3GPP TSG SA WG 4 Meeting 118-e TDoc S4-22xxxx

Electronic, 6th–14th April 2022

**Title: LS on Security architecture for 5G multicast/broadcast services**

**Response to: —**

**Release: Rel-17**

**Work Item: 5MBUSA**

**Source:** **3GPP SA4**

**To:** **3GPP SA3**

**Cc: SA2**

**Contact person: Richard Bradbury**

 **richard dot bradbury at bbc dot co dot uk**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** —

# 1 Overall description

*SA4 provides a progress update on the 5MBUSA work item and has some questions regarding the security architecture for 5G multicast/broadcast services.*

## 1.1 Progress update on User Services architecture for 5G multicast/broadcast services

In relation to the Release 17 normative work item 920010 ("5G Multicast-Broadcast User Service Architecture and related 5GMS Extensions"), SA4 would like to inform you that **TS 26.502 V17.0.0** was agreed at the recent SA#95-e plenary meeting.

This specification includes the stage 2 design of the MBSF and MBSTF functions defined by SA2 in TS 23.247 but delegated to SA4. As well as a **static domain model** (in clause 4.5) and a **dynamic life-cycle model** (in clause 4.6) for these two functions, and a set of informative **protocol stack diagrams** for the user plane operation of the MBSTF (in annex B), TS 26.502 defines the following Network Function services they expose, *viz:*

- Nmbsf service operations exposed by the MBSF to the AF at reference point **Nbm10** (in clause 7.2).

- Nmbstf service operations exposed by the MBSTF to the MBSF at reference point **Nmb2** (in clause 7.3).

Furthermore, at its SA4#117-e meeting SA4 has reviewed draft Change Requests to TS 26.502 intended for presentation at SA#96-e in June. These add **procedural call flows** and providing essential additions to the aforementioned static domain model.

## 1.2 Security architecture for 5G multicast/broadcast services

SA2 has brought to SA4’s attention a recent update to TS 33.501 V17.5.0 that defines a security architecture for 5G multicast/broadcast services in annex W.

Having reviewed this annex, SA4 has the following comments and questions for SA3 regarding annex W of TS 33.501:

**Question 1:** Which of the following primitives fall within the scope of “security protection” that may be applied to MBS traffic: encryption, integrity, authenticity or non-repudiation.

**Commentary:** *It would be helpful if clause W.1 of TS 33.501 were to define the meaning of “security protection” as it applies to 5G multicast/broadcast services.*

**Question 2:** Does SA3 intend to specify at which layer in the protocol stack these security primitives are applied by different Network Functions involved, such as the MBSTF and/or MB-UPF?

**Commentary:** *If SA3 does not indent to specify these things, it would be helpful if clause W.1 of TS 33.501 were to clarify that these aspects are left to other specifications.*

**Question 3:** Can security protection be applied to both Multicast MBS Sessions and Broadcast MBS Sessions?

**Commentary:** *The heading of clause W.4 of TS 33.501 implies that security mechanisms apply to all MBS traffic, but clause W.4.1.2 refers only to “multicast session security”. It would be helpful if this ambiguity could be resolved.*

**Question 4:** When “locally configured policy” demands that security protection is applied, but information provided by the AF demands that security protection is not applied, what is the intended outcome? Conversely, when information provided by the AF demands that security protection is applied, but “locally configured policy” demands that security protection is not applied, what is the intended outcome?

**Commentary:** *It would be helpful if clause W.4.1.2 included a clear, unambiguous precedence rule to specify the intended outcome when the security protection requirements of the AF are at odds with “locally configured policy”.*

**Question 5:** Is security protection an optional feature that implementations of the MBS System may choose not to support?

**Commentary**: *Clause W.4.1.1 of TS 33.501 states: “...security protection of MBS traffic... are optionally supported in service layer”. To be interoperable, and therefore useful, SA4 believes that this needs to be a mandatory feature provided by all implementations of the MBS System.*

**Question 6:** Is security protection intended to be available only in deployments of the MBS System where the optional MBSF and MBSTF are both present? How is the security architecture intended to work in deployments where an MBSF is present, but the MBSTF is absent or bypassed?

