3GPP TSG SA WG3 Security — S3#26 **Tdoc S3-020642**

19th – 22nd November 2002, Oxford, UK

Source: **Hutchison 3G UK**

Title: **Proposed message flows for joining a multicast service**

Document for: **Discussion / Decision**

Agenda Item:

Introduction

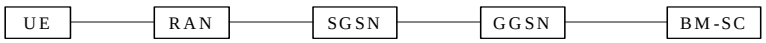
The multicast mode of the MBMS has a clear requirement to deliver data only to those users who are entitled to receive a specific multicast service. To address this requirement, the security of MBMS needs to provide the following capabilities:

- Ensuring only valid users are allowed to join a multicast service
- Distributing and updating the keys needed by the users.
- Protecting the data during transmission.

This contribution looks at the high level flows necessary to achieve the first capability. It does not cover the full details of those flows. The contribution also does not address the issue of how to distribute keys to the authorised users or protect the data during transmission.

Architecture

The following is an overview of the architecture used in this document. The BM-SC represents the logical element that delivers Broadcast/Multicast data to the GGSN. The actual multicast data could be provided to the BM-SC by another source.



Choices made in designing message flows

This section describes the choices made in designing the high level message flows for a user joining and leaving a multicast service.

Before a user is allowed to join a particular multicast service, they must be both authenticated and authorised. There could be considered two different levels of authentication and authorisation needed for a multicast service, firstly to get access to a bearer to carry the data and secondly to access to the service.

The SGSN provides a method of both authenticating and authorising the bearer and clearly this should be used. The re-use of this authentication to provide authentication at the service layer is a good optimisation, as it avoids the need for a second authentication method. This means the SGSN will be responsible for authenticating a user and authorising the use of the bearer.

To allow operators sufficient flexibility to offer a rich and diverse set of multicast services, we believe that the service level authorisation should fulfil at least the following requirements:

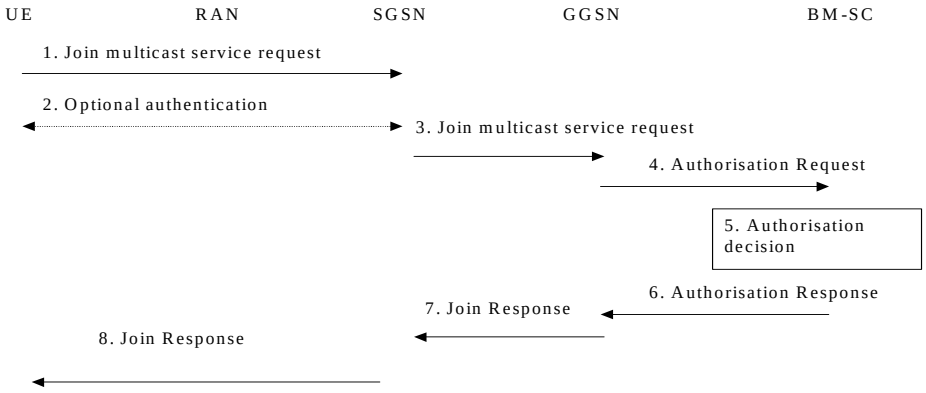
- Allow a user and/or operator to tailor the multicast services available to users on an individual basis.

- Allow a user to subscribe to a multicast service and instantly get access to the data transmitted on that service (e.g. a user goes to a web page to modify the set of multicast services they want available on a subscription basis and within a few minutes they can access that multicast service).
- Allow an operator to rapidly create a new multicast service and make it available to users.

We believe that the BM-SC is most appropriate element to fulfil these requirements, as it offers the flexibility to modify the set of multicast services available to a user independently of the transport network. The disadvantage of using the BM-SC are the need for additional signalling traffic compared to authorisation at say the SGSN. Hence it is proposed that the BM-SC holds the service level authorisation information.

Authentication and Authorisation

This section considers the flows that allow a user to join a Multicast Service and the network to authorise a user. The contribution only considers the flow form the security perspective and does not go into the details of the set-up of bearers etc, as this is outside the scope of security. It is necessary to perform this security functionality at the set-up of the bearer.



The above steps proceed as follows

1. The UE attempts to join a particular multicast service.

2. The SGSN is responsible for authenticating the user and hence can initiate a standard 3GPP authentication, if it chooses to do this. An unsuccessful authentication results in the SGSN rejecting the UE request. The SGSN also performs the normal bearer authorisation.

3. The SGSN passes the join request on to the GGSN.

4, 5 and 6. The GSGN uses the BM-Source to authorise a subscriber to a particular MBMS service. This could be done by either interrogating the BM-SC for each subscriber or downloading the subscriber information to the GGSN. The actual method is ffs. The transfer of identity from the GGSN to the BM-SC or authorisation from the BM-SC to the GGSN needs to be secured.

7. The join response message is sent from the GGSN to the SGSN.

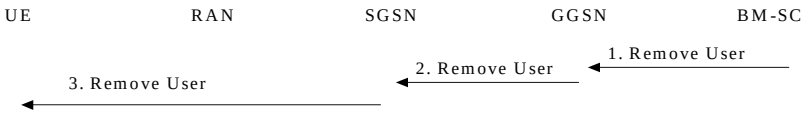
8. The response message is sent from the SGSN to the UE.

A UE that has successful joined a multicast service requires the relevant keys for that service. These keys could be sent in the above flows, but should be considered as part of the key management process.

Network Initiated Leaving

It should be possible for the network to remove a user from the multicast service, if that user is no longer authorised to receive the multicast service (either because of PS domain reasons or the users subscription has run out at the BM-SC). It is important to remove the bearer as well as ensure the user

does not have the latest transport keys for the multicast service, as data will be transmitted to that user on the bearer whether the user has the correct keys or not.



1. The BM-Source informs the relevant GGSN that it wants to remove a user.

2. The GGSN informs the relevant SSGN that it should remove a user

3. The SGSN removes the user from the multicast service.

Note: The flows could start with this message 3, if the SGSN initiates the removal of the user.

Note: The flows could be used to remove all the users, i.e. close a multicast service, if required.

Conclusion

This contribution proposes some high level flows for the authentication and authorisation of a user joining a multicast service. It also includes some flows for the network to remove users from a multicast services. It is proposed to add the attached psuedo CR to the MBMS TS.

3GPP TSG SA WG3 Security — S3#26
19 - 22 November 2002, Oxford, UK

Attachment to S3-020642

CR-Form-v7

CHANGE REQUEST

⌘ **33.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.0.2** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Joining message flows
Source:	⌘	H3G
Work item code:	⌘	MBMS
Date:	⌘	12/11/2002
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Proposed message flows for a user joining a multicast service
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.1.1

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

********** First Change **********

5.1 Authenticating and authorizing the user

As part of joining a multicast service, the UE establishes a PS domain bearer to carry the data transmitted in a multicast service. Part of the process of establishing this bearer is mutual authentication between the network and the UE. This authentication is provided by the UTMS AKA (see [4]) protocol.

MBMS shall use this network layer authentication procedure to provide authentication of a UE attempting to access a mulitcast service. Furthermore in addition to the normal bearer authorisation provided by the PS domain, there will be a service level authorisation (subscription check) provided by the BM-SC to ensure the UE is allowed to join that particluar multicast service. A failure in the authentication or either of the authroisation shall result in the both the UE not joining the multicast service and the bearer not being established.

Section 6.1 contains the flows describing how a UE joining a multicast service is authenticated and authorised.

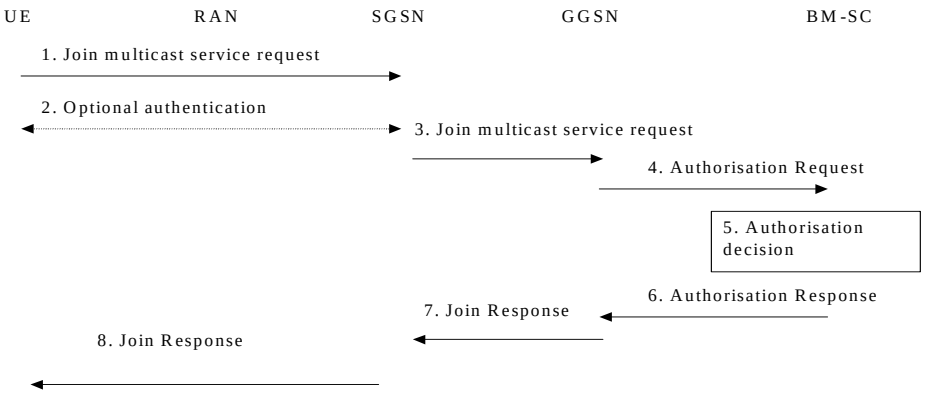
~~The user and the network could mutually authenticate each other using the AKA protocol that is used for standard point-to-point communication. Once authenticated, there should be an authorisation to determine whether a particular user is allowed to access that particular multicast service or not, e.g. some multicast services may be only available to some users.~~

********** Next Change **********

6.1 Authentication and authorisation of a user

~~Editor's note: this section will contain the details of how a user joins a particular Multicast Service~~

This section describes the process of a user joining a multicast service. The process relies on the standard 3GPP process [4] security procedures for establishment of a bearer except the keys provided by AKA are not used to protect the user plane over the air interface (the management of keys to protect the user plane for a multicast service is covered in section 6.2). In addition to this security, there is also a subscription check performed using data stored in the BM-SC. Figure xx details the joining procedure.



The steps proceed as follows

1. The UE attempts to join a particular multicast service.

2. The SGSN is responsible for authenticating the user and hence can initiate a standard 3GPP authentication, if it chooses to do this. An unsuccessful authentication results in the SGSN rejecting the UE request. The SGSN also performs the normal bearer authorisation.

3. The SGSN passes the join request on to the GGSN.

4, 5 and 6. The GSGN uses the BM-Source to authorise a subscriber to a particular MBMS service. This could be done by either interrogating the BM-SC for each subscriber or downloading the subscriber information to the GGSN. The actual method is ffs. The transfer of identity from the GGSN to the BM-SC or authorisation from the BM-SC to the GGSN needs to be secured.

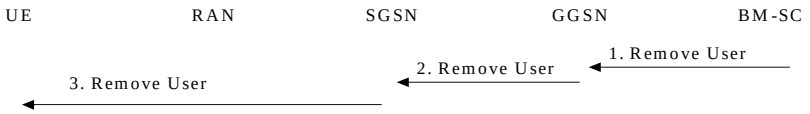
7. The join response message is sent from the GGSN to the SGSN.

8. The response message is sent from the SGSN to the UE.

A UE that has successful joined a multicast service requires the relevant keys for that service. These keys could be sent in the above flows, if necessary.

6.1.1 Network initiated leaving

It is possible that a user's subcription will expire and the user will no longer be authorised to access the multicast service. Under these circumstances the BM-SC would remove the user from the multicast service, if the user is currently accessing the service. Figure xx details this procedure.



1. The BM-Source informs the relevant GGSN that it wants to remove a user.

2. The GGSN informs the relevant SSGN that it should remove a user

3. The SGSN removes the user from the multicast service.

Note: The flows could start with this message 3, if the SGSN initiates the removal of the user.

Note: The flows could be used to remove all the users, i.e. close a multicast service, if required.