Univerza v Ljubljani
Fakulteta za elektrotehniko

internet INSTITUTE://

Varnostna arhitektura 5G za internet stvari

Janez STERLE (ININ), Luka KORŠIČ(ININ), Urban SEDLAR (ULFE) in Mojca VOLK (ULFE)

janez.sterle@iinstitute.eu

VITEL 2019, Maj 2019, Brdo pri Kranju, Slovenija

INTERNET INSTITUT d.o.o.

- Zagonsko podjetje iz Ljubljane, Slovenija
  - ustanovljeno 2014
- Področja delovanja in ekspertiza
  - rešitve za zagotavljanje kakovosti (QA) v mobilnih, fiksnih in oblačnih sistemih – www.qmon.eu
  - rešitve za kritične komunikacije (PPDR, Javna Varnost) na tehnologijah IoT/5G – www.imon.si

MATILDA
www.matilda-5g.eu

5GINFIRE
5Ginfire.eu

PPDRONE
5GSafety.net

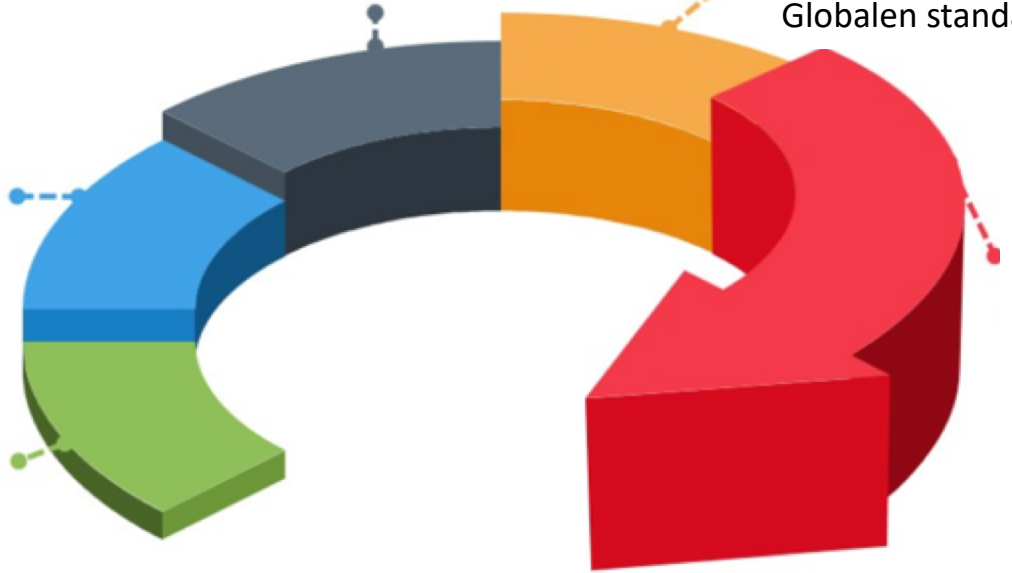
5G PPP PUBLIC-PRIVATE PARTNERSHIP
5g-ppp.eu

