**3GPP TSG-SA3 Meeting #101-e *S3-20xxxx***

**e-meeting, 9th – 20th November 2020 revision of S3-203110**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **0068** | **rev** | **-** | **Current version:** | **16.5.0** |  |
|  |
| *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 | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Enforcement of password change after initial login R16  |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS-SA3  |  | ***Date:*** | 30-10-2020 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-16 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | In clause 4.2.3.4.3.2 of TS 33.117 R16, it is required that: “*If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time……* *Password change shall be enforced after initial login*”. However, for certain network products like base stations (eNB and gNB), the first login at these products is usually done by a 3rd party installer locally on site who is not responsible for eNB/gNB password management. Enforcing mandatory password update after first login at the eNB/gNB will have to make password management and database separately and assign new password at the time of first commissioning or during system recovery to factory default software, which would impact the operational model used by operators working with NMS for authentication.Therefore, it is proposed to add a note to relax the mandatory requirement in TS 33.117 clause 4.2.3.4.3.2 for certain types of network products. |
|  |  |
| ***Summary of change:*** | Added a note in clause 4.2.3.4.3.2 of TS 33.117 R16. |
|  |  |
| ***Consequences if not approved:*** | Mandatory requirement not inline with the practical operation and management of certain types of network products like eNB and gNB. |
|  |  |
| ***Clauses affected:*** | 4.2.3.4.3.2 |
|  |  |
|  | **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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

###### 4.2.3.4.3.2 Password changes

*Requirement Name*: tba

*Requirement Description*:

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it is possible to redirect or implement this function on this system.

Password change shall be enforced after initial login.

NOTE: The initial login mentioned above means the login initially performed by the admin responsible for password management of the system.

The system shall enforce password change based on password management policy. In particular, the system shall enforce password expiry.

Previously used passwords shall not be allowed up to a certain number (Password History).
The number of disallowed previously used passwords shall be:

- Configurable;

- Greater than 0;

- And its default value shall be 3. This means that the network product shall store at least the three previously set passwords. The maximum number of passwords that the network product can store for each user is up to the manufacturer.

When a password is about to expire a password expiry notification shall be provided to the user.

Above requirements shall be applicable for all passwords used(e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.

*Security Objective references*: tba.

*Test case*:

**Test Name**: TC\_PASSWORD\_CHANGES

**Purpose:**

- To check whether the network product is provisioned with the functionality that enables its user to change the password at any time.

- The network product enforces password change after initial login.

- To verify the new password adheres to the password management policy and also to verify whether it has password expiry rule.

- The network product is configured to disallow specified number of previously used passwords (Password History).

**Procedure and execution steps:**

**Pre-Conditions:**

1. Tester has account with username and password in the network product.

2. Network product vendor will provide documentation for password management policy which should include details on how to change the password, configure password expiry rule and disallowing specified number of previously used passwords.

3. The network product vendor shall supply information on how many passwords the network product can store for each user in the password history.

4. The tester has privilege to modify the number of disallowed previously used password.

**Execution Steps**

**Execute the following steps:**

A. Positive Test

Case 1:

Test case to enforce password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

1 The tester logs into network product application using a privileged account.

2 The network product application generates password expiry notification for user Y to force user Y to change the password.

3 The tester logs out as a privileged user and logs on as user Y.

4. The tester is prompted to change his password and creates a new password by following the password policy management.

5 The network product application confirms change in password by, for example, displaying "Password Changed Successfully".

6 The tester successfully logs-in the network product application as user Y using the new password.

Case 3:

1. The tester logs into network product application using a privileged account.

2. Tester configures the network product application for number of disallowed previously used passwords to x

3. The tester requests for a password change for user Y.

4. The tester logs out of the privileged account and logs on as user Y

5. The tester creates a new password by following the password policy management.

6. If the password is not equal to any of the x previously used passwords, the network product application still accepts the new password and displays "Password Changed Successfully".

B. Negative Test

Case 1:

Test case to enforce password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

No negative test case for this scenario.

Case 3:

1. The tester logs into network product application using privileged account.

2. Tester configures the network product application for number of disallowed previously used passwords to x for user Y.

3. The tester logs out of the privileged account and logs in as user Y

4. The tester requests for a password change.

5. The tester sets the new password to a value that is among the last x passwords used previously x times.

**Expected Results:**

A. Positive Test

Case 1:

Expected result for enforce password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

Tester can successfully change the password.

Case 3:

Tester can successfully change the password.

B. Negative Test

If the negative test case passes, this shows that network product application does not work properly and it violates the requirement.

Case 1:

Expected result for enforce password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

No negative test case for this scenario.

Case 3:

The tester cannot successfully change the password.

**Expected format of evidence:**

Evidence suitable for the interface, e.g. screenshot contains the operation result.

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