Net-Centric 2020

[Toward Slice-Specific Authentication and Access Control for 5G]

Shanay.behrad@b-com.com

What is the objective of the presentation?

The objective of the presentation is **not** to provide a new AAC (Authentication and Access Control) mechanism for 5G

The objective is:

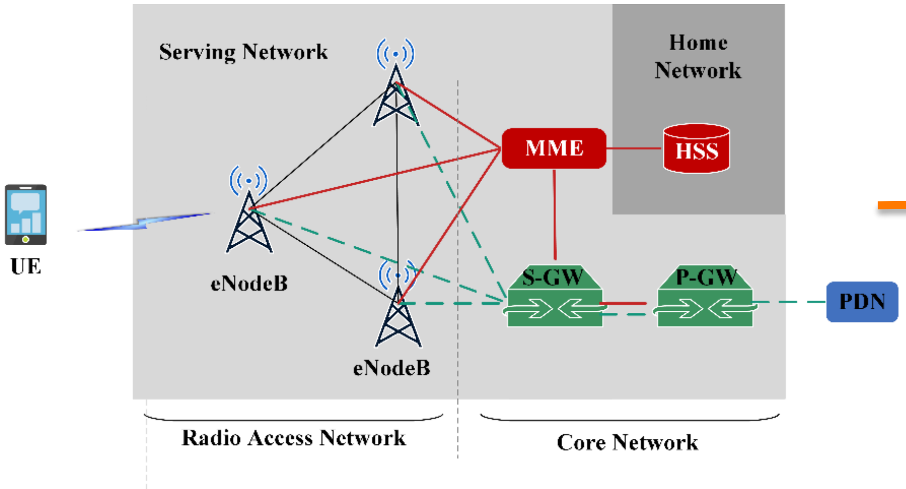
To make the 5G network more flexible

with

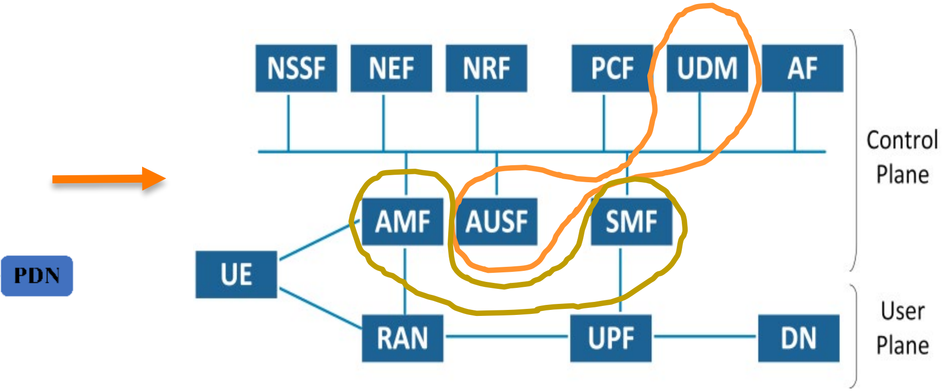
Enabling it to support different AAC mechanism

Network function virtualization

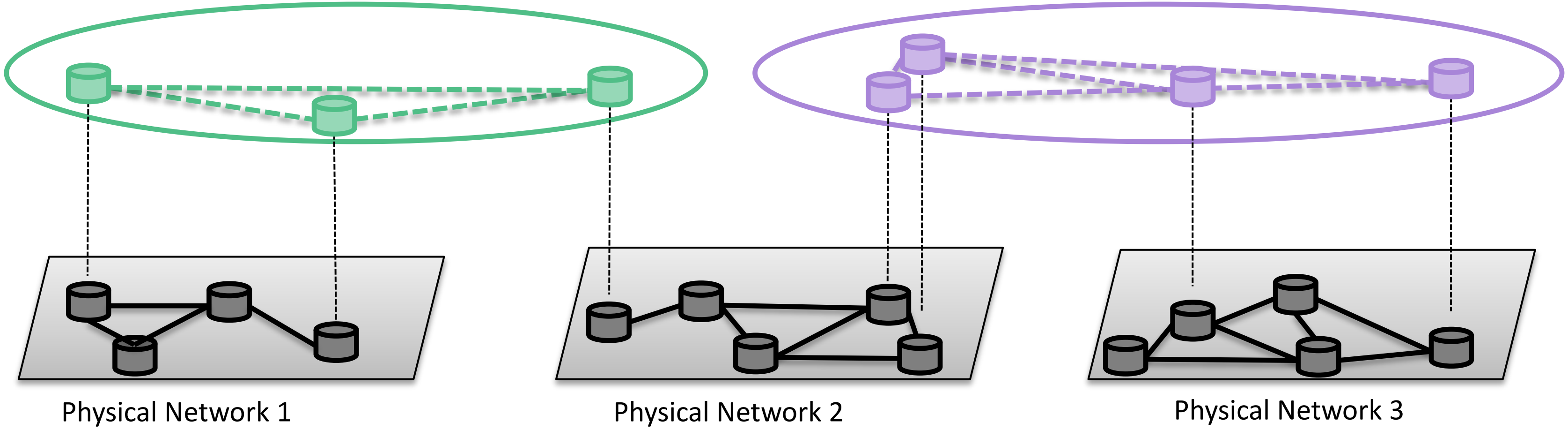
Physical Entities (hardwares)



