**3GPP TSG-SA3 Meeting #108e *S3-221963***

**e-meeting, 22 - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Addressing authentication and authorization for EDGE-9 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, InterDigital | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-08-15 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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 can be 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Rel-17 TS 33.558 doesn’t specify the authentication and authorization mechanisms for EDGE-9 reference point (between edge enabler servers). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | X.509 certificates usage for authentication and local policy for authorization are proposed to address the authentication and authorization for EDGE-9 reference point. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Authentication and authorization for EDGE-9 reference point will be missing in the Rel-17 specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.1, 5.1.1, 6.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 1st Change \*\*\*

## 5.1 General security requirements

The Edge application architecture defined in the TS 23.558 [5] shall satisfy the following requirements.

\*\*\* End of 1st Change \*\*\*

\*\*\* Start of 2nd Change \*\*\*

### 5.1.1 Authentication and Authorization

**Authentication and Authorization between Edge Enabler Client (EEC) and Edge Configuration Server (ECS):** Edge Configuration Server (ECS) shall be able to provide mutual authentication with Edge Enabler Client (EEC) over EDGE-4 Interface. ECS shall determine whether EEC is authorized to access ECS's services.

**Authentication and Authorization between EEC and EES:** Edge Enabler Server (EES) shall provide mutual authentication with EEC over EDGE-1 Interface. EES shall determine whether EEC is authorized to access EES's services.

**Authentication and Authorization between Edge Enabler Server (EES) and ECS**: ECS shall provide mutual authentication with EES over EDGE-6 Interface. ECS shall determine whether EES is authorized to access ECS's services.

**Authentication and Authorization between EESs:** EES shall provide mutual authentication with another EES over EDGE-9 Interface. EES shall determine whether peer EES is authorized to access EES's services.

**Authentication and Authorization in EES capability exposure to EAS**: EES shall provide mutual authentication with EAS over EDGE-3 Interface. EES shall determine whether EAS is authorized to access EES's services and expose EEC Capabilities. The Edge application architecture shall support EASs to obtain the user's authorization to access sensitive information (e.g. user's location).

NOTE1: The corresponding security requirements defined in TS 23.558 [5] is AR-5.2.6.2-a/b/d/e/f/g.

\*\*\* End of 2nd Change \*\*\*

\*\*\* Start of 3rd Change \*\*\*

## 6.X Authentication and Authorization between EES and EES

As specified in clause 6.1, TLS is used for EDGE-9 reference point (between edge enabler servers) security. For authentication between EES and EES, X.509 certificates shall be used. The certificates shall follow the profile given in clause 6.1.3a of TS 33.310 [10]. The identities in the end-entity certificates shall be used for authentication and policy checks. Identities in the end-entity certificate shall be based on endpoint information (e.g., URI, FQDN, IP address) as described in TS 23.558 [5].

For authorization between edge enabler servers, local authorization policy or token can be used. If the EES requires access token for authorization, then the peer EES shall authorize the EES by using the token. Otherwise, the peer EES shall authorize the EES by its local authorization policy. For token based authorization of EES by the peer EES, the EES shall send the OAuth 2.0 [15] access token to the peer EES. The token profile is specified in clause 6.2 of the present document.

After successful authentication and authorization, the peer EES shall process the request and send the service response back to the EES.

\*\*\* End of 3rd Change \*\*\*