internet INSTITUTE//

Evolucija mobilnih tehnologij

3G/UMTS
Podatki
Multimedija

4G/LTE
All IP
Globalen standard



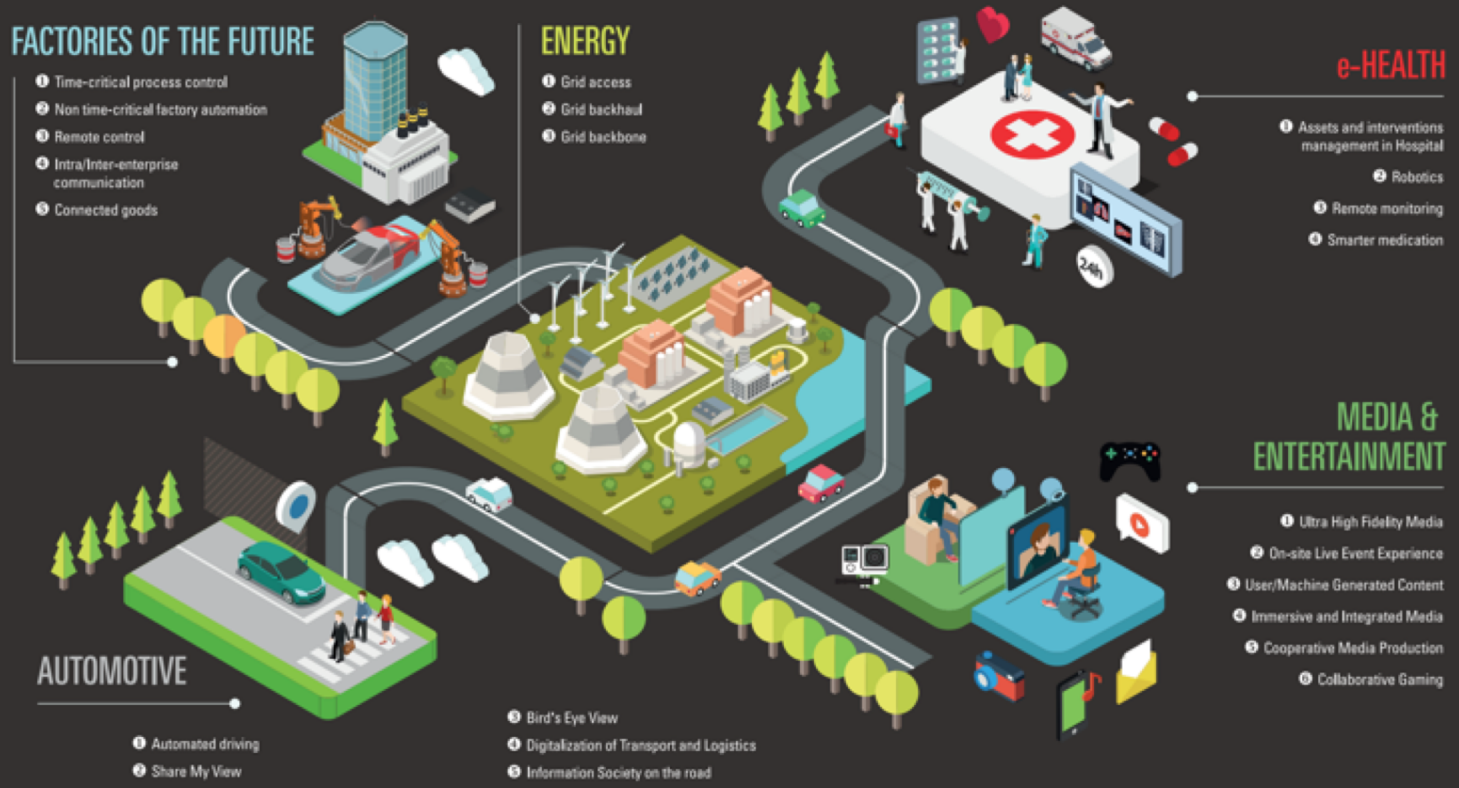
2G/GSM
Digitalen sistem
Gostovanje

NMT
Analogen sistem
Govor

5G
VNF/SDN, mMTC, eMBB, URLLC

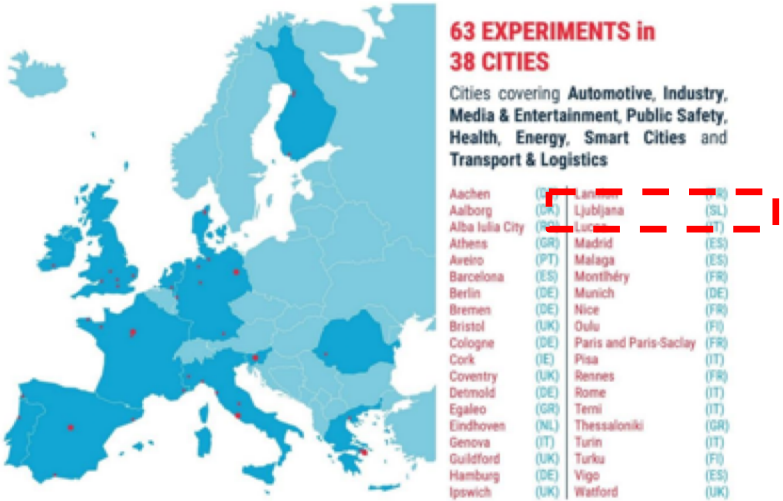
Podpora industrijskim vertikalam

Industrijske vertikale



Vir: 5g-ppp.eu

Pilotne postavitve 5G v EU



63 EXPERIMENTS in 38 CITIES

Cities covering **Automotive, Industry, Media & Entertainment, Public Safety, Health, Energy, Smart Cities** and **Transport & Logistics**

Aachen	(DE)	Ljubljana	(SL)
Aalborg	(DK)	Luxembourg	(LU)
Alba Iulia City	(RO)	Madrid	(ES)
Athens	(GR)	Malaga	(ES)
Aveiro	(PT)	Montbéry	(FR)
Barcelona	(ES)	Munich	(DE)
Berlin	(DE)	Nice	(FR)
Bremen	(DE)	Oulu	(FI)
Bristol	(UK)	Paris and Paris-Saclay	(FR)
Cologne	(DE)	Pisa	(IT)
Cork	(IE)	Rennes	(FR)
Coventry	(UK)	Rome	(IT)
Detmold	(DE)	Terni	(IT)
Egaleo	(GR)	Thessaloniki	(GR)
Eindhoven	(NL)	Turin	(IT)
Genova	(IT)	Turku	(FI)
Guildford	(UK)	Vigo	(ES)
Hamburg	(DE)	Watford	(UK)
Ipswich	(UK)		

