RADEXT WG
Internet-Draft
Intended status: Standards Track
Expires: 24 January 2024

S. Gundavelli
S. Kishore
M. Grayson
O. Pekar
Cisco

23 July 2023

RADIUS Attributes for 3GPP 5G AKA Authentication Method
draft-gundavelli-radext-5g-auth-01

Abstract

This document proposes extensions to the Remote Authentication Dial-In User Service (RADIUS) protocol for supporting the 3rd Generation Partnership Project (3GPP) 5G Authentication and Key Agreement (5G-AKA) authentication method.

The 5G-AKA protocol is a key authentication method used in 5G networks for mutual authentication and key derivation between user devices and the network. By integrating 5G-AKA into RADIUS, enterprises can leverage existing RADIUS-based authentication infrastructure for authenticating 5G devices.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 24 January 2024.

Table of Contents

1. Introduction

Authentication and key management are critical for ensuring secure communication within the access network. These mechanisms enable mutual authentication between the device and the access network, verifying identities and establishing trust. By validating the identities of both parties, these procedures ensure that only authorized devices can access the network. Additionally, these procedures derive cryptographic keys that safeguard both signaling

and user plane data. By doing so, they protect the integrity and confidentiality of the transmitted information, preventing unauthorized access and maintaining a secure communication environment within cellular networks.

3GPP 5G System architecture has defined support for different authentication methods - 5G AKA, EAP AKA' and EAP TLS and EAP TTLS. The 5G system defines a new service based architecture together with new network elements (e.g., AUSF, UDM) to support these authentication methods. Appendix A shows signalling exchanges associated with 5G registration between the 5G network functions and the AUSF and UDM.

Integrating this authentication method into RADIUS allows network operators to leverage existing RADIUS infrastructure for user authentication and authorization in enterprise 5G deployments. This document defines new RADIUS attributes to support the 5G-AKA procedure, enabling interoperability between RADIUS servers and 5G network elements.

2. Conventions and Terminology

2.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Terminology

All the mobility terms used in this document are to be interpreted as defined in the IETF and 3GPP specifications. For convenience, the definitions for some of the terms are provided below.

Subscription Permanent Identifier (SUPI))

A globally unique 5G Subscription Permanent Identifier (SUPI) is allocated to each subscriber in the 5G System. The SUPI value is provisioned in USIM and UDM/UDR function in 5G Core. The structure of SUPI and its privacy is specified [TS23501]

Subscription Concealed Identifier (SUCI)

The Subscription Concealed Identifier (SUCI) is a privacy preserving identifier containing the concealed SUPI. The UE generates a SUCI using the public key of the Home Network provisioned to the USIM. The structure of SUCI is specified in 3GPP specification [TS33501].

Permanent Equipment Identifier (PEI)

In 5G System, the Permanent Equipment Identifier (PEI) is a unique identifier of a UE accessing the private 5G System. The structure of the PEI is specified in 3GPP specification [TS23003].

International Mobile Station Equipment Identifier (IMEI)

IMEI is a number that uniquely identifies a mobile device in Global System for Mobile Communications (GSM) The structure of the IMEI is specified in 3GPP specification [TS33102].

Sequence Number (SQN)

The sequence number stored in the UE is termed SQN-UE and the sequence number stored in the home network is termed SQN-HN.

3. Motivation

Enterprises now have the opportunity to expand and enhance their wireless coverage density by complementing their existing IEEE 802.11-based wireless architectures with 3GPP-based 5G access networks.

There are multiple deployment options available for implementing an enterprise 5G system. It can be deployed through a System Integrator (SI), a mobile operator, a Wi-Fi operator in collaboration with a cellular provider, potentially a cloud provider, or by the enterprise IT themselves if they can access 5G spectrum. While these options provide a strong foundation for enabling basic 5G access connectivity, there is considerable value in achieving convergence across these diverse access architectures and leveraging the already deployed network elements. It is highly desirable for enterprise IT to possess the capability to correlate identities across different access technologies and enforce consistent enterprise policies.