**Commentary**: *The design currently documented in TS 33.501 annex W requires that the MBS Service Key is assigned by the MBSF and the MBS Traffic Key is assigned by the MBSTF. However, the design also requires the MB-SMF to make the MBS Traffic Key available to the UE via the SMF (paragraph 5 of clause W.4.1.2: “In the multicast session join and session establishment procedure, the SMF interacts with the MB-SMF to obtain the multicast session security context”).*

*This means that the MB-SMF must have knowledge of security protection applied to the MBS Session that it is managing, irrespective of whether the MBSF and MBSTF are deployed, but the MB-SMF has no control over that security context because ownership of the security context resides with more northerly functions.*

*Furthermore, in deployments where the MBSF is present but the MBSTF is absent (or bypassed), there is no function capable of generating the MBS Traffic Key.*

**Question 7:** Would SA3 consider a different design in which a control plane function (MB-SMF) assigns the MBS Service Key and the MBS Traffic Key and makes them available to the hence to the MBSTF)? Or a design where the MBSF assigns both the MBS Service Key and the MBS Traffic Key

**Commentary:** *Since there is a one-to-one correspondence between MBS Session and “multicast session security context” it seems more logical for the MB-SMF to manage the security context (including assignment of the MBS Service Key and MBS Traffic Key) as part of the MBS Session state, and for the MB-SMF to expose this to the MBSF via the existing MBS Session resource at reference point Nmb1 or (in cases where the optional MBSF is not present or bypassed) directly to the AF via reference point Nmb13.*

*Such a design would make security protection of MBS traffic available in all MBS System deployments, regardless of whether the optional MBSF and MBSTF entities are deployed (or bypassed).*

*By locating the security context in a single, mandatory control plane entity available in all deployments of the MBS System, the management of state is simplified, particularly in “cold start” scenarios where state needs to be re-established by neighbouring entities.*

*Such a design would also eliminate the need to specify “pull” and “push” interfaces at reference points Nmb1 and Nmb13, thereby simplifying the integration between the MBSF and MB-SMF (at Nmb1), as well as between the AF and the MB-SMF (at Nmb13 when the MBSF is bypassed or not deployed).*

*The MB-SMF could instead offer an initial MBS Traffic Key in the MBS Session Context returned in response to the* Nmbsmf\_MBSSession\_Create *operation (if security protection is requested by the invoker). And the MB‑SMF could define a new operation to support assignment of a fresh MBS Traffic Key during the course of an ongoing MBS Session, or rotation of the current MBS Traffic Key using an index (“key ID”) into a set of keys previously assigned by the MB-SMF.*

*Alternatively, the MBSF could take responsibility for key management, with the disadvantage that this feature could not be supported in deployments of the MBS System that lack the optional MBSF.*

**Question 8:** Why does the SA3 design assign responsibility for authorising UEs to the MBSTF?

**Commentary:** *TS 33.501 clause W.4.1.3 specifies that the UE authenticates with the MBSTF (playing the role of BM-SC) and the MBSTF checks with the UDM, if necessary. According to SA4’s understanding of TS 23.247, this interaction is not possible because only one-way communication from the MBSTF to the UE is possible. The MBSTF therefore lacks an endpoint to receive the HTTP POST message referenced in TS 33.246. Furthermore, the SA2 architecture for MBS in TS 23.247 does not specify interaction between the MBSTF and UDM.*

*It seems more appropriate for a control plane entity (like the MBSF or MB‑SMF) to perform authentication operations of this sort. In TS 26.502, SA4 has specified two-way communication between the UE's MBSF Client and the MBSF at reference point MBS-5. Something like this seems more suitable for authenticating the MBS Session and providing the current MBS Traffic Key.*

# 2 Actions

**To SA3**

**ACTION:** SA4 kindly asks SA3 to take into consideration the feedback in section 1.2 above.

**ACTION:** SA4 kindly asks SA3 to respond to the questions in section 1.2 above.

# 3 Dates of next TSG SA WG 4 meetings

SA4#119-e 11th–20th May 2022 E-meeting

SA4#120 22nd–26th August 2022 Málaga, ES