5G IA INFRASTRUCTURE ASSOCIATION

5G PPP PUBLIC-PRIVATE PARTNERSHIP

Trial roadmap version 4.0
November 2018

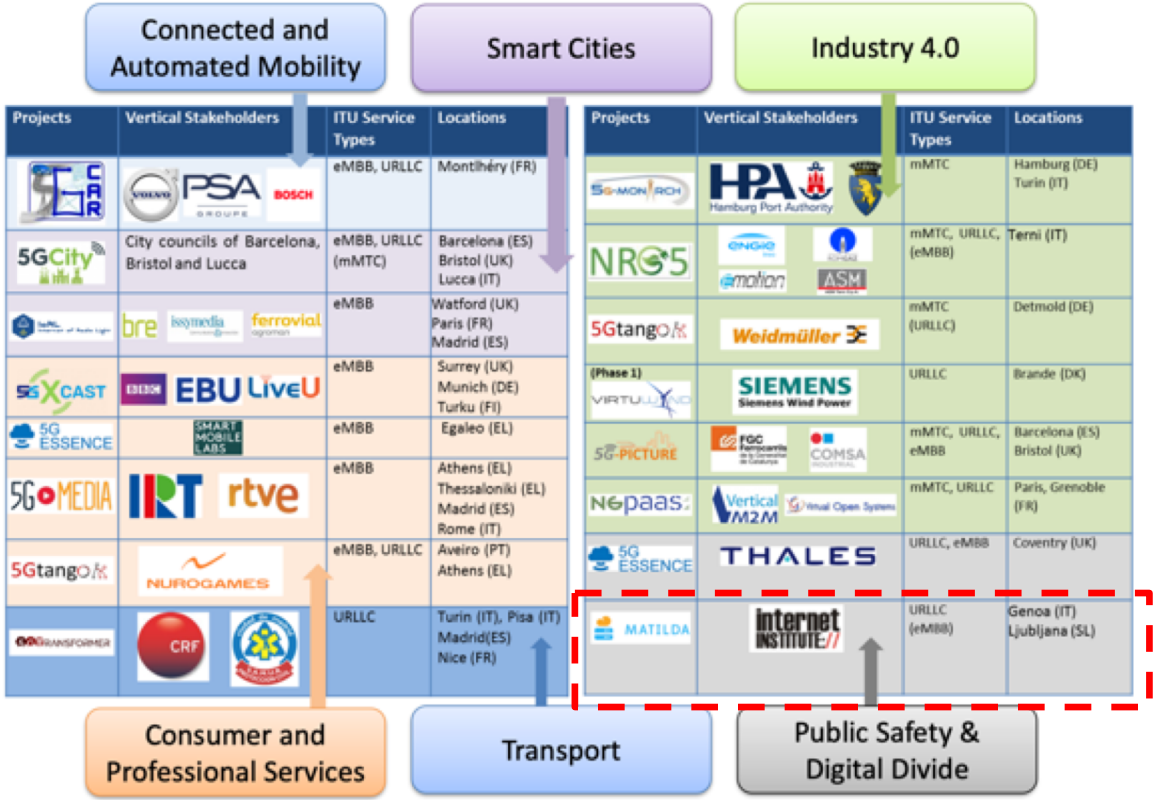
Source: **Vertical Cartography** (http://global5g.org/cartography) *
- 63 trials in 38 cities across 13 Member States covering 8 vertical sectors

*Developed in the context of the TB Vertical Cartography ad-hoc Team and Trials WG Roadmap Version 4.0