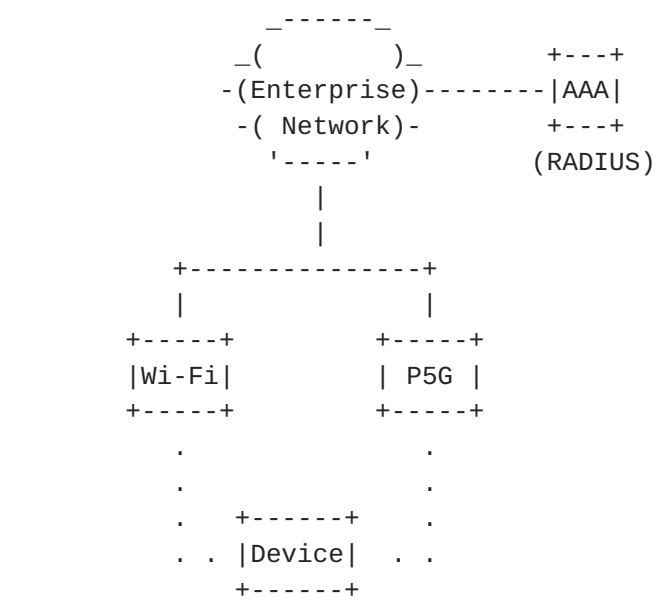


Figure 1: Enterprise Architecture

Enterprise network architectures have undergone extensive evolution over an extended period, resulting in intricate structures. These architectures are designed to be technology-agnostic, accommodating both Ethernet and Wi-Fi-based connections seamlessly. RADIUS-based infrastructure is widely employed for authentication and policy management purposes. As 5G-based private networks become integrated into enterprise environments, it is a natural progression to consider private 5G as another access technology, allowing the utilization of the existing RADIUS infrastructure to authenticate 5G devices. The adoption of a unified authentication and policy infrastructure across different access technologies enables the realization of identity correlation and ensures consistent policy enforcement.

Based on this motivation, we put forward proposals for extending the RADIUS protocol to support the 5G-AKA authentication method.

4. Overview of 5G Security

The 5G security architecture is given below.

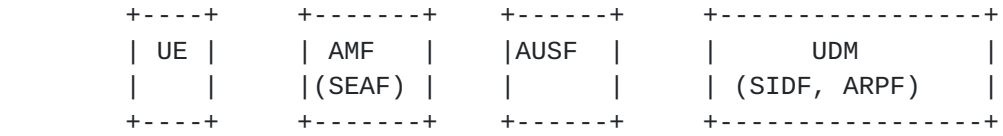


Figure 2: Enterprise Architecture

ARPF (Authentication credential Repository for Procession Function)

ARPF is part of UDM as per the standard. ARPF contains subscriber credentials, i.e. long term keys and Subscriber Identifier (SUPI). Subscriber credentials may alternatively be stored in UDR [TS23003].

AMF (Access and Mobility Management Function)

The AMF is a control plane function in the visited network. It is UE responsible for providing registration (authentication and authorization) services as well as connectivity and mobility management services.

AUSF (Authentication Server Function)

It is standalone NF located in subscriber's home network. It is handling authentication in home network based on information received from UE and UDM/ARPF

SEAF (Security Anchor Function)

SEAF is functionality provided by the AMF It is handling authentication in serving network based on information received from UE and AUSF.

SIDF (Subscriber Identifier De-concealing Function)

SIDF is a service offered by UDM in home network. It is responsible for resolving the SUPI from the SUCI.

UDM (Unified Data Management)

UDM is responsible for managing all user data.

In 5G UE is authenticated by home network(AUSF) and serving network(SEAF).

5. RADIUS Support for 5G-AKA Authentication Method

In the proposed approach, the RADIUS server will implement the 5G-AKA algorithm. Furthermore, it is assumed that as this is a private 5G deployment, there are no requirements to support inter-operator roaming.

