Source: Lucent Technologies*

Title: Use of AAA from SIP servers in the IP Multimedia CN Subsystem

For: Discussion/Approval

Introduction

The IP Multimedia Core Network Subsystem (IM CN SS) contains three types of CSCFs: Proxy CSCFs (P-CSCFs), which are the servers in direct contact with the SIP endpoints (UEs); Serving CSCFs (S-CSCFs), which are actually responsible for call features; and Interrogating CSCFs (I-CSCFs), which are responsible for routing SIP messages to and allocation of S-CSCFs. The servers (e.g., S-CSCF) may have a need to authenticate wireless users, authorize them for service, and to account for service usage. This contribution proposes that such functionality be agreed to be part of the IM CN SS architecture and recommends that an IETF AAA protocol (e.g., DIAMETER) be used for these purposes. In addition to providing the necessary AAA features for 3GPP, this step will assist in inter-working with with various other SIP based IP networks.

Discussion

Current CSCF Architecture

In the current definition of the IM CN SS three kinds of CSCFs are defined. The P-CSCF is the first point of contact with the UE. The UE sends a SIP REGISTER message to the P-CSCF. Based on the home domain name supplied in the REGISTER message, the P-CSCF forwards the registration to an I-CSCF associated with the home network. The I-CSCF interacts with the HSS to determine an S-CSCF in the home network. The I-CSCF forwards the registration to the identified S-CSCF in the home network. The S-CSCF interacts with the HSS to authenticate the request and retrieve subscriber profile information, and returns the SIP response via the one or more I-CSCFs to the P-CSCF, which returns the response to the UE.

The Cx interface is defined between the HSS and the CSCFs. It is this interface that allows the home I-CSCF to determine which S-CSCF should be allocated, and which allows the S-CSCF to authenticate the UE and retrieve service subscription information. Although the UE authentication shall be done by the S-SCSF (homeHSS/AAA), this document assumes that the P-CSCF and I-CSCF may also make use of this interface for authentication (e.g., to support some operotor specific operational practices), and that the protocol to be used on Cx be the IETF AAA DIAMETER protocol.

Figure 1 shows a canonical arrangement of CSCFs and AAA servers. The exact set of CSCFs involved in a particular SIP session depends on which CSCFs the operator determines are involved in AAA activities. it may be that the I-CSCF is involved in authorization, and the S-CSCF is involved with authentication. This contribution does not address all variations on Figure 1, rather it argues for the support of AAA clients on the CSCF to achieve as wide a range of AAA functionality as possible.

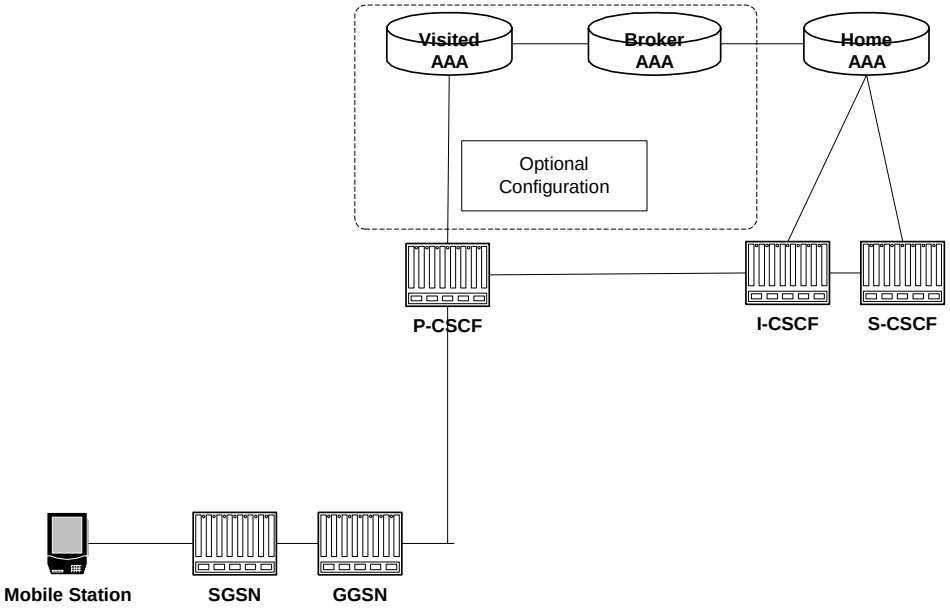

Figure 1: Architecture

Need for AAA Functionality

The existing architecture already recognizes the need for the S-CSCF to authenticate the UE and to retrieve subscriber information. This authentication and service authorization functionality will be carried out with the use of an IETF AAA protocol. However, in this section we argue that the P-CSCF and I-CSCF may also have a need for access to AAA functionality and, if so, should make use of DIAMETER for this purpose. For each kind of element, we examine each of the three A's in turn (Authentication, Authorization, and Accounting) and argue how each is best supported by a DIAMETER interface.