Vir: https://5g-ppp.eu/5g-trials-roadmap/

internet INSTITUTE://

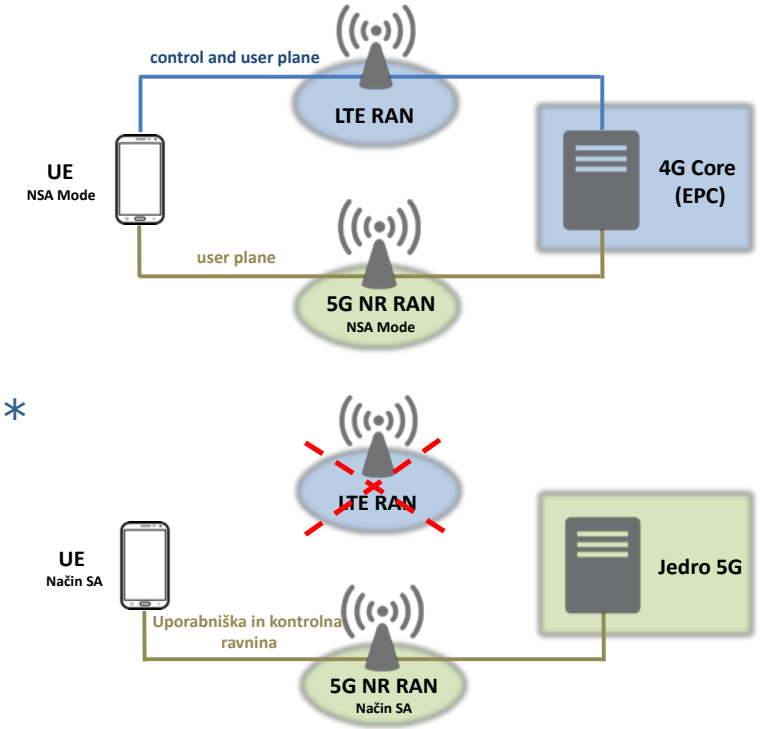
Pilotne postavitve 5G v EU



Vir: https://5g-ppp.eu/

Uvajanje 5G

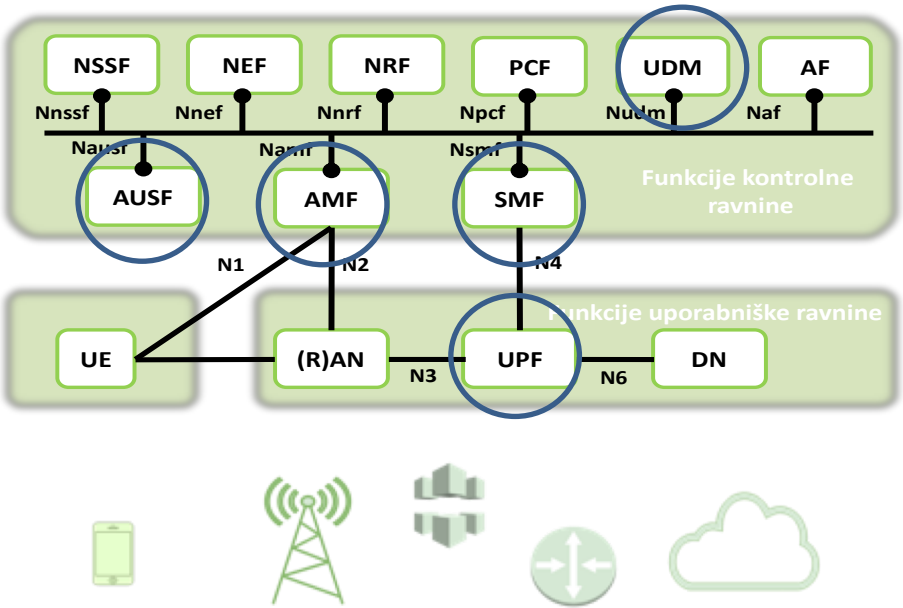
- 5G v načinu NSA (angl. Non-Standalone mode)*
  - Kontrolno ravnino zagotavlja 4G
  - Varnostna arhitektura LTE/4G
    - Avtentikacija EPS AKA
    - Varnostne storitve EN-DC (Dual Connectivity)
- 5G v načinu SA (angl. Standalone mode)*
  - Samostojno delovanje sistema 5G
  - Nova varnostna arhitektura 5G**
    - Avtentikacija 5G AKA in EAP-AKA
    - Novi varnostni model in hierarhija ključev



*Ref.: 3GPP TS 23.501, Rel. 15
**Ref.: 3GPP TS 33.501

Storitveno usmerjena arhitektura 5G

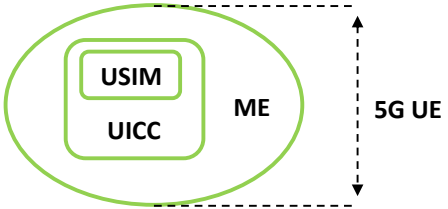
- Strogo ločevanje uporabniških in kontrolnih funkcij
- Krmilna ravnina
  - en vmesnik na funkcijo
  - povezovanje po princip enotnega vodila
- Implementacija komponent – navidezne omrežne funkcije (VNF)

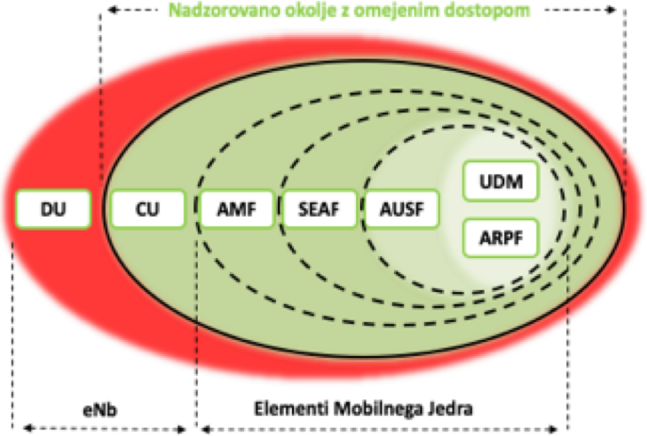


Ref.: 3GPP TS 23.501

Varnostni koncepti 5G – gNb

- Uporabniški agent (5G UE)
  - varnostni modul UICC*
  - modul USIM
  - mobilna oprema ME
- Bazna postaja 5G
  - centralna enota (angl. CU – Central Units)
    - nadzorovano okolje
    - signalizacijske funkcije
    - varnostne storitve (enkripcija in integriteta)
  - distribuirana (angl. DU – Distributed Units)
    - "odprto" okolje
    - transparentno posredovanje signalizacije in uporabniškega prometa med 5G UE in CU

