5G
Lawful Interception
Security

Contesto di riferimento

Questa presentazione prende spunto:

- dal Position paper 8268/19 - 11 April 2019 5G prodotto da Europol per il Council of the European Union Brussels.

In cui sono indicate possibili criticità per l'intercettazione delle comunicazioni nelle reti 5G e le protezioni introdotte dal nuovo framework 5G security

L'analisi ha lo scopo di rappresentare le funzionalità di LI e 5G Security definiti dal 3GPP SA3 Security Group.

Argomenti trattati

- Nuove specifiche LI per 5G
- Evoluzione dinamica della rete da 4G a 5G

Impatti LI su:

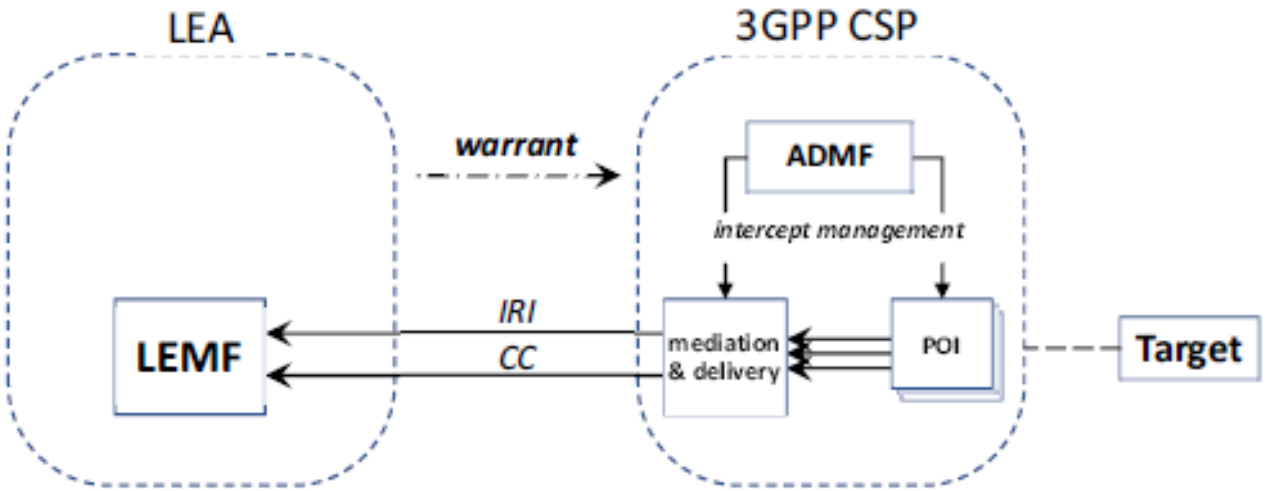
- Network slicing
- Network Function Virtualization – NFV
- Multi Edge Computing – MEC
- Interworking LI 3G, 4G, 5G e impatto sui LEMF

Intercettazione delle comunicazioni - LI

La tecnologia 5G (R15), presenta una nuova architettura di rete orientata ai servizi SBA (Service Based Architecture) introducedo elementi e funzioni aggiuntivr rispetto al 4G

Contestualmente al cambio di architettura il 3GPP Security Group SA3 ha prodotto un nuovo gruppo di specifiche, in materia d'intercettazione delle comunicazioni, mantenendo inalterato il medello ETSI / 3GPP.

Nella figura seguente è rappresentata la mappa delle specifiche per 5G (opzione 2) che sostituiscono quelle applicate fino alle release R14.



