**3GPP TSG-SA3 Meeting #102-e *draft-S3-210498-r2***

**e-meeting, 18-29 January 2021 *A merger of S3-210498 and S3-210189***

**Source: Ericsson, CATT**

**Title:** **Key issue on** **security of data via Messaging Framework**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***Approve this contribution to add a new key issue in the eNA study TR33.866***

# 2 References

[1] 3GPP TR 23.700-91: “Study on enablers for network automation for the 5G System (5GS); Phase 2”

# 3 Rationale

In [1], in the conclusions for the Key Issue #11 ‘Increasing efficiency of data collection’, DCCF (Data Collection Coordination Function) is defined for efficient data collection in 5GS. The DCCF is a control-plane function that coordinates data collection and triggers data delivery to Data Consumers.

TR 23.700-91 [1] lists several agreed principles for normative work, some of which are as follows:

- "When a Data Collection Coordination Functionality (DCCF) is deployed, it is used to coordinate collection of data from one or more NF(s) based on data collection requests from one or more Consumer NF(s)."

- "Data Collection notification to one or more Consumer NF(s) may be supported via a Messaging Framework. Adaptors supporting 3GPP services allow NFs to interact with the Messaging Framework.

NOTE 2: The Messaging Framework is outside the scope of 3GPP. Adaptors are not expected to be standardized by 3GPP, only the interface between 3GPP entities and the adaptors is under 3GPP scope. This includes 3GPP services offered by adaptors to allow NFs to interact with the Messaging Framework."

- "The DCCF coordinates data collection so the same data is not requested multiple times from the same Data Source."

The Messaging Framework is not expected to be standardized by 3GPP. It contains Messaging Infrastructure that propagates event information and data (e.g.: streaming and notifications) from Data Sources to Data Consumers.

In TR 23.700-91 [1], the Figure 6.9.3-1: "Data Collection & Distribution for Event Notifications (Subscribe/Notify)" shows how the data can be transferred via Messaging Framework from Data Sources to Data Consumer.

Since the Messaging Framework is not expected to be standardized by 3GPP, it may not be trusted.

The DCCF and the Messaging Framework decouple the data collection between the consumer and producer; however, this may induce a security problem because the data consumer cannot verify that the data from the data producer is not modified by the Messaging Framework and the confidentiality of the data cannot be guaranteed by the Messaging Framework.

# 4 Detailed proposal

\*\*\* BEGINNING OF 1st CHANGES \*\*\*

### 5.1.X Key Issue #1.X: Security protection of data via Messaging Framework

### 5.1.X.1 Key issue details

In [1], in the conclusions for the Key Issue #11 ‘Increasing efficiency of data collection’, DCCF (Data Collection Coordination Function) is defined for efficient data collection in 5GS. The DCCF is a control-plane function that coordinates data collection and triggers data delivery to Data Consumers.

TR 23.700-91 [1] lists several agreed principles for normative work, some of which are as follows:

- "When a Data Collection Coordination Functionality (DCCF) is deployed, it is used to coordinate collection of data from one or more NF(s) based on data collection requests from one or more Consumer NF(s)."

- "Data Collection notification to one or more Consumer NF(s) may be supported via a Messaging Framework. Adaptors supporting 3GPP services allow NFs to interact with the Messaging Framework.

NOTE 2: The Messaging Framework is outside the scope of 3GPP. Adaptors are not expected to be standardized by 3GPP, only the interface between 3GPP entities and the adaptors is under 3GPP scope. This includes 3GPP services offered by adaptors to allow NFs to interact with the Messaging Framework."

- "The DCCF coordinates data collection so the same data is not requested multiple times from the same data source."

The Messaging Framework is not expected to be standardized by 3GPP. It contains Messaging Infrastructure that propagates event information and data (e.g.: streaming and notifications) from data sources to data consumers.

In TR 23.700-91 [1], the Figure 6.9.3-1: "Data Collection & Distribution for Event Notifications (Subscribe/Notify)" shows how the data can be transferred via Messaging Framework from data sources to data consumer.

Since the Messaging Framework is not expected to be standardized by 3GPP, it may not be trusted.

As concluded in clause 8 in TR 23.900-71[1], Data Collection Coordination Function (DCCF) and Data Repository Function (DRF) and the related interfaces (e.g., interfaces between 3GPP entities and the adaptors) are to be standardized.

The DCCF and the Messaging Framework decouple the data collection between the data consumer and the data source; however, this may induce a security problem because the data consumer cannot verify that the data from the data source is not modified by the Messaging Framework and the confidentiality of the data cannot be guaranteed by the Messaging Framework.

### 5.1.X.2 Threats

An attacker may eavesdrop or manipulate or replay the communication or initiate the MitM attacks on the interface.

If the integrity of the data collected from the data source is not protected, then the Messaging Framework may modify the data, which results in producing wrong analytics.

If the confidentiality of the data collected from the data source is not protected, then the Messaging Framework may access the sensitive data, which may cause privacy leakage.

Replay attacks may lead to usage of same data more than once, and therefore, it may cause wrong analytic results.

### 5.1.X.3 Potential Security requirements

The transfer of the data between data source and data consumer via the messaging framework shall be confidentiality, integrity and replay protected end-to-end between data source and data consumer.

Confidentiality protection, integrity protection and replay-protection shall be supported on the new interfaces.

\*\*\* END OF 1st CHANGES \*\*\*