From P-CSCF

The P-CSCF is always in the serving network (home or visited). We propose that a DIAMETER interface should be allowed on the P-CSCF and that, for the visited case, an optional Visited AAA (VAAA) server be introduced. Connecting to a DIAMETER broker infrastructure will provide for roaming users, even when no direct, pairwise roaming agreement is in place between the home and visited network, and will allow for a scalable and secure trust management among the various operators. DIAMETER forms a convenient interface for all forms of inter-domain communication that need to leverage the trust distribution features of the brokers.

Authentication. The P-CSCF should gain assurance that it is dealing with a valid user, so that the visited network operator is assured of receiving payment for services delivered on the visited network. In some scenarious, simply using DNS to find a home I-CSCF and trusting the I-CSCF to authenticate the user may not satisfy the security requirements of inter-domain authentication, especially if no a priori agreement exists between the operators of the P-CSCF and the I-CSCF.

Authorization. The P-CSCF may want to obtain assurance that the user is authorized to make use of services on the visited network.

Accounting. The P-CSCF will monitor all SIP requests and send call data records through the DIAMETER infrastructure to the home network. This will be used for later billing and settlement with the visited network.

Figure 2 shows a user performing SIP registration and the P-CSCF using an AAA infrastructure to authenticate and authorize the user.

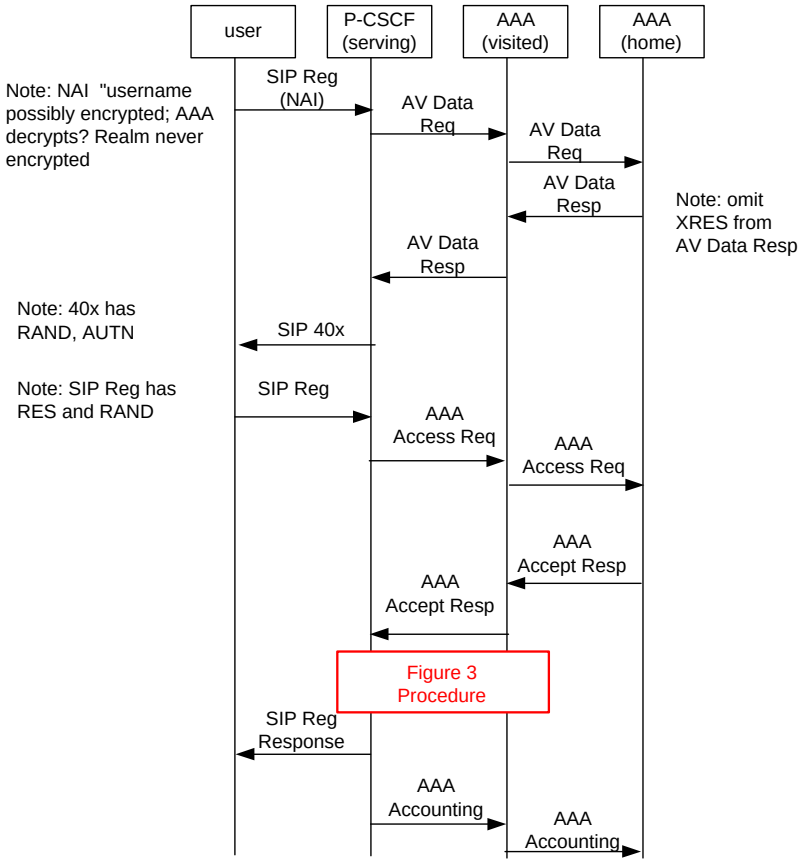

Figure 2: Example of optional P-CSCF and AAA use

The possibility exists for the home AAA server to send multiple Authentication Vectors (AV) to be used in subsequent authentication requests. This avoids a two round-trip delay.

From I-CSCF

Typically there will be at least one I-CSCF in the home network. The home I-CSCF must obtain information from the HSS about requirements for the S-CSCF to be allocated, and perform the allocation of the S-CSCF in the home network.

Authentication. The I-CSCF may be the only point of contact with the home network. As such, it should be able to make sure that the user credentials being used for registration are authentic. Even if the S-CSCF will later perform authentication, the I-CSCF, at an operator's option, may want to authenticate prior to S-CSCF allocation. Note that the S-CSCF may be owned by a different operator and may not be trusted by the home I-CSCF. Therefore, the I-CSCF may want to consult the HSS on its own, and DIAMETER can be used for this purpose.

Authorization. The I-CSCF may want to make sure the user is authorized for the services used. In particular, the most common form of authorization will probably be the type of S-CSCF the user is authorized to use in the home.

Accounting. Accounting records may be generated by the I-CSCF, but these are more likely to come from P-CSCF or S-CSCF. If any accounting information is generated by an I-CSCF it should be propagated with the use of DIAMETER to the home AAA server.

Figure 3 shows a user performing SIP registration and a home network I-CSCF using an AAA infrastructure to authenticate and authorize the user.

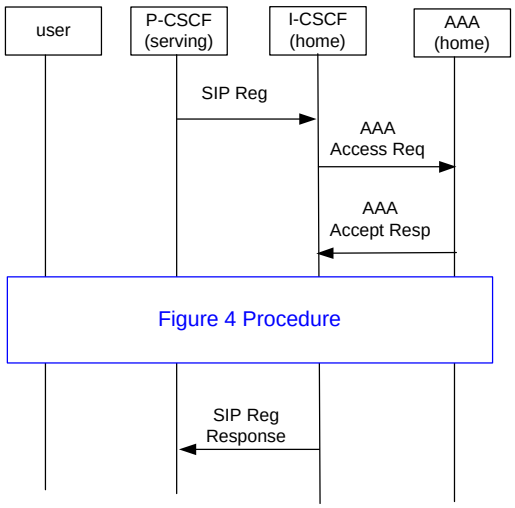

Figure 3: Example of home I-CSCF and AAA

Note that in Figure 3, the I-CSCF used the RAND and the RES found in the SIP Reg and sends this to home AAA. The home AAA sends the Access Request to the I-CSCF. The I-CSCF then sends the SIP Response onward to the P-CSCF.

From S-CSCF

Authentication. The need for UE authentication by the S-CSCF has already been identified by S3 and S2. We propose that DIAMETER be used for this functionality.

Authorization. The need for downloading subscriber profile information to the S-CSCF has also already been identified by S2. The S-CSCF will want to authorize the UE prior to downloading such information.

Accounting. Records of user activity should be sent from the S-CSCF to the HSS via DIAMETER.

Figure 4 shows a user performing SIP registration and a serving network S-CSCF using an AAA infrastructure to authenticate and authorize the user.

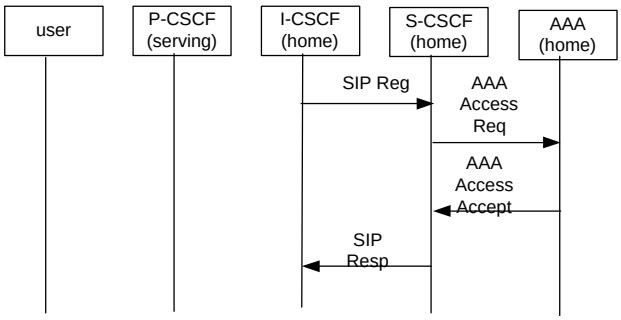

Figure 4: Example of S-CSCF and AAA

The S-CSCF uses the RAND and RES as above to authenticate the user with the home AAA via the visited AAA server.

Use of DIAMETER

We advocate the use of DIAMETER as a robust inter-domain AAA protocol among CSCFs. DIAMETER has been selected in other wireless networks for access control to both basic IP service and application-layer services.

NAI

The Network Access Identifier (NAI) should be supplied in the SIP REGISTER message and should be used for routing the request through the DIAMETER infrastructure towards the home network. The NAI is of the form `userID@example.com` where `example.com` is the user's home domain that is authenticating the user and authorizing service on the visited network. Settlement will eventually be made between the visited network and this home domain, possibly via the intervening brokers.

It would also be possible to include the entire SIP REGISTER message in the DIAMETER Access-Request that travels through the broker infrastructure. The home domain could then route the REGISTER message directly to the appropriate I-CSCF based on per-user policy. Note that this would imply routing based on NAI rather than DNS: an NAI should not be confused with a DNS name because the method of resolving it is the hop-by-hop routing through the AAA infrastructure, rather than a DNS query. Using the AAA infrastructure ensures that the request will be routed to a responsible home network with an established settlement relationship with some broker, rather than to a random SIP server somewhere on the Internet. Such use of AAA for SIP registration is for further study.

SIP-AKA

See Nokia's draft proposal S3-000456. We advocate extending SIP with AKA parameters and procedures. Also, DIAMETER servers should be augmented with the capability of verifying AKA credentials and returning session keying material to the proper SIP servers. AKA may need to be modified to reduce the number of round-trips required and to support fast re-keying in the visited network without additional round-trips. This issue is for further study by S3.

Session Keying Material

During registration, the session keys CK and IK should be distributed, as in basic AKA. These keys should be used to protect the confidentiality and integrity of subsequent SIP exchanges.

Authentication by Home AAA Server

It was decided that the Home AAA server should perform the actual authentication and authorization.

Recommendations

It is proposed that the above Diameter-AAA architecture be incorporated in 3G TR 33.8xxx and the requirements be forward to S2 for corresponding changes in TS 23.228 document and/or 23.002 as required.