Virtual Network Functions



Network slicing



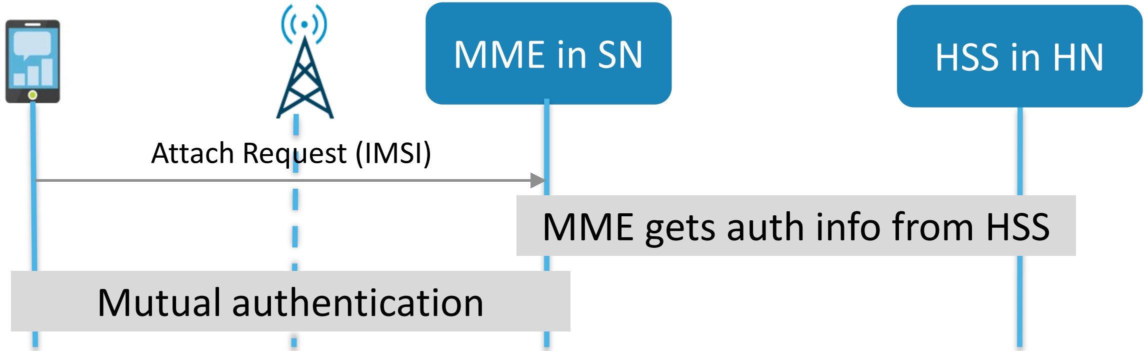
What are the AKA protocols? How do they work?

EPS-AKA

IMSI

(International Mobile Subscriber Identity)

Secret Key



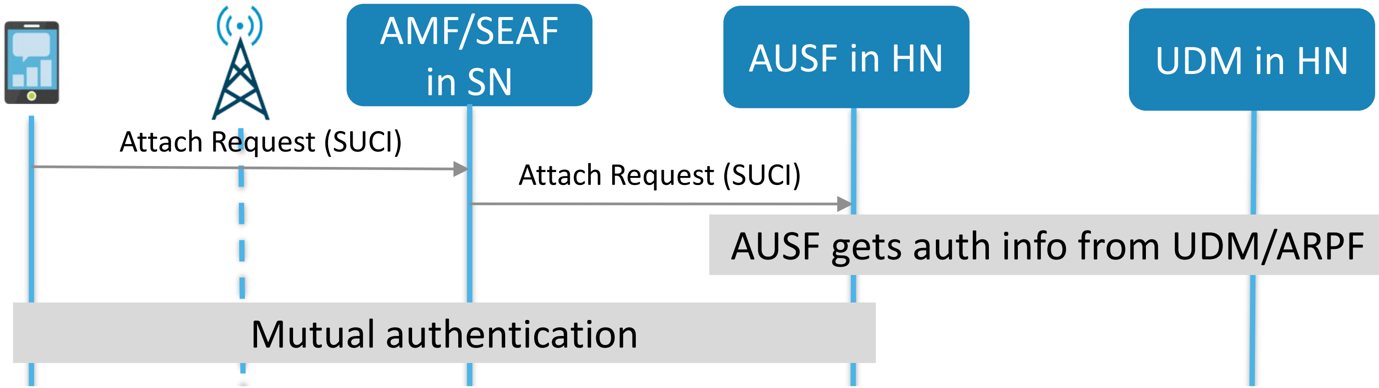
5G-AKA

SUCI

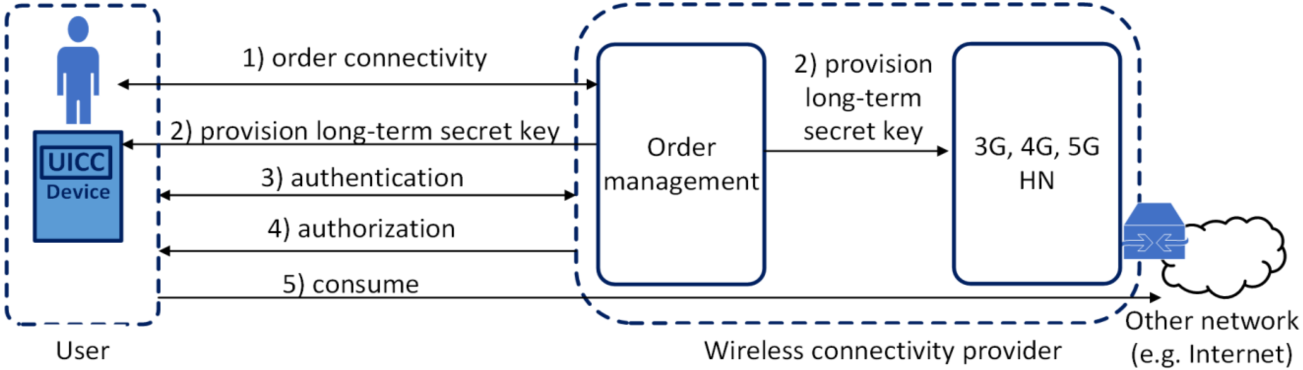
(concealed SUPI)

Secret Key

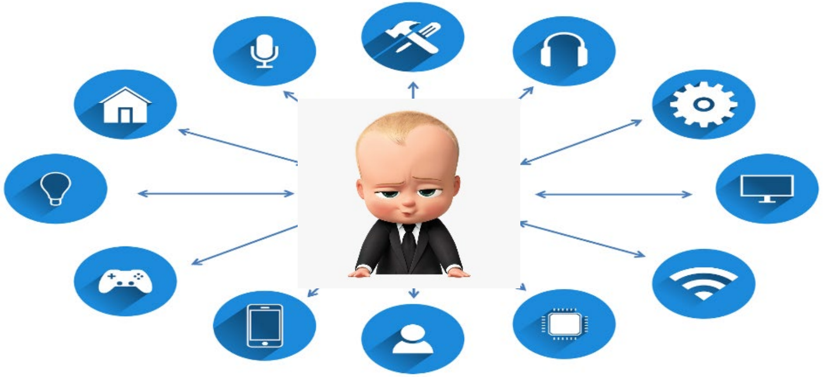
HN Public Key



How are the AAC models in Cellular, WiFi and LoRaWAN?

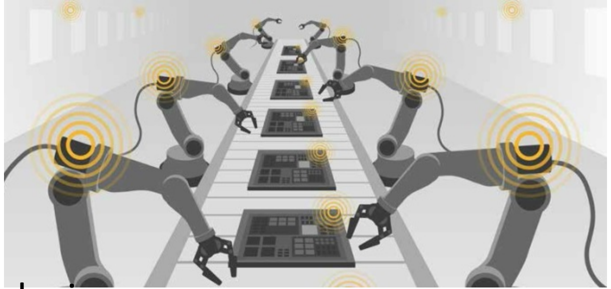

UICC
Device
User
1) order connectivity
2) provision long-term secret key
3) authentication
4) authorization
5) consume
Order management
2) provision long-term secret key
3G, 4G, 5G HN
Wireless connectivity provider
Other network (e.g. Internet)

The connectivity provider has a central role in the AAC of devices



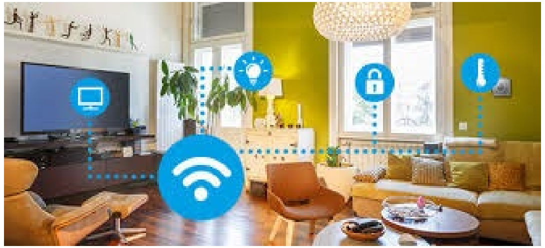
What are the new use cases? What are the requirements?

Allow 3rd parties to choose **their own AAC methods**



Provide **embedded connectivity** inside devices

Allow 3rd parties to **manage the lifecycles** of their devices



Provide AAC mechanisms for **constrained devices**

Support for a **massive number of devices**

Do the AAC mechanisms address the requirements?

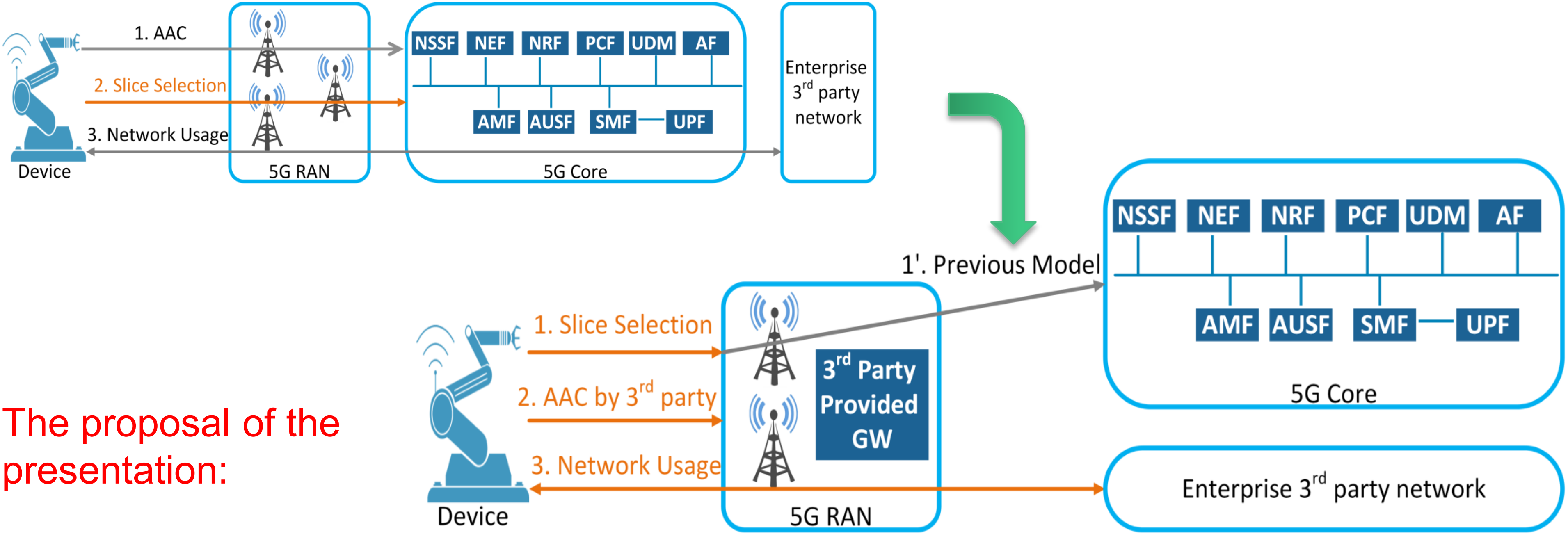
	Cellular AKA	eSIM (AKA)	Group based (AKA)	Service-oriented and anonymity based (AKA + service provider's AAC)	WiFi AAC	LoRaWAN AAC
Provide embedded connectivity inside devices	-	+	-	-	-	-
Allow 3rd parties to choose their own AAC methods	-	-	-	+/-	-	-
Allow 3rd parties to manage the lifecycles of their devices	-	-	-	-	+	+
Provide AAC mechanisms for constrained devices	-	-	+	-	-	+
Support for a massive number of devices	-	-	+	-	-	+

So, what is the solution? A distributed AAC approach!

What does it mean? Delegate AAC to the 3rd parties!

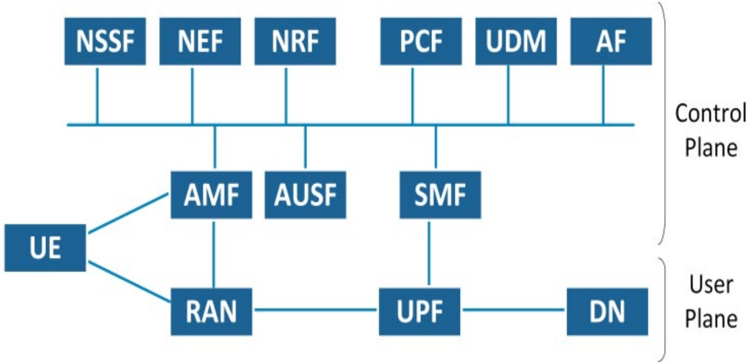
But how?

The proposal of the presentation:



What are the benefits for MNOs?

