3GPP TSG SA WG3 Security — S3#29 **S3-030403**
15 - 18 July 2003
San Francisco, USA

Source: **Siemens**

Title: **MBMS authentication architectures evaluation**

Document for: **Discussion and decision**

Agenda Item: **MBMS (7.19)**

Abstract

This paper provides an evaluation of possible authentication architectures for MBMS: direct AKA based [1] and BSF-based [2]. The conclusion is that further study is needed before deciding on this issue. Especially a general discussion is needed on Rel-6 authentication architectures. The outcome of this (i.e. guidelines or requirements) could useful in the evaluation of authentication solution for MBMS.

1 Introduction and terminology

During last SA3 meeting, S3-030248 [1] was presented by Ericsson and proposed a new authentication procedure based on AKA supported between the BM-SC and the UE. It was considered that the bootstrapping function and the visited network case need to be analysed before deciding on the proposal. This contribution analyses the use of BSF in the context of MBMS and compares this with [1].

Before starting the architectural discussion and implications, a short description is given. This tries to clarify how the BSF may fit into the MBMS architecture (see also figures from section 2) and fixes some definitions used within this paper.

Before the MBMS-UE is able to obtain a TEK[1], he needs to share a security association (SA; contains KEK[2] among other parameters) with the BM-SC that can be used to protect the TEK transfer. This SA may be established by http-digest-AKAv2 each time a TEK need to be distributed (as proposed in [1]) or may be established prior to the TEK distribution. An example of the latter is to base it on BSF derived secrets. For a BSF-based authentication in MBMS, the BM-SC will take the role of a NAF[3]. These BSF derived secrets could be used by the BM-SC for several TEK distributions. In order to generate BSF secrets, the MBMS user needs to run http-digest-AKA with the BSF according to protocol A [2], and the BM-SC needs to retrieve the secret according to protocol D [2]. The BM-SC shall be able to decide on the lifetime of the received secrets (SA).

The required functionality for TEK distribution is independent on the requirement for a hierarchy of KEKs. Any further KEKs (I.e. those shared by a subset of UE's), can be transferred by the BM-SC over the SA created by both authentication approaches (BSF-based or direct-AKA based), using the UE-specific KEK to protect the transfer. Any TEK distribution to a specific UE needs a UE-specific KEK, while distribution to a group needs a shared-KEK. This paper only focuses on the issues for generation of a UE-specific KEK.

---

[1] Traffic Encryption Key

[2] Key Encryption Key

[3] Operator-controlled network application function functionality

It should also be noted that authentication based on subscriber certificates, or coupled with IMS are other alternatives. These however have not been analysed. The first one while certificates based authentication introduces extra performance requirements and delays with respect to secrets based authentication. The latter one while MBMS should not rely on the presence of IMS.

2 Overview of different Architectures

In this section an overview of the possible configurations is given. In order to ease the analysis-text provided by section 3, each possible configuration is named *'Arch-X'* with X being assigned a number.

2.1 BM-SC in Visited Network

Stage-1 specification TS 22.146 contains following requirement in section 5.3:

> *'In case of roaming a user should also be able to subscribe and join Multicast Services that are provided locally in the visited network, as allowed by the user's home environment.'*

Stage-2 specification TS 23.246 contains currently only *one little note* on the visited network placement of the BM-SC in section 10:

> "It shall be possible to collect charging information for the multicast mode. It shall also be possible to collect charging information for MBMS services in visited networks."

So far SA3 had not taken into account the placement of the BM-SC in the visited network.

2.2 BSF based configurations [2]

The different configurations which base on BSF derived secrets can be summarized in following table according to the placement of the different servers in the Network:

NE placement	**BM-SC in HN**	**BM-SC in VN**
BSF –HN	Arch-A	Arch-B
BSF –VN	---	Arch-C

Arch-D (BSF in VN but BM-SC in HN) has not been considered as it provides an un-natural configuration.

