**3GPP TSG-SA3 Meeting #102-e *draft\_S3-210116-r3***

**e-meeting, 18 – 29 January 2021** Revision of S3-210116

**Source : Nokia, Nokia Shanghai Bell**

**Title : KI on Authorization of consumers for data access via DCCF**

**Document for : Approval**

**Agenda Item : 5.16**

# 1 Decision/action requested

***This pCR proposes a Key Issue to TR 33.866 to address authorization aspects for data access via DCCF***

# 2 References

[1] 3GPP TR 33.866 for eNA

# 3 Rationale

According the conclusions drawn in SA2 study, the Data Collection Coordination Function (DCCF) 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) with Data Collection Coordination Function (DCCF) and Data Repository Function (DRF) to be standardized. The NWDAF analytics function interacts directly with the DCCF to request the collection of data. The NFs interact directly with the DCCF to request analytics to an NWDAF. The DCCF interacts with the NFs to collect data.

Further, data is collected in a standardized manner from one or more NF(s) (including NWDAF) and OAM system. The collected data and/or produced data can be stored in the DRF, which exposes the standardized interface for storage. In this case, DRF act as data source for the stored data. Consumers NF(s) (e.g. NWDAF) access the data from DRF either directly or via a request to DCCF. The data that the NWDAF obtains directly from the DRF will be determined in the normative phase. If a consumer NF makes a request for data via DCCF and that data are already available at the DRF, the DCCF forwards the request to DRF instead of forwarding the request to NF. It is possible to use the NRF for discovery of new DCCF and DRF.

The following NOTE has been added in SA2 conclusions in [1]: *NOTE 4: Additional authorization for Consumers to access data from a Data Source via the DCCF and to access data from DRF (directly or via DCCF) needs to be coordinated with SA3.*

To allow addressing NOTE 4 it is proposed to introduce a KI on Authorization of consumers for data access via DCCF.

# 4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.866.

\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

### 5.1.X Key Issue #1.X: Authorization of NF Service Consumers for data access via DCCF

#### 5.1.X.1 Key issue details

A Data Collection Coordination Function (DCCF) 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). DCCF and Data Repository Function (DRF) can be standalone NFs, possibly co-located with NWDAF, or can be hosted by NWDAF. 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. 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.

TR 23.700-91-100 conclusion mentions that “Additional authorization for Consumers to access data from a Data Source via the DCCF and to access data from DRF (directly or via DCCF) needs to be coordinated with SA3“. According to SA2 KI#11 conclusions, if a consumer subscribes to analytics notifications to the DCCF, the DCCF can subscribe itself to the data source and notify the data source that notifications are directly to be sent to the consumer. The data source will then send notifications to the consumer via the MF or via the DCCF.

This key issue addresses the authorization aspects of the DCCF being allowed to subscribe the data on behalf of the consumer at the data source or the DRF, i.e. the security aspect on usage subscription/notification mechanisms for a consumer to receive notifications on a different path (as adapted in SA2 conclusions) will be studied.

#### 5.1.X.2 Security threats

DCCF introduces a new path for a NF Service Consumer (NFc) to access the data from data sources or a NF Service Producer (NFp). Due to the introduction of DCCF between consumer and producer, the existing security mechanism will not be sufficient, and the following threats needs to be addressed:

Based on a request from a DCCF, the Messaging Framework may provide data from a producer to a requesting data consumer, even though the consumer is not authorized to receive this data.

Based on a request from a DCCF data received from a data producer is stored in the DRF. When the data are later retrieved, the DCCF may provide the stored data to a non-authorized consumer if requested.

The data producer may be unable to correctly verify the identity of the data consumer since the data request is coming from DCCF on behalf of the consumer.

#### 5.1.X.3 Potential security requirements

TBD

\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES