

RADIUS Attributes for 5G Authentication

(<https://datatracker.ietf.org/doc/draft-gundavelli-radext-5g-auth/>)

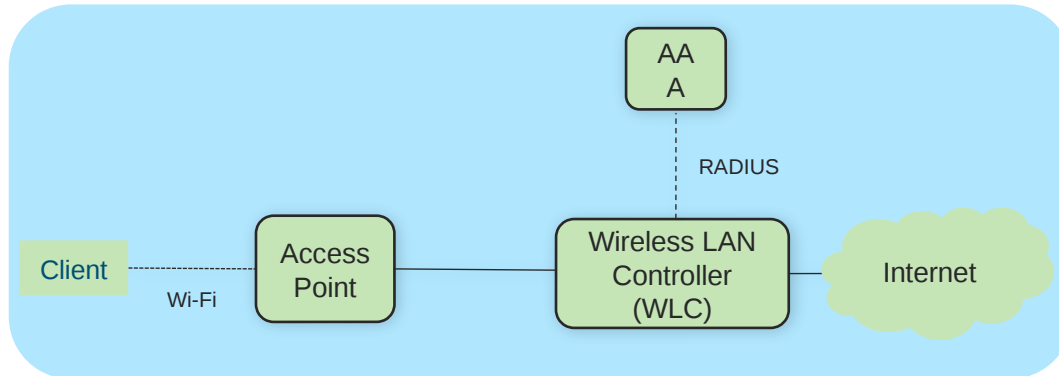
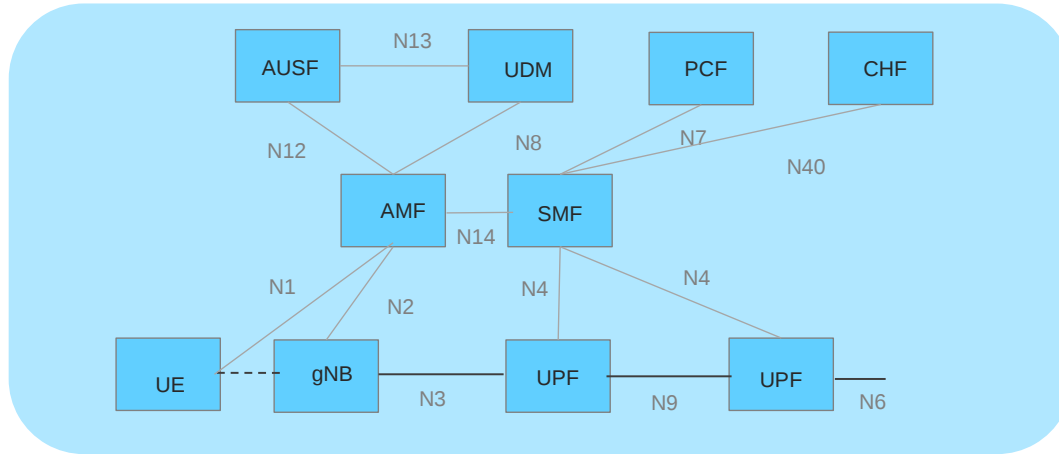
Authors: Sri Gundavelli (Cisco), Sangram L Kishore (Cisco), Mark Grayson (Cisco) & Oleg Pekar (Cisco)

IETF 117 San Francisco, July 24th,
2023

Motivation

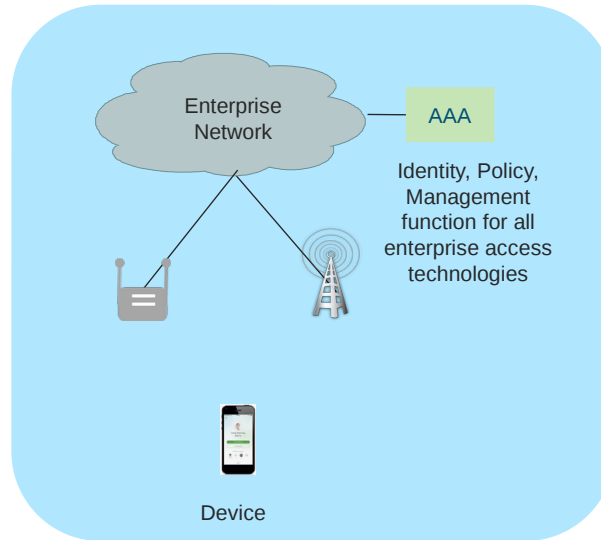
- Private network architectures in general are very complex and have evolved over a long period of time. These architectures are access agnostic, supporting Ethernet and Wi-Fi based access technologies, with deployed network elements for performing identity, policy, mobility, security and network management functions.
- As 5G makes it into enterprise environments, the key objective from the private network operator point of view is to make Private 5G as just another access technology, operated by one identity, policy management system.

