**3GPP TSG-SA3 Meeting #114e *ad-hoc S3-240040-r1***

Electronic meeting, online, 22 - 26 January 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **0155** | **rev** | **1** | **Current version:** | **18.2.0**  |  |
|  |
| *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 |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Update to the clause 4.2.3.4.3.1 - Password Structure  |
|  |  |
| ***Source to WG:*** | Samsung |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS |  | ***Date:*** | 2023-12-09 |
|  |  |  |  |  |
| ***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:*** | According to NESAS, clause 4.2.3.4.3.1 of TS 33.117 states that "Absolute minimum length of 8 characters" (for a password), but then goes on to state "The network product shall use a default minimum length of 10 characters", which appears contradictory.Therefore, it is recommended to clarify whether the network product is required to support a password with a minimum length of 8 or 10 characters |
|  |  |
| ***Summary of change:*** | Based on the understanding of testcase, the network can set a default minimum length of password to be 10 characters. But the network should allow length of password to be 8 characters or more than 8 characters for the user to be able to set (taking the anology of strong/weak password strength). Any password less than 8 characters should be rejected. |
|  |  |
| ***Consequences if not approved:*** | Unclear test cases in TS 33.117.  |
|  |  |
| ***Clauses affected:*** | 4.2.3.4.3.1 |
|  |  |
|  | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*

4.2.3.4.3.1 Password Structure

*Requirement Name*: Password Complexity rule

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*:

The setting by the vendor shall be such that a network product shall only accept passwords that comply with the following complexity criteria:

1) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the network product). It shall not be possible setting this absolute minimum length to a lower value by configuration.

2) Comprising at least three of the following categories:

- at least 1 uppercase character (A-Z)

- at least 1 lowercase character (a-z)

- at least 1 digit (0-9)

- at least 1 special character (e.g. @;!$.)

The network product shall use a default minimum length of 10 characters (even though the allowed minimum length is 8 characters). The minimum length of characters in the passwords shall be configurable by the network operator. The default minimum length is the value configured by the vendor before any network operator-specific configuration has been applied. The special characters can be categorized in sets according to their Unicode category.

The network product shall at least support passwords of a length of 64 characters or a length greater than 64 characters.

If a central system is used for user authentication, password policy is performed on the central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this subclause. If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Network Product.

When a user is changing a password or entering a new password, the system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).

*Threat References*: TR 33.926 [4]

*Test case*:

**Test Name**: TC\_PASSWORD\_STRUCT

**Purpose:**

To verify that password structure adheres to the password complexity criteria.

To verify that password structure is configurable as per the complexity criteria.

**Procedure and execution steps:**

**Pre-Conditions:**

1. Tester has rights to create user account.

**Execution Steps**

Execute the following steps:

A. Test Case 1

1. The tester logs into Network Product application using admin account.

2. The tester creates user A following the password complexity criteria.

3. The tester logs in as user A and attempts to change their password which contains characters from all four categories mentioned in the password complexity criteria.

B. Test Case 2

1. The tester logins with privileged account.

2. The tester modifies password structure policy on the network product by strengthening the policy (e.g. changing the minimum password length to 8+x, changing the minimum number of character Unicode categories to 4).

3. The tester logs in as user A and attempts to change their password to a password with a strength of less than that permitted by the policy strengthened in step 2 above.

**Expected Results:**

Tester can change password only if new password fulfil the password complexity criteria

**Expected format of evidence:**

Evidence suitable for the interface, e.g. screenshot containing the operation result or report in text form.

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