**3GPP TSG-SA3 Meeting #116 *S3-242621-r1***

Jeju, South Korea, 20th - 24th May 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.558** | **CR** | **0018** | **rev** | **1** | **Current version:** | **18.1.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Clarification on the authentication method(s) between EEC and ECS  |
|  |  |
| ***Source to WG:*** | Samsung, Nokia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eEDGE\_5GC |  | ***Date:*** | 2024-05-10 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SA3 received LS from CT1 (**C1-242674**) for clarification on ECS configuration.Based on the LS it is stated that there is an ambiguity in text related to authentication method.*Q3: (To SA3) In TS 33.558, clause 6.2, SA3 defines that details of the authentication methods used in TLS (while providing examples of them) is out of the scope of the work in SA3. However, a UE behavior is indicated based on the authentication methods in the same clause. We would like to get clarification on the authentication methods and the intention of the above mentioned clause. Additionally, SA3 might consider updating their specification to clarify on this ambiguity.*To resolve the ambiguity, it is proposed to provide clarification on the supported authentication methods and the details of the authentication procedure. |
|  |  |
| ***Summary of change:*** | It is clarified that, in addition to the server side certificate-based TLS authentication, other mutual authentication methods are possible and details of TLS connection establishment procedure is outside the scope of this specification. |
|  |  |
| ***Consequences if not approved:*** | Ambiguity might exist on the supported authentication methods between the EEC and the ECS. |
|  |  |
| ***Clauses affected:*** | 6.2 |
|  |  |
|  | **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\*\*\*\*\*\*\*

6.2 Authentication and authorization between EEC and ECS

The ECS shall be configured with the information of authorization methods (token-based authorization or local authorization) used by EESes.

Authentication between EEC and ECS shall be done during the execution of the TLS handshake protocol. Server side certificate-based TLS authentication shall be supported. A mutual authentication method should be supported and used between EEC and ECS (e.g., TLS certificates (client and server certificate based authentication), usage of AKMA [11] or GBA [12] as methods to arrange the PSK for TLS). Details of such authentication method performed during the execution of the TLS handshake protocol is out of scope of the present document.

NOTE 1: Usage of application layer solutions for EEC authentication is left to implementation.

NOTE 2: If only server side certificate-based TLS authentication is performed, it is left to implementation on which information within a service procedure and services will be provided by the ECS.

The authentication method negotiation mechanism shall re-use the existing TLS v1.3 negotiation. UE may receive the supported authentication method of the ECS optionally as part of the ECS configuration information. Details of the ECS configuration information are specified in TS 23.558 [5]. If the UE has the information about the authentication method supported by the ECS, then the EEC/UE may use this information for the authentication method negotiation.

NOTE 3: Further optimization regarding having prior knowledge about the capability, such as UE storing the selected algorithm from the past negotiation results, is left to EEC/UE implementation. Authentication method received in the ECS configuration information takes precedence. If more than one authentication methods are included in the ECS configuration information, then it is up to the UE implementation to select an authentication method.

If the GPSI is required, the ECS shall retrieve the GPSI from the core network no matter whether the EEC sends the GPSI to the ECS.

NOTE 4: If the ECS identifies a mismatch between the GPSI received from the EEC and the GPSI received from the network, the decision and action to be taken by the ECS for such mismatch cases are left to implementation.After successful authentication, the ECS shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the ECS decides whether OAuth 2.0 [15] access tokens are required for the candidate EESes using the configuration information and issues separate EES access tokens to be used for each candidate EESes that use token-based authorization. The ECS, EEC and EES respectively assume the role of authorization server, client and resource server roles defined in [15]. "Client Credentials" grant type and bearer tokens [16] shall be used. JSON Web Token (JWT) as specified in IETF RFC 7519 [17] for encoding and the JSON signature profile as specified in IETF RFC 7515 [18] for protection of tokens shall be followed. This token profile also applies for clause 6.3 of the present document. The claims of the EES service tokens in the form of JWT [17] shall include the ECS FQDN (issuer), EEC ID (client\_id), GPSI (subject), expected EES service name(s) (scope), EES FQDN (audience), expiration time (expiration). The ECS shall send the service response back to the EEC, which may include EES access token(s).

\*\*\*\*\*\*\*End of Change\*\*\*\*\*\*\*