- Reduces signalling load on the MNO’s Core network
  - Today every attach request go the MNO’s CN then to the slice
- No AMF as a single point of failure and the single point of entrance for IoT
- The MNO has not to design AAC mechanisms for 3rd parties
- The MNO has not to change its information system

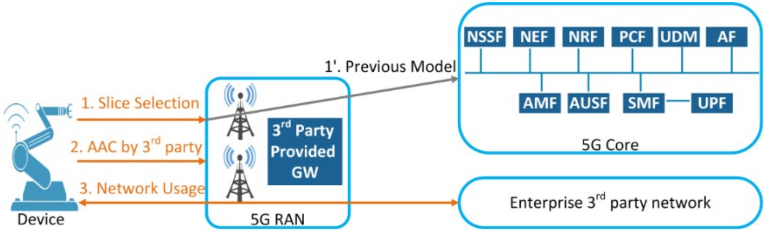


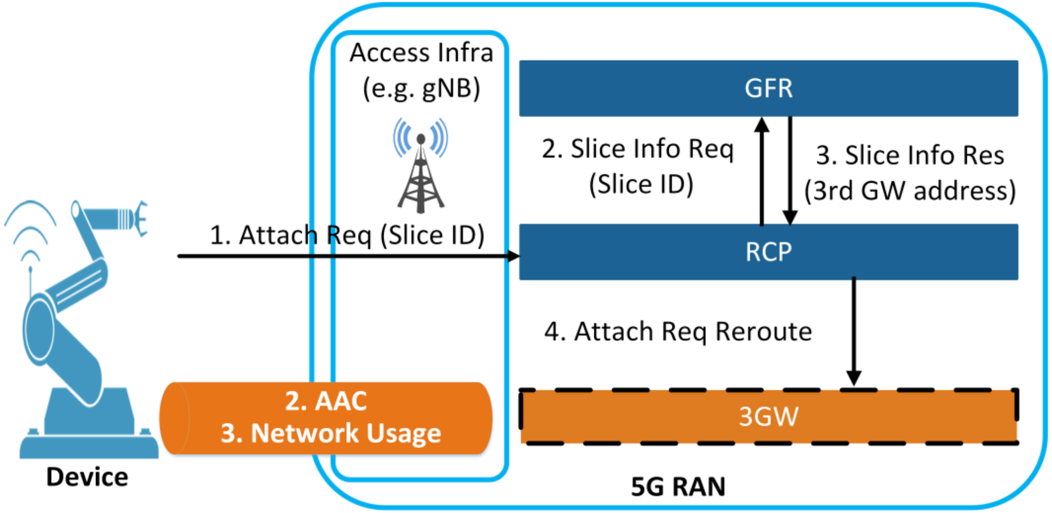
What are the benefits for 3rd parties?

- Has not to connect its Information system to the MNO's Information system

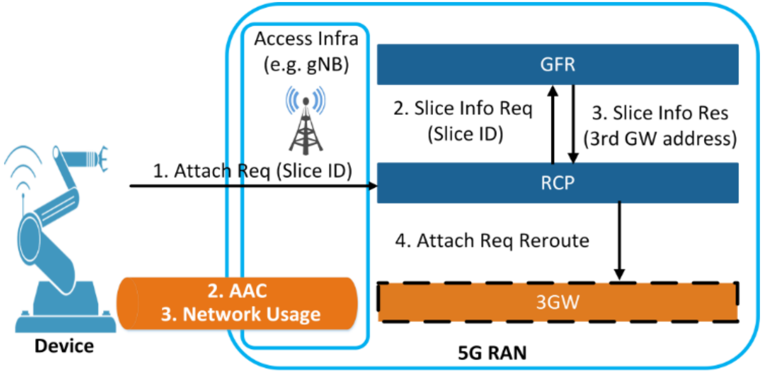
- Chooses the most suitable AAC mechanism
    - The 3rd parties have different security requirements

Proposal: Which networks functions are defined in the RAN?



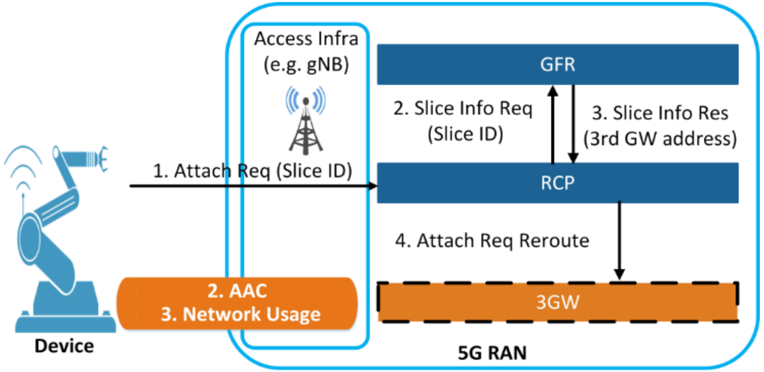


What is the 3GW function?