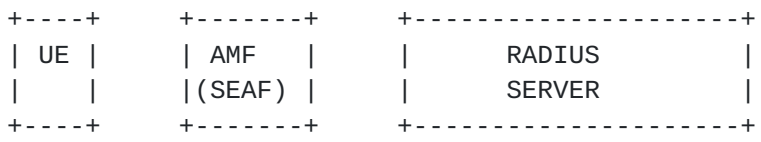


Figure 3: Enterprise Architecture

5.1. Call Flow

In the proposed approach, the RADIUS server will be the primary authentication function. Following are the interactions between the 5G system and the RADIUS Server.

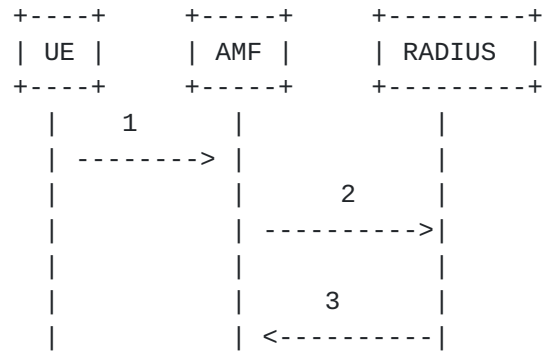


Figure 4: 5G-AKA Authentication Flow

* Step-1: UE Sends the NAS Registration Request message to AMF which includes SUCI or 5G-GUTI.

* Step-2: AMF creates a RADIUS Access-Request message, which includes the RADIUS User-Name attribute that contains the 5G subscriber identifier in format SUCI or SUPI and the RADIUS 5G-SN-NAME attribute that identifies the serving network name.

* Step-3: Once the RADIUS server receives the request it converts the SUCI to SUPI using SIDF function. The RADIUS server consults the database of users to find the user whose name matches with SUPI in the request. This is equivalent to the ARPF function in the UDM. The RADIUS server generates an Authentication Vector using the 5G-AKA algorithm. This vector consists of RAND, AUTN, HXRES* and KAUSF parameters. The AUSF function takes KAUSF and generates KSEAF. The RADIUS server responds with a RADIUS Access-Accept message containing authentication vector attributes 5G-Auth-RAND, 5G-Auth-AUTN, 5G-Auth-HXRES-STAR, 5G-Auth-KSEAF, 3GPP-IMSI, 5G-DNN, 3GPP-IMEISV. All key derivations for 5G-AKA shall be performed using the key derivation function (KDF) specified in Annex B.2.0 of TS 33.220.

* On successful lookup of 5G subscriber identity in the database and calculation of resulting 5G-AKA authentication vector, the RADIUS server sends Access-Accept message that contains the resulting authentication vector in 5G authentication RADIUS attributes specified in section 6 of this document.

* If the RADIUS server fails to execute one or more operations it sends a RADIUS Access-Reject message indicating that 5G-AKA authentication failed.

* Note-1: The RADIUS server must be provided with the 128-bit long K and the 128-bit long OPC 5G-AKA parameters per subscriber identity SUPI to perform authentication vector calculations according to 5G-AKA algorithm.

* Note-2: The RADIUS server must be provided with the SQN-HN parameter that represents a 48-bits long sequence number. The initial value of SQN-HN for 5G subscriber should be 1. The SQN-HN parameter is increased on every 5G-AKA authentication for the specific 5G subscriber and when it reaches 0x7FFFFFFFFFFF it is rolled over to 1 as specified in TS 33.102 section C.3.2

