3GPP TR 23.791 V16.2.0 (2019-06)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study of Enablers for Network Automation for 5G

(Release 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

3GPP, 5G, Architecture, Network, Automation

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [10](#__RefHeading___Toc11149720)

1 Scope [11](#__RefHeading___Toc11149721)

2 References [11](#__RefHeading___Toc11149722)

3 Definitions and Abbreviations [12](#__RefHeading___Toc11149723)

3.1 Definitions [12](#__RefHeading___Toc11149724)

3.3 Abbreviations [12](#__RefHeading___Toc11149725)

4 Architecture Assumptions [12](#__RefHeading___Toc11149726)

4.1 General [12](#__RefHeading___Toc11149727)

4.2 General Framework [13](#__RefHeading___Toc11149728)

5 Use Cases and Key Issues [14](#__RefHeading___Toc11149729)

5.1 Use Cases [14](#__RefHeading___Toc11149730)

5.1.0 Introduction and guidelines [14](#__RefHeading___Toc11149731)

5.1.1 Use Case 1: <how to get information from AF> [14](#__RefHeading___Toc11149732)

5.1.1.1 Description [14](#__RefHeading___Toc11149733)

5.1.2 Use Case 2: <NWDA-Assisted QoS Provisioning> [15](#__RefHeading___Toc11149734)

5.1.2.1 Description [15](#__RefHeading___Toc11149735)

5.1.3 Use Case 3: <NWDA-Assisted Traffic Handling> [15](#__RefHeading___Toc11149736)

5.1.3.1 Description [15](#__RefHeading___Toc11149737)

5.1.4 Use Case 4: Using NWDAF output to customize mobility management [15](#__RefHeading___Toc11149738)

5.1.4.1 Description [15](#__RefHeading___Toc11149739)

5.1.5 Use Case 5: <NWDA-assisted Determination of Policy> [16](#__RefHeading___Toc11149740)

5.1.5.1 Description [16](#__RefHeading___Toc11149741)

5.1.6 Use Case 6: <NWDAF-Assisted QoS Adjustment> [16](#__RefHeading___Toc11149742)

5.1.6.1 Description [16](#__RefHeading___Toc11149743)

5.1.7 Use Case 7: NWDAF assisting 5G edge computing [16](#__RefHeading___Toc11149744)

5.1.7.1 Description [16](#__RefHeading___Toc11149745)

5.1.8 Use Case 8: Performance improvement and supervision of mIoT terminals [17](#__RefHeading___Toc11149746)

5.1.8.1 Description [17](#__RefHeading___Toc11149747)

5.1.9 Use Case 9: <NWDAF-assisted load balancing/re-balancing of network functions> [17](#__RefHeading___Toc11149748)

5.1.9.1 Description [17](#__RefHeading___Toc11149749)

5.1.10 Use Case 10: NWDA-assisted determination of areas with oscillation of network conditions [17](#__RefHeading___Toc11149750)

5.1.10.1 Description [17](#__RefHeading___Toc11149751)

5.1.11 Use Case 11: Prevention of various security attacks [18](#__RefHeading___Toc11149752)

5.1.11.1 Description [18](#__RefHeading___Toc11149753)

5.1.12 Use Case 12: < NWDA-Assisted predictable network performance > [19](#__RefHeading___Toc11149754)

5.1.12.1 Description [19](#__RefHeading___Toc11149755)

5.1.13 Use Case 13: <UE driven analytics sharing> [19](#__RefHeading___Toc11149756)

5.1.13.1 Description [19](#__RefHeading___Toc11149757)

5.1.14 Use Case 14: How to ensure that slice SLA is guaranteed [19](#__RefHeading___Toc11149758)

5.1.14.1 Description [19](#__RefHeading___Toc11149759)

5.2 Key Issues [20](#__RefHeading___Toc11149760)

5.2.1 Key Issue 1: Analytic Information Exposure to 5GS NF [20](#__RefHeading___Toc11149761)

5.2.1.1 Description [20](#__RefHeading___Toc11149762)

5.2.1.1 Requirements [21](#__RefHeading___Toc11149763)

5.2.2 Key Issue 2: Analytic Information Exposure to AF [21](#__RefHeading___Toc11149764)

5.2.2.1 Description [21](#__RefHeading___Toc11149765)

5.2.2.2 Requirements [21](#__RefHeading___Toc11149766)

5.2.3 Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection [21](#__RefHeading___Toc11149767)

5.2.3.1 Description [21](#__RefHeading___Toc11149768)

5.2.3.2 Requirements [22](#__RefHeading___Toc11149769)

5.2.4 Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure [22](#__RefHeading___Toc11149770)

5.2.4.1 Description [22](#__RefHeading___Toc11149771)

5.2.4.2 Requirements [22](#__RefHeading___Toc11149772)

5.2.5 Key Issue 5: NWDAF-Assisted QoS Profile Provisioning [23](#__RefHeading___Toc11149773)

5.2.5.1 Description [23](#__RefHeading___Toc11149774)

5.2.5.2 Requirements [23](#__RefHeading___Toc11149775)

5.2.6 Key Issue 6: NWDAF assisting traffic routing [23](#__RefHeading___Toc11149776)

5.2.6.1 Description [23](#__RefHeading___Toc11149777)

5.2.7 Key Issue 7: NWDAF assisting Future Background Data Transfer [23](#__RefHeading___Toc11149778)

5.2.7.1 Description [23](#__RefHeading___Toc11149779)

5.2.7.1 Requirements [23](#__RefHeading___Toc11149780)

5.2.8 Key Issue 8: performance improvement and supervision of mIoT terminals [23](#__RefHeading___Toc11149781)

5.2.8.1 Description [23](#__RefHeading___Toc11149782)

5.2.9 Key Issue 9: Customizing mobility management based on NWDAF output [24](#__RefHeading___Toc11149783)

5.2.9.1 Description [24](#__RefHeading___Toc11149784)

5.2.9.2 Requirements [24](#__RefHeading___Toc11149785)

5.2.10 Key Issue 10: NWDAF service support to select NF instances [24](#__RefHeading___Toc11149786)

5.2.10.1 Description [24](#__RefHeading___Toc11149787)

5.2.10.2 Requirement [25](#__RefHeading___Toc11149788)

5.2.11 Key Issue 11: NWDA-Assisted predictable network performance [25](#__RefHeading___Toc11149789)

5.2.11.1 Description [25](#__RefHeading___Toc11149790)

5.2.11.2 Requirements [25](#__RefHeading___Toc11149791)

5.2.12 Key Issue 12: Support of Northbound Network Status Exposure [25](#__RefHeading___Toc11149792)

5.2.12.1 Description [25](#__RefHeading___Toc11149793)

5.2.12.2 Requirement [26](#__RefHeading___Toc11149794)

5.2.13 Key Issue 13: UE driven analytics [26](#__RefHeading___Toc11149795)

5.2.13.1 Description [26](#__RefHeading___Toc11149796)

5.2.13.2 Requirements [26](#__RefHeading___Toc11149797)

5.2.14 Key Issue 14: How to ensure that slice SLA is guaranteed [26](#__RefHeading___Toc11149798)

5.2.14.1 Description [26](#__RefHeading___Toc11149799)

5.2.14.2 Requirements [27](#__RefHeading___Toc11149800)

6 Solutions [27](#__RefHeading___Toc11149801)

6.1 Solution 1: Network Data Analytics Feedback [27](#__RefHeading___Toc11149802)

6.1.1 Description [27](#__RefHeading___Toc11149803)

6.1.1.0 General [27](#__RefHeading___Toc11149804)

6.1.1.1 Network data analytics Subscribe/Unsubscribe [27](#__RefHeading___Toc11149805)

6.1.1.2 Network data analytics Request [28](#__RefHeading___Toc11149806)

6.1.1.3 How a NF requests or subscribes to analytics [28](#__RefHeading___Toc11149807)

6.1.1.3.1 Content of Analytics requests/subscribe [28](#__RefHeading___Toc11149808)

6.1.1.3.1.1 General [28](#__RefHeading___Toc11149809)

6.1.1.3.1.2 Scope of analytics [29](#__RefHeading___Toc11149810)

6.1.1.3.1.3 Level of aggregation [29](#__RefHeading___Toc11149811)

6.1.1.4 How NWDAF provides analytics [29](#__RefHeading___Toc11149812)

6.1.1.4.1 General [29](#__RefHeading___Toc11149813)

6.1.1.4.2 Content of Analytics responses/notifications [29](#__RefHeading___Toc11149814)

6.1.2 Impacts on Existing Nodes and Functionality [30](#__RefHeading___Toc11149815)

6.1.3 Solution Evaluation [30](#__RefHeading___Toc11149816)

6.2 Void [30](#__RefHeading___Toc11149817)

6.3 Solution 3: QoS Profile Provisioning [31](#__RefHeading___Toc11149818)

6.3.1 Description [31](#__RefHeading___Toc11149819)

6.3.1.1 Information for the support of QoS Profile Provisioning [31](#__RefHeading___Toc11149820)

6.3.1.2 Procedure to support QoS Provisioning and Adjustment [33](#__RefHeading___Toc11149821)

6.3.2 Impacts on Existing Nodes and Functionality [34](#__RefHeading___Toc11149822)

6.3.3 Solution Evaluation [34](#__RefHeading___Toc11149823)

6.4 Solution 4: Optimizing registration area management and Service area restriction adjustment based on NWDAF output [34](#__RefHeading___Toc11149824)

6.4.1 Description [34](#__RefHeading___Toc11149825)

6.4.1.1 General [34](#__RefHeading___Toc11149826)

6.4.1.2 Procedures [35](#__RefHeading___Toc11149827)

6.4.2 Impacts on Existing Nodes and Functionality [36](#__RefHeading___Toc11149828)

6.4.3 Solution Evaluation [36](#__RefHeading___Toc11149829)

6.5 Solution 5: Optimization based on paging failure prediction from NWDAF [37](#__RefHeading___Toc11149830)

6.5.1 Description [37](#__RefHeading___Toc11149831)

6.5.1.1 General [37](#__RefHeading___Toc11149832)

6.5.1.2 NWDAF Input Procedure - Paging event report procedure [38](#__RefHeading___Toc11149833)

6.5.1.3 NWDAF Output Procedure - Optimization based on paging failure prediction [39](#__RefHeading___Toc11149834)

6.5.2 Impacts on Existing Nodes and Functionality [39](#__RefHeading___Toc11149835)

6.5.3 Solution Evaluation [39](#__RefHeading___Toc11149836)

6.6 Solution 6: Data Collection from NFs/AFs using a new service [40](#__RefHeading___Toc11149837)

6.6.1 Description [40](#__RefHeading___Toc11149838)

6.6.1.1 Service definition [40](#__RefHeading___Toc11149839)

6.6.1.2 Subscription parameters [40](#__RefHeading___Toc11149840)

6.6.1.3 Notifications [41](#__RefHeading___Toc11149841)

6.6.1.4 Scope of Collectable Data Items [41](#__RefHeading___Toc11149842)

6.6.1.5 Procedure for Interactions with 5GC NFs for Data Collection Notification from 5GC NFs [42](#__RefHeading___Toc11149843)

6.6.1.6 Procedure for Interactions with 5GC NFs for Data Collection from 5GC NFs [43](#__RefHeading___Toc11149844)

6.6.1.7 Procedure Interactions with AFs for Data Collection Notification from AF [43](#__RefHeading___Toc11149845)

6.6.1.8 Procedure Interactions with AFs for Data Collection Notification from AF [44](#__RefHeading___Toc11149846)

6.6.1.9 Definition of CDIs in NFs and AFs [44](#__RefHeading___Toc11149847)

6.6.1.10 Procedure for Interactions with 5GC NFs for update of Data Collection Subscription to 5GC NFs [45](#__RefHeading___Toc11149848)

6.6.1.11 Procedure Interactions with AFs for update of Data Collection Subscription to AF [46](#__RefHeading___Toc11149849)

6.6.2 Impacts on Existing Nodes and Functionality [46](#__RefHeading___Toc11149850)

6.6.3 Solution Evaluation [46](#__RefHeading___Toc11149851)

6.7 Solution 7: Customizing mobility management based on NWDAF output [47](#__RefHeading___Toc11149852)

6.7.1 Description [47](#__RefHeading___Toc11149853)

6.7.2 Impacts on Existing Nodes and Functionality [48](#__RefHeading___Toc11149854)

6.7.3 Solution Evaluation [48](#__RefHeading___Toc11149855)

6.8 Solution 8: Performance improvement and supervision of mIoT terminals [48](#__RefHeading___Toc11149856)

6.8.1 Description [48](#__RefHeading___Toc11149857)

6.8.1.1 Information for the support of Performance improvement and supervision of mIoT terminals [48](#__RefHeading___Toc11149858)

6.8.1.2 Procedure for expected UE behavioural information provisioning [49](#__RefHeading___Toc11149859)

6.8.1.3 Procedure for mIoT terminals misused or hijacked Recognition [52](#__RefHeading___Toc11149860)

6.8.2 Impacts on Existing Nodes and Functionality [53](#__RefHeading___Toc11149861)

6.8.3 Solution Evaluation [53](#__RefHeading___Toc11149862)

6.9 Solution 9: Recommendations produced by NWDAF [53](#__RefHeading___Toc11149863)

6.9.1 Description [53](#__RefHeading___Toc11149864)

6.9.1.1 Service principles [53](#__RefHeading___Toc11149865)

6.9.1.2 Service definition [53](#__RefHeading___Toc11149866)

6.9.1.3 Recommendations Subscribe/Unsubscribe [54](#__RefHeading___Toc11149867)

6.9.1.4 Recommendations Request [54](#__RefHeading___Toc11149868)

6.9.1.5 Contents of subscribe and request operations [54](#__RefHeading___Toc11149869)

6.9.1.6 Contents of notifications and responses [55](#__RefHeading___Toc11149870)

6.9.2 Impacts on Existing Nodes and Functionality [56](#__RefHeading___Toc11149871)

6.9.3 Solution Evaluation [56](#__RefHeading___Toc11149872)

6.10 Solution 10: <NWDAF assisted Handover decision> [56](#__RefHeading___Toc11149873)

6.10.1 Description [56](#__RefHeading___Toc11149874)

6.10.1.1 General [56](#__RefHeading___Toc11149875)

6.10.1.2 Procedures [57](#__RefHeading___Toc11149876)

6.10.2 Impacts on Existing Nodes and Functionality [58](#__RefHeading___Toc11149877)

6.10.3 Solution Evaluation [58](#__RefHeading___Toc11149878)

6.11 Solution 11: UPF selection based on output from NWDAF [58](#__RefHeading___Toc11149879)

6.11.1 Description [58](#__RefHeading___Toc11149880)

6.11.1.1 General [58](#__RefHeading___Toc11149881)

6.11.1.2 Data Analytics-Based UPF Selection for Many UEs [58](#__RefHeading___Toc11149882)

6.11.1.2.1 Input Information for the support of NWDAF assisting traffic routing [58](#__RefHeading___Toc11149883)

6.11.1.2.2 Input Information from the SMF to request/subscribe for UPF selection related information [59](#__RefHeading___Toc11149884)

6.11.1.2.3 Output Information from the NWDAF for UPF selection [59](#__RefHeading___Toc11149885)

6.11.1.2.4 Procedure [59](#__RefHeading___Toc11149886)

6.11.2 Impacts on Existing Nodes and Functionality [61](#__RefHeading___Toc11149887)

6.11.3 Solution Evaluation [61](#__RefHeading___Toc11149888)

6.12 Solution 12: Data Collection from OAM using the existing SA WG5 services [61](#__RefHeading___Toc11149889)

6.12.1 Description [61](#__RefHeading___Toc11149890)

6.12.1.1 General [61](#__RefHeading___Toc11149891)

6.12.1.2 Procedure for the support of Data Collection from OAM [62](#__RefHeading___Toc11149892)

6.12.2 Impacts on Existing Nodes and Functionality [62](#__RefHeading___Toc11149893)

6.12.3 Solution Evaluation [62](#__RefHeading___Toc11149894)

6.13 Solution 13: Metadata exposure to 5GS NF and AF [63](#__RefHeading___Toc11149895)

6.13.1 Description [63](#__RefHeading___Toc11149896)

6.13.1.1 Metadata request by 5G NF [63](#__RefHeading___Toc11149897)

6.13.1.2 Available analytic information request by AF [63](#__RefHeading___Toc11149898)

6.13.1.3 How 5GS NF/AF request the metadata of the available analytic information [64](#__RefHeading___Toc11149899)

6.13.1.4 How NWDAF provides the available analytics metadata [64](#__RefHeading___Toc11149900)

6.13.2 Impacts on Existing Nodes and Functionality [64](#__RefHeading___Toc11149901)

6.13.3 Solution Evaluation [64](#__RefHeading___Toc11149902)

6.14 Solution 14: Data Collection from NFs via NF Event Exposure services [65](#__RefHeading___Toc11149903)

6.14.1 Description [65](#__RefHeading___Toc11149904)

6.14.1.1 Data Collection via NF/AF Event Exposure [65](#__RefHeading___Toc11149905)

6.14.1.2 Usage of Current exposure framework by the NWDAF [66](#__RefHeading___Toc11149906)

6.14.1.3 Collectable Data Item (CDI). [67](#__RefHeading___Toc11149907)

6.14.1.4 Discovering Collectable Data Item (CDI). [67](#__RefHeading___Toc11149908)

6.14.2 Impacts on Existing Nodes and Functionality [67](#__RefHeading___Toc11149909)

6.14.3 Solution Evaluation [68](#__RefHeading___Toc11149910)

6.15 Solution 15: Providing UE Analytics to the NWDAF via the User Plane [68](#__RefHeading___Toc11149911)

6.15.1 Description [68](#__RefHeading___Toc11149912)

6.15.1.1 Principles of the Solution [68](#__RefHeading___Toc11149913)

6.15.1.2 Requirements of the Header [68](#__RefHeading___Toc11149914)

6.15.1.3 Activating and Indicating Support for the Solution [68](#__RefHeading___Toc11149915)

6.15.1.4 Providing Analytic Data to the NWDAF [69](#__RefHeading___Toc11149916)

6.15.1.5 Privacy and Integrity Protection of the Analytic Data [69](#__RefHeading___Toc11149917)

6.15.2 Impacts on Existing Nodes and Functionality [69](#__RefHeading___Toc11149918)

6.15.3 Solution Evaluation [70](#__RefHeading___Toc11149919)

6.16 Solution 16: Use of UE analytics in the 5GC [70](#__RefHeading___Toc11149920)

6.16.1 Description [70](#__RefHeading___Toc11149921)

6.16.2 Impacts on Existing Nodes and Functionality [71](#__RefHeading___Toc11149922)

6.16.3 Solution Evaluation [71](#__RefHeading___Toc11149923)

6.17 Solution 17: Trace based solution to collect UE related information in NWDAF [71](#__RefHeading___Toc11149924)

6.17.1 Description [71](#__RefHeading___Toc11149925)

6.17.1.1 NWDAF subscribes the trace events to TCE [71](#__RefHeading___Toc11149926)

6.17.1.2 NWDAF triggers trace procedure [72](#__RefHeading___Toc11149927)

6.17.2 Impacts on Existing Nodes and Functionality [73](#__RefHeading___Toc11149928)

6.17.3 Solution Evaluation [73](#__RefHeading___Toc11149929)

6.18 Solution 18: NWDAF assisting Future Background Data Transfer (BDT) [73](#__RefHeading___Toc11149930)

6.18.1 Description [73](#__RefHeading___Toc11149931)

6.18.1.1 Information to support Future Background Data Transfer [74](#__RefHeading___Toc11149932)

6.18.1.2 Procedure for Future Background Data Transfer [74](#__RefHeading___Toc11149933)

6.18.2 Impacts on Existing Nodes and Functionality [74](#__RefHeading___Toc11149934)

6.18.3 Solution Evaluation [74](#__RefHeading___Toc11149935)

6.19 Solution 19: NWDAF/NWDAF service registration and metadata exposure to NFs [74](#__RefHeading___Toc11149936)

6.19.1 Description [74](#__RefHeading___Toc11149937)

6.19.1.1 Registration of NWDAF/NWDAF service into the NRF [75](#__RefHeading___Toc11149938)

6.19.1.2 NWDAF/NWDAF service discovery [75](#__RefHeading___Toc11149939)

6.19.2 Impacts on Existing Nodes and Functionality [76](#__RefHeading___Toc11149940)

6.19.3 Solution Evaluation [76](#__RefHeading___Toc11149941)

6.20 Solution 20: NWDAF analytics usage for UPF selection [76](#__RefHeading___Toc11149942)

6.20.1 Description [76](#__RefHeading___Toc11149943)

6.20.1.1 General [76](#__RefHeading___Toc11149944)

6.20.1.2 Procedures [77](#__RefHeading___Toc11149945)

6.20.2 Impacts on Existing Nodes and Functionality [78](#__RefHeading___Toc11149946)

6.20.3 Solution Evaluation [78](#__RefHeading___Toc11149947)

6.21 Solution 21: Supervision of IoT devices for risk precaution [78](#__RefHeading___Toc11149948)

6.21.1 Description [78](#__RefHeading___Toc11149949)

6.21.1.1 General [78](#__RefHeading___Toc11149950)

6.21.1.2 Identifying misbehaving UE(s) [78](#__RefHeading___Toc11149951)

6.21.1.3 Solving the risk brought by misbehaving UE(s) [80](#__RefHeading___Toc11149952)

6.21.1.4 Procedures [80](#__RefHeading___Toc11149953)

6.21.2 Impacts on Existing Nodes and Functionality [82](#__RefHeading___Toc11149954)

6.21.3 Solution Evaluation [82](#__RefHeading___Toc11149955)

6.22 Solution 22: Optimizing connection management based on NWDAF output [83](#__RefHeading___Toc11149956)

6.22.1 Description [83](#__RefHeading___Toc11149957)

6.22.1.1 General [83](#__RefHeading___Toc11149958)

6.22.1.2 Procedures [83](#__RefHeading___Toc11149959)

6.22.2 Impacts on Existing Nodes and Functionality [84](#__RefHeading___Toc11149960)

6.22.3 Solution Evaluation [84](#__RefHeading___Toc11149961)

6.23 Solution 23: AMF using NWDAF outputs to optimize UE mobility procedures [84](#__RefHeading___Toc11149962)

6.23.1 Description [84](#__RefHeading___Toc11149963)

6.23.1.1 General [84](#__RefHeading___Toc11149964)

6.23.1.2 Procedures [85](#__RefHeading___Toc11149965)

6.23.2 Impacts on Existing Nodes and Functionality [86](#__RefHeading___Toc11149966)

6.23.3 Solution Evaluation [86](#__RefHeading___Toc11149967)

6.24 Solution 24: Analytics Information Exposure to AF [86](#__RefHeading___Toc11149968)

6.24.1 Description [86](#__RefHeading___Toc11149969)

6.24.1.1 Procedure for AF subscription to NWDAF analytics [86](#__RefHeading___Toc11149970)

6.24.2 Impacts on Existing Nodes and Functionality [87](#__RefHeading___Toc11149971)

6.24.3 Solution Evaluation [87](#__RefHeading___Toc11149972)

6.25 Solution 25: Exposure with bulk subscription and NWDAF collecting data from UDR [87](#__RefHeading___Toc11149973)

6.25.1 Description [87](#__RefHeading___Toc11149974)

6.25.1.1 General [87](#__RefHeading___Toc11149975)

6.25.1.2 Procedures [88](#__RefHeading___Toc11149976)

6.25.2 Impacts on Existing Nodes and Functionality [89](#__RefHeading___Toc11149977)

6.25.3 Solution Evaluation [89](#__RefHeading___Toc11149978)

6.26 Solution 26: Data Collection using NRF services [89](#__RefHeading___Toc11149979)

6.26.1 Description [89](#__RefHeading___Toc11149980)

6.26.1.1 Service definition [89](#__RefHeading___Toc11149981)

6.26.2 Impacts on Existing Nodes and Functionality [89](#__RefHeading___Toc11149982)

6.26.3 Solution Evaluation [90](#__RefHeading___Toc11149983)

6.27 Solution 27: NWDAF assisting Determination of Background Data Transfer Policy [90](#__RefHeading___Toc11149984)

6.27.1 Description [90](#__RefHeading___Toc11149985)

6.27.1.1 NWDAF Data Collection [90](#__RefHeading___Toc11149986)

6.27.1.2 NWDAF output [91](#__RefHeading___Toc11149987)

6.27.2 Impact on Existing Nodes and Functionality [91](#__RefHeading___Toc11149988)

6.27.3 Solution Evaluation [91](#__RefHeading___Toc11149989)

6.28 Solution 28: Exposure to AF for Background Data Transfer [92](#__RefHeading___Toc11149990)

6.28.1 Description [92](#__RefHeading___Toc11149991)

6.28.1.1 NWDAF Data Collection [92](#__RefHeading___Toc11149992)

6.28.1.2 NWDAF output [92](#__RefHeading___Toc11149993)

6.28.1.3 PCF output [93](#__RefHeading___Toc11149994)

6.28.2 Impact on Existing Nodes and Functionality [93](#__RefHeading___Toc11149995)

6.28.3 Solution Evaluation [94](#__RefHeading___Toc11149996)

6.29 Solution 29: NWDAF assisted MICO mode for mIoT terminals [94](#__RefHeading___Toc11149997)

6.29.1 Description [94](#__RefHeading___Toc11149998)

6.29.1.1 MICO mode configuration by AMF [94](#__RefHeading___Toc11149999)

6.29.1.2 NWDAF assisted MICO mode configuration by AMF [95](#__RefHeading___Toc11150000)

6.29.1.2.1 Input Information for external parameter estimation [96](#__RefHeading___Toc11150001)

6.29.1.2.2 Output Information to AMF [96](#__RefHeading___Toc11150002)

6.29.1.2.3 Procedure [97](#__RefHeading___Toc11150003)

6.29.2 Impacts on Existing Nodes and Functionality [98](#__RefHeading___Toc11150004)

6.29.3 Solution Evaluation [98](#__RefHeading___Toc11150005)

6.30 Solution 30: Network Status in a specific geographic area [98](#__RefHeading___Toc11150006)

6.30.1 Description [98](#__RefHeading___Toc11150007)

6.30.1.1 General [98](#__RefHeading___Toc11150008)

6.30.1.2 Procedures [98](#__RefHeading___Toc11150009)

6.30.1.2.1 Procedure for one-time or continuous reporting of network status in a geographic area [98](#__RefHeading___Toc11150010)

6.30.1.2.2 Cancelling continuous reporting of network status [101](#__RefHeading___Toc11150011)

6.30.2 Impacts on Existing Nodes and Functionality [102](#__RefHeading___Toc11150012)

6.30.3 Solution Evaluation [102](#__RefHeading___Toc11150013)

6.31 Solution 31: Network Status for a specific UE [102](#__RefHeading___Toc11150014)

6.31.1 Description [102](#__RefHeading___Toc11150015)

6.31.1.1 General [102](#__RefHeading___Toc11150016)

6.31.1.2 Procedure for one-time or continuous reporting of network status for a specific UE [102](#__RefHeading___Toc11150017)

6.31.2 Impacts on Existing Nodes and Functionality [105](#__RefHeading___Toc11150018)

6.31.3 Solution Evaluation [105](#__RefHeading___Toc11150019)

6.32 Solution 32: Ensure slice SLA is guaranteed within certain region area [105](#__RefHeading___Toc11150020)

6.32.1 Description [105](#__RefHeading___Toc11150021)

6.32.1.1 Information for slice SLA guarantee [106](#__RefHeading___Toc11150022)

6.32.1.2 Procedure to support slice SLA guarantee with certain region area [106](#__RefHeading___Toc11150023)

6.32.2 Impacts on Existing Nodes and Functionality [107](#__RefHeading___Toc11150024)

6.32.3 Solution Evaluation [107](#__RefHeading___Toc11150025)

6.33 Solution 33: Ensure slice SLA is guaranteed within certain region area [107](#__RefHeading___Toc11150026)

6.33.1 Description [107](#__RefHeading___Toc11150027)

6.33.1.1 A Use Case [107](#__RefHeading___Toc11150028)

6.33.1.2 Providing Analytics to OAM to assist SLA monitoring [108](#__RefHeading___Toc11150029)

6.34 Solution 34: NWDAF collecting analytic information directly from UE [110](#__RefHeading___Toc11150030)

6.34.1 Description [110](#__RefHeading___Toc11150031)

6.34.1.1 General [110](#__RefHeading___Toc11150032)

6.34.1.2 UE sending IDLE related location information directly to the NWDAF [110](#__RefHeading___Toc11150033)

6.34.1.3 Usage of IDLE related location information by other NFs [111](#__RefHeading___Toc11150034)

6.34.1.4 Method to provide IDLE related location information to the NWDAF [111](#__RefHeading___Toc11150035)

6.34.2 Impacts on Existing Nodes and Functionality [111](#__RefHeading___Toc11150036)

6.34.3 Solution Evaluation [111](#__RefHeading___Toc11150037)

7 Overall Evaluation [111](#__RefHeading___Toc11150038)

7.1 Key Issue 1& Key Issue 2 [111](#__RefHeading___Toc11150039)

7.2 Key Issue 2: Analytic Information Exposure to AF [112](#__RefHeading___Toc11150040)

7.3 Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection [112](#__RefHeading___Toc11150041)

7.4 Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure [112](#__RefHeading___Toc11150042)

7.5 Key Issue 5: NWDAF-Assisted QoS Profile Provisioning [112](#__RefHeading___Toc11150043)

7.6 Key Issue 6: NWDAF assisting traffic routing [113](#__RefHeading___Toc11150044)

7.7 Void [113](#__RefHeading___Toc11150045)

7.8 Key Issue 8: Performance improvement and supervision of mIoT terminals [113](#__RefHeading___Toc11150046)

7.8.1 General mode for mIoT terminals [113](#__RefHeading___Toc11150047)

7.8.2 MICO mode for mIoT terminals [113](#__RefHeading___Toc11150048)

7.9 Key Issue 9: Customizing mobility management based on NWDAF output [113](#__RefHeading___Toc11150049)

7.9.1 Registration area allocation [114](#__RefHeading___Toc11150050)

7.9.2 Mobility restriction area handling [114](#__RefHeading___Toc11150051)

7.9.3 Paging handling [114](#__RefHeading___Toc11150052)

7.9.4 Handover decisions [114](#__RefHeading___Toc11150053)

7.9.5 Connection management [114](#__RefHeading___Toc11150054)

7.10 Void [114](#__RefHeading___Toc11150055)

7.11 Void [114](#__RefHeading___Toc11150056)

7.12 Key Issue 12: Support of Northbound Network Status Exposure [114](#__RefHeading___Toc11150057)

7.13 Void [115](#__RefHeading___Toc11150058)

7.14 Key Issue 14: How to ensure that slice SLA is guaranteed [115](#__RefHeading___Toc11150059)

8 Conclusions [117](#__RefHeading___Toc11150060)

8.0 Conclusions on the framework for analytics [117](#__RefHeading___Toc11150061)

8.1 Key Issue 1: Analytic Information Exposure to 5GS NF [117](#__RefHeading___Toc11150062)

8.2 Key Issue 2: Analytic Information Exposure to AF [117](#__RefHeading___Toc11150063)

8.3 Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection [117](#__RefHeading___Toc11150064)

8.4 Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure [118](#__RefHeading___Toc11150065)

8.5 Key Issue 5: NWDAF-Assisted QoS Profile Provisioning [118](#__RefHeading___Toc11150066)

8.6 Key issue 6: NWDAF assisting traffic routing [118](#__RefHeading___Toc11150067)

8.7 Key Issue 7: NWDAF assisting Future Background Data Transfer [118](#__RefHeading___Toc11150068)

8.8 Key Issue 8: Performance improvement and supervision of mIoT terminals [118](#__RefHeading___Toc11150069)

8.8.1 General mode for mIoT terminals [118](#__RefHeading___Toc11150070)

8.8.2 MICO model for mIoT terminals [118](#__RefHeading___Toc11150071)

8.9 Key Issue 9: Customizing mobility management based on NWDAF output [118](#__RefHeading___Toc11150072)

8.10 Void [119](#__RefHeading___Toc11150073)

8.11 Void [119](#__RefHeading___Toc11150074)

8.12 Key Issue 12: Support of Northbound Network Status Exposure [119](#__RefHeading___Toc11150075)

8.13 Key Issue 13: UE Driven Analytics [119](#__RefHeading___Toc11150076)

8.14 Void [119](#__RefHeading___Toc11150077)

8.14A Key Issue 14: How to ensure that slice SLA is guaranteed [119](#__RefHeading___Toc11150078)

Annex A: Examples on Network Data Analytics Feedback [120](#__RefHeading___Toc11150079)

A.1 Examples for EventID [120](#__RefHeading___Toc11150080)

A.2 Examples of Event Filter [120](#__RefHeading___Toc11150081)

A.3 Example of content of Subscription/Request [120](#__RefHeading___Toc11150082)

A.4 Example of content of notification/response [121](#__RefHeading___Toc11150083)

Annex B: Examples of usage of the CDI concept defined in solution 14 [122](#__RefHeading___Toc11150084)

Annex C: RRMPolicyRatio2 (extract from TS 28.541 [27]) [123](#__RefHeading___Toc11150085)

C.1 Definition [123](#__RefHeading___Toc11150086)

Annex D: Change history [124](#__RefHeading___Toc11150087)

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The aim of this Technical Report is to study and specify how to collect data and how to feedback data analytics to the network functions.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 23.502: "Procedures for the 5G System".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[5] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[6] 3GPP TS 23.724: "Study on Cellular Internet of Things (IoT) support and evolution for the 5G System".

[7] 3GPP TS 32.426: "Telecommunication management; Performance Management (PM); Performance measurements Evolved Packet Core (EPC) network".

[8] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[9] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[10] 3GPP TS 29.520: "5G System; Network Data Analytics Services; Stage 3".

[11] ITU‑T Recommendation P.1203.3: "Parametric bitstream-based quality assessment of progressive download and adaptive audiovisual streaming services over reliable transport - Quality integration module ".

[12] IETF RFC 8300: "Network Service Header (NSH)".

[13] 3GPP TS 28.550: "Management and orchestration of networks and network slicing; Performance Management; Stage 1".

[14] 3GPP TS 28.551: "Management and orchestration of networks and network slicing; Performance Management (PM); Stage 2 and stage 3".

[15] 3GPP TS 28.552: "Management and orchestration of networks and network slicing; NR and NG-RAN performance measurements and assurance data".

[16] 3GPP TS 28.553: "Management and orchestration of networks and network slicing; 5G Core Network (5GC) performance measurements and assurance data".

[17] 3GPP TS 28.554: "Management and orchestration of networks and network slicing; 5G End to end Key Performance Indicators (KPI), performance measurements and assurance data ".

[18] 3GPP TS 28.545: "Management and orchestration of networks and network slicing; Fault Supervision (FS); Stage 1".

[19] 3GPP TS 28.546: "Management and orchestration of networks and network slicing; Fault Supervision (FS); Stage 2 and stage 3".

[20] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[21] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[22] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[23] 3GPP TS 28.531: "Management and orchestration; Provisioning".

[24] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[25] OMA API Inventory: "http://technical.openmobilealliance.org/API/APIsInventory.aspx".

[26] 3GPP TR 28.805: "Telecommunication management; Study on management aspects of communication services".

[27] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

# 3 Definitions and Abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] apply.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply.  
An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

DN Data Network

NWDAF Network Data Analytics Function

OAM Operation, Administration, and Maintenance

OTT Over The Top

URSP UE Route Selection Policy

# 4 Architecture Assumptions

## 4.1 General

The following architectural assumptions are applicable for all potential solutions:

1 The NWDAF (Network Data Analytics Function) as defined in TS 23.503 [4] is used for data collection and data analytics in centralized manner. An NWDAF may be used for analytics for one or more Network Slice.

2 For instances where certain analytics can be performed by a 5GS NF independently, a NWDAF instance specific to that analytic maybe collocated with the 5GS NF. The data utilized by the 5GS NF as input to analytics in this case should also be made available to allow for the centralized NWDAF deployment option.

3 5GS Network Functions and OAM decide how to use the data analytics provided by NWDAF to improve the network performance.

4 NWDAF utilizes the existing service based interfaces to communicate with other 5GC Network Functions and OAM.

5 A 5GC NF may expose the result of the data analytics to any consumer NF utilizing a service based interface.

6 The interactions between NF(s) and the NWDAF take place in the local PLMN (the reporting NF and the NWDAF belong to the same PLMN).

7 Solutions shall neither assume NWDAF knowledge about NF application logic. The NWDAF may use subscription data but only for statistical purpose.

8 It is further assumed that NWDAF and NFs cooperate adequately to contribute to consistent policies, analytics output results, and finally decision-making in the PLMN.

## 4.2 General Framework

The Figure 4.2-1 shows general framework for 5G network automation in Release 16, depicting that the NWDAF should be able to collect data from the operator OAM, AFs and 5GC network functions.



Figure 4.2-1: general framework for 5G network automation

As part of this study, exchange of information between NWDAF and OAM may be defined. Interactions between OAM and NWDAF shall be based on use case requirements. The OAM could be a potential consumer or provider of the information for the NWDAF. The definition of such interaction shall be coordinated with SA WG5.

For the collection of OAM data, the NWDAF shall reuse existing mechanisms and interfaces defined by SA WG5. For OAM information exchange beyond existing mechanisms and interfaces defined by SA WG5, close co-operation with SA WG5 is needed.

Depending on network deployments and on AF(s), the AF may exchange information with the NWDAF via the NEF, or use the service based interfaces to access the NWDAF directly.

NWDAF accesses network data from data repositories (e.g. UDR).

For 5GC NFs, the NWDAF utilizes the service based interfaces to communicate to get network data and dedicated analytics.

Based on the aforementioned data collection, the NWDAF performs data analysis and provides the analytical result to the AF, the 5GC NFs and the OAM.

The output of the analytics provided to the AF, NFs, and OAM by the NWDAF and vice versa will be defined depending on the selected solutions for the key issues.

# 5 Use Cases and Key Issues

## 5.1 Use Cases

### 5.1.0 Introduction and guidelines

The NWDAF may serve use cases belonging to one or several domains, e.g. QoS, traffic steering, dimensioning, security.

The input data of the NWDAF may come from multiple sources, and the resulting actions undertaken by the consuming NF or AF may concern several domains (e.g. Mobility management, Session Management, QoS management, Application layer, Security management, NF life cycle management).

Use case descriptions should include the following aspects:

1. General characteristics (domain: performance, QoS, resilience, security; time scale).

2. Nature of input data (e.g. logs, KPI, events).

3. Types of NF consuming the NWDAF output data, how data is conveyed and nature of consumed analytics.

4. Output data.

5. Possible examples of actions undertaken by the consuming NF or AF, resulting from these analytics.

6. Benefits, e.g. revenue, resource saving, QoE, service assurance, reputation.

### 5.1.1 Use Case 1: <how to get information from AF>

#### 5.1.1.1 Description

Operators have already been able to collect some network information, e.g. through OAM to obtain the network data. However, the operators lack information from the service applications, especially for the 3rd party service applications. As a result, it is difficult for the operators to measure the actual service experience for the users and also don't know how to optimize the service.

Different service applications usually have different service requirement and probably could change their service frequently since the OTT behavior may often change based on its own requirement. Thus it is needed to:

- define a framework for data retrieval from AF(s).

- define common data that could be retrieved across multiple applications.

NOTE: The Study cannot define all data that may be retrieved from an application as such data may be application dependant.

Also some parameters, e.g. communication pattern and background traffic policy have already been defined in TS 23.501 [2] / TS 23.502 [3], which could be useful for the NWDAF architecture.

The use case is required to study how and what information the NWDAF obtains from the service applications.

In case of an AF belonging to a 3rd party would provide data to support NWDAF analytics, the AF may provide data to the NWDAF via the NEF. This use case requires to study potential signalling load impacts on the NEF.

### 5.1.2 Use Case 2: <NWDA-Assisted QoS Provisioning>

#### 5.1.2.1 Description

Currently, the 5G network can provide a QoS framework to support different QoS requirements of different traffic types and the QoS parameters are maintained by the system during the lifetime of the PDU sessions.

It is not clear how the network derives QoS profiles especially for non-standardized values and therefore it may be beneficial to leverage NWDA to perform/provide the big data analytics in order to help the CP functions to derive suitable QoS profiles.

The use case describes scenarios in which the NWDAF provides analytics that are used to improve the network resource utilization and user QoS experience, which includes:

- How/what types of network information that could be provided by NWDAF to the network to improve the network resource utilization and user QoS experience.

NOTE: This use case is not meant to support traffic congestion control i.e. the expected reaction time is assumed to be in order of magnitude of minutes.

### 5.1.3 Use Case 3: <NWDA-Assisted Traffic Handling>

#### 5.1.3.1 Description

Currently the SMF can select UPF for individual PDU Sessions based on multiple factors including the current load information of UPFs, UPF connection information, and UE request. However, the SMF may not have full statistics of network traffic.

This use case describes the information that may be provided by the network and the 5G-RAN and applications in DNs and analyzed by NWDAF in order to assist the UPF selection. In addition the NWDAF may assist for the definition of URSP(s).

### 5.1.4 Use Case 4: Using NWDAF output to customize mobility management

#### 5.1.4.1 Description

As investigated by SA WG1 and SA WG2, diverse service scenarios in 5G will introduce different requirements on mobility support, which requires on demand mobility management in 5G network, i.e. the 5G network should apply customized mobility management for UEs with different mobility and/or different usage patterns.

In 5G phase 1, SA WG2 has introduced mobility pattern to differentiate UE mobility behaviours, and discussed how to use the mobility pattern, but did not define the exact content of the UE mobility pattern and how to obtain the UE mobility pattern. This use case considers that the NWDAF can provide UE mobility related analytical report based on analysis on historical UE location, UE mobility behaviours and so on. Then, it will be feasible for the 5GC to use the NWDAF analytical results on a UE to customize the mobility management applied to the UE.

With the help of analytical results from the NWDAF, the 5GC can customize or optimize mobility management for each UE, including:

- Optimizing registration area allocation to reduce mobility registration update.

- Paging handling optimization.

- Adjusting mobility restriction area to accurately determine restriction area.

- NAS signalling connection management optimization to improve system efficiency and promise user experience.

- Adjusting periodic registration timer value to signalling saving.

- Handover optimization.

- Overload avoidance.

### 5.1.5 Use Case 5: <NWDA-assisted Determination of Policy>

#### 5.1.5.1 Description

Currently, the PCF can provide one or more policies for background data transfer based on requests from the 3rd party, before UE establishes the PDU session. Then, the PCF adopts the policies stored in the UDR. However, the network condition in the particular location may change after the UE establishes PDU session. Then, there are certain scenarios that the policy becomes unsuitable. Therefore, it is required that the PCF considers the latest network condition and the policy shall be updated based on some condition.

It is beneficial to leverage NWDAF to perform the big data analysis in order to create and to update a suitable policy. However, it is not clear how the network creates or updates the policy and notifies it of the 3rd party.

This use case considers the following scenarios in which the NWDAF provides the analysed information (e.g. traffic volume, congestion level, load status information in the specific network area), and which includes:

- How/what types of information that could be provided by NWDAF in order that the PCF creates the policy?

- How/what types of information that could be provided by NWDAF in order that the PCF updates the policy?

- How the updated policy is exposed to the 3rd party, if it is necessary?

- How information is made available to NWDAF for the data analysis?

### 5.1.6 Use Case 6: <NWDAF-Assisted QoS Adjustment>

#### 5.1.6.1 Description

3rd Party/Vertical provides an initial SLA(s) for the given services and 5GS maps the initial SLA(s) to the 5GS QoS parameters to guarantee service performance:

- For some services with stringent requirement e.g. from Vertical, the initial SLA(s) could be over-demanding with high network cost though the service performance is quite good.

- For some services e.g. from 3rd Party, no initial SLA is provided at all and the 5GS just uses default QoS flow, which is undemanding with rather low network cost but results in bad service performance.

Deriving an optimum QoS profile is a typical multi-objective optimization and involves MCDM (Multiple Criteria Decision Making), which means one single best QoS parameter combination may not exist with respect to all the objectives and instead there exists a set of QoS parameter combination(s), which are superior to the rest when considering all the objectives but inferior to the other in one or more objectives.

Therefore for either over-demanding or undemanding cases, based on the non-real time data information from 5GS and Application Server, NWDAF should provide data analytic to 5GS e.g. PCF prior to or during PDU session establishment, helping 5GS derive a set of QoS parameters combination(s) per service (which is different from the one derived from the initial SLA) and determine which combination(s) are in use per NF situation per time per UE location.

### 5.1.7 Use Case 7: NWDAF assisting 5G edge computing

#### 5.1.7.1 Description

Based on current 5G edge computing design, edge computing traffic routing is only influenced by Application Function based on relatively static configuration and field experience (AF influence has been defined in clause 5.6.7 of TS 23.501 [2] and clause 4.3.6 of TS 23.502 [3]), while AF doesn't have the dynamic performance information of whole network, as such, it's hard for PCF and SMF to make more accurate traffic routing decision by just taking AF's input into consideration. But NWDAF should have additional network information (e.g. load information based on time and spatial information, which service is subject to edge computing in some location, UE's mobility information) to assist the decision of PCF and SMF to route the traffic subject to edge computing.

To better satisfy this use case, SA WG2 needs to look into:

- Which information the NWDAF should have access to.

- Which information the NWDAF can provide to PCF/SMF to assist them making more accurate decision on whether and how to route traffic subject to edge computing with applying appropriate PCC rule(s).

### 5.1.8 Use Case 8: Performance improvement and supervision of mIoT terminals

#### 5.1.8.1 Description

The 5G mIoT feature is supposed to be popular in diverse usage scenarios and vertical industries. In some vertical industries, for a specific group, the service behaviours, data traffic (frequency, size) and moving areas probably have obvious regularity.

The business models for 5G mIoT are diversified, and the behaviours of mIoT terminals may vary a lot for different use cases, so requirements for quality of service and power saving are different.

The massive number of IoT terminals (such as street lamp, bicycle sharing etc.) may be misused or hijacked, which may result in security issue and may need special mechanisms for monitoring and supervision.

Therefore, for the operators, it is beneficial to be able to analyze the data produced by these IoT services to meet the requirements, e.g. to prevent the network congestion because of group activity, and manage or optimize the service parameters for better performance. An example is the detection of botnets.

### 5.1.9 Use Case 9: <NWDAF-assisted load balancing/re-balancing of network functions>

#### 5.1.9.1 Description

In Rel-15, the specification for load balancing/re-balancing of AMF was defined in clauses 5.19.3 and 5.19.4 TS 23.501 [2]. Currently, the operator, the NRF, or the AMF can judge the timing when the load balancing/re-balancing are executed for the AMF. In Rel-16, the specification for load balancing/re-balancing may be studied for the other network function as described in TR 23.724 [6] (FS\_eSBA). This use case targets a various types of network functions.

NWDAF can be leveraged to create the analysis based on the data information collected from the different network functions per network slices and/or per types of services, and provide analytics about the timing to execute the load balancing/ re-balancing per network slices and/or per types of services. It is beneficial to leverage the NWDAF to perform the big data analysis in order that the operator or the network function judges the timing to execute load balancing and re-balancing per network slices and/or per types of services. The big data analysis may estimate the suitable timing. Then, the operator can prevent the congestion beforehand and utilize their facility in an effective manner.

This use case considers the following scenarios in which the NWDAF provides the analysed information, and which includes:

- What kind of information is made available to the NWDAF for the data analysis.

NOTE 1: Any implementation specific parameter (e.g. resource of CPU and memory) is out of scope.

- Which kind of information should the NWDAF output to the other network function as the data analysis.

NOTE 2: Interaction with OAM including for NF LCM (life cycle management) will require interactions with SA WG5.

### 5.1.10 Use Case 10: NWDA-assisted determination of areas with oscillation of network conditions

#### 5.1.10.1 Description

Operators already use mechanisms for collection of information that enable CP and OAM to detect situations affecting the QoS of provided services. These current mechanisms are designed in a compartmentalized way i.e. focusing on per NF information data collection (e.g. TS 32.426 [7] defines measurements related to EPC entities - such as MME, etc. - which are aggregated values such as mean number of dedicated EPS bearers in active mode). In 5G, different services, such as URLLC (as defined in TS 22.261 [8]) and V2X (as recently defined in the SA WG1 FS\_V2XIMP and 5GAA NESQO), may require a network wide analysis to verify/improve NF deployment and configuration (e.g. wrt. the selection of the UPF). Operators will also be able to improve how to handle the effects of network slice dynamicity in E2E QoS assurance per slice and/or per type of service (i.e. performance requirements for groups of UEs associated with a type of service, e.g. V2X).

This use case investigates how NWDAF can be leveraged to collect information from the different sources NF(s), and Application Function, and provide analytics about segments/areas of the network where the provided QoS could be improved. By correlating and analyzing information coming from NF(s) with information coming from the AF (like MOS), NWDAF can provide statistical information that enables operators to change network deployment and configuration to improve E2E QoS.

Examples of potential improvements that could be triggered by analytics/prediction are:

a) The Application function offline report the service data (like MoS) to NWDAF, allowing NWDAF to have a snapshot of service experience for specific UEs.

b) The NWDAF correlates the service data with the information provided by the 5GS NF(s) to find out why the service experience is good or bad.

c) With the data analytics provided by NWDAF, the 5GS NF is able to improve service experience (e.g. in areas with dense traffic, for instance, the best compromise (cost / service delay) for UPF location could be determined).

d) In addition, the network could inform the application Function when UE is getting close to a potentially overloaded area, so that application Function can know that there is a higher chance of oscillation on network conditions.

### 5.1.11 Use Case 11: Prevention of various security attacks

#### 5.1.11.1 Description

Known issues belonging to the security domain that may take benefit of NWDAF services include:

1) Fraudulent access to services: potentially Fraudulent access may be detected by a disruption of traffic compared to known habits of the user. Services can be data, voice or other.

For these use cases, the aspects summarized in the following table need to be investigated.

Table 5.1.11.1-1

|  |  |
| --- | --- |
| Use case criteria | Description |
| Use characteristics | Security, not real-time |
| Potential provider NFs or AF | example :UPF, SMF, charging systems, AF (e.g. service chain on N6) |
| Input data | Statistics about traffic towards a service or destination address (e.g. IP address range). |
| Potential consumer NFs or AF | example :PCF, OSS, AF |
| Output data | Alerts, list of risky UE or destinations |
| Differentiation criteria | Traffic patterns: correlations between same UE and same target (voice call, data request towards same host), abnormal number of requests towards same target; abnormal number of request from usually less active UE. |
| Possible resulting actions by the consuming NF/AF | Security alerts, traffic blocking, temporary user blocking |
| Benefits | Avoid loss of revenue, service assurance, reputation |

NOTE 1: Security alerts are intended to be sent to a supervision system that is seen as an AF from the 5GS.

NOTE 2: SA WG3 will be involved as needed in the development of solutions addressing this use case.

### 5.1.12 Use Case 12: < NWDA-Assisted predictable network performance >

#### 5.1.12.1 Description

During autonomous driving, it would be helpful for advancing vehicles case to get predictable network performance (e.g. latency, reliability) of upcoming NG-RAN, i.e. eV2X application server can decide whether keeping autonomous driving mode in the upcoming NG-RAN based on the predicted network performance. Network performance of upcoming NG-RAN analyzed/predicted by NWDAF may consider the factors, e.g. speed and direction or upcoming location of the vehicle, network performance related information (load information based on time and spatial information).

In order to assist the decision of eV2X application server bases on predictable network performance from NWDA output, this use case considers the following issues:

- What analytical result is required to be provided by the NWDA to V2X application server?

- What input information is required for NWDAF to derive the analytical result and how to get this input information?

NOTE: Prediction period may be also studied, e.g. based on the requirement of service.

### 5.1.13 Use Case 13: <UE driven analytics sharing>

#### 5.1.13.1 Description

As UEs can simultaneously connect to or switch across different slices (e.g. in case of mobility), UEs can have more prominent role for data preparation for the NWDAF to provide relevant localised contextual information and to identify earlier any changes in the network compared to the past intra-slice and/or cross-slice information they have gathered. The processed information can be used for network slice selection for the UEs.

Examples of data that the UE can provide are positioning information (e.g. collected from inertial sensors of the UE, geo-referenced radio data from Wi-Fi), user profiling info (e.g. when a UE changes environment from outdoor to indoor, or from vehicular to pedestrian mode). Such information may help the NWDAF to make more intelligent decisions on slice selection (e.g. to switch from a slice with more flexible resources to a resilient one or vice versa).

Different types of enhancements can be envisioned for NWDAF to collect/process UE-driven analytics in order to improve slice selection.

For this use case, the following issues to be investigated:

- Exact role of NWDAF and/or other NFs in treating UE-driven analytics.

- Potential interaction/new services to be triggered between UE, AMF, NWDAF and other NFs (e.g. NSSF) to leverage UE-driven analytics.

- Security/trust aspects on integrity of such UE-driven analytics to avoid misleading information to the network.

- Privacy aspects related to the provision of UE-driven analytics.

### 5.1.14 Use Case 14: How to ensure that slice SLA is guaranteed

#### 5.1.14.1 Description

Considering the limited network resources (e.g., RAN/Transport/ CN resource) and a changing condition (e.g., Signal to Noise Ratio, more and more slices competing shared network resources), there is a risk for operators to guarantee the slice SLA at any time, e.g., how many percent of UEs' Service Experience (i.e. UE QoE or UE Service MoS ) is satisfied in a slice.

It is also not clear for operators how to assert that a slice SLA can be satisfied, and if this is not possible, what SLA can probably be promised to be met for each slice based on the overall consideration of meeting slice SLA of many slices. For example, as follows:

- When the SLA requirement(s) of some existing slice(s) changes, whether operators can meet the new SLA requirements of the existing slices, if not, what the slice SLA can be supported for operators.

- After several slices are already created and maintained, whether operators can meet the SLA of the existing slices and the new slice when receiving a new slice instantiation request from a slice customer. If not, what slice SLA can be supported for operators.

The case that UEs in one slice in different geographical areas may have different service experiences due to different network situation (e.g. possibly different transport path from RAN to TN to CN) can be considered.

Required Analytics information shall provide information on how the network meets or is expected to meet SLA:

- Globally.

- On a per slice level.

- On a per geographical area per slice level.

Editor's note: The granularity of the geographical area is FFS and needs the coordination with SA WG5.

Editor's note: Whether information on the type (CP or UP) of potential issues is to be provided is FFS and needs the coordination with SA WG5.

The use case describes scenarios in which analytics information that are used to assist the guarantee of slice level SLA, which includes:

- How/what types of data analytics information that could be provided to OAM to assist the guarantee of slice SLA. Whether there is any need to provide analytics information to NFs.

- How/what types of network information that are needed for analysis from OAM or from NFs.

The analytics result can be used for operators to assist the adjustment of network resource scheduling to maximize the slices SLA from several aspects, for example, as follows:

- Whether the SLA of a slice can be satisfied?

- What distribution of UEs' Service Experience per slice (e.g., how many percent of UE's Service MoS is between 3 and 4 and how many percent of UE's Service MoS is between 4 and 5) can be met?

## 5.2 Key Issues

### 5.2.1 Key Issue 1: Analytic Information Exposure to 5GS NF

#### 5.2.1.1 Description

A 5GS NF may request or subscribe from NWDAF for providing analytic information to facilitate the NF for decision making. The analytic information may be requested and/or provided prior to or after UE registration or a PDU session establishment.

The 5GS NF may indicate in the request the expected output from the NWDAF. Based on the input from the 5GS NF, the NWDAF needs to provide the analytic information to the NF.

A 5GS NF may query to the NWDAF to obtain the metadata of the available analytic information (e.g. list of available analytic information, metrics, etc.), and the NWDAF should provide the analytic information metadata when a query from 5GS NF is received through 5G service based interface.

In this key issue, the following mechanisms need to be studied:

- How a 5GS NF requests or subscribes to the NWDAF for providing analytic information (or relevant analytic information subset).

- How the NWDAF provides/updates the analytic information to the 5GS NF.

- How the NWDAF provides/updates the available analytic information metadata to the 5GS NF (or subset of relevant analytic information metadata).

#### 5.2.1.1 Requirements

The NWDAF services shall permit to specify which relevant analytic information subsets are requested or notified.

### 5.2.2 Key Issue 2: Analytic Information Exposure to AF

#### 5.2.2.1 Description

AF may request or subscribe to the NWDAF for providing analytic information to facilitate AF to derive requirements to the network.

The analytic information may be provided prior to or during an AF session.

AF may indicate in the request the expected output. Based on the AF input, the NWDAF needs to provide the analytic information to the AF.

An AF may query to the NWDAF to obtain the metadata about the available analytic information (e.g. list of available analytic information, metrics, etc), and the NWDAF should provide the analytic information metadata when a query received through 5G service based interface. This message exchange may occur via NEF.

The AF may be an operator owned AF or an 3rd party AF.

In this key issue, the following mechanisms need to be studied:

- How an AF requests or subscribes to the NWDAF for providing analytic information (or relevant analytic information subset).

- How the NWDAF provides/updates the analytic information to the AF.

- How the NWDAF provides/updates the available analytic information metadata to the AF (or subset of relevant analytic information metadata).

#### 5.2.2.2 Requirements

The NWDAF services shall permit to specify which relevant analytic information subsets are requested or notified.

### 5.2.3 Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection

#### 5.2.3.1 Description

Use cases listed have a common requirement that NWDAF collects the data information present in the 5G system from other 5G NFs and AF(s) for analytic purposes.

NWDAF may access data of different data types, e.g. data related to a UE, a PDU session, an NF and a slice instance.

Such data can be described according to various aspects:

1. Granularity: individual events, KPIs, list of events.

2. Temporality: periodical, on demand by NWDAF, triggered by specific criteria, with validity period.

3. Format: data files (e.g. event logs), SBI requests.

4. Individuality: aggregated data (several UE) vs single scoped data (single UE) with possible anonymization.

In order to permit interoperability between NFs and NWDAF, it is necessary to define a framework for the provision of data to the NWDAF by 5GC NFs and/or AFs, and the associated basic information set.

In addition, some of the information to be collected may be vendor / operator / deployment specific and so the data collection framework should be flexible enough to carry previously undefined / non-standard data (e.g. syslogs, call logs, vendor specific KPIs).

In this key issue, the following issues need to be studied:

- Framework for data collection.

- Which/how 5GC NFs/AF can provide the data information to NWDAF?

- Scoping and filtering: should the NWDAF be able to request (or subscribe) for the collection of analytics subsets in order to avoid uploading high volumes of unnecessary data, for instance on-demand analytics requested by the NWDAF to an NF, on the basis of an API allowing structured query (e.g. list of SBI events of type S during timeframe T, for instance related to certain KPIs for a subset of UEs on a specific DNN during last hour)?

- Authentication and authorisation: how does the 5G system enforce authentication and authorization of the NWDAF for a certain data access, if required?

#### 5.2.3.2 Requirements

The NWDAF shall be able to collect data from the 5GS NFs and AFs.

A flexible framework for data collection (interfaces, basic information model and extension rules) should be defined.

The NWDAF should be able to refine the scope of collected information, on a per request basis.

The 5GC should enforce authentication and authorization of the NWDAF for a certain data access.

### 5.2.4 Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure

#### 5.2.4.1 Description

Use cases listed have a common requirement that NWDAF can use for analytic purposes some data that is available in OAM system.

The following topics should be addressed by SA WG2 in collaboration with SA WG5.

- Framework for making OAM data available to NWDAF:

- How/whether NWDAF is to retrieve the network level KPIs from OAM.

- Framework for making NWDAF data analytics available to OAM:

- Granularity of Data analytics provided by NWDAF to OAM.

- What data and how the data can be provided from OAM to NWDAF?

- Several metrics and KPIs are already defined for OAM (TS 28.XXX series). Could such metrics be reused for NWDAF as set of basic data from each NF?

- Could NWDAF use the already existing services provided by the OAM?

- How to ensure that different NFs and OAM will not consume the same analytics from NWDAF and avoid the triggering of simultaneous and potentially unnecessary changes in 5GS network?

#### 5.2.4.2 Requirements

The NWDAF shall be able to have access to data from the OAM.

The NWDAF shall be able to provide analytics to OAM if required by SA WG5.

A flexible framework for making OAM data available to NWDAF (interfaces, basic information model and extension rules) should be defined.

The NWDAF should be able to refine the scope of required information as needed.

The 5GC should be able to enforce authentication and authorization of the NWDAF for a certain data access.

### 5.2.5 Key Issue 5: NWDAF-Assisted QoS Profile Provisioning

#### 5.2.5.1 Description

A NF may request or subscribe from NWDAF for providing analytic information in order for the NF to define the appropriated non standardized 5QI characteristic and accordingly it is needed to identify what information is needed by the NWDAF from NF or AF as input for data analytics.

In this key issue, the following mechanisms need to be studied:

- What/How a NF requests or subscribes to the NWDAF for providing analytic information to define the appropriated non standardized 5QI characteristic.

- What information is provided to the NWDAF for data analytics (i.e. what information from the relevant NF(s) and/or OAM and/or other AF(s) is provided to the NWDAF);

NOTE: This key issue is to discuss and list the potential and necessary information for the support of this key issue. Data collection framework and how NWDAF collects the data is to be addressed by Key Issue X: Data Collection Framework.

#### 5.2.5.2 Requirements

The NWDAF shall be able to provide analytic information helping a client NF to define the appropriate non standardized 5QI characteristic based on e.g. the requirement of the 5GS NF or AF.

### 5.2.6 Key Issue 6: NWDAF assisting traffic routing

#### 5.2.6.1 Description

To satisfy the identified use case #3 and #7, following issues need to be studied:

- which information the NWDAF should have access to for analytics purpose in assisting of traffic routing;

- which information the NWDAF can provide to PCF/SMF to assist them making more accurate decision on how to select DNAI for traffic routing with applying appropriate PCC rule(s).

### 5.2.7 Key Issue 7: NWDAF assisting Future Background Data Transfer

#### 5.2.7.1 Description

To satisfy the identified use case #5, where NWDAF provide analytics information for Future Background Data Transfer, the following issues need to be studied:

- What types of analytics information for Future Background Data Transfer could be provided by NWDAF for the PCF to determine the policy of future background data transfer;

- What information does NWDAF need as input to determine such analytics information.

#### 5.2.7.1 Requirements

Editor's note: This clause provides the requirements the solutions to this key issue need to address.

### 5.2.8 Key Issue 8: performance improvement and supervision of mIoT terminals

#### 5.2.8.1 Description

As introduced in use case 8, the 5G mIoT feature is supposed to be popular in diverse usage scenarios and vertical industries. In some vertical industries, for a specific group, the service behaviors, data traffic (frequency, size) and moving areas probably have obvious regularity. The business models for 5G mIoT are diversified, and the behaviors of mIoT terminals may vary a lot for different use cases, thus requirements for quality of service and power saving are different. The IOT terminals with massive number of users may be misused or hijacked, which may result in security issue and may need special mechanisms for monitoring and supervision.

In order to support performance improvement and supervision of mIoT terminals based on NWDA output, the following issues are required to be investigated:

- What necessary input is required for the NWDAF- considering both operator owned and third party mIoT terminals;

- What analytical results can be provided by the NWDAF for performance improvement and supervision of mIoT terminals?

### 5.2.9 Key Issue 9: Customizing mobility management based on NWDAF output

#### 5.2.9.1 Description

As introduced in the investigated use case 4, diverse service scenarios in 5G will introduce different requirements on mobility support, which requires on demand mobility management in 5G network, i.e. the 5G network should apply customized mobility management for UEs with different mobility and/or different usage patterns.

In this key issue, it is supposed that the NWDAF can provide UE mobility related analytical report based on analysis on historical UE location, UE mobility behaviours and so on. Then, it will be feasible for the 5GC to use the NWDAF analytical results on a UE to customize the mobility management applied to the UE.

In order to support customizing mobility management based on NWDAF output, following issues are required to be investigated:

- What analytical results can be provided by the NWDAF for per UE mobility management optimization and what information is provided to the NWDAF (i.e. what information from the relevant 5GS NF(s) and/or OAM and/or the other AF(s) is provided to the NWDAF)?

NOTE: This key issue is to discuss and list the potential information for the support of providing mobility related analytical report while data collection framework and how NWDAF collects the data is to be addressed by Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection and/or Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure.

- Which network function(s) can directly interact with the NWDA to retrieve/receive the analytical results?

- Potential areas of investigation for customized mobility management are: registration area allocation, paging handling, mobility restriction area handling, NAS signalling connection management, periodic registration timer handling, handover decisions, overload avoidance, RFSP index change.

#### 5.2.9.2 Requirements

The NWDAF shall collect the data related to UE mobility from the OAM and/or 5G NF(s).

The NWDAF shall provide the mobility analytic and/or prediction information for a UE to the requested 5G NF(s).

### 5.2.10 Key Issue 10: NWDAF service support to select NF instances

#### 5.2.10.1 Description

It is beneficial to leverage the NWDAF to perform data analytics for assistance in selection of an optimal NF instance where multiple instances of that NF exist within a slice or shared across multiple slices. Consumers of this analytic information can be an SMF used for UPF steering/selection or an NRF. The optimization of NF instance selection by the consumer AF/NF for example can be influenced by analytics of network deployment topology for NF instances and historic/current network condition aspects such as load levels information across multiple instances of a NF in the geographic location of the service area. The intent in such a scenario of an operator's NF instance selection policies maybe for example to optimally distribute overall load or the load specific to a service across multiple instances of NFs within a slice and in a geographic location. However, in Rel-15, the NWDAF just outputs the load level information of the network slice instance. It is not used by the NF consumer to select the suitable NF instance in consideration of network slice, and/or per types of services. Therefore, the update of NWDAF service is necessary. It is also necessary to consider the case that the NF instance would be shared among the multiple network slices.

When the NWDAF provides the suitable analysis information the NF consumer is able to select the optimal NF instance, thereby helping the operator with optimal running of the network in alignment with it's policies. This key issue is related to use case #9.

NOTE 1: The solution needs to coordinate with FS\_eSBA, SA WG5 and CT WG4 work.

In this key issue, the following mechanisms need to be studied:

- What available information in the network function is accessed by the NWDAF.

- What kind of information is provided by the NWDAF; and

- Which network function shall utilize the NWDAF service.

NOTE 2: Any implementation specific parameter (e.g. resource of CPU and memory) is out of scope.

#### 5.2.10.2 Requirement

- The NWDAF shall be able to collect data from the NF instance per network slices, and/or per types of services.

- The NWDAF shall create the analysis information in consideration of network slices and/or per types of services.

The NWDAF shall provide the analysis information to the NF consumer to assist in its selection of a NF instance.

### 5.2.11 Key Issue 11: NWDA-Assisted predictable network performance

#### 5.2.11.1 Description

This key issue is to address the use case #12. An AF may request or subscribe to the network for providing analytic information related to the expected network performance. The AF may take actions for their devices such as charging automotive driving into human control driving.

In this key issue, the following issues need to be studied:

- What network parameter information does NWDAF should have access to for analytics purpose in expected network performance and how can it be obtained?

- How does NWDAF output network performance information to the ASP?

- What network performance information can be considered? (e.g. QoS/load information based on time and spatial information, etc.).

- Whether NWDAF could provide network performance information to other 5G NF except AF and how?

- What type of expected network performance can be provided?

NOTE: The related work will be coordinated with SA WG5.