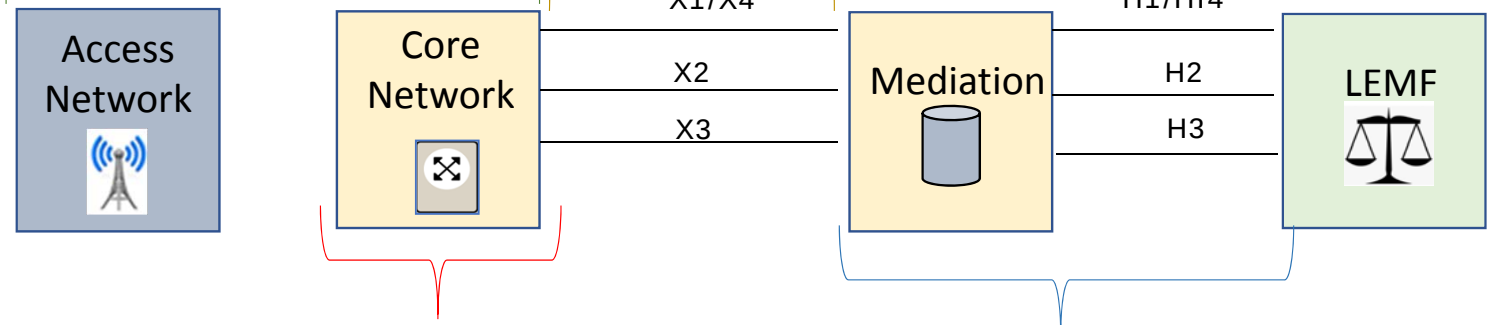
Generic Lawful Interception model
Source 3GPP TS 33 126

Lawful Interception - Specification MAP

New ETSI TS 103 221-1 V1.1.1
Part 1: Internal Network Interface X1 for Lawful Interception
New ETSI TS 103 221-2 V1.1.1 Lawful Interception (LI);
Part 2: Internal Network Interface X2/X3 for Lawful Interception

Frozen

3GPP TS 33.126 v. 15.0.0
LI requirements



3GPP TS 33.127 v. 15.0.0
LI Architecture and functions

3GPP TS 33.128 version 15.0.0 Release 15
Protocol and procedures for Lawful Interception (LI);

Lawful Interception - Specification MAP

Il ciclo di vita e l'architettura delle interfacce LI replicano il modello già definito da ETSI/3GPP per le tecnologie 2G, 3G, 4G.

Nell'architettura LI 5G le interfacce HI sono 4 anziché 3 specificate per le tecnologie precedenti.

- **HI1** per inviare l'ordine di intercettazione o altre informazioni dal LEA (Lawful Enforcement Agency = AG) al CSP (Communication Service Provider).

  E' stato specificata l'interfaccia per l'invio della richiesta da AG a CSP: ETSI TS 103 120 V1.2.1 (2016-03)Lawful Interception (LI); Interface for warrant information

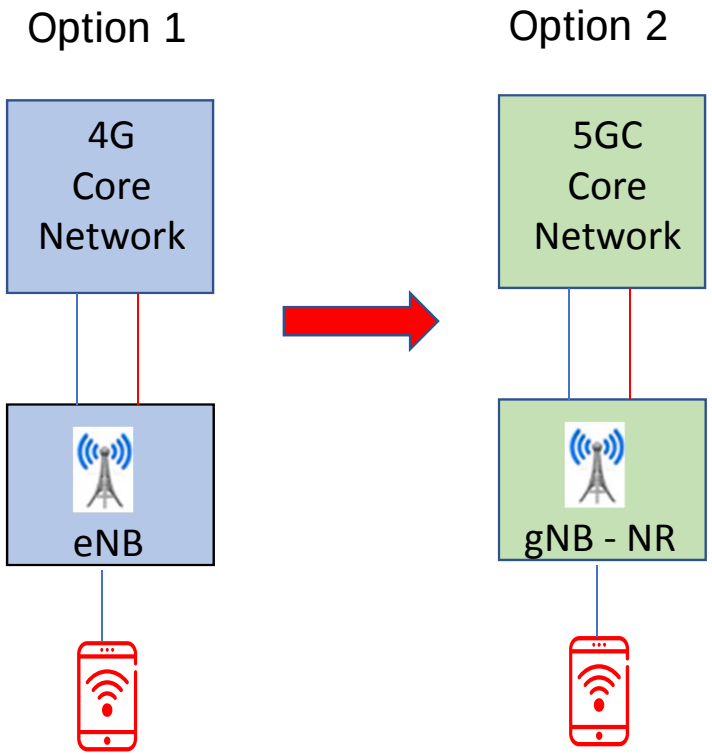
- **HI2** per inviare gli IRI da CSP al LEMF

- **HI3** per inviare il CC payload da CSP a LEMF

- **H4** per inviare le informazioni di attivazione, cessazione, proroga, data/ora attivazione e cessazione richiesta da CSP a LEMF .

