**3GPP TSG-SA3 Meeting #112 *S3-234196***

**Goteborg, Sweden, 14-18 August 2023** (revision of S3-233841)

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.558** | **CR** | **draftCR** | **rev** | -1 | **Current version:** | **17.3.0** |  |
|  |
| *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:***  | Authentication and authorization between Edge Entities |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | EDGE\_Ph2 |  | ***Date:*** | 2023-07-14 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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:*** | This contribution proposes the living CR of EDGE\_Ph2, according to the conclusion of the TR 33.739 with new clauses and changes.. |
|  |  |
| ***Summary of change:*** | Requirements on the Authentication and Authorization between Application Client (AC) and EEC, between V-ECS and H-ECS.New clause on authentication and authorization between AC and EES.New clause on authentication and authorization between V-ECS and H-ECS.Clarification on authentication and authorization between EEC and ECS, between EEC and EES. |
|  |  |
| ***Consequences if not approved:*** | Incomplete work for the phase 2 edge features. |
|  |  |
| ***Clauses affected:*** | 5.1.1, 6.1, 6.2, 6.3, 6.X (new), 6.Y(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 draftCR's revision history:*** |  |

\*\*\*\* Start of Changes \*\*\*\*

### 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 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.

**Authentication and Authorization between Application Client (AC) and EEC:** EEC should provide mutual authentication with the Application Client over EDGE-5 interface, and the EEC should determine whether Application client is authorized to access EEC’s service.

**Authentication and Authorization between V-ECS and H-ECS**：V-ECS shall provide mutual authentication with H-ECS over EDGE-10 Interface. V-ECS shall determine whether H-ECS is authorized to access V-ECS's services.

\*\*\*\* Next Changes\*\*\*\*

## 6.1 Security for the EDGE interfaces

For the interfaces (EDGE-1/4), the EEC, EES and ECS shall support and use HTTP/2 with "https" URIs as specified in RFC 9113 [19] and RFC 9110 [20]. In addition, the TLS profile shall be compliant with the profile given in clause 6.2 of TS 33.210 [2] .

For the interfaces EDGE-2/7/8,

- If the NEF APIs are selected, security aspects of Network Exposure Function including the protection of NEF-AF interface and support of CAPIF defined in TS 33.501 clause 12 [2] shall be reused, i.e., use of TLS.

- If the SCEF APIs are selected, the Security procedures for reference point SCEF-SCS/AS defined in TS 33.187 clause 5.5 [3] can be reused here, i.e., use of TLS.

For the interfaces (EDGE-3/6/9/10), the EAS, EES and ECS shall support and use HTTP/2 with "https" URIs as specified in RFC 9113 [19] and RFC 9110 [20]. In addition, the TLS profile shall be compliant with the profile given in clause 6.2 of TS 33.210 [2] .

\*\*\*\* Next Changes\*\*\*\*

## 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. Details of the authentication method (e.g., TLS certificates, usage of AKMA [11] or GBA [12] as methods to arrange the PSK for TLS) are 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.

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).

\*\*\*\* Next Changes\*\*\*\*

## 6.3 Authentication and authorization between EEC and EES

Authentication between EEC and EES shall be done during the execution of the TLS handshake protocol. Server side certificate-based TLS authentication shall be supported. Details of the authentication method (e.g., TLS certificates, usage of AKMA [11] or GBA [12] as methods to arrange the PSK for TLS) are 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 EES.

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

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

NOTE 4: If the EES 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 EES for such mismatch cases are left to implementation.

For authorization of EEC by the EES, the EEC shall send the OAuth 2.0 [15] access token, if received from the ECS, to the EES. The token profile is specified in clause 6.2 of the present document. If the EES requires access token for authorization, then the EES shall authorize the EEC by using the token. Otherwise, the EES shall authorize the EEC by its local authorization policy.

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

\*\*\*\* Next Changes\*\*\*\*

## 6.X Authentication and authorization between V-ECS and H-ECS

The V-ECS and H-ECS are provisioned with credentials (e.g., certificate, shared keys/secrets) for mutual authentication. The mutual authentication between V-ECS and H-ECS shall be done based on the preconfigured credentials. The V-ECS shall authorize the H-ECS based on local authorization policy.

## 6.Y Authentication and Authorization between AC and EEC

Authentication and authorization between AC and EEC in UE are based on local policy.

NOTE 1: Security mechanisms for authentication and authorization between AC and EEC in UE are left to implementation.

\*\*\*\* End of Changes\*\*\*\*