ATIS-1000103.v002

Invocation/Revocation of the National Security / Emergency Preparedness (NS/EP) Data Transport Service for the 5G System (5GS)

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-1000103.v002, *Invocation/Revocation of the National Security / Emergency Preparedness (NS/EP) Data Transport Service for the 5G System (5GS)*

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000103.v002

ATIS Technical Report on

Invocation/Revocation of the National Security / Emergency Preparedness (NS/EP) Data Transport Service for the 5G System (5GS)

Alliance for Telecommunications Industry Solutions

Approved May 22, 2024

Abstract

The National Security / Emergency Preparedness (NS/EP) Data Transport Service enables an NS/EP Service Provider to provide acceptable throughput and performance to the Service User for applications using the Default QoS Flow within a designated PDU Session in the 5G System (5GS) during periods of severe network congestion when normal commercial data service is degraded.

This Technical Report (TR) analyzes NS/EP Data Transport Service invocation / revocation for several use case scenarios and identifies the implied requirements on the 5GS, in order to facilitate a common approach for NS/EP Data Transport Service invocation / revocation across multiple NS/EP Service Providers.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

> NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [https://www.atis.org/policy/patent-assurances/] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, the PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice Chair (Peraton Labs)

Table of Contents

Table of Figures

Table of Tables

ATIS Technical Report on –

Invocation/Revocation of the National Security / Emergency Preparedness (NS/EP) Data Transport Service for the 5G System (5GS)

1. Scope, Purpose, & Application

1.1 Scope

The proliferation of advanced data communications introduces new opportunities and challenges for National Security / Emergency Preparedness (NS/EP) communications. Expanded data capabilities enhance the ability for Service Users to carry out their NS/EP mission. At the same time, high data traffic volumes place significant demands upon Service Provider's networks and can hamper their ability to support the offered traffic load when these networks are impaired due to congestion and/or damage from natural or human-caused disasters. The NS/EP Data Transport Service is designed to address these needs.

This Technical Report (TR) analyzes NS/EP Data Transport Service invocation / revocation for a 5G System (5GS), including the associated user interactions with the NS/EP Service Provider, for several key use case scenarios as specified in TS 22.153, *Multimedia priority service (Release 17)* [Ref 1]. It describes support of the NS/EP Data Transport Service based on updated Policy and Charging Control (PCC) features for the Priority Protocol Data Unit (PDU) Connectivity Service as specified in 3GPP Release 17, plus an enhancement that is recommended for 3GPP Release 18 deployments of the NS/EP Data Transport Service.

1.2 Purpose

The purpose of this TR is to use the TS 22.153 [Ref 1] use case scenarios to identify the implied requirements on the 5GS and the Policy and Charging Control (PCC) architecture supporting the NS/EP Data Transport Service.

The objective is to facilitate a common approach for NS/EP Data Transport Service invocation / revocation across multiple NS/EP Service Providers.

1.3 Application

This TR is applicable to the public network infrastructure. It could also be utilized within a non-public network infrastructure.

2. Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

3rd Generation Partnership Project (3GPP)

[Ref 1] 3GPP TS 22.153, Multimedia priority service (Release 17).[1]

[Ref 2] 3GPP TS 23.501, System Architecture for the 5G System; Stage 2 (Release 17).[1]

[Ref 3] 3GPP TS 23.502, Procedures for the 5G System (5GS); Stage 2 (Release 17).[1]

[Ref 4] 3GPP TS 24.501, Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 17).[1]

[Ref 5] 3GPP TS 29.244, Interface between the Control Plane and the User Plane Nodes; Stage 3. (Release 17).[1]

[Ref 6] 3GPP TS 29.503, 5G System; Unified Data Management Services; Stage 3 (Release 17).[1]

[Ref 7] 3GPP TS 29.505, 5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3 (Release 17).[1]

[Ref 8] 3GPP TS 29.512, 5G System; Session Management Policy Control Service; Stage 3 (Release 17).[1]

[Ref 9] 3GPP TS 29.513, 5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3 (Release 17).[1]

[Ref 10] 3GPP TS 29.514, 5G System; Policy Authorization Services; Stage 3 (Release 17).[1]

[Ref 10a] 3GPP TS 29.514, 5G System; Policy Authorization Services; Stage 3 (Release 18).[1]

[Ref 11] 3GPP TS 29.518, 5G System; Access and Mobility Management Services; Stage 3 (Release 17).[1]

[Ref 12] 3GPP TS 29.519, 5G System: Usage of the Unified Data Repository service for Policy Data, Application Data and Structured Data for exposure; Stage 3 (Release 17).[1]

[Ref 13] 3GPP TS 29.521, 5G System; Binding Support Management Service; Stage 3 (Release 17).[1]

[Ref 14] 3GPP TS 31.102, Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 17).[1]

[Ref 15] 3GPP TS 38.321, NR; Medium Access Control (MAC) protocol specification (Release 16).[1]

[Ref 16] 3GPP TS 38.331, NR; Radio Resource Control (RRC) protocol specification (Release 17).[1]

[Ref 17] 3GPP TS 38.413, NG-RAN; NG Application Protocol (NGAP) (Release 17).[1]

Alliance for Telecommunications Industry Solutions (ATIS)

[Ref 18] ATIS-1000090, National Security Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS): Transport Level Packet Marking and Packet Scheduling in 5GS Technical Report.[2]

[Ref 19] ATIS-1000102, Invocation/Revocation of the National Security / Emergency Preparedness (NS/EP) Data Transport Service for the Evolved Packet System (EPS).[2]

Internet Engineering Task Force (IETF)

[Ref 20] IETF RFC 2818, HTTP Over TLS.[3]

[Ref 21] IETF RFC 7239, Forwarded HTTP Extension.[3]

3. Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

[1] This document is available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org >.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/ >.

[3] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >.

3.1 Definitions

Dedicated QoS Flow: A Quality of Service (QoS) Flow that is associated with uplink packet filters in the User Equipment (UE) and downlink packet filters in the User Plane Function (UPF) where the filters only match certain packets.

Default QoS Flow: A QoS Flow that gets established with every new PDU Session. Its context remains established throughout the lifetime of that PDU Session.

Designated DNN: The Data Network Name (DNN) which identifies the specific Data Network (DN) that is the target for the NS/EP Data Transport Service.

Designated PDU Session: The PDU Session for which the QoS of the Default QoS Flow is upgraded when the NS/EP Data Transport Service is invoked.

Non-NS/EP-subscribed UE: A UE that is not subscribed to NS/EP service.

NS/EP-subscribed UE: A UE that is subscribed to NS/EP service, including authorization for the NS/EP Data Transport Service.

PDU Connectivity Service: A service that provides exchange of PDUs between a UE and a Data Network. [3GPP TS 23.501, *System Architecture for the 5G System; Stage 2 (Release 17)*]

PDU Session: Association between the UE and a Data Network that provides a PDU connectivity service. [Ref 2]

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
5GC	5G Core network
5GS	5G System
5QI	5G QoS Identifier
AF	Application Function
AI1	Access Identity 1
AMF	Access and Mobility management Function
ARP	Allocation and Retention Priority
ATIS	Alliance for Telecommunications Industry Solutions
BSF	Binding Support Function
DN	Data Network
DNN	Data Network Name
DNS	Domain Name System
DoH	DNS over HTTPS
DSCP	DiffServ Code Point
DTS	Data Transport Service
GBR	Guaranteed Bit Rate
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IETF	Internet Engineering Task Force

IP	Internet Protocol
MAC	Medium Access Control
MPS	Multimedia Priority Service
NAS	Non-Access Stratum
NAT	Network Address Translation
NGN-PS	Next Generation Network Priority Service
NS/EP	National Security and Emergency Preparedness
PCC	Policy and Charging Control
PCF	Policy Control Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PRACH	Physical Random Access Channel
QoS	Quality of Service
RAN	Radio Access Network
RRC	Radio Resource Control
SBI	Service Based Interface
SMF	Session Management Function
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
UDM	Unified Data Management
UDP	User Datagram Protocol
UDR	User Data Repository
UE	User Equipment
UPF	User Plane Function
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module

4. Overview of the NS/EP Data Transport Service

4.1 General

The NS/EP Data Transport Service provides the Service User acceptable throughput and performance for applications using the Default QoS Flow within a Designated PDU Session in periods of severe network congestion during which normal commercial data service is degraded. The Designated DNN is determined by Service Provider policy for the NS/EP Data Transport Service subscription.

The associated performance improvements are attained through appropriate settings of the Allocation and Retention Priority (ARP) and the 5G QoS Identifier (5QI) values that are assigned to the Default QoS Flow within the Designated PDU Session, and also upgrades the QoS for any PCC rules for that PDU Session that have the same QoS settings as for that Default QoS Flow.

NOTE: Each standardized 5QI value represents a set of default QoS characteristics. The 5QI Priority Level is one of these QoS characteristics, which is important for prioritization of NS/EP traffic. However, the default values assigned

to particular individual QoS characteristics may be replaced with alternate values that override the default values. For the purpose of this TR, the **5QI*** designation is used to refer to the 5QI, including any optional override of the default 5QI Priority Level.

At the time the NS/EP Data Transport Service is invoked, the Policy Control Function (PCF) upgrades the QoS of the Default QoS Flow within the Designated PDU Session. Corresponding QoS adjustments are also applied for PCC rules that were assigned the same ARP and 5QI* values as applied to the Default QoS Flow for that PDU Session prior to invocation of the NS/EP Data Transport Service. This allows all traffic, as transported via that Default QoS Flow prior to invocation of the NS/EP Data Transport Service, to be given priority treatment upon successful invocation of the NS/EP Data Transport Service.

4.2 Assumptions

The following general assumptions are applicable to the NS/EP Data Transport Service.

- ***Relationship to 3GPP Priority PDU Connectivity Service:*** NS/EP Data Transport Service builds upon functionality as specified in TS 29.512, *5G System; Session Management Policy Control Service; Stage 3 (Release 17),* Clause 4.6.2.12.2 [Ref 8] for the Priority PDU Connectivity Service. This functionality applies appropriate updates to the ARP and 5QI* values assigned to the Default QoS Flow within the Designated PDU Session, and also modifies the settings for particular PCC rules (with the same ARP and 5QI* values as that Default QoS Flow). NS/EP Data Transport Service extends those PCC capabilities, by introducing into 3GPP Release 17 the 3GPP mpsAction attribute to explicitly support the dynamic on demand invocation and revocation of the NS/EP Data Transport Service in a 3GPP specified manner. It also extends the PCC event notification capabilities, to enable the originating Service User to be notified of the successful or unsuccessful invocation/revocation of the NS/EP Data Transport Service. Other Release 17 extensions are discussed in Clause 7.1.1.
- ***Priority signalling between the UE and the Data Transport Service (DTS) Server:*** This TR describes the functionality of a DTS Server that interacts with the UE to control the dynamic invocation and revocation of the NS/EP Data Transport Service. In order to support communications between the UE and the DTS Server when network congestion is experienced, an Application Function (AF) Signalling Flow can be established to support priority signalling between the UE and the DTS Server. Clause 6.3 describes flows that illustrate the establishment of a Dedicated QoS Flow for this priority signalling prior to or during the invocation of the NS/EP Data Transport Service, as may be applicable to particular use case scenarios.

  NOTE: Priority signalling between the UE and the DTS Server can be established [a] at the time a PDU Session is established, [b] when the user activates (opens) a DTS application on their UE, or [c] when the user invokes the NS/EP Data Transport Service. This topic is discussed further in Clause 7.1.2.

- ***Mechanism used for UE interactions with DTS Server:*** A variety of mechanisms can be used to invoke and revoke NS/EP Data Transport Service. Whereas the specific mechanisms, and details concerning particular interactions, are considered to be implementation and deployment choices, this TR considers two general types of mechanisms that can be used: use of a UE browser to access the DTS Server and use of a special DTS application that is installed on the UE to facilitate the Service User's access to the DTS Server. Further assumptions and considerations, as applicable to each of these mechanisms, are described in Clauses 6.1 and 7.1.3.
- ***User Authorization:*** Various forms of user authorization are considered in this TR. The choice of particular mechanism(s) can vary based on the particular use case. Whereas a browser-based mechanism may allow the Service User to enter NS/EP credentials into a HyperText Markup Language (HTML) form that is sent to the DTS Server, a simplified process can be enabled for UEs with network-resident NS/EP subscription information and does not require NS/EP credentials to be entered by the user. Further discussion of this topic is provided in Clauses 6.1 and 7.1.4.
- ***Access to DTS Server:*** The selection of a particular DTS Server by the UE (and routing of messages to that DTS Server) can be based on configuration of specific IP address(es) for the DTS Server or assignment of a unique Uniform Resource Locator (URL) to reach the appropriate DTS Server. Clause 6.1 considers a use case involving a UE with a special DTS application that is configured with specific IP address(es) for the DTS Server, and a use case involving the entry of a Service Provider-specific URL via a web browser. Other potential use cases can alternately be pursued. Further discussion of this topic is provided in Clause

7.1.5.

- ***Use of Advance Priority:*** Clause 6.3.3 includes sub-flows that illustrate an Advance Priority mechanism as applicable in the 5GS, for giving priority treatment (i.e., setting an ARP value corresponding to a higher priority) for NS/EP-subscribed UEs.
- ***Applicability of NS/EP Data Transport Service to particular PDU Session(s)***: This TR assumes that the priority treatment, as applicable upon successful invocation of the NS/EP Data Transport Service, is applicable to traffic carried via a specific PDU Session associated with a Designated DNN. The Designated DNN is configured by the Service Provider as part of the NS/EP subscription. This TR assumes that the DTS invocation request (and other messages used to support the UE communications with the DTS Server) are exchanged over that same PDU Session. Further discussion of this topic is provided in Clause 7.1.6.

  NOTE: Whereas the NS/EP Data Transport Service impacts traffic sent via the Default QoS Flow of the Designated PDU Session, the DTS invocation request (and subsequent signalling messages exchanged between the UE and the DTS Server) may be exchanged via a Dedicated QoS Flow within that PDU Session (established for priority signalling between these entities, as discussed above) rather than via the Default QoS Flow of that PDU Session.

- ***DTS Server determination of PCF:*** As specified in TS 29.513, *5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3 (Release 17)* [Ref 9], the Binding Support Function (BSF) is required when multiple and separately addressable PCFs are deployed, in order to ensure that the DTS Server accesses the PCF holding the designated PDU session information. Clause 7.1.7 discusses the information used by the DTS Server and the BSF to facilitate the identification of the appropriate PCF, based on specifications provided in TS 29.521, *5G System; Binding Support Management Service; Stage 3 (Release 17)* [Ref 13].
- ***NS/EP Data Transport Service Revocation:*** Clause 6.3.7 of this TR illustrates procedures that enable the NS/EP Data Transport Service to be explicitly revoked by the Service User, patterned after similar procedures used for invocation of the NS/EP Data Transport Service. In addition, to prevent a UE from inadvertently enabling the NS/EP Data Transport Service for an extended period of time, the network may support revocation of the NS/EP Data Transport Service after a predetermined time. To support this capability, the DTS Server starts a DTS timer when the NS/EP Data Transport Service is successfully invoked. If the DTS timer expires before deactivation of the NS/EP Data Transport Service, the DTS Server sends a PCC request to the PCF in order to revoke the NS/EP Data Transport Service, as discussed in Clause 7.1.11.

This TR only considers the NS/EP Data Transport Service functionality for the 5GS, based on the non-roaming architecture as described in Clause 5.2. Roaming solutions are not discussed in this TR. The DTS Server is assumed to be located in the managed IP network of the UE's Service Provider. It assumes Release 17 extensions to the Priority PDU Connectivity Service functionality, to support priority treatment for the transport of the Service User's data within the Service Provider's network, extending from the UE to the UPF. Priority treatment is not considered beyond the UPF, other than the setting of priority transport level indications, e.g., DiffServ Code Point (DSCP), on the outgoing N6 interface, and potential further priority treatment within the Service Provider network.

More detailed assumptions, as applicable to specific use cases, are provided in Clause 6.1.

4.3 Key Features and Characteristics

This clause discusses key features of the NS/EP Data Transport Service.

The use of HyperText Transfer Protocol (HTTP) and HyperText Transfer Protocol Secure (HTTPS) in this TR is illustrating two possible methods for Service Users to initiate invocation and revocation of NS/EP Data Transport Service. NS/EP Service Providers may implement other methods to initiate invocation or revocation of NS/EP Data Transport Service.

4.3.1 Invocation of the NS/EP Data Transport Service

To initiate NS/EP Data Transport Service, an HTTP or HTTPS invocation request is sent from the UE to a DTS Server via a Designated PDU Session, with the intent to upgrade the QoS of the Default QoS Flow for that PDU

Session, and to adjust PCC rules that are mapped to that Default QoS Flow. Details concerning these HTTP and HTTPS interactions are provided in Clause 6.3.5.

At the time the NS/EP Data Transport Service is invoked, the DTS Server sends a request to the PCF, causing the PCF to change the ARP and/or 5QI* of the Default QoS Flow within the Designated PDU Session to appropriate value(s) for the NS/EP Data Transport Service according to PCF decision. The PCF also modifies the PCC rules that have the same ARP and 5QI* values as for the present Default QoS Flow, building upon specifications for the 3GPP Priority PDU Connectivity Service. Details concerning this processing are provided in Clause 6.3.6.

4.3.2 Sustaining Performance of the NS/EP Data Transport Service

The NS/EP Data Transport Service achieves greater throughput by means of a higher-priority 5QI*, and/or by an NS/EP specific ARP, which results in preferential scheduler treatment in the Radio Access Network (RAN) for both downstream and upstream transmissions. This improved throughput is experienced by applications using the Default QoS Flow within the Designated PDU Session and also for applications under control of PCC rules with the same ARP/5QI* as that Default QoS Flow. In addition to the higher-priority 5QI*, the service is assigned an NS/EP ARP value that provides for higher admission capabilities and exemptions during congestion controls, including less likelihood of connection drop during handover. Details concerning the 5G QoS model are provided in Clause 5.7 of TS 23.501 [Ref 2].

4.3.3 Revocation of the NS/EP Data Transport Service

When the need for priority communications ends, the Service User explicitly revokes the NS/EP Data Transport Service. If not explicitly revoked, the service is automatically revoked upon UE detachment/deregistration, e.g., power down. A timer may also be used to ensure that the NS/EP Data Transport Service does not remain enabled for an excessive period of time. Details concerning this processing are provided in Clause 6.3.7.

5. Architectural Reference Model

5.1 Overview

This clause provides the reference architectural model used in describing the use case scenarios.

The NS/EP functionality as described in this TR pertains to the 5G Radio Access Network and the 5G Core network (5GC).

> NOTE: Aspects related to an Evolved UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access (E-UTRA) access network and the Evolved Packet Core (EPC) are described in ATIS-1000102, *Invocation/Revocation of the National Security / Emergency Preparedness (NS/EP) Data Transport Service for the Evolved Packet System (EPS)* [Ref 19], and are not considered further within the scope of this TR.

In support of NS/EP services, the 5GC may interconnect to various DNs, one of which is identified using a Designated DNN. In the flows as illustrated in this TR, the DTS Server is assumed to identify the Designated PDU Session based on UE IP address information together with a DNN value that is preconfigured in the DTS Server, although other options are possible.

5.2 Reference Architecture for NS/EP Data Transport Service

Figure 5-1 illustrates the general non-roaming architecture (using reference point notation) as applicable for invocation of NS/EP Data Transport Service. Solid lines represent user plane interfaces, and dashed lines represent control plane interfaces.

