**3GPP TSG-SA3 Meeting #107-e *S3-221130***

**e-meeting, 16 - 20 May 2022** *revision of S3-220921*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0001** | **rev** | **1** | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Editorial corrections and technical clarifications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-05-09 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Editorial and technical corrections are necessary to allow clarity in the specification. Some of the phrases incorrectly identify documents as specifications.  It is not necessary to mention TLS 1.2 and 1.3 because TS 33.210 defines TLS profile.  Since HTTP usage is specified in stage 3 specification, the related note in clause 6.5 is not necessary. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Editorial and technical corrections. TS 33.210 is referred instead of explicitly stating TLS versions. The note about HTTP protocol usage is removed from clause 6.5. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misleading and unclear information in TS 33.558. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 5.1.2, 6.1, 6.2, 6.3, 6.5 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[4] 3GPP TS 33.187: "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[5] 3GPP TS 23.558: "Architecture for enabling Edge Applications."

[6] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[7] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs"

[8] void

[9] void

[10] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[11] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[12] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[XX] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[YY] RFC 2818: "HTTP Over TLS".

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

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

### 5.1.2 Interface security

Confidentiality, integrity, and replay protection shall be supported on the EDGE-1-4 and EDGE 6-9 interfaces.

NOTE 1: The interfaces are defined in the Figure 6.2.4 of TS 23.558 [5]. The corresponding security requirement defined in TS 23.558 [5] is AR-5.2.6.2-c.

NOTE 2: The security requirement of EDGE 5 is out of the scope of this specification, since its details are out of the scope of this release of this specification, according to TS 23.558 [5].

The privacy requirements AR-5.2.6.2-h defined in TS 23.558 [5] are implicitly supported, since all the interfaces will be confidentiality and integrityprotected.

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

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

## 6.1 Security for the EDGE interfaces

For the interfaces (EDGE-1/4), the EEC, EES and ECS shall support TLS and HTTPS as specified in RFC 7540 [XX] and RFC 2818 [YY]. TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [1] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [XX]. TLS shall be used for transport protection.

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), the EAS, EES and ECS shall support TLS and HTTPS as specified in RFC 7540 [XX] and RFC 2818 [YY]. TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [1] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [XX]. TLS shall be used for transport protection, unless security is provided by other means, e.g., physical security.

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

\*\*\* Start of 4th 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. 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. If the EEC sends the GPSI to the ECS, then the ECS shall also authenticate the GPSI. The details of how to authenticate the GPSI is out of scope of the present document.

After successful authentication, the ECS shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the ECS decides whether 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 claims of the EES service tokens shall include the ECS FQDN (issuer), EEC ID (subject), expected EES service name(s) (Scope), EES FQDN (audience), expiration time (expiration). The ECS sends the service response back to the EEC, which may include EES access token(s).

\*\*\* End of 4th Change \*\*\*

\*\*\* Start of 5th Change \*\*\*

## 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. 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. If the EEC sends the GPSI to the EES, then the EES shall also authenticate the GPSI. The details of how to authenticate the GPSI is out of scope of the present document.

For authorization of EEC by the EES, the EEC shall send the access token, if received from the ECS, to the EES and the EES shall authorize the EEC by using the token. Otherwise, the ECS shall authorize the EEC by its local authorization policy.

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

\*\*\* End of 5th Change \*\*\*

\*\*\* Start of 6th Change \*\*\*

## 6.5 Authentication and Authorization in EES capability exposure

According to clause 8.7.3 of TS 23.558 [5], the EES may re-expose the network capabilities of the 3GPP core network to the EAS(s) as per the CAPIF architecture specified in TS 23.222 [6]. If the CAPIF architecture is used, the CAPIF functional security model specified in TS 33.122 [7] shall be used for Authentication and authorization in EES capability exposure.

If CAPIF is not used, mutual authentication with TLS certificates using TLS shall be used. The TLS and certificates shall follow the profiles defined in TS 33.210 [2] and TS 33.310 [10], and the authorization is based on local authorization policy at the EES.

\*\*\* End of 6th Change \*\*\*