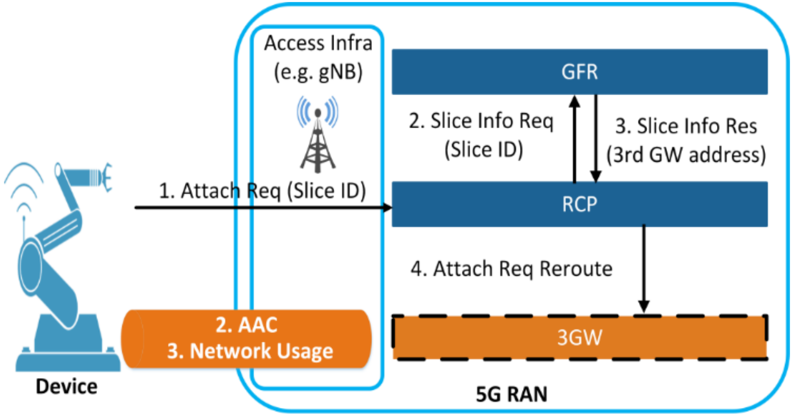
- A dedicated AAC function for the 3rd party
- Under the responsibility of the 3rd party
- The 3rd party may design this function according to its own security requirements
  - Simple (password based)
  - Complex (post-quantum cryptography)
  - A routing function
- Its software code may differ from the software code of the other 3GWs

What is the GFR function?



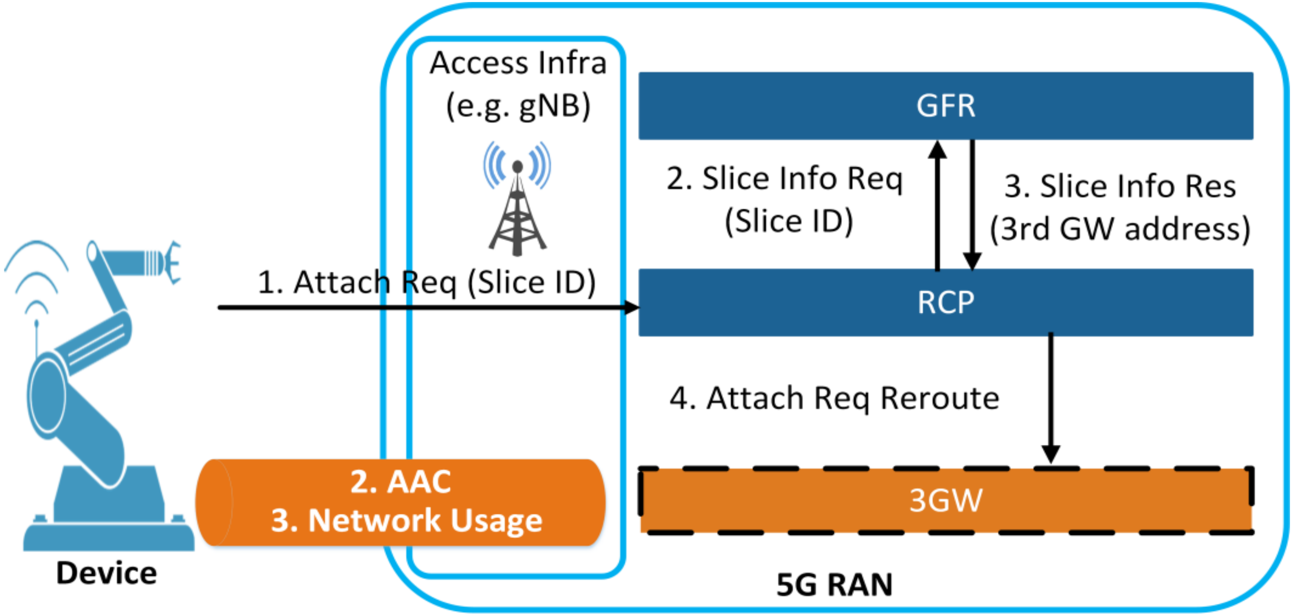
- Stores the information of different 3GW functions
  - The modality of this information depends on the convention between the MNO and the 3rd party
- Enables the RAN to communicate with the different 3GW functions
- It is under the responsibility of the MNO

What is the RCP function?