Access Architectures



Enterprise Use Case

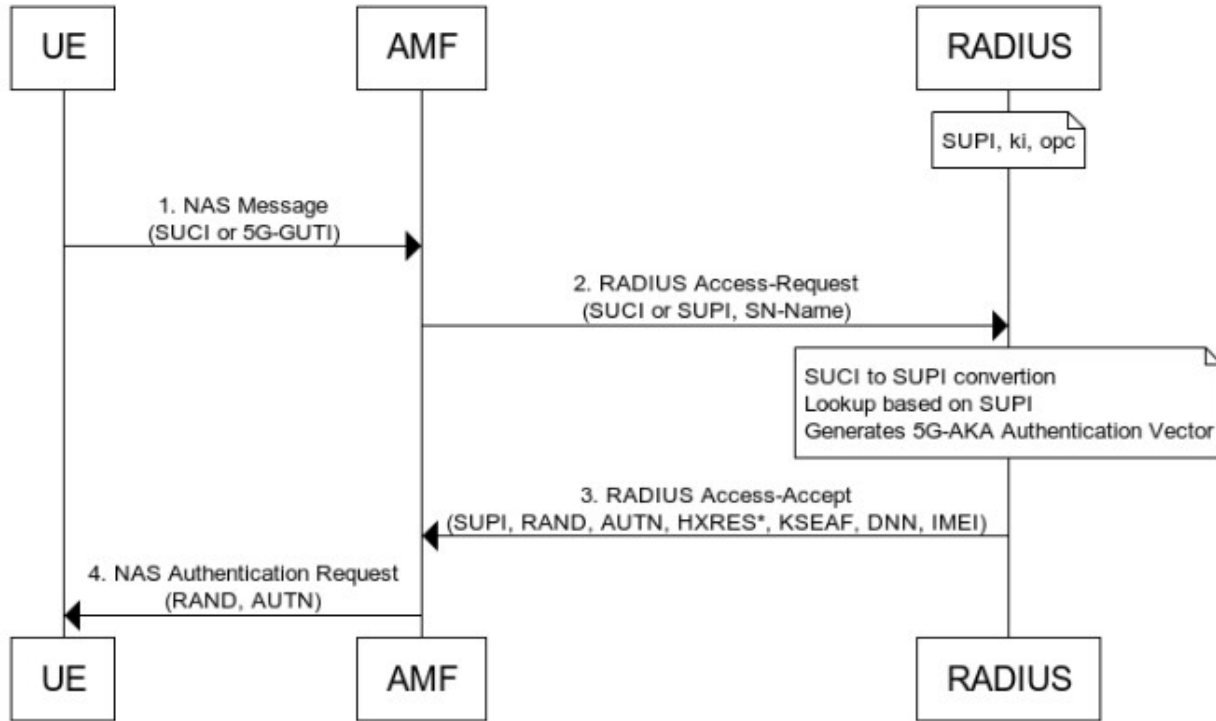
- It is logical to reuse much of the deployed elements in the enterprise network. Enterprises have deployed AAA infrastructure for identity, authentication and policy management. There is value in extending its scope to Private 5G.



Proposal Summary

- 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.

Example Call Flow



RADIUS Attributes

Name	Type	Description
5G-Auth-RAND	String	Random number part of the authentication vector.
5G-Auth-AUTN	String	Authentication token part of the authentication vector.
5G-Auth-HXRES-STAR	String	It is a hash expected response which is part of the authentication vector.
5G-Auth-KSEAF	String	Security anchor key used to derive KAMF key.
5G-SN-NAME	String	Network Identifier includes PLMN and NID.
5G-Auth-AUTS	String	Value of authentication token used for resync.
5G-DNN	String	5G Construct for service name.

Next Steps

- Plan to revise the draft with resync call flows, service authorization attributes and other details.
- We need some feedback from the working group.

COMMENTS?

IETF 117 San Francisco, July 24th,
2023