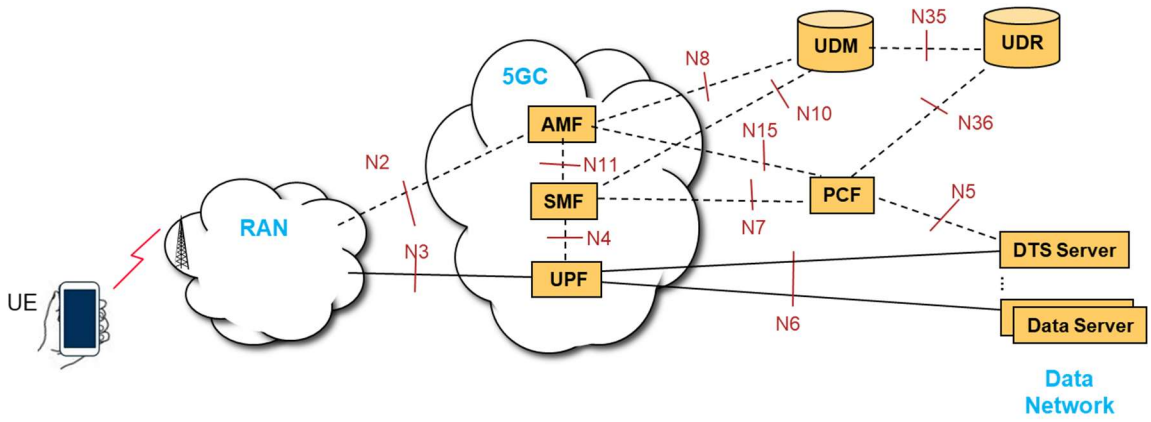

Figure 5-1 – Non-roaming architecture for NS/EP Data Transport Service

This architecture is adapted from TS 23.501 [Ref 2] Figure 4.2.3-2 ("Non-Roaming 5G System Architecture in reference point representation"). It is simplified to only illustrate elements that are pertinent to the NS/EP Data Transport Service, and is expanded to identify key elements that the UE is required to communicate with, in the context of the NS/EP Data Transport Service:

- The **DTS Server** exchanges (e.g., HTTP) signalling messages with the UE, as used to control the invocation / revocation of the NS/EP Data Transport Service. These signalling messages are transported transparently through the 5GS as user plane packets between the UE and the UPF, and are exchanged with the DTS Server via the N6 interface. The DTS Server uses the N5 interface to request the PCF to invoke / revoke the NS/EP Data Transport Service, and the PCF uses the N7 interface to transfer (QoS) policy and charging rules to the Session Management Function (SMF).
- The **Data Server(s)** illustrated in Figure 5-1 represent the server(s) that support various applications used by the UE (e.g., an HTTP Server hosting content that needs to be accessed by the UE).

In Figure 5-1, the DTS Server and the Data Server(s) are assumed to be accessed via QoS Flows within the same PDU Session.

> NOTE: Further study is needed to determine how (or if) the DTS Server can upgrade a Default QoS Flow on other than the DN used for UE-to-DTS Server communications. This requires the DTS Server to be aware of the IP address assigned to the UE in a different DN. Such capabilities are not supported in 3GPP Release 17 and are not considered within this TR.

The NS/EP Data Transport Service allows a Service User to experience greater responsiveness and QoS when using data applications during network congestion. QoS and performance improvement is limited to priority treatment in the transport of the Service User's data within the Service Provider's network, and excludes any priority treatment for the corresponding data application processing in the far-end Data Server. The aggregate data performance will be affected by possible congestion in the Data Server, which is not mitigated by the priority of the NS/EP Data Transport Service.

The priority treatment supported by the NS/EP Data Transport Service is focused on the transport of the Service User's data within the Service Provider's network, extending from the UE to the UPF. Priority transport may extend to the DTS Server (e.g., via use of special DSCP values for transport of priority packets within the Service Provider network), when the Data Server is accessed directly via the Service Provider's network. Beyond this, any additional priority treatment is not considered beyond the UPF (neither within the external DN nor for the corresponding data application processing in the far-end Data Server).

5.3 Use of QoS Flows for the NS/EP Data Transport Service

The NS/EP Data Transport Service provides improved throughput during times of congestion for applications which use the Default QoS Flow within the Designated PDU Session, and applications which require the same ARP/5QI*

as that Default QoS Flow. The Default QoS Flow is established when a PDU Session is established, and persists for the lifetime of the PDU Session. The Default QoS Flow can transport traffic for multiple applications.

Figure 5-2 illustrates the intended use of QoS Flows for the NS/EP Data Transport Service, superimposed on the reference architecture of Figure 5-1.

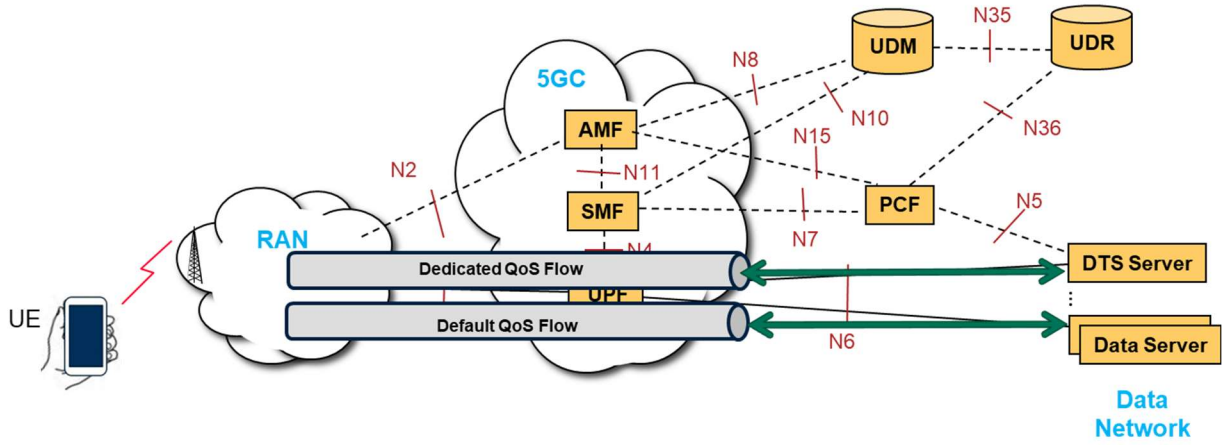

Figure 5-2. Use of QoS Flows for the NS/EP Data Transport Service

As illustrated in Figure 5-2, the Default QoS Flow within the Designated PDU Session for the NS/EP Data Transport Service is used for the exchange of packets between the UE and the far-end Data Server(s), allowing for the priority transport of IP packets subsequent to the successful invocation of the NS/EP Data Transport Service. Details concerning the establishment of a Default QoS Flow in conjunction with the establishment of a PDU Session are provided in Clause 6.3.3.

Figure 5-2 also illustrates the use of an optional Dedicated QoS Flow for priority signalling between the UE and the DTS Server. Details concerning the establishment of an AF Signalling Flow to transport priority signalling between the UE and the DTS Server are provided in Clauses 6.3.3.2 and 6.3.4.

6. Use Cases (Flow Descriptions)

This clause identifies several NS/EP Data Transport Service use cases, and illustrates various call/session flows for each use case.

- Clause 6.1 introduces the particular use cases that are considered in this TR, along with a set of assumptions that are used in the analysis of each use case.
- Clause 6.2 illustrates high-level flows for the NS/EP Data Transport Service use cases identified in Clause 6.1, each described as a particular sequence of sub-flows that may apply during particular stages of the lifecycle for the particular use case.
- Clause 6.3 provides detailed descriptions of the NS/EP Data Transport Service sub-flows as identified in the high-level flows of Clause 6.2. Given that many of the sub-flows are common to several use cases, this structure avoids the replication of such information for each use case.

The specific sequence of messages (plus the corresponding set of parameters) can vary, depending on the specific Service Provider decisions that are made for the deployment of the NS/EP Data Transport Service. Therefore, the flows depicted in the following subclauses are illustrative, and served as the basis for the identification and analysis of related standards gaps that were subsequently addressed in 3GPP Release 17.

6.1 Use Cases / Assumptions

The NS/EP Data Transport Service can be used to support a range of use cases, involving different types of UEs that may but need not be subscribed for NS/EP, and that may involve a variety of mechanisms to invoke the NS/EP Data Transport Service. Such mechanisms might use a normal browser to access the DTS Server or might make use of a special DTS application that is installed on the UE to facilitate the Service User's access to the DTS Server.

Various alternative mechanisms and associated options might be deployed and used to support the NS/EP Data Transport Service. Whereas the specific mechanisms and options for deployment of the NS/EP Data Transport Service will be determined by Service Providers in consultation with the designated government agency for the NS/EP Data Transport Service, the material in the following subclauses targets two primary use cases:

- The first use case pertains to UE invocation and revocation of NS/EP Data Transport Service via a **web browser**. This use case is applicable from either an NS/EP-subscribed UE or from a non-NS/EP subscribed UE.
- The second use case pertains to invocation and revocation of NS/EP Data Transport Service for an NS/EP-subscribed UE that is pre-configured with a **special DTS application**.

  NOTE: The special DTS application is assumed to be installed on the NS/EP-subscribed UE in advance, avoiding the need for the Service User to download that DTS application during the onset of congestion due to an NS/EP event.

The above use cases, in combination with the additional set of assumptions that are applied to each of these use cases, as summarized in

Table 6-1, illustrate several of the different mechanisms and options that may need to be supported. These are not intended as service requirements, but are provided to illustrate how NS/EP Data Transport Service invocation can operate. They served as the basis for the identification and analysis of related standards gaps which were subsequently addressed in 3GPP Release 17. Such analysis focuses on PCC protocol-related aspects associated with the NS/EP Data Transport Service.

NOTE: Aspects related to application-layer interactions between the UE and the DTS Server are subject to operator-specific implementation of the DTS Server, and how that DTS Server is designed to interact with the Service User (e.g., dependent on the use of specific HTML forms with browser-based invocation and/or dependent on the specific design of a particular UE DTS application). These aspects are beyond the scope of the analysis presented in this TR.

Table 6-1. Use Case Assumptions: Invocation / Revocation of NS/EP Data Transport Service

Topic	Non-NS/EP-subscribed UE with Browser	NS/EP-Subscribed UE with Browser	NS/EP-Subscribed UE with DTS application
[01] Priority treatments prior to DTS invocation	No priority treatment prior to DTS invocation can be provided to non-NS/EP-subscribed UEs.	Priority treatment prior to DTS invocation can be provided to NS/EP-subscribed UEs via configuration of Universal Subscriber Identity Module (USIM) Access Identity 1 / "mps-PriorityAccess" Establishment cause	
		Advance Priority mechanism provides upgraded ARP	
[02] DTS invocation mechanism	On-demand via browser		On demand via a special DTS application that is installed on the UE
[03] User designation of a particular DTS Server	User enters Service Provider-specific URL for NS/EP Data Transport Service that identifies DTS Server. This TR assumes that the URL used from an NS/EP-subscribed-UE is the same as the URL used from a non-NS/EP-subscribed UE. As a consequence, the DTS Server must first check if the UE is an NS/EP-subscribed UE, and if not, proceed with procedures associated with a non-NS/EP-subscribed UE.		Special DTS application may be pre-configured with IP address(es) or URL of the target DTS Server(s).

Topic	Non-NS/EP-subscribed UE with Browser	NS/EP-Subscribed UE with Browser	NS/EP-Subscribed UE with DTS application
[04] Domain Name System (DNS) over HTTPS (DoH) impacts	No solution available to allow DTS Server access via a DNS Server external to the Service Provider when DoH is enabled, unless Service Provider advocates user entry of DTS Server's IP address (contrary to topology hiding practices) rather than URL.	User responsible for configuring / disabling DoH on their browser, as necessary to adhere to use of Service Provider's DNS Server.	DTS application can be configured to use DTS Server's IP address rather than use a URL that requires a DNS query. Same restrictions as for a browser apply otherwise.
[05] Support for priority signalling between UE and DTS Server	Not applicable for non-NS/EP-subscribed UEs. See further discussion in Clause 7.1.2.	DTS Server may optionally establish an AF Signalling Flow for IP traffic (carrying priority signalling) between the UE and the DTS Server, when the DTS invocation request is received. See further discussion in Clause 7.1.2.	The special DTS application can contact DTS Server when the user activates (opens) the DTS application, causing the DTS Server to establish an AF Signalling Flow for IP traffic (to carry priority signalling) between the UE and the DTS Server. Other options are described in Clause 7.1.2.
[06] Authorization for DTS	The Service User enters NS/EP credentials via HTML form that is sent to the DTS Server. The DTS Server verifies the entered credentials via the NS/EP database. See further discussion in Clause 7.1.4.	The Service User invokes the NS/EP Data Transport Service in a manner that requires no NS/EP credentials to be entered by the Service User. The PCF performs the authorization by querying the User Data Repository (UDR). See further discussion in Clause 7.1.4.	
[07] Information obtained from the UE during interactions with the DTS Server (to support PCF selection)	The DTS Server obtains the request type (invocation or revocation) during DTS invocation. The local UE IP address is provided by the UE to the DTS Server as part of the IP header. See further discussion in Clause 7.1.7.		The DTS application provides the necessary information to the DTS Server during the initial UE interactions with the DTS Server, i.e., when the Service User activates (opens) the DTS application and establishes an AF Signalling Flow for priority signalling. The request type (invocation or revocation) is indicated at the time of invocation / revocation of the NS/EP Data Transport Service.

6.2 NS/EP Data Transport Service – Flow Descriptions

This clause illustrates potential realizations of the NS/EP Data Transport Service, partitioned into a series of sub-flows. These flows illustrate invocation of the NS/EP Data Transport Service for the following cases, based on the applicable architecture in Clause 5.

- Clause 6.2.1 illustrates invocation of the NS/EP Data Transport Service using a browser. The method applies both for a UE that is subscribed to NS/EP services and for a UE that is not subscribed to NS/EP

services.

- Clause 6.2.2 illustrates invocation of the NS/EP Data Transport Service for an NS/EP-subscribed UE, using a special DTS application.

6.2.1 NS/EP Data Transport Service – use of Browser

Figure 6-1 provides a high-level view of processing related to the NS/EP Data Transport Service using a web browser. As the same URL is assumed to be used from an NS/EP-subscribed UE and from a non-NS/EP-subscribed UE, the procedure differs in only a few aspects.

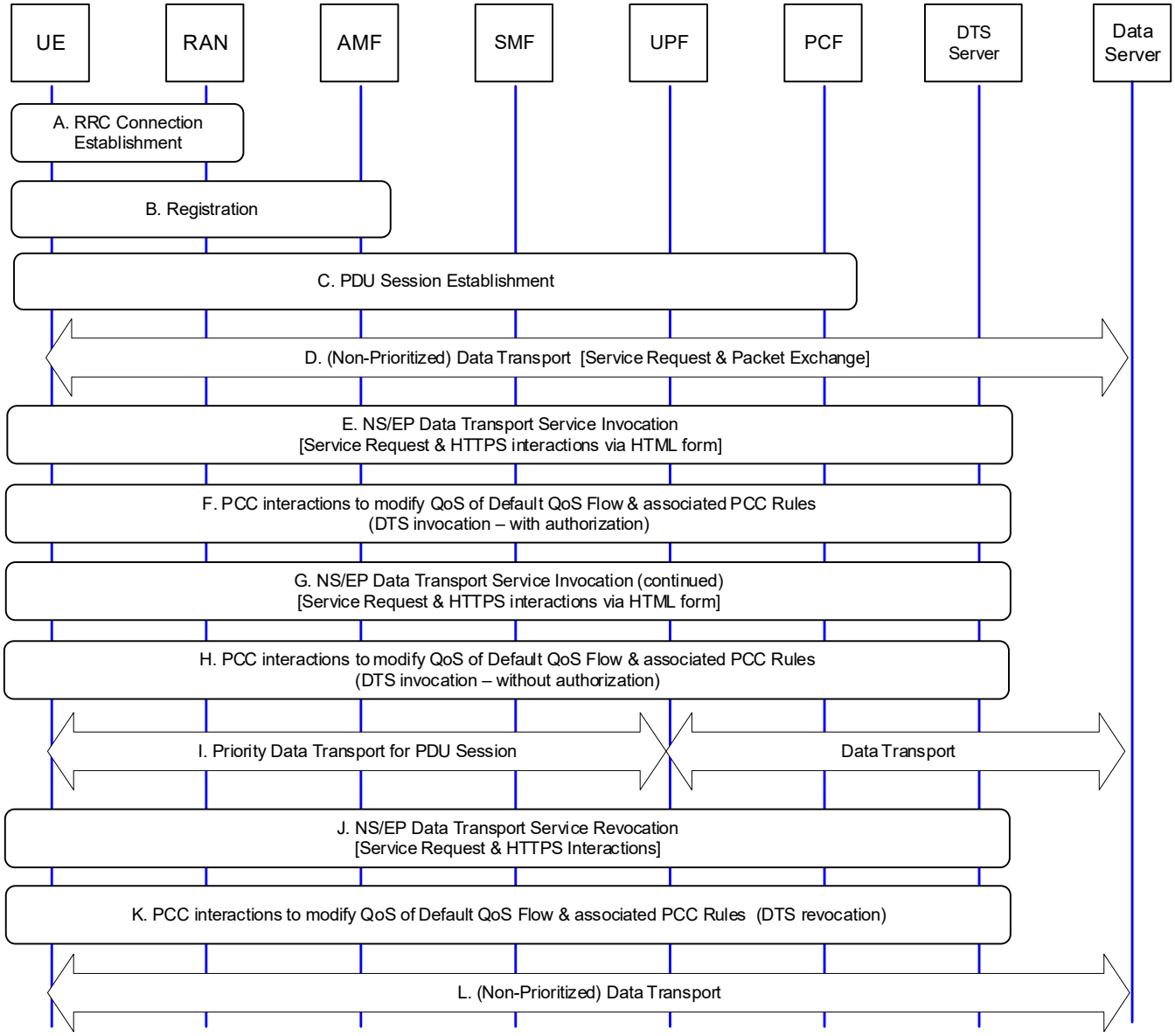

Figure 6-1. Overview of NS/EP Data Transport Service Flow – use of Browser

In Figure 6-1, the Service User initially makes use of normal procedures to access information provided by a Data Server.

The first four sub-flows (labeled as A through D) illustrate this basic functionality, prior to invocation of the NS/EP Data Transport Service. Assuming the use of a non-NS/EP-subscribed UE, no special priority treatments are applied

during this processing. Special treatments for an NS/EP-subscribed UE are provided in the step details when applicable.

A. The UE first invokes procedures to establish a Radio Resource Control (RRC) Connection with the RAN. These procedures are briefly described in Clause 6.3.1. An NS/EP-subscribed UE receives special priority treatments within the Access Class Barring test, as described in Clause 5.3.14.5 of TS 38.331, *NR; Radio Resource Control (RRC) protocol specification (Release 17)* [Ref 16].

B. The UE invokes procedures to register to the 5GC, as described in Clause 6.3.2.

C. The UE establishes a Default QoS Flow that is used to transport the Service User's HTTP and other non-Guaranteed Bit Rate (GBR) data traffic via the default DN. For the NS/EP-subscribed UE, Advance Priority is applied at the time of PDU Session Establishment. These procedures are described in Clause 6.3.3.

D. Triggered by Service User activity, the UE's browser sends an IP packet to the lower layers to be transmitted to the 5GC.[4] When instructed to do so by the RAN, the IP packet is transmitted to the 5GC and routed to the Data Server.

For this use case, the Service User experiences poor data performance during the above interactions (in sub-flow D of Figure 6-1), and therefore the Service User invokes the NS/EP Data Transport Service to improve performance.

E. For this use case, the Service User uses a browser to invoke the NS/EP Data Transport Service. The Service User enters the URL for the NS/EP Data Transport Service, the UE establishes a Transmission Control Protocol (TCP) connection to the DTS Server, and the Service User interacts with the DTS Server to invoke the NS/EP Data Transport Service. Clause 6.3.5 illustrates HTTPS-based interactions for the invocation of the NS/EP Data Transport Service.