- The termination point of the signalling messages with the devices on the MNO's side
- Gets the message from the device, selects the right 3GW function
- Waits for the response from the 3rd party's 3GW function or the 5G Core
- Creates appropriate structures for the further steps
- Calls the appropriate security functions

How do the network functions interact with each other?

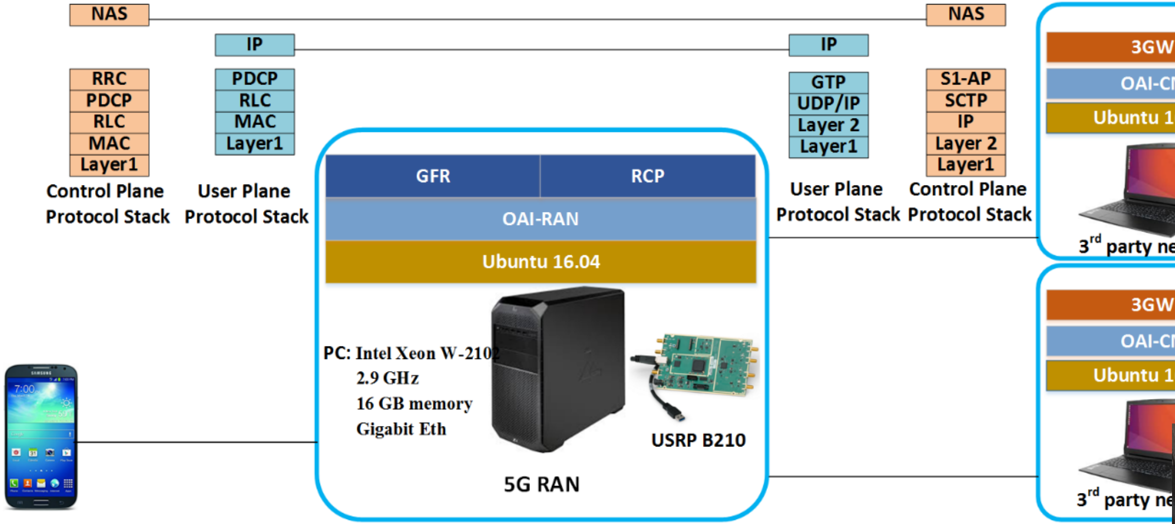


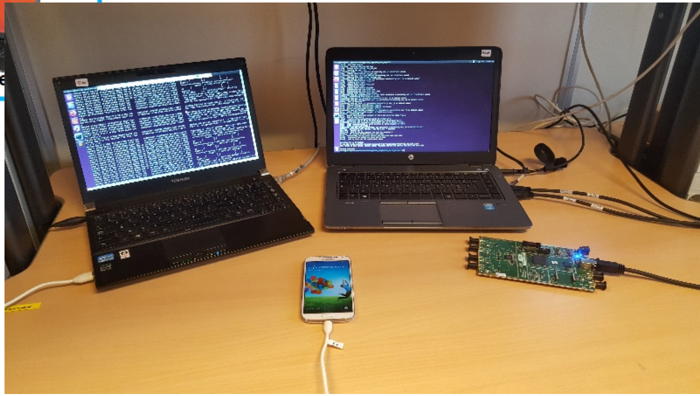
Does 5G-SSAAC address the requirements?

	Cellular AKA	eSIM (AKA)	Group based (AKA)	Service-oriented and anonymity based (AKA + service provider's AAC)	WiFi AAC	LoRaWAN AAC	5G-SSAAC
Provide embedded connectivity inside devices	-	+	-	-	-	-	+
Allow 3rd parties to choose their own AAC methods	-	-	-	+/-	-	-	+
Allow 3rd parties to manage the lifecycles of their devices	-	-	-	-	+	+	+
Provide AAC mechanisms for constrained devices	-	-	+	-	-	+	+
Support for a massive number of devices	-	-	+	-	-	+	+

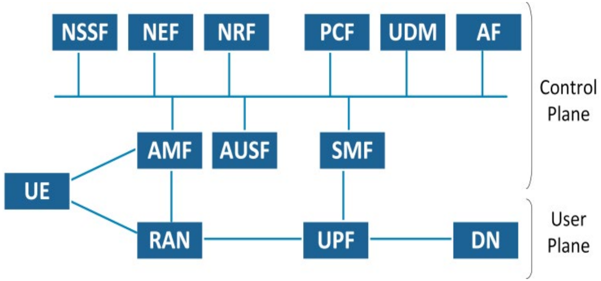
Testbed

Where did we implement the new nework function?