* SQN-HN and SQN-UE sync flow <TBD>

6. 5G-AKA RADIUS Attribute Definitions

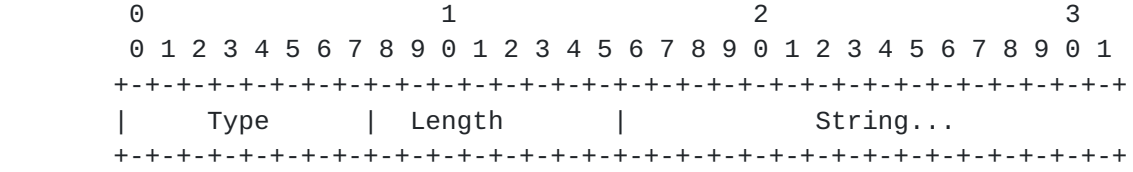
This section describes the attributes that are required for supporting 5G-AKA Authentication Method.

In addition to the new 5G-AKA specific attributes, the standard 3GPP-defined vendor specific attributes 3GPP-IMSI and 3GPP-IMEISV are used for identity exchange between RADIUS client and RADIUS server.

6.1. 5G-Auth-RAND

Description

The 5G-Auth-RAND is of type binary and contains the random number which is part of the authentication vector generated by 5G-AKA algorithm. The size of this value is 128 bits.



Type

<TBD>

Length

18

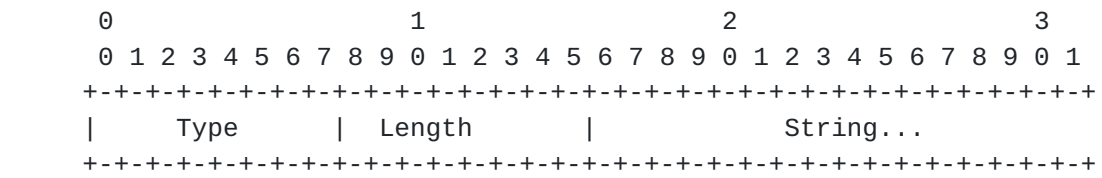
String

A random value.

6.2. 5G-Auth-AUTN

Description

The 5G-Auth-AUTN is of type binary and contains the authentication token which is part of the authentication vector generated by 5G-AKA algorithm. The size of this value is 128 bits. AUTN is generated using this formula (SQN ^ AK) || AMF || MAC_A. AMF is set to 0x8000.



Type

<TBD>

Length

18

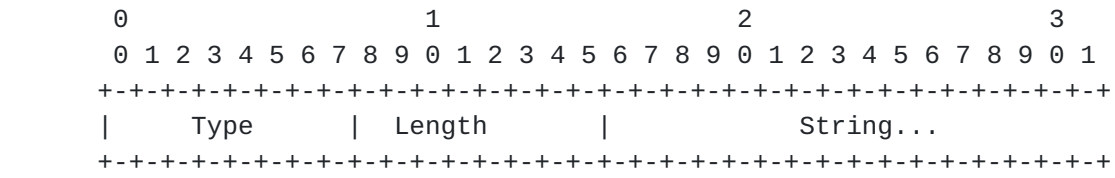
String

The value of Authentication Token parameter of 5G-AKA algorithm.

6.3. 5G-Auth-HXRES-STAR

Description

The 5G-Auth-HXRES-STAR is of type binary and contains the 5G hash expected response which is part of the authentication vector generated by 5G-AKA algorithm. Refer TS33.501 Annex A.5 to generate this value. The maximum size of this value is 128 bits.



Type

<TBD>

Length

18

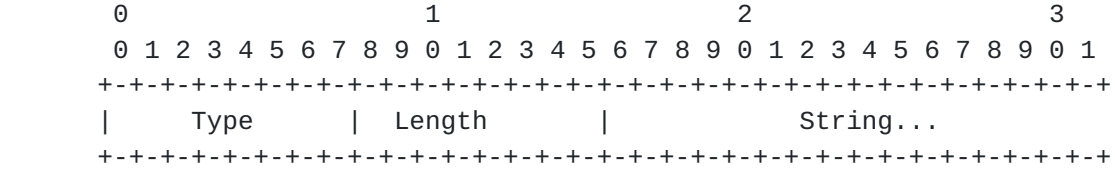
String

The value of Hash Expected Response parameter of 5G-AKA algorithm.