#### 5.2.11.2 Requirements

The NWDAF shall be able to provide expected network performance information to the ASP.

### 5.2.12 Key Issue 12: Support of Northbound Network Status Exposure

#### 5.2.12.1 Description

A Release 15 NEF currently supports a subset of SCEF Northbound APIs. One of the APIs currently not supported by NEF is for Reporting of Network Status. TS 29.122 [9] describes the functionality of this API as follows:

*"The ReportingNetworkStatus API is a RESTful API that allows the SCS/AS to be one-time or continuous notified of the network status in a geographic area."*

This key issue would study the collection of information related to user plane congestion from OAM based on which network congestion status being experienced by a UE in its current location can be exposed. Work related with getting network status in a location will be done at SA WG5.

#### 5.2.12.2 Requirement

NEF shall expose network status using an API equivalent type to T8's *ReportingNetworkStatus* API.

### 5.2.13 Key Issue 13: UE driven analytics

#### 5.2.13.1 Description

To satisfy the identified use case #13, where the network enhancements can be envisioned based on the UE-driven analytics in NWDAF, the following issues will be studied:

- The types of analytics information that could be provided by NWDAF to other NFs to leverage the data provided by the UE;

- How the NWDAF uses the data provided by the UE to do analytics and provides the analytics information to other NFs;

- How the network utilizes the analytics information from NWDAF;

- What type of information from the UE is collected by the network;

- How frequently such analytics are to be shared with the NWDAF;

- How the NWDAF collects the UE's information;

- What are the triggers for the UE to provide analytics to the network;

- How to ensure the integrity of UE-provided information in order to avoid using misleading information in the network;

- Whether there are privacy aspects, related to the information provided by the UE.

#### 5.2.13.2 Requirements

The NWDAF shall be able to receive UE's analytics data.

It shall be possible to ensure the privacy and integrity of the analytics data from the UE (e.g. in the case of roaming).

The NWDAF shall be able to provide prediction information to other NFs to leverage UE-driven analytics.

NOTE 1: It's not assumed that there is a direct interface between the UE and NWDAF.

NOTE 2: If the RRC procedure is triggered due to NWDAF requires UE's information from RAN, the detail of the RRC procedure will be discussed in RAN group.

### 5.2.14 Key Issue 14: How to ensure that slice SLA is guaranteed

#### 5.2.14.1 Description

Based on use case #14, following issues need to be studied:

- Which network slice level KPIs defined in OAM (e.g. TS 28.554 [17]) can be used for analysis to guarantee slice level SLA?

- Whether OAM may need any information from NF or NWDAF the guarantee of slice level SLA?

- What and how analytic data is provided to OAM or NFs for the purpose of guaranteeing slice level quality?

The following are examples of how analytics result can be used:

- Whether slice(s) SLA of a slice can be satisfied?

- What distribution of UEs' Service Experience per slice (e.g., how many percent of UE's Service MoS is between 3 and 4 and how many percent of UE's Service MoS is between 4 and 5) can be met?

NOTE: The feature supporting this use case should be defined in Rel-16. And it requires SA WG5 to start the related work, and more coordination with SA WG2. The solution investigation in SA WG2 is suggested to wait for the response of SA WG5 on it.

#### 5.2.14.2 Requirements

It shall be possible to use analytics information to ensure that the SLA with the ASP is guaranteed (on global level, or slice level or in a geographical area per slice level).

# 6 Solutions

## 6.1 Solution 1: Network Data Analytics Feedback

### 6.1.1 Description

#### 6.1.1.0 General

This is a solution to Key Issue#1: Analytic Information Exposure to 5GS NF.This solution is to define the framework for network data analytics feedback and the detailed parameters of the network data analytics will be defined in each of the solutions to the key issues corresponding to specific use cases.

The solution extends the features of NWDAF as exposed in clause 4.19 of TS 23.502 [3] by enabling statistics for data or events collected in the past and based on these statistics, predictions for data or events in the future. It integrates Event Filter Information, Event Reporting Information, and Target of Event Reporting as defined for network exposure framework in clause 4.15.1 of TS 23.502 [3].

#### 6.1.1.1 Network data analytics Subscribe/Unsubscribe

This procedure is used by any NF service consumer) to subscribe/unsubscribe at NWDAF to be notified on analytic information, using existing Nnwdaf services defined in TS 23.502 [3]. Any entity can consume this service as far as they follow SBI defined in TS 23.502 [3].



Figure 6.1.1.1-1: Network data analytics Subscribe/unsubscribe

1. The NF service consumer subscribes to or cancels subscription to analytic information by invoking the Nnwdaf\_EventsSubscription\_Subscribe/ Nnwdaf\_EventsSubscription\_Unsubscribe service operation.

2. If NF service consumer subscribes to analytic information, the NWDAF notifies the NF service consumer with the analytic information by invoking Nnwdaf\_EventsSubscription\_Notify service operation.

#### 6.1.1.2 Network data analytics Request

This procedure is used by the NF service consumer (e.g. UDM, AMF, SMF, PCF) to request and get from NWDAF analytic information, using Nnwdaf\_AnalyticsInfo\_Request defined in TS 23.502 [3].



Figure 6.1.1.2-1: Network data analytics Request

1. The NF service consumer requests analytic information by invoking Nnwdaf\_AnalyticsInfo\_Request service operation.

2. The NWDAF responds with analytic information to the NF service consumer.

#### 6.1.1.3 How a NF requests or subscribes to analytics

A NF subscribes or requests analytics using the Nnwdaf service defined in clause 6.1.1.1 that needs to allow new EventIds to resolve the existing key issues.

NOTE: If Subscription information includes a UE identity or a list of UE identities, privacy issues should be taken into account, e.g. user consent.

Each analytics defined in other solutions should reuse the following same framework to define the parameters of the analytics request to the NWDAF.

#### 6.1.1.3.1 Content of Analytics requests/subscribe

##### 6.1.1.3.1.1 General

In addition to basic SBI parameters defined in TS 29.520 [10], the requests or the subscription to analytics should contain:

- Type of analytics: Event ID as defined in TS 23.502 [3] clause 4.15.1 , possibly extended to fit to use cases.

- Analytics filtering information: Event Filter Information (as defined in TS 23.502 [3] clause 4.15), this set of parameter types and values enables to select which type of analytics information are requested (e.g. subset of all available analytics produced by NWDAF for the given Event ID value). Details on this information are described in clause 6.1.1.3.1.2.

- Target of Event Reporting (as defined in TS 23.502 [3] clause 4.15.1): the object targeted by analytics/predictions (UEs, group of UE(s), any UEs). The Target of event reporting defined in TS 23.502 [3] clause 4.15.1 is reused (and extended) for that purpose. Details on this information is described in clause 6.1.1.3.1.2.

- Level of aggregation. Details on this information is described in clause 6.1.1.3.1.3.

- Observation period: time interval [start..end] covered by the computation, either in the past or in the future, expressed as positive or negative offsets to the present. An interval in the past is a request for statistics. An interval in the future is a request for predictions. A default value means statistics in the recent past, with a time range defined by the NWDAF.

- A Notification Target Address (+ Notification Correlation ID) as defined in TS 23.502 [3] clause 4.15.1, allowing the Event Receiving NF to correlate notifications received from the NWDAF with this subscription.

- Event Reporting Information (as described in the TS 23.502 [3] Table 4.15.1-1).

This parameter already supports the configuration of the Mode of Reporting (e.g. reporting up to a maximum number of reports allowing a one-shot analytics request, periodic reporting along with periodicity, reporting up to a maximum duration) or the request to notify immediately the current status of the subscribed statistics, if available, to the requesting NF.

- Optional preferences on analytics (e.g. computation constraints) : list of preference items.

NOTE: The exact definition of preferences items on analytics/predictions is left for the normative phase. A first proposed item is the preferred level of accuracy of the analytics (values low/high). There is a trade-off between the level of accuracy and the computation load.

##### 6.1.1.3.1.2 Scope of analytics

The scope of analytics is denoted by the combination of Target of Event Reporting (TER) and Event Filtering Information (EFI).

As specified in TS 23.502 [3] clause 4.15.1, the target of event reporting indicates entities such as specific UEs, a group of UE(s) or any UE (i.e. all UEs).

The Event Filter Information (as specified in TS 23.502 [3] clause 4.15) is a set of value assertions (i.e., Type = value) which determines which restricts the production of relevant analytics.

Each parameter may or may not support wildcards. In case of wildcards, it shall be possible to specify either an empty wildcard meaning "all values", or a constrained wildcard by denoting a range of values.

The parameters may be organized as a set of additional value assertions (e.g. equality assertions, wildcards).

##### 6.1.1.3.1.3 Level of aggregation

In complement, the consumer may provide the level of aggregation which may be used to determine whether the provided statistics are aggregated for all entities or individually listed i.e. provided for each individual value. The parameter Level of aggregation may take one of the following values: explicit lists per UE, per UE group, per TA, per Cell, or per DNN. Additional values may be proposed in further studies. The parameter is only mono-instantiated, therefore restricts on one single dimension the collection of statistics.

When level aggregation is chosen, the cumulative value of the measurement shall be provided, depending on the type of statistics. The cumulative value uses the same computation rules as each individual item, with just a broader computation scope.

When individually listed, all matching values corresponding to the wildcard are requested.

#### 6.1.1.4 How NWDAF provides analytics

##### 6.1.1.4.1 General

A NF subscribes to or requests analytics using the Nnwdaf service defined in clause 6.1.1.1 that needs to allow new EventIds to resolve the existing key issues.

The NWDAF functionality does not overlap the existing NF functionality.

Each analytics defined in other solutions should reuse the same following framework to define the parameters of the analytics request to the NWDAF. This framework follows the framework already defined in TS 23.502 [3] clause 4.15.

##### 6.1.1.4.2 Content of Analytics responses/notifications

In addition to basic SBI parameters defined in TS 29.520 [10], the response or the notification to analytics should contain:

- Identification of the request/subscription including:

- Notification Correlation Id (provided in the subscription request);

- The Event ID (one of the Event Id provided in the request),

- The analytics output includes:

- Related list of analytics on the requested observation period;

- Optional additional information:

- Timestamp of analytics generation, which allows consumers to decide until when the received information shall be used. For instance, an NF can deem a received notification from NWDAF for a given feedback as invalid based on this timestamp;

- Probability assertion: level of certainty, degree of confidence in statistics/prediction. A probability assertion may be provided per each analytics if an explicit list has been requested.

### 6.1.2 Impacts on Existing Nodes and Functionality

NWDAF: New EventIds are provided. No impacts on the existing Nnwdaf interface, except for the slicing information that should become optional, as other event filters should be allowed.

Consumer NF: For a NF such as PCF or NSSF that are consumers of Nnwdaf service, the impacts are to support new EventIds if required by each of the solutions. For other new consumers, the impacts are listed the solutions to each key issue.

The solution is compatible with the existing NWDAF services as exposed in clause 4.19 of TS 23.502 [3] (NnwdafAnalyticsInfo and Nnwdaf\_EventSubscription). The content of the operations for subscribe/request and notify/response of such services are extended. The solution extends the features of NWDAF as exposed in TS 23.502 [3], by enabling both analytics in the past and predictions in the future.

It integrates Event Filter Information, Event Filter information, and event target, parameters as defined for network exposure framework in clause 4.15 of TS 23.502 [3] or clause 5.3 of TS 29.518 [22].

Usage of non UE targets (NFs or groups of NFs) is optional. It needs to be defined in conjunction with SA WG5. Non UE targets (e.g. NFs) may typically be requested to help optimizing NF selection.

### 6.1.3 Solution Evaluation

The solution provides application-agnostic analytics.

It enables to collect statistics in the past and predictions in the future related to various domains, leaving all decisions to the consumer NF.

This solution preserves the current defined services for analytics exposure defined in NWDAF, i.e., Nnwdaf\_EventSubscription and Nnwdaf\_AnalyticsInfo, as it indicates that the procedures for analytics exposure are the same as in Solution 1.

This solution keeps the alignment with the Network Exposure defined in TS 23.502 [3] clause 4.15. Nevertheless, this solution defines in detail the content of subscribe/request and notify/response messages associated with such services.

The proposed content of these messages requires the current definition of the NWDAF service operations in TS 23.502 [3] to be extended to support such solution.

The proposed extensions of the NWDAF service operations allows NWDAF to provide analytics that go beyond network slice load analytics as defined in Rel‑15 (TS 23.501 [2]) and supports thus the analytics identified as required in the Use Cases defined in clause 5.1.

## 6.2 Void

## 6.3 Solution 3: QoS Profile Provisioning

### 6.3.1 Description

This solution is for Key Issue 5: NWDAF-Assisted QoS Profile Provisioning.

At the moment, it is still not clear how to drive the value of the non-standardized 5QI, though 5GS e.g. PCF may derive the initial 5G QoS parameter combination based on operator policies that may take into account the SLA between the MNO and the Vertical/3rd Party.

Application server from vertical/3rd party will measure their own important service i.e. vertical/3rd party is aware of the service experience and therefore if vertical/3rd party have strong requirement to better guarantee/improve their service quality, they should provide both service characteristics and observed service experience to operator, which allows operator to check if the observed service experience is according to the SLA and then modify the 5G QoS parameter combination (together with Network data).

However, the accurate QoS parameter combination could be more than one due to multi-objective optimization/MCDM (Multiple Criteria Decision Making), which means one single globally best QoS parameter combination may not exist with respect to all the objectives and instead there exists a set of QoS parameter combination(s), which are superior to the rest when considering all the objectives but inferior to the other in one or more objectives:

- For example, QoS parameters per Service MOS (e.g. one is for Service MOS∈{3.0, 4.0} and the other is for Service MOS∈{4.0, 5.0}) are initially assigned by PCF, and then if gNB may not be able to comply with the target QoS , the gNB sends QNC to notify the that QoS requirements cannot be met any longer.:

- In weak coverage, gNB may transmit the same Packets to UE several times in order to improve Packet Error Rate, which on the contrary increases Packet Delay and may further have an impact on Guaranteed Flow Bit Rate. If gNB finds that the QoS contract cannot be fulfilled it will send a QNC.

- While in good coverage, gNB does not need to transmit the same Packets to UE several times as both Packet Error Rate and Packet Delay is good enough, then gNB is able to fulfil the QoS contract.

Therefore, for the given application, there is no need to provide multiple QoS combinations per the given Service Experience (i.e. Service MOS window) to PCF depending on network conditions, since the existing QoS solution in TS 23.501 [2] can deal with changing network conditions today.

Please note that the vertical/3rd party should provide the correct service experience data to operator if they have strong requirement to better guarantee/improve their service quality. However, the operator cannot fully trust/rely on the service experience observed by vertical/3rd party and therefore the operator also need to measure/monitor the service quality and if the service quality observed by operator is very close to the one observed by vertical/3rd party, then it means the trade-off between service quality and network cost is achieved, which is a win-win state for operator and vertical/3rd party.

The estimated Service Experience is provided to the PCF that can check how good the used QoS Parameters satisfy the Application SLA.

#### 6.3.1.1 Information for the support of QoS Profile Provisioning

The service data from the AF and the network data from 5GC NFs for QoS profile Provisioning are defined in Table 6.3.1.1-1 and Table 6.3.1.1-2 here below, which allows NWDAF to have a snapshot of service experience for specific UEs as offline reported by AF.

Table 6.3.1.1-1: Service Data from AF related to the observed service experience

|  |  |  |  |
| --- | --- | --- | --- |
| Information | Presence | Source | Description |
| Correlation ID | M | AF | Could be e.g. IP address 5-tuple or newly allocated temporary ID by 5GC , which is used by NWDAF to correlate the service data from AF and the network data from 5GC NF for the service. (NOTE 1) |
| Application ID | O | AF | To identify the service and support analytics per type of service (the desired level of service) |
| Service Experience | O | AF | E.g. Service MOS, MOS or video MOS as specified in ITU-T P.1203.3 [11], to characterize the experience for the service. (The observed level of service by AF) |
| Timestamp | M | AF | A time stamp associated to the observed level of Service Experience provided by the AF, mandatory if the observed Service Experience is provided by the ASP. |
| NOTE 1: The PCF could newly assign a correlation ID per UE per service, when receiving Npcf\_PolicyAuthorization Create Request from AF, and send this correlation ID to AF and 5GC NFs, e.g. SMF, allowing NWDAF to correlate the service data from AF and the network data from 5GC NF as defined in Table 6.3.1.1-2. | | | |

Table 6.3.1.1-2: QoS flow level Network Data from 5GC NF related to the QoS profile assigned for a particular service (identified by an Application Id or IP filter information)

|  |  |  |  |
| --- | --- | --- | --- |
| Information | Presence | Source | Description |
| Correlation ID | M | PCF | Could be e.g. IP address 5-tuple or newly allocated temporary ID by 5GC , which is used by NWDAF to correlate the service data and the network data for the service |
| Timestamp | M |  | The timing for the service. |
| Location Info | O | AMF | The location information for the service. |
| DNN | O | PCF | To identify the DNN for the PDU Session which contains the QoS flow |
| S-NSSAI | M | PCF | To identify the S-NSSAI for the PDU Session which contains the QoS flow |
| Application ID | M | PCF | Provided by the AF, which is used by NWDAF to identify the application service provider and application for the QoS flow |
| IP filter information | O | PCF | Provided by the AF, which is used by NWDAF to identify the service data flow for policy control and/or differentiated charging for the QoS flow |
| QoS flow Bit Rate | M | PCF | To determine the QoS parameter: GFBR/MFBR |
| QoS flow Packet Delay | M | PCF | To determine the QoS parameter: PDB |
| QoS flow Packet Error Rate | M | PCF | To determine the QoS parameter: PER |

NOTE: How the QoS flow level Network Data is obtained depends on the conclusion on key issue#3 and the input data from RAN OAM may be needed, which will be finalized in normative phase.

#### 6.3.1.2 Procedure to support QoS Provisioning and Adjustment



Figure 6.3.1.2-1: Procedure to support QoS Profile Provisioning during PDU Session Modification

For an application Id, a set of initial QoS parameter combinations per service MoS window (e.g. one is for 3<Service MOS<4 and the other is for 4<Service MOS<5) is defined in PCF (e.g. by configuration of operator policies),.

1a. PCF send an Analytics request/subscribe (Event ID = Estimated Service Experience statistics Event Filter information = (Application ID, time window, Media/application bandwidth, S-NSSAI, DNN)) to NWDAF by invoking a Nnwdaf\_EventSubscription\_Subscribe.

1b~1d. NWDAF subscribes the network data from 5GC NF(s) as defined Table 6.3.1.1-2 by invoking a Nnf\_EventExposure\_Subscribe (Event ID = 5QI Statistics, Event Filter information = Application ID, Target of event reporting = Any UE) and the service data from AF as defined in Table 6.3.1.1-1 by invoking a Naf\_EventExposure\_Subscribe (Event ID = Service Data, Event Filter information = Application ID, Target of event reporting = Any UE). With these data, the NWDAF offline trains a Service MOS Model for the given application, which will be used to determine the Service MOS for an application later on.

NOTE 1: The data collection call flow only shows a subscription-notification model for the simplicity instead of both request-response model and subscription-notification model.

NOTE 2: The explicit list of input data is not finalised and whether NWDAF needs to collect management data from OAM, such as PM measurements, is to be resolved in normative phase and some discussion with SA WG5 is needed to see what measurements are available and needed.

NOTE 3: QoE measurements from the applications are based on outcome of the ongoing SA WG5 Rel-16 WID "Management of QoE measurement collection" which addresses how to collect the QoE measurements from the applications in the UE.

1e. The NWDAF provides the data analytics, i.e. the estimated Service Experience statistics (maybe a range) to the PCF by means of Nnwdaf\_EventSubscription\_Notify, indicating how well the used QoS Parameters satisfy the Application SLA:

a) the estimated Service Experience statistics e.g. average Service MoS .

b) Spatial validity condition, when the estimated Service Experience applies.

c) Time validity condition, when the estimated Service Experience applies.

d) NWDAF transaction id.

For example, time window could be from 20180601 to 20180630, which means PCF requests NWDAF to provide the average Service MoS score from, 20180601 to 20180607.

NOTE 4: The NWDAF service consumed here by the PCF will be decided when a solution to key issue#1 is selected.

Please note that the call flow only shows a request-response model for the simplicity instead of both request-response model and subscription-notification model.

1f. Based on the estimated Service Experience (this can be a range) provided by NWDAF, and the operator policies that takes into account the SLA (including the required Service Experience), the PCF takes into account to determine the used QoS parameters to be applied for the service if PCF determines that application SLA is not satisfied.

NOTE 5: The non-real time data information from AF includes the service experience data (see Table 6.3.1.1-1), which indicates the service quality during the service lifetime.

### 6.3.2 Impacts on Existing Nodes and Functionality

NWDAF:

- Collects QoS Flow level network data from 5GC NF(s), service data from AF, PM measurements and QoE data from UE (which is dependent on the discussion outcome of Key Issue 13: UE driven analytics or on the discussions with SA WG4);

- The NWDAF provides the estimated Service Experience range, indicating how good the used QoS Parameters satisfy the Application SLA.

PCF:

- Receives the estimated Service Experience range from the NWDAF and decided whether to update the used QoS profile;

- If receiving a notification from NG RAN via SMF that current target QoS parameters combination cannot be fulfilled, the PCF may re-determine a new QoS parameters combination that still meets the Service Experience in the SLA.

AF:

- Provides service data to the NWDAF.

5G NFs (include AMF, SMF, UPF, UDM, and PCF):

- Provides QoS Flow level network data to the NWDAF.

### 6.3.3 Solution Evaluation

This solution provides a solution how PCF derives the value of the non-standardized 5QI with assistance information from the NWDAF i.e. the estimated Service Experience range.

## 6.4 Solution 4: Optimizing registration area management and Service area restriction adjustment based on NWDAF output

### 6.4.1 Description

#### 6.4.1.1 General

As there is a trade-off between the number of Registration Area Update and the load of paging signalling, the 5GC needs to allocate a suitable Registration Area to the UE. In order to allocate a suitable Registration Area, it is important for the AMF to take UE mobility information into account.

In current carrier networks, the operators have already been able to collect network data such as UE mobility information from OAM, 5GC and/or application server(s), thus it is possible for network operator to mine their network data for system optimization. In this solution, if the NWDAF can obtain historical UE mobility information, the NWDAF can learn UE mobility history and discover the laws/patterns of UE mobility. If any law/pattern of the UE mobility is found, the NWDAF can provide the analytical result to the 5GC. The analytical result on UE mobility contains:

- A cell/TA list or a geographical area which the UE might enter;

- The time that the UE might enter the list of cells/TAs or the geographical area;

- The duration time that the UE might stay in the list of cells/TAs or the geographical area.

NOTE 1: How the NWDAF performs data analysis is out of 3GPP scope.

The analysed UE mobility information is provided from the NWDAF to PCF or AMF based on the request or the subscription from the consumer NF(s). If the PCF was requested by the AMF to adjust Service area restrictions for the UE, the PCF takes the mobility analytic/prediction information into account to adjust the Service area restriction. Further, the PCF includes the adjusted UE Service area restriction in the Access and Mobility Policy and send it to the AMF.

If the AMF receives the mobility analytic/prediction information from NWDAF, the AMF uses the information for the UE as an input to optimize UE mobility management, e.g. registration area determination, paging area determination.

#### 6.4.1.2 Procedures

The provision of UE mobility information from the NWDAF to the AMF is shown in the Figure below.



Figure 6.4.1.2-1: Procedure of using NWDAF out to optimize Registration Area allocation

1-2. As specified in the current specification TS 23.502 [3], during the initial registration or mobility registration with AMF change, the AMF serving the UE contacts the PCF by initiating Policy Association Establishment procedure. The AMF may provide Service area restriction information for the UE to the PCF for Service area restriction adjustment.

3. The PCF, based on local policies, requests NWDAF to provide mobility analytic information for the UE, using either Nnwdaf\_Analytics\_Info or Nnwdaf\_EventsSubscription service.

4. The NWDAF collects UE mobility history information and performs data analysis. The analytical result on UE mobility, e.g. UE mobility pattern, is provided to the PCF. The analytical result contains mobility analytic/prediction information for the UE.

5. If the PCF was requested to adjust Service area restriction for the UE, based on the UE mobility information and local policies, the PCF adjust Service area restrictions for the UE.

6. The PCF provides the AMF with the Access and mobility related policy control information which includes the adjusted Service area restrictions for the UE.

7. If the AMF has no Mobility analytic/prediction information for the UE, based on local policies, the AMF performs service discovery to determine which NWDAF instance can provide the required information. The NRF returns the selected NWDAF instance to the AMF.

8. The AMF requests the selected NWDAF for mobility information for the UE, using either Nnwdaf\_AnalyticsInfo or Nnwdaf\_EventsSubscription service. The AMF can request the NWDAF to provide one time or continuous mobility analytics/predictions for the UE.

9. The NWDAF provide requested Mobility analytic/prediction information for the UE to the AMF according to the AMF request.

10. The AMF allocates Registration Area to the UE based on the received UE mobility information.

NOTE: The AMF logic for deriving registration area is out of scope of 3GPP.

11. The AMF provide the allocated Registration Area to the UE.

12. If the AMF detects that the UE stays in some cells for a long time based on the predictable UE mobility information, the AMF pages UE in those cells first, if the paging failure, the AMF then pages the UE in the whole Registration Area.

### 6.4.2 Impacts on Existing Nodes and Functionality

AMF impacts:

1. Requests for Mobility analytic/prediction information for the UE from the NWDAF.

PCF impacts:

1. Requests for Mobility analytic/prediction information for the UE from the NWDAF.

2. Determines the Service area restrictions for the UE based on Mobility analytic/prediction information for the UE received from the NWDAF.

NWDAF impacts:

1. Collects UE mobility information from OAM, 5GC NFs and/or Application server(s).

2. Provides UE mobility analytic/prediction information.

### 6.4.3 Solution Evaluation

This solution allows the AMF to optimize registration area allocation and paging handling, and the PCF to adjust service area restriction adjustment based on mobility analytic/prediction information for the UE from the NWDAF.

The mobility analytic/prediction information from the NWDAF reveals how often a UE moves into an area and how long time the UE stays in that area, it is feasible to use such NWDAF output to identify appropriate registration areas with minimized frequency of mobility registration. Furthermore, such mobility analytic/prediction information for the UE is also useful to adjust the service area restriction, e.g. to define a precise Allowed/non-Allowed area, which could enhance user's experiences.

In Rel 15, the PCF is able to adjust service area restrictions and the interface between PCF and NWDAF has been supported, therefore, the solution enhancing the PCF to adjust service area restriction for the UE based on the Mobility analytic/prediction information for the UE from the NWDAF has good backward compatibility and minimized system impacts.

The AMF is allowed to request for Mobility analytic/prediction information for the UE from the NWDAF. If the AMF serving the UE is changed, the new AMF may need to re-analyse UE analytic/prediction information for registration area allocation optimization.

## 6.5 Solution 5: Optimization based on paging failure prediction from NWDAF

### 6.5.1 Description

#### 6.5.1.1 General

For the UEs in CM-IDLE or CM-CONNECTED and RRC inactive states, the CN paging failure or RAN paging failure may occur due to certain reasons. Paging failure will cause negative impact on both the network and the service.

1. For CN paging:

For DL signalling or data for a UE in CM-IDLE state, the AMF may page the UE several times in order to reach the UE if the paging failure occurs. The repeated paging messages may cause additional signalling load. The situation is even worse when the AMF is overloaded and congested.

In addition, the AMF may reduce the paging area when first paging the UE, and then enlarge the paging area if the previous paging fails. But the reduction of paging area may not be suitable for certain UEs and causes paging failure, so the inappropriate paging area will result in additional signalling load and delay for the services.

2. For RRC Inactive state:

For DL signalling or data for a UE in RRC inactive state, the NG RAN pages the UE in the RAN Notification area. However, the RAN paging may fail due to certain reasons. In addition, the RAN paging failure may leads to loss of data, which negatively influences service experience. Besides, keeping the UE in RRC inactive state in the area where a UE may have a high paging failure rate is a waste of network resources.

If the NWDAF supports the paging failure prediction, it is very useful to the mobile network in the following aspects:

1. The MNO can further optimize the network coverage based on the paging failure prediction information.

2. The network can further optimize CN paging and RRC Inactive state based on the paging failure prediction information.

For example, the AMF can optimize CN paging, e.g. adjusting paging area, reducing paging times, based on the NWDAF output.

The NG RAN, based on the paging failure prediction information, considers whether to send a UE into RRC inactive state if it has a higher paging failure possibility in this area.

In this solution, the NWDAF input and output procedures are proposed. The basic steps are as follows:

1. If the NWDAF supports the paging failure prediction function, it sends the subscription of the paging failure report to the NG RAN and AMFs.

2. If the CN paging event or RAN paging event occurs, the AMF or NG RAN notifies the NWDAF the paging event with the type of the event (i.e., success or failure).

3. The NWDAF predicts the paging failure possibility in certain time frame and area for the UEs. The NWDAF notifies the network if the paging failure possibility is above certain limit.

4. The network can further optimize CN paging and RRC Inactive state based on the paging failure prediction information.

For example, the NWDAF derives the conclusion that a UE or a group UEs statistically have a higher paging failure possibility at gNB 1 on weekday between 9-10am. If the RAN paging failure possibility exceeds a certain limit, the NWDAF notifies the network. The gNB 1 considers this information when it decides whether to send UE 1 or the group UEs into RRC inactive state.

NOTE: The term "RAN paging" in this solution is the RAN initiated paging for the UEs in RRC Inactive state.

#### 6.5.1.2 NWDAF Input Procedure - Paging event report procedure



Figure 6.5.1.2-1: NWDAF Input Procedure- Paging event report procedure

1. If NWDAF supports the analysis of the paging failure possibility, it sends paging event report subscription to the NG RAN and AMFs.

2a. If the RAN paging event occurs, the NG RAN sends the RAN paging event report to NWDAF, including UE ID, RAN paging area, paging event time point, and paging event type (i.e., success or failure). The NG RAN can also send RAN paging failure to the NWDAF through OAM.

Editor's note: Whether RAN or AMF shall send the paging event report to NWDAF for every event, which has same event type (e.g., paging success), is FFS.

The NWDAF records the UE ID, NG RAN node ID for RAN paging event, the paging event time point, the failure paging area, and the paging event type.

Editor's note: Regards to RAN paging failure report, the interaction with RAN WG is needed.

2b. If the CN paging event occurs, the AMF sends the CN paging event report to the NWDAF, including UE ID, CN paging area, paging event time point and the paging event type (i.e., success or failure).

Editor's note: Whether RAN or AMF shall send the paging event report to NWDAF for every event, which has same event type (e.g., paging success), is FFS.

The NWDAF records the UE ID, AMF ID for CN paging event, the paging event time point, the failure paging area, and the paging event type.

#### 6.5.1.3 NWDAF Output Procedure - Optimization based on paging failure prediction



Figure.6.5.1.3-1: NWDAF Output Procedure- optimization based on paging failure prediction

1. The NWDAF analyses the paging failure possibility for UEs. If the paging failure possibility for certain UEs at certain area and certain time exceeds the limit which is set by the operator or local policy, it will perform step 2.

2. The NWDAF sends the paging failure prediction information to the AMF which serves the possible failure area, including UE ID, paging failure alert indication, possible paging failure area, and the possible paging failure time.

3. The AMF optimizes the CN paging for UEs based on the paging failure prediction information.

4. The AMF sends RAN paging failure alert indication as one of the RRC Inactive assistance information to the NG RAN during the registration procedure. The AMF only send the RAN paging failure alert indication at the time which is within or very close to the 'possible failure time', and to the NG RAN which serves the indicated 'possible failure area'.

The NG RAN takes the RAN paging failure alert indication into consideration when deciding whether to send the UE into RRC inactive state.

### 6.5.2 Impacts on Existing Nodes and Functionality

Editor's note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.5.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.6 Solution 6: Data Collection from NFs/AFs using a new service

### 6.6.1 Description

#### 6.6.1.1 Service definition

This solution addresses the Key Issue #3: "Interactions with 5GS NFs/AFs for Data Collection".

An NF of AF provides periodically, according to a subscription, a list of data blocks called Collectable Data Items (CDI).

This solution complements the current solutions defined in SA WG5 for data collection. TS 28.552 [15] (5G performance measurements - Rel‑15) define the measurements and KPIs that can be retrieved from OAM services. The current version of such specification, from the point of view of NWDAF, does no not support data collection for generation of analytics per region, or per application, or per groups of UEs. The measurements defined in TS 28.552 [15], for instance, about NFs are aggregated at best by S-NSSAI and the measurements about the RAN are aggregated per 5QI, The advantage of this solution is that the definition of the new service in NFs/AFs for data collection allows the generation of analytics that are not restricted to network load level, but that can provide more fine grain analytics per region of the network and/or based on populations (i.e. groups of UEs or application IDs).

According to this solution, a Collectable Data Item (CDI) may be either:

- An elementary metric, either standardized, or implementation specific, in both cases with a documented semantic and format. A metric is a statistical data (e.g. average, total, standard deviation, maximum, minimum) relative to a given quantity (e.g. counter, gauge, delay, ratios).

- An implementation-specific block of data, in textual or binary form, structured or not (e.g. log, array of metrics, traces).

Each NF of AF offers a generic service interface NF<X>\_DataCollection Service offering the following operations.

Table 6.6.1.1-1

|  |  |
| --- | --- |
| Operations | Description of each operation of the Analytics Exposure Service |
| Subscribe | Subscription to a subset of existing CDIs computed by the NF or the AF |
| Update | Update of a specific subscription |
| Unsubscribe | Cancel of a specific subscription |
| Notify | CDI(s) is sent to the consumers |
| Retrieve | A consumer explicitly requests the CDI(s) and receive the requested information |

When a subscription is accepted, an NF notifies of the requested CDIs to the NWDAF. Each notification either contains a single timestamped set of instances of CDIs, or information on a file containing several instances.