   NOTE: The DTS Server does not know at this time if the UE is an NS/EP-subscribed UE or a non-NS/EP-subscribed UE, and 3GPP supports no means to make this determination before the DTS Server contacts the PCF. Therefore, the DTS Server first attempts to invoke the NS/EP Data Transport Service assuming it is an NS/EP-subscribed UE. If this fails, the DTS Server then attempts to invoke the NS/EP Data Transport Service assuming it is a non-NS/EP-subscribed UE.

F. The DTS Server sends a PCC request to the PCF, including an indication that the PCRF should verify that the UE is authorized for the NS/EP Data Transport Service, as described in Clause 6.3.6.

   If the NS/EP Data Transport Service invocation request is authorized, the PCF invokes PCC procedures that trigger modification of the Default QoS Flow (i.e., assignment of a particular 5QI* value for the Default QoS Flow), plus updates to any PCC rules that map to the Default QoS Flow.

   Upon successful or failed invocation of the NS/EP Data Transport Service, the DTS Server is informed. In the case of success, the user is informed, and processing continues as described in step I.

G. In the case of failed invocation of the NS/EP Data Transport Service, the Service User is required to enter NS/EP credentials as part of the HTTP interactions (e.g., via entry of NS/EP credentials into an HTML form, along with an indication of the request type [invocation or revocation]). The DTS Server uses these credentials to authorize the user, and provides feedback to the user concerning the status of this authorization.

H. Assuming the NS/EP Data Transport Service invocation request is authorized (e.g., via an NS/EP database to validate the NS/EP credentials), the DTS Server initiates PCC procedures to facilitate subsequent transport of that UE's non-GBR data packets exchanged over the Default QoS Flow (i.e., upgrades to the ARP and 5QI* values) between the UE and the UPF, as described in Clause 6.3.6. The DTS Server invokes PCC procedures that trigger these QoS upgrades of the Default QoS Flow, plus updates to any PCC rules that map to the Default QoS Flow, without requesting the PCF to verify that the UE is authorized for the NS/EP Data Transport Service. Upon successful or failed invocation of the NS/EP Data Transport Service,

[4] If the UE is 5GMM-CONNECTED, the packet is immediately queued for transmission under control of the RAN scheduler. If on the other hand, the UE is 5GMM-IDLE, the UE invokes Service Request procedures to transition to 5GMM-CONNECTED. When instructed to do so by the RAN, the IP packet is transmitted to the 5GC and routed to the Data Server. Note that this same clarification applies elsewhere in this clause, and in Clause 6.2.2.

the DTS Server is informed, and notifies the user of this event.

I. After the NS/EP Data Transport Service is successfully invoked, the corresponding priority treatment is applied to facilitate subsequent transport of that UE's non-GBR data packets over the Default QoS Flow between the UE and the UPF. Priority transport can also be enabled within the Service Provider's network (e.g., via the use of a special DSCP marking).

J. When the need for priority communications ends, the Service User uses their browser to revoke the NS/EP Data Transport Service, in a manner similar to that described in step E. Clause 6.3.7 describes HTTPS-based interactions for revocation of the NS/EP Data Transport Service.

NOTE: Various methods (either explicit or implicit) could be used for revocation of the NS/EP Data Transport Service, as discussed in Clause 7.1.11.

K. When the DTS Server receives the NS/EP Data Transport Service revocation request from the UE, the DTS Server initiates PCC procedures to trigger any associated QoS downgrades of the Default QoS Flow, plus corresponding modifications as applied to any PCC rules that were mapped to the Default QoS Flow. Upon successful or failed revocation of the NS/EP Data Transport Service, the DTS Server is informed, and notifies the user of this event. These PCC interactions are described in Clause 6.3.7.

L. Upon revocation of the NS/EP Data Transport Service, the UE continues to interact with Data Server(s) via the Default QoS Flow, without the benefits of the NS/EP Data Transport Service priority treatment.

6.2.2 NS/EP Data Transport Service - use of special DTS Application by NS/EP-Subscribed UE

Figure 6-2 provides a high-level view of processing related to the NS/EP Data Transport Service, as applicable to an NS/EP subscriber. In this use case, the NS/EP subscriber is assumed to use a special DTS application that is installed on their UE.

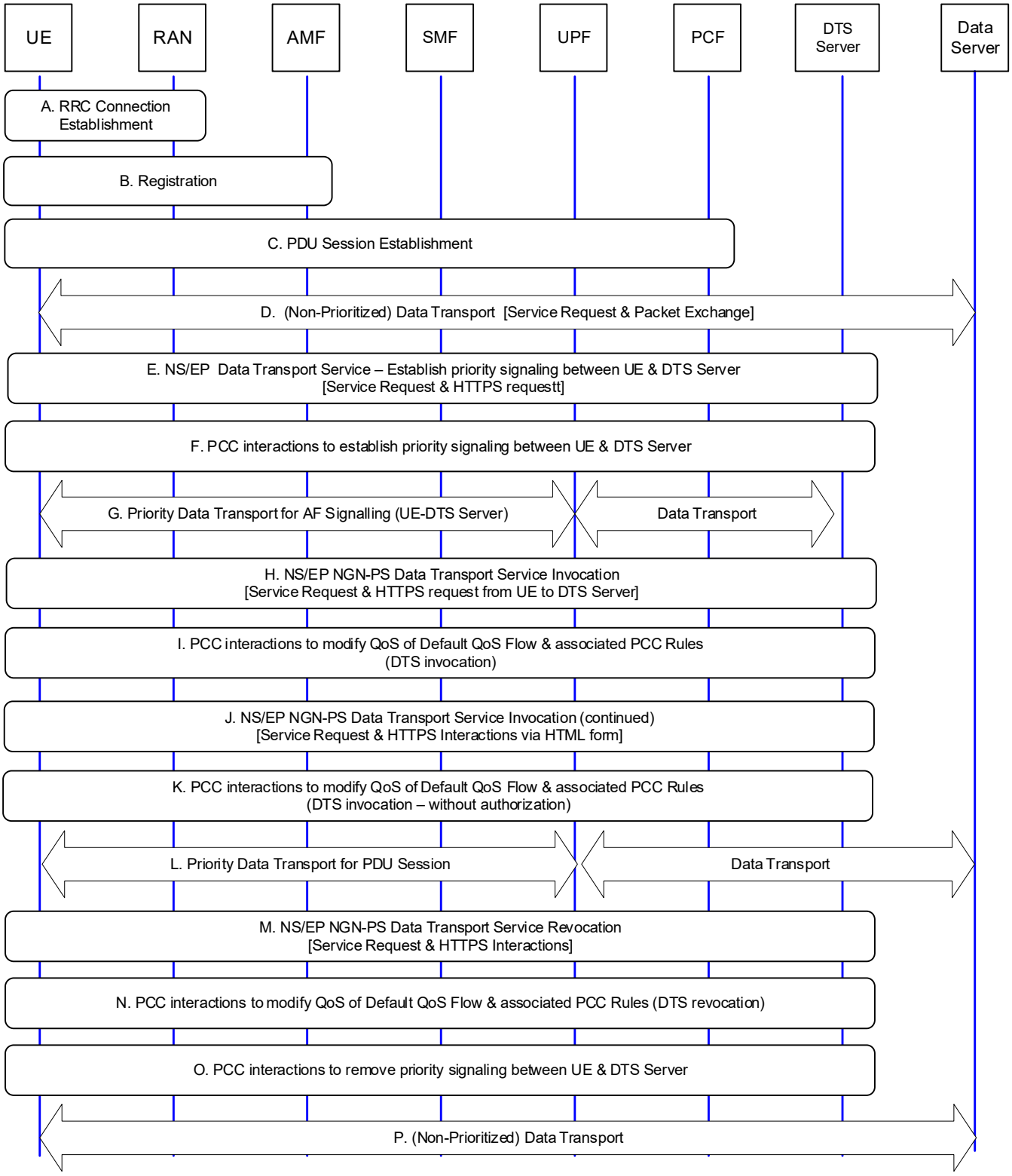

Figure 6-2. Overview of NS/EP Data Transport Service Flow - use of special DTS application by NS/EP-Subscribed UE

In Figure 6-2, the Service User initially makes use of normal procedures to access information provided by a Data Server. The first four sub-flows (labeled as A through D) are identical to the steps described in Figure 6-1.

For this use case, the Service User experiences poor data performance during the above interactions (in sub-flow D of Figure 6-2) and therefore the Service User prepares to invoke the NS/EP Data Transport Service to improve performance. This use case assumes the Service User opens a special DTS application that has previously been installed on their NS/EP-subscribed UE to facilitate the invocation of the NS/EP Data Transport Service. This DTS application functionality may include the ability to request the establishment of an AF Signalling Flow for priority signalling between the UE and the target DTS Server (e.g., at the time the DTS application is activated (opened) by the Service User, prior to the invocation of the NS/EP Data Transport Service), as discussed in steps E, F, and G below.

NOTE: Various alternatives for establishing an AF Signalling Flow for this purpose are discussed further in Clause 7.1.2.

E. When the Service User activates the special DTS application (e.g., by clicking on the application's icon on their UE), the DTS application generates a signalling packet destined for the DTS Server, and sends that signalling packet to the lower layers to be transmitted via the 5GC towards the DTS Server.

F. The DTS Server initiates PCC functionality, used to establish an AF Signalling Flow for the subsequent exchange of priority signalling between the UE and the DTS Server. The PCF authorizes the request and establishes an AF Signalling Flow with appropriate QoS characteristics. The corresponding call flow is provided in Clause 6.3.4.

NOTE: The DTS Server needs to obtain sufficient information to allow it to initiate PCC interactions with the proper PCF. Clause 7.1.7 discusses the mechanism used by the DTS Server to direct a PCC request towards the appropriate PCF.

G. Assuming the AF Signalling Flow is established successfully, this may result in the establishment of a Dedicated QoS Flow for priority data transport between the UE and the UPF, for the exchange of signalling messages between the UE and the DTS Server, as illustrated in sub-flow G of Figure 6-2.

H. When the Service User decides to invoke the NS/EP Data Transport Service (e.g., by clicking an invocation button on the DTS application), the DTS application generates an NS/EP Data Transport Service invocation request that is sent from the UE to the DTS Server via the Dedicated QoS Flow (as established in step F above) or alternatively via the Default QoS Flow as established in step C (if a Dedicated QoS Flow was not previously established). Clause 6.3.5 illustrates an example using HTTPS-based interactions for the invocation of the NS/EP Data Transport Service.

I. When the DTS Server receives the NS/EP Data Transport Service invocation request from the UE, the DTS Server sends a PCC request to the PCF, including an indication of whether the PCF should verify that the UE is authorized for NS/EP Data Transport Service.

NOTE: Various mechanisms can be used to determine whether the Service User is authorized as an NS/EP subscriber, as described in Clause 7.1.4. If the UE was previously authorized when an AF Signalling Flow was established (in step F above), then no further PCF authorization is needed.

If the NS/EP Data Transport Service invocation request is authorized, the PCF invokes PCC procedures that trigger modification of the Default QoS Flow (i.e., assignment of a particular 5QI* value for the Default QoS Flow), plus updates to any PCC rules that map to the Default QoS Flow.

Upon successful or failed invocation of the NS/EP Data Transport Service, the DTS Server is informed. In the case of success, the user is informed and processing continues as described in step L.

Steps J through N of Figure 6-2 are identical to the case of activation by a browser, as described by steps G through K of Figure 6-1.

O. When the Service User closes the special DTS application, the DTS application initiates actions to remove the AF Signalling Flow, as previously established in sub-flow F of Figure 6-2 for the exchange of priority signalling between the UE and the DTS Server. The DTS Server initiates PCC functionality, used to request the removal of the AF Signalling Flow. The corresponding call flow is illustrated in Clause 6.3.8.

P. Upon revocation of the NS/EP Data Transport Service, the UE continues to interact with Data Server(s) via the Default QoS Flow, without the benefits of the NS/EP Data Transport Service priority treatment.

6.3 Sub-Flow Descriptions

This clause provides detailed descriptions for the sub-flows as introduced in Clause 6.2 and identifies potential gaps or issues in the NS/EP processing, based on analysis of related standards. These aspects have been addressed in 3GPP Release 17.

- Clause 6.3.1 describes procedures to establish an RRC Connection with the RAN.
- Clause 6.3.2 describes procedures to register to the 5GC.
- Clause 6.3.3 describes the establishment of a PDU Session, including a Default QoS Flow and zero or more Dedicated QoS Flows.
- Clause 6.3.4 describes PCC procedures to establish priority treatment for transport of signalling packets between the UE and the DTS Server, in order to facilitate the necessary exchange of messages between the UE and the DTS Server.
- Clause 6.3.5 describes HTTPS-based procedures to invoke the NS/EP Data Transport Service.
- Clause 6.3.6 describes PCC procedures to establish priority treatment for transport of the IP packets, upon successful invocation of the NS/EP Data Transport Service.
- Clause 6.3.7 describes HTTPS-based procedures to revoke the NS/EP Data Transport Service.
- Clause 6.3.8 describes PCC procedures to remove the AF Signalling Flow that was previously established for priority signalling between the UE and the DTS Server.

6.3.1 RRC Connection Establishment

Prior to the transmission of Non-Access Stratum (NAS) messages in support of Mobility Management and Session Management, and the transmission of Application Layer data from the UE, or the delivery of Application Layer data to the UE, a UE must first establish an RRC Connection with the RAN.

The establishment of an RRC Connection requires Layer 1 and 2 procedures – involving the Physical, Medium Access Control (MAC), and RRC Layers of the NR Interface. The RAN broadcasts information to selectively bar UEs from gaining access to the network (radio resources) during network congestion.

The RRC Connection Establishment mechanisms include the ability to prioritize RRC requests from an NS/EP-subscribed UE.

- Access Class Barring

  The RAN broadcasts information to support the Access Class Barring capability. NS/EP-subscribed UEs are statically provisioned with Access Identity 1 (AI1) in the USIM, as specified in TS 31.102, *Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 17)* [Ref 14]. The Service Provider provides AI1 prioritized access to radio resources during times of network congestion.

- PRACH Prioritization

  Physical Random Access Channel (PRACH) prioritization is a Release 15 5G feature that increases the likelihood of a faster successful completion of the random access procedure for handover and beam failure recovery. This feature was extended in Release 16 (3GPP TS 38.321, *NR; Medium Access Control (MAC) protocol specification (Release 16)* [Ref 15]*)* to allow NS/EP-subscribed UEs to ramp up their power faster and use a smaller backoff period during the random access procedure leading to higher chances of successfully completing the procedure.

- RRC Connection Establishment

  The RRC Connection Establishment prioritizes RRC requests from an NS/EP-subscribed UE. NS/EP-subscribed UEs mark their requests by setting the Establishment Cause to the “mps-PriorityAccess” value, as specified in TS 38.331 [Ref 16]. This allows the RAN to apply priority in the decision to allocate signalling

resources for subsequent RRC and NAS messages. This also allows certain classes of traffic to be throttled by the RAN, thereby providing benefits for all UEs (for traffic not belonging to those targeted traffic classes). The Overload Control action is used to signal the RAN to reject RRC Connection Requests that are for specific Establishment Causes.

6.3.2 Initial Registration

The Initial Registration procedure allows a UE to register with the 5GC to receive services that require registration. Figure 6-3 illustrates the sequence of messages used to support the initial registration procedure.

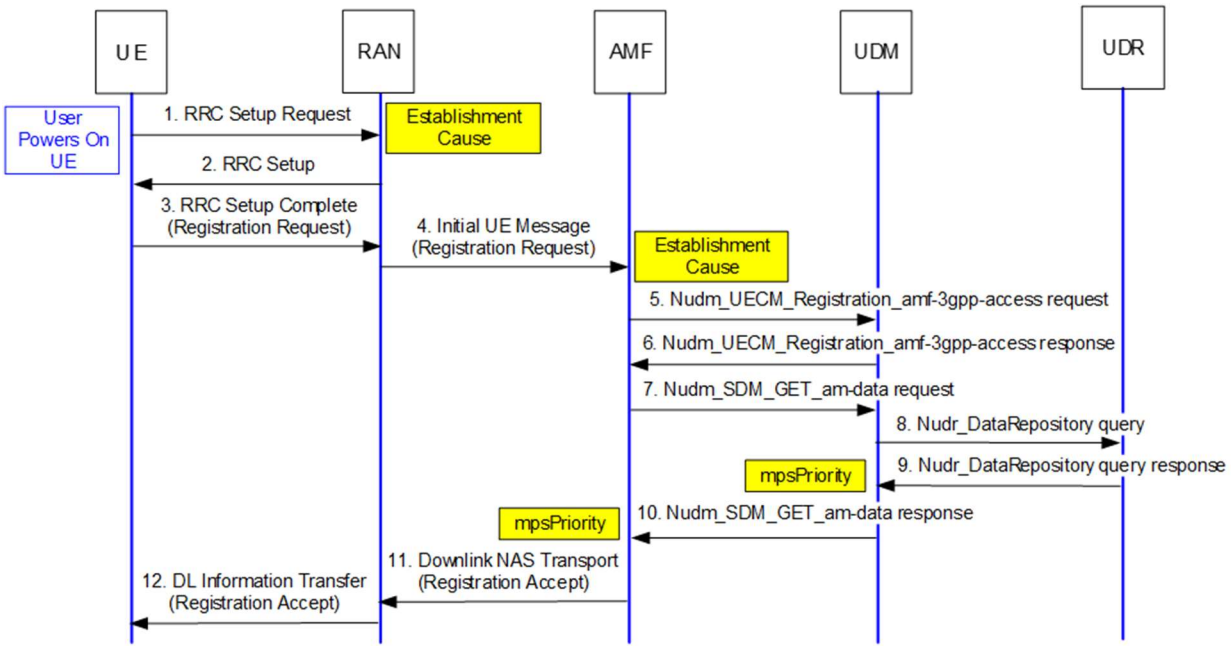

Figure 6-3. RRC Connection Establishment and Initial Registration Procedure Message Flow

Following RRC Connection Establishment, the “mps-PriorityAccess” Establishment Cause is sent by the UE to the RAN, and is sent by the RAN to the Access and Mobility management Function (AMF) in the **Initial UE Message**, as illustrated in Figure 6-4. This results in priority handling of the Initial Registration procedures as described in Clause 6.1.2 of ATIS-1000090, *National Security Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS): Transport Level Packet Marking and Packet Scheduling in 5GS Technical Report* [Ref 18].

The AMF registers the UE for 3GPP access, and retrieves the UE’s Access and Mobility Subscription data from the Unified Data Management (UDM). The UDM retrieves Access and Mobility Subscription data from the UDR, as specified in TS 29.505, *5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3 (Release 17)* [Ref 7]. The subscription profile for the subscriber is returned from the UDM to the AMF in the **Nudm_SDM_GET_am-data response** in step 10, as specified in Clause 6.1.3.5.3 of TS 29.503, *5G System; Unified Data Management Services; Stage 3 (Release 17)* [Ref 6]. This response may include the mpsPriority attribute (in the amData attribute of the subscription profile), which is a boolean that indicates whether the UE is subscribed to Multimedia Priority Service (MPS). When the AMF receives this value, it informs the UE that the use of access identity 1 is valid (in the registered Public Land Mobile Network [PLMN] or equivalent PLMN) by setting the MPS indicator bit of the 5GS network feature support IE to "Access identity 1 valid" in the **Registration Accept** message.

Unlike the LTE Attach procedure, the 5GS Registration procedure does not support concurrent initiation of PDU Session establishment. Therefore, at the end of the 5GS Registration procedure, the UE does not have a PDU Session established to any DN. A separate PDU Session Establishment procedure, described in Clause 6.3.3, is required to establish a PDU Session and a default QoS Flow to a particular DN.