6.4. 5G-Auth-KSEAF

Description

The 5G-Auth-KSEAF is of type binary and contains the 128 bit long 5G security anchor key used to derive KAMF key. This is part of the authentication vector generated by 5G-AKA algorithm. Refer to: TS33.501 Annex A.6 to generate this value.



Type

<TBD>

Length

18

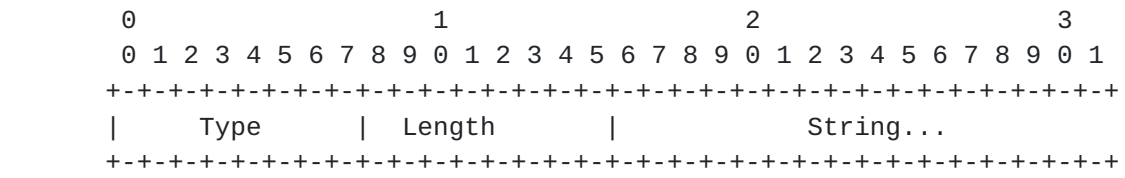
String

The value of security anchor key of 5G-AKA algorithm.

6.5. 5G-DNN

Description

The 5G-DNN is of type string and contains the 5G data network name which is basically a address pool name. This is part of authorization attribute.



Type

<TBD>

Length

>= 3

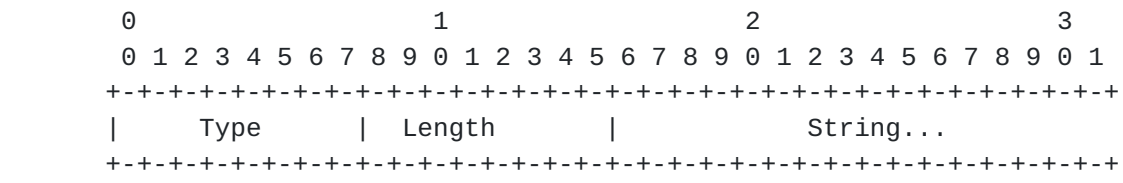
String

The string that contains the 5G data network name.

6.6. 5G-SN-NAME

Description

The 5G-SN-NAME is of type string and contains the serving network name.



Type

<TBD>

Length

>= 3

String

The string that represents serving network name in the following format:

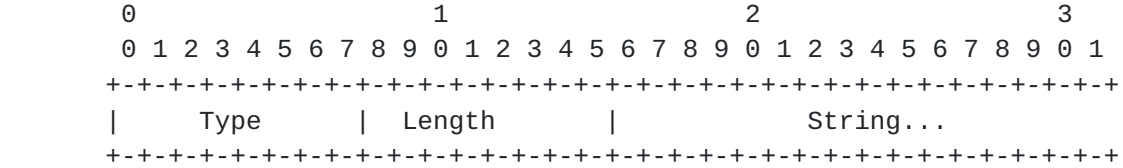
* If NID is not present: "5G:mnc<ddd>.mcc<ddd>.3gppnetwork.org", where 'd' is single decimal digit

* If NID is present: "5G:mnc123.mcc456.3gppnetwork.org:CAFECAFECAFE", where 'd' is single decimal digit and 'X' is single capitalized hexadecimal digit

