**3GPP TSG-SA3 Meeting #123 draft\_S3-252583-r1**

Goteborg, Sweden, 25 - 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Update TC on account protection | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | MITRE-FFRDC, Deutsche Telekom, BSI (DE) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2025-08-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | Rel-20 |
|  | *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:*** | | Industry best practice has changed, so that now two authentication attributes are needed for account protection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Changes the TC\_ACCOUNT\_PROTECTION to align with the parent heading which is about account protection via authentication attributes. Since this TC only tests for authentication, the TC name should reflect this accordingly.  Modifies the requirements and TC procedures to at least two authentication attributes, instead of one, to align with industry best practice.  Adds additionaly biometric authentication attribute. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 5GA systems will not be compliant with regulation and will not follow industry best practices. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.3.4.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **N** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **N** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **N** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

4.2.3.4.2.1 Account protection by at least two authentication attributes.

*Requirement Name:* Account protection by at least two authentication attributes.

*Requirement Reference*: In accordance with industry best practice.

*Requirement Description:* The various user and machine accounts on a system shall be protected from misuse. To this end, at least two authentication attributes is typically used, which, when combined with the user name, enables strong authentication and identification of the authorized user.

Authentication attributes include:

- Cryptographic keys

- Token

- Passwords

This means that authentication based on a parameter that can be spoofed (e.g. phone numbers, public IP addresses or VPN membership) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

NOTE: Several of the above options can be combined (multi-factor authentication) to achieve a higher level of security. Whether or not this is suitable and necessary depends on the protection needs of the individual system and its data and is evaluated for individual cases.

*Threat References:* TR 33.926 [4], 5.3.3.5, IP Spoofing

*Test Case:*

**Test Name**: TC\_ACCOUNT\_PROTECTION\_AUTHENTICATION

**Purpose:**

To ensure that all accounts are protected by at least two authentication attributes.

**Procedure and execution steps:**

**Pre-Conditions:**

1) All predefined accounts are identified in the documentation accompanying the Network Product.

2) Instructions of how to create new accounts are provided in the documentation accompanying the Network Product.

3) Instructions of how administrator user can view all existing accounts in the database are provided in the documentation accompanying the Network Product.

NOTE: No test is provided here for finding undocumented hard coded accounts as such tests be impossible to define in a general way.

**Execution Steps:**

1) After login via account with necessary access rights (e.g. Admin) search in the database for any undocumented account.

2) Attempt login to all predefined accounts identified (either documented or not) with and without using all the respective authentication attributes.

3) Create a new account by following instructions in documentation.

4) Attempt login to the newly created account.

**Expected Results:**

1) It is not possible to login to any predefined account without using at least two authentication attributes that satisfy the conditions in the requirement.

2) It is not possible to login to any newly created account without usage of at least two authentication attributes that satisfy the conditions in the requirement.

**Expected format of evidence:**

Evidence containing the results of all login attempts, e.g. screenshots, log files, error messages.

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