6.3.3 PDU Session Establishment

Upon the completion of registration, a UE may establish a PDU Session to support IP connectivity to a DN. DN Connectivity includes an associated Default QoS Flow that remains established for the lifetime of the PDU Session.

> NOTE: The UE may establish DN connectivity with additional DNs, e.g., to connect to the IMS Core Network. The UE is assigned a different IP address for each PDU session. Each PDU Session will include an associated Default QoS Flow, and may involve the establishment of zero or more Dedicated QoS Flows. The establishment of multiple PDU Sessions is not pertinent to the NS/EP Data Transport Service functionality, as assumed in this TR, as the priority upgrade is only applied for the Default QoS Flow associated with an indicated IP address.

Advance Priority for an NS/EP-subscribed UE provides subscription-based QoS parameters for the Default QoS Flow within the 5GS. The 5GC PDU Session Establishment procedure supports the concept of Advance Priority, which is used to provide priority treatment for an NS/EP-subscribed UE.

The following subclauses describe aspects of the PDU Session Establishment call flows that are pertinent to NS/EP. More complete descriptions of these PDU Session Establishment call flows are provided in Clause 6.1.7 of ATIS-1000090 [Ref 18].

Clause 6.3.3.1 illustrates the use of Advance Priority for an NS/EP-subscribed UE, assuming that a single PDU Session is established with a Default QoS Flow to support Best Effort data traffic. For a UE that is not subscribed to NS/EP, similar procedures apply, with the exception that Advance Priority is not provided.

Clause 6.3.3.2 extends the material in Clause 6.3.3.1 by also illustrating the establishment of a Dedicated QoS Flow during PDU Session Establishment. This procedure can be applied to support the establishment of a priority Dedicated QoS Flow from an NS/EP-subscribed UE to the UPF towards the DTS Server, to carry signalling traffic between the UE and the DTS Server for supporting the NS/EP Data Transport Service.

6.3.3.1 Advance Priority during PDU Session Establishment

This clause describes the establishment of DN Connectivity with the Default DN at the time of PDU Session Establishment when only the Default QoS Flow is established. Advance Priority is assumed, as described in Clause 6.1.7 of ATIS-1000090 [Ref 18].

Figure 6-4 illustrates the sequence of messages used to support the PDU Session Establishment procedure, including the establishment of a Default QoS Flow.

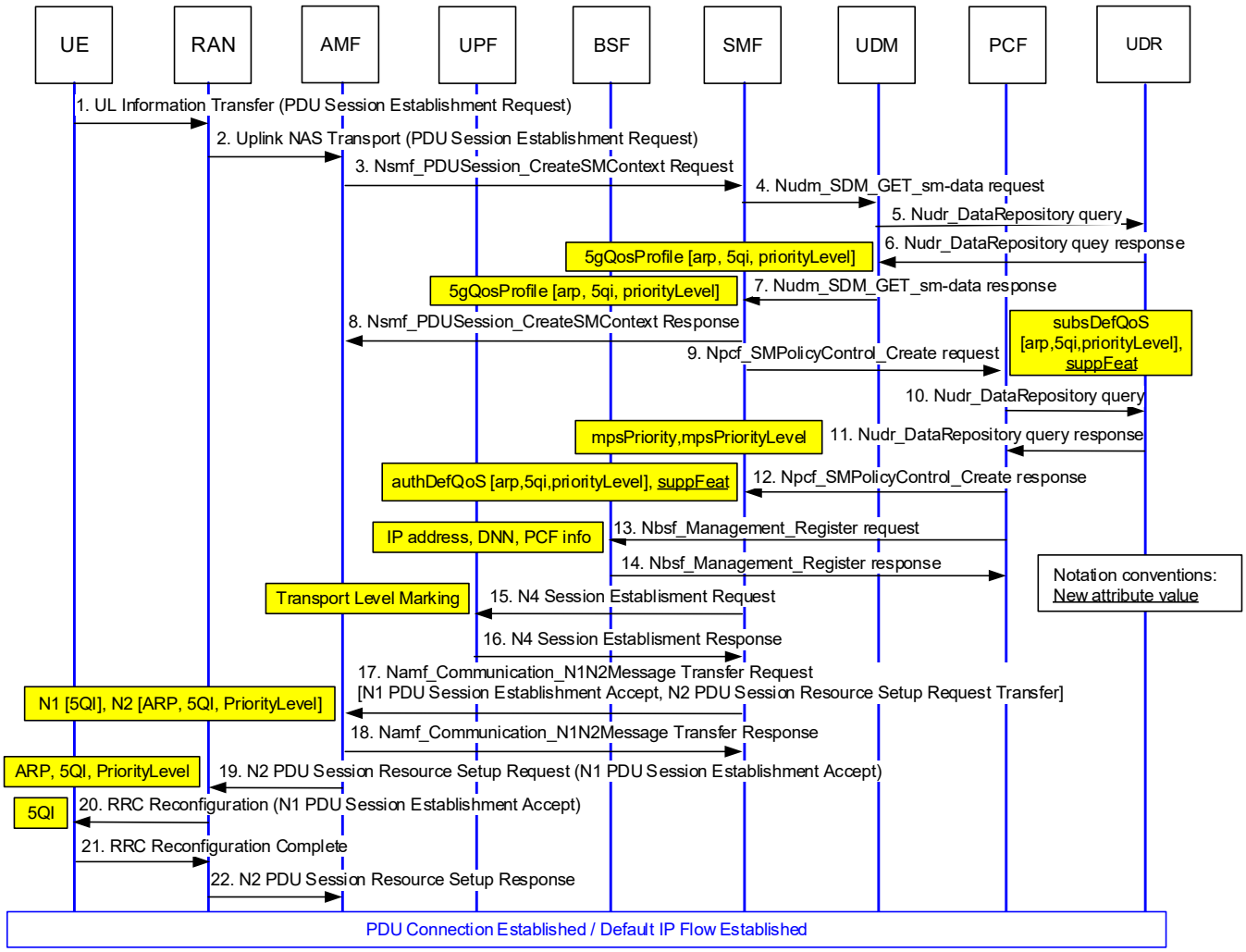

Figure 6-4. PDU Session Establishment Procedure Illustrating Advance Priority

To initiate establishment of a PDU Session, the UE sends a **PDU Session Establishment Request** message, as specified in TS 24.501, *Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 17)* [Ref 4]. When the AMF receives this NAS message, the AMF includes this NAS message, along with the requested DNN, within an **Nsmf_PDUSession_CreateSMContext request** to the SMF. When establishing the PDU session, the SMF requests Session Management data from the UDM. The UDM retrieves Session Management Subscription Data from the UDR, as specified in TS 29.505 [Ref 7]. The list of DNNs that the UE is permitted to access, an indication of which DNN is the Default DNN, and the 5GS Subscribed QoS profile for each permitted DNN are returned from the UDM to the SMF in the **Nudm_SDM_GET_sm-data response** in step 7. The 5gQosProfile attribute contains the arp and 5qi attributes plus an optional priorityLevel attribute within the dnnConfigurations attribute of the SessionManagementSubscriptionData data structure, as specified in TS 29.503 [Ref 6]. If Advance Priority is enabled, the ARP Priority Level of the Default QoS Flow for this DN is set to the highest priority (lowest numerical value) Priority Level from the set allocated by the Service Provider for NS/EP use.

Assuming the use of dynamic PCC for the PDU Session, the SMF establishes an SM Policy Association with the PCF via the **SMPolicyControl_Create request** to obtain the default PCC Rules for the PDU Session. This request includes the Subscribed Default QoS (as received from the UDM) in the subsDefQos attribute; and UE information (SUPI, GPSI, and IP Address). It also includes the suppFeat attribute to inform the PCF about the required and optional features that the SMF supports, including the "MPSforDTS" feature number.

The PCF retrieves the subscriber's subscription related information from the UDR in steps 10 and 11, using the Nudr_DataRepository API for policy data, as specified in TS 29.519, *5G System: Usage of the Unified Data Repository service for Policy Data, Application Data and Structured Data for exposure; Stage 3 (Release 17)* [Ref

12]. The UDR provides the smPolicyDnnData attribute, which contains the mpsPriority attribute to indicate whether the subscription supports MPS and the mpsPriorityLevel attribute to provide the relative priority level for MPS.

The PCF sends an **SMPolicyControl_Create response** to the SMF (in step 12 of Figure 6-4), including the arp and 5qi attributes plus an optional priorityLevel attribute, in the authDefQos attribute. The authorized QoS of the Default QoS Flow provides an upgraded ARP value for an NS/EP-subscribed UE. The PCF also includes the suppFeat attribute, to indicate the set of features that the PCF has in common with the SMF, and that the PCF supports within the N7 session.

NOTE: In addition to an upgraded ARP, the PCF could also provide an upgraded 5QI* for the Default QoS Flow. This can support an “always on” deployment of the NS/EP Data Transport Service.

The PCF uses the **Nbsf_Management_Register** service operation to register the session binding information in the BSF, as illustrated in step 13. This binding information includes the UE's IP address that the DTS Server uses to query the BSF to find the correct PCF.

NOTE: The BSF stores this binding information, allowing the DTS Server to subsequently use the **Nbsf_Management_Discovery** service operation to identify the appropriate PCF when an AF Signalling Flow is established for priority signalling between the UE and the DTS Server (as illustrated in step 1 of Clause 6.3.4) or when the NS/EP Data Transport Service is invoked. See further discussion in Clause 7.1.7.

The SMF derives a Transport Level Marking (i.e., DSCP value), based on mapping from the 5QI, the Priority Level (if explicitly signalled) and optionally the ARP priority level configured at the SMF, as specified in TS 29.244, *Interface between the Control Plane and the User Plane Nodes; Stage 3. (Release 17)* [Ref 5]. The SMF includes the derived DSCP value in the Transport Level Marking IE contained in the N4 **Session Establishment Request** in step 15.

The SMF sends an **Namf_Communication_N1N2Message Transfer request** (as specified in TS 29.518, *5G System; Access and Mobility Management Services; Stage 3 [Release 17]* [Ref 11]) to the AMF in step 17, containing information pertaining to the N2 **PDU Session Resource Setup Request** and the N1 **PDU Session Establishment Accept** message. The N2 **PDU Session Resource Setup Request** (as specified in TS 38.413, *NG-RAN; NG Application Protocol (NGAP) [Release 17]* [Ref 17]) is sent to the RAN in step 19, containing the assigned ARP, 5QI, and Priority Level values for the Default QoS Flow. The assigned 5QI value for the Default QoS Flow is sent to the UE via the RAN in a **PDU Session Establishment Accept** message (as specified in TS 24.501 [Ref 4]) in step 20.

6.3.3.2 Advance Priority with an Additional Dedicated QoS Flow

This clause extends the material in Clause 6.3.3.1 by also illustrating the establishment of a Dedicated QoS Flow at the time of PDU Session Establishment.

NOTE: The establishment of a Dedicated QoS Flow (within the same PDU Session as established at the time of PDU Session Establishment) can be used to support priority signalling between the UE and the DTS Server. Alternatively, priority signalling between the UE and the DTS Server can be established when the user activates (opens) a DTS application on their UE (as described in Clause 6.3.4), or when the user invokes NS/EP Data Transport Service (as described in Clause 6.3.5). These mechanisms are discussed further in Clause 7.1.2.

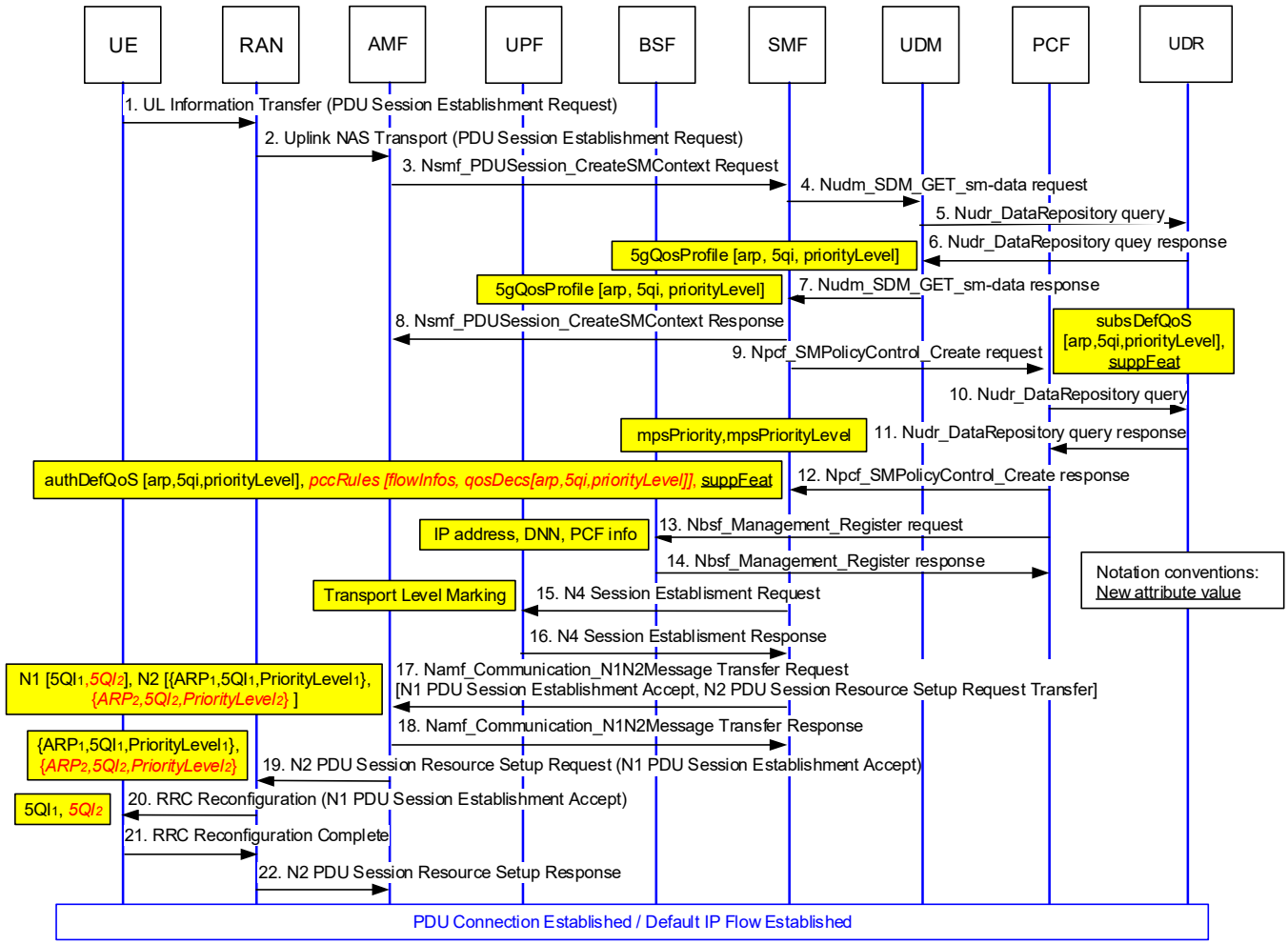

Figure 6-5. PDU Session Establishment Procedure Illustrating Advance Priority, including Dedicated QoS Flow

Figure 6-5 illustrates the sequence of messages (differentiated from those depicted in Figure 6-4 via red italics font) used to establish a Dedicated QoS Flow (with appropriate ARP and 5QI* values) at the time of PDU Session establishment, in addition to the Default QoS Flow (assigned an appropriate ARP value).

One manifestation of this processing involves the establishment of a priority Dedicated QoS Flow from an NS/EP-subscribed UE to the UPF towards the DTS Server, to carry signalling traffic between the UE and the DTS Server for supporting the NS/EP Data Transport Service. The Dedicated QoS Flow between the UE and the UPF towards the DTS Server is associated with the same PDU Session as the Default QoS Flow portrayed in this figure.

The PCF may choose to establish an AF signalling flow between the UE and the DTS Server based on the mpsPriority attribute received from the UDR in step 11. The PCF installs the corresponding dynamic PCC rules in the SMF by including the pccRules attribute in the **SMPolicyControl_Create response** (in step 12 of Figure 6-5). The pccRules attribute includes the flowInfos attribute that provides IP flow packet filter information for the AF Signalling Flow between the UE and the DTS Server, and includes the refQosData attribute that references appropriate QoS (5qi and arp attributes and optional priorityLevel attribute) as specified in the qosDecs attribute. These attribute values are used to establish appropriate QoS for the AF Signalling Flow, used to support signalling between the UE and the DTS Server.

NOTE: Clause 7.1.12 discusses the assignment of 5QI* value(s) for NS/EP Data Transport Service.

NOTE: To populate the flowInfos attribute in the **SMPolicyControl_Create response**, the PCF requires the IP addresses of the UE and the DTS Server, to identify the signalling flow between the UE and the DTS Server. Given that communications have not yet been established between the PCF and the DTS Server at the time of PDU Session establishment, the PCF must determine the IP address of the DTS Server. See Clause 7.1.2.

The corresponding QoS Flow Establishment procedures, used to install appropriate PCC rules for the new Dedicated QoS Flow, are illustrated in steps 17 – 22 of Figure 6-5.

The SMF sends an **Namf_Communication_N1N2Message Transfer request** (as specified in TS 29.518 [Ref 11]) to the AMF in step 17, containing information pertaining to the N2 **PDU Session Resource Setup Request** and the N1 **PDU Session Establishment Accept** message. The AMF sends an N2 **PDU Session Resource Setup Request** (as specified in TS 38.413 [Ref 17]) to the RAN in step 19, containing the assigned ARP, 5QI, and Priority Level values for each QoS Flow. The assigned 5QI values for each QoS Flow are sent to the UE via the RAN in a **PDU Session Establishment Accept** message (as specified in Clause 8.3.2 of TS 24.501 [Ref 4]) in step 20.

6.3.4 Establishment of AF Signalling Flow between UE and DTS Server

This clause illustrates the establishment of an AF Signalling Flow for priority signalling between the UE and the DTS Server prior to the subsequent invocation of the NS/EP Data Transport Service. If the NS/EP-subscribed UE is configured with a special DTS application to facilitate the invocation of the NS/EP Data Transport Service, this flow can be initiated when the user opens that DTS application (e.g., by clicking on that special application's icon on their UE), allowing the UE's DTS application to initiate HTTP signalling with the DTS Server, in order to allow the DTS Server to initiate the establishment of an AF Signalling Flow for priority signalling between the UE and the DTS Server. This is only one possible deployment scenario. Alternatively, an AF Signalling Flow for priority signalling between the UE and the DTS Server could be established at a later time when the UE invokes the NS/EP Data Transport Service. This procedure is based on Clause 4.2.2.12.3 of TS 29.514, *5G System; Policy Authorization Services; Stage 3 (Release 17)* [Ref 10].

NOTE: Several options for establishing an AF Signalling Flow for priority signalling between the UE and the DTS Server are discussed in Clause 7.1.2.