6.7. User-Name

Description

A standard RADIUS User-Name attribute is used to represent the UE Identifier



Type

1

Length

>= 3

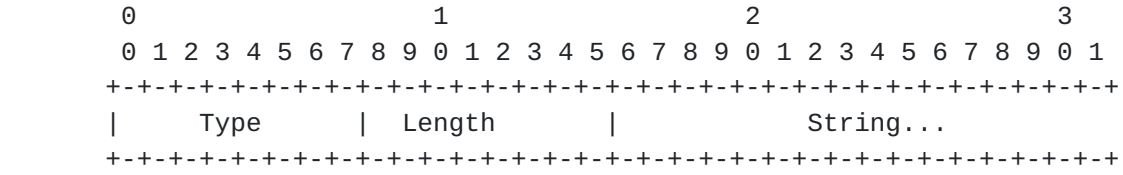
String

The User-Name is of type string and contains the UE identifier SUPI or SUCI. The format of SUPI identifier is given below. SUPI-xxxxxxxxxxxxxx (15 digits) e.g. SUPI-123456789012345. The format of SUCI identifier is given below. SUCI-SUCI Type - Home Network Identifier - Routing Indicator - Protection Scheme - HN Public key ID - Protection Scheme Output e.g. SUCI-0-123-456-0-0-0-150000100

6.8. 5G-Auth-AUTS

Description

The 5G-Auth-AUTS is of type binary and contains SQN-UE. The size of this value is 112 bits. AUTS is generated using this formula Conc(SQN-UE) || MAC_S. Refer to: TS33.102 Section 6.3.3 to generate this value.



Type

<TBD>

Length

16

String

The value of authentication token used for re-synchronization.

6.9. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	#	Attribute
1	0-1	0	0	1	User-Name
0	0-1	0	0	TBD	5G-Auth-RAND
0	0-1	0	0	TBD	5G-Auth-HXRES-STAR
0	0-1	0	0	TBD	5G-Auth-KSEAF
0	0-1	0	0	TBD	5G-Auth-DNN
0-1	0	0	0	TBD	5G-Auth-SN-NAME
0	0-1	0	0	TBD	3GPP-IMEISV
0	0-1	0	0	TBD	3GPP-IMSI

7. IANA Considerations

IANA is requested to assign the following values for the new RADIUS attributes defined in this document: TBD

8. Security Considerations

The security of the 5G-AKA authentication method relies on the integrity and confidentiality of the exchanged authentication vectors, security algorithms, and cryptographic keys. Appropriate measures must be taken to protect these sensitive attributes during transmission between the RADIUS client and server.

9. Acknowledgements

TBD

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

10.2. Informative References

[TS23003] 23.003, 3. T., "Numbering, addressing and identification", 2021.

[TS23501] 23.501, 3. T., "Numbering, addressing and identification", 2021.

[TS33102] 33.102, 3. T., "3GPP Security Architecture", 2021.

[TS33501] 33.501, 3. T., "Architecture enhancements for non-3GPP accesses", 2021.

Appendix A. Standard 5G Authentication and Session Establishment Signalling Flow

The standard 5G authentication and session establishment signalling flow is illustrated in Figure 5.

1. In step 1, the UE sends a registration request.

2. The AMF sends a POST to the AUSF with the path /nausf-auth/v1/ue-authentications including (supiOrSuci, servingNetworkName).

3. The AUSF sends a POST to the UDM with the path /nudm-ueau/v1/{suciOrSuci}/security-information/generate-auth-data including the (servingNetworkName).

4. The UDM responds to the AUSF with a 200 OK incluing (authType, authVector(avType,rand,autn,xresStar,kausf)).

5. The AUSF responds to the AMF with a 201 OK including (authType:5G_AKA,5GAuthData(rand,autn,hxresStar)).

6. The AUSF sends the UE an Authentication Request including (rand,autn).

7. The UE responds to the AMF with an Authentication Response including (res*).

8. The AMF calculates hres* and compare with hxresStar.

9. The AMF sends a PUT to the AUSF with the path /nausf-auth/v1/ue-authentications/1/5g-aka-confirmation including (resStar).

10. The AUSF compare resStar with xresStar.

11. The AUSF responds to the AMF with a 200 OK including (authResult,supi,kseaf).

12. The AMF sends a PUT to the UDM with the path /nudm-uecm/v1/{supiOrSuci}/registrations/amf-3gpp-access including (deregCallbackURri, guami,ratType).

