3GPP TSG SA WG3 Security — S3#25 **S3-020538**
8 - 11 October 2002
Munich, Germany

Title: **MBMS Security Architecture Proposal**

Source: **Nortel Networks**

Agenda Item: **7.19**

1. Introduction

In this proposal, we propose mechanisms for MBMS user authentication, authorisation and data encryption.

2. Assumptions

The mechanisms proposed in this document are based on the following assumptions about the way in which MBMS services will be developed and deployed:

- There is no single standardised MBMS client for the UE. Services, or service types, will have a client component, which is installed on the UE, and a server component, which is the BM-SC.
- Different services, or types of service, may be supported on different BM-SCs.
- The ciphering key shall be common to all users receiving the same MBMS service. Ciphering key cannot be specific to a particular user.
- The ciphering key used at any given moment shall be the same for the whole MBMS distribution tree so that a UE is not obliged to get a new cipher key each time it changes its location within a same MBMS distribution area.

3. Authentication and Authorisation

Before a user can access an MBMS service they must be authenticated and an authorisation decision taken as to whether this particular user is entitled to access this particular service. In addition, an authorisation decision must be taken with respect to the MBMS service information, such as Quality of Service, MBMS service area, that the user has requested, namely that it must be the correct for the service (or negotiated to a correct value). We propose that the MBMS service authentication and authorisation be done by the BM-SC as described in this section

Following the service announcement, a UE wishing to receive the service contacts BM-SC using ~~the~~ a standard unicast PDP context and an application-specific protocol. The BM-SC performs the authentication and authorisation exchange with the UE.

Once the user is authenticated and authorized, the BM-SC sends a service token to the UE. The UE uses this service token, to activate the PDP Context. The GGSN would use this service token to confirm the validity of the ~~service token~~PDP Context request through an interaction with the BM-SC. ~~and to request/negotiate~~The GGSN obtain the MBMS service information during the same interaction. Once the GGSN receives a successful response from the BM-SC, the PDP Context establishment is completed.

There may be a requirement for subscription information in the HLR indicating whether a particular user may access MBMS services, or all users may be allowed to attempt MBMS service invocation

The protocol message flows are subject to further contributions, based on the acceptance of the proposed solution.

4. Encryption

We propose that encryption be handled at the application layer. That is, the content server distributing the content performs the encryption.

This approach has a number of advantages:

- the encryption scheme can be tailored to the particular application. For example, some applications may send several data streams encrypted using different keys for users with different subscription levels to the service.
- reduced impact on network elements (e.g. RNC, SGSN)
- flexibility in update of encryption schemes (does not require a network upgrade – rather it is the responsibility of the service, and is not visible to the GPRS network elements)
- faster time to market – encryption schemes do not need to be standardised, as they are a matter for the application developers

The GPRS network simply distributes the data provided by the content provider, with no encryption.

5. Key distribution

After successful completion of the authentication and authorisation, the BM-SC should support the possibility of securing the MBMS data. This ~~could be~~is accomplished by having the BM-SC to distribute and manage the ciphering keys. However, the key generation may be controlled by the Service Provider, so that, the MBMS service accounting is accounted for. When a user leaves a multicast session, the BM-SC may decide to distribute new keys (key refresh process).

Various approaches to key management are possible. As with the encryption, we propose that these be left to the application layer.

Keys can be refreshed when users leave/join the service, either through direct interaction with each UE over a point to point PDP Context or inband in the MBMS data using standard multicast key management techniques such as Logical Key Heirarchy.

Alternatively, keys could be refreshed on a periodic basis. For example, where users subscribe to a service for a period of days, weeks or months, then the points at which users ‘leave’the service are synchonised at the end of each day, week or month. It is sufficient only to change the keys at those points in time.

6. Encryption

~~6 Proposal~~

It is proposed that the following functions be carried out at the application layer (between UE and BM-SC/Content server):

- Authentication
- Authorisation
- Encryption

- Key generation and distribution

Standardistion of the application layer for MBMS has not yet been discussed as part of the MBSM discussions. There are three possibilities:

- 3GPP will standardise the application layer interface between MBMS client (on the UE) and MBMS Server (BM-SC/Content server).

  This will involve detailed definition of the media stream formats and of the application protocol between client and server.

  In this case the above four items will need to be addressed in detail.

- 3GPP does not standardise the application layer

  In this case, application designers will be free to address the above four issues in a way appropriate for their own application. There would be no need for further work in 3GPP on these items.

- 3GPP does not standardise the application layer, but does study how some existing applications could be used as the application layer for MBMS (e.g. PSS or IMS).

  In this case, application designers would be free to either design their own protocol/media stream formats, or reuse the clients and servers defined for PSS or IMS.

If it is agreed that these are application layer functions, it is proposed to reply to SA2 clarifying this, and asking for guidance on what, if any, standardisation should be carried out by SA3.