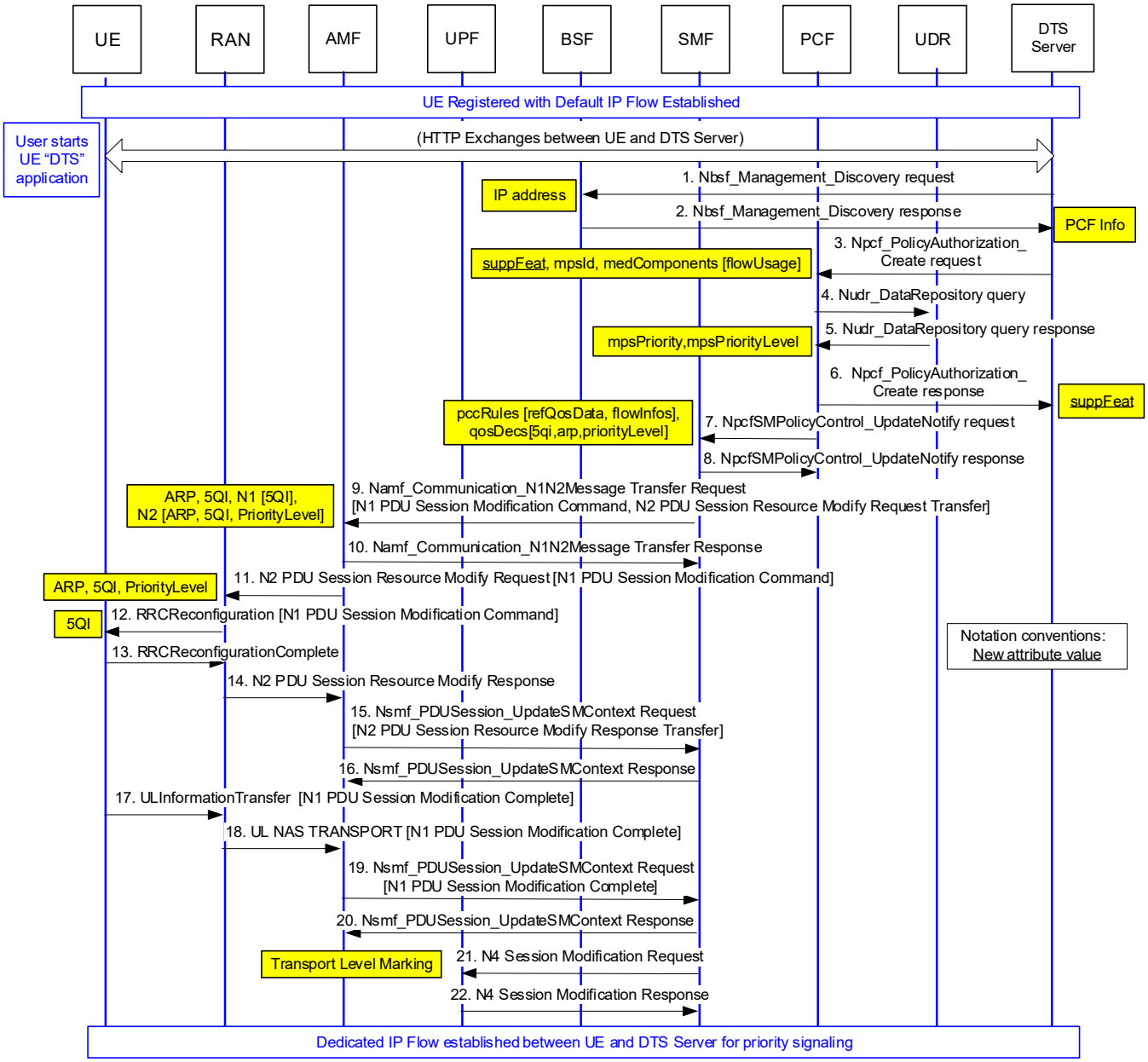

Figure 6-6. Establishment of AF Signalling Flow for UE to DTS Server Communications

Figure 6-6 illustrates the establishment of an AF Signalling Flow (with appropriate ARP and 5QI* values) for priority signalling between the UE and the DTS Server, at the time the DTS Server is initially contacted by the UE, but prior to the invocation of NS/EP Data Transport Service (e.g., triggered by Service User activation of a special DTS application on an NS/EP-subscribed UE). Information concerning the target DTS Server (e.g., a Service Provider-specific URL or specific IP address(es)) is configured for the special DTS application, allowing the UE to establish a connection to an appropriate DTS Server.

The DTS application establishes communications with the DTS Server (e.g., via the Default QoS Flow, as illustrated in Figure 6-7). For establishing communications with the DTS Server in a non-roaming scenario, this TR assumes that a valid UE IP address is received by the DTS Server in the source IP address of the initial message that it receives from the UE. The DTS Server uses the UE's IP address, in combination with the Designated DNN, to retrieve the PCF address. To accomplish this, the DTS Server interacts with the BSF by using the **Nbsf_Management_Discovery** service, as specified in TS 29.521 [Ref 13]. The DTS Server sends the local UE IP address and the Designated DNN to the BSF in order to facilitate the BSF's identification of the correct PCF, as illustrated in steps 1 and 2 of Figure 6-6.

The DTS Server interacts with the PCF by using the **Npcf_PolicyAuthorization** service as specified in TS 29.514 [Ref 10] to establish an AF Signalling Flow for priority signalling between the UE and the DTS Server. The medSubComps attribute within the medComponents attribute represents the AF signalling IP flow. The flowUsage attribute is set to the value "AF_SIGNALLING," the fDesc attribute describes the AF Signalling Flow between the UE and DTS Server, and the fStatus attribute is set to the value "ENABLED." The suppFeat attribute informs the PCF about the required and optional features that the DTS Server supports, including the "MPSforDTS" feature number. The mpsId attribute is included to indicate a request to apply priority treatment for the AF signalling between the UE and the DTS Server for NS/EP Data Transport Service.

Beginning in 3GPP Release 18, the DTS Server also includes the mpsAction attribute, set to the value "AUTHORIZE_AND_ENABLE_MPS_FOR_AF_SIGNALLING," in the **Npcf_PolicyAuthorization_Create request**. The DTS Server and PCF indicate support for this new mpsAction attribute value via the inclusion of the "AuthorizationForMpsSignalling" feature number in the suppFeat attribute.

> NOTE: The new "AUTHORIZE_AND_ENABLE_MPS_FOR_AF_SIGNALLING" value is added to the mpsAction attribute, as specified in TS 29.514 [Ref 10a] (Release 18). This value enhances the prior 3GPP Release 17 mechanism used to trigger the appropriate PCF behavior as specified for the NS/EP Data Transport Service, by providing an explicit indication that the PCF should authorize the UE for the NS/EP Data Transport Service prior to establishment of the AF Signalling Flow.

When the PCF receives the **Npcf_PolicyAuthorization_Create request**, the PCF retrieves the subscriber's subscription related information from the UDR in steps 4 and 5, using the Nudr_DataRepository API for policy data, as specified in TS 29.519 [Ref 12]. The UDR provides the smPolicyDnnData attribute, which contains the mpsPriority attribute to indicate whether the subscription supports MPS and the mpsPriorityLevel attribute to provide the relative priority level for MPS. Assuming the UE is authorized for NS/EP Data Transport Service, the PCF responds to the DTS Server with an **Npcf_PolicyAuthorization_Create response** in step 6. Assuming support for the "MPSforDTS" feature, the suppFeat attribute includes the corresponding "MPSforDTS" feature number to indicate this feature is commonly supported by both the PCF and the DTS Server. Receipt of the **Npcf_PolicyAuthorization_Create response** by the DTS Server indicates the associated request was received and understood by the PCF, but does not imply that all the requested actions were completed successfully.

> NOTE: If the request is not authorized, the PCF sends an HTTP "403 Forbidden" response message to the DTS Server, including the cause attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

Based on receipt of the **Npcf_PolicyAuthorization_Create request** as indicated above (including the flowUsage attribute set to "AF_SIGNALLING" plus the mpsId attribute), the PCF installs corresponding dynamic PCC rules to establish an AF Signalling Flow for priority signalling between the UE and the AF. The PCF includes the pccRules attribute, using the refQosData attribute to reference appropriate QoS (5qi and arp attributes and optional priorityLevel attribute) for the AF Signalling Flow, used to support priority signalling between the UE and the DTS Server. The PCF notifies the SMF of the updated Session Management policies via the **NpcfSMPolicyControl_UpdateNotify** service operation, as illustrated in step 7 of Figure 6-6.

> NOTE: Clause 7.1.12 discusses the assignment of 5QI* value(s) for NS/EP Data Transport Service.

The SMF responds to the PCF with an **NpcfSMPolicyControl_UpdateNotify** response, which confirms the SMF received and understood the associated **NpcfSMPolicyControl_UpdateNotify** service operation. It does not imply that all requested actions were completed successfully by the 5GC and RAN.

The corresponding QoS Flow Establishment procedures, used to install appropriate PCC rules for the new Dedicated QoS Flow, are illustrated in steps 9 - 22 of Figure 6-6. The SMF sends an **Namf_Communication_N1N2Message Transfer request** (as specified in TS 29.518 [Ref 11]) to the AMF in step 9, containing information pertaining to the N2 **PDU Session Resource Modify Request** and the N1 **PDU Session Modification Command.** The AMF sends an N2 **PDU Session Resource Modify Request** (as specified in TS 38.413 [Ref 17]) to the RAN in step 11, containing the assigned ARP, 5QI, and Priority Level values for the new Dedicated QoS Flow. The assigned 5QI value for the new Dedicated QoS Flow is sent to the UE via the RAN in a **PDU Session Modification Command** message (as specified in TS 24.501 [Ref 4]) in step 12. Further details concerning the overall PDU Session Modification flow are provided in Clause 4.3.3 of TS 23.502, *Procedures for the 5G System (5GS); Stage 2 (Release 17)* [Ref 3].

6.3.5 HTTPS-based Invocation of the NS/EP Data Transport Service

This clause describes HTTPS-based invocation of the NS/EP Data Transport Service.

It is assumed that the UE is 5GMM-CONNECTED; if instead, the UE is 5GMM-IDLE, a Service Request procedure as described in Clause 6.1.5 of ATIS-1000090 [Ref 18] must first be completed to transition the UE from 5GMM-IDLE to 5GMM-CONNECTED and to reestablish QoS Flows and IP connectivity with the 5GC.

Figure 6-7 illustrates the sequence of messages used to support the HTTPS-based method of invocation for the NS/EP Data Transport Service. This figure illustrates the exchange of DNS, TCP, Secure Sockets Layer (SSL) / Transport Layer Security (TLS), 5G Service Based Interface (SBI), and HTTPS packets that are used to support HTTPS interactions between a UE and the DTS Server.

- When the Service User uses the UE's browser to enter the URL to invoke the NS/EP Data Transport Service, Figure 6-7 (step A) illustrates the exchange of a Domain Name System (DNS) query and response between the UE and a DNS Server (to translate the URL to the IP address of the DTS Server). See Clause 6.3.5.1.

- Using the IP address of the DTS Server, Figure 6-7 (step B) illustrates the establishment of a TCP connection between the UE and the DTS Server (see Clause 6.3.5.2) and (step C) the subsequent SSL/TLS handshake used to establish a secured connection between these entities (see Clause 6.3.5.3).

- Figure 6-7 (steps D1 through D3) also illustrates the optional establishment of an AF Signalling Flow for priority signalling between the UE and the DTS Server, as described in Clause 6.3.4. Clause 7.1.2 provides further analysis of this topic.

- Figure 6-7 illustrates the exchange of HTTPS messages between the UE and the DTS Server via the secured connection. Clauses 6.3.5.4 and 6.3.5.5 describe the potential use of steps E1 through E6, as applicable for particular use cases for invocation of NS/EP Data Transport Service with and without entry of NS/EP Credentials respectively.

  NOTE: Figure 6-7 illustrates three potential points at which NS/EP authorization can be performed, depending upon the particular use case: [a] as an integrated function during the establishment of the AF Signalling Flow, as discussed in Clause 6.3.4; [b] as an integrated function during the invocation of NS/EP Data Transport Service, as discussed in Clause 6.3.6, or [c] using NS/EP credentials collected from a non-NS/EP-subscribed UE by the DTS Server, as discussed in Clause 6.3.5.5. These options are discussed further in Clause 7.1.4.

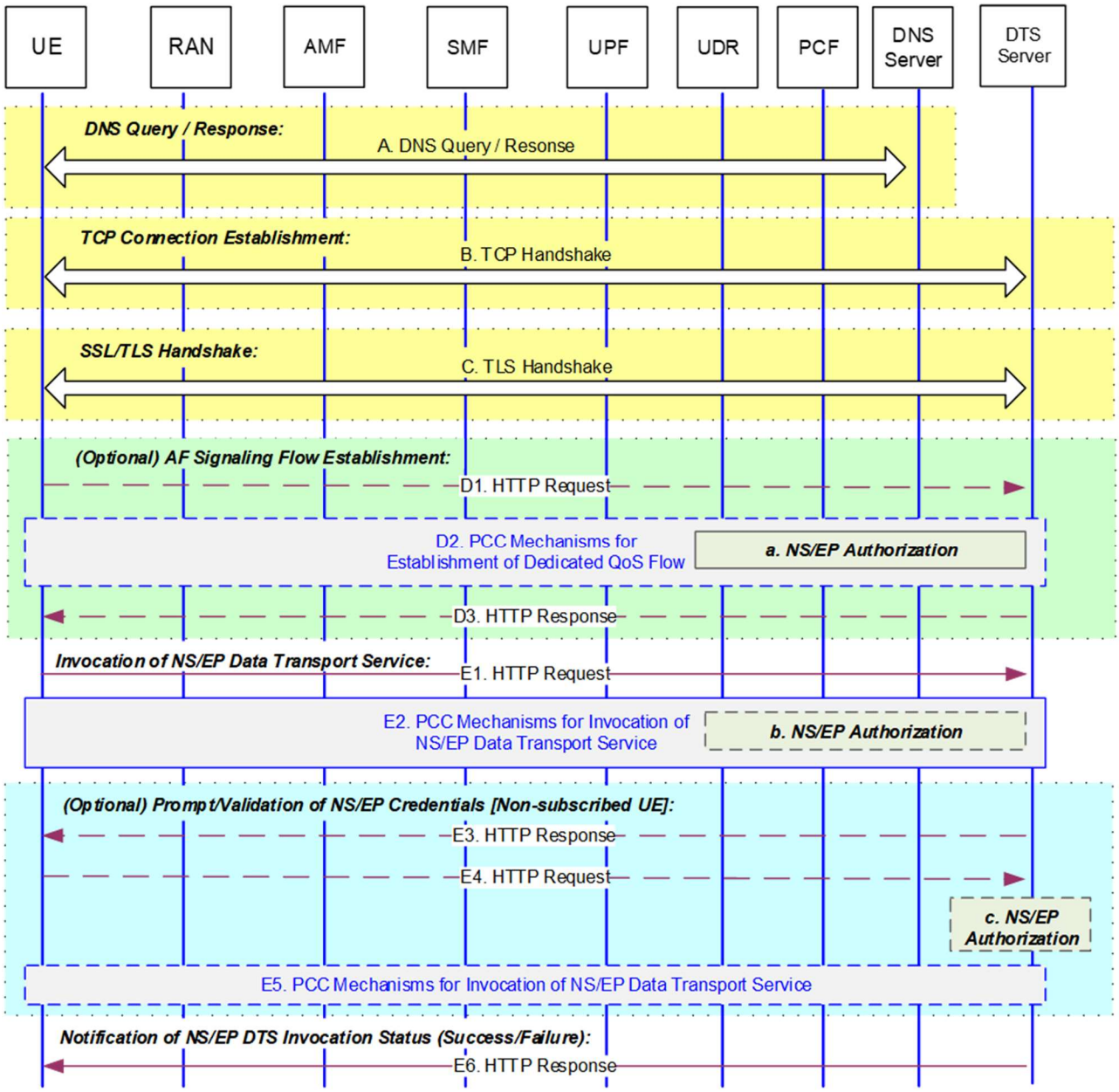

Figure 6-7. Illustrative Service Request Flow (for HTTPS-based Service Invocation)

6.3.5.1 DNS Query and Response

For the scenario illustrated in Figure 6-7, the Service User enters a Service Provider-specific URL to invoke the NS/EP Data Transport Service via the Service Provider's DTS Server. Before the UE establishes a TCP connection with the DTS Server, and subsequently exchanges HTTPS requests and responses with the DTS Server, the UE must determine the DTS Server's IP address. In this example, the UE generates a query to a DNS Server, to translate the URL to an IP address of the Service Provider's DTS Server. These steps can be eliminated, if the IP address of the DTS Server is entered directly in the URL bar of the web browser, or is provided by an NS/EP Application on an NS/EP-subscribed UE.

NOTE: Figure 6-7 assumes that the DNS query and response are transported via User Datagram Protocol (UDP). If TCP is instead used, a TCP connection is established between the UE and the DNS Server prior to exchanging the DNS query and response (between the UE and a DNS Server).

The increasing adoption of DNS over HTTPS (DoH) deployments (i.e., via modern web browsers) could potentially complicate the implementation of the NS/EP Data Transport Service. This TR assumes that the Service User is responsible for configuring / disabling DoH, as necessary to adhere to use of the Service Provider's designated DNS Server.

6.3.5.2 TCP Connection Establishment

Before a UE attempts to connect with the DTS Server, the UE establishes a TCP connection to the DTS Server, by initiating a handshake as illustrated in Figure 6-7. Upon completion of this handshake, both the UE and DTS Server have received an acknowledgment of the TCP connection, thus enabling full-duplex communication.

6.3.5.3 SSL/TLS Handshake

The TLS protocol provides privacy and data integrity between the UE and the DTS Server, in order to prevent eavesdropping and tampering. A SSL/TLS handshake is used to establish a secured connection for an HTTPS exchange between the UE and the DTS Server (RFC 2818, *HTTP Over TLS* [Ref 20]). TLS uses symmetric cryptography to encrypt the data transmitted between the UE and the DTS Server, to ensure the connection is private (secure). The keys for this symmetric encryption are generated based on a shared secret that is negotiated via a TLS handshake in a secure and reliable manner. The UE and the DTS Server negotiate the details of which encryption algorithm and cryptographic keys to use prior to initiating the secure data transmission.

Applications can communicate either with or without TLS (or SSL). For the example use case as illustrated in Figure 6-7, the UE indicates the setup of a TLS connection to the DTS Server (e.g., via the use of port 443). The UE and the DTS Server then use the handshaking procedure to agree on various parameters used to establish the connection's security. The specific messages exchanged between the UE and the DTS Server during the TLS handshake vary based on the key exchange algorithm that is used and the supported cipher suites. The protocols use a handshake with an asymmetric cipher to establish not only cipher settings but also a session-specific shared key that enables encryption of further communication using a symmetric cipher. Upon completion of the SSL/TLS handshake, the secured connection begins. The UE and the DTS Server use the session keys to encrypt and decrypt the data they exchange and to validate the integrity of the data.

Upon completion of the SSL/TLS handshake, the UE and the DTS Server are able to exchange HTTPS messages using the secured connection, as discussed in the following clauses.

6.3.5.4 HTTP Message Exchange – without Subsequent Entry of NS/EP Credentials

The following material describes an example of DTS invocation without entry of NS/EP credentials. First, an optional AF Signalling Flow is established to support priority signalling between an NS/EP-subscribed UE and the DTS Server (depicted in steps D1 through D3), followed by a single HTTP request / response pair that supports the required interactions between the UE and the DTS Server:

E1. For the scenario illustrated in Figure 6-7, the **HTTP request** is sent from the UE to the DTS Server to request the invocation of the NS/EP Data Transport Service.

E2. The DTS Server initiates PCC interactions with the PCF to invoke the NS/EP Data Transport Service. The DTS Server generates an N5 interface message to initiate the required actions, as described in Clause 6.3.6. In the PCC request, the DTS Server instructs the PCF whether to verify that the UE is authorized for the NS/EP Data Transport Service.

> NOTE: The optional establishment of an AF Signalling Flow includes an NS/EP subscription check by the PCF to authorize the UE (depicted as NS/EP Authorization option "a" in Figure 6-7). If this authorization was already completed (in step D2) prior to invocation of the NS/EP Data Transport Service, the DTS Server instructs the PCF to invoke the NS/EP Data Transport Service without requesting further authorization of the UE in step E2. Otherwise, the DTS Server instructs the PCF to authorize the UE as an integral part of the NS/EP Data Transport Service invocation procedures.

Assuming an appropriate event notification is reported from the PCF to the DTS Server after successful invocation of the NS/EP Data Transport Service (as illustrated in step 21 of Figure 6-8), processing continues as indicated in step E6.