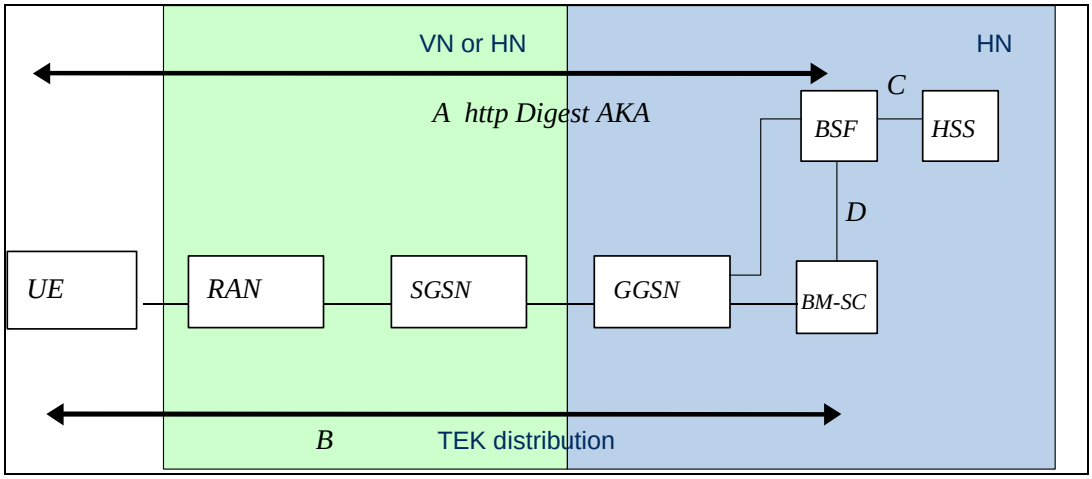

Figure 1: Solution with BSF and BM-SC in HN (Arch-A).

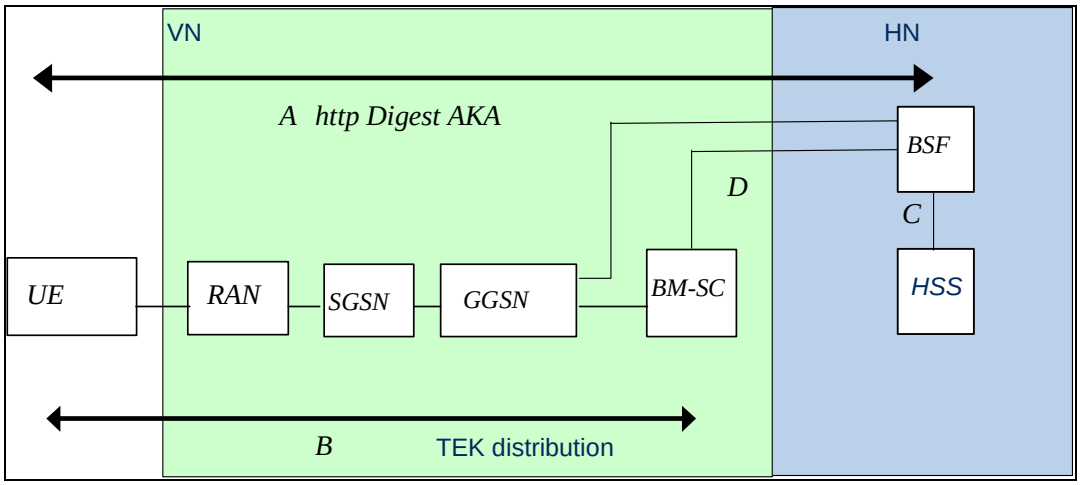

Figure 2: Solution with BSF in HN and BM-SC in VN (Arch-B)[4].

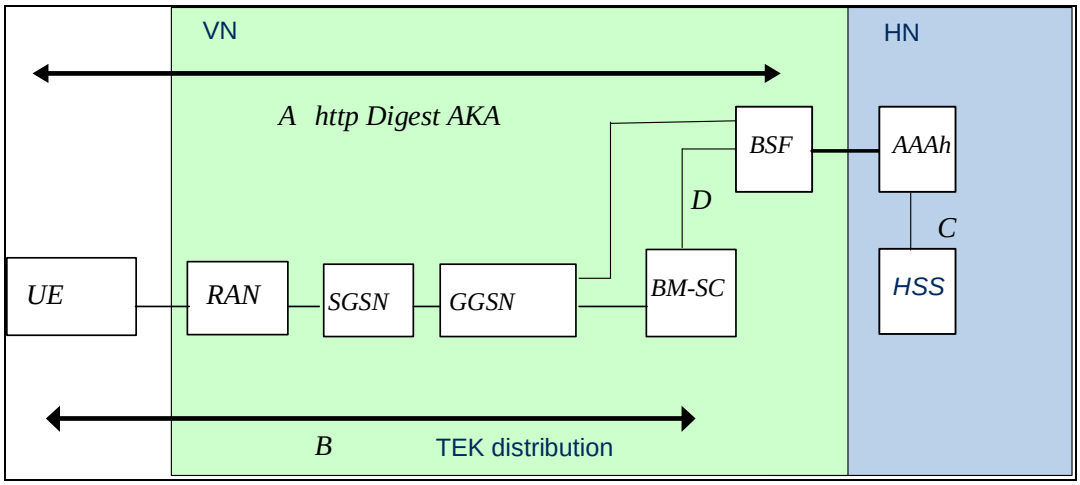

Figure 3: Solution with both BSF and BM-SC in VN (Arch-C)

[4] This picture has been simplified. Two different GGSN might be involved. For the BSF run, a GGSN in the HN, and for the TEK distribution a GGSN in the VN.

2.3 Direct AKA based configurations [1]

Following configurations are possible:

NE placement	BM-SC in HN	BM-SC in VN
	Arch-F	Arch-E

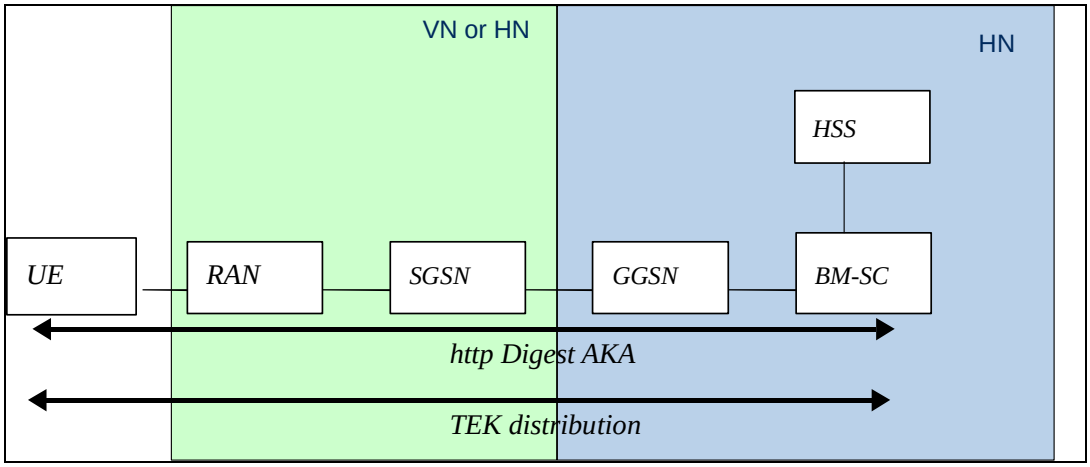

Figure 4: Solution from S3-030248 for BM-SC placed in HN 'Arch-E'

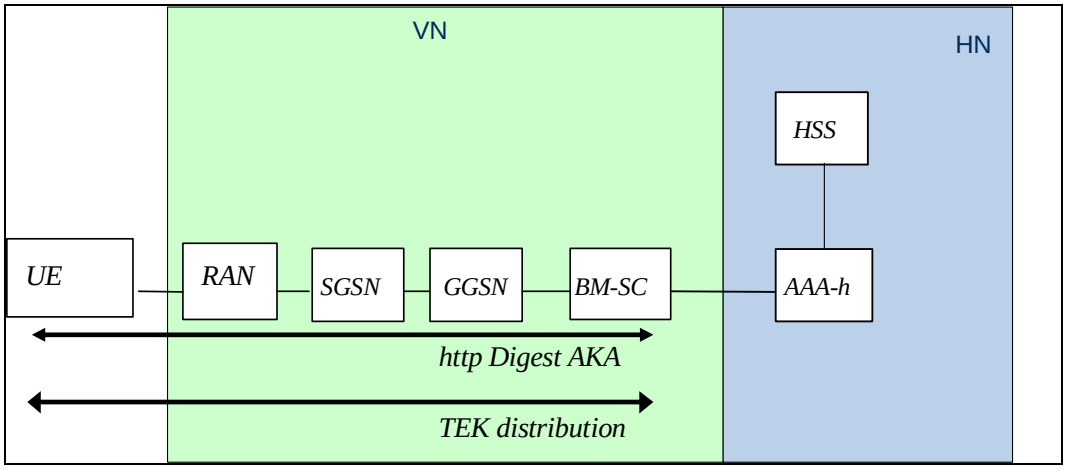

Figure 5: Solution from S3-030248 with BM-SC placed in VN 'Arch-F'

3 Evaluation

3.1 Approach

In this clause a comparison is done between Arch-A, and the solution proposed by Ericsson in S3-030248 [1] which we called Arch-E in section 2. This comparison will contain the basic differences of both approaches. Some additional complexities introduced due to BM-SC in a visited network (Arch-B/C) and [1] applied for the VN (Arch-F) are mentioned whenever applicable.

At first sight, as an extra node (BSF) is involved, the authentication interworking for Arch-A seem to be more complex then in Arch-E. It is analysed if these drawbacks can be compensated by some optimisations/benefits. First a look is taken to authentication relevant issues in section 3.2, thereafter general issues are analysed in section 3.2

3.2 Evaluation against authentication relevant issues

A companion Siemens contribution to this meeting proposes that the below listed guidelines *(G-x)* are taken into account for all features currently being specified for 3GPP Release 6, and features in future releases. This therefore could also be applied to MBMS authentication solutions. Whenever applicable these guidelines will be referred to.

G-1. The number of nodes and the number of different types of nodes with access to authentication vectors should be limited in order to reduce the possibility of illegitimate access to authentication vectors.

G-2. The number of different types of interfaces to the HSS should be limited in order to keep the complexity of the HSS low.

G-3. For reasons of HSS and AuC-performance, the number of authentication vectors requested from the authentication centre as well as the number of requests should be kept low. Mechanisms which make economical use of authentication vectors should be preferred.

G-4. The number of authentication domains as well as the number of nodes within a domain for which authentication vectors for one user are stored and not forwarded should be kept small. This is to avoid frequent re-synchronisation.

G-5. Mechanisms which ensure in a uniform way that the same client credentials are not used in different contexts should be preferred in order to prevent man-in-the-middle attacks in tunnelled authentication.

Start of evaluation:

Issue-A. Timing of the MBMS user authentication/SA creation for use at TEK distribution:

a. Arch-A: The UE needs to initiate the A-interface protocol ***separately*** towards the BSF in order to generate an SA that it can share with the BSF. The initiation of the A-interface protocol may be done independently from the TEK distribution (e.g. whenever a PDP context is available; the same PDP context could be used for the joining as well as for the A-Interface authentication (the creation of BSF secrets)).

b. Arch-F: There are ***no independent flows*** between the AKA authentication and the TEK distribution. In case the BM-SC has no valid SA available this may add delays to the execution of the TEK distribution in case there are problems with AV retrieval.

c. Guidelines: This indirectly refers to G-3 as independent flows provide a slight conceptual advantage in fulfilling the design goal to specify an authentication concept that allows a more time-spread AV's retrieval.

Issue-B. Authentication delays affecting the TEK distribution.

a. Arch-A: The generation of the 'BSF secrets' may be done once (e.g. some time before the TEK distribution) or whenever the BM-SC decides. The 'BSF secrets' shall be removed from the BSF at retrieval and the SA (including KEK) shall be deleted at the BM-SC after the user leaves explicitly the MBMS-service or when its lifetime expires (BM-SC setting etc…). The delay of the BSF secrets generation will add to the TEK distribution delay if the BM-SC has not proactively (some time before) informed the UE about the necessity of a fresh BSF-secret. A carefully designed concept may minimise the TEK distribution delays to a minimum. The BSF-concept has the potential to reduce the delays to a minimum.

b. Arch-F: A full authentication may need to be done before the TEK distribution. The HSS/HLR may need to be able to respond to a **burst of AV-retrievals** causing additional delays to the TEK distribution. The BM-SC has to implement some logic to handle this, as well as the AuC does. A possible measure for avoiding this is to proactively retrieve AV's and store them in the BM-SC. This however may also lead to more re-synchronisations due to interleaved authentications and the use of more AVs than needed when BM-SC deletes the stored ones when the user leaves the MBMS-service. Another measure (similar as the BSF-case) is to derive some Security Association *that can be reused* at the BM-SC and the UE to avoid the extra delays due to AV-retrieval.

c. Guidelines: This refers to G-3 and G-4

Issue-C. The number of needed authentication vectors

a. Arch-A: The AV consumption will be limited (one up to a few dependent on the BM-SC settings).

b. Arch-B: For each Authentication (during TEK distribution), an AV will be consumed if no optimisation are included (See Issue-B) for reusing an existing SA.

c. Guidelines: This refers to G-3

Issue-D. Interleaving authentications causing authentication re-synchronisations

a. Arch-A: One or a few BSF nodes will retrieve AVs. Reserving one array element for BSF based authentication avoids effects to other authentication domains.

b. Arch-F: The number of BM-SC nodes in a network is expected to be more then the number of required BSF-nodes. It will require at least one array element (if there would exist many BM-SC) in addition to the BSF for subscriber certificates enrolment.

c. Guideline: This refers to G-4

Issue-E. The storage of secrets respectively AV's within the BM-SC.

a. Arch-A: A hacker compromising the BM-SC and retrieving KEKs is able to compromise the MBMS-service but not the other service domains. (TEK, KEK can all be retrieved and MBMS users can be impersonated). To rectify the consequences of this attack (after being detected) the BM-SC has to ask a new BSF secrets generation and generate new TEKs. The Interface between the BSF and the BM-SC shall be secured (this could be an inter-operator interface for the VN-cases)

b. Arch-F: A hacker compromising the BM-SC and retrieving AVs may be able to use this AV (once) towards the other service domains. To rectify the consequences of this attack (after being detected) the BM-SC has to generate new TEKs.

c. Guideline: This refers to G-1

Issue-F. Storage of a shared secret at the TE

a. Arch-A: If a hacker can obtain a BSF generated secret from the TE, then he can impersonate the MBMS-user for MBMS access. A hacker that manages to obtain the BSF secret (e.g. Rogue terminal), is also able to obtain current and future TEKs (within the validity period of the BSF secrets).

b. Arch-F: There is no additional shared secret that needs to be managed unless optimisations are incorporated to reduce AV-consumption. In case of optimisations the same issues as with Arch-A apply.

3.3 Evaluation against non-authentication relevant issues

Issue-G. Finding the authenticator

a. Arch-A: The UE needs to find the BSF which is trusted by the BM-SC. This addressing information may be supplied to the UE during MBMS-service subscription (this may be automated or may be manual). This is a similar issue as with the Subscriber certificates enrolment, the same techniques may therefore be used.

b. Arch-F: The BM-SC acts as authenticator. No separate addressing is needed.

Issue-H. The processing load caused by authentication on UE, BM-SC and HSS

a. Arch-A: is mainly proportional to the number of joined MBMS services.

b. Arch-F: is proportional to TEK-distribution frequency per joined MBMS service if no optimisations are incorporated (as suggested by issue-B) otherwise similar to arch-A.

c. Guidelines: This refers to G-3

Issue-I. The reuse of Rel-6 functionality and timing issues

a. Arch-A: BSF-HN functionality needs to be specified within Rel-6 functionality (Rel-6 timeframe is March 2004 for Stage 2). As this is a basic component of the subscriber certificates architecture it can be expected that this functionality can be specified on time.

b. Arch-F: There are no dependencies except if AKAv2 [1] would be used. The RFC shall be ready on time and is out of control of 3GPP.

Issue-J. Required authentication protocols at the TE

a. Arch-A: HttpDigest AKAv1 for use in protocol A (BSF- UE) which is available already if the UE has IMS client-functionality or BSF client-functionality for the subscriber certificates feature.

b. Arch-F: HttpDigestAKAv2 as proposed by [1] for use in between BM-SC and UE. This would be additional AKA functionality that is needed in the UE and would affect HSS. 3GPP may need to check the provided ietf-draft against the claimed security improvements.

Issue-K. Interworking complexity

a. Issue-S1: How can the BM-SC select the right SA for TEK distribution or initiate renewal?

    i. Arch-A: It shall be assured that the BM-SC can indicate to the UE that it needs to generate new BSF secrets (New SA).

    ii. Arch-F: There seem to be no such issues.

b. Issue-S2: The need for the UE to support multiple simultaneous PDP contexts.

    i. Arch-A: if BSF based architecture are allowed where BM-SC reside in the VN and the BSF resides in the HN, then the UE should support simultaneous PDP contexts.

    ii. Arch-B: There are no such issues.

4 Conclusion

No clear decision can yet be made in favour of a BSF based authentication [2] or a direct AKA-based authentication [1]. The BSF based authentication performs better with respect to authentication relevant issues whereas the direct-AKA based authentication has less inter-working complexity.

Following issues were identified:

- Optimizations to the direct AKA-based authentication shall be done along the included guidelines (G-x). Care has to be taken to avoid bursty retrieval of AVs towards the AuC. This is applicable to both analysed solutions.
- For the BSF-based approach it has been identified that BM-SC[5] shall be able to indicate to the UE that a new BSF key generation is needed within protocol-B. Another Siemens contribution to this meeting details similar requirements for protocol-B when used for subscriber certificates enrolment.

Further work is needed to understand the architectural consequences for a BM-SC located in the visited network:

- Further progress on the BSF architecture may give further insights for the reuse within MBMS.
- Currently stage 2 MBMS focus seems rather on GGSN and BM-SC in the HN.

Siemens proposes to further study the different authentication alternatives taking into account the suggestions made by this contribution. Especially a general discussion is needed on Rel-6 authentication architectures. The outcome of this (i.e. guidelines or requirements) is useful in the evaluation of authentication solution for MBMS.

[5] T*he need for re-authentication may be managed by the BM-SC i.e. initiation of re-authentication after e.g. a fixed number secret based authentications (TEK/KEK distributions using a ptp KEK) or a certain amount of time.*

5 References

[1] S3-030248: Authentication in MBMS, Ericsson, SA3#28 Berlin, Germany

[2] S3-030317: TS on Subscriber certificates and Bootstrapping Server, SA3#29, San Francisco, USA