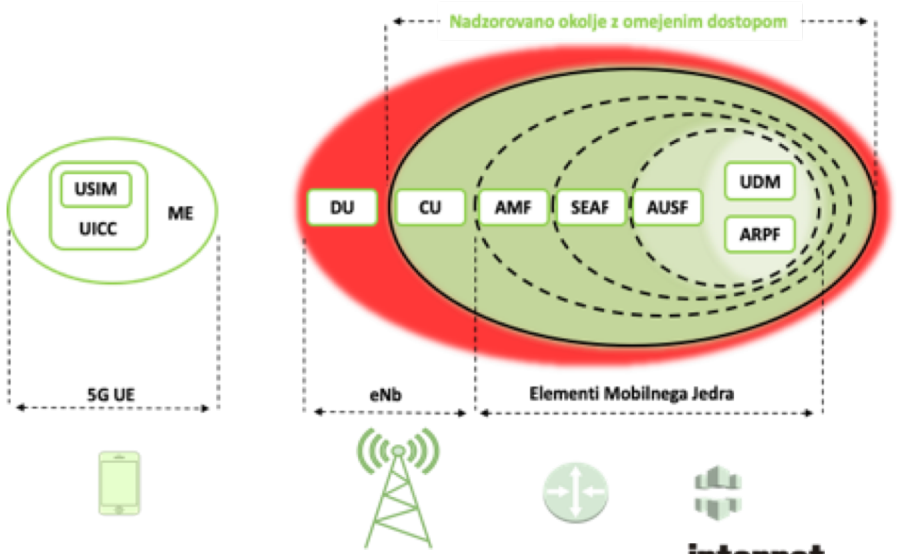




Varnostni koncepti 5G – CN

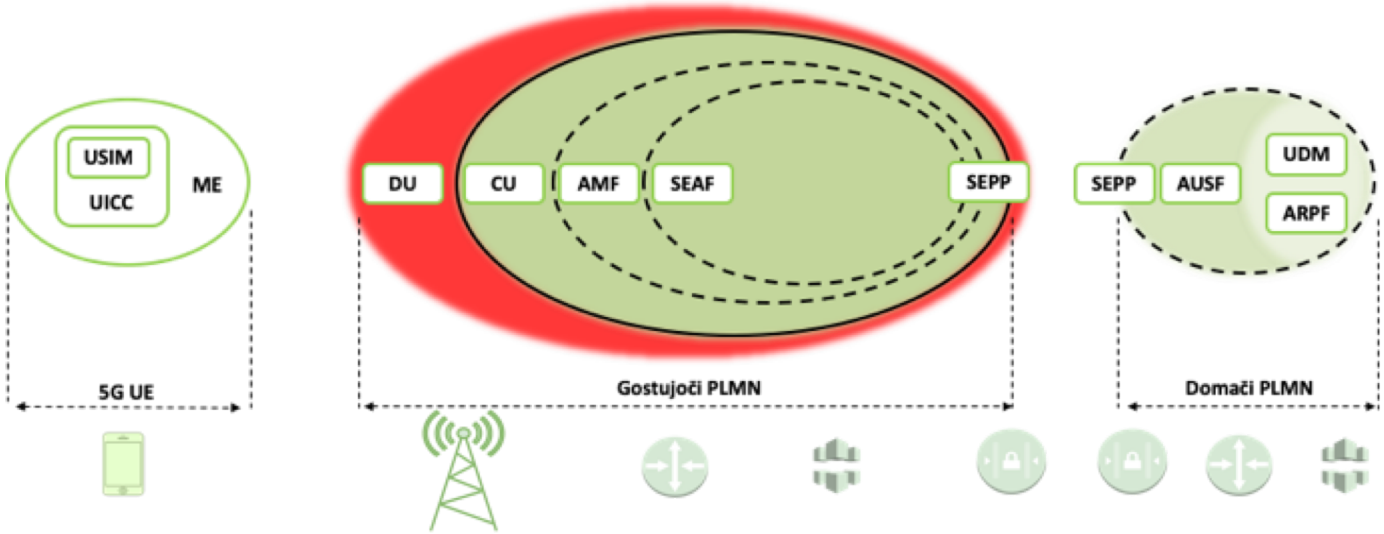
- Mobilno jedro (angl. CN – Core Network)
  - centralizirana funkcija avtentikacijskega centra ARPF
    - dolgoročni varnostni ključi
    - primarna avtentikacija
  - funkcija avtentikacijkega strežnika AUSF
    - korenski ključ uporabnika
    - prijava na več različnih dostopovnih sistemov (npr. 5G in WiFI)
  - funkcija varnostnega sidra SEAF
    - hrani varnostne vektorje uporabnikov
  - funkcija za upravljanje dostopa in mobilnosti AMF
    - terminacija varnostnih relacij

Arhitektura omogoča ločitev nalog za izvajanje mobilnosti in varnostnih storitev



Varnostni koncepti 5G – gostovanje

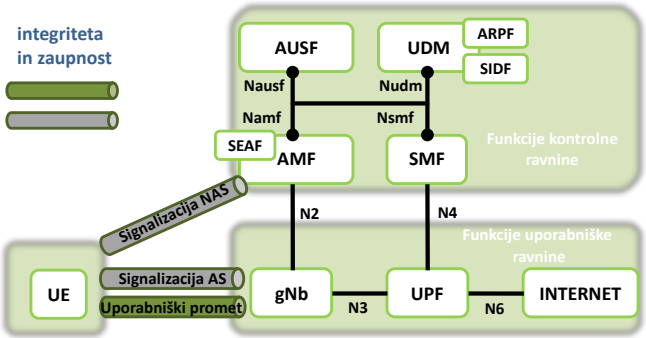
- Varnostnim proksi prehod SEPP
  - povezuje gostujoči in domači PLMN
  - kontrola in varna izmenjavo signalizacije



internet INSTITUTE//

Varnostne storitve 5G

- Zasebnost (identitete) uporabnika
  - asimetrična enkripcija identitete SUPI* (Subscription Identifier/IMSI)
- Vzajemna avtentikacija med terminalom UE in sistemom 5G
  - komplementarni avtentikacijski metodi 5G-AKA ter EAP-AKA
  - opcijske metode npr. EAP-TLS
- Razširjena avtentikacija med napravo UE in storitvenimi podsistemi
  - Procedure EAP
- Integriteta in zaupnost kontrolne ravnine**
  - dostopovne relacije AS in jedrne relacije NAS
- Integriteta in zaupnost uporabniške ravnine**
  - uporabniški promet med UE in gNb

