**3GPP TSG-SA3 Meeting #114e *ad-hoc draft\_S3-240049-r1***

Electronic meeting, online, 22 - 26 January 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **0164** | **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:***  | Address GSMA comments and add pre-condition excution steps and evidence to 4.2.5.3 |
|  |  |
| ***Source to WG:*** | Huawei; HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  SCAS\_5G\_Ph3 |  | ***Date:*** | 2024-01-22 |
|  |  |  |  |  |
| ***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:*** | GSMA commentted that number of times is subjective, and recommended that the minimum number of times should be specified. But we think the minimum time is left to the negotiation between vendor and testlab, because the times may rely on how many user ID will be used.Thus additional NOTE is added to clarify this.The change is proposed to align the test case from clause 2.3.1.25 of AIS\_N2 document which is for NESAS CCS\_GI.  |
|  |  |
| ***Summary of change:*** | Delete a number of times, and add a NOTE to clarify the repeated times is left to vendor and test lab.Update pre-condition, execution steps and Expected format of evidence. |
|  |  |
| ***Consequences if not approved:*** | Misalignement with NESAS documents. |
|  |  |
| ***Clauses affected:*** | 4.2.5.3 |
|  |  |
|  | **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:*** |  |

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

#### 4.2.5.3 HTTP User sessions

*Requirement Name*: User sessions

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*:

To protect user sessions the Network Product shall support the following session ID and session cookie requirements:

1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.

2. The session ID shall be unpredictable.

3. The session ID shall not contain sensitive information in clear text (e.g. account number, social security, etc.).

4. In addition to the Session Idle Timeout (see clause 4.2.3.5.2 Protecting sessions – Inactivity timeout), the Network Product shall automatically terminate sessions after a configurable maximum lifetime This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.

5. Session ID's shall be regenerated for each new session (e.g. each time a user logs in).

6. The session ID shall not be reused or renewed in subsequent sessions.

7. The Network Product shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.

8. Where session cookies are used the attribute 'HttpOnly' shall be set to true.

9. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.

10. Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.

11. The Network Product shall not accept session identifiers from GET/POST variables.

12. The Network Product shall be configured to only accept server generated session ID's.

*Threat References*: TR 33.926 [4]

*Test case*:

**Purpose:**

Verify that the above 12 session ID and session cookie requirements have been met.

**Procedure and execution steps:**

**Pre-Conditions:**

- The Network Product uses a session ID that is communicated between the client and Network Product to establish and maintain a session.

- Documentation describing how a session is maintained and where the session ID is stored / and how this is communicated and after how long sessions expire.

- The documentation should describe the algorithm used to generate the session IDs.

- The session ID does not contain sensitive information.

**Execution Steps**

1. The tester logs in repeatedly with different user IDs and with the same user ID in a row and collects the session IDs according to the documentation and the user IDs associated with them. The tester verifies that:

a. The session IDs are different between sessions of the same and different users;

b. The session IDs seems random based on his/her own experience. The tester may use tests like the bitstream test or the count-the-1s-tests from the diehard test suite. The tester documents how randomness was verified;

c. The session IDs are always different between sessions, also when the user ID is the same.

NOTE: the repeated times is lfet to vendor and test lab decide.

2. The tester verifies that when session cookies are used

a. neither the "expire" or the "max-age" is set;

b. the 'HttpOnly' is set to true;

c. the 'domain' attribute is set to the correct domain;

d. the 'path' attribute is set to the correct directory or sub-directory.

3. The tester verifies that it is impossible to:

a. access a session by retrieving the session ID and communicating the session ID through a POST or GET variable.

b. generate a session ID on the client by attempting to login with a custom generated session ID.

c. keep a session alive for longer than the configured maximum lifetime (by default 8 hours).

 4. The tester verifies that the default maximum lifetime is set to 8 hours.

**Expected Results:**

1. A list of session IDs and user IDs that are different between sessions even when the tester has logged in with the same user and that are unpredictable as is confirmed by the entropy calculation.

2. A confirmation from the tester that the correct variables are indeed set.

3. A denied access to the tester when attempting the two login steps of step 3 and an expired session in step 3c.

**Expected format of evidence:**

A confirmation that the tester has confirmed that (by providing e.g. network traffic request/response etc):

1. Session IDs follow the rules 1-3, 5, 6.

2. A session times out after 8 hours or sooner according to the documentation.

3. The correct cookie settings are used.

4. The network product does not accept customly generated session IDs and that session IDs over GET or POST are ignored.

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