The CDIs can be made available on a periodical time frame basis, depending on the subscription parameters, or it can be requested by NWDAF within a time frame.

An CDI is a couple (CDI\_ID, {[ADI\_tag] CDI\_value}+). An CDI\_list\_ID references a predefined (i.e. standardized or documented) list of CDI\_IDs.

The CDIs are computed on a periodic basis, in the form a Measurement Instances (MI). A Measurement Instance is a timestamped occurrence of a set of one or more CDIs.

Results can be provided either as a continuous streaming flow of events (periodic notifications of a single MI) or by grouping multiple MIs in a single notification or file.

#### 6.6.1.2 Subscription parameters

The parameters for subscription include:

- Subscription ID;

- The subscription duration, expressed as a positive number D of time frames;

- The list of desired CDIs, which either be an explicit list of CDI\_IDs, a default value, or a list of CDI\_list\_ID;

- The CDI scope, describing the targeted services, areas, UEs, activities, with possible wildcards, possibly common to all NFs, e.g. NSSAI, DNN, SUPI/PEI/GPSI, GUAMI;

- Additional filters with possible wildcards;

- Optional triggers for measurement start/stop based on thresholds of NF metrics used to calculate CDIs (e.g. maximum or minimum value of load level);

- The time frame for measurement, and optionally the sampling interval;

- The period between two notifications, expressed as a positive number N of time frames.

NOTE: Value N=1 is used to request a notification for each MI. When N>1, multiple MIs will be provided in a single notification, or in a file for higher values of N.

An NWDAF may optimize the strategy of data collection across different NFs, depending on the services it provides, by requesting or subscribing only to the relevant information and by minimizing its interactions with NFs/AFs.

The parameters for Update include the subscription ID, newly requested subscription duration, an optionally the new time frame for measurement, the new sampling interval, and the newly requested period between two notifications.

#### 6.6.1.3 Notifications

According to the subscription parameters, the NF/AF should send unique or periodic notifications towards the NWDAF as depicted in Figure 6.6.1.3-1.



Figure 6.6.1.3-1: The relationship between time frame for MI and notification period for consumer

#### 6.6.1.4 Scope of Collectable Data Items

A NWDAF may request an NF/AF for the provision of CDI at different levels, for example for a given slice, for a group of UEs, or for a specific Tracking Area.

For this purpose, CDI\_tags are used to act as filters in order to define the scope of requested ADIs. The resource modelling of CDI\_tags may be organized as a tree of different depth levels.

The support of different scoping parameters on CDI\_tags may depend on each NF/AF, but the levels and the order of levels should be structured with the same descending pattern.

Table 6.6.1.4-1

|  |  |  |  |
| --- | --- | --- | --- |
| Level | Level role | Example of scoping parameters on ADI\_tags | Example |
| 0 | slice ID | S-NSSAI | CDI\_tag = « MBB » |
| 1 | Location ID | Geographical area, TAI, | CDItag = "lac code" |
| 2 | Access ID | Access type, Cell ID, | CDI tag = "Cells in range [a..c]" |
| 3 | Application ID | DNN, AFid, | CDI tag = "All DNN" |
| 4 | user ID | SUPI/PEI/GPSI, group ID | CDI\_tag= "All UEs" |
| 5 | Terminal ID | PEI/TEI or terminal type | CDI-tag= "All teminals of type X" |
| 6 | Activity ID | Registration, mobility, sessions, flows | CDI tag ="registration counter" |
| 7 | Time Window | Interval of time associated with the requested information | CDI tag = "collection interval" |

NOTE: The exact definition of levels is left for the normative phase.

Each scoping level may or may not support wildcards. In case of wildcards, it should be possible to specify either an empty wildcard meaning "all ID\_tags", or a constrained wildcard by denoting a range of ID\_tags.

The use of wildcards enables the discovery of new CDI\_tags (e.g. different values of DNNs).

The CDIs can be either aggregated or explicitly listed. On only one single wild carded level and one single parameter within a subscription, it should be possible to specify that the CDI is explicitly listed.

When level aggregation is chosen, the cumulative or mean value of the measurement shall be provided, depending on the type of CDI. For instance, if the CDI "registration counter" is requested aggregated on all cells, only one aggregated counter is provided which totalizes all cells. Aggregation rules should be specified per ADI type.

When explicitly listed, all CDI\_tags of the parameter corresponding to the wildcard are requested. The filter, when applied to the set of CDI\_tags stored in the NF/AF repository, produces a subset of fully defined CDI\_tags in the level. For instance, if the CDI "number of registrations" is requested as a an explicit list, an array of counters is provided on a single dimension, one per each CDI\_tag Cell-ID in the range [a..c].

Considering this feature, a time stamped Measurement Instance may contain, per CDI, either a single value or an array of tagged values. It may also be possible for the NF/AF to produce one MI notification per member of the subset.

Table 6.6.1.4-2

|  |  |
| --- | --- |
| CDI | Array of <CDI\_tag, CDI values> |
| CDI a | <Cell1; CDI a for Cell1>, <Cell2; CDI a for Cell2>,<Cell3; CDI a for Cell3>,etc.. |
| CDI b | <Cell1; CDI b for Cell1>, <Cell2; CDI b for Cell2>,<Cell3; CDI b for Cell3>,etc.. |

The types of filtering (wildcarding with all values or range of values, versus a single specific value) and the possibility to obtain explicit lists both depend on each NF and operator policy.

#### 6.6.1.5 Procedure for Interactions with 5GC NFs for Data Collection Notification from 5GC NFs



Figure 6.6.1.5-1: Procedure for Interactions with 5GC NFs for Data Collection Notification from 5GC NFs

1. To subscribe to NFs data, the NWDAF invokes an Nnf\_DataCollectionService\_Subscribe service operation from the 5GC NFs with the parameters listed in clause 6.6.1.2. The 5GC NFs respond to the request service operation with the indication of success or failure of the subscription request.

2. To report the data from 5G NFs when it is available to be collected, the 5GC NFs invoke an Nnf\_DataCollectionService\_Notify service operation to notify NWDAF with the requested CDI(s).

NOTE: If the 5GC NFs such as UPF are not allowed to access the NWDAF through the service based interface, the NWDAF may indirectly interact with the UPF through the SMF, respectively.

#### 6.6.1.6 Procedure for Interactions with 5GC NFs for Data Collection from 5GC NFs



Figure 6.6.1.6-1: Procedure for Interactions with 5GC NFs for Data Collection from 5GC NFs

1a. To request data from NFs, the NWDAF invokes an Nnf\_DataCollectionService retrieval service operation from the 5GC NFs with the parameters listed in clause 6.6.1.2.

1b. 5GC NFs responds the request data in the response message of the Nnf\_DataCollectionService Retrieval response service operation to the NWDAF with the requested CDI(s).

NOTE: If the 5GC NFs such as UPF is not allowed to access the NWDAF through the service based interface, the NWDAF may indirectly interact with the UPF through the SMF, respectively.

#### 6.6.1.7 Procedure Interactions with AFs for Data Collection Notification from AF



Figure 6.6.1.7-1: Procedure for Interactions with AFs for Data Collection from AF

0. In order for AF to provide data to NWDAF, a registration of the available data at AF is performed.

NOTE 1: The registration process is for NWDAF to discover the address of AFs and the data they can provide to NWDAF. The specifics of the registration is FFS.

1. To subscribe to data to be collected from AF, the NWDAF invokes a Naf\_DataCollectionService\_Subscribe service operation from AF with the parameters listed in clause 6.6.1.2. The AF responds the request service operation with the indication of success or failure of the subscription request.

2. To report the data to be collected from AF when it is available to be collected, the AF invokes a Naf\_DataCollectionService\_Notify service operation to notify NWDAF with the requested CDI(s).

NOTE 2: If the AF is not allowed by the operator to access directly the NF(s) as specified in clause 6.2.10, TS 23.501 [2], the service operations in step 0-2 should use the NEF to interact between the AF and the NWDAF.

NOTE 3: The exact definition of alternatives for data transfer from AF through NEF is left for the normative phase.

#### 6.6.1.8 Procedure Interactions with AFs for Data Collection Notification from AF



Figure 6.6.1.8-1: Procedure for Interactions with AFs for Data Collection from NWDAF

0. This step is the same as the step 0 in Figure 6.6.1.7-1.

1a. To request data from AFs, the NWDAF invokes an Naf\_DataCollectionService retrieval service operation from the AF with the parameters listed in clause 6.6.1.2.

1b. AF responds the request data in the response message of the Naf\_DataCollectionService Retrieval response service operation to the NWDAF with the requested CDI(s).

NOTE 1: If the AF is not allowed by the operator to access directly the NF(s) as specified in clause 6.2.10 of TS 23.501 [2], the service operations in steps 0-2 should use the NEF to interact between the AF and the NWDAF.

NOTE 2: The exact definition of alternatives for data transfer from AF through NEF is left for the normative phase.

#### 6.6.1.9 Definition of CDIs in NFs and AFs

A key aspect is the definition of metrics for each AF and NF.

Two complementary proposed techniques in order to define and implement quickly for each NF a standardized set of CDIs would be to have predefined CDI lists:

- "CDI\_set\_op": a set of CDI per NF/AF counting each service operation, globally and also depending on its return codes (2XX, 3XX, 4XX, 5XX, e.g. ServiceXOperationY\_2XXcounter, ServiceXOperationY\_3Xxcounter) or causes (USER NOT FOUND, e.g. ServiceXOperationY\_USER\_NOT-FOUND) or group of causes (e.g. UE identification), etc.

- "CDI\_set\_status": a set of CDI counters per NF/AF, on UEs and sessions status types (e.g. UE\_REGISTERED).

As a consequence, each NF shall have to implement basic database queries on its log of service operations, or on its active contexts in order to obtain the requested metrics.

The following table provides an example of predefined CDIs for the AMF operation "CreateUEContext".

Table 6.6.1.9-1: Illustration of predefined CDIs example for the AMF operation "CreateUEContext"

|  |  |  |  |
| --- | --- | --- | --- |
| Operation | Error causes | List of proposed CDIs | Scoping CDI parameter |
| CreateUEContext | All causes, plus no errors | Total count of requests (success and errors) | Application ID = "all Application IDs"  Location ID = "all TA" |
| No error | Total count of successful requests | …. |
| UE Identification causes | Total count per error group |  |
| Subscription causes | Total count per error group |  |
| Congestion network failure causes | Total count per error group |  |
| Invalid message causes | Total count per error group |  |

The following table provides an example of CDIs for the UE CM state and UE RM state.

Table 6.6.1.9-2: Illustration of predefined CDIs example for the UE CM state and UE RM state

|  |  |  |  |
| --- | --- | --- | --- |
| Status | Status values | List of proposed CDIs | Scoping CDI parameter |
| RM state | REGISTERED | Total count of UE with this status | Access ID =" All "  Application ID = "all Application IDs" |
| DEREGISTERED | Total count of UE with this status | Access ID =" All "  Application ID = "all Application IDs" |
| CM state | IDLE | Total count of UE with this status | Access ID =" All "  Application ID = "all Application IDs" |
| CONNECTED | Total count of UE with this status | Access ID =" All "  Application ID = "all Application IDs" |

#### 6.6.1.10 Procedure for Interactions with 5GC NFs for update of Data Collection Subscription to 5GC NFs



Figure 6.6.1.10-1: Procedure for Interactions with 5GC NFs for update of Data Collection Subscription to 5GC NFs

1. To update the subscription to NFs data, the NWDAF invokes an Nnf\_DataCollectionService\_Update service operation from the 5GC NFs with the subscription ID, newly requested subscription duration, new time frame for measurement, optionally new sampling interval, and the newly requested period between two notifications as described in clause 6.6.1.2. The 5GC NFs respond to the request service operation with the indication of success or failure of the subscription update request.

Editor's note: The update of subscription for the other parameters (i.e., CDI scope, etc.) is FFS.

2. To report the data from 5G NFs when it is available to be collected, the 5GC NFs invoke an Nnf\_DataCollectionService\_Notify service operation to notify NWDAF with the requested CDI(s) according to revised time interval.

NOTE: If the 5GC NFs such as UPF are not allowed to access the NWDAF through the service based interface, the NWDAF may indirectly interact with the UPF through the SMF, respectively.

#### 6.6.1.11 Procedure Interactions with AFs for update of Data Collection Subscription to AF



Figure 6.6.1.11-1: Procedure for Interactions with AFs for update of Data Collection Subscription to AF

1. To update of subscription for data to be collected from AF, the NWDAF invokes a Naf\_DataCollectionService\_Update service operation from AF with the subscription ID, newly requested subscription duration, new time frame for measurement, optionally new sampling interval, and the newly requested period between two notifications as described in clause 6.6.1.2. The AF responds the request service operation with the indication of success or failure of the subscription update request.

NOTE 1: The update of subscription for the other parameters (i.e., CDI scope, etc.) is left for the normative phase.

2. To report the data to be collected from AF when it is available to be collected, the AF invokes a Naf\_DataCollectionService\_Notify service operation to notify NWDAF with the requested CDI(s) according to revised time interval.

NOTE 2: If the AF is not allowed by the operator to access directly the NF(s) as specified in clause 6.2.10, TS 23.501 [2], the service operations in step 1-2 should use the NEF to interact between the AF and the NWDAF.

NOTE 3: The exact definition of alternatives for data transfer from AF through NEF is left for the normative phase.

### 6.6.2 Impacts on Existing Nodes and Functionality

The solution requires the implementation of a new interface on CN NFs for data collection.

It is clearly oriented towards the collection of data that allows spacial (i.e., in specific regions of the network slice) and temporal aspects of data that can be collected from NFs.

### 6.6.3 Solution Evaluation

This solution allows both the collection of data related to individual UEs and the collection of statistical data related to multiple UEs.

This solution adds a mechanism in addition to the existing ones based OAM and Rel‑15 event exposure.

The solution enables data collection from any NF and AF, for any use case.The solution enables to collect data with a fine grain scoping level (e.g. UE groups, TAI), either aggregated or detailed.

Techniques are described to facilitate the definition of metrics (see clause 6.6.1.9).

In order to reduce computation effort on NWDAF and data volume, each NF or AF can provide the NWDAF with pre-processed analytics (metrics) instead of raw events.The solution encourages Collectable Data Items to be standardized. In order to encourage a fruitful data ecosystem, it may also be possible for an implementation to propose specific metrics to the community.

## 6.7 Solution 7: Customizing mobility management based on NWDAF output

### 6.7.1 Description

This is a solution to Key Issue#9: Customizing mobility management based on NWDAF output.

There are customization of mobility management Use Cases that are done in an offline fashion with low signalling frequency. There are other Use Cases that are done more in an online fashion with higher signalling frequency. The Solution below describes how associated analytics is used to support all Use Cases that can be performed by a 5GS NF independently.



Figure 6.7.1-1: Customizing mobility management with associated analytics

Figure 6.7.1-1 shows a NWDAF instance that is associated with AMF and provides analytics for customized mobility management.

1. First the NWDAF instance registers in NRF the Event-ID it supports (e.g. "UE expected geographical movement").

2. AMF discovers the NWDAF instance that supports a specific Event-ID (e.g. "UE expected geographical movement").

3. AMF subscribes to NWDAF Event-ID.

4. NWDAF carries out analytics to determine the "UE expected geographical movement".

NOTE: AMF obtains input data using existing procedures in TS 23.502 [3]. How the input data is collected by NWDAF will follow the conclusions on key issue #3

5. NWDAF sends a notification to AMF including the Event-ID and the analytics value for the "UE expected geographical movement".

The NWDAF instance providing "UE expected geographical movement" can be collocated with AMF, then NRF registration and discovery are not needed. In this case the NWDAF may provide analytics to AMF via internal interfaces.

Alternatively, AMF may have locally configured the NWDAF instance that provides "UE expected geographical movement", then discovery via NRF may not be needed.

### 6.7.2 Impacts on Existing Nodes and Functionality

**NWDAF:** NWDAF needs to register the Event-ID with NRF.

**NF:** A NF exposes network analytics, using existing Event Exposure framework, that needs to include new Event Ids. The NF also needs to discover the associated NWDAF instance using the Event-ID.

**NRF**: Needs to include the Event-ID in the NWDAF register and discovery processes.

### 6.7.3 Solution Evaluation

By using an associated analytic solution:

- The signalling and network load are lowered.

- The delay is minimized.

## 6.8 Solution 8: Performance improvement and supervision of mIoT terminals

### 6.8.1 Description

This solution is for Key Issue 8: Performance improvement and supervision of mIoT terminals.

#### 6.8.1.1 Information for the support of Performance improvement and supervision of mIoT terminals

The UE behavioural information from 5GC NFs for performance improvement and supervision of mIoT terminals is defined in Table 6.8.1.1-1.

Table 6.8.1.1-1: UE behavioural information collected from 5GC NF(s)

|  |  |  |  |
| --- | --- | --- | --- |
| Information | Presence | Source | Description |
| UE ID | M | AMF/SMF | Could be e.g. SUPI, which is used by NWDAF to correlate the UE behavioural information from different 5GC NFs. |
| **Location info** |  |  |  |
| >Timestamp | O | AMF | The timing for the UE |
| >Location | O | AMF | The location info for the UE e.g. Cell ID or TA ID |
| **Communication Pattern Info** |  |  |  |
| >Communication start time | O | SMF | Start time when the UE is available for communication |
| >Communication end time | O | SMF | End time when the UE is unavailable for communication |
| **Network Configuration Info** |  |  |  |
| >UL or DL Packet Latency | O | SMF | Indicating the delay for uplink or downlink packets transfers for the UE |

#### 6.8.1.2 Procedure for expected UE behavioural information provisioning

Based on large amount of UE behavioural information from 5GC NF(s) corresponding to UEs in a SUPI list, NWDAF could clusters the UEs into one or more UE groups, where each UE group has an expected UE behavioural information, as defined in Table 6.8.1.2-1.

Table 6.8.1.2-1: Expected UE behavioural information for a UE group provided by the NWDAF

|  |  |  |
| --- | --- | --- |
| Information | Presence | Description |
| Stationary indication | O | Identifies whether the UE is stationary or mobile, e.g. only on demand. (TS 23.682 [5], clause 5.10.1). |
| UE Moving Trajectory | O | Identifies the UE's expected geographical movement (TS 23.502 [3], clause 4.15.6).  Example: A planned path of movement |
| Periodic communication indicator | O | Identifies whether the UE communicates periodically or not, e.g. only on demand. (TS 23.682 [5], clause 5.10.1). |
| Communication duration time | O | Duration interval time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1).  Example: 5 minutes |
| Periodic time | O | Interval Time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1).  Example: every hour |
| Scheduled communication time | O | Time zone and Day of the week when the UE is available for communication (TS 23.682 [5], clause 5.10.1).  Example: Time: 13:00-20:00, Day: Monday |
| Maximum Latency | O | Indicating maximum delay acceptable for downlink data transfers (TS 23.682 [5], clause 4.5.21). |
| Maximum Response Time | O | Indicating the time for which the UE stays reachable to allow the AF to reliably deliver the required downlink data (TS 23.682 [5], clause 4.5.21). |
| Suggested Number of Downlink Packets | O | Indicating the number of packets that the UPF shall buffer in case the UE is not reachable (TS 23.682 [5], clause 4.5.21). |



Figure 6.8.1.2-1: Procedure for expected UE behavioural information provisioning

1. The UDM may subscribe expected UE behavioural information to the NWDAF by invoking Nnwdaf\_EventsSubscription\_Subscribe service operation. The input for the service operation should be:

- Event ID.

- Event Filter Information: SUPI List.

- Target (list of SUPI, any UE).

2. Based on analytical result for large amount of UE behavioural information from 5GC NF(s) as defined in Table 6.8.1.1-1, NWDAF clusters the UE behavioural information into one or more UE groups in which each UE group has an expected UE behavioural information.

3. The NWDAF notifies the expected UE behavioural information as defined in Table 6.8.1.2-1 and UE group ID to the UDM by invoking the Nnwdaf\_EventsSubscription\_Notify service operation. The UDM stores the expected UE behavioural information as part of the subscription data for the corresponding UE(s).

#### 6.8.1.3 Procedure for mIoT terminals misused or hijacked Recognition



Figure 6.8.1.3-1: Procedure for Massive UE are misused or hijacked Recognition

0. As specified in clause 6.8.1.2-1, the NWDAF provides the expected UE behavioural information as defined in Table 6.8.1.2-1 for each UE to the UDM. Considering the received expected UE behavioural information, the UDM may store the expected UE behavioural information as part of the subscription data for the corresponding UE. This contains also NWDAF subscription onto NF(s) about the Event ID = Deviation from UE behaviour.

1. UDM/UDR notifies the updated subscriber data i.e. the expected UE behavioural information and UE group ID to the corresponding 5GC NFs (e.g. AMF, SMF).

2. During a UE communicates with the 5GC, NF e.g. AMF, the NF determines whether the UE's behavioural information matches its expected UE behavioural information, if not, the UE is regarded as an exception UE, then the NF should notify the NWDAF per the subscription received in step 1.

3. The NWDAF may perform further data analysis on certain UE exception UE behavioural information and find that does not match the expected UE behavioural information, then abnormal behaviour could be expected e.g. be UE misused or hijacked.

4. Based on analytical result, the NWDAF notifies exception UE ID list, corresponding Exception ID, corresponding Exception level to the AF according to the subscription to such notification. Based on these information, the AF may adjust e.g. recommended TCP Window Size, recommended Service Start and End time(e.g. for background data transfer), etc. For the untrusted AFs, the message can be send via the NEF.

5.1. According to the subscription to such notification, the NWDAF notifies exception UE ID list, corresponding Exception ID and Exception level to the relevant UDM/UDR. Taking these received information into account, the UDM/UDR may further update the UE subscription information, e.g. Supported SSC mode, default SSC mode, Subscribed S-NSSAI and periodic registration update timer. UE subscription change is sent to the registered NF (Serving AMF, serving SMF).

5.2. According to the subscription to such notification, the NWDAF notifies exception UE ID list, corresponding Exception ID and Exception level to the relevant PCF(s). Taking these received information into account, the PCF(s) may create or update the UE policy accordingly.

### 6.8.2 Impacts on Existing Nodes and Functionality

Editor's note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.8.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.9 Solution 9: Recommendations produced by NWDAF

### 6.9.1 Description

#### 6.9.1.1 Service principles

This solution addresses Key issue #1: "Network Data Analytics feedback".

The NWDAF offers a Recommendations service in order to propose recommendations (parameter values) to NFs.

This solution extends the objective of the SID which is for the NWDAF to provide statistics and predictions.

The use of the Recommendations service by an NF is optional. The recommendation service shall not assume application knowledge and configuration in the NWDAF.

The purpose of the service is to better assist some NFs in the elaboration of its strategy, in certain use cases.

Each NF may request the NWDAF Recommendations service for instance in case its decision may impact other NFs behaviours.

Each type of recommendation belongs to a given domain (e.g. registration, reachability, mobility, service and application, forwarding, routing, roaming, security, resilience). There may different types of recommendations per domain.

The NWDAF apart from providing statistical/prediction information, shall not intervene in the area of responsibility of each NF, which shall remain solely responsible for its decisions. The NFs may additionally coordinate their decisions with other NFs.

After receiving a recommendation that the NF has requested, the NF shall then, according to its own criteria (for example applicative and business criteria) and its own service logic, make its optimal choice within its area of responsibility.

The NF consumers of the NWDAF Recommendations service are fully in charge of all decisions concerning their own tuning. As a consequence, they should be able to operate with good performance in most situations, even in case of NWDAF absence or failure.

The NWDAF should strive to ensure consistency in its recommendations, taking into account the previous recommendations performed across the different domains and the other NFs, in order to avoid conflicted decisions.

#### 6.9.1.2 Service definition

The NWDAF should expose a generic service interface NWDAF\_RecommendationsService offering the following operations.

Table 6.9.1.2-1

|  |  |
| --- | --- |
| Operations | Description of each operation of the Recommendations Service |
| Subscribe | Subscription to recommendations |
| Unsubscribe | Cancel of a previous subscription |
| Notify | Notification of recommendations to the consumer NF |
| Request | Request to recommendations |

The Recommendations service proposes pre-computed vectors of optimal parameter recommended values to NFs.

A parameter recommended value is a single value or a range, for possible integration in the rules of the consumer NF.

Each consumer NF shall provide in input, for a given type of recommendation, the target objects that are related to the parameter recommend values that will be derived. The NF may impose computational constraints (e.g. ranges of parameters to explore) on the results.

The NWDAF in return shall provide, for each requested recommendation, a list of one or more suggested parameter combinations. For instance, these combinations can be lists of candidate QoS dedicated parameters, or lists of candidate UPFs for selection.

Each combination is a vector of recommended parameter values, possibly with associated impacts (predicted KPIs) and a preference order, consistent between different domains.

#### 6.9.1.3 Recommendations Subscribe/Unsubscribe

This procedure is used by any NF service consumer to subscribe/unsubscribe at NWDAF and to be notified of recommendation information.



Figure 6.9.1.3-1: NWDAF Recommendations Subscribe/Unsubscribe/Notify

1. The NF service consumer subscribes to or cancels subscription to recommendations by invoking the Nnwdaf\_Recommendations\_Subscribe or Nnwdaf\_ Recommendations \_Unsubscribe service operation.

2. If NF service consumer has subscribed to recommendations, the NWDAF notifies the NF service consumer with the recommendations by invoking Nnwdaf\_ Recommendations \_Notify service operation.

#### 6.9.1.4 Recommendations Request

This procedure is used by the NF service consumer (e.g. UDM, AMF, SMF, PCF) to request and get from NWDAF recommendations, using Nnwdaf\_Recommendations\_Request.



Figure 6.9.1.4-1: NWDAF Recommendations Request and Response

1. The NF service consumer requests recommendations by invoking Nnwdaf\_Recommendations\_Request service operation.

2. The NWDAF responds with recommendations to the NF service consumer.

#### 6.9.1.5 Contents of subscribe and request operations

In addition to basic SBI parameters defined in TS 29.520 [10], the requests or the subscription should contain:

- The desired recommendation on a given domain, expressed as a recRequirement object.

- Observation period [start..end] in the future on which recommendations are requested.

- Maximum tolerable delay for the provision of the recommendations.

- Event parameters for periodic notification (as defined in Solution#1),

- Optional preferences on recommendations (as defined in Solution#1)..

- Target of Event Reporting (TER), Event Filtering Information (EFI) and Denotation of Explicit Lists (as defined in Solution #1).

A recRequirement object is composed of:

- the recommendation registered ID in the given domain.

- optional optimization goals: this parameter denotes the objectives of optimization requested, if several optimizations methods are possible. Several simultaneous objectives may be requested and hierachized. The requesting NF should use these goals parameters in order to fit its own strategy.

- optional constraints per requested parameter, expressed as parameter ranges. These constraints may be used by NFs to guide recommendations by passing UE up-to-date subscription profile values.

#### 6.9.1.6 Contents of notifications and responses

In addition to the basic SBI parameters defined in TS 29.520 [10], the response to Request or the notification should contain:

- Identification of the Request /Subscribe operation.

- Optional confidence score on recommendations.

- Possible limitations on the observation period and requested delay.

- Recommendations: candidate recommendations relevant for the observation period, expressed as an array of elementary recommendation objects recResult.

Each recResult is a composed of:

- Reference to the recommendation registered ID in the recommendation domain.

- The vector of tagged parameter recommended values or value ranges.

- Optionally: the associated impacts (a set of predicted analytics) if such parameters are chosen.

- Optionally: a preference order in order to suggest a preference among the various recResult objects.

A recommended parameter may belong to the following categories.

Table 6.9.1.6-1

|  |  |
| --- | --- |
| Parameters categories | Example of parameters |
| Time | Periodic registration timer, back-off timers |
| QoS | QoS profiles |
| NF | Identification of proposed UPF |
| Load ratio | Load reduction ratio, load balancing ratio |
| UEs | Identification of UEs suspected of performing a security attack |
| Location | List of relevant TA for the UE e.g. for paging or mobility restriction |
| Activity | Handover/No handover, blacklist UEs |

Each parameter should have a clearly defined semantic and format, and should typically be defined in a 3GPP standard.

NOTE: The exact definition of parameter types is to be defined by other solutions.

The NWDAF may return an error if the parameters (in immediate response to subscription or request), or the traffic conditions do not permit to deliver relevant recommendations in due time. It may also return, in case of error, limitations of requested observation period and tolerable delay. It may also return, in case of coordination between different recommendations, the action it should take to use the response (wait a delay, wait for an event of another domain, etc.).

### 6.9.2 Impacts on Existing Nodes and Functionality

The solution requires the implementation of a new service on the NWDAF.

### 6.9.3 Solution Evaluation

This solution extends the objective of the SID which is for the NWDAF to provide statistics and predictions.

In addition to solutions providing statistics and predictions, this solution allows to go one step further by allowing the NFs delegate some calculation of optimal parameters to the NWDAF, while remaining responsible for the final choices they make according to their own application logic. For instance, it can facilitate the decisions related to QoS provisioning (see Solution #3) and adjustment, or NF selection.

The arrays of recommendations provided by the NWDAF are only support data for NF decision. These recommendations are based on computational analysis guided by NF specific constrains (considering that NF knowledge and logic shall not be replicated in NWDAF), enabling the NWDAF to provide processed data. For instance, the NF may choose a solution of secondary preference order in the array, for reasons relevant to the NF logic. The NF may also simply ignore all recommendations, for the same reason.

Solution #1 provides statistics and predictions, while Solution #9 provides recommendations. Both are compatible, which means that a consumer NF may request a prediction, and then, knowing the results, decide to obtain recommendations on a subset of possible options.

The solution #9 requires additional study on several aspects:

- NF logic in the NWDAF;

- expression of associated impacts (response parameter as described in clause 6.9.1.6);

- possibility of subscribing simultaneously to multiple recommendations;

- consistency of recommendations.

## 6.10 Solution 10: <NWDAF assisted Handover decision>

### 6.10.1 Description

#### 6.10.1.1 General

In current carrier networks, the operators have already been able to collect network data, such as UE mobility information, via OAM, thus it is possible for network operator to mine their network data for system optimization.

In current 5GS, while the source NG-RAN node is selecting a target cell for a CONNECTED mode UE, it has taken the UE last visited cells into account. However, the historical cells may be useless to select a suitable target cell in some cases, e.g. if the UE will change its moving direction with a relative large angel.

In order to select a more suitable cell in such cases, the prediction on UE mobility will be helpful when the UE mobility is predictable. Since NWDAF can learn UE mobility history and discover the laws/patterns of UE mobility, the 5GC can apply the discovered laws/patterns of UE mobility to predict the UE mobility, e.g. the moving trajectory of an officer may be relatively static from 8AM to 9AM and from 6PM to 7PM. Therefore, the 5GC can use the NWDAF output to predict the UE mobility and indicate the predicted UE location to the NG-RAN node serving the UE. Then the NG-RAN node can select a more suitable target cell during the handover or redirection.

Moreover, during the handover or redirection procedure, if the source NG-RAN knows that some candidate NG-RAN nodes will be subject to overload soon, it can kick them out of the candidate list if there is a better choice, which reduces the probability of serving RAN node change.

With the above considerations, in this solution, it is expected that the NWDAF can provide the following information to the AMF (maybe via PCF):

- UE mobility information (law/pattern):

- A cell/TA list or a geographical area which the UE might enter;

- The time that the UE might enter the list of cells/TAs or the geographical area;

- The duration time that the UE might stay in the list of cells/TAs or the geographical area.

The predicted UE mobility information is provided to the NG-RAN serving the UE during the Registration or Serving Request procedure.

#### 6.10.1.2 Procedures

The procedure of providing the analytical information from the NWDAF to assist the NG-RAN to make handover decisions is shown in the Figure 6.10.1.2-1.



Figure 6.10.1.2-1: Procedure of using NWDAF out to assist handover decision

0. This solution assumes that network load prediction can be used to assist the source RAN node to select a suitable cell or RAN node. The network load prediction is out of the scope of SA WG2.

1. A UE registers to the 5GC.

2. Based on operator's configuration or UE subscription, the AMF may contact the PCF to retrieve Access and Mobility policies including predictable UE mobility information, or contact the NWDAF directly to retrieve the predictable UE mobility information.

3. If the PCF has stored the predictable UE mobility information for this UE, the PCF provides the information to the AMF. Otherwise, the PCF contacts the NWDAF first.

4. The NWDAF performs data analysis on historical UE mobility information obtained from the OAM. The analytical result on UE mobility, e.g. UE mobility pattern, is provided to the PCF. The PCF stores the analytical result in the UDR as the predictable UE mobility information, which allows other NFs to retrieve the UE mobility information directly, i.e. without consulting the NWDAF.

5. The AMF checks the UE mobility information and determines whether current UE mobility can be predicted, if yes, the AMF calculates the potential waypoint(s) (e.g. RAN node ID(s)) of the UE based on the predictable UE mobility information and the current UE location. The AMF provides the potential waypoint(s) of the UE to the NG-RAN node serving the UE.

6. The Registration Accept is forwarded by the NG-RAN from the AMF to the UE.

7. When a NG-RAN node serving the UE tries to initiate a handover, to select a suitable target NG-RAN node, besides the radio signal strength, it may also take into account the network overload information and the potential UE waypoint(s) if it has.

### 6.10.2 Impacts on Existing Nodes and Functionality

Editor's note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.10.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.11 Solution 11: UPF selection based on output from NWDAF

### 6.11.1 Description

#### 6.11.1.1 General

This solution is for key issue 6# NWDAF assisting traffic routing.

To enable the efficient traffic routing, the proper UPF selection is required. The SMF may use data analytics services of NWDAF to support UPF selection for important traffic types, which is applicable to several UEs or individual UEs. The NWDAF collects data related with UPF selection from various sources, and provides the analytic result to the SMF. During UPF selection, SMF considers the UE's communication, mobility, UPF's load level patterns and other information from the NWDAF.

The communication patterns have been defined in TS 23.682 [5] clause 5.10.1. The mobility pattern has been defined in TS 23.501 [2] clause 5.3.4.2.

According to communication patterns and mobility pattern analytics of UE and UPF's network performance pattern (i.e. estimated load in a network area at a given time and date) from NWDAF, the SMF can select a proper UPF for the UE. Example, for a college student, an UPF near the campus may be selected according to the communication patterns and mobility pattern of the UE and network performance pattern. But for a business man, a higher UPF may be selected.

During the PDU session establishment, the SMF sends the DNN and S-NSSAI for this PDU session to the NWDAF. The NWDAF perform analysis and response the communication patterns and mobility patterns and network performance pattern to SMF. SMF select the UPF for the UE according to the analytics.

During UE mobility, the SMF can insert the proper UPF according to above information.

The SMF can use the solution in the 6.1 to request the analytics from NWDAF.

#### 6.11.1.2 Data Analytics-Based UPF Selection for Many UEs

##### 6.11.1.2.1 Input Information for the support of NWDAF assisting traffic routing

The information to be collected for the NWDAF can be divided into four groups, network data from the NFs, service data from the AF, edge computing topology data from the AF, and management data from the OAM. The data to collect from NFs, from OAM and AF is defined in Table 6.11.1.3.1-1.

Table 6.11.1.2.1-1: Collecting Data for analysing traffic characteristics

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| Location Info | AMF or SMF | The location information of UE. |
| DNN | SMF or PCF | To identify the DNN for the PDU Session which contains the QoS flow |
| S-NSSAI | SMF or AMF | To identify the S-NSSAI for the PDU Session which contains the QoS flow |
| Traffic volume | SMF | The consumed traffic volume for the application identified by the Application Id. |
| UE ID | AMF or SMF | To identify UE |
| UPF resource status | OAM | The status of assigned resources such as CPU and memory |
| UPF load | OAM/NRF | The load of specific NFs |
| Communication and mobility patterns | AF | To characterize the communication and mobility patterns for the service, as specified in TS 23.682 [5] |

NOTE: The correlation of analysed traffic information per DNN, per Slice, per service, per group of UE is dependent on usage of the information. Timestamp can be used to correlate the collected data from different entities.

##### 6.11.1.2.2 Input Information from the SMF to request/subscribe for UPF selection related information

The SMF (or another CP function) may subscribe or request UPF selection related information from the NWDAF by providing one or more of following parameters DNN, S-NSSAI, Application ID, (R)AN Address, Internal Group ID, UE IDs, DNAI, time(s) of the day(s).

##### 6.11.1.2.3 Output Information from the NWDAF for UPF selection

The NWDAF may notify or response to the SMF with time information and average ad peak load information on the list of UPFs requested as shown in Table 6.11.1.2.3-1.Table 6.11.1.2.3-1: Associated Information for UPF Selection from the NWDAF

|  |  |  |
| --- | --- | --- |
| Associated Information | Presence | Description |
| Time information | O | Time of the day, day of the week that the UPF selection information is applied. |
| Load information | O | Expected load of each UPF and associated N3, N6, N9 interface during the time described in Time information. |

##### 6.11.1.2.4 Procedure

Procedure 6.11.1.3.3-1 is used for SMF or other CP functions to obtain data analytics to select UPF for many UEs before the PDU Session is established.



Figure 6.11.1.3.4-1: Procedure to support NWDAF assisting traffic routing

1. The SMF requests to obtain NWDAF analytic information. Two information consuming strategies are possible; subscription/notification and request/response according to TS 23.502 [3], clause 5.2.11. If the SMF wants to obtain analytic information from NWDAF periodically or conditionally, then Nnwdaf\_EventsSubscription service is applicable. If SMF needs to obtain analytic information immediately, then SMF requests the analytic information through Nnwdaf\_AnalyticsInfo service.

The SMF may provide the following information:

- DNN: if the SMF wants to have analytic information for specific DNN(s), and service(s) as an optional part of DNN;

- S-NSSAI: if the SMF wants to have analytic information for a specific network slice instance(s);

- Internal Group ID: if the SMF wants to have analytic information for specific UE Group(s);

- Application ID: if the SMF wants to have analytic information for specific application;

- UPF ID: if the SMF wants to have analytic information for specific UPF(s);

- DNAI: if the SMF wants to have analytic information for specific DNAI(s);

- UE ID: If the SMF wants to have analytic information for a specific UE (e.g. what UPF(s), DNAI(s), and network slice instance(s) are used by the UE).

2. The NWDAF analyses the traffic characteristics based on the collected data from NFs and external entities. The example of collected data is defined in Table 6.11.1.2.1-1.

3. The NWDAF notifies/responses to the SMF with the result of the collected data analysis as described in the clause 6.11.1.2.3. An event notification can be delivered to SMF periodically or conditionally according to the SMF's subscription request. An event response should be delivered immediately when the NWDAF's analysis processing is finished.

The traffic analytic information may include time information (time of the days, days of the week) and/or average load and/or peak load of each UPF. The time of the days could be certain periods, for example 8:00 - 10:00 AM, 19:00 - 23:00 PM.

The SMF may take into account data analytics information from NWDAF to make a decision on UPF (including UL CL) selection/re-selection/modification/removal and utilize existing procedures in TS 23.502 [3].

### 6.11.2 Impacts on Existing Nodes and Functionality

**NWDAF:** The NWDAF should be able to collect data from NFs, AFs, and OAM, and should implement internal logic to analyse UPF, including UL CL, related information.

**SMF:** The SMF should have an interface to interact with the NWDAF to obtain the analytic information. Internally, the SMF may implement UPF, including UL CL, control decision mechanism based on the analytic information from the NWDAF.

### 6.11.3 Solution Evaluation

1. This solution addresses the requirements of key issue 6, and it describes the data to be collected for traffic routing in clause 6.11.1.2.1. The solution defines the analytic source data for traffic routing from various sources. The output analytic data can be utilized by the consumer SMF to assist traffic routing decision.

2. The solution for the SMF to request or subscribe UPF selection information described in clause 6.11.1.2.2, 6.11.1.2.3, and 6.11.1.2.4. The Release 15 NWDAF services, e.g. nwdaf\_EventsSubscription\_Subscribe/Notify and Nnwdaf\_AnalyticsInfo\_Request/Response shall be extended to provide traffic routing assistance service to the consumer SMF.

3. To realize this solution, the expected impacts to NFs are describe in clause 6.11.3. Basically, the solution requires the extension of the existing NWDAF operation.

## 6.12 Solution 12: Data Collection from OAM using the existing SA WG5 services

### 6.12.1 Description

This solution is for Data Collection from OAM associated with *Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure*.

#### 6.12.1.1 General

Based on current definitions from SA WG5, NWDAF have access to the following information provided by OAM:

‐ NG RAN or 5GC performance measurements as defined in TS 28.552 [15] and TS 28.553 [16].

‐ 5G End to end KPIs as defined in TS 28.554 [17].

NWDAF shall use the following SA WG5 services to have access to the information provided by OAM:

- Generic performance assurance and fault supervision management services as defined in TS 28.532 [24].

‐ PM (Performance Management) services as defined in TS 28.550 [13].

‐ FS (Fault Supervision) services defined in the TS 28.545 [18].

OAM shall be responsible for performing:

- the configuration i.e. running Provisioning Services as defined in TS 28.531 [23];

- data collection from job measurements.

Data Collection is expected from OAM (and not from NF) when the target of data collection is not related with an UE or a group of UE (or their PDU Sessions) but is global e.g. corresponds to a slice, a geographical region, a NF set, a NF Id (and no detail on a per UE/PDU Session basis is needed). Another usage of OAM services is when the target of data collection is related to MDT based retrieval of information which is a per UE mechanism.

#### 6.12.1.2 Procedure for the support of Data Collection from OAM

The interactions between NWDAF and OAM for data collection are illustrated in Figure 6.12.1.2-1. The data collected depends on the use cases. This figure is an abstraction of the actual services that are actually defined in 3GPP SA WG5 specifications such as TS 28.532 [24].

The flow below assumes the NWDAF is configured on how to address the relevant OAM services.

OAM shall setup the proper mechanism to guarantee the continuous data collection requested by NWDAF.

NOTE 1: Coordination with SA WG5 is required to clarify if measurements and KPIs required by NWDAF (as defined in the solutions for the key issues) can be provided on top of measurements and KPIs already defined in R15.



Figure 6.12.1.2-1: Data collection from OAM services

1. NWDAF subscribes to OAM services for receiving information from one of OAM services.

NOTE 2: SA WG5 does not restrict the consumers of the 5G management services and therefore NWDAF invokes the existing SA WG5 service to retrieve the management data.

2. OAM perform the required configuration in order to provide the information requested by NWDAF subscription. It is up to the OAM to identify if already deployed/configured support for data collection related to the subscription request will be reused for each request from NWDAF or if new support for data collection of information associated with the subscription needs to be deployed/configured.

3. OAM perform the tasks, e.g. data collection, data processing, associated with the subscribed request from NWDAF.

4. OAM services send notification to NWDAF about subscribed information.

NOTE 3: The call flow in Figure 6.12.1.2-1 only shows a subscribe/notify model for the simplicity, however both request-response and subscription-notification models should be supported.

### 6.12.2 Impacts on Existing Nodes and Functionality

NWDAF is to invoke the current SA WG5 defined service(s) for data collection.

### 6.12.3 Solution Evaluation

This solution defines the framework for data collection from OAM by NWDAF and the detailed parameters of OAM data will be defined in other solutions.

This solution reuses the current SA WG5 defined service(s) for data collection and NWDAF is to invoke the current SA WG5 defined service(s) to collect data as SA WG5 does not restrict the consumers of the 5G management services.

## 6.13 Solution 13: Metadata exposure to 5GS NF and AF

### 6.13.1 Description

This is a solution to Key Issue #1: Analytic Information Exposure to 5GS NF, and Key Issue #2: Analytic information exposure to AF. Metadata refers a set of descriptive data on the analytic information provided by the NWDAF. For example, the metadata could contain the list of the available analytic information, the analytic information name/ description, the calculation algorithm, the analysed data granularity, the sampling rate, etc.

NOTE 1: Metadata structure will be defined in the normative work.

#### 6.13.1.1 Metadata request by 5G NF

This procedure is used by any NF service consumer to obtain the metadata of the available analytic information from the NWDAF such as the list of the available analytics. If the consumer NF needs to obtain the available analytic information, this procedure may be triggered.



Figure 6.13.1.1-1: Metadata request/response by a 5G NF

1. The 5G NF service consumer requests to obtain the metadata of the available analytic information to NWDAF by invoking the request operation via service-based interface with several parameters to efficiently filter out non-related with the request. For example, the parameters of the request operation may be NF type, analytic information category, NF ID, and etc.

2. When the NWDAF successfully received the request from the NF, the metadata containing the analytic information list should be returned via available analytic information response operation.

3. (Optional) If the NF require to get notified when the metadata of the available information is changed, the NWDAF may notify the NF by invoking an analytic information update operation.

#### 6.13.1.2 Available analytic information request by AF

This procedure is used by an AF service consumer to obtain the metadata of the available analytic information from the NWDAF. Unlike a case of 5G NF, the request from an AF may be bypassed via NEF to filter out not authorized requests from 3rd party AFs. This procedure is optional. If the consumer AF needs to obtain the available analytic information, this procedure may be triggered.



Figure 6.13.1.2-1: Metadata request/response by an AF via NEF

1. An AF service consumer request to obtain the metadata of the available analytic information to NWDAF by invoking the request operation via service-based interface with several parameters to efficiently filter out non-related with the request. For example, parameters of the request operation may be NF type (AF), analytic information category, AF ID, and etc. The request message may be bypassed by NEF.

2. When the NWDAF successfully received the request from the AF, the metadata of the analytic information list should be returned via available analytic information response operation. The response message may be bypassed by NEF.

3. (Optional) If the NF require to get notified when the metadata of the available information is changed, the NWDAF may notify the NF by invoke analytic information update operation. The update message may be bypassed by NEF.

#### 6.13.1.3 How 5GS NF/AF request the metadata of the available analytic information

5G NF or AF request the metadata of the available analytics using the Nnwdaf service defined in clauses 6.13.1.1 and 6.13.1.2 that may input information category to efficiently filter out highly related analytics only. The information category can be defined to categorize the available information into several groups. For example, the available information could be categorized by NF type, NF identifier (for a specific NF or AF), and keyword (load, session, mobility, and etc.).

#### 6.13.1.4 How NWDAF provides the available analytics metadata

As a response of the metadata for the available analytic information request, the NWDAF should provide the information to support that NF and/or AF can subscribe or request analytics successfully. NWDAF should provide the available analytic information metadata with event ID and available event filters at least. The candidate information contained in the response (or update) can be detailed in clause 6.1.1.3.

### 6.13.2 Impacts on Existing Nodes and Functionality

NWDAF: A new Nwdaf service should be provided to allow requests from 5G NF/AF. No impacts on the existing Nnwdaf interface.

Consumer 5G NF/AF: For a NF such as PCF or NSSF that are consumers of new Nnwdaf service, the impact is that need to allow the processing of the response/update message from NWDAF.

NEF: To connect NWDAF and AFs, NEF should allow the newly defined NWDAF service.

### 6.13.3 Solution Evaluation

This solution could address the requirements of key issues 1 and 2 for metadata exposure to both NFs and AFs successfully, and it complies the architectural assumptions without any violation. The main idea of this solution is to service operations for metadata exposure. The advantages of this solution are 1) allow metadata exposure to NFs and AFs at the same time, 2) possible to support filtering mechanism for scalability, 3) support of boot string discovery of the available analytic information, and 4) support of notification when metadata is updated. To realize this solution, the expected impact is that the NWDAF and the consumers (NFs and AFs) need to implement new service operations for metadata exposure.

## 6.14 Solution 14: Data Collection from NFs via NF Event Exposure services

### 6.14.1 Description

This solution addresses the Key Issue #3: "Interactions with 5GS NFs/AFs for Data Collection".

This solution proposes to use the existing exposures services (Event Exposure Service) offered by NF such as AMF, SMF, PCF and UDM in order to collect individual behaviour data for producing services related to individual UEs. This solution is used by NWDAF to subscribe/unsubscribe at any NFs to be notified for data collection on a set of events, using existing Event Exposure Service framework defined in TS 23.502 [3]. It extends the principles of the existing exposures services to enable data collection from 5GC NFs and AFs.

The solution is also enhanced to collect pre-computed metrics covering UE populations (geographical areas, cells, NFs, massive IoT, etc.) or other non-OAM groups of information (e.g., application ID), per spatial and temporal dimensions (e.g., per region for a period of time).

Therefore, the extension proposed in solution 14 may be used in complement of the current mechanisms defined in SA WG5 for data collection (see Solution #12).

Basically, OAM services (as defined per TS 28.552 [15], 28.553 [16], 28.554 [17]) may be used to retrieve information targeting a NF, a slice, a gNB while solution 14 may be used to retrieve additional information targeting an UE (or a list of UE(s)) or group(s) of UE(s)).

#### 6.14.1.1 Data Collection via NF/AF Event Exposure

The procedure in Figure 6.14.2-1 is used by NWDAF to subscribe/unsubscribe at NFs (e.g. UDM, AMF, SMF, PCF and AF) to be notified for data collection on a related event (s), using existing Event Exposure Service on Namf, Nsmf, Nudm defined in TS 23.502 [3] ; it also defines a Naf exposure service along the same principles.



Figure 6.14.2-1: Event Exposure Subscribe/unsubscribe for NFs/Operators AFs

NOTE 1: The invoking service operations for PCF are Npcf\_PolicyAuthorization\_Subscribe and Npcf\_PolicyAuthorization\_Notify as defined in clause 5.2.5.3 of TS 23.502 [3]

1. The NWDAF subscribes to or cancels subscription for a (set of) Event ID(s) by invoking the Nnf\_EventExposure\_Subscribe/ Nnf\_ EventExposure \_Unsubscribe service operation.

NOTE 2: The Event ID (s) defined in TS 23.502 [3] could be used or new Event ID(s) could be needed which depends on the use cases.

2. If NWDAF subscribes to a (set of) Event ID(s), the NFs notifies the NWDAF (e.g. with the event report) by invoking Nnf\_EventsExposure\_Notify service operation.

NOTE 3: The NWDAF could use the reporting flag as defined in Table 4.15.1-1 of TS 23.502 [3] to meet the request-response model for data collection from NFs.

The procedure in Figure 6.14.2-2 is used by NWDAF to collect information from 3rd Party AFs and the interaction is done via the NEF.



Figure 6.14.2-2: Event Exposure Subscribe/unsubscribe for 3rd party AFs

0. In order for AF to provide data to NWDAF, a registration of the available data at AF shall be performed.

NOTE 4: The registration process is for NWDAF to discover the address of AFs and the data they can provide to NWDAF. The specifics of the registration is left for normative phase.

1. The NWDAF subscribes to or cancels subscription to data in AF via NEF by invoking the Nnef\_EventExposure\_Subscribe/ Nnef\_EventExposure\_Unsubscribe service operation. If the analytic information event subscription is authorized by the NEF, the NEF records the association of the event trigger and the requester identity.

2. Based on the request from the NWDAF, the NEF subscribes to or cancels subscription to data in AF by invoking the Naf\_EventExposure\_Subscribe/ Naf\_EventExposure\_Unsubscribe service operation.

3. If the NEF subscribes to data in AF, the AF notifies the NEF with the data by invoking Naf\_EventExposure\_Notify service operation.

4. If the NEF receives the notification from the AF, the NEF notifies the NWDAF with the data by invoking Nnef\_EventExposure\_Notify service operation.

#### 6.14.1.2 Usage of Current exposure framework by the NWDAF

The NWDAF can subscribe (and unsubscribe) to the Event exposure service from NF(s) reusing the framework already defined in TS 23.502 [3] subclause 4.15. This framework supports the possibility for the NWDAF to indicate / request:

- One or multiple Event ID(s). Dedicated new Event Id(s) may be (should be) further defined in other solutions of this TR. New Event ID(s) may be defined by non-framework related endorsed ENA solutions. Such Event IDs are called Data Collection Event ID(s).

- The objects targeted by the Events (e.g. an UE identified by its SUPI or GPSI, any UE, a group of UE(s)). The target of event reporting defined in TS 23.502 [3] subclause 4.15.1 is reused (and extended) for that purpose.

- Event Filter Information defined in TS 23.502 [3] subclause 4.15.1. It provides Event Parameter Types and Event Parameter Value(s) to be matched against; In the case of NWDAF, the request may correspond to following optional filters:

- location filters e.g. network Area Of Interest. The Area Of Interest may be defined as a list of cells, a list of Tracking areas, an access type (3GPP, Untrusted Non 3GPP, Wireline), an area type (urban, rural).

- service information filter (e.g. DNN, S-NSSAI, Application ID).

This is further detailed in clause 6.14.1.3.

- A Notification Target Address (+ Notification Correlation ID) as defined in TS 23.502 [3] clause 4.15.1, allowing the NWDAF to correlate notifications received from the NF with this subscription.

- Event Reporting Information described in TS 23.502 [3] Table 4.15.1-1.

The Network Exposure Framework already supports the configuration of Mode of reporting (e.g. reporting up to a maximum number of reports allowing a "one shot" analytics request, periodic reporting along with periodicity, reporting up to a maximum duration) or the request to notify the current status of the subscribed event, if available, immediately to the NWDAF.

This framework could also be supported by AF(s).

The notifications from NF contain on top of the Event being reported (and of dedicated information being reported for this event):

- The Notification Correlation Information provided by the NWDAF in its request;

- (when it applies to the event) the target Id e.g. UE ID (SUPI and if available GPSI);

- A time stamp.

#### 6.14.1.3 Collectable Data Item (CDI).

A CDI corresponds to the minimum granularity of the information that a NF/AF may report as part of a NWDAF subscription request for the newly defined EventId (Data Collection Event ID(s)).

The combination of Data Collection Event Id, Event Target type and possibly Event Parameter Types within the Event Filter Information defines a Collectable Data Item (CDI) type. A corresponding notification may contain multiple CDI(s) that share the same type but may correspond at least to different Target Id(s).

Collectable Data Item (CDI) offered by an NF/AF is information relative to an elementary quantity that the NF can report. It is associated with a type (e.g. one type within: counter, maximum / minimum value, gauge, delay, ratio). The type is defined in 3GPP specification and not reported on interfaces. It may be reported as an individual value only or (for some CDI types) as an average value that may be associated with a maximum and minimum value within a reporting period.

The provision of metrics by NFs reduces the amount of signalling due to exposure of individual events towards the NWDAF.

Each (object) targeted by an Event may optionally support wildcards (meaning any instance of the Target) or range of values within the target identifier. The use of wildcards enables the discovery of new target values (e.g. different values of DNNs).

The CDIs can be either aggregated or explicitly listed. On only one single wildcarded CDI and one single parameter for the event filter information provided within a subscription, it should be possible to specify that the CDI is explicitly listed.

When aggregation level is chosen, the cumulative value of the measurement shall be provided, depending on the type of statistics. The cumulative value uses the same computation rules as each individual item, with just a broader computation scope. For example, if the statistics "counter X" is requested aggregated, only one aggregated counter is provided which totalizes counters on the various elements. When explicitly listed, all parameter types and values of the event filter information from a CDI corresponding to the wildcard are requested. The filter, when applied to the set of CDI\_tags stored in the NF/AF repository, produces a subset of fully defined CDI for each targeted object. For instance, if the requested Data Collection Event ID is associated with a CDI type "XXX" with an explicit list of "TAIx, TAIy, TAIz, as Event Filter, the notification content associated with the Data Collection Event ID is generated with an CDI Value per TAI.

When a CDI is specified by 3GPP, it will be defined whether this CDI can be aggregated or explicitly listed or both.

Within a given subscription, it is possible to request CDIs only along one single dimension (i.e. only per TA, or either only per UE). The available dimensions shall be defined in the normative phase.

#### 6.14.1.4 Discovering Collectable Data Item (CDI).

The NWDAF shall be able to discover the CDI supported by a NF/AF.

### 6.14.2 Impacts on Existing Nodes and Functionality

The NWDAF uses existing network interfaces and services, which are already defined in R15 for event exposure from AMF, SMF, PCF and UDM.

Definition of the AF service and operations for the event exposure.

Extensions on the types of monitoring events from the Exposure Framework from R15 are required.

No additional interface is required on the NFs for the purpose of collection individual UE behaviour.

### 6.14.3 Solution Evaluation

The proposed solution is fit to the need of collecting dedicated information.

This solution allows data collection from NFs/AFs and 3rd Party AFs. It also allows the non-OAM data collection per groups of UEs, or different criteria for defining information populations to be exposed to NWDAF (e.g., per application ID).

The proposed extensions on R15 Exposure Framework for data collection consumption by NWDAF enable NFs/AFs to expose pre-processed data from populations, as well as individual events.

## 6.15 Solution 15: Providing UE Analytics to the NWDAF via the User Plane

### 6.15.1 Description

This clause describes a solution to Key Issue #13: UE Driven Analytics. The solution focuses on addressing the question of *"How the NWDAF collects the UE information"* and fulfilling the requirement that *"The NWDAF shall be able to receive UE's analytics data."*

#### 6.15.1.1 Principles of the Solution

The principles of the solution are that the UE optionally adds a header to each uplink PDU and that the header is populated by the UE with analytics information. The UPF removes the optional header before forwarding the uplink PDU to a Data Network. The UPF provides the analytic information from the header to the NWDAF. The End-to-End Applications whose PDU sessions get used to carry the analytics information may be unaware of the data collection.

Editor's note: It is FFS what analytic data will be carried in the header.

#### 6.15.1.2 Requirements of the Header

The header, or protocol, that is used by the UE to encapsulate the uplink PDU and send analytics data to the UPF should be defined by stage 3. Additionally, the semantics of the analytics data should be defined by stage 3. Stage 2 requirements of the header are as follows:

- Whether the UE populates the header with analytics information should be optional for the UE.

- Which analytic data is included in the header can be based on UE implementation.

- The frequency with which a UE includes a given piece of analytic data should be based on UE implementation (e.g. whether geo-referenced radio data from Wi-Fi is reported once an hour or once a day).

- Data Analytic policies are communicated to the UE via NAS as SM Polices from the PCF to the UE via AMF to indicate the network's preferences of what analytic data should be collected by the UE (including its frequency of collection, etc.). What analytic data the UE collects is based on the network preferences and UE implementation.

- When the UE has analytic data to send and no PDU data to send, the UE may send the only the header and an empty PDU in order to convey the analytic data to network.

NOTE: An existing protocol, such as Network Services Headers (NSH) (RFC 8300 [12]), may fulfil the above requirements and be used to encapsulate the uplink PDU.

#### 6.15.1.3 Activating and Indicating Support for the Solution

The solution is enabled on a PDU Session basis.

The UE indicates to the network, in the 5GSM Core Network Capability, if it supports the optional header and if local UE policies dictate that analytic data may be provided as part of this PDU session.

If SMF policies dictate that the header should be enabled and the UE indicated its support in the 5GSM Core Network Capability, then the SMF indicates to the UPF, then the SMF selects a UPF to process header and indicates to the UPF, in the N4 Session Establishment/Modification Request, if the header will be enabled in the PDU session.

The SMF indicates to the UE, in the PDU Session Establishment Accept, if the optional header should be included in the uplink PDUs.

The SMF indicates to the (R)AN, in the N2 SM information, if the optional header will be included in uplink PDUs of the PDU session. (R)AN can take this information into account when performing header compression for the PDU session.

#### 6.15.1.4 Providing Analytic Data to the NWDAF

The UPF provides collected analytic data directly to the NWDAF. How and when the UPF provides the analytic data information to the NWDAF will be determined by the Key Issue #3 conclusion.

#### 6.15.1.5 Privacy and Integrity Protection of the Analytic Data

Integrity protection and ciphering may be applied to the header as if it is part of the PDU.

### 6.15.2 Impacts on Existing Nodes and Functionality

UE:

- Requires support for the new header or protocol.

- Indicates its support of the header in 5GSM Core Network Capability.

- Enables the header when the SMF indicates, in the PDU Session Establishment Accept, that it should be enabled.

- Receives data collection policies from the PCF.

(R)AN:

- Receives an indication of whether the header is enabled for the PDU session.

SMF:

- Receives an indication of the UE's support for the header in 5GSM Core Network Capability.

- If PDU session has multiple UPFs, selects which of these will process the header.

- Indicates to the UPF, in the N4 Session Establishment/Modification Request, if the header will be enabled.

- Indicates to the UE, in the PDU Session Establishment Accept, when the header should be enabled.

- Indicates to the (R)AN, through the N2 SM information, if the header will be enabled.

PCF:

- Creates and communicates data collection policies to the UE.

UPF:

- Requires support for the new header or protocol.

- Receives an indication, in the N4 Session Establishment/Modification Request, if the header will be enabled.

- Removes the Header and Analytics information from the PDU.

- Provides the Analytics information to the NWDAF.

### 6.15.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.16 Solution 16: Use of UE analytics in the 5GC

### 6.16.1 Description

This is a solution to Key Issue 13: UE Driven analytics. In particular, to address:

- How the NWDAF collects the UE's information.

- How the NWDAF uses the data provided by the UE to do analytics and provides the analytics information to other NFs.

There are already defined services in the NWDAF for sharing analytics to NFs within 5GC. The PCF and NSSF are two key consumers of such services. To provide access to UE Terminal Analytics, procedures can be defined to convey such information from UE to 5GC NFs, leveraging already available interfaces to 5GC.

The NWDAF collects network analytics from other NFs and combines terminal analytics coming from the UE) with the network analytics. In the example below the NSSF requests the combined analytics information from the NWDAF to assist in making slice selection decisions.



Figure 6.16.1-1 Procedure for sharing terminal analytics between UE and NWDAF

Table 6.16.1-1 below shows what information elements are sent by the UE in the Terminal Analytics Update message and how they are used.

Table 6.16.1-1: Analytics information reported by the UE

|  |  |  |  |
| --- | --- | --- | --- |
| Information | Presence | Service user | Description |
| UE  out-of-coverage entries | O | AF, NWDAF, OAM | The UE in idle mode may monitor and report the number of out-of-coverage entries (i.e. loosing service) per defined time. There may be cases when the UE loses service in low coverage areas which is not noticeable by the network if the UE is back to service before the next periodic update timer expires (when the UE is due to trigger a periodic update with the network).  The information about the number of out-of-coverage service entries without change of the registration area, excluding those due to rejection from the network, may indicate problems like UE often being in no or low coverage area (i.e. loosing service) for short periods of time. This information may be notified to the network operator or Service Provider (e.g. AF). The 3GPP network operator may improve the radio coverage conditions in general or at the locations where the UEs loose service. |

NOTE: SA WG2 to enquire with RAN WG2 and SA WG5 on whether any of the above listed UE analytics information is already available via the MDT or is to be made available within an ongoing SI/WI in these groups so that a duplications is avoided.

Editor's note: Identify what triggers the UE to send a Terminal Analytics Update message.

Editor's note: Identify whether the Terminal Analytics Update is sent via new or existing messages.

### 6.16.2 Impacts on Existing Nodes and Functionality

- UE, AMF and NWDAF:

- New procedure to be defined to share Terminal Analytics via already available interfaces to 5GC.

- NWDAF:

- New functionality at NWDAF to combine NW analytics with Terminal Analytics.

### 6.16.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.17 Solution 17: Trace based solution to collect UE related information in NWDAF

### 6.17.1 Description

This is a solution to Key Issue#13: UE Driven Analysis.

#### 6.17.1.1 NWDAF subscribes the trace events to TCE

A new interface between NWDAF and TCE is supported to collect trace recording information.

Figure 6.17.1-1 specified the Trace event subscribe procedure. NWDAF subscribes the trace events to the TCE with SUPI. The Trace events subscribe procedure can be applied to single UE or multiple UE.



Figure 6.17.1-1: Trace event subscribe procedure

Editor's note: The details of trace event in Trace events subscribe request is FFS.

#### 6.17.1.2 NWDAF triggers trace procedure

A new interface between NWDAF and Management System is supported to exposure the Trace event request from NWDAF.

NWDAF collects UE based information by triggering the Trace procedure in EM as specified in Figure 6.17.1-2.



Figure 6.17.1-2: NWDAF triggers trace procedure

1. NWDAF sends the Trace request message to Management System. The one or more SUPI and requested Trace event are included in this request message.

Editor's note: The details of Trace event in the Trace request message is FFS.

Steps 2 to be defined in TS 32.422 [20] and they are extrapolated by what is defined is defined already for E-UTRAN:

2. EM initiates the Trace Session Activation to NG-RAN according to the request received from NWDAF.

3. NG-RAN starts the Trace session and stores MDT parameters.

4. NG-RAN performs the MDT procedure. The more details about MDT procedure and parameters are discussed in RAN WG2 and RAN WG3. NG-RAN sends the information to the TCE/OAM which received from UE.

Editor's note: The impacts to the NG-RAN will be evaluated by RAN group.

5. NG-RAN sends the Trace recording report to TCE/OAM.

6. f NWDAF subscribed the trace events as described in clause 6.17.1.1, TCE reports the trace events to NWDAF.

### 6.17.2 Impacts on Existing Nodes and Functionality

Editor's note: Capture impacts on existing 3GPP nodes and functional elements.

NWDAF:

- Support interface to Management System.

- Trigger the trace procedure to Management System.

- Support interface to TCE.

- Subscribe the trace event request in TCE.

Management System:

- Initiates trace procedure due to the trigger from NWDAF.

TCE/OAM:

- Support trace event subscribe service for NWDAF.

- Report the trace recording to NWDAF.

### 6.17.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.18 Solution 18: NWDAF assisting Future Background Data Transfer (BDT)

### 6.18.1 Description

This solution is for Key Issue 7: NWDAF assisting Future Background Data Transfer.

As currently specified in clause 4.16.7 Negotiations for future background data transfer in TS 23.502 [3], H-PCF can provide one or more transfer policies for the future background data transfer based on requests from the AF, The transfer policy is generated by the H-PCF based on e.g. analytics information, the list of already agreed BDT stored in the UDR, and some other information listed in TS 23.503 [4]. The transfer policy is stored in UDR. At the time the ASP indicates that transfer of background data to the UE starts. The PCF retrieves the transfer policy and enforces it.

It is considered that the network condition at the UE location could directly impact the transfer policy for future background data transfer provided to the ASP in particular:

- UE Moving Trajectory.

- Network performance information such as NF available capacity of 5G NF which serves the UE.

There are 2 variants of the solution:

- AF knowledge of UE area: in this variant the AF provides the target area where Future Background Data Transfer is expected. This variant focuses on the fact that the AF has a better knowledge than the network on where the UE(s) should be at the expected time of the background data transfer.

- NWDAF prediction of the UE area: in this variant the AF does not provide the target area where Future Background Data Transfer is expected but the NWDAF has to determine (guess/predict) it based on:

‐ the knowledge of the list of UE corresponding to the AF transfer. To avoid AF providing huge lists of UE(s) it is assumed that all these UE are configured to belong to a group and the AF only refers to the Group ID.

‐ predictions on UE mobility: NWDAF derives the UE Moving Trajectory by collecting the UE level information such as location information from AMF.

In both cases Network performance information is collected from OAM by NWDAF, possibly RAN OAM.

#### 6.18.1.1 Information to support Future Background Data Transfer

The UE level information related to background data transfer per UE is defined in Table 6.18.1.1-1.

This information is not needed in case of AF knowledge of UE area.