What are the security advantages in 5G-SSAAC?



Address the attacks against AMF as the single point of failure

Address software attacks against AMF

Provide business confidentiality for the 3rd parties

the security of each 3rd party network slice and its provided devices are under the responsibility of the 3rd party itself

What are the security concerns in 5G-SSAAC?

our proposal is a distributed approach and the security monitoring in this approach is more challenging than the security monitoring in a centralized approach

Securing the isolation of the 3rd parties' slices requires more attention

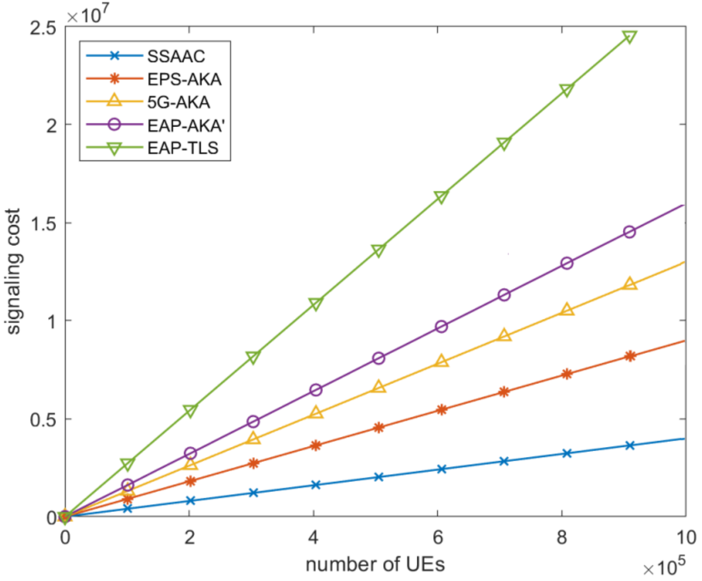
- well-defined security SLAs (Service Level Agreement)
- proper implementations of them
- forcing all the actors to respect these SLAs

How about the performance?

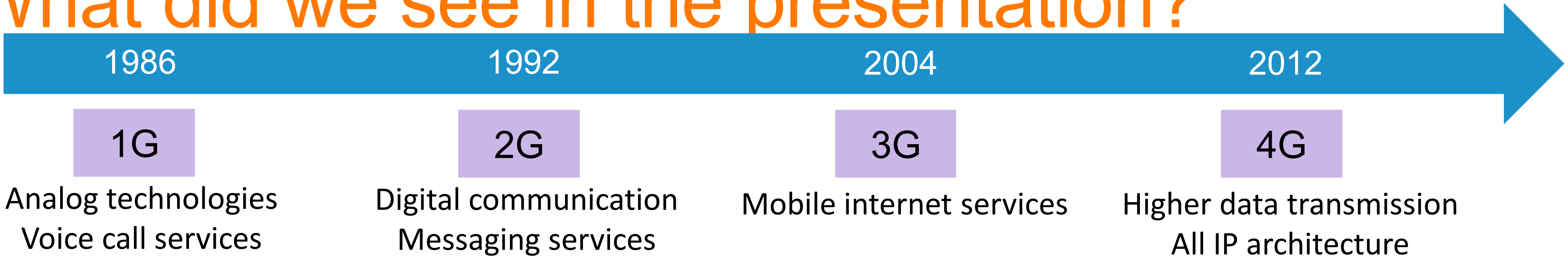
Protocol	Signaling cost on CN	Signaling cost on RAN	Overall signaling cost
EPS-AKA	5n	4n	9n
5G-AKA	9n	4n	13n
EAP-AKA'	11n	5n	16n
EAP-TLS	18n	9n	27n
SSAAC	0	4n	4n

Signaling cost: number of signaling messages exchanged between the device and the network, until it is attached to the network

n: number of devices



What did we see in the presentation?



1986

1G

Analog technologies
Voice call services

1992

2G

Digital communication
Messaging services

2004

3G

Mobile internet services

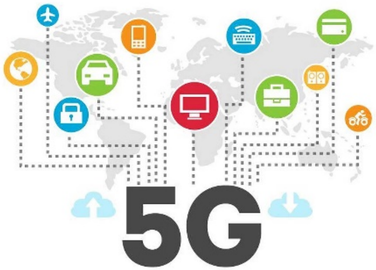
2012

4G

Higher data transmission
All IP architecture

No slicing in the AAC level
only one way of AAC for all types of slices

~2020



Connectivity provider has the central role in AAC

LoRaWAN

Thank You