**3GPP TSG-SA3 Meeting #98e *S3-200081***

**e-meeting, 2 – 6 March 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.180** | **CR** | **00136** | **rev** | **-** | **Current version:** | **16.2.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | [33.180] R16 Gateway security |
|  |  |
| ***Source to WG:*** | Motorola Solutions, Inc |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | MCXsec |  | ***Date:*** | March 2, 2020 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-16 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Security for interconnection with an MC gateway server is not defined. |
|  |  |
| ***Summary of change:*** | 1. Remove editor’s note about MC gateway security being FFS.
2. Replace figure 11.1.1-1 because diagram is not complete and some reference points are incorrect.
3. Add security for interconnection when using an MC gateway server.
 |
|  |  |
| ***Consequences if not approved:*** | Interconnection using MC gateway will be vulnerable to attack. |
|  |  |
| ***Clauses affected:*** | 11.1.1, 11.1.X (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 11.1.1 Overview

MC Systems may interconnect as described in TS 23.379 [2], TS 23.280 [36] and TS 23.281 [37]. This allows inter-system communications to occur.

To ensure interconnection is secure, MC clients only connect to MC Servers within their own system (unless migrating). When information is required by a MC client from another interconnected system, the information is first transferred from the interconnected partner system to the interconnected primary system via MCX server to MCX server communications followed by the distribution of that information to the MC client. For example, group management information is transferred between Group Management Servers in Clause 10.2.7 of TS 23.280 [36], prior to distribution to MC clients.

MC systems should protect themselves at the system border from external attackers. During interconnection, the MC system should use an HTTP proxy and an MC gateway containing an IS proxy as described in clause 11.1.X to enforce policies and apply security functions (such as topology hiding). Among the security functions that can be performed at both proxies are preventing any direct MC client connection over this interface. Figure 11.1.1-1 shows the security architecture for interconnected MC systems.

Cross-system authentication of interconnection signalling requests may be implicit or explicit, subject to the policy of each MC system. Where authentication is implicit, the HTTP Proxy and IS Proxy should prevent messages that do not have an external MC service ID in the source of the request. MC servers should enforce policy to limit the information provided to a signalling requests from external MC service IDs.

Where authentication is explicit, the signalling request shall contain an Element for Authenticating Requests, (EAR), as defined in Clause 9.6. It is recommended that an authorised identity should be used within the EAR, to convey the source's authorisation to make the request.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 11.1.X Interconnection security with MC gateway server

A MC gateway server is part of the mission critical architecture for interconnection as defined in 3GPP TS 23.280 [36]. The MC gateway server includes an IS Proxy for inter-domain security as defined in Annex I. The IS Proxy provides protection of the SIP-3 interface (i.e. SIP payload and RTCP protection using a SPK as defined in clause 9 and clause 6.3.2). The SIP-3 interface is covered as part of the interconnection MCX-1 reference point.

Figure 11.1.X-1 shows an interconnection architecture between two MC domains (MC domain A and MC Domain B) each with the MC gateway server which contains the IS proxy for interconnection security. The MC gateway provides the necessary topology hiding and address translation along with signalling protection via the IS proxy. HTTP communications for interconnection over the HTTP-3 reference point are provided for via the HTTP proxy as described in 3GPP TS 23.280 [36] and protected as defined in clause 6.1.3 of this specification.



Figure 11.1.X-1: Interconnection security using MC gateway with HTTP and IS proxies

In Figure 11.1.X-1, the interface between the MC domains shall be protected hop-by-hop as defined in Clause 6.3.2. The SIP-3 interface between IS Proxies may be protected at the application layer using a shared SPK as defined in Clause 9 and the HTTP-3 interface between HTTP Proxies may be protected using TLS as defined in Clause 6.1.3.For interconnection communications with an MC gateway server (e.g. MC domain A to MC domain B in this example), HTTP and SIP messages are sent by an MC service server or a server in the common services core within the MC domain, towards the MC gateway server or HTTP proxy for processing, protection, and external routing to a partner MC domain.

For HTTP messages, the HTTP proxy applies topology hiding by replacing the internal to/from addresses in the HTTP message with the associated external HTTP routing addresses. The HTTP proxy determines the target HTTP proxy for MC domain B and choses the certificates appropriate for that TLS tunnel. The HTTP message is protected and sent towards MC domain B on the HTTP-3 interface. The HTTP proxy in MC domain B receives the HTTP message where it is decrypted from the external TLS tunnel. The HTTP proxy in MC domain B then replaces any external HTTP routing addresses with internal HTTP addresses applicable to MC domain B and forwards the message to the appropriate server within MC domain B.

For SIP messages, the MC gateway server in MC domain A applies topology hiding by replacing the internal to/from SIP addresses (e.g. Public Service Identities) in the SIP header with the associated external SIP routing addresses and passes the SIP message to the MC gateway IS proxy. The IS proxy removes any internal SIP payload encryption, then based on the target MC domain (MC domain B) selects the appropriate inter-domain SPK to re-encrypt the SIP payload(s). The SIP message is then sent towards the MC gateway server in MC domain B over the SIP-3 interface where the MC gateway IS proxy in MC domain B receives the SIP message and decrypts it using the inter-domain SPK it has in common with MC domain A. The IS proxy in MC domain B may then re-encrypt the SIP payload(s) with an internal MC domain B SPK. The topology hiding function of the MC gateway server in MC domain B then replaces the external SIP routing addresses with internal SIP addresses applicable to MC domain B and forwards the message to the appropriate server within MC domain B.\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*