Table 6.18.1.1-1: NWDAF input data

|  |  |  |  |
| --- | --- | --- | --- |
| Information | Presence | Source | Description |
| UE ID or Internal group Id | C |  | Present if NWDAF requests location information |
| ***Location info*** |  |  |  |
| >Timestamp | C | AMF | The age of the information |
| >Location Info | C | AMF | The location info for the UE e.g. Cell ID or TA ID |
| ***Network performance info*** |  |  |  |
| *Area information* | C | OAM | Present if NWDAF requests network performance information |
| *Load information* | C |  | Statistics on load in the area. |

NOTE Network performance information is required for a BDT policy, we need to ask and cooperate with SA WG5 which NW performance indicators are available.

#### 6.18.1.2 Procedure for Future Background Data Transfer

Prerequisite: The PCF may subscribe to or periodically requests upon AF:

- NWDAF prediction of the number of UEs of an ASP in an area and the expected load in that area at a certain time and date.

### 6.18.2 Impacts on Existing Nodes and Functionality

Editor's note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.18.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.19 Solution 19: NWDAF/NWDAF service registration and metadata exposure to NFs

### 6.19.1 Description

This is an extension of Solution #1 to describe the following aspects of Key Issue #1: Analytic Information Exposure to 5GS NF:

- How the NWDAF provides/updates the available analytic information metadata to the 5GS NF (or subset of relevant analytic information metadata).

Metadata refers a set of descriptive data on the analytic information provided by the NWDAF such as list of available analytic information, metrics, calculation algorithms, sampling rate etc, although the most relevant metadata is the available analytic information that will allow a NF to select a NWDAF instance that supports an analytic information (e.g. UE expected trajectory) while other metadata such as supported metrics, calculation algorithms or sampling rate are considered not needed in the context of the use cases defined in this TR so far and as such not used any longer in this description.

The proposal uses the Event ID as one example of the required analytics metadata information, but this proposal is generic for any metadata and therefore can be extended when other metadata is required though the Event ID is the only example so far.

The Registration and Discovery of a NWDAF instance/NWDAF service that supports analytics metadata of a specific analytic type is described below. Note that according to TS 23.502 [3], procedures to update the supported analytics are available although not mentioned here.

#### 6.19.1.1 Registration of NWDAF/NWDAF service into the NRF

This procedure extends the NF service Registration described in TS 23.502 [3], to include specific service parameters for NWDAF, i.e. analytics type.



Figure 6.19.1.1-1: NWDAF/NWDAF Service Registration

1. An NWDAF instance sends Nnrf\_NFManagement\_NFRegister Request message (the NWDAF profile) to NRF to inform the NRF of its NF profile when the NWDAF becomes operative for the first time. The NWDAF includes NF type: "NWDAF", FQDN or IP address of NWDAF, Names of supported NWDAF services, Endpoint information of instance(s) of each supported service and other service parameter. The other service parameters are the analytics metadata information, e.g. type of analytics that the NWDAF instance supports. In solution #1 this type of analytics is identified by an EventId. If some of the Events may be used by NFs that are not in the same domain as NWDAF then the NWDAF profile includes this information.

2. The NRF stores the NWDAF profile, as described in TS 23.502 [3].

3. The NRF acknowledge NWDAF Registration is accepted via Nnrf\_NFManagement\_NFRegister response, as described in TS 23.502 [3].

#### 6.19.1.2 NWDAF/NWDAF service discovery

This procedure extends the NF/NF service discovery described in TS 23.502 [3], to include discovery of a NWDAF instance supporting specific service parameters, e.g. analytics type. Note that if an AF discovers a NWDAF instance supporting specific analytic type, then the same procedure will be invoked by NEF if AF is external or by the AF itself if it is an NF.



Figure 6.19.1.2-1: NWDAF/NWDAF Service Discovery

1. The NF service consumer intends to discover analytics services available in the network based on service name and target NF type "NWDAF", invokes Nnrf\_NFDiscovery\_Request (Nnwdaf\_EventSubscription/Nnwdaf\_AnalyticsInfo, NWDAF, NF type of the NF consumer). The parameter includes the requested analytics type, identified by an EventId.

2. The NRF authorizes the Nnrf\_NFDiscovery\_Request as described in TS 23.502 [3],

3. If allowed, the NRF determines the discovered NWDAF instance(s) or Nnwdaf\_EventsSubscription or Nnwdaf\_AnalyticsInfo service instance(s) and provides the information of a set of discovered NWDAF instance(s) or NWDAF service instance(s) to the NF service consumer via Nnrf\_NFDiscovery\_Request Response message. as described in TS 23.502 [3].

### 6.19.2 Impacts on Existing Nodes and Functionality

NWDAF: NWDAF registration to NRF following NF/NF Service Framework defined in TS 23.501 [2] for any NF, extended to provide the analytics metadata information (e.g. analytic type, identified by an EventID) in the Nnrf\_NFRegistration\_Request.

During discovery, if the target NF is a NWDAF then if the fields related to analytics metadata information (e.g., Event ID) are used in the request, the NRF shall provide the corresponding NWDAF instance(s) that supports the fields related to the analytics metadata information. Otherwise, if fields related to analytics metadata information (e.g., Event ID) are not provided in the request, the NRF shall return all applicable NWDAF instance(s) supporting the requested Nnwdaf service(s).

NF service consumer, needs to provide the requested analytics in metadata information, when using Nnrf\_NFDiscovery\_Request.

### 6.19.3 Solution Evaluation

This solution has minor impacts on the NF/NF service discovery framework, that only needs to include the analytics metadata information in service parameter.

The solution proposes a smooth evolution from Rel-15 functionality.

## 6.20 Solution 20: NWDAF analytics usage for UPF selection

### 6.20.1 Description

#### 6.20.1.1 General

This is a solution to Key Issue #6: NWDAF assisting traffic routing.

For UPF selection, SMF is considering different parameters, among which the UE location information and the UPF dynamic load. UPF selection can be enhanced with NWDAF functionality. For example, SMF can use mobility information for the UE, such as analytics but also predictions. SMF can also consider UPFs load predictions coming from NWDAF.

#### 6.20.1.2 Procedures

The procedure is based on SMF using NWDAF outputs. Current description reuses mechanisms as proposed in solution #1 for SMF to retrieve analytics from NWDAF, but any framework solution adopted for key issue #1: Analytic Information Exposure to 5GS NF can be reused.

In this procedure, the SMF only has to contact the NWDAF once for UE mobility information and the UPF load.



Figure 6.20.1.2-1: UPF selection based on NWDAF outputs

1. SMF subscribes towards NWDAF to be notified about UPF load information, if SMF is configured with the list of UPFs.

2. NWDAF accepts the subscription and provides already information available on UPFs load, which can be statistics (e.g. which NWDAF could get from e.g. OAM) or predictions.

3. During PDU session establishment, UPF selection is needed.

4. SMF request NWDAF for mobility information for the UE, e.g. analytics or predictions or both.

5. NWDAF returns UE mobility information to the SMF. The information is based on e.g. information which NWDAF retrieved previously from other NFs such as AMF.

6. If SMF needs to discover the UPF as defined in TS 23.501 [2].

7. The result of the discovery is provided to SMF. If SMF already has stored the load per UPF steps 8 and 9 are skipped.

8. SMF request NWDAF to provide load per UPF(s).

9. NWDAF provides the load for the UPF(s), both based on historical information and predictions.

10. SMF selects the target UPF using information listed in TS 23.501 [2] for UPF selection and the analytics information provided by NWDAF, both statistics and predictions in UPF load and in UE mobility.

### 6.20.2 Impacts on Existing Nodes and Functionality

Impacts to NFs:

- SMF: Support UPF selection with analytics information on both UE mobility and UPF load.

- Request NWDAF for analytics on UE mobility during PDU session establishment;

- When SMF knows the list of UPFs (via configuration or by discovery via NRF), SMF subscribes to NWDAF or requests NWDAF to receive UPF load analytics.

- NWDAF: provide analytics on UPFs load based on e.g. information from OAM.

### 6.20.3 Solution Evaluation

This solution reuses the existing UPF discovery procedure defined in TS 23.501 [2] and reuses existing information and configuration in the SMF for UPF discovery.

## 6.21 Solution 21: Supervision of IoT devices for risk precaution

### 6.21.1 Description

#### 6.21.1.1 General

In the key issue 8, it is mentioned that the IoT devices may be misused or hijacked, and hence brings security issues to the 3GPP system or application layer services. This solution proposes that, first, the NWDAF analysis is relied to detect the misbehaviours of IoT UE(s) and evaluate the risk brought by the misbehaviour UE(s). The NWDAF can perform analysis such as:

- Detect out of the ordinary behaviour of a specific UE from within a group of mIoT UEs over a period of time. This can help identify a misbehaving UE, a theft of service from a UE or a hijacked UE.

- Detect out of the ordinary behaviour for set of UEs in a group within a short term to identify sudden change in behaviour that may indicate hijacking of multiple UEs, denial of service attacks, etc.

Once the NWDAF deems that any risk brought by the misused or hijacked UEs is serious enough to notify or alert the subscribers, the NWDAF notifies the related subscribers (could be network functions or service providers) about the suspicious events or risk, so that the 3GPP system or service provider can adopt an appropriate action(s) for the risk.

NOTE: The misused or hijacked UEs are UEs in which there are malicious applications running or UEs which have been stolen.

#### 6.21.1.2 Identifying misbehaving UE(s)

When the network operator or IoT service provider asks the NWDAF for supervision of a specific or a group of IoT devices, the NWDAF performs data analysis on such devices based on the collected information from the application server and the 3GPP network to identify rogue behaviour for a single or multiple UEs. In order to identify misbehaving UEs, the NWDAF compare the UE runtime data with expected UE behaviours.

NWDAF becomes aware of UE IDs belonging to a group of mIoT UEs via consulting the UDM for subscriber information. The expected behaviour for a group of mIoT UEs can be:

- Provisioned into the UDM by the network operator based on for example its expectation about the behaviour, SLAs with IoT service providers managing groups of UEs, etc.;

- Identified by application server and provided directly to the NWDAF; or

- learned by the NWDAF itself via collection of historical data for that group.

The following table 6.21.1.2-1 gives an example of the expected UE behaviour parameters.

Table 6.21.1.2-1: An example of expected UE behavioural information

|  |  |  |
| --- | --- | --- |
| Information | Presence | Description |
| Stationary indication | O | Identifies whether the UE group is stationary or mobile, e.g. only on demand. (TS 23.682 [5], clause 5.10.1). |
| Periodic communication indicator | O | Identifies whether the UE group communicates periodically or not, e.g. only on demand. (TS 23.682 [5], clause 5.10.1). |
| Communication duration time | O | Duration interval time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1).  Example: 5 minutes |
| Periodic time | O | Interval Time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1).  Example: every hour |
| Scheduled communication time | O | Time zone and Day of the week when the UE is available for communication (TS 23.682 [5], clause 5.10.1).  Example: Time: 13:00-20:00, Day: Monday |
| Maximum Latency | O | Indicating maximum delay acceptable for downlink data transfers (TS 23.682 [5], clause 4.5.21). |
| Maximum Response Time | O | Indicating the time for which the UE stays reachable to allow the AF to reliably deliver the required downlink data (TS 23.682 [5], clause 4.5.21). |
| Suggested Number of Downlink Packets | O | Indicating the number of packets that the UPF shall buffer in case the UE is not reachable (TS 23.682 [5], clause 4.5.21). |

In order to collect some runtime data like UE current location, data rate etc., the NWDAF may request the 3GPP network to start monitoring the UE states, i.e. the NWDAF sends monitoring request to the NFs to collect the required network data, e.g., as reported by monitoring events listed in table 6.21.1.2-2.

The information for the support of Performance improvement and supervision of mIoT terminals could also additionally be the information listed in Table 6.8.1.1-1.

Table 6.21.1.2-2: Examples of monitoring events

|  |  |  |
| --- | --- | --- |
| Event | Description | Which NF detects the event |
| Location Reporting | As specified in the table 4.15.3.1-1 in TS 23.502 [3] | As specified in the table 4.15.3.1-1 in TS 23.502 [3] |
| Change of SUPI-PEI association |
| Roaming status |
| Communication failure |
| Availability after DNN failure |
| Number of UEs present in a geographical area |
| UL or DL Packet Latency | Indicating the delay for uplink or downlink packets transfers for the UE | SMF |
| UL or DL data rate | Indicating the bit rate for uplink or downlink packets transfers for the UE | SMF |
| Frequent mobility re-registration | A stationary UE may re-select between neighbor cells due to radio coverage fluctuations. This may lead to multiple re-registrations if the cells belong to different registration areas. The number of re-registrations may be an indication for abnormal behavior. | AMF |

#### 6.21.1.3 Solving the risk brought by misbehaving UE(s)

After the NWDAF completes the data analysis and detects some UEs with serious misbehaviours, e.g. unexpected UE location, abnormal traffic pattern, wrong destination address etc., the NWDAF determines whether to notify or alert the related 5GC NFs or application layer based on the subscriptions from these 5GC NFs.

If PCF subscribes the notification, the NWDAF sends the PCF a notification about the risk or suspicious events, which triggers the PCF to update the AM/SM policies. The NWDAF can also send the notification directly to the AMF or SMF, if the AMF or SMF subscribes the notification, so that the AMF or SMF can, based on operator policies, adopt pre-defined anti-risk mechanisms. The following table gives examples of policies and actions for risk solving. The exact policies and actions to solve specific risks depend on operator's configurations.

Table 6.21.1.3-1: Examples of policies and actions for risk solving

|  |  |  |
| --- | --- | --- |
| Risk description | AM/SM policy | Actions of NFs |
| Unexpected UE location | Add the area of current UE location into mobility restriction | AMF Applies mobility restriction |
| Unexpected elephant flows | Decrease the MBR for the related QoS flow | SMF updates the QoS rule |
| Unexpected wakeup | Apply MM back-off timer to the UE | AMF applies MM back-off timer to the UE |
| Suspicion of DDoS attack | Release the PDU session and Apply SM back-off timer | SMF releases the PDU session and applies SM back-off timer |
| Wrong destination address | Update the packet filter of the related QoS flow to block the wrong SDF | SMF updates the packet filter of the related QoS flow and configures the UPF |
| Ping-ponging stationary UE | NWDAF notifies the AMF or AF (Service Provider) | AMF may adjust UE registration area.  AF (Service Provider) may adjusts UE location. |

Based on the subscription of the application server, the NWDAF sends the notification/alert to the application server, which may trigger application layer to activate some risk precaution methods.

#### 6.21.1.4 Procedures

The procedure of using NWDAF to identify the misbehaviour IoT devices and trigger risk precaution for such IoT devices is shown in the Figure below.



Figure 6.21.1.4-1: Procedure of using NWDAF to supervise IoT devices and enable risk precaution

0. When an IoT UE is registering to the network, the network decides whether to subscribe risk analytic report from the NWDAF. NWDAF becomes aware of the mIoT UE group that the UE belongs to and the expected behaviour for that group based mechanisms described in clause 6.21.1.2. During the registration procedure, UDM provides the expected UE behaviour parameters together with a UE group ID to the AMF/SMF.

1a. The AMF/SMF serving the UE may subscribe risk analytic report from the NWDAF for a specific UE. In the subscription message, the AMF/SMF may include expected UE behaviour parameters retrieved from the UDM.

1b. The PCF may subscribe risk analytic report from the NWDAF for a specific UE or a group of UEs. In the subscription message, the PC may include expected UE behaviour parameters for the UE or the UE group.

1c. The application layer SCS/AS may subscribe the risk analytic report from the NWDAF, where the subscription message may contain expected UE behaviour parameters identified on the application layer. The subscription message can be UE specific or UE group specific.

2. The NWDAF starts the data analysis for the UEs indicated in the subscription message.

3-4. The NWDAF may collect some runtime data of the UE(s) by sending monitoring request to the related NFs. The monitoring request may be sent to the NFs directly or via NEF based on operator's configuration.

5. The 5GC NFs (e.g. AMF, SMF) send event reports to the NWDAF based on the report requirements received in the monitoring request.

NOTE: The detailed monitoring procedures via NEF refer to clause 4.15.3 in TS 23.502 [3].

6. The NWDAF analyses the collected data for the IoT devices, and may detect some suspicious events which may be a risk, e.g., unexpected UE location, abnormal traffic pattern, wrong destination address. Based on the risk type and operator policies, The NWDAF determines whether to send a notification or alert to the application layer and the 3GPP network.

7. The notification or alert sent to the application layer indicates an exception ID, which is used by the SCS/AS to choose appropriate security precaution methods, e.g. isolating the misbehaviour UE, locking the account etc.

8. The notification or alert may be sent to the PCF, so that the PCF can promptly adjust the related AM/SM policies (e.g. as described in the Table 6.21.1.3-1) to prevent the deterioration of the security issue.

9. The updated AM/SM policies are provisioned to the AMF/SMF via PCF service Npcf\_AM/SMPolicycontrol\_Update Notify.

10. The AMF/SMF enforce the updated policies.

11. The notification or alert containing the exception ID may be sent to the related 5GC NFs directly, e.g. AMF or SMF.

12. Once the AMF or SMF receives the exception ID, based on the operator policies, it adopts appropriate actions (e.g. as described in the Table 6.21.1.3-1) to relieve the risk.

### 6.21.2 Impacts on Existing Nodes and Functionality

AMF:

- Subscribes risk report from the NWDAF;

- Collects network data and sends data report to NWDAF if collecting network data was requested;

- Determines and enforces anti-risk mechanism if receiving an Exception ID from the NWDAF.

SMF:

- Subscribes risk report from the NWDAF;

- Collects network data and sends data report to NWDAF if collecting network data was requested;

- Determines and enforces anti-risk mechanism if receiving an Exception ID from the NWDAF.

PCF:

- Subscribes risk report from the NWDAF;

- Defines anti-risk policies based on received Exception IDs.

NEF:

- Receives monitoring request from the NWDAF and forwards monitoring report to the NWDAF if needed.

NWDAF:

- Collects network data from 5G NFs and/or SCS/AS;

- Sends monitoring request to the NEF if it supports;

- Performs data analysis to identify misbehaving UEs and risks;

- Notifies 5G NFs or SCS/AS about the identified risks and related UEs based on subscriptions.

### 6.21.3 Solution Evaluation

This solution relies on the NWDAF to identify misbehaving UEs and the risk(s) brought by such UEs. If the NWDAF identifies any risk, based on operator's policies, it sends notification or alert to subscribers who are interested in the risk report. A risk is indicated by an Event/Exception ID, if the PCF receives the Exception ID, it may define some anti-risk policies, e.g. adjusting MM/SM policies; if the AMF/SMF receives the Exception ID, it determines the anti-risk mechanism if needed, and then enforces the anti-risk mechanism.

This solution allows the network to automatically identify misbehaving UEs, evaluate the risk(s) brought by such UEs, and solve the risk(s), which is useful to improve the efficiency of network management and strengthen the network capability of resisting risk, especially for the network serving massive IoT devices.

## 6.22 Solution 22: Optimizing connection management based on NWDAF output

### 6.22.1 Description

#### 6.22.1.1 General

This solution would like to utilize NWDAF to predict the time window in which the UE has or doesn't have UL/DL data transmission, so that the AMF can optimize connection management. Such prediction can be specified as the UE communication pattern. In order to obtain UE communication pattern, it is necessary to let the NWDAF know the communications that UE has.

In Rel‑15, communication pattern is defined as per UE level and the 5GC has been able to understand communication pattern (called "Expected UE Behaviour parameters" in TS 23.501 [2]) which is provisioned by external party via the NEF. However, in the case of the UE simultaneously communicating with multiple application servers, it may be not easy for application layer to know that per UE communication pattern.

In this solution, the NWDAF is expected to discover UE communication pattern to optimize connection management. The NWDAF collects the UE communication history from 3rd party Application Servers, such as the time that the UE started each communication (identified by the application server IP and UE IP), service type, and the duration of the communication etc.

By applying data mining, the NWDAF may be able to model the UE communication pattern, and then provide the analytical result to the AMF. The analytical result for a specific UE or a group of UE may be traditional communication pattern defined in TS 23.682 [5] with following additions:

- The time and day that the UE might start a low latency communication, e.g. Time: 8:00-9:00, Day: Monday-Friday; and/or

- The time and day that the UE might not have any communication, e.g. Time: 23:00-7:00, Day: Sunday-Friday;

The 5GC can utilize the UE mobility information and UE communication pattern to optimize connection management for a UE:

- If the UE communication pattern indicates that the UE has a low latency communication for a time period, the AMF may keep the UE in CM-CONNECTED mode to reduce the latency of UE obtaining the service;

- If the UE communication pattern indicates that the UE has no communication in a time period, the AMF may advise the UE to adopt power saving method, e.g. PSM or MICO;

- If the UE communication pattern indicates that the UE has frequent communications in a time period, and the UE mobility information shows that the UE stay in a same place in that time period, the AMF may keep the UE in CM-CONNECTED mode to reduce the signalling on CM state transitions but without bring frequent handover.

#### 6.22.1.2 Procedures

The provision of UE communication pattern and UE mobility prediction from the NWDAF to the 5GC is shown in the Figure below.



Figure 6.22.1.2-1: procedure of using NWDAF out to optimize connection management

1. A UE registers to the AMF.

2. The AMF subscribes analytic result on UE communication.

3. The NWDAF provides the UE communication pattern and UE mobility prediction to the AMF.

4. The AMF has received UE communication pattern, and the UE communication pattern indicates that the UE has no communication in a time period, the AMF may suggest the UE adopting power saving, and then the AMF includes the time period that the power saving can be activated in the Registration Accept message.

NOTE: Whether to adopt power saving and which power saving method is adopted are up to UE decision.

5. The AMF stores the received analytic results, and then optimizes connection management for the UE as described in clause 6.22.1.1.

### 6.22.2 Impacts on Existing Nodes and Functionality

Editor's note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.22.3 Solution Evaluation

Editor's note: Use this section for evaluation at solution level.

## 6.23 Solution 23: AMF using NWDAF outputs to optimize UE mobility procedures

### 6.23.1 Description

#### 6.23.1.1 General

This is a solution to Key Issue #9: Customizing mobility management based on NWDAF output.

In this solution, the AMF uses UE mobility information as provided by NWDAF. Current description reuses mechanisms as proposed in solution #1 for AMF to retrieve analytics from NWDAF, but any framework solution adopted for key issue #1: Analytic Information Exposure to 5GS NF can be reused.

The UE mobility information as provided by NWDAF can contain historical UE mobility information or predictions, or both, and can be used by AMF as an input for optimizing UE mobility, e.g. registration area determination, paging area determination.

#### 6.23.1.2 Procedures



Figure 6.23.1.2-1: AMF using NWDAF outputs to optimize UE mobility procedures

1. The UE initiates registration.

2. The AMF, based on local policies, requests NWDAF for mobility information for the UE, using either Nnwdaf\_AnalyticsInfo or Nnwdaf\_EventsSubscription service. The AMF can request for analytics or for predictions or for both.

3. The NWDAF derives requested mobility information for the UE.

NOTE 1: NWDAF can derive UE mobility information based on data collected for the UE, e.g. using framework procedure that will be agreed to be progressed as part of normative work for eNA data collection.

4. The NWDAF provide requested UE mobility information to the AMF.

5. During AM Policy Association Establishment, the PCF provides AMF with the Access and mobility related policy control information (e.g. service area restrictions).

6. The AMF derives registration area for the UE based on the UE mobility information provided by NWDAF and the service area restrictions as instructed by PCF.

NOTE 2: The AMF logic for deriving registration area is out of scope of 3GPP.

7. The AMF sends a Registration Accept message to the UE containing the allocated Registration Area to the UE.

8. If the AMF used Nnwdaf\_EventsSubscription service in step 2, the AMF may receive updated mobility information from NWDAF for that UE.

9. When AMF detects that paging the UE is needed, the AMF may use the information as provided by NWDAF to determine the paging area.

NOTE 3: The AMF logic for deriving paging area is out of scope of 3GPP.

10. The AMF pages the UE in the area determined at step 8.

### 6.23.2 Impacts on Existing Nodes and Functionality

The Nnwdaf\_EventsSubscription and Nnwdaf\_AnalyticsInfo services need to be enhanced to allow provisioning of analytics or predictions or both for mobility information for a specific UE.

### 6.23.3 Solution Evaluation

This solution only impacts the Nnwdaf\_EventsSubscription and Nnwdaf\_AnalyticsInfo services, with the addition of UE mobility event and request for either statistics or predictions or both.

The main difference between this solution and solution 4 resides in the non-involvement of PCF: in the present solution, PCF is not involved in any recommendation regarding registration areas or paging areas, only AMF derives registration areas and paging areas for the UE based on inputs provided by NWDAF.

## 6.24 Solution 24: Analytics Information Exposure to AF

### 6.24.1 Description

This solution addresses the issues of how to expose analytics information to AF as described in Key Issue #2 (Analytic Information Exposure to AF).

NOTE: What information could expose to AF is based on the specific use case discussion outcome.

#### 6.24.1.1 Procedure for AF subscription to NWDAF analytics



Figure 6.24.1.1-1: Procedure for AF subscription to NWDAF analytics

1. AF invokes the Nnwdaf\_ EventSubscription Subscribe operation for subscribing to NWDAF analytics or Nnwdaf\_EventSubscription Unsubscribe operation to unsubscribe for NWDAF notifications.

2. NWDAF uses the Nnwdaf\_ EventSubscription Notify operation to expose the analytics information that AF subscribed to receive.

The interaction between AF and NWDAF is direct if the AF is located inside operator network or the interaction is done via the NEF if the AF belongs to 3rd party as follows.



Figure 6.24.1.1-2: Procedure for AF subscription to NWDAF analytics (for AF not allowed for direct access to NWDAF)

1. The AF subscribes to or cancels subscription to analytic information via NEF by invoking the Nnef\_EventExposure\_Subscribe/ Nnef\_EventExposure\_Unsubscribe service operation. If the analytic information event subscription is authorized by the NEF, the NEF records the association of the event trigger and the requester identity.

2. Based on the request from the AF, the NEF subscribes to or cancels subscription to analytic information by invoking the Nnwdaf\_EventsSubscription\_Subscribe/ Nnwdaf\_EventsSubscription\_Unsubscribe service operation. In the subscription to NWDAF analytics, NEF may apply restrictions to the subscription request to NWDAF (e.g., restrictions to parameters or parameter values from Nnwdaf\_EventSubscription\_Subscribe service operations) based on operator configuration.

3. If the NEF subscribes to analytic information, the NWDAF notifies the NEF with the analytic information by invoking Nnwdaf\_EventsSubscription\_Notify service operation.

4. If the NEF receives the notification from the NWDAF, the NEF notifies the AF with the analytic information by invoking Nnef\_EventExposure\_Notify service operation.

NOTE: The call flows only show a subscription-notify model for the simplicity instead of both request-response model and subscription-notification model.

### 6.24.2 Impacts on Existing Nodes and Functionality

NEF: The NEF needs to be enhanced to handle the analytics information exposure between NWDAF and AF.

### 6.24.3 Solution Evaluation

This solution is required in particular to provide NWDAF analytics exposure to AFs allowed to access the NWDAF and for 3rd Party AFs.

## 6.25 Solution 25: Exposure with bulk subscription and NWDAF collecting data from UDR

### 6.25.1 Description

#### 6.25.1.1 General

This is a solution to Key Issue #3: Interactions with 5GS NFs/AFs for Data Collection.

This solution reuses exposure with bulk subscription as defined in Rel‑15 in TS 23.502 [3] clause 4.15.3.2.4, combined with the feature that NWDAF retrieves collected data from UDR directly via existing Nudr services.

Editor's note: Whether the solution can be translated into a solution with NWDAF doing bulk subscription directly to Event Exposure services from 5GC NFs, or to a solution with NFs reporting directly to NWDAF after NEF subscribed to NF events on behalf of NWDAF, is FFS.

#### 6.25.1.2 Procedures



Figure 6.25.1.2-1: Exposure with bulk subscription and NWDAF collecting data from UDR

1. NEF registers with the NRF for any newly registered NF along with its NF services.

2. When an NF instantiates, it registers itself along with the supported NF services with the NRF.

3. NRF acknowledges the registration.

4. NRF notifies the NEF with the newly registered NF along with the supported NF services.

5. NWDAF 1 subscribes to notification to data modified in the UDR. The events can be changes on existing data, addition of data. The events can be related to specific data subset(s), either for a single UE, group of UE(s) (e.g. identifying a certain type of UEs such as IoT UEs) or any UE.

6. NEF evaluates the NF and NF services supported against the pre-configured events within NEF. Based on that, NEF subscribes with the corresponding NF either for a single UE, group of UE(s) (e.g. identifying a certain type of UEs such as IoT UEs), any UE. NF acknowledges the subscription with the NEF.

7-8. When the event trigger happens, NF notifies the requested information towards the subscribing NEF along with the time stamp. NEF stores the information in the UDR along with the time stamp using either Nudr\_DM\_Create or Nudr\_DM\_Update service operation as appropriate. UDR shall maintain history for information, i.e. UDR shall not erase similar type of information which was stored earlier.

9. If step 5 was performed by NWDAF 1, the update of UDR in previous step triggers a notification towards NWDAF 1.

10. Any NF can request analytics information to NWDAF 1.

11. NWDAF 1 directly interrogates UDR for any relevant data needed to build analytics as requested in step 10. The request can be for specific data, or related to specific data subsets, either for a single UE, group of UE(s) or any UE. NWDAF 1 may also specify a time period in the request, in which case the answer from UDR will contain the requested information for timestamps belonging to the requested time period.

12. Based on data received in step 11b, NWDAF 1 can build analytics and provide them to the requesting NF.

13a-b. NWDAF 2 may also query UDR for some data to provide analytics or predictions to other NFs.

### 6.25.2 Impacts on Existing Nodes and Functionality

UDR stores the history of the various events received, which allows multiple NWDAFs in the PLMN to access the data.

NWDAF is a consumer of Nudr\_DM service (query, subscribe, unsubscribe and notify service operations).

Nudr\_DM service operations enhanced to allow query and subscription for a group of UEs or for any UEs.

Nudr\_DM\_Query service enhanced to add a time or period parameter as key for the query. If no value is provided, regular Rel‑15 behaviour applies, i.e. UDR will provide the last value stored.

### 6.25.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.26 Solution 26: Data Collection using NRF services

### 6.26.1 Description

#### 6.26.1.1 Service definition

This solution addresses the Key Issue #3: "Interactions with 5GS NFs/AFs for Data Collection", and the various use cases which identify the need to obtain load information and sometimes locality (e.g. Use cases #3: "NWDA-Assisted Traffic Handling", #4: "Using NWDA output to customize mobility management"; #5: "NWDA-assisted Determination of Policy"). The NWDAF uses the NRF services (see TS 29.510 [21]) in order to discover the NFs and obtain information about the status of the discovered NFs.

The service operation for NF discovery is Request from the Nnrf\_NFDiscovery service. The service operations for obtaining status information are NFStatusSubscribe and NFStatusNotify, from the Nnrf\_NFManagement service.

The information provided by the NRF to the NWDAF with the Nnrf\_NFDiscovery\_Request and the Nnrf\_NFManagement\_NFStatusNotify operations are the NFProfile and the NFService. Most information elements are static and can be used for all purposes in order to set-up and maintain a consistent network map for data collection. Other dynamic information elements can be used by the NWDAF, depending on use cases, in order to perform estimations:

- NF profile: NF capacity, NF load information, NF status, NF recovery time, NF locality.

- NF service: service capacity, service load information, service status, service recovery time.

### 6.26.2 Impacts on Existing Nodes and Functionality

NFs: Provide the relevant information (NF capacity, NF load information, NF status, NF recovery time, NF locality) to NRF.

NWDAF: No impacts on the existing NWDAF interface.

NRF: No impact.

### 6.26.3 Solution Evaluation

This solution enables retrieving global NF static and dynamic information from all NFs. It can be used as a complement and in conjunction with other Data Collection solutions (e.g. Network Exposure services of the AMF or SMF).

The solution is needed at least in order to obtain a consistent view of network map and status of NFs.

## 6.27 Solution 27: NWDAF assisting Determination of Background Data Transfer Policy

### 6.27.1 Description

This solution is for Key Issue 7: NWDAF assisting Future Background Data Transfer.

As specified in clause 4.16.7 Negotiations for future background data transfer, in TS 23.502 [3], PCF can provide one or more background data transfer (BDT) policies for the future background data transfer based on requests from the 3rd party. Those requests consist of the following parameters: ASP identifier, Data volume per UE, number of UEs, Desired time windows, and optionally network area information.

To determine BDT policy, it is essential to estimate the available data volume in the network. Therefore, it is beneficial that NWDAF outputs the maximum available data volume per UE optionally network area information in consideration of number of UEs as the analytics information. It aims to assist the determination of the BDT policy in the PCF. The PCF can easily judge that the policy request from the 3rd party is acceptable, when the requested data volume is less than the maximum available data volume.

The value of the maximum available data volume per UE depends on not only network condition, but also how many UEs connect to the network. The algorithm to calculate the maximum available data volume should be implemented in the NWDAF. This is not scope of SA WG2 work.

This solution assumes that the operator maps ASP identifier into Internal-Group identifier described in TS 23.501 [2]. In the UDR, the operator can retrieve the UEs belonging to the particular ASP by using Internal-Group identifier.

#### 6.27.1.1 NWDAF Data Collection

Table 6.27.1.1-1 shows the data collected by the NWDAF in a certain interval. To output the maximum available data volume per UE in consideration of how many UEs from the ASP connect in the network, the NWDAF utilizes the following information.

