**3GPP SA3LI#96 *s3i250068***

**28-31 January 2025**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at  http://www.3gpp.org/Change-Requests.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Stage 2 logging / audit requirements | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | SA3-LI (NTAC) | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | LI19 | | | | |  | ***Date:*** | | | 30 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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. | | | | | | | | *Use one of the following releases: 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) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | As discussed in s3i240484 and s3i250042, additional stage 2 text is required to properly explain how the the security and audit requirements in TS 33.126 clauses 6.5 and 6.6 are met. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adds stage 2 descriptions of which interception lifecycle events are required to be logged and how. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Security and audit requirements in TS 33.126 cannot be reliably met. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.1, 8.1, 8.X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Revised from s3i250045 | | | | | | | | |

CHANGE 1

5.1 General

The following clauses describe the high-level functional architecture for LI for 3GPP-defined services and network technologies. It describes the architectural elements necessary for LI, their roles and responsibilities, and the interfaces and interactions between them.

Clauses 6 and 7 of the present document describe how the LI for various 3GPP-defined network technologies and services are realised within the generic LI architecture, including associations of LI architectural elements with the network functions involved.

Clause 8 of the present document describes security requirements for the LI system.

Specific logging requirements for the LI system are described in clause 8.X.

Not all LI architectural elements and interfaces are used in all network technologies and services.

CHANGE 2

8.1 Introduction

The most sensitive information in the LI system is the target list. This is the list of all the subjects in the network currently under surveillance, whether active, suspended or in any other state. The security measures used by the carrier to prevent unauthorized access to this list is not subject to standardization, but the architectural choices made in the design of the LI system do impact the security of the target list directly.

Since completeness of the interception product is a legal requirement in most jurisdictions, the LI system shall ensure that no events that are lawfully authorized for interception are missed (or collected in error). To ensure that no events are missed there are two architectural alternatives described in clause 8.2.

Requirements for the management of LI keys at the ADMF is described in clause 8.3.

Requirements for virtualised LI environments are described in clause 8.4.

Requirements for POI security are described in clause 8.5.

Other deployment considerations are described in clause 8.6.

Clause 8.X describes baseline logging requirements for the LI system.

CHANGE 3

8.X Logging

LI functions shall support securely creating, buffering and transporting log records of relevant lifecycle events, pursuant to the requirements of TS 33.126 [1] clause 6.5.

LI functions shall support logging at least the following lifecycle events, where they occur at a given LI function:

* Addition, deletion, modification and retrieval of interception tasks.
* Addition, deletion, modification and retrieval of delivery destinations.
* Querying of the status of the LI function.
* Reporting or altering the configuration of the LI function via LI\_X0.
* Reporting of an error or issue, including abnormal message flows.
* Establishment or disconnection of an LI\_T2 / LI\_T3 / LI\_HI2 / LI\_HI3 transport connection.
* Any unsuccessful communication attempt over any of the interfaces defined in the present document.

Where there are additional minimum requirements for logging for a specific LI function, they are listed in the relevant clause for that LI function.

Logging shall comply with the security requirements in TS 33.126 [1] clause 6.6; particular attention should be given to ensuring that logs cannot be accessed or modified by unauthorised actors.

Which events are logged and the retention period of any logs shall be configurable by the CSP. By default logging shall be enabled.

The LI function shall support transmission of buffered log records to multiple destinations, and the destinations shall be configurable. The network shall support transmitting and storing log records generated pursuant to this clause separately from any other logging system in the network, to the extent necessary to comply with the requirements in TS 33.126 [1] clause 6.6.

END OF CHANGES