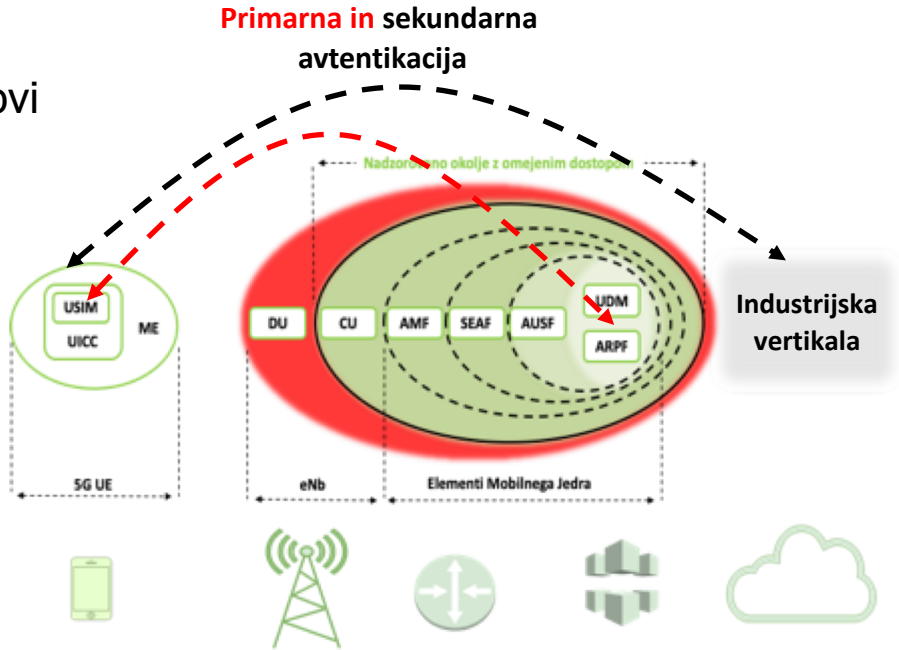


**algoritmi AES, SNOW, ZUC

*uporaba javnega ključa operaterja in algoritma ECIES

Avtentikacija

- Primarna avtentikacija
  - mehanizma 5G AKA ali EAP-AKA
  - primarni avtentikacijski vektor zagotovi dolgoročni ključ uporabnika LSK
    - shranjen na modulu USIM in v avtentikacijskem centru ARPF
- Sekundarna avtentikacija
  - mehanizem EAP
  - avtentikacija me UE in storitvenimi sistemi 5G (industrijske vertikale)

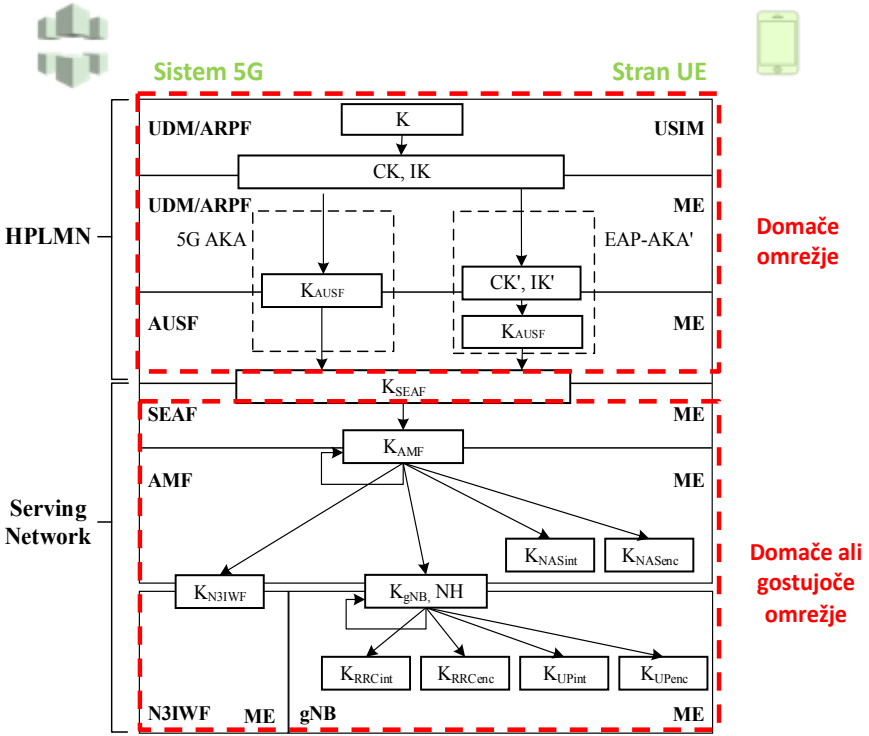


Hierarhija varnostnih ključev

- Hierarhija varnostnih ključev
- Procesa distribucije varnostnih ključev
  - izračun delovnih integritetnih in enkipcijskih ključev
  - zaščita signalizacije AS in NAS
  - zaščita uporabniškega prometa