Table 6.27.1.1-1: Data collected by NWDAF

|  |  |  |  |
| --- | --- | --- | --- |
| **Data collected by NWDAF** | **Presence** | **Source** | **Description** |
| Number of UEs | M | UDR | The operator estimates the number of UEs which will be requested by 3rd party in order that the NWDAF calculates the analysis information. |
| ASP identifier | O | UDR | When NWDAF outputs the analysis information per ASP, ASP identifier will be used. |
| UE ID | O | UDR, UDM, PCF | e.g., SUPI, which is used by NWDAF to correlate the information from AMF/OAM. From Internal-Group identifier, UE IDs is listed up per ASP. |
| Network area | O | AMF | The location info for the UE belonging to the particular ASP, e.g. Cell ID or TA ID |
| UE Mobility pattern | O | AMF | mobility pattern of UEs belonging to the particular ASP. |
| Network Performance information per timestamp | M | OAM | See the following editor's note |

Editor´s note: How to align NWDAF input to the solutions to get input data from NF, either via Nxx\_DataCollection or Nxxx\_EventExposure is FFS.

#### 6.27.1.2 NWDAF output

Table 6.27.1.2-1 and 6.21.2.3-2shows the event id and the analytics information output by the NWDAF based on the input described in Table 6.27.1.1-1. This solution assumes that Solution 1 (clause 6.1) or 2 (clause 6.2) will be used as the method of analytics information feedback. The NWDAF outputs the maximum available data volume per UE for the particular ASP based on the total number of UEs in the particular network area at the particular time.

Editor´s note: How to align NWDAF output to the combined solution 1 and 2 is FFS.

Table 6.27.1.2-1: Event Id to provide analytics to enhance BDT functionality

| Event ID | Event Filter | Description |
| --- | --- | --- |
| List of Maximum available data volume per UE | ASP identifier,  Number of UEs,  Network area,  Time, Date | As defined in Table 6.27.2-1 |

Table 6.27.1.2-2: Content of List of Maximum available data volume per UE

|  |  |  |
| --- | --- | --- |
| IE/Group Name | Presence | Description |
| *List of Maximum available data volume per UE* |  |  |
| **> IEs** |  |  |
| >>number of UEs | M | As defined in Table 6.27.2-1 |
| >> ASP identifier | O | As defined in Table 6.27.2-1 |
| >>Maximum available data volume per UE | M | NWDAF calculates this by considering the total number of UEs, time, date, network area and network performance information |
| >>Time | O | As defined in Table 6.27.2-1 |
| >>Date | O | As defined in Table 6.27.2-1 |
| >>Network area | O | As defined in Table 6.27.2-1 |

### 6.27.2 Impact on Existing Nodes and Functionality

NWDAF: NWDAF service is updated from Rel‑15 specification. The existing Nnwdaf interface shall be updated in order to output the parameters in Table 6.1.1.2-2. The NWDAF also needs to have the feature to collect the data described in Table 6.27.1.1-1.

NF service consumer: the impacts are to only support receiving the new analytics requests/responses/notifications.

There is no impact on the negotiation procedures for BDT policy described in clause 4.16.7.2 TS 23.502 [3].

### 6.27.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.28 Solution 28: Exposure to AF for Background Data Transfer

### 6.28.1 Description

This is a solution to Use Case #5 NWDA-assisted Determination of Policy and Key Issue #2: Analytic information exposure to AF. The network condition may be changed, after the background data transfer (BDT) policy is agreed between MNO and 3rd party. We assume that there are the cases where the background data traffic may get discarded for example when the network becomes congested, then other traffic is prioritized rather than the background data traffic.

The NWDAF collects the network performance information, and the location information for each UE belonging to the particular ASP. Then, the NWDAF predicts which UEs will experience network condition, and notifies this analysis information of the PCF.

We propose that the NWDAF notifies the PCF that the UE of an ASP will experience congestion and then PCF determines if the BDT policy should be re-negotiated for the particular ASP. The PCF judges whether this notification should be transferred to the particular AF. When the PCF transfers this, due to this, the AF may try to negotiate with the MNO regarding the BDT policy again. The final decision is up to 3rd party.

#### 6.28.1.1 NWDAF Data Collection

Table 6.28.1.1-1 shows the data collected by the NWDAF in a certain interval. To predict the network performance information of the particular UEs, the NWDAF needs to take the following information into account.

Table 6.28.1.1-1: Data collected by NWDAF

|  |  |  |  |
| --- | --- | --- | --- |
| Information | Presence | Source | Description |
| UE ID | M | AMF, UDR | Could be e.g. SUPI, which is used by NWDAF to correlate the information from AMF |
| ***Location info*** |  |  |  |
| >Timestamp | O | AMF | The timing for the UE |
| >Location Info | O | AMF | The location info for the UE e.g. Cell ID or TA ID |
| UE Mobility pattern | O | AMF | UE mobility pattern |
| ***Network performance info*** |  |  |  |

#### 6.28.1.2 NWDAF output

Table 6.28.1.2-1 and 6.28.1.2-2 show the event id and the analytics information output by the NWDAF based on the input information described in Table 6.28.1.1-1. This solution assumes that Solution 1 (clause 6.1) or 2 (clause 6.2) will be used as the method of analytics information feedback. The NWDAF notifies of the PCF that the BDT policy should be re-negotiated.

Table 6.28.1.2-1: EventId to provide analytics to enhance BDT functionality

| Event ID | Event Filter | Description |
| --- | --- | --- |
| Network Condition list | List of UE identities,  Time,  Date,  Network area | As defined in Table 6.18.1.2-2 |

Table 6.28.1.2-2: Content of Network Condition List

|  |  |  |  |
| --- | --- | --- | --- |
| IE/Group Name | Presence | Range | Semantics description |
| Network Condition list |  | *1* |  |
| **> Network Condition IEs** |  | ***1 to M*** |  |
| >>list of UE IDs | M |  |  |
| >> Expected Moving Trajectory | M | 1 to N | UE´s expected geographical movement (e.g. as described in TS 23.502 [3] clause 14.5.6.3). |
| >>Network Performance Info |  |  | Performance information on the NF where the UE is expected to be according to the expected moving trajectory |

#### 6.28.1.3 PCF output

Table 6.28.1.3-1 and 6.28.1.3-2 show the event id and the output by the PCF based on the input information described in Table 6.28.1.2-1. The solution assumes to use the outcome of Key Issue #2: Analytic information exposure to AF as the interface between AF and PCF.

Table 6.28.1.3-1: PCF requesting the ASP to renegotiate the BDT policy

| Event ID | Event Filter | Description |
| --- | --- | --- |
| BDT policy warning | ASP identifier,  Time, Date, Network area information | PCF requests the ASP to renegotiate the BDT policy, due to potential delays in the transmission of background data. The ASP may trigger a procedure to negotiate the BDT policy with the MNO. |

Table 6.28.1.3-2: Content of List of BDT policy warning

|  |  |  |
| --- | --- | --- |
| IE/Group Name | Presence | Description |
| List of BDT policy warning |  |  |
| **> IEs** |  |  |
| >> ASP identifier | M | Identifier to identify the ASP |
| >>BDT policy reference ID | M | Reference ID of agreed BDT policy |
| >>Time | O | It indicates the time when the background data of the UEs of this ASP may be delayed due to network conditions |
| >>Date | O | It indicates the date when background data of the UEs of this ASP may be delayed due to network conditions |
| >>Network area | O | indicates the network area where background data of the UEs of this ASP may be delayed due to network conditions |
| >>UE ID | O | Indicates the list of UEs whose background data of the UEs of this ASP may be delayed due to network conditions |

### 6.28.2 Impact on Existing Nodes and Functionality

NWDAF: NWDAF service is updated from Rel-15 specification. The existing Nnwdaf interface shall be updated in order to output the parameters in Table 6.28.1.2-1. The NWDAF also needs to have the feature to collect the data described in Table 6.28.1.1-1 from the other NFs.

PCF: PCF is required to support the new EventId to request NW conditions for the and have the logic to judge whether the NW conditions impact the UEs of the ASP and then a notification should be transferred to the particular AF to renegotiate a BDT. Note that the BDT feature in Rel-15 indicates to the ASP on the recommended time or date to deliver traffic to its UEs, and the rating that the MNO will apply if the ASP complies with the BDT policy. With this notification, the MNO tries to ensure that the SLA can be fulfilled with the ASP, so that the ASP needs to renegotiate the BDT policy or expect that the MNO applies a rating for traffic that may experience delays.

AF: the impacts are to support the request to renegotiate a new BDT policy due to network conditions.

### 6.28.3 Solution Evaluation

The NWDAF notifies the analysis information of the PCF in the same manner with the other solutions. The PCF judges whether the NW conditions impacts on the UEs of the ASP and notifies it of the particular AF in the ASP in order to renegotiate a BDT policy. This is the new feature for the PCF. As this situation does not occur frequently, the impact on the PCF is small.

This solution is beneficial for the MNO and ASP, because this solution helps the MNO ensure that the SLA is fulfilled with the ASP. This solution contributes to detect the situation where the quality of the communication for the UE in is bad.

## 6.29 Solution 29: NWDAF assisted MICO mode for mIoT terminals

### 6.29.1 Description

This is a solution to Key Issue #8: performance improvement and supervision of mIoT terminals.

To enhance the mIoT terminal's battery life, the proper configuration of MICO related parameters are required. The AMF decides configuration parameters for MICO mode such as 1) Allow/disallow MICO mode, 2) periodic registration timer, 3) minimal reachable time before entering MICO mode, 4) the buffering duration and size for DL packets. The NWDAF may provide analytic information to AMF by collecting and analyse network, service, management, and user data from multiple entities.

#### 6.29.1.1 MICO mode configuration by AMF

In the current 5GC, AMF may utilize the external parameters provisioned by external AFs such as the behavioural pattern and communication pattern. Table 6.29.1.1.1-1 shows the communication pattern parameters from TS 23.682 [5] , and Table 6.29.1.1-2 shows the behavioural parameters from TR 23.724 [6].

Table 6.29.1.1-1: Communication Pattern Parameters

|  |  |
| --- | --- |
| CP parameter | Description |
| 1) Periodic communication indicator | Identifies whether the UE communicates periodically or not, e.g. only on demand. [optional] |
| 2) Communication duration time | Duration interval time of periodic communication [optional, may be used together with 1)]  Example: 5 minutes |
| 3) Periodic time | Interval Time of periodic communication [optional, may be used together with 1)]  Example: every hour |
| 4) Scheduled communication time | Time zone and Day of the week when the UE is available for communication [optional]  Example: Time: 13:00-20:00, Day: Monday |
| 5) Stationary indication | Identifies whether the UE is stationary or mobile [optional] |
| 6) Battery indication | Identifies power consumption criticality for the UE: if the UE is battery powered with not rechargeable/not replaceable battery, battery powered with rechargeable/replaceable battery, or not battery powered.  [optional] |
| X) Traffic Profile | Identifies the type of data transmission: single packet transmission (UL or DL), dual packet transmission (UL with subsequent DL or DL with subsequent UL), multiple packets transmission.  [optional] |

Table 6.29.1.1-2: The expected UE behavioural parameters

|  |  |
| --- | --- |
| Expected UE Behaviour parameter | Description |
| Expected UE Moving Trajectory | Identifies the UE's expected geographical movement.  Example: A planned path of movement.  [optional] |
| Stationary Indication (see TS 23.682 [5] clause 5.10.1) | Identifies whether the UE is stationary or mobile [optional] |
| Communication Duration Time (see TS 23.682 [5] clause 5.10.1) | Indicates for how long the UE will normally stay in CM-Connected for data transmission.  Example: 5 minutes.  [optional] |
| Periodic Time (see TS 23.682 [5] clause 5.10.1) | Interval Time of periodic communication  Example: every hour.  [optional] |
| Scheduled Communication Time (see TS 23.682 [5] clause 5.10.1) | Time and day of the week when the UE is available for communication.  Example: Time: 13:00-20:00, Day: Monday.  [optional] |
| Battery Indication (see TS 23.682 [5] clause 5.10.1) | Identifies power consumption criticality for the UE: if the UE is battery powered with not rechargeable/not replaceable battery, battery powered with rechargeable/replaceable battery, or not battery powered.  [optional] |
| Scheduled Communication Type | Indicates that the Scheduled Communication Time is Downlink only or Uplink only or Bi-directional [To be used together with Scheduled Communication Time]  Example: <Scheduled Communication Time>, DL only.  [optional] |

These parameters may be highly coupled with the decision making algorithms of AMF for MICO mode. The absence of these parameters could cause poor management of MICO mode, and also, not correctly provisioned parameters can lead not desired MICO mode behaviour for mIoT terminals.

#### 6.29.1.2 NWDAF assisted MICO mode configuration by AMF

The NWDAF may provide the parameters, not provisioned by AFs, by analysing data collected from various sources such as NFs, OAM, AFs, and UEs.

##### 6.29.1.2.1 Input Information for external parameter estimation

The information to be collected for the NWDAF to estimate external parameters, not provisioned by AFs. The data sources can be divided into three groups, 1) network data from the NFs, 2) service data from the AF, and 3) management data from the OAM. The network data from 5GC to collect is defined in Table 6.29.1.2.1-1. Estimating the missing external provisioned parameter is the NWDAF implementation whether it implements regression algorithms, and/or deep learning algorithms. The input of required inputs could be categorized into two groups 1) the inputs for identification of the specific target, 2) the inputs to extract the estimation from the similar past situations or the similar group of targets.

Table 6.29.1.2.1-1: Network Data Collection for the analysis

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| Location Info | AMF or SMF | The location information of the UE. |
| DNN | SMF or PCF | To identify the DNN |
| S-NSSAI | SMF or AMF | To identify the S-NSSAI for the PDU Session which contains the QoS flow |
| UE ID | AMF or SMF | To identify UE |
| Internal Group ID | SMF | To identify UE group if available |
| Traffic usage report | UPF or SMF | To extract traffic characteristics such as flow length, size, and inter packet arrival time. |
| Subscription data | UDR/UDM | To extract the specific UE related information. To extract UE's service contract, UE context, application data, UE specific policy data, and etc. |
| External provisioned parameters | UDR/UDM | To extract the provisioned external parameters such as network configuration parameters, provisioned communication and behavioural patterns. |
| NF resource status | OAM/NRF | The status of assigned resources such as CPU and memory. |
| NF load | OAM/NRF | The load of specific NFs. |
| Service experience | AF | User or service provide feedback on service experience such as MOS. |

NOTE: The correlation of analysed traffic information per DNN, per Slice, per service, per group of UE is dependent on usage of the information. Timestamp can be used to correlate the collected data from different entities.

##### 6.29.1.2.2 Output Information to AMF

When the AMF not have enough parameters for MICO mode configuration, it may request to the NWDAF with event ID and event filter to obtain the necessary parameters. The NWDAF may response to the AMF request with the estimated external parameter. Optionally, the accuracy and confidence interval can be contained on the response. It provides that the confidence on the results of the NWDAF compared to the past observed data. The examples of parameters are described in Table 6.29.1.1-1 and Table 6.29.1.1-2. After receiving the output from the NWDAF, the AMF can use them for the calculation of MICO mode parameters such as:

1) Allow/disallow MICO mode;

2) Periodic registration timer;

3) Minimal reachable time before entering MICO mode;

4) The buffering duration and size for DL packets.

##### 6.29.1.2.3 Procedure



Figure 6.29.1.2.3-1: Procedure to support NWDAF assisted MICO mode configuration

0. The NWDAF may collect and analysed data from various sources described on the clause 6.29.1.2.1.

1. A UE sends registration request with MICO preference.

2. The AMF fetches UE related data from PCF and UDM/UDR according to the registration process according to TS 23.502 [3].

3. The AMF detects the missing external provisioned parameters necessary for deciding MICO mode configuration parameters such as allow/disallow MICO mode, periodic registration timer, minimal reachable time, and the size and duration of the buffer.

4. The AMF sends Nnwdaf\_analtic\_request with the event ID and event filters for the UE.

5. The NWDAF responses to the AMF with the estimated external parameter values with the accuracy or the confidence interval.

(Optional) The accuracy and confidence interval can be provided to indicate the confidence on the results of the NWDAF compared to the past observed data.

6. The AMF calculates the MICO mode related configuration parameters.

7. The AMF response to the UE with the registration accept message that contains the MICO mode indication, the periodic registration timer value. Optionally, the minimum reachable time value can be delivered to the UE and/or the RAN via N2 interface. The minimum reachable timer value may be transformed into the active timer or connected timer value according to the TR 23.724 [6].Before entering MICO mode, the UE (or RAN) may wait a certain amount of time during the minimum reachable time value. The detailed mechanism are described in TR 23.724 [6].

8. UPF and SMF notify DL packets to the AMF.

9. The AMF detects that the UE is not reachable due to MICO mode.

10. The AMF request SMF (or UPF) for the extended buffering with the buffering size and duration according to TR 23.724 [6].

### 6.29.2 Impacts on Existing Nodes and Functionality

NWDAF: The NWDAF should be able collect data from NFs, AFs, and OAM, and should implement internal logic to analyse/estimate the missing external parameters.

AMF: The AMF should have an interface to interact with the NWDAF to obtain the analytic information. Internally, the AMF may implements decision mechanism for MICO mode configuration based on the output of the NWDAF.

### 6.29.3 Solution Evaluation

The Solution 29 addresses Key Issue #8: performance improvement and supervision of mIoT terminals, and provides procedures and parameters to achieve performance enhancement on the battery lifetime of mIoT terminals using NWDAF assistance information.

The solution clarifies effectively the two main requirements identified for the Key Issue:

- What necessary input is required for the NWDAF - considering both operator owned and third party mIoT terminals?

The solution defined a set of Network Data Collection parameters in Table 6.29.1.2.1-1 as input for NWDAF. The parameter set includes such parameters as 'External provisioned parameters' to deal with the information configured at mIoT terminals by operators or third party mIoT service providers.

- What analytical results can be provided by the NWDAF for performance improvement and supervision of mIoT terminals?

The solution defined a set of output parameters in Table 6.29.1.1-1 and Table 6.29.1.1-2 which can be used by AMF to decide MICO mode parameters for mIoT terminals.

The solution resolves a battery lifetime issue for mIoT terminals.

## 6.30 Solution 30: Network Status in a specific geographic area

### 6.30.1 Description

#### 6.30.1.1 General

This is a solution to Key Issue #12: Support of Northbound Network Status Exposure.

The solution allows for one-time or continuous reporting of user plane congestion status (congestion for RAN nodes) in a geographic area.

#### 6.30.1.2 Procedures

##### 6.30.1.2.1 Procedure for one-time or continuous reporting of network status in a geographic area

This procedure is used by an AF to retrieve Network Status Information (NSI) from the network for a specific geographic area. The procedure can be used to request a one-time or continuous reporting of network status, as described in figure 6.30.1.2.1-1.



Figure 6.30.1.2.1-1: Procedure for one-time or continuous reporting of network status in a geographic area

1. When the AF needs to retrieve NSI in a geographic area, the AF sends a Network Status Request (Geographical area, AF Identifier, Duration, Threshold) message to the NEF. Duration indicates the time for which a continuous reporting is requested. The absence of Duration indicates a one-time reporting. Threshold indicates a range at which the AF wishes to be informed of the network status for the continuous reporting. Multiple Threshold values may be included. The AF may indicate whether NSI should be slice specific or not. The NEF assigns a TLTRI that identifies the Network Status Request.

NOTE 1: Geographical area specified by AF could be at cell level (ECGI), TA level or other formats e.g. shapes (e.g. polygons, circles etc.) or civic addresses (e.g. streets, districts etc.) as referenced by OMA Presence API [25].

2. The NEF authorizes the AF request for notifications about potential network issues. The NEF stores AF Identifier, TLTRI, Duration, if present, and Threshold, if present. The NEF assigns an NEF Reference ID.

3. The NEF sends a Network Status Response (TLTRI, cause). The cause value indicates that the network has accepted the request in step 1. Based on operator policies, if either the AF is not authorized to perform this request (e.g. if the SLA does not allow for it) or the AF has exceeded its quota or rate of submitting requests, the cause value indicates the error and the flow stops at this step.

4. The NEF derives a Location Area from the Geographical Area provided by the AF. The Location Area is according to operator configuration either a 3GPP location area (e.g. list of TAs, list of cell(s) etc.). The NEF identifies, based on local configuration or via NRF, the NWDAF(s) responsible for the provided Geographical Area. If multiple NWDAF(s) need to be involved the NEF will have to aggregate the answers.

For one-time reporting:

5. The NEF sends Nnwdaf\_AnalyticsInfo\_Request to NWDAF, indicating request for user plane congestion status in a specific location.

6-7. The NWDAF requests the user plane congestion status for the requested location to OAM, and OAM provides back the requested information. If the NWDAF already has information about the user plane congestion status for the requested location, these steps are omitted.

8. The NWDAF provides the user plane congestion status information to the NEF.

9. The NEF verifies whether the Network Status Request identified via the NEF Reference ID is valid and active and stores the report. After receiving reports from all the involved NWDAF(s) to which step 5 was executed, the NEF derives the NSI for the requested Geographical Area by combining all reports with the same NEF Reference ID in an operator configurable way (governed by SLAs, network topology, usage, etc.).

NOTE 2: Either exact values for congestion status, as reported by NWDAF(s) to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF. The calculation and the reporting of the NSI to the AF depends on operator configuration (SLAs, network topology, usage, etc.).

10. The NEF sends a Network Status Report (TLTRI, NSI) message to the AF.

NOTE 3: Either exact values for congestion status, as reported by NWDAF to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF.

11. The AF sends a Network Status Acknowledgement to the NEF.

For continuous reporting:

12. The NEF sends Nnwdaf\_EventsSubscription\_Subscribe Request to the NWDAF, indicating request for user plane congestion status in a specific location, possibly with thresholds.

13-14. The NWDAF subscribe to OAM to get the user plane congestion status for the requested location, possibly providing congestion level thresholds, and OAM provides back the first report for requested information in the response.

15. The NWDAF provides the user plane congestion status information to the NEF.

16. The NEF verifies whether the Network Status Request identified via the NEF Reference ID is valid and active and stores the report. After receiving reports from all the involved NWDAF(s) to which step 12 was executed, the NEF derives the NSI for the requested Geographical Area by combining all reports with the same NEF Reference ID in an operator configurable way (governed by SLAs, network topology, usage, etc.).

NOTE 4: Either exact values for congestion status, as reported by NWDAF(s) to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF. The calculation and the reporting of the NSI to the AF depends on operator configuration (SLAs, network topology, usage, etc.).

17. The NEF sends a Network Status Report (TLTRI, NSI) message to the AF.

NOTE 5: Either exact values for congestion status, as reported by NWDAF to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF.

18. The AF sends a Network Status Acknowledgement to the NEF.

19. A change of user plane congestion status corresponding to crossing a threshold set by the NWDAF is detected by OAM and notified to NWDAF.

20. The NWDAF provides a notification for the user plane congestion status information to the NEF.

21. The NEF verifies whether the Network Status Request identified via the NEF Reference ID is valid and active and stores the report. After receiving reports from all the involved NWDAF(s) to which step 12 was executed, the NEF derives the NSI for the requested Geographical Area by combining all reports with the same NEF Reference ID in an operator configurable way (governed by SLAs, network topology, usage, etc.).

NOTE 6: Either exact values for congestion status, as reported by NWDAF(s) to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF. The calculation and the reporting of the NSI to the AF depends on operator configuration (SLAs, network topology, usage, etc.).

22. The NEF sends a Network Status Report (TLTRI, NSI) message to the AF.

23. The AF sends a Network Status Acknowledgement to the NEF.

##### 6.30.1.2.2 Cancelling continuous reporting of network status

The procedure as depicted in figure 6.30.1.2.2-1 is used for termination of the continuous reporting of network status. It can be triggered by the AF at any time before the Duration is over or if no Duration was provided. The NEF will trigger this procedure when the Duration is over.



Figure 6. 30.1.2.2-1: Cancelling continuous reporting of network status

1a. The NEF detects that the requested Duration for an ongoing continuous reporting of network status to an AF is over and identifies the corresponding NEF Reference ID.

1b. When the AF needs to terminate an ongoing continuous reporting of network status, the AF sends a Cancel Network Status Request (AF Identifier, TLTRI) message to the NEF.

2b. If the AF requested to terminate an ongoing continuous reporting of network status in step 1b, the NEF authorizes the AF request and identifies the corresponding NEF Reference ID.

3b. If the AF requested to terminate an ongoing continuous reporting of network status in step 1b, the NEF sends a Cancel Network Status Response (Cause) message to the AF.

4. The NEF identifies the NWDAF(s) involved in the continuous reporting represented by the NEF Reference ID. The NEF sends a Nnwdaf\_EventsSubscription\_Unsubscribe Request (subscription correlation ID) to the identified NWDAF(s).

5-6. The NWDAF unsubscribe from OAM for the requested information and the OAM confirms unsubscription.

7. Afterwards, the NWDAF sends Nnwdaf\_EventsSubscription\_Unsubscribe Response to the NEF.

### 6.30.2 Impacts on Existing Nodes and Functionality

The NEF has to implement NetworkStatus API as defined for SCEF.

The Nnwdaf\_AnalyticsInfo\_Request and Nnwdaf\_EventsSubscription\_Subscribe service operations have to be enhanced to allow requests for user plane congestion status for a given location, possibly with indication of thresholds.

The SA WG5 services should allow for retrieving user plane congestion status for a specific location and thresholds.

NOTE: Whether SA WG5 services allow for retrieving user plane congestion status for a specific location should be checked with SA WG5.

### 6.30.3 Solution Evaluation

This solution is the adaptation of T8 NetworkStatus API to NEF and 5GC. It provides the same level of functionality, i.e. for user plane congestion status.

## 6.31 Solution 31: Network Status for a specific UE

### 6.31.1 Description

#### 6.31.1.1 General

This is a solution to Key Issue #12: Support of Northbound Network Status Exposure.

The solution allows for one-time or continuous reporting of user plane congestion status (congestion for RAN nodes) for a specific UE.

#### 6.31.1.2 Procedure for one-time or continuous reporting of network status for a specific UE

This procedure is used by an AF to retrieve Network Status Information (NSI) from the network for a specific UE. The procedure can be used to request a one-time or continuous reporting of network status, as described in figure 6.31.1.2-1.



Figure 6.31.1.2-1: Procedure for one-time or continuous reporting of network status for a specific UE

1. When the AF needs to retrieve NSI for a given UE, the AF sends a Network Status Request (GPSI, AF Identifier, Duration, Threshold) message to the NEF. Duration indicates the time for which a continuous reporting is requested. The absence of Duration indicates a one-time reporting. Threshold indicates a range at which the AF wishes to be informed of the network status for the continuous reporting. Multiple Threshold values may be included. The AF may indicate whether NSI should be slice specific or not. The NEF assigns a TLTRI that identifies the Network Status Request.

2. The NEF authorizes the AF request for notifications about potential network issues. The NEF stores AF Identifier, TLTRI, Duration, if present, and Threshold, if present. The NEF assigns an NEF Reference ID.

3. The NEF sends a Network Status Response (TLTRI, cause). The cause value indicates that the network has accepted the request in step 1. Based on operator policies, if either the AF is not authorized to perform this request (e.g. if the SLA does not allow for it) or the AF has exceeded its quota or rate of submitting requests, the cause value indicates the error and the flow stops at this step.

4. The NEF assigns a NEF Reference ID and identifies, based on local configuration or via NRF, the NWDAF responsible for providing network status for a UE.

For one-time reporting:

5. The NEF sends Nnwdaf\_AnalyticsInfo\_Request to NWDAF, requesting for user plane congestion status for a specific UE id.

6-9. The NWDAF may already know the UE location. If not, the NWDAF checks the UE location by first retrieving the AMF serving the UE (steps 6-7) and then by interrogating the AMF about the UE location.

10-11. The NWDAF requests the user plane congestion status for the UE location to OAM, and OAM provides back the requested information. These steps are omitted if the NWDAF already has the information.

12. The NWDAF provides the user plane congestion status information to the NEF.

13. The NEF verifies whether the Network Status Request identified via the NEF Reference ID is valid and active and stores the report. The NEF derives the NSI for the UE.

NOTE 1: Either exact values for congestion status, as reported by NWDAF(s) to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF. The calculation and the reporting of the NSI to the AF depends on operator configuration (SLAs, network topology, usage, etc.).

14. The NEF sends a Network Status Report (TLTRI, NSI) message to the AF.

NOTE 2: Either exact values for congestion status, as reported by NWDAF to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF.

15. The AF sends a Network Status Acknowledgement to the NEF.

For continuous reporting:

16. The NEF sends Nnwdaf\_EventsSubscription\_Subscribe Request to the NWDAF.

17. The NWDAF determines the UE location, either via internal information or by applying the same steps as steps 6 to 9. The NWDAF then determines an area of interest.

18-19. The NWDAF subscribe to OAM to get the user plane congestion status for the UE location, possibly providing congestion level thresholds, and OAM provides back the first report for requested information in the response.

20. The NWDAF provides the user plane congestion status information to the NEF.

21-22. The NWDAF subscribes to UE mobility event notification in order to be informed when the UE moves out of the area of interest (in order to define a new area of interest and request new information to OAM if the UE moves to a different area).

23. The NEF verifies whether the Network Status Request identified via the NEF Reference ID is valid and active and stores the report. The NEF derives the NSI for the UE.

NOTE 3: Either exact values for congestion status, as reported by NWDAF(s) to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF. The calculation and the reporting of the NSI to the AF depends on operator configuration (SLAs, network topology, usage, etc.).

24. The NEF sends a Network Status Report (TLTRI, NSI) message to the AF.

25. The AF sends a Network Status Acknowledgement to the NEF.

26. A change of user plane congestion status corresponding to crossing a threshold set by the NWDAF is detected by OAM and notified to NWDAF.

27. The NWDAF provides a notification for the user plane congestion status information to the NEF.

28. The NEF verifies whether the Network Status Request identified via the NEF Reference ID is valid and active and stores the report. The NEF derives the NSI for the UE.

NOTE 4: Either exact values for congestion status, as reported by NWDAF(s) to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF. The calculation and the reporting of the NSI to the AF depends on operator configuration (SLAs, network topology, usage, etc.).

29. The NEF sends a Network Status Report (TLTRI, NSI) message to the AF.

NOTE 5: Either exact values for congestion status, as reported by NWDAF to NEF or abstracted values e.g. (High, Medium, Low) can be reported by the NEF to the AF.

30. The AF sends a Network Status Acknowledgement to the NEF.

### 6.31.2 Impacts on Existing Nodes and Functionality

The NEF has to implement NetworkStatus API as defined for SCEF, with the addition of GPSI as an input parameter.

The Nnwdaf\_AnalyticsInfo\_Request and Nnwdaf\_EventsSubscription\_Subscribe service operations have to be enhanced to allow requests for user plane congestion status for a given UE, possibly with indication of thresholds.

The NWDAF has to retrieve UE location information using existing UDM and AMF services.

The SA WG5 services should allow for retrieving user plane congestion status for a specific location and thresholds.

NOTE: Whether SA WG5 services allow for retrieving user plane congestion status for a specific location should be checked with SA WG5.

### 6.31.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

## 6.32 Solution 32: Ensure slice SLA is guaranteed within certain region area

### 6.32.1 Description

This solution is for Key Issue 14: How to ensure that slice SLA is guaranteed.

What slice customer care is, how many subscribers (e.g. 1 millions) can be served by the slice and the Service Experience statistics per application (e.g. average Service MOS 4.0 for Application X for the slice customer) and how many percent (e.g. 90% for Application X) UEs' service experience satisfy per application ID.

A new slice may be created with dedicated 5GC resource e.g., dedicated SMF/UPF/PCF. Usually 5GC resource is enough while NG RAN is the bottleneck, therefore NG-RAN could be initially configured (e.g., by OAM) with reserved/prioritised resources for the new slice, for example give the slice customer 's devices guaranteed access up to X% (e.g. 20%) of the resources of NG-RAN, in particular area. Other existing slices can access to the reserved/prioritised X% resources of NG-RAN when the new slice is not using them.

However, the initially configured X% of the resources of NG-RAN could overfit or underfit the slice customer requirement and may need to be modified based on the slice SLA fulfilment Info from 5GC.

#### 6.32.1.1 Information for slice SLA guarantee

The information for slice SLA guarantee is similar as the information for the support of QoS Profile Provisioning, see clause 6.3.1.1 for details.

#### 6.32.1.2 Procedure to support slice SLA guarantee with certain region area

NSSF should control subscribers to access the new slice gradually in order to avoid/minimize the negative impact on the other existing slice SLA fulfilment (with signed SLA).



Figure 6.32.1.2-1: NWDAF-Assisted Slice SLA guarantee with certain region area

0a. OAM creates a new slice and configures initial resources in RAN (e.g. 20% for the new slice) and in CN allocated to the slice.

0b: OAM notify the initial number of users and Slice SLA requirement e.g. the average Service MOS requirement and/or the requested number of subscribers and/or the requirement of percentage of the user satisfied to NSSF.

1. For the newly created slice, NSSF only allow partial number of subscribers to access the slice.

NOTE 1: NSSF initially allows partial (e.g. 10%) users number to access the slices assuming that users number do not impact the other existing slice SLA, allow NWDAF to train Service MOS Model and then calculate QoE information according to Solution 3: QoS profile Provisioning.

2. The NSSF sends an Analytics request/subscribe (Event ID = Slice statistics Info, Event Filter information = (S-NSSAIs, Tracking Area, Time Window)) to NWDAF by invoking a Nnwdaf\_EventSubscription\_Subscribe.

3. NWDAF monitor QoE per user or group of users and provides the QoE data analytics (e.g. the estimated average Service MOS and/or the number of registered subscribers and/or percentage of the user satisfied) to the NSSF and/or OAM.

4. Based on QoE data analytics provided by NWDAF, NSSF determines whether slice SLA fulfilment (including the new and existing slices with SLA requirement) is overfitting or underfitting or fitting.

5. NSSF determines the allowed number of the user for the slice and notifies slice SLA fulfilment to RAN via AMF or OAM. RAN could take into account slice SLA fulfilment to schedule Resource per slice within the RAN resource configured by OAM.

NOTE 2: NSSF informs RAN is dependent on RAN WG3 and SA WG5 feedback.

