-305
263 Shuman Blvd

Naperville, IL 60566-7050
USA

Phone: +1 630 713 9359
FAX: +1 630 713 4982
EMail: mccap@lucent.com

Tom Hiller
Lucent Technologies
Rm 2F-218
263 Shuman Blvd
Naperville, IL 60566-7050
USA

Phone: +1 630 979 7673
FAX: +1 630 979 7673
EMail: tom.hiller@lucent.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement