3GPP TSG SA WG3 Security #29 **S3-030367**

15th – 18th July, 2003

San Francisco, CA, USA

Agenda Item: MBMS (7.20)

Source: Ericsson

Title: Access to Application Servers using HTTP in MBMS

Document for: Discussion/Decision

1. Introduction

At SA3#28 the impacts on introducing a new AKA procedure between the BM-SC and UE in MBMS was discussed. Several issues were raised as SQN problems with a new AKA procedure in MBMS and possibilities with sharing the authentication infrastructure with other services (e.g. use of bootstrapping function, re-use of IMS AKA in IMS and so on). The need to look into the authentication infrastructure for the case when the user is roaming and BM-SC is located in the visited PLMN was also raised.

This document discusses in chapter 2 and 3 the problems and solutions for potential SQN synchronization failure related to the re-use of AKA with several HTTP based applications. MBMS is one application where Ericsson foresees the need for HTTP support, for initial keying and possibly re-keying of the TEK. The document promotes architectural means to solve the problem. It is suggested that SA3 should take a working assumption that access to all such applications can be implemented using HTTP proxy as a centralized access point. Ericsson proposes to involve SA2 in these architecture discussions as soon as possible, as we see this as a general problem with several 3GPP services.

In addition, this document will also discuss authentication architecture for MBMS, when MBMS does not share the authentication infrastructure with other services, as requested by companies in SA3 #28.

Regarding the possibility to use the bootstrapping function in MBMS that has been developed in SA3 for services like Subscriber Certificates, no further evaluation is made in this contribution as it's unclear to Ericsson whether the NAF acts as a proxy between the UE and BSF. With the bootstrapping function the number of AKA procedures would not be decreased, as each application in this authentication infrastructure would still require that AKA is performed for each service.

The use of subscriber certificates in MBMS has never been discussed in SA3 and no such requirements exists in the [TS 33.246] for MBMS. It can also be noted that SA2 has commented to SA3 on the work on Mt reference point and Presence and it's relation to work on Subscriber Certificates in LS [S3-030210], that "dependencies on work, which is uncertain to meet the release 6 deadline should be avoided, given that the Mt reference point and Presence are important parts of release 6. This applies to dependencies with work done inside and outside 3GPP, in particular as the latter is outside the control of 3GPP." Ericsson believes that this comment applies to MBMS as well.

2. Problem statement

It seems that SA3 has a clear interest of re-using AKA with several applications. For this reason, all new applications that re-use AKA authentication, such as Presence Ut interface or MBMS, should consider carefully about the potential problems related to synchronization failures.

AKA authentication challenges need to arrive to USIM at specific order [TS 33.102]. Otherwise, USIM will generate a synchronization failure message.

For the freshness checking purposes, the AKA challenge includes a sequence number (SQN). The SQN space is divided into subspaces by using an index (IND). IND is part of SQN, and it refers to an array in the USIM where the highest used SQNs are stored. If every new SQN(IND) is greater than the previously used SQN with the same index value, then the freshness of the challenge is guaranteed. Implementations may also use a parameter L to set a limit to the highest acceptable difference between the new SQN and the highest previously accepted SQN anywhere in the array. Small

values in parameter L may cause more SQN synchronization failure problems if the same USIM is used with several applications.

Possibility that the USIM will reject a valid authentication challenge depends a lot on the USIM/ISIM implementation and how they are deployed. Since these issues are Operator dependent, they cannot be solved by SA3 without changing [TS 33.102]. Using the current specifications, there are still some ways to cope with the problem depending on the USIM/ISIM implementation. For example, one or more IND values from the SQN array in the USIM/ISIM can be dedicated for specific application. In theory, the maximum number of applications using the same USIM/ISIM is the size of SQN array. In practice, several IND values may need to be reserved for one application in order to find a balance between risks for synchronization failures, load of HSS, and frequency of authentication. Also, the number of AVs returned at a time to the entity requesting them is an important deployment decision.

Ericsson believes that the remaining means to solve the problem without changing USIM/ISIM standards boils down to following two:

1. Minimizing the number of network entities that are able to request Authentication Vectors (AVs) for the same USIM.

2. The frequency of authentication.

The next section describes how this can be achieved in HTTP context.