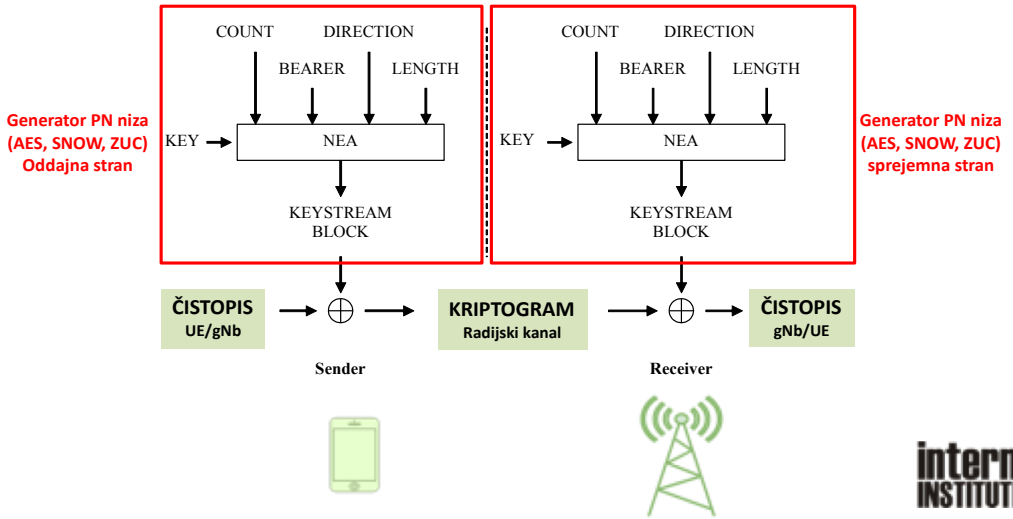
Integritetni ključ za zaščito signalizacije NAS (KNASint) in AS (KASint) ter uporabniške ravnine (KUPint)

Enkripcijski ključi za zaščito signalizacije NAS (KNASenc) in AS (KASenc) ter uporabniške ravnine (KUPenc)



Proces zaupnosti

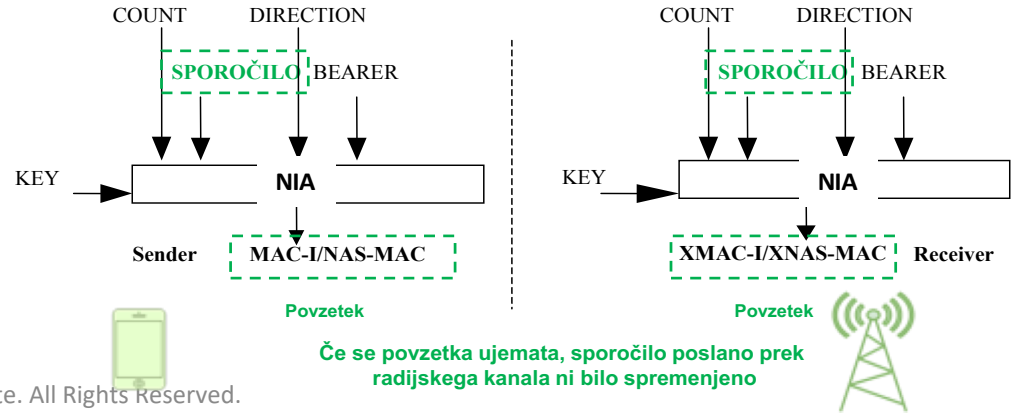
- Omogoča zaupnost komunikacije prek radia 5G NR
  - uporaba enkripcijskih algoritmov AES, SNOW ali ZUC
  - delovanje v načinu »stram cipher«
  - Kriptogram, na osnovi XOR operacije nad čistopisom in psevdo-naključnim nizom



Nizi PN, ki jih generirajo algoritmi AES, SNOW in ZUC, so končne dolžine, zato je potrebna redna menjava vektorjev, iz katerih se izračunavajo

Proces integritete

- Izvede se pred prenosom signalizacije oz. uporabniških podatkov preko radia 5G
- Uporaba funkcij MAC (Message Authentication Codes)
  - izračunani povzetki so odvisni tudi od uporabljenega varnostnega ključa
  - detekcija sprememb v sporočilih/podatkih pri prenosu



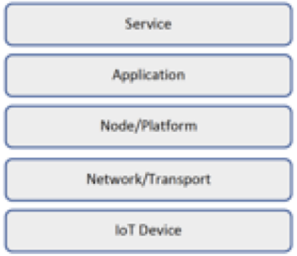
Primerjava pristopov 4G/5G

Varnostna funkcija	Tehnologija 5G	Tehnologija 4G
Zasebnost (identitete) uporabnika SUPI/IMSI (prijava v omrežje)	✓	✗
Začasna identiteta 5G/GUTI	✓	✓
Zaupnost kontrolne ravnine	✓	✓
Integriteta kontrolne ravnine	✓	✓
Zaupnost uporabniške ravnine	✓	✓
Integriteta uporabniške ravnine	✓	✗
Funkcija SEPP - gostovanje	✓	✗
Opcijski avtentikacijski mehanizmi	✓	✗