13. The UDM responds to the AMF with a 201 OK.

14. The AMF sends a GET to the UDM with the path /nudm-sdm/v2/{supiOrSuci}/am-data.

15. The UDM responds ot the AMF with a 200 OK including (subscribedUeAmbr,nssai).

16. The AMF sends a GET to the UDM with the path /nudm-sdm/v2/{supiOrSuci}/smf-select-data.

17. The UDM responds to the AMF with a 200 OK including (subscribedSnssaiInfos(dnnInfos,defaultDnnIndicator)).

18. The AMF sends a GET to the UDM with the path nudm-sdm/v2/{supiOrSuci}/ue-context-in-smf-data.

19. The UDM responds to the AMF with a 200 OK.

20. The AMF sends a POST to the PCF with the path npcf-am-policy-control/v1/policies including (supi,accessType,servingPlmnueAmbr).

21. The PCF repsonds to the AMF with a 201 OK.

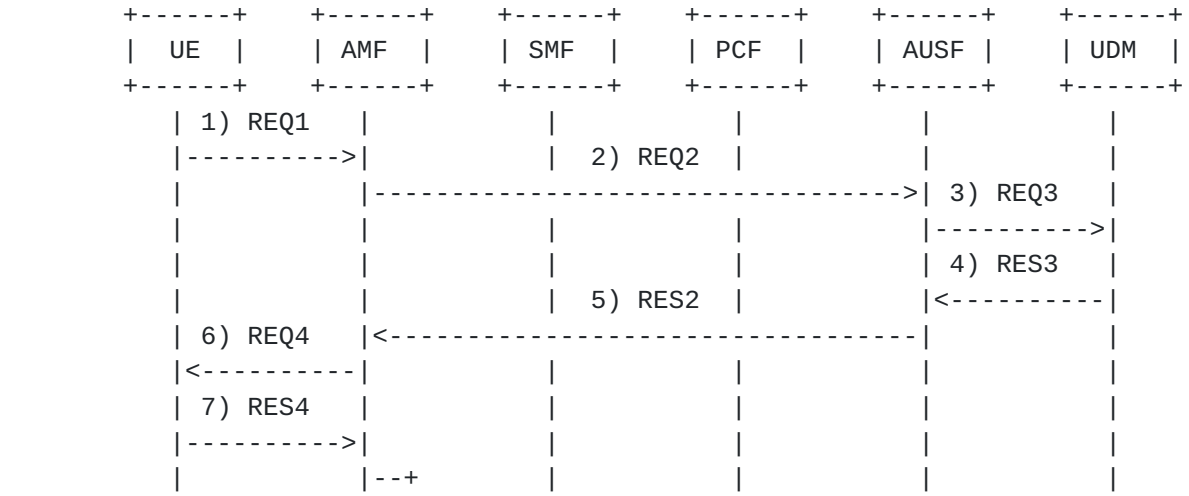
22. The AMF sends a POST to the SMF with the path nsmf-pdusession/v1/sm-contexts including (supi,dnn,sNssai,servingnetwork).