6. OAM trains slice resource model with the KPIs from OAM and QoE from NWDAF and then adjust slice resource until slice is stable e.g. RAN resource from 20% (initially configured by OAM when creating slice) to 15%.

7. When slice is stable i.e. the RAN and CN resource configure is fixed, OAM notifies NSSF to update the allowed number of the user for the slice.

### 6.32.2 Impacts on Existing Nodes and Functionality

NWDAF: Provides QoE data analytics to the NSSF.

NSSF:

- Get the QoE data analytics from NWDAF;

- Determines the per slice SLA fulfilment information (per TA) based on the QoE from NWDAF;

- Controls partial number of subscribers to access the slice to avoid negative impact on the existing slice SLA;

- Provides the SLA fulfilment information to RAN via AMF or via OAM.

OAM:

- Notifies NWDAF to do QoE for a slice.

- May obtain information on SLA fulfilment from NSSF and determines the resource usage for RAN and notifies NSSF to update the allowed number of the user for the slice.

AMF:

- Transfers the per slice SLA fulfilment information per TA from NSSF to RAN.

RAN:

- Receives slice SLA fulfilment information from NSSF via AMF or via OAM, which may be taken into account when scheduling radio resource;

### 6.32.3 Solution Evaluation

This solution allows NSSF to determine per slice SLA fulfilment information based on QoE from NWDAF.

With per slice SLA fulfilment information, NSSF could control subscribers to access a new slice gradually in order to avoid/minimize the negative impact on the other existing slice SLA fulfilment.

Optionally, this solution also allows RAN to take into account the per slice SLA fulfilment information to schedule radio resource.

The solution applies effectively in some region areas (may also in certain time period), in which the slice SLA is concerned.

## 6.33 Solution 33: Ensure slice SLA is guaranteed within certain region area

### 6.33.1 Description

#### 6.33.1.1 A Use Case

A possible use case from Key issue#14, is that an SLA has been agreed between MNO and a customer that covers the following KPIs:

- Number of users (group of users) per slice and even per TA or other larger defined area.

- Different fulfilment for different applications such as:

- 80% of users running application 1 shall have a at least QoE\_1 or higher (where QoE\_1 might be an agreed MOS value).

- 90% of users running application 2 shall have a at least QoE\_2 or higher (where QoE\_2 might be an agreed MOS value).

- etc.

Here it is assumed that a specific slice is going to be used for this customer.

#### 6.33.1.2 Providing Analytics to OAM to assist SLA monitoring

Assume that the MNO would like to assure that it can support the SLA by allocating a new slice. One way to do this is to set up resources in RAN and in CN allocated to the slice.

One way to proceed is to start letting the customer populate the slice with users by introducing an initial number of users and add more and more UEs into the network and let them start using the applications. Each user is allocated an initial QoS Flow, either per application if multiple QoS Flows are to be used or one general QoS Flow. The QoS profiles shall reflect the requirements of the services mapped on the QoS Flows as well as desired packet treatment at congestion.

For a newly created slice, NSSF may only allow partial number of subscribers to access the slice. This admission control of the UEs allows to increase the maximum number of users belonging to the group in a controlled manner. OAM is aware of the number of users in the slice and add more and more when it sees it feasible. NSSF receives admission control information per slice and TA, which may be retrieved directly in OAM. If OAM does not have information per TA, such counter may be added in SA WG5.

NWDAF monitor QoE per user in the allocated slice. But it also monitors all other groups of user's QoE that it has received a similar KPI for. NWDAF calculates continuously the fulfilment per application in the groups. OAM may subscribe to QoE info from NWDAF.

For users with no agreements, the solution can be pure dimensioning, by letting for instance the large ordinary MBB slice have a minimum amount of resources. Or the proposed solution may also be applicable for slices without an associated SLA.

OAM then uses this info and other info important for reaching the slice KPIs to optimize the resources in RAN and in CN if needed. For optimization done by OAM no further description is done in here in this document and is left for other groups in 3GPP, such as SA WG5 and considered outside of the scope of SA WG2. Only an overview of possible steps are added below for clarity of the overall solution.

NOTE: OAM for RAN, CN and Transport Network most certainly have a better view on what optimizations can be done compared to letting SA WG2 decide upon this. Also RAN has a very good view on how UEs belonging to a certain slice is being supported by different RAN resources from a characteristics point of view.

The convergence time shall be up to implementation, since it may depend on e.g. how the SLA is defined, the statistics involved and how active users are. Also, since the SLA is a statistical measure it needs some time to converge. A predictive model in Management Data Analytics Service (MDAS) in OAM may be used to act proactively. In conclusion the convergence time is dependent on how fast the SLA can be evaluated after corrective actions has been taken.

**Flow Diagram.**



Figure 6.33.1.2-1

The steps are described here:

0. The admission control info per slice and TA or other larger defined area is forwarded from OAM to NSSF. NWDAF receives only the KPI used for QoE monitoring.

1. NSSF may do admission control by accepting or not accepting more users to the slice. This acceptance may be done per TA. At each registration AMF forwards a slice request to NSSF. This is done by either local configuration, or UE request a general slice (not available in AMF) which forces AMF to ask NSSF.

2. OAM subscribes to QoE information per user belonging to specific slices with KPIs. And optionally to other/all users in general slices such as MBB, IoT from NWDAF.

3. Users register and use the slice.

4. NWDAF monitor QoE per user.

5. NWDAF notify continuously the QoE and slice ID per user. The NWDAF may add the gNB used per user.

6. Some example steps OAM might take here are as follows:

6.1 OAM continuously evaluate input, including the info received from NWDAF to evaluate towards the KPIs.

6.2 Optionally the analytics function in Management Data Analytics Service (MDAS) has a QoE prediction model and uses the input to update it.

6.3 Optionally, the predictive model is used for SLA evaluation, which will allow proactive measures.

6.4 If the SLA is breached OAM determines the cause and triggers appropriate actions in RAN, Transport Network and/or CN domain to remedy the breach.

7. OAM notify new admission control info per slice and TA if number of users per slice and TA has been breached.

To support the SLA admission control in NSSF may be done by controlling number of users in slice and even in TAs or other larger defined areas, as described in the flow diagram above. NSSF receives information from OAM to take decision on when users in a specific slice and TA may not access the slice.

Admission could be done on registered users in NSSF dependent on SLA. Thus, it could also be used to gradually ramp up the number of allowed registered users to the contractual level of an SLA if desired.

NOTE 1: There is an option that RAN continuously act upon the fast dynamicity within the slice inside the RAN domain, to assure that the slice KPIs are not being underfitting. RAN has knowledge of what UEs belonging to a slice and what resources they are using and the relation to other UEs. It should be considered that there is existing mechanism defined in RAN to monitor a slice. But this is left for other standardizations group, such as SA WG5.

NOTE 2: This solution needs co-operation between standardization groups as described in the key issue #14

## 6.34 Solution 34: NWDAF collecting analytic information directly from UE

### 6.34.1 Description

#### 6.34.1.1 General

This solution addresses key issue X and addresses the following:

- What analytic data can be provided by the UE directly to the NWDAF.

- What analytic information can the NWDAF derive based on the information provided by the UE.

- How other NFs can use the NWDAF derived UE analytic information.

The solutions in the FS\_eNA TR specify that any UE-related analytic information is collected by the NWDAF indirectly, i.e., either from the AMF for any UE location related information, or from the RAN based on information collected by OAM analytic functions.

A solution is proposed for the UE to track its location when in IDLE mode and report to the NWDAF. The NWDAF uses the location information provided "indirectly" with the location information provided by the UE to derive statistical data with better confidence.

#### 6.34.1.2 UE sending IDLE related location information directly to the NWDAF

Examples of usage data provided by the UE can be the following:

- Report duration: 10:35am - 11:35pm.

- Visited cells: (Cell-1, entry time, exit time), (Cell-2, entry time, exit time), etc.

- Location: (X1, Y1, Z1 @ 10:36am), (X2, Y2, Z2 @ 11:14am).

The UE does not send usage data in real-time. Rather, such data is internally collected in the UE and is sent to the NWDAF in batches (e.g. every X hours). It is up to the UE implementation how often the UE provides such usage data.

#### 6.34.1.3 Usage of IDLE related location information by other NFs

The NWDAF uses the UE location information from the AMF (location information in connected State) and directly from the UE (location information in IDLE) to derive more accurate statistical prediction of the UE location.

The NWDAF can provide mobility prediction based on combining UE location information reported from the AMF (when UE is in CONNECTED state) and the UE (when the UE is in IDLE state).

Editor's note: The usage of the NWDAF output that includes mobility predictions based on the UE historical location information requires further study

#### 6.34.1.4 Method to provide IDLE related location information to the NWDAF

The UE can provide the "Location information in IDLE mode" by using a control plane procedure as specified in Solution 16 or via a user plane procedure as specified in Solution 15 in TR 23.791.

### 6.34.2 Impacts on Existing Nodes and Functionality

Editor's note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.34.3 Solution Evaluation

Editor's note: Use this clause for evaluation at solution level.

# 7 Overall Evaluation

## 7.1 Key Issue 1& Key Issue 2

For analytic services, two types of solutions are described in the TR 23.791:

- Generic solutions, which apply to multiple use cases: Solutions #1 and #9.

- Solutions specific to use cases: Solution #3, #4, #5, #7, #8, #10, #11, #18, #20, #21, #22, #23, #27, #29. These solutions might potentially reuse (refer to) the generic solutions.

The services provided by the generic solutions can be further classified into three levels of analytics:

- **Statistics of the past**, which may be considered simply as a report, but also as a "vanilla" estimation of the future in general, with the underlying paradigm that "future" shall be very similar to "past" (therefore no need to refine the prediction).

- **Predictions**, which are a step beyond the previous, because trend analysis may determine evolving drivers for the future which cannot be detected by basic statistics. But in this step, a major part of the decision-making process remains in the consumer NF.

- **Recommendations**, where the NF delegates some calculation of optimal parameters to the NWDAF, but still remains responsible for the final choices.

Solution #1 provides statistics and predictions, while Solution #9 provides recommendations.

Solution #9 (Recommendations produced by NWDAF) is a solution that has been evaluated to possibly only cover a limited number of key issues/use cases, which are a subset of what can be solved by analytics. It is not recommended for Release 16, because it requires additional study. It is desirable that this Solution be reconsidered following the results obtained on the implementations of Release 16, in order to examine its relevancy on stronger use case basis.

For metadata exposure, Solution #13 supports the metadata exposure to NFs by introducing new service operation on NWDAF, and Solution #19 provides the metadata to NFs via NRF as a part of NF profile.

## 7.2 Key Issue 2: Analytic Information Exposure to AF

Solution 24 supports how to expose analytics information to an AF directly from NWDAF or via NEF.

Regarding how to expose metadata information to an AF in untrusted domain, the exposure needs to be made via NEF. Solution 13 supports the metadata exposure to NFs by introducing new service operation on NWDAF while Solution 19 provides the metadata to NFs via NRF as part of NF profile. It is considered that Solution 19 can be used for the NEF to retrieve the NWDAF metadata. With this, the NEF service and the structure for metadata are needed to be defined.

## 7.3 Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection

For Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection, there are four solutions, i.e.:

- Solution 6: Data Collection from NFs/AFs using a new service, i.e. introduce new services to collect massive pre-computed metrics over populations of UEs or groups of information (e.g., application ID), per spatial and temporal dimensions (e.g., per region of a network slice for a period of time); as well as for data collection from AF.

- Solution 14: Data Collection from NFs/AF via NF Event Exposure services, i.e. reuse the R15 NF event exposure services to collect not only individual UE data but also populations of UEs or groups of information (e.g., application ID), per spatial and temporal dimensions (e.g., per region of a network slice for a period of time) with following extensions:

- Extensions on Data Collection via Event Exposure from AF directly and from 3rd Party AFs via the NEF.

- Extensions on Exposure Framework (on Object Target and Event Filter Information, Collectable Data Item (CDI)) in order to collect massive pre-computed metrics over large populations (e.g. groups of UE, applications IDs).

- Solution 25: Exposure with bulk subscription and NWDAF collecting data from UDR, i.e. to reuse bulk subscription service of NEF defined in R15 that supports any NF to subscribe event exposure for multiple UEs; needs to be extended to collect data from AFs, and to be able to collect groups of information (e.g., application ID). This solution is a special case of EventSubscription. Some drawbacks are seen with this solution:

1) It is a bulk subscription meaning all data is stored, even data that is not of interest for analytics in NWDAF.

2) UDR must be dimensioned for long term data lake storing of massive amount of data.

3) Signalling towards UDR will be heavy for Data collection.

4) Signalling towards UDR will be heavy for Data retrieval from NWDAF.

With the drawbacks mentioned above the method in this solution shall not be the primary way to retrieve NF related data.

- Solution 26: Data Collection using NRF services, i.e. reuses NRF services defined in R15 for the NWDAF to discover NFs and associated NF profiles.

## 7.4 Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure

For Key Issue 4 Interactions with OAM for Data Collection and Data Analytics Exposure, there is only one solution:

- Solution 12: Data Collection from OAM using the existing SA WG5 services i.e. reuse the already defined SA WG5 services to collect data from OAM.

## 7.5 Key Issue 5: NWDAF-Assisted QoS Profile Provisioning

Solution 3 supports NWDAF-Assisted QoS Profile Provisioning for the non-standardized 5QI.

## 7.6 Key Issue 6: NWDAF assisting traffic routing

Table 7.6-1

|  |  |  |
| --- | --- | --- |
| Criteria | Solution #11 | Solution #20 |
| UPF discovery and selection by SMF | NWDAF input data for traffic analysis are addressed.  Time information and UPF load information is provided to SMF. | Evolves UPF discovery and selection by SMF as defined in Rel-15 to take predictions on UPF load and UE location into account.  Maintains existing configuration in SMF, no extra operational cost.  Step 1 and 2 are better directly requested by and responded to SMF |
| Compliance with solution# to KI#1 | Compliant, reuses solution#1 | Compliant, reuses solution#1 |

## 7.7 Void

## 7.8 Key Issue 8: Performance improvement and supervision of mIoT terminals

### 7.8.1 General mode for mIoT terminals

There are two alternative solutions on how misused or hijacked UEs are recognized by using data analysis.

NOTE: The misused or hijacked UEs are UEs in which there are malicious applications running or UEs which have been stolen.

Solution 8 requires AMF/SMF to identify IoT UEs with unexpected behaviour first by comparing runtime UE behaviours with expected UE behaviours provided by UDM or NWDAF and optionally to take actions locally. The NWDAF will make further analysis on the result provided by the AMF/SMF to determine the misused or hijacked UEs. The analytic result from the NWDAF can be sent to 5G NFs or AF to trigger corresponding actions.

Solution 21 relies on the NWDAF to identify the misused or hijacked UEs by itself. The NWDAF needs to collect runtime data of IoT UEs from the 5GC and compare the UE runtime behaviour with expected UE behaviours which may be obtained from AF or UDM, or learned by the NWDAF itself. The analytic result from the NWDAF is also sent to 5G NFs or AF to trigger corresponding actions.

### 7.8.2 MICO mode for mIoT terminals

Solution 29 NWDAF assisted MICO mode for mIoT terminals addresses performance enhancement on the battery lifetime of mIoT terminals. The solution provides necessary procedures and parameters for NWDAF to obtain required input data from NFs and/or AFs and deliver output data to an AMF. Based on the solution, the AMF can use the NWDAF assisted analytic information to decide MICO mode parameters values for mIoT terminals. The solution 29 can be selected as base for the normative work in Release 16.

## 7.9 Key Issue 9: Customizing mobility management based on NWDAF output

There are 6 different solutions described for this key issue.

### 7.9.1 Registration area allocation

Solution 4, 7 and 23 relate to optimizing registration areas:

- Solution 4 "Optimizing registration area management and service restriction areas adjustment based on NWDAF output": this solution relies on the AMF using service area restrictions from PCF and statistics and/or predictions on UE mobility from NWDAF to derive registrations areas.

- Solution 7 "Customizing mobility management based on NWDAF output": some aspects of this solution are more related to the framework for eNA, such as the NWDAF registering the supported Event-IDs into NRF (e.g. "UE expected geographical movement") or NWDAF possibly being co-located with AMF. There is no specific AMF behaviour specified in this procedure.

- Solution 23 "AMF using NWDAF outputs to optimize UE mobility procedures": The Nnwdaf\_EventsSubscription and Nnwdaf\_AnalyticsInfo services need to be enhanced to allow provisioning of analytics or predictions or both for mobility information for a specific UE. Only AMF derives registration areas and paging areas for the UE based on inputs provided by NWDAF.

### 7.9.2 Mobility restriction area handling

Solution 4 "Optimizing registration area management based on NWDAF output": this solution supports PCF using statistics and/or predictions on UE mobility from NWDAF to optimize service area restrictions adjustment.

### 7.9.3 Paging handling

Solution 5 "Optimization based on paging failure prediction from NWDAF": for this solution, a couple of issues still need to be addressed or discussed. Some aspects of the proposal are related to RAN paging and would need to be discussed by RAN WGs. Regarding CN paging failures, whether aspects related to paging strategy need to be standardized between the AMF and the NWDAF is unclear, e.g. the AMF reporting the paging areas to the NWDAF.

### 7.9.4 Handover decisions

Solution 10 "NWDAF assisted Handover decision": in this solution, the 5GC can use the NWDAF output to predict the UE mobility and indicate the predicted UE location to the NG-RAN node serving the UE. Then the NG-RAN node can select a more suitable target cell during the handover or redirection.

This solution is not under SA WG2 remit, rather it would require analysis from RAN WGs.

### 7.9.5 Connection management

Solution 22 "Optimizing connection management based on NWDAF output": this solution allows the AMF to optimize connection management for a UE based on communication pattern information and mobility information received from NWDAF.

## 7.10 Void

## 7.11 Void

## 7.12 Key Issue 12: Support of Northbound Network Status Exposure

Solution 30 allows to expose Network Status related to user plane congestion to an AF for a specific geographic area. The solution is an adaptation of SCEF procedure to expose Network Status (as defined in TS 23.682 [5]).

Solution 31 allows to expose Network Status related to user plane congestion to an AF for a specific UE.

## 7.13 Void

## 7.14 Key Issue 14: How to ensure that slice SLA is guaranteed

There are two different solutions described for this key issue, that are analysed below, using the comparation criteria in table 7.14-1, i.e. impacts on 5GS, amount of signalling, cost, deployment aspects, configuration effort.

Table 7.14-1

|  |  |  |
| --- | --- | --- |
| Comparation criteria | Solution#32 | Solution#33 |
| Impacts in the existing Radio Resource Management in OAM  (NOTE 1) | According to SA WG5 TS, RAN may be OAM configured with RRM policies per slice (see TS 28.541 [27], clause 4.3.36.1, Annex C). | Existing RRM policies are used (According to SA WG5 TS, RAN may be OAM configured with RRM policies per slice (see TS 28.541 [27], clause 4.3.36.1 and Annex C), unless SA WG5 decides to extend them.  (RAN) OAM can receive QoS notifications and react accordingly.  Actually it is up to OAM to determine where the issue is (RAN, transport, core) and to react accordingly. |
| Impacts in the existing NG-RAN RRM  (NOTE 2) | This solution impacts RAN RRM (new message 5a : "NWDAF notifies the new slice QoE fulfilment to RAN within the problematic area via AMF. RAN within the problematic area could take into account the new slice QoE fulfilment to schedule Resource per slice within the RAN resource configured by OAM)": This impacts RAN RRM. | NG-RAN monitors if RRM policies are fulfilled, and then take actions.  Analysis: No impacts on NG-RAN, besides OAM RRM policy configuration. |
| Impacts on 5GS NF | SLA monitoring functionality is placed in OAM with NWDAF assistance on QoE in the slice.  NSSF, AMF, and NG-RAN are impacted to be able to transfer the indication that QoE is not fulfilled and then take actions in NG-RAN.  NSSF role is extended to do admission control while this baseline feature was not defined in Rel-15; It may be needed to first define whether (and if yes how) to support admission control on a per slice basis (this requires that the entity doing admission control knows when slice resource are used and are no more used). | NSSF role is extended to do admission control while this baseline feature was not defined in Rel-15; It may be needed to first define whether (and if yes how) to support admission control on a per slice basis (this requires that the entity doing admission control knows when slice resource are used and are no more used). |
| Amount of signalling to NG-RAN that is assumed to be a bottleneck) | Signalling from AMF to RAN on QoE fulfilment cause extra signalling. | Signalling from NWDAF to OAM to provide QoE in the slice.  Analysis: No unnecessary signalling from AMF to NG-RAN. |
| Cost | **Analysis:** There are additional cost on the new requirements of NSSF, AMF and NG-RAN. However, the NSSF, AMF, NWDAF are expected to be deployed in a central way. The benefit is achieved in view of fast parameter convergence and more efficient radio resource usage. | Cost would be estimated by SA WG5, NWDAF service may need some extensions as well as defining SLA monitoring functionality.  **Analysis:** The cost is not clear yet since the SA WG5 solution is under development in TR 28.805 [26]. |
| Deployment issues | SA5 defined e2e SLA monitoring as defined in TR 28.805 [26] and QoE monitoring defined in this TR.  Analysis: The solution in this TR can be a compliment solution as for the OAM solution to be defined by SA WG5. | OAM solution only, implies that each NF complies with OAM SA5 TSs.  Solution feasibility is unclear since the NWDAF monitor QoE per user and the granularity of notification from NWDAF to OAM is FFS.  **Analysis:** 5GS implements OAM TSs for SLA monitoring. The TR 28.805 [26] is still under progress and lack of complete solutions yet. |
| NOTE 1: Impacts are only estimated since the RRM functionality is currently defined at SA WG5.  NOTE 2: Impacts are only estimated since NG-RAN is defined by RAN WGs.  NOTE 3: Proprietary OAM solutions are not considered. | | |

# 8 Conclusions

## 8.0 Conclusions on the framework for analytics

The analytics framework in Rel-16 shall be based on the following principles:

- Evolves the Network Data Analytics architecture and the NWDAF NF defined in TS 23.501 [2] and Nnwdaf services defined in TS 23.502 [3].

- Complies with the specification of NF framework defined in TS 23.501 [2].

- NWDAF discovery functionality is required.

- NWDAF profile and Nnwdaf\_EventExposure and Nnwdaf\_Analytics service include service authorization information to indicate the NF type, the NF realms which are allowed to consume each NWDAF service.

- Multiple instances of NWDAF may exist. Each NWDAF instance informs the NRF of the list of NF services that it supports.

NOTE: The relation with eSBA SID has not been investigated in this TR, any potential impact from eSBA will be handled during the normative phase.

## 8.1 Key Issue 1: Analytic Information Exposure to 5GS NF

On how a consumer request or subscribes to analytics, solution 1 is selected as basis for the normative work.

On how analytics information is provided to consumers, solution 1 is selected as basis for the normative work.

On how metadata is retrieved by each consumer of analytics, solution 19 is selected as basis for the normative work when NF discovers NWDAF via NRF, otherwise local configuration in each NF applies.

## 8.2 Key Issue 2: Analytic Information Exposure to AF

Regarding how to expose analytics information to AF, Solution 24 is selected for the normative work.

Regarding how to expose metadata information to an AF in untrusted domain:

- NEF should provide a service to expose NWDAF metadata to the AF,

- The NEF service and the structure for metadata will be defined in the normative phase,

- The NEF shall retrieve the NWDAF metadata using Solution 19.

## 8.3 Key Issue 3: Interactions with 5GS NFs/AFs for Data Collection

Regarding how to collect data from 5GC NFs/AFs to NWDAF, Solution 14 is selected for the normative phase and Solution 26 is selected from the aspects of NRF services as complementary solution.

## 8.4 Key Issue 4: Interactions with OAM for Data Collection and Data Analytics Exposure

Regarding how to collect data from OAM to NWDAF, Solution 12 is selected as the basis for the normative work.

## 8.5 Key Issue 5: NWDAF-Assisted QoS Profile Provisioning

Solution 3 is proposed to be selected for KI 5 in the normative work.

## 8.6 Key issue 6: NWDAF assisting traffic routing

To enable NWDAF assistance to traffic routing, both UPF selection and AF influence on traffic routing, it is recommended to select solution 20 as the basis for normative work and the list of input parameters for analytics listed in Table 6.11.1.2.1-1: Collecting Data for analysing traffic characteristics in solution 11.

## 8.7 Key Issue 7: NWDAF assisting Future Background Data Transfer

On what type of analytics information for Future Background Data Transfer could be provided by NWDAF for the PCF to determine the policy of future background data transfer, solution 18 is selected as a basis for normative work.

On what information does NWDAF need as input to determine such analytics information, solution 18 is selected as a basis for normative work.

In addition, solution 28 is selected as basis for normative work. The information flow for BDT described in solution 27 is selected for normative work.

## 8.8 Key Issue 8: Performance improvement and supervision of mIoT terminals

### 8.8.1 General mode for mIoT terminals

It is concluded that Solution 8 and Solution 21 are used as the basis for normative work on how misused or hijacked UEs are recognized.

NOTE: The misused or hijacked UEs are UEs in which there are malicious applications running or UEs which have been stolen.

### 8.8.2 MICO model for mIoT terminals

For the Key Issue 8: performance improvement and supervision of mIoT terminals,

The solution 29 is selected as the basis for normative work on NWDAF assisted performance enhancement for the battery lifetime management of mIoT terminals.

## 8.9 Key Issue 9: Customizing mobility management based on NWDAF output

For optimizing registration area allocation, solution 23 and solution 4 are selected as basis for further normative work. The NWDAF service operations should be enhanced to allow for new Event-ID providing statistics or predictions on UE geographical movement, e.g. as described in solution 7. The AMF behaviour based on such statistics or predictions shall be left to implementation.

For optimizing mobility restriction area handling, solution 4 is selected as basis for further normative work.

For optimizing connection management for the UE, NWDAF service operations should be enhanced to allow for providing statistics or predictions on communication patterns for the UE, as described in solution 22.

For optimizing paging or handover decisions, no specific normative work is required in SA WG2.

## 8.10 Void

## 8.11 Void

## 8.12 Key Issue 12: Support of Northbound Network Status Exposure

For exposure of Network Status to Northbound entities, procedures developed during normative phase will allow exposure of user plane congestion related information and will be based on:

- solution 30 for Network Status in a specific geographic area; and

- solution 31 for Network Status for a specific UE.

## 8.13 Key Issue 13: UE Driven Analytics

It has been concluded that it would be useful for the NWDAF to collect the "UE Out of Coverage Entries" parameter. The "UE Out of Coverage Entries" parameter is described in solution 16. How the NWDAF collects the "UE Out of Coverage Entries" parameter has not been concluded.

Further study is required before SA WG2 can conclude on a complete list of what UE Data Analytics parameters would be useful for the NWDAF and how those parameters should be collect by the NWDAF.

There will be no normative work in Rel-16 on this topic.

## 8.14 Void

## 8.14A Key Issue 14: How to ensure that slice SLA is guaranteed

The following conclusions are agreed for normative work related to Key Issue 14:

- NWDAF provides analytics for slice QoE.

- The slice QoE analytics granularity when consumed by OAM will be per slice ID per user.

- SLA fulfilment evaluation is performed by OAM as indicated in TR 28.805 [26].

Any slice admission control mechanism in 5GC, based on NWDAF analytics and OAM triggers, requires further SA2 investigation and will not be progressed in Rel-16.

No interaction between 5GC and NG-RAN on slice SLA or slice QoE will be progressed in Rel-16.

Annex A:  
Examples on Network Data Analytics Feedback

# A.1 Examples for EventID

The following are examples of EventIDs and EventFilters. The list of EventIds and Event Filters are described in each solution for the different key issues.

Table A.1-1: Examples for EventID

| Event ID | Event Filter ( | Description (examples of patterns) |
| --- | --- | --- |
| UE Behavior parameters  Expected Moving Trajectory | List of UE identities, Time, Date | UE´s expected geographical movement  (e.g. as described in TS 23.502 [3] clause 14.5.6.3). |
| UE Behavior parameters  Communication pattern |  | UE expected communication  (e.g. communication of low latency applications at a given time and date, or |
|  | Time and date when UE does not have any communication) |
| NW performance Pattern | NW area,  Time, Date | NW expected performance pattern  (e.g. Estimated load in a network area at a given time and date). |

# A.2 Examples of Event Filter

Table A.2-1: Example of Event Filter

|  |  |
| --- | --- |
| Example of Event Filter Information | Value assertion (examples) |
| S-NSSAI | = "MBB" |
| NF, NF set, NF region | = "all NFs" |
| TAI, Cell ID, geographical area, area type (rural/urban) | = "Cell-3" |
| DNN, Application Identifier | = "MMS" |

# A.3 Example of content of Subscription/Request

Table A.3-1 describes a simplified example of content of Subscription/Request focusing on UEs-groups= "UE-group1, UE-group2, UE-group3", SliceID= "SliceA", AfID="App1", and denotation of explicit list "per UE groups".

Table A.3-1: Simplified example of content of Subscription/Request

|  |  |  |  |
| --- | --- | --- | --- |
| Event Parameter value | Target of Event Reporting | Event Filtering Information | Denotation of Explicit Lists |
| Number of registrations (N) | "UE-group1"; "UE-group2"; "UE-group3" | Slice ID = "SliceA"  AFId = "App1" | DOE="per UE-group" |
| Service satisfaction level (R) |

# A.4 Example of content of notification/response

Table A.4-1 describes an example of content of Notification/Response focusing.

Table A.4-1: Example of content of notification/response

|  |  |
| --- | --- |
| analytics for N-SSAI="SliceA" and AFId= "App1" | Statistics in the case of explicit list |
| Number of registrations (N) | <UE-group1, N=1973>; <UE-group2, N=29382>; <UE-group3, N=293> |
| Service satisfaction level (R) | <UE-group1, R=90%>; <UE-group2, R=95%>; <UE-group3, R=85%> |

Annex B:  
Examples of usage of the CDI concept defined in solution 14

This clause contains examples of usage of the CDI concept defined in solution 14: CDI examples described in this clause are not meant to be endorsed as part of this study as only endorsed solutions from this TR are meant to define CDI(s) to be specified in the normative WID output of this study.

EXAMPLE 1: In this situation, the consumer NF requests two counters (registration counter, QCN counter) for 3 TAI, and expresses an explicit list per TAI.

Table 6.14.1.3-2 - Example of Event IDs with explicitly listed CDIs

|  |  |  |
| --- | --- | --- |
| Event ID | CDI associated with Event ID | |
| Targeted Object | Event Filter Information |
| #1 | TAI | < TAI 1; "registration counter" a for TAI 1>, < TAI 2; "registration counter" a for TAI 2>,< TAI 3; "registration counter" a for TAI 3>,etc.. |
| #2 | TAI | < TAI 1; "QCN counter" b for TAI 1>, < TAI 2; "QCN counter" b for TAI 2>,< TAI 3; "QCN counter" b for TAI 3>,etc.. |

EXAMPLE 2: The NWDAF wants to know the number of UE within a group (IMSI-group-X = IMSI-1, IMSI-2, IMSI-3, IMSI-4) that have a PDU Session to a list of DNN (DNN=toto or tata) and that are located in set of Presence Reporting Area (PRA range 1-3). NWDAF does not need a counter per DNN and PRA but a counter per PRA.

NWDAF subscribes to Event Id = Location information counting, target = IMSI-group-X, Filter 1 = [(PRA range 1-3) + reporting tag = Explicit], Filter 2 = [DNN=toto or tata].

This relates to a CDI type = number-of-UE-in-PRA-with-set-of-DNN;

The NF reports 3 CDI(s) with the same type. Each CDI is associated with a different assertion (PRA value) and one CDI value e.g. (number-of-UE-in-PRA-with-set-of-DNN, PRA=1, value =0), (number-of-UE-in-PRA-with-set-of-DNN, PRA=2, value =3), (number-of-UE-in-PRA-with-set-of-DNN, PRA=2, value =1).

Annex C:  
RRMPolicyRatio2 (extract from TS 28.541 [27])

# C.1 Definition

This <<DataType>> represents the properties of RRMPolicyRatio2. The RRM policy setting the ratios for the split of the Radio resources between the supported S-NSSA Lists. in average over time. RRMPolicyRation2 is a list and each item of the list has seven attributes. Four of them specify the percentage of radio resources to be allocated to the corresponding sNSSAIList. The attribute rRMPolicyMaxRatio defines the maximum resource limitation for the sNSSAIList. The attribute rRMPolicyMarginMaxRatio defines the safety margin that allows for maximum float limit use with other sNSSAIs borrowing free resources while keeping safety margin to ensure that resources are available for quota specific sNSSAIList. The attribute rRMPolicyMinRatio defines the minimum resource limitation for the sNSSAIList. The attribute rRMPolicyMarginMinRatio defines the safety margin that allows for minimum float limit use with other sNSSAIs borrowing free resources while keeping safety margin to ensure that resources are available for quota specific sNSSAIList.

Annex D:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-09 | SP#81 | SP-180741 | - | - | - | MCC editorial update for presentation to TSG SA#81 for information | 1.0.0 |
| 2018-12 | SP#82 | SP-181108 | - | - | - | MCC editorial update for presentation to TSG SA#82 for approval | 2.0.0 |
| 2018-12 | SP#82 | - | - | - | - | MCC editorial update for publication after approval at TSG SA#82 (Release 16) | 16.0.0 |
| 2019-03 | SP#83 | SP-190176 | 0001 | 5 | B | Evaluation for KI#14 (How to ensure that slice SLA is guaranteed) | 16.1.0 |
| 2019-03 | SP#83 | SP-190176 | 0002 | 2 | B | Updates and removal of Editor's Notes for solution 33 | 16.1.0 |
| 2019-06 | SP#84 | SP-190432 | 0009 | - | F | Removal of Editor's Note for solution 33 | 16.2.0 |
| 2019-06 | SP#84 | SP-190432 | 0014 | 4 | B | Conclusion for Key Issue 14 | 16.2.0 |