internet INSTITUTE://

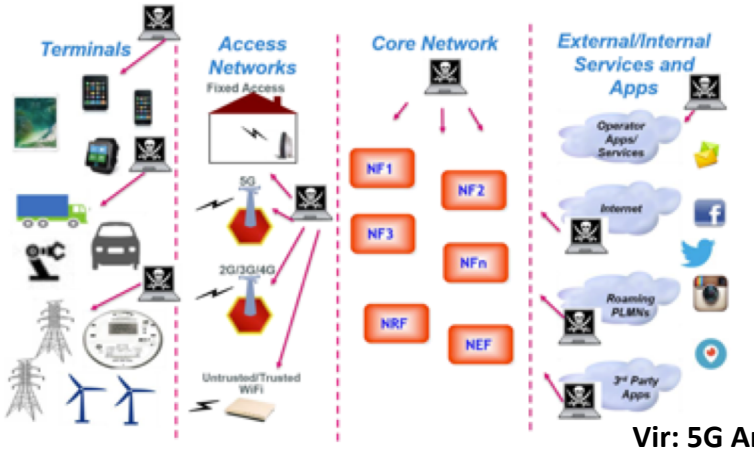
Varnostni izzivi 5G

- Manjko praktičnih implementacij sistemov 5G
- Manjko primerov dobrih praks in operativnih postopkov
- Identifikacija varnostnih groženj "threat surface"
- Definicija varnostnih ukrepov "mitigation techniques"
- Pilotne postavitve, testiranje, verifikacija,...!



Varnostni nivoji za IoT

5G THREAT SURFACE FOR MASSIVE IOT
UE THREATS
RAN THREATS
Rogue Base Station
UBSCRIBER PRIVACY THREATS
CORE NETWORK THREATS
NETWORK SLICING THREATS
NFV AND SDN THREATS
INTERWORKING AND ROAMING THREATS



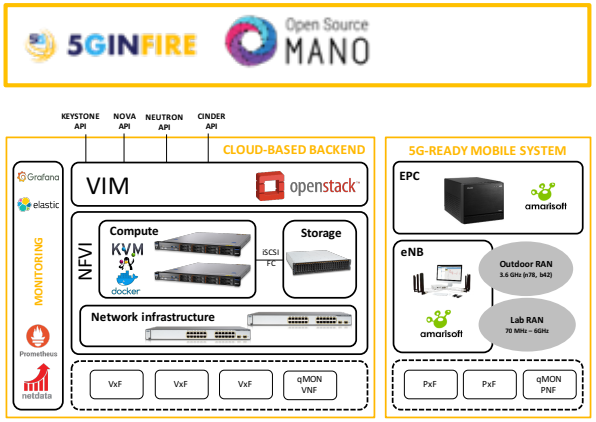
Vir: 5G Americas

PPDR ONE

5GINFIRE

- "5G-ORIENTED EXPERIMENTAL PLAYGROUND FOR VERTICAL INDUSTRIES"
  - Odprta infrastruktura namenjena pilotnim postavitvam in verifikaciji okolij VNF/5G
  - H2020 EU projekt, št. 732497, Obdobje: 1/2017 – 12/2019
  - Info o projektu: www.5ginfire.eu
  - Info o PPDR ONE Facility: 5Gsafety.net

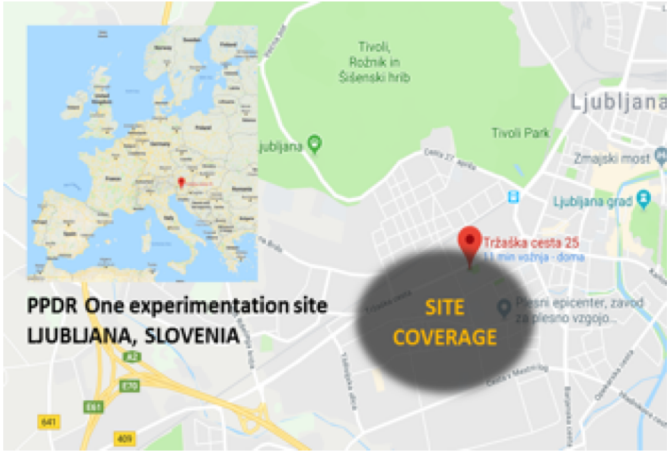
EURESCOM b com



PPDR ONE

5GINFIRE

- **PPDR ONE stacionarni mobilni sistem**
  - **"Indoor" postavitev**
    - Laboratorijsko testiranje na vseh operativnih frekvencah LTE/4G, od 70 MHz do 6 GHz
  - **"Outdoor" postavitev**
    - Zunanja postavitev na "5G pioneering band" (3.6 GHz, 5G band n78) in "4G band" (3.6 GHz, b42)
- **PPDR ONE prenosen mobilni sistem**
  - **Prenosen kompakten sistem**
    - Namenjen za postavitve na lokaciji eksperimentov
    - Pokriva laboratorijsko testiranje (frekvence od 70 MHz do 6.0 GHz) ter zunanje postavitve



internet INSTITUTE://

INTERNET INSTITUT d.o.o.
PE Ljubljana
Tržaška cesta 25
SI-1000 Ljubljana
Slovenija (EU)

Sedež podjetja
Črna vas 128
SI-1000 Ljubljana
Slovenija (EU)

info@iinstitute.eu

www.matilda-5g.eu

5Ginfire.eu

5GSafety.net

5g-ppp.eu

Hvala!