3. Solution 1

The number of network entities requesting AVs for the same USIM should be kept in minimum also in HTTP context. This can be achieved already now by centralizing the interface to HSS for fewer nodes in the implementations. It would also be possible to standardize such architecture in 3GPP.

Ericsson has studied solution based on the use of Reverse HTTP proxy. Term reverse proxy is often used to referee to certain alternate uses of a proxy server. For example, reverse proxy can be used outside the firewall to represent a secure content server to a client outside. It typically prevents unauthorized access to data inside secured network. In 3GPP context, the reverse HTTP proxy could be used both as an authenticator on behalf of Application Servers, and as a centralized access point to HSS in order to minimize the risk for potential synchronization failures with AKA SQNs.

The use of reverse HTTP proxy could lead to a centralization approach, in which all new interfaces using the same protocol could be implemented in a centralized node. For example, Presence/Ut interface and access to MBMS BM-SC will most probably all use HTTP as the transport protocol. In this case, the implementation strategy could be to provide access to all these functions via a HTTP proxy, see Figure 1. Because the interfaces towards HSS are now minimized, the danger of causing synchronization failures in the USIM is much less than if all different applications used separate interface. The interface between UE and HTTP proxy is protected using TLS. Only one TLS connection should be used between the UE and the HTTP Proxy even when communicating with several Applications Servers. The solution does not require new AV's for the proxy each time a new TLS connection is established if the HTTP Digest AKAv2 passwords are re-used.

HTTP proxy should be seen as a functional node rather than as a fixed network entity. If the Mobile Operator had only one Application Server, then the functionality of the proxy is not necessarily needed. This helps in creating different implementation strategies, e.g. having a migration path from one Application Server to several ones.

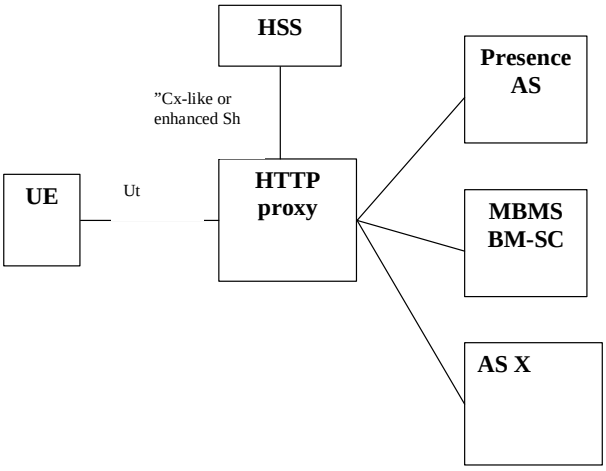


Figure 1: Optimized implementation of HTTP access to Presence AS and MBMS BM-SC

The same kind of implementation could be possible even if the UE was roaming in the visited network. In this case, the HTTP proxy in the home network would require also AAA server functionality, but it could still take responsibility of distributing AKA AVs in specific order in order to avoid synchronization failures, see figure 2. This requires enhancements for Diameter Multimedia application to work with AAA proxies; however, this work is already progressing in IETF [draft-belinchon-aaa-diameter-mm-app-01.txt].

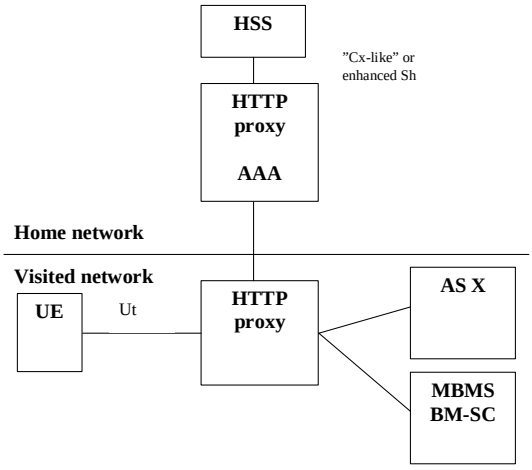


Figure 2: Optimized implementation of HTTP access to Application Servers in the Visited Network

The interface between HTTP proxy and the Application Servers could use TLS or NDS/IP (TS 33.210) in order to have more security. However, this should be a policy decision by the Operator. This interface should also be enhanced using similar approach that is currently used in IMS, i.e. allowing the proxy to communicate the asserted identity to the AS. This kind of extension should not be a problem because HTTP in general is considered as a "common good" and it already has been extended locally as well as globally. Several alternative solutions exist. For example, this could be achieved by including authentication specific information to HTTP cookies. More specifically, the cookies could include information about the authenticated identity, authentication method, time of authentication, session related information, access type (PS, CS, fixed) and even end-user IP-address information. Alternatively, some existing header could be re-used (e.g. some potential extension header from OMA) or a 3GPP extension header could be developed following the HTTP extension framework [RFC2774]. Also, the re-use of Authorization header to carry identity information could be considered.

The frequency of authentication may also affects to the deployment model that is used when USIM/ISIM is used for several applications. In the HTTP context, HTTP Digest AKAv2 passwords can be re-used if needed (see more details in Ericsson contribution related to AKAv2). However, the benefits of using of this mechanism are implementation dependent, and for this reason, the mechanisms should be seen as an additional tool for building Operator dependent security architecture rather than as a general mechanism.

3.1 MBMS

3.1.1 TEK distribution in MBMS

In MBMS a secured TEK distribution from the BM-SC to the UE needs to be considered as well in this architecture.

This architecture (see figure 3) would have hop-by-hop encryption. TLS would be used to protect the interface between the UE and the Proxy-Authenticator. The interface between the Proxy-Authenticator and BM-SC needs to be protected as well (e.g. NDS/IP (TS 33.210) or TLS), but this is an operator choice. Notice that end-to-end encryption of TEK from BM-SC to UE is not possible with this solution.

The protection of TEK would rely on the security provided by TLS. This means that network nodes, as HTTP Proxy in home and visited networks would get access to the TEK. MIKEY could still be used though with HTTP for TEK transportation. See flows in Annex A in this paper for further details.

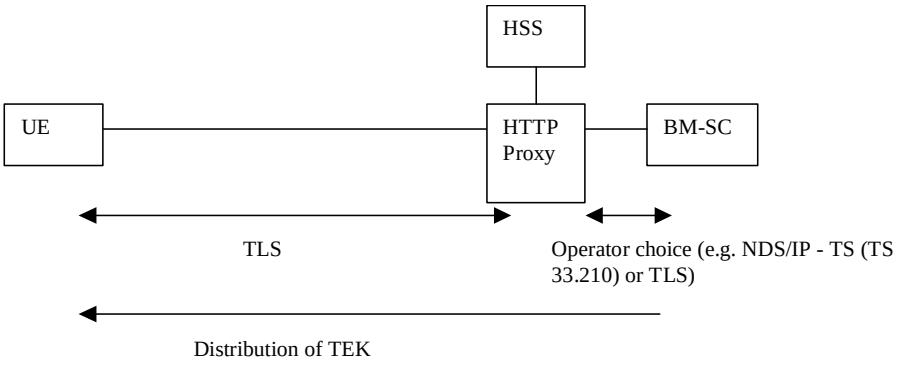


Figure 3 TEK distribution in MBMS

4 Solution 2

At SA3 #28 when [S3-030248] was presented, companies asked Ericsson whether the architecture when BM-SC is located in the visited PLMN has been considered in MBMS. If no shared authentication infrastructure with other services is used in MBMS, then Ericsson proposes the following architectures for 1) BM-SC located in Home PLMN; and 2) BM-SC located in Visited PLMN:

4.1 BM-SC located in Home PLMN

At SA3 #28 Ericsson presented in [S3-030248] the architecture in MBMS when BM-SC is located in Home PLMN.

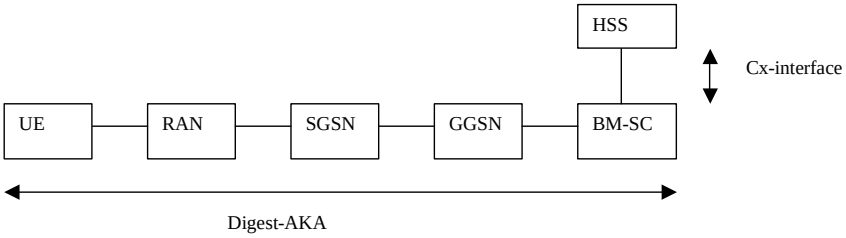


Figure 4 BM-SC located in Home PLMN

SA3 sent at #28 an LS to CN4 about the re-use of a Cx-like interface in MBMS. CN4 has responded in LS [S3-030337], where CN4 has responded that this is feasible but see two different options here, either 1. “Adding an AVP to the Cx

protocol or as a vendor specific AVP in Diameter Base Protocol"; or 2. "Each application having separate protocols based on Cx interface protocol (or not)". Enhancing the Cx could be more flexible instead of defining a new application for each node.

In this architecture, the frequency of AKA procedures in MBMS could be decreased by the re-use of password from Digest AKA v.2. as described in Ericsson contribution in [Re-use of password].

4.2 BM-SC located in Visited PLMN

When the BM-SC is located in a Visited PLMN, a AAA node in the Visited PLMN could act as a proxy and a AAA node in the Home PLMN could act as the authenticator.

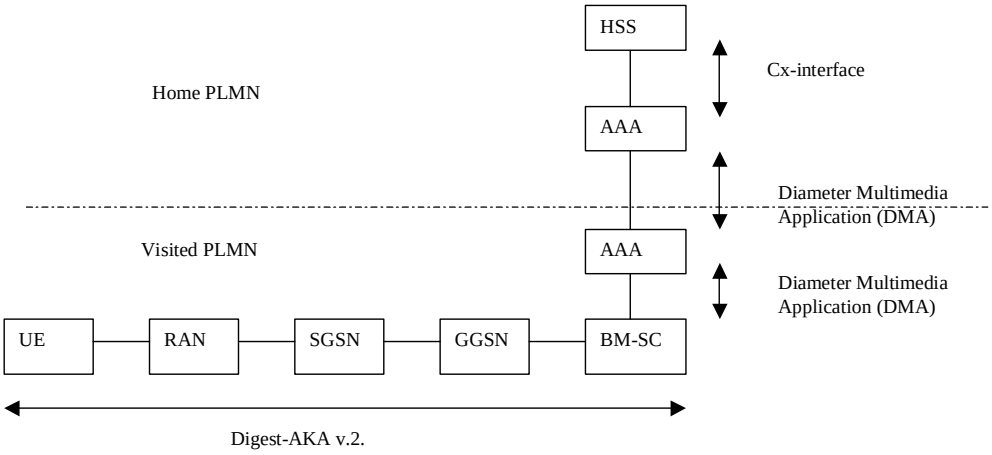


Figure 5 BM-SC located in Visited PLMN

It should be noted that the BM-SC requires the security keys CK (and IK) from the HSS. Currently Diameter Multimedia Application (DMA) does not support this, but IETF is trying to solve the key transportation in Diameter Multimedia Application (DMA). The same problem applies in WI WLAN inter-working.

In this architecture the frequency of AKA procedures in MBMS could be decreased by the re-use of password from Digest AKA v.2 as described in Ericsson contribution in [Re-use of password].

5. Recommendations

Ericsson proposes that SA3 takes a working assumption that access to all applications that use HTTP as a transport protocol, and that re-use AKA for authentication, can be implemented using a reverse HTTP proxy in order to solve potential synchronization problems as described in chapter 3 as solution 1.

SA3 should inform SA2 and CN4 that architectural means would play an important role when solving the problems related to potential SQN synchronization failures.

6. References

[TS 33.102] 3GPP, 3G Security; Security Architecture.

[TS 33.246] Security of Multimedia Broadcast/Multicast Service (Release 6), version 0.2.0.

[S3-030210] Response to LS (S2-030445) on use of HTTP between UE and AS in the IMS, from SA2.

[S3-030248] Authentication in MBMS, from Ericsson.

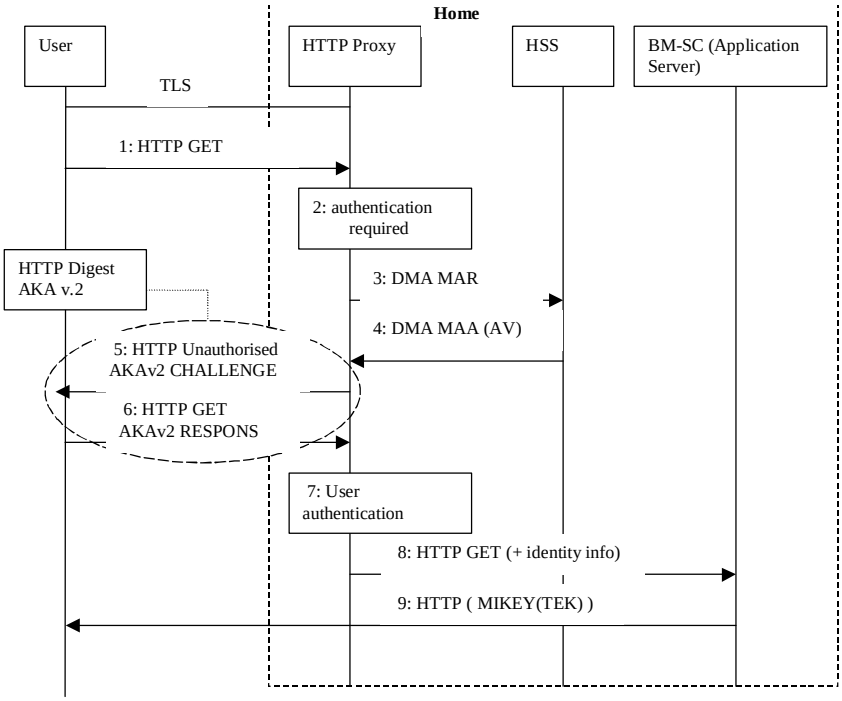
[S3-030337] LS on adapting Cx interface protocols for security purposes, source: CN4, N4-030722.

[S3-030xxx] HTTP Digest AKAv2 status and SQN issues, from Ericsson.

[draft-belinchon-aaa-diameter-mm-app-01.txt] Diameter Multimedia Application, IETF, Work in progress, June 16 2003.

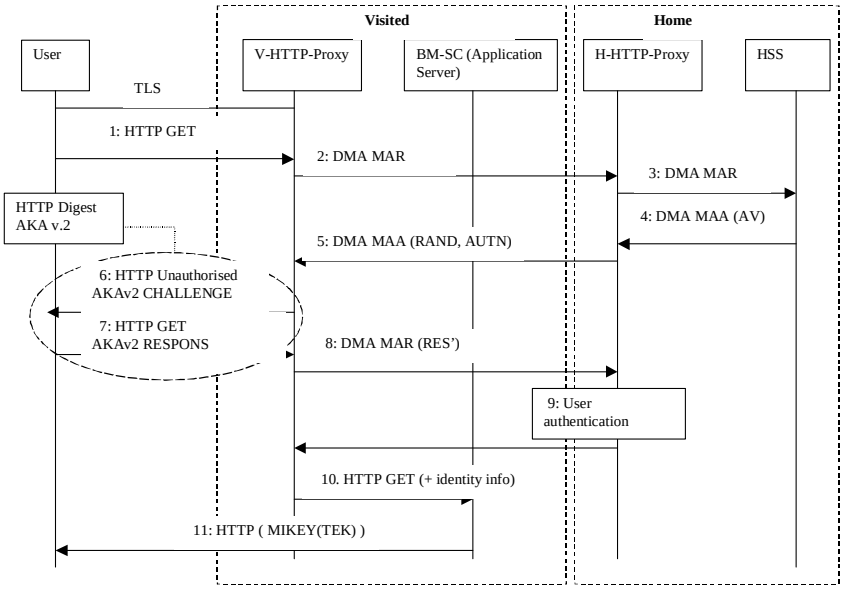
Annex A

A.1 Authentication proxy in home network:



DMA MAR & MAA: Commands of Diameter Multimedia Application currently developed in IETF, see more in (draft-belinchon-aaa-diameter-mm-app-01.txt).

A.2 Proxy of home network acts as Diameter server for the visited network:



DMA MAR & MAA: Commands of Diameter Multimedia Application currently developed in IETF, see more in (draft-belinchon-aaa-diameter-mm-app-01.txt).