23. The SMF sends a GET to the UDM with the path nudm-sdm/v2/{supiOrSuci}/sm-data including (single-nssai,dnn).

24. The UDM responds to the SMF with a 200 OK including (singleNssai,dnnconfigurations).

25. The SMF responds to the AMF with a 201 OK.

26. The AMF responds to the UE with a Registration Accept.



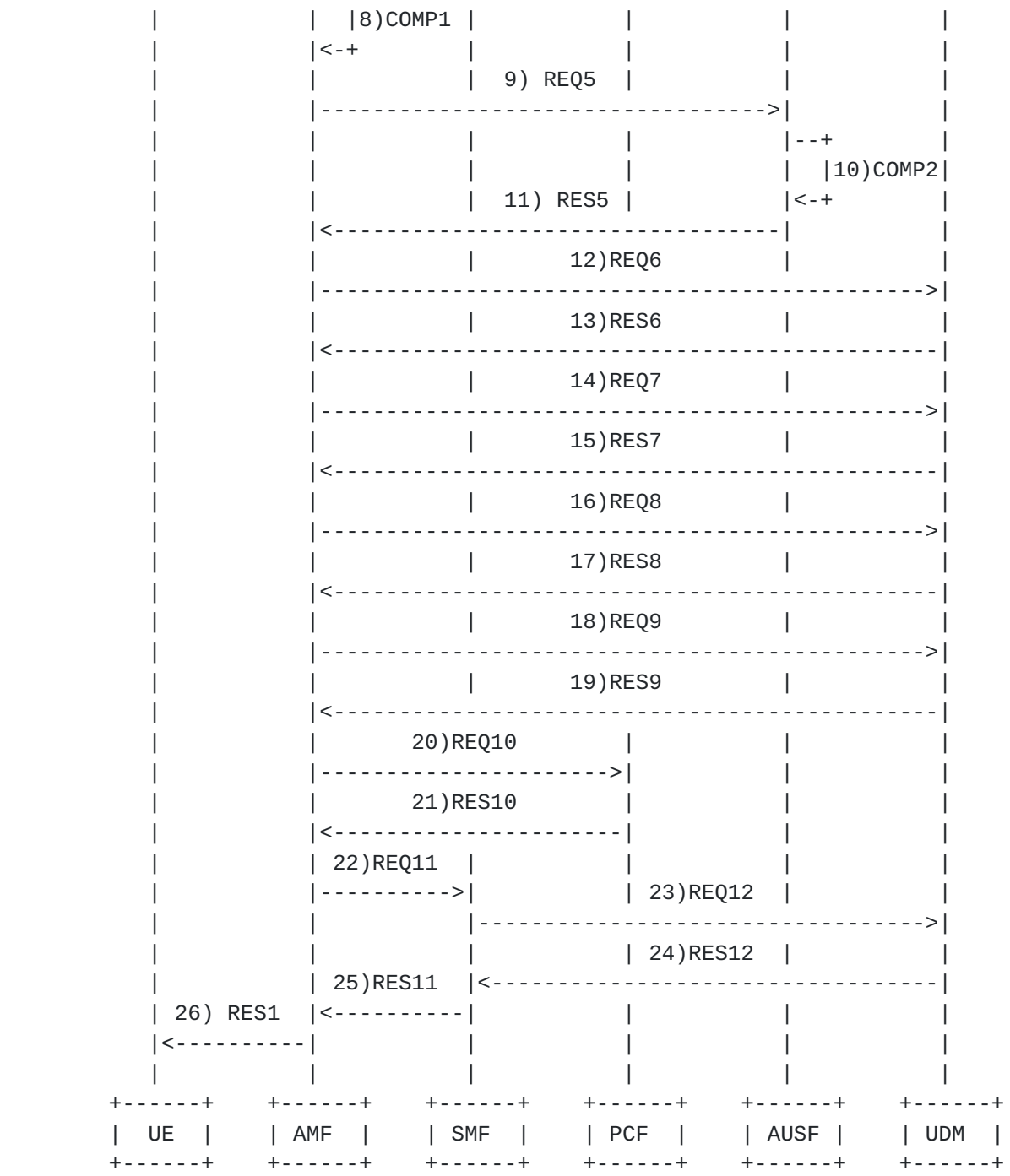


Figure 5: Standard 5G Registration Signalling Flow

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
United States of America
Email: sgundave@cisco.com

Sangram L Kishore
Cisco
Bangalore
India
Email: sanl@cisco.com

Mark Grayson
Cisco
11 New Square Park
Bedfont Lakes
United Kingdom
Email: mgrayson@cisco.com

Oleg Pekar
Cisco
1st Floor, EE5-6
South Netanya
Israel
Email: olpekar@cisco.com