NOTE: If the DTS Server is notified (in step E2) that the UE is not authorized for the NS/EP Data Transport Service, the DTS Server may optionally prompt the user to enter NS/EP credentials in order to treat the request in the same manner as applicable to a non-NS/EP-subscribed UE. This involves processing as illustrated in steps E3 through E5 of Figure 6-7, including authorization of the UE as depicted for NS/EP Authorization option "c". These procedures are described in Clause 6.3.5.5.

E6. Assuming successful invocation of the NS/EP Data Transport Service, the DTS Server notifies the Service User that the requested service has been invoked successfully.

6.3.5.5 HTTP Message Exchange – with Subsequent Entry of NS/EP Credentials

The Service User may use a browser to interact with the DTS Server. If the UE is not subscribed to NS/EP service and does not have access to a special DTS application, multiple HTTP request / response pairs can be used to accomplish the required UE interactions to enable the DTS Server to collect NS/EP credentials and other required information from the Service User, as described below.

E1. The UE's browser sends an **HTTP request**, containing the URL associated with the DTS Server, to request the invocation of the NS/EP Data Transport Service.

E2. The DTS Server may generate a PCC request for invocation of the NS/EP Data Transport Service, as described in Clause 6.3.5.4.

NOTE: If the DTS Server needs to provide differentiated treatment for NS/EP-subscribed UEs vs. non-NS/EP-subscribed UEs based on a common HTTP request, the DTS Server may generate a PCC request (as described in step E2). If the UE is authorized (as applicable for an NS/EP-subscribed UE), this results in the successful invocation of the NS/EP Data Transport Service, as described in Clause 6.3.5.4. If the DTS Server is instead notified that the UE is not authorized, the DTS Server assumes that the UE is not subscribed to NS/EP, and proceeds as described in step E3, below.

E3. The DTS Server sends an **HTTP response**, containing a message body that provides an HTML document used to prompt the Service User for NS/EP credentials (plus other information as described below in step E4). This HTML document provides a form, to present the Service User with a page that displays a number of user interface widgets, such as text fields and pulldown menus, along with a submit button.

E4. The Service User interacts with the widgets in some manner, e.g., by selecting whether DTS invocation or DTS revocation is desired, filling in any required NS/EP credentials, and then clicking the submit button. At this point, the UE's browser takes the current values of all the widgets, builds a string that carries their values, and constructs an **HTTP request** to the DTS Server.

The DTS Server accesses an NS/EP database to validate the NS/EP credentials received from the Service User, as depicted for NS/EP Authorization option "c" in Figure 6-7.

E5. Assuming the request is authorized, the DTS Server initiates the required PCC actions, as described in Clause 6.3.6.

E6. Assuming an appropriate event notification is reported from the PCF to the DTS Server after successful invocation of the NS/EP Data Transport Service (as illustrated in step 21 of Figure 6-8), the DTS Server then sends an **HTTP response**, containing a message body that provides an HTML document that can be rendered and displayed to the Service User (to indicate that the requested service has been invoked successfully).

6.3.6 PCC Mechanisms for Invocation of the NS/EP Data Transport Service

This clause illustrates PCC procedures (triggered by the DTS Server) and associated QoS Flow modification procedures associated with invocation of the NS/EP Data Transport Service. Figure 6-8 illustrates PCC procedures used to enable priority treatment for the transport of data traffic via the Default QoS Flow, in conjunction with the successful invocation of the NS/EP Data Transport Service. This TR assumes that the HTTP invocation request, as described in Clauses 6.3.5.4 and 6.3.5.5, is sent from the UE to a DTS Server via the Designated PDU Session,

with the intent to upgrade the QoS of the Default QoS Flow for that same PDU Session, and to adjust PCC rules that are mapped to that Default QoS Flow. This is discussed further in Clause 7.1.6.

Steps 1 through 4 of Figure 6-8 illustrate the messages exchanged over the N5 interface [Ref 10] (between the DTS Server and the PCF) and over the N7 interface [Ref 8] (between the PCF and the SMF).

Steps 5 through 18 of Figure 6-8 illustrate the invocation of QoS Flow Modification procedures, used to enable priority treatment for the subsequent transport of data traffic over the Default QoS Flow.

Steps 19 through 22 pertain to the notification event from the SMF to the PCF, and on to the DTS Server, based on success of the attempted invocation of the NS/EP Data Transport Service.

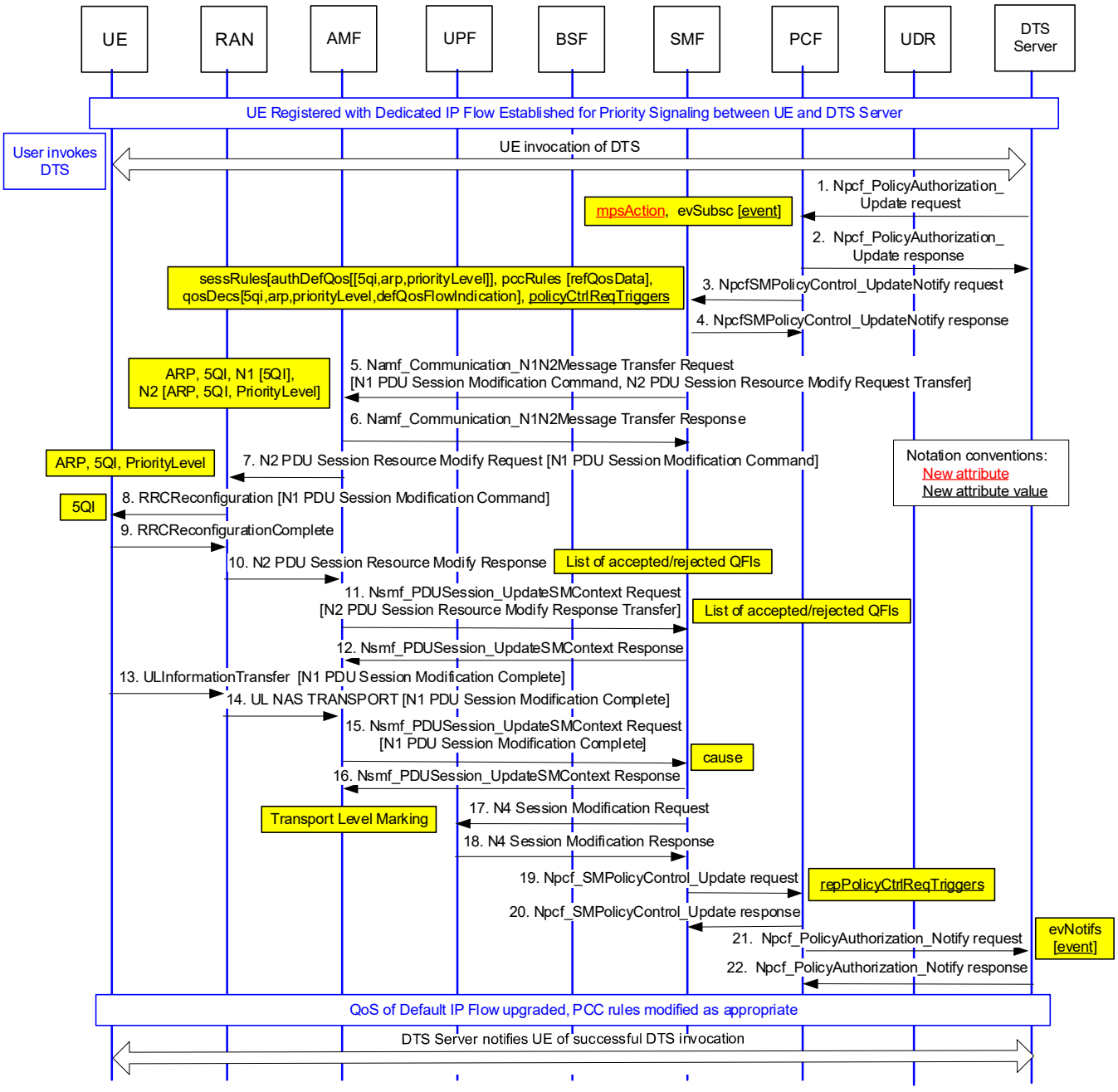

Figure 6-8. NS/EP Data Transport Service Invocation - PCC Interactions

This procedure assumes that an N5 session was established previously, to establish an AF Signalling Flow for priority signalling between the UE and the DTS Server, as described in Clause 6.3.4. In this case, the NS/EP Data Transport Service authorization was already performed by the PCF as illustrated in steps 4 and 5 of Figure 6-6. Alternate procedures for authorizing the NS/EP Data Transport Service, as applicable to other use cases, are described in Clause 7.1.4.

NOTE: If the N5 session is instead established at the time that the NS/EP Data Transport Service is invoked, the **Npcf_PolicyAuthorization_Update** service in steps 1 and 2 of Figure 6-8 would be replaced with the **Npcf_PolicyAuthorization_Create** service, which would include the exchange of the suppFeat attribute to indicate that the "MPSforDTS" feature number is supported by the PCF and the DTS Server and would include the dnn attribute to identify the Designated DNN.

The DTS Server includes the mpsAction attribute in the **Npcf_PolicyAuthorization_Update request** in step 1 of Figure 6-8 to invoke the NS/EP Data Transport Service. Assuming the Service User has already been authorized, the DTS Server sets the mpsAction attribute value to "ENABLE_MPS_FOR_DTS," to trigger the PCF to upgrade the QoS of the Default QoS Flow within the Designated PDU Session, without further authorization by the PCF.

NOTE: The DTS Server sets the mpsAction attribute value to "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS" to indicate that the PCF should verify that the UE is authorized for the NS/EP Data Transport Service prior to upgrading the QoS of the Default QoS Flow and associated PCC rules.

The DTS Server also includes the evSubsc attribute in the **Npcf_PolicyAuthorization_Update request**, populated with the event attribute including values "SUCCESSFUL_QOS_UPDATE" and "FAILED_QOS_UPDATE" to request notification when the request has been processed successfully or has failed. The medComponents attribute is not included.

When the PCF receives the **Npcf_PolicyAuthorization_Update request**, the PCF recognizes that the request is associated with an NS/EP Data Transport Service invocation, based on the inclusion of the mpsAction attribute set to the value "ENABLE_MPS_FOR_DTS" or "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS".

NOTE: When the mpsAction attribute value "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS" is received by the PCF, the PCF retrieves the subscriber's subscription related information from the UDR, using the Nudr_DataRepository API for policy data, as specified in TS 29.519 [Ref 12]. The UDR provides the smPolicyDnnData attribute, which contains the mpsPriority attribute to indicate whether the subscription supports MPS and the mpsPriorityLevel attribute to provide the relative priority level for MPS. The PCF uses the mpsPriority attribute to determine whether the UE is authorized for NS/EP Data Transport Service. If the request is not authorized, the PCF sends an HTTP "403 Forbidden" response message to the DTS Server, including the cause attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

The PCF derives the QoS values of the Default QoS Flow as appropriate for the NS/EP Data Transport Service and sends an **NpcfSMPolicyControl_UpdateNotify request** to the SMF, including the arp, 5qi, and optional priorityLevel attributes in the authDefQos attribute for the Session Rule, to indicate the appropriate priority treatment that should be applied for the Default QoS Flow. The PCF also modifies the dynamic PCC rules that have the same ARP, 5QI, and optional Priority Level values as were previously assigned to the Default QoS Flow. The PCF may set the defQosFlowIndication attribute, to accomplish a binding of the corresponding PCC rules to the Default QoS Flow. Alternatively, the PCF may explicitly change the arp, 5qi, and optional priorityLevel attributes associated with the pccRules attribute for the PCC Rules, as discussed in Clause 7.1.9.

NOTE: Clause 7.1.12 discusses the assignment of 5QI* value(s) for the NS/EP Data Transport Service.

Based on inclusion of the evSubsc attribute with the event attribute set to "SUCCESSFUL_QOS_UPDATE" in the **Npcf_PolicyAuthorization_Update request** from the DTS Server (in step 1), the PCF also requests the SMF to confirm that the resources associated to the Default QoS Flow and PCC rules mapped to the Default QoS Flow are successfully updated, by including the policyCtrlReqTriggers attribute with the value "SUCC_QOS_UPDATE" in the **NpcfSMPolicyControl_UpdateNotify request**. The SMF responds to the PCF with an **NpcfSMPolicyControl_UpdateNotify** response which indicates the **NpcfSMPolicyControl_UpdateNotify request** was received and understood by the PCF, but does not imply that the requested actions were taken.

When the SMF receives the **NpcfSMPolicyControl_UpdateNotify request**, it invokes QoS Flow Modification procedures to modify the QoS characteristics of the Default QoS Flow, based on the authDefQos attribute received

from the PCF for the Session Rule. To support binding or mapping of other flows to the Default QoS Flow, the SMF uses the received defQosFlowIndication attribute to trigger binding of the designated PCC rules to the Default QoS Flow, or the arp, 5qi, and optional priorityLevel attributes associated with the pccRules attribute to update these QoS values of the PCC rules. The SMF responds to the PCF with the **NpcfSMPolicyControl_UpdateNotify response** which indicates the **NpcfSMPolicyControl_UpdateNotify request** was received and understood by the SMF, but does not imply that the requested actions were taken in the 5GC and RAN.

The SMF sends an **Namf_N1N2Message Transfer Request** to the AMF (as specified in TS 29.518 [Ref 11]) to the AMF in step 5, containing information pertaining to the N2 **PDU Session Resource Modify Request** and the N1 **PDU Session Modification Command**. The AMF sends an N2 **PDU Session Resource Modify Request** (as specified in TS 38.413 [Ref 17]) to the RAN in step 7, containing the assigned ARP, 5QI, and Priority Level values for the QoS Flow. The assigned 5QI value for the QoS Flow is sent to the UE via the RAN in a **PDU Session Modification Command** (as specified in TS 24.501 [Ref 4]) in step 8. Further details concerning the overall PDU Session Modification flow are provided in Clause 4.3.3 of TS 23.502 [Ref 3].

Figure 6-8 includes messages used to support a notification to the DTS Server, based on the outcome of the attempted invocation of the NS/EP Data Transport Service. This reporting is triggered by the DTS Server's inclusion of the evSubsc attribute with the event attribute set to "SUCCESSFUL_QOS_UPDATE" in the **Npcf_PolicyAuthorization_Update request** (in step 1).

Assuming that the desired actions as requested by the mpsAction attribute (i.e., QoS updates of the Default QoS Flow plus PCC rules that are mapped to the Default QoS Flow) are successfully completed, the SMF sends a **Session Modification Request** to the UPF (in step 17 of Figure 6-6) to update Packet Detection Rules in the UPF. The SMF then sends an **NpcfSMPolicyControl_Update request** to the PCF in step 19, including the repPolicyCtrlReqTriggers attribute set to "SUCC_QOS_UPDATE", to notify the PCF of the successful completion of the requested actions (as previously requested by the **NpcfSMPolicyControl_UpdateNotify request** as illustrated in step 3). Based on this event notification, the PCF informs the DTS Server by sending an **Npcf_PolicyAuthorization_Notify request** in step 21, with the event attribute in the evNotifs attribute set to the value "SUCCESSFUL_QOS_UPDATE."

When the DTS Server is informed of successful invocation of the NS/EP Data Transport Service via the **Npcf_PolicyAuthorization_Notify request** with the event attribute in the evNotifs attribute set to "SUCCESSFUL_QOS_UPDATE" from the PCF, it initiates procedures to notify the UE that the NS/EP Data Transport Service has been successfully invoked.

> NOTE: If the QoS of the Default QoS Flow fails to be updated successfully, this is reported by the SMF to the PCF in accordance with Clause 4.2.4.21 of TS 29.512 [Ref 8]. If the DTS Server included the evSubsc attribute with the event attribute set to "FAILED_QOS_UPDATE" in the **Npcf_PolicyAuthorization_Update request** (in step 1), the PCF informs the DTS Server by sending an **Npcf_PolicyAuthorization_Notify request** with the event attribute in the evNotifs attribute set to the value "FAILED_QOS_UPDATE". The DTS Server notifies the UE accordingly.

6.3.7 HTTPS-based Revocation of the NS/EP Data Transport Service

Figure 6-9 illustrates PCC procedures used to disable priority treatment for the transport of data traffic over the Default QoS Flow, in conjunction with the successful revocation of the NS/EP Data Transport Service.

Steps 1 through 4 of Figure 6-9 illustrate the messages exchanged over the N5 interface [Ref 10] (between the DTS Server and the PCF) and over the N7 interface [Ref 8] (between the PCF and the SMF).

Steps 5 through 18 of Figure 6-9 illustrate the PDU Session Modification procedures, used to disable priority treatment for the subsequent transport of data traffic over the Default QoS Flow.

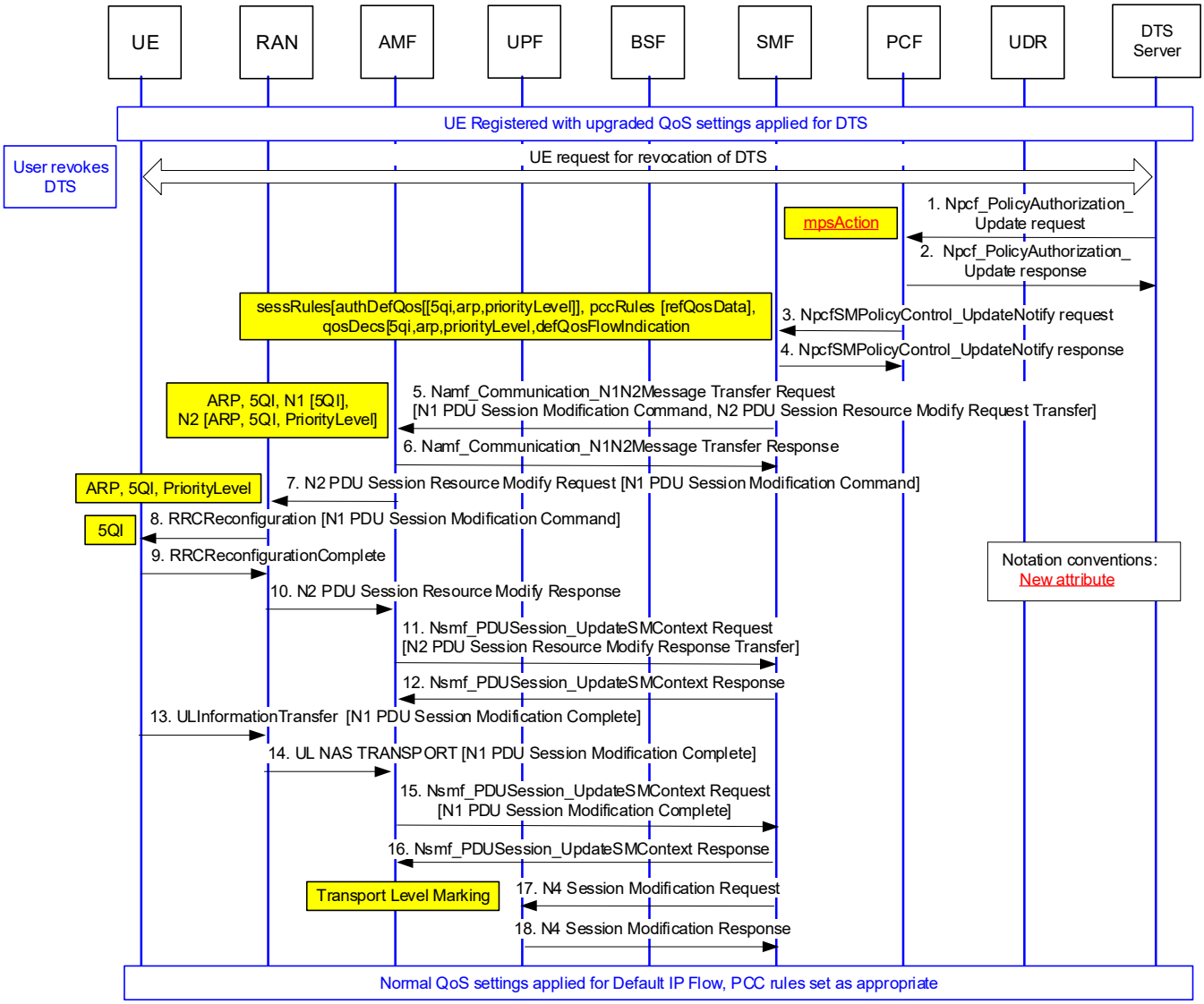

Figure 6-9. NS/EP Data Transport Service Revocation - PCC Interactions

Figure 6-9 contains the same sequence of messages as illustrated in Figure 6-8, but excludes the (optional) event notification.

Steps 1 through 4 of Figure 6-9 illustrate the messages exchanged over the N5 interface (between the DTS Server and the PCF) and over the N7 interface (between the PCF and the SMF). The DTS Server includes the mpsAction attribute in the **Npcf_PolicyAuthorization_Update request** in step 1 of Figure 6-9 to revoke NS/EP Data Transport Service. The mpsAction attribute value "DISABLE_MPS_FOR_DTS" triggers the PCF to downgrade the QoS of the Default QoS Flow within the Designated PDU Session, without further authorization by the PCF.

When the PCF receives the **Npcf_PolicyAuthorization_Update request** and recognizes that the request is associated with an NS/EP Data Transport Service revocation, the PCF indicates the appropriate priority treatment that should be applied for the Default QoS Flow by restoring appropriate values for the arp, 5qi, and optional priorityLevel attributes in the authDefQos attribute for the Session Rule.

> NOTE: This may require more complex logic on the part of the PCF, beyond simply restoring the prior ARP and 5QI* values as set prior to invocation of the NS/EP Data Transport Service, if these values and/or the defQosFlowIndication attribute value were modified by another service during the time that the NS/EP Data Transport Service was enabled. Similarly, the PCF may require more complex logic, beyond simply restoring the PCC rules as set prior to invocation of the NS/EP Data Transport Service. The corresponding logic is dependent on the identification of particular services that may be deployed, and the desired interactions between the NS/EP Data Transport Service and any such services. These aspects are not considered in this TR.

The PCF also modifies the 5QI* and ARP values for the dynamic PCC rules that were previously modified during invocation of the NS/EP Data Transport Service (based on having the same 5QI* and ARP as the Default QoS Flow, as discussed in Clause 6.3.6), by setting the defQosFlowIndication attribute to remove the previous binding to the Default QoS Flow for the corresponding PCC rules, and by setting the arp, 5qi, and optional priorityLevel attributes associated with the pccRules attribute for the PCC Rules, as discussed in Clause 7.1.9.

The PCF sends an **NpcfSMPolicyControl_UpdateNotify request** to the SMF, to indicate the appropriate treatment that should be applied for the Default QoS Flow and for the dynamic PCC rules, as described above. The SMF responds to the PCF with an **NpcfSMPolicyControl_UpdateNotify response**.

When the SMF receives the **NpcfSMPolicyControl_UpdateNotify request**, it invokes QoS Flow Modification procedures to modify the QoS characteristics of the Default QoS Flow, based on the authDefQos attribute received from the PCF for the Session Rule. The SMF also restores other flows that were bound or mapped to the Default QoS Flow when the NS/EP Data Transport Service was previously invoked, based on the received defQosFlowIndication, arp, 5qi, and optional priorityLevel attributes associated with the pccRules attribute.

The SMF sends an **Namf_N1N2Message Transfer Request** to the AMF (as specified in TS 29.518 [Ref 11]) to the AMF in step 5, containing binary information pertaining to the N2 **PDU Session Resource Modify Request** and the N1 **PDU Session Modification Command**. The AMF sends an N2 **PDU Session Resource Modify Request** (as specified in TS 38.413 [Ref 17]) to the RAN in step 7, containing the assigned ARP, 5QI, and Priority Level values for the QoS Flow. The assigned 5QI value for the QoS Flow is sent to the UE via the RAN in a **PDU Session Modification Command** (as specified in TS 24.501 [Ref 4]) in step 8. Further details concerning the overall PDU Session Modification flow are provided in Clause 4.3.3 of TS 23.502 [Ref 3].

6.3.7.1 TCP Connection Release

When their communication is complete, the UE and DTS Server release the TCP connection, to free the resources for other uses.

6.3.8 Removal of AF Signalling Flow Previously Established for Priority Signalling between UE and DTS Server

Various mechanisms can be used to trigger the removal of the AF Signalling Flow between the UE and the DTS Server. Symmetrical procedures are recommended for the establishment and removal of the AF Signalling Flow. For example, assuming that the AF Signalling Flow was established when the Service User activated (opened) the special DTS application on their UE, that AF Signalling Flow may persist until the user closes that DTS application. For this use case, when the DTS application is closed, the DTS Server is notified that no further NS/EP Data Transport Service actions are needed. When the DTS Server receives this notification from the UE, the DTS Server closes the N5 session by sending an **Npcf_PolicyAuthorization_Delete request** to the PCF, which is acknowledged with an **Npcf_PolicyAuthorization_Delete response**, as described in Clause 5.2.2.2.2.3 of TS 29.513 [Ref 9].

> NOTE: If the DTS Server decides to remove the AF Signalling Flow between the UE and the DTS Server, but decides to retain the N5 session, the DTS Server sends an **Npcf_PolicyAuthorization_Update request** that contains the fStatus attribute set to the value "REMOVED" within the media subcomponent containing the AF signalling IP flow, as specified in Clause 4.2.3.17 of TS 29.514 [Ref 10].

7. Analysis and Recommendations

7.1 Analysis

The following subclauses provide further analysis pertaining to key topics for the NS/EP Data Transport Service. All the needed functionality has been included in 3GPP Release 17 at the time of completion of this TR.

7.1.1 Relationship to 3GPP Priority PDU Connectivity Service

The NS/EP Data Transport Service builds upon functionality as specified in Clause 4.2.6.2.12.2 of TS 29.512 [Ref 8] for the Priority PDU Connectivity Service. This functionality applies appropriate updates to the ARP and 5QI* values assigned to the Default QoS Flow within the Designated PDU Session, and also modifies the settings for particular PCC rules (with the same 5QI* and ARP as the Default QoS Flow), by binding those PCC rules to the Default QoS Flow or by setting the ARP and 5QI* of those particular PCC rules to the updated ARP and 5QI* values. This TR proposes the following extensions and clarifications, and specific usage of Priority PDU Connectivity Service capabilities, as applicable for the NS/EP Data Transport Service:

- It introduces the mpsAction attribute to explicitly support the dynamic on demand invocation and revocation of NS/EP Data Transport Service in a 3GPP-specified manner, as described further in Clause 7.1.8.
- It assumes that when the DTS Server invokes an **Npcf_PolicyAuthorization** service operation for invocation of the NS/EP Data Transport Service, the DTS Server optionally requests the PCF to check whether the originating UE is authorized as an NS/EP-subscribed UE. The DTS Server selects an appropriate authorization mechanism for the NS/EP Data Transport Service, as discussed in Clause 7.1.4.
- It extends the PCC event notification capabilities, to enable the DTS Server to receive a success or failure indication pertaining to invocation/revocation of the NS/EP Data Transport Service, which the DTS Server uses to notify the originating Service User of this event. These extensions are described in Clause 7.1.10.
- It enables the establishment of an AF Signalling Flow to support priority signalling between the UE and the DTS Server, as described in Clause 7.1.2.
- It extends the suppFeat attribute, to support the "MPSforDTS" feature.

7.1.2 Priority Signalling between the UE and the DTS Server

A DTS Server interacts with the UE to control the dynamic invocation and revocation of the NS/EP Data Transport Service. The messages exchanged between the UE and the DTS Server would normally be transported via the Default QoS Flow. However, the exchange of these messages over the Default QoS Flow may be hampered during congestion, since the QoS of the Default QoS Flow is not upgraded until the NS/EP Data Transport Service is successfully invoked, i.e., after the HTTPS request(s) in Figure 6-7 are processed and corresponding procedures as illustrated in Figure 6-8 of Clause 6.3.6 are successfully completed.

In order to support communications between the UE and the DTS Server when network congestion is experienced, an AF Signalling Flow is established to support priority signalling between the UE and the DTS Server. This AF Signalling Flow may result in the establishment of a new Dedicated QoS Flow, as illustrated in Clause 5.3. This capability may be useful for selected use cases as described in Clause 6.1. Clause 6.3 includes sub-flows that illustrate the establishment of an AF Signalling Flow for this priority signalling prior to the invocation of the NS/EP Data Transport Service, as may be applicable to particular use case scenarios.

Priority signalling between the UE and the DTS Server can be established:

[a] at the time a PDU Session is established;

[b] when the user activates (opens) a DTS application on their UE; or

[c] when the user invokes NS/EP Data Transport Service.

> NOTE: This capability is only applicable for NS/EP subscribed UEs, since it relies on PCF retrieval of the subscriber's subscription related information (i.e., the mpsPriority attribute) from the UDR to trigger the AF Signalling Flow establishment procedures with option [a], or to authorize the AF Signalling Flow establishment request with options [b] and [c].

Option [a] is described in Clause 6.3.3.2. Options [b] and [c] make use of procedures based on Clause 4.2.2.12.3 of TS 29.514 [Ref 10], as described in Clause 6.3.4.

> NOTE: The DTS Server needs to include the mpsId attribute for either option [b] or [c].

> NOTE: The resPrio attribute may be used to indicate the Service User's priority level. However, no PCF distinctions based on Service User priority level have been identified, so this attribute is not required based on the analysis in this TR.

Option [a]: Establishment of priority signalling between the UE and the DTS Server at the time a PDU Session is established

Clause 6.3.3.2 describes the potential establishment of a Service Data Flow from the UE towards the DTS Server at the time of PDU Session establishment, to carry priority AF signalling traffic between the UE and the DTS Server for supporting the NS/EP Data Transport Service. To accomplish these actions, an appropriate Dedicated QoS Flow (with appropriate 5QI* and ARP values) may be established to provide priority access to a DTS Server. This requires PCF configurations to support the following functionality:

- The PCF must be configured with appropriate NS/EP ARP and 5QI* values for the PCC rule(s) that are used for establishing the Dedicated QoS Flow for DTS signalling on the Designated PDU Session.

  NOTE: This functionality is in addition to Advance Priority procedures used to set an upgraded ARP for the Default QoS Flow of the Designated PDU Session, as discussed in Clause 6.3.3.1.

- The PCF must be able to trigger the Dedicated QoS Flow establishment procedures. During the Advance Priority procedures, this can be triggered by the PCF via the mpsPriority attribute that the PCF retrieves from the UDR in step 11 of Figure 6-5.

- The PCF needs the IP addresses of the UE and the DTS Server to identify the signalling flow between the UE and the DTS Server.

  NOTE*:* The PCF uses this information to populate the flowInfos attribute in the **SMPolicyControl_Create response** as illustrated in step 12 of Figure 6-5.

Since communications have not yet been established between the PCF and the DTS Server at the time of PDU Session establishment, the PCF must determine the IP address of the DTS Server. A fixed IP address of the DTS Server can be pre-configured in the PCF for this purpose. Alternatively, the PCF may generate a query to a DNS Server, to translate a URL to an IP address of the DTS Server.

NOTE: Option [a] is only applicable to NS/EP-subscribed UEs.

Option [b]: Establishment of priority signalling between the UE and the DTS Server when the user activates a DTS application on their UE

Option [b] is illustrated in sub-flows E and F of Clause 6.2.2. In sub-flow E, the Service User activates (opens) the special DTS application, which causes a UE request to establish priority AF signalling with the DTS Server. This request triggers the DTS Server to initiate the corresponding PCC interactions, as illustrated in sub-flow F. For the PCC interactions as described in Clause 6.3.4, an AF Signalling Flow is established for priority signalling between the UE and the DTS Server. This procedure is specified in Clause 4.2.2.12.3 of TS 29.514 [Ref 10]. The DTS Server includes the mpsId attribute in the **Npcf_PolicyAuthorization_Create request** that it sends to the PCF, as illustrated in step 3 of Figure 6-6.

NOTE: Option [b] is only applicable to UEs with the associated DTS application.

Option [c]: Establishment of priority signalling between the UE and the DTS Server when the user invokes NS/EP Data Transport Service

For option [c], the DTS Server initiates PCC procedures to establish an AF Signalling Flow for subsequent priority signalling after it receives a request to invoke the NS/EP Data Transport Service. This provides more limited benefits than options [a] or [b], since it does not help with the establishment of the TCP connection and SSL/TLS handshake procedure (as illustrated in steps B and C of Figure 6-7), but only helps for HTTP transfers after the HTTP connection has been established.

- For a UE that invokes the NS/EP Data Transport Service via a browser as illustrated in Clause 6.2.1, the DTS Server may initiate PCC procedures to establish an AF Signalling Flow for subsequent priority signalling after it receives the invocation request (in step E1 of Figure 6-7). This would result in priority

treatment only for subsequent HTTP message(s) as illustrated in Figure 6-7.

- For a UE that uses a special DTS application as illustrated in Clause 6.2.2, only a single HTTP request is required within the HTTP interactions, as described in Clause 6.3.5.4. Thus, establishing the AF Signalling Flow upon receipt of the initial HTTP request would provide no value.

The specific option(s) need to be chosen by the Service Provider, consistent with the specific use case(s) that are deployed.

7.1.3 Mechanism used for UE interactions with DTS Server

A variety of mechanisms can be used to invoke and revoke NS/EP Data Transport Service. Whereas the specific mechanisms and details concerning particular interactions are considered to be implementation and deployment choices, this TR considers two general types of mechanisms that can be used: use of a UE browser to access the DTS Server and use of a special DTS application that is installed on the UE to facilitate the Service User's access to the DTS Server.

Further assumptions and considerations, as applicable to each of these mechanisms, are described in Clause 6.1.

7.1.4 Authorization Mechanism(s) for the NS/EP Data Transport Service

The NS/EP Data Transport Service must support authentication of the originating Service User (or the NS/EP-subscribed UE) and the ability to verify that the originator is authorized to invoke the NS/EP Data Transport Service. The specific mechanism(s) used to support this functionality should be chosen based on detailed security assessments that consider the specific security objectives established by particular Service Providers in consultation with the designated government agency for the NS/EP Data Transport Service. This clause describes mechanisms that may apply for the use cases as described in Clauses 6.2.1 and 6.2.2.

Authorization for NS/EP-Subscribed UE

For authorization of NS/EP-subscribed UEs in a non-roaming scenario, this TR assumes that the source IP address, as received by the DTS Server in the IP header of the AF Signalling establishment request or DTS invocation request, is used to route the request from the DTS Server to the correct PCF, and to identify the specific UE. To support this assumption, there should be no Network Address Translation (NAT) of the UE's IP address between the UPF and the DTS Server. If the packets went through any HTTP proxies between the UPF and DTS Server, the “forwarded” field should be included in the HTTP header, as specified in RFC 7239, *Forwarded HTTP Extension* [Ref 21], to enable the DTS Server to retrieve the original UE IP address.

The use case as described in Clause 6.2.2 assumes that the PCF is used to authorize the NS/EP-subscribed UE for the NS/EP Data Transport Service. When the DTS Server requests the PCF to establish an AF Signalling Flow, authorization of the NS/EP-subscribed UE is an integral part of the PCF's processing of the **Npcf_PolicyAuthorization_Create** service operation, as illustrated in steps 3 and 4 of Figure 6-6. When the DTS Server requests the PCF to invoke the NS/EP Data Transport Service, the DTS Server indicates whether the PCF should first authorize the DTS invocation request, as an integral part of the PCF's processing of the **Npcf_PolicyAuthorization_Create** or **Npcf_PolicyAuthorization_Update** service operation, as illustrated in steps 1 and 2 of Figure 6-8.

Authorization for Non-NS/EP-Subscribed UE

For the browser-based mechanism as discussed in Clauses 6.2.1 and 6.3.5.5, the Service User enters NS/EP-specific user credentials into an HTML form that is sent to the DTS Server. These credentials are maintained in a logical NS/EP credentials database, which can be collocated with the DTS Server or accessed remotely. The DTS Server must be able to reliably access the NS/EP credentials data in an appropriate manner, which may be tailored for the specific use cases and deployment options that are chosen by the Service Provider. The specific architecture used to support this functionality is not specified in this TR.

When the DTS Server requests the PCF to invoke or revoke the NS/EP Data Transport Service after having already authorized the non-NS/EP subscribed UE (as discussed above), the DTS Server requests the PCF to process the **Npcf_PolicyAuthorization_Create request** or **Npcf_PolicyAuthorization_Update request** (as illustrated in steps 1 and 2 of Figure 6-8) without any further authorization of the DTS invocation request.

Composite Procedures for UE Authorization

Assuming the use of a common URL (or IP address) to access the DTS Server for both NS/EP subscribed UEs and non-NS/EP subscribed UEs, the DTS Server may perform UE authorization as follows: The DTS Server first applies the procedure as described above for an NS/EP-subscribed UE. If successful, the UE is determined to be an authorized NS/EP subscribed UE. However, if the PCF notifies the DTS Server that the UE is not authorized, the DTS Server then applies the corresponding procedure as applicable for a non-NS/EP subscribed UE. This two-step process is shown in Clause 6.2.1.

7.1.5 Access to DTS Server

The selection of a particular DTS Server by the UE (and routing of messages to that DTS Server) can be based on [a] configuration of specific IP address(es) for the DTS Server, or [b] assignment of unique URL for the DTS Server.

Clause 6.1 considers option [a] in the context of a use case involving a UE that is configured with a special DTS application, and option [b] in the context of a use case involving the invocation of the NS/EP Data Transport Service via a web browser. Other potential use cases can be pursued.

> NOTE: For option [a] (where the DTS Server's IP address is stored in the DTS application), if the DTS application is unable to successfully access the DTS Server via its IP address, it may subsequently attempt to access the DTS Server via a URL.

To facilitate the ability of the DTS Server to authorize a DTS request received from a UE, and to support subsequent PCC interactions with a PCF serving that UE, the use of a Service Provider-specific URL is recommended, to enable the DTS invocation request to be routed to a DTS Server for the Service Provider to which the UE is subscribed. To support such functionality, the UE should be configured to use a DNS server that is designated by the UE's subscribed Service Provider and can map the Service Provider-specific URL to the IP address assigned to the DTS Server.

A DTS Server supports functionality to authorize DTS requests (via access to information used to validate NS/EP credentials for non-NS/EP-subscribed UEs) and to initiate appropriate N5 signalling towards a PCF. The DTS Server that receives the DTS invocation request is assumed to support the required authorization functionality, and uses the BSF to provide access to the appropriate PCF.

7.1.6 Applicability of NS/EP Data Transport Service to particular PDU Session(s)

This TR assumes that the priority treatment, as applicable upon successful invocation of the NS/EP Data Transport Service, is applicable to traffic carried via the same PDU Session as used to communicate with the DTS Server. The DTS invocation request (and other messages used to support the UE communications with the DTS Server) are assumed to be exchanged over that same PDU Session, as illustrated in Clause 5.2. The priority treatment is associated with that single PDU Session. The DTS Server is assumed to be configured with a DNN value that is used as the Designated DNN for the NS/EP Data Transport Service.

7.1.7 DTS Server / BSF determination of PCF

A BSF may be optionally used to assist the DTS Server in determining the particular PCF used to enable the PCC interactions for the NS/EP Data Transport Service. A BSF supports the selection of an appropriate PCF in case an administrative domain has more than one PCF. The inclusion of a BSF in the architecture is dependent on the option deployed by the Service Provider.

As specified in Clause 4.2.2.2 of TS 29.521 [Ref 13], the **Nbsf_Management_Register** service operation is used to register PCF Session Binding information in the BSF. The BSF obtains PCF Binding information during the establishment of a PDU Session (i.e., based on attributes received by the BSF in the **Nbsf_Management_Register request** from the PCF, as illustrated in step 13 in Figure 6-4 of Clause 6.3.3.1). The PCF Session Binding information maintained by the BSF, as specified in Clause 4.2.2.2 of TS 29.521 [Ref 13], includes the UE's IP address, the DNN, the S-NSSAI, the user identity, and the PCF address for the PDU Session.

The **Nbsf_Management_Discovery** service operation is used to obtain address information of the selected PCF for a PDU session in the BSF. As specified in Clause 4.2.4.2 of TS 29.521 [Ref 13], the **Nbsf_Management_Discovery request** includes the UE's IP address, and may include the UE identity (SUPI or GPSI), the DNN and optionally S-NSSAI, and the IPv4 address domain. The BSF finds the correct PCF by matching information received in the **Nbsf_Management_Discovery request** from the DTS Server (in step 1 of Figure 6-6 in Clause 6.3.4) with the corresponding information stored in the BSF. For the NS/EP Data Transport Service, the DTS Server includes the UE's IP address and the Designated DNN in the **Nbsf_Management_Discovery request**.

7.1.8 Addition of new mpsAction attribute

This TR illustrates the use of the mpsAction attribute (introduced in 3GPP Release 17), with values "ENABLE_MPS_FOR_DTS", "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS", and "DISABLE_MPS_FOR_DTS" for invocation and revocation of the NS/EP Data Transport Service. The DTS Server uses mpsAction attribute value "ENABLE_MPS_FOR_DTS" or "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS" to request invocation of the NS/EP Data Transport Service. If the PCF receives the "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS" value, the PCF will confirm that the UE is an authorized NS/EP subscriber before initiating the requested actions. Use of these values is described further in Clause 6.3.6.

The addition of this new attribute is recommended as a preferred 3GPP-based approach (e.g., rather than the specification of unique values for the mpsId attribute).

> NOTE: The suppFeat attribute is used during establishment of N5 and N7 sessions to indicate support for the NS/EP Data Transport Service functionality, via inclusion of the "MPSforDTS" feature number.

The existing 3GPP mpsId attribute is optional, and is left for specification in particular national standards. 3GPP does not specify values for the mpsId attribute, nor the specific treatment to be applied for related functionality. Thus, if the mpsId attribute was used to invoke and revoke the NS/EP Data Transport Service, the details concerning such functionality would be left to national standardization, and would not achieve the benefits of international standardization.

This TR also describes a new ("AUTHORIZE_AND_ENABLE_MPS_FOR_AF_SIGNALLING") value of the mpsAction attribute, introduced in 3GPP Release 18, which allows the DTS Server to explicitly signal that authorization for the NS/EP Data Transport Service is required for priority AF signalling.

> NOTE: Inclusion of the "AuthorizationForMpsSignalling" feature number in the suppFeat attribute is used to indicate support for the new "AUTHORIZE_AND_ENABLE_MPS_FOR_AF_SIGNALLING" value of the mpsAction attribute.

7.1.9 PCC Mechanism used for Modification of PCC Rules

Two mechanisms have been defined, either of which can be used to adjust the PCC rules that are mapped to the Default QoS Flow, in order to ensure that the ARP, 5QI and optional Priority Level values for those service data flows continue to match the corresponding QoS values as assigned to the Default QoS Flow when the NS/EP Data Transport Service is invoked:

- The PCF can explicitly change the ARP and 5QI* values of the PCC rules to match the new ARP and 5QI* values assigned to the Default QoS Flow by explicitly setting the arp, 5qi, and optional priorityLevel attributes associated with the pccRules attribute for those PCC Rules.
- The PCF can set the defQosFlowIndication attribute, to accomplish a binding of the corresponding PCC rules to the Default QoS Flow (without the need to explicitly modify the ARP and 5QI* values of those PCC rules).

Either PCF mechanism could be pursued for invocation of the NS/EP Data Transport Service, based on corresponding specifications as described in Clause 4.2.6.2.10 of TS 29.512 [Ref 8].

7.1.10 Extensions to PCC Event Notification Capabilities

This TR illustrates the use of PCC event notification capabilities (as introduced in 3GPP Release 17), to enable an indication to be delivered to the DTS Server, upon successful or failed invocation/revocation of the NS/EP Data Transport Service. The event attribute within the evSubsc and evNotifs attributes is extended to include a "SUCCESSFUL_QOS_UPDATE" value on the N5 interface (to report a successful update of the QoS of the Default QoS Flow within the Designated PDU Session plus PCC rules that are mapped to that Default QoS Flow), and the PolicyCtrlReqTriggers and repPolicyCtrlReqTriggers attributes are extended to include a new "SUCC_QOS_UPDATE" value on the N7 interface. The event attribute within the evSubsc and evNotifs attributes is extended to include a "FAILED_QOS_UPDATE" value on the N5 interface (to report a failed update of the QoS of the Default QoS Flow).

This functionality supports the ability to report the successful or failed completion of the QoS upgrade (due to invocation of the NS/EP Data Transport Service) to the DTS Server, to enable the DTS Server to subsequently inform the originating user of this event. This functionality is intended to discourage subsequent NS/EP Data Transport Service invocation re-attempts by the user, if the QoS performance is not improved noticeably after the NS/EP Data Transport Service is invoked (e.g., if the perceived quality problems are due to problems experienced by the far end Data Server, rather than due to difficulties triggered by network congestion).

7.1.11 NS/EP Data Transport Service Revocation

Clause 6.3.7 illustrates procedures that enable the NS/EP Data Transport Service to be explicitly revoked by the Service User, patterned after similar procedures used for invocation of the NS/EP Data Transport Service. Other mechanisms can be used to trigger the revocation of the NS/EP Data Transport Service, e.g., when the user closes the special DTS application on their UE. The NS/EP Data Transport Service is automatically revoked upon UE detachment/deregistration (e.g., power down).

In addition, to prevent a UE from inadvertently enabling the NS/EP Data Transport Service for an extended period of time, the network may support revocation of the NS/EP Data Transport Service after a predetermined time. To support this capability, the DTS Server starts a DTS timer when the NS/EP Data Transport Service is successfully invoked. If the DTS timer expires before deactivation of the NS/EP Data Transport Service, the DTS Server sends an **Npcf_PolicyAuthorization_Update request** to the PCF (as discussed in Clause 6.3.7), in order to revoke the NS/EP Data Transport Service. The DTS Server may close the N5 session by sending an **Npcf_PolicyAuthorization_Delete request** to the PCF, which is acknowledged with an **Npcf_PolicyAuthorization_Delete response**.

When the NS/EP Data Transport Service is revoked, the PCF restores appropriate QoS values for the Default QoS Flow within the Designated PDU Session, and updates PCC rules that were previously mapped or bound to that Default QoS Flow when the NS/EP Data Transport Service was previously invoked. Clause 6.3.7 describes the PCF procedures, as needed to restore the prior QoS settings that were applicable prior to invocation of the NS/EP Data Transport Service. It also discusses the need for more complex PCF logic, to accommodate potential updates to the QoS of the Default QoS Flow and/or to the related PCC rules by other services during the time that the NS/EP Data Transport Service was enabled, rather than simply restoring the previous QoS settings. The corresponding logic is dependent on the identification of particular services that may be deployed, and the desired interactions between the NS/EP Data Transport Service and any such services. These aspects are not considered in this TR.

7.1.12 Configuration of QoS Values for NS/EP Data Transport Service

The NS/EP Data Transport Service relies on the setting of appropriate 5QI and optional Priority Level values when an AF Signalling Flow is established to support priority signalling between the UE and the DTS Server, and when the NS/EP Data Transport Service is invoked.

As described in step F of Clause 6.2.1, invocation of the NS/EP Data Transport Service entails the assignment of a special 5QI* value to support priority treatment of packets that are transported via the Default QoS Flow of the

Designated PDU Session. The specific 5QI* value is configured in the PCF for this purpose. If a standardized 5QI value is used, the one with the highest priority for a non-GBR QoS Flow (other than used for signalling) is recommended for the NS/EP Data Transport Service. Additional flexibility can be enabled via the use of an appropriate Priority Level value, as populated in the priorityLevel attribute, to override the default Priority Level that is otherwise associated with a particular 5QI value.

> NOTE: 5QI value "6" or "70,"' as specified in Table 5.7.4-1 of TS 23.501 [Ref 2], could be used for this purpose. 5QI value "5", as used for signalling, cannot be used. Table 5.7.4-1 of TS 23.501 [Ref 2] specifies a recommended priority level of 55 for 5QI value "70", which is numerically lower than the recommended priority level (60) as specified for 5QI value "6". Therefore, 5QI value "70" is recommended over 5QI value "6" for the NS/EP Data Transport Service. Table 5.7.4-1 of TS 23.501 [Ref 2] indicates a Packet Delay Budget value of 200 msec for 5QI value "70" versus 300 msec for 5QI value "6".

As described in step F of Clause 6.2.2, a special 5QI* value is assigned to support priority treatment of signalling packets that are exchanged between the UE and the DTS Server. The specific value is configured in the PCF for this purpose. A 5QI* value with the highest priority as allowed by local policy is recommended for the NS/EP Data Transport Service.

> NOTE: Table 5.7.4-1 of TS 23.501 [Ref 2] indicates that 5QI values "5" and "69" have the highest priority level assignments, and therefore may be considered for the corresponding PCF variable.

The NS/EP Data Transport Service relies on the prioritized transport of IP packets when the NS/EP Data Transport Service is invoked (e.g., via setting of appropriate DSCP values). Appropriate values are to be determined by Service Providers to facilitate priority transport of NS/EP data packets within the NS/EP Service Provider's network, as well as values to be used across network boundaries. See ATIS-1000090 [Ref 18].

7.2 Recommendations

This clause describes various recommendations pertaining to the NS/EP Data Transport Service. Many of these items pertain to mechanisms and options for deployment of the NS/EP Data Transport Service that will need to be chosen by Service Providers in consultation with the designated government agency for the NS/EP Data Transport Service.

Information sent to BSF in the Nbsf_Management_Discovery request

Clause 7.1.7 discusses information that is sent to the BSF in the **Nbsf_Management_Register request** from the PCF, as illustrated in step 13 in Figure 6-4 of Clause 6.3.3.1, in order to enable the DTS Server to retrieve relevant information from the BSF via the **Nbsf_Management_Discovery** service operation (in steps 1 and 2 of Figure 6-6 in Clause 6.3.4). For the NS/EP Data Transport Service, the DTS Server should include the UE's IP address and the Designated DNN in the **Nbsf_Management_Discovery request**.

Preservation of local UE IP address

For use cases that rely on the local UE IP address to be provided by the UE to the DTS Server as part of the IP header, there should be no NAT of the UE's IP address between the UPF and the DTS Server. In addition, the “forwarded” field should be included in the HTTP header, as specified in RFC 7239 [Ref 21], to enable the DTS Server to retrieve the original UE IP address if the packets went through any HTTP proxies between the UPF and DTS Server.

Configuring / disabling DoH

To avoid complications in the implementation of the NS/EP Data Transport Service based on adoption of third-party DoH deployments as discussed in Clause 6.3.5.1, this TR assumes that the Service User is responsible for configuring / disabling DoH, as necessary to adhere to use of the Service Provider's designated DNS Server[5].

This TR recommends that guidance be provided to the Service User such that:

- DoH, if supported by the web browser selected by the user to invoke the NS/EP Data Transport Service, is able to be manually disabled or overridden by the Service User, and
- Prior to activation of the NS/EP Data Transport Service, the third-party DoH has been disabled (e.g., by the Service User in the web browser selected by the user to invoke the NS/EP Data Transport Service).

Security considerations

The NS/EP Data Transport Service must support security mechanisms to ensure that the UE is able to securely and effectively communicate with the DTS Server. These security capabilities include message integrity mechanisms and the ability to verify that the originator is authorized to invoke the NS/EP Data Transport Service. The specific security objectives will be established by particular Service Providers in consultation with the designated government agency for the NS/EP Data Transport Service. A detailed security assessment is recommended, including the choice of appropriate authentication mechanisms for the NS/EP Data Transport Service, based on the specific use case(s) that are deployed.

The use case as presented in Clause 6.2.1 assumes that the Service User uses a browser to invoke the NS/EP Data Transport Service. When using a non-NS/EP-subscribed UE, the Service User enters NS/EP credentials via an HTML form that is sent to the DTS Server. The DTS Server verifies these entered credentials via an NS/EP database. When using an NS/EP-subscribed UE, no NS/EP credentials need to be entered by the Service User.

The use case as presented in Clause 6.2.2 assumes that the Service User uses an NS/EP subscribed UE, and no entry of NS/EP credentials is required.

The DTS Server requests the PCF to perform UE authorization for the NS/EP Data Transport Service. The DTS Server sends to the PCF the "trusted" IP address received from the UE in the IP header of the AF Signalling Flow establishment request or DTS invocation request. The PCF retrieves NS/EP subscription information from the UDR using this UE IP address (and its associated DNN) received from the DTS Server to check whether this UE is authorized or not for the NS/EP Data Transport Service.

Further discussion of these procedures is provided in Clause 7.1.4.

Extended PCF procedures to establish priority AF signalling

Clauses 6.3.3.2 and 6.3.4 describe the potential establishment of an AF Signalling Flow from the UE towards the DTS Server, to carry priority signalling traffic between the UE and the DTS Server for supporting the NS/EP Data Transport Service. To accomplish these actions, the PCF establishes an appropriate AF Signalling Flow (with appropriate 5QI* and ARP values) to provide priority access to a DTS Server.

Clause 6.3.3.2 describes the possible establishment of a priority Dedicated QoS Flow from an NS/EP-subscribed UE towards the DTS Server when the user activates (opens) a DTS application on their UE (option [b]) or when the user invokes NS/EP Data Transport Service (option [c]). Options [b] and [c] require the inclusion of the mpsId attribute by the DTS Server in the **Npcf_PolicyAuthorization_Create request**, used to establish the priority AF Signalling Flow from the UE towards the DTS Server, as described in Clause 6.3.4. Inclusion of mpsAction attribute value "AUTHORIZE_AND_ENABLE_MPS_FOR_AF_SIGNALLING" is recommended for NS/EP Data Transport Service deployments beginning with 3GPP Release 18, to allow the DTS Server to explicitly signal that authorization for the NS/EP Data Transport Service is required for priority AF signalling.

Clause 6.3.3.2 describes an alternative (option [a]) that would involve the establishment of an AF Signalling Flow from the UE towards the DTS Server at the time of PDU Session Establishment. This would require extensions to the PCF configuration, as discussed in Clause 7.1.2 for option [a].

[5] Alternate solutions, such as user entry of the DTS Server's IP address rather than a URL, or making the DTS Server accessible via a DNS Server external to the Service Provider, are not recommended, and would require a detailed security assessment.

Based on the additional PCF functionality required for option [a] and the limited utility of option [c] as described in Clause 7.1.2, option [b] is recommended. Clause 7.1.2 provides additional material concerning these procedures.

Trigger for removal of AF Signalling Flow between the UE and the DTS Server

The specific mechanism used to trigger the removal of the AF Signalling Flow between the UE and the DTS Server can vary, based on the particular use case. Symmetrical procedures are recommended for the establishment and removal of the AF Signalling Flow used for priority signalling between the UE and the DTS Server.

If the NS/EP-subscribed UE is configured with a special DTS application to facilitate the invocation of the NS/EP Data Transport Service, and that DTS application is designed to establish the AF Signalling Flow upon activation (as described in Clause 6.3.4), then the removal of that AF Signalling Flow may be triggered in a symmetrical manner (i.e., that DTS application can initiate HTTP signalling with the DTS Server prior to terminating, in order to first remove the AF Signalling Flow). Corresponding procedures are described in Clause 6.3.8.

> NOTE: Adoption of non-symmetrical procedures could complicate the DTS Server logic that is applied when the NS/EP Data Transport Service is invoked. For example, if an AF Signalling Flow was established for priority signalling when the Service User activated (opened) the DTS application, yet if that AF Signalling Flow is removed when the NS/EP Data Transport Service is revoked (rather than when the DTS application is closed), the DTS Server logic may need to first determine whether or not an AF Signalling Flow is already established before it invokes the PCC procedures for NS/EP Data Transport Service invocation.

If the AF Signalling Flow is established when the NS/EP Data Transport Service is invoked (as discussed in Clause 6.3.6), the subsequent revocation of the NS/EP Data Transport Service (as discussed in Clause 6.3.7) can be designed to trigger the removal of the AF Signalling Flow.

Authorization of NS/EP Data Transport Service revocation requests

The set of credentials required to authorize an NS/EP Data Transport Service revocation request can vary, depending on the particular use case. The added burden of having to manually enter NS/EP credentials to authorize service revocation requests may be deemed unnecessary, when considering that the NS/EP Data Transport Service is automatically revoked upon UE detachment/deregistration (e.g., power down). To authorize an NS/EP Data Transport Service revocation request from a UE that is not subscribed to NS/EP, authorization may be performed in an implementation-specific manner (e.g., via information used to correlate the NS/EP Data Transport Service revocation request with a previously-authorized NS/EP Data Transport Service invocation request). Eliminating the need to enter NS/EP credentials to authorize service revocation requests provides a simplified procedure, facilitating the Service User’s ability to quickly revoke the service before returning a borrowed UE to its owner.

Annex A
(Informative)

A. NS/EP Data Transport Service - 3GPP Release 17 Extensions

The NS/EP Data Transport Service functionality for 5GS as described in this TR includes several extensions that have been added in the 3GPP Release 17 specifications, as discussed below.

Use of mpsId attribute to request priority treatment for AF signalling

The procedure illustrated in Clause 6.3.4 to establish an AF Signalling Flow for priority signalling between the UE and the DTS Server is based on Clause 4.2.2.12.3 of TS 29.514 [Ref 10], including the mpsId attribute within the N5 **Npcf_PolicyAuthorization_Create request**, sent from the DTS Server to the PCF in step 3 of Figure 6-6.

NOTE: A specific value of the mpsId attribute is not required for this purpose.

New suppFeat attribute value for "MPSforDTS" feature

The **Npcf_PolicyAuthorization_Create request**, sent by the DTS Server to the PCF in step 3 of Figure 6-6, includes the suppFeat attribute, which informs the PCF about the required and optional features that the DTS Server supports. The **Npcf_PolicyAuthorization_Create response** includes the suppFeat attribute, to enable the PCF to respond with an indication of the set of features that it has in common with the DTS Server, and that the PCF supports within the N5 session. The suppFeat attribute is extended to support the "MPSforDTS" feature number for the NS/EP Data Transport Service.

The suppFeat attribute, as exchanged between the PCF and the SMF within an N7 session, is similarly extended to support the "MPSforDTS" feature number for the NS/EP Data Transport Service.

Addition of new mpsAction attribute

3GPP Release 17 extends the PCC capabilities, by introducing the mpsAction attribute to explicitly support the dynamic on demand invocation and revocation of the NS/EP Data Transport Service and request for PCF authorization during invocation of the NS/EP Data Transport Service in a 3GPP-specified manner. These extensions are discussed further in Clause 7.1.8.

Extensions to PCC event notification capabilities

3GPP Release 17 extends the PCC event notification capabilities, to enable the DTS Server to be notified of the disposition of processing pertaining to the invocation/revocation of the NS/EP Data Transport Service. The event attribute within the evSubsc and evNotifs attributes is extended to include new "SUCCESSFUL_QOS_UPDATE" and "FAILED_QOS_UPDATE" values on the N5 interface, and the PolicyCtrlReqTriggers and repPolicyCtrlReqTriggers attributes are extended to include a new "SUCC_QOS_UPDATE" value on the N7 interface. These extensions are discussed further in Clause 7.1.10.