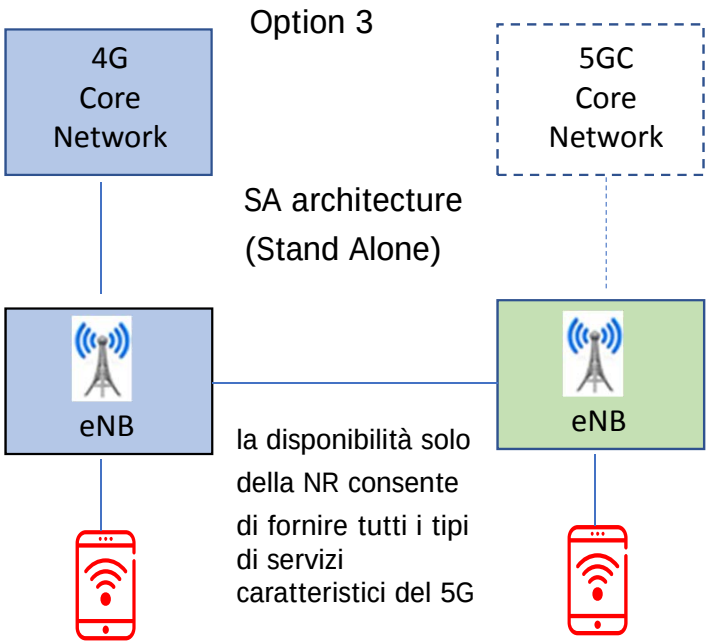
4G – 5G replacement

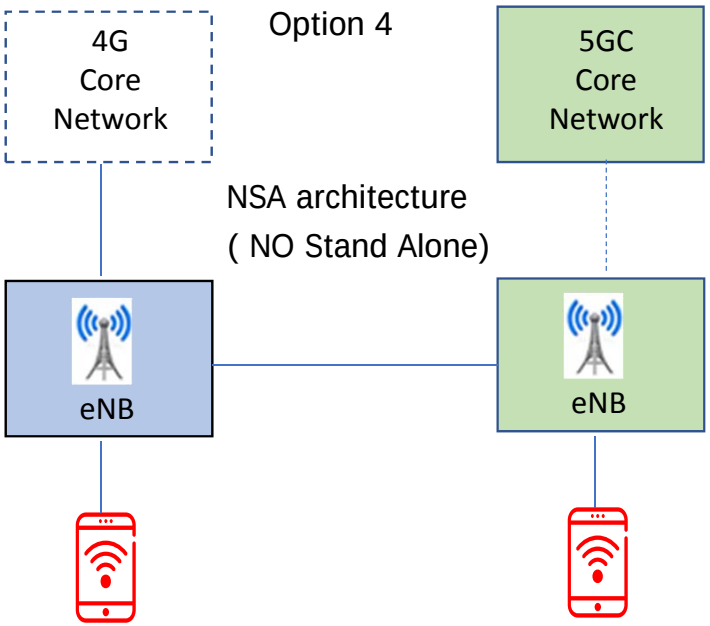
L'applicazione delle specifiche LI 5G deve considerare il contesto dinamico di evoluzione della rete.



4G – 5G replacement

Per la transizione da 4G a 5G sono previsti sei opzioni di modifica delle architetture.
L'opzione 3 prevede la disponibilità della nuova rete radio NR non della Core Network 5GC.
E' la soluzione architetturale che verosimilmente sarà utilizzata da tutti gli Operatori.
Con l'opzione 3 per le funzioni di intercettazione continuano ad essere applcate le specifiche ETSI / 3GPP già in uso





Network slicing

Lo slicing di rete è una tecnologia che consente di creare più reti logiche all'interno di un'infrastruttura fisica condivisa comune. Slicing sfrutta i principi della virtualizzazione delle funzioni di rete (NFV)

La suddivisione della rete in slices consente agli Operatori di

- allocare la quantità appropriata di risorse di rete a una specifica slice
- fornire con la medesima porzione di rete servizi utilizzano l'accesso radio con le stesse caratteristiche

Esempi di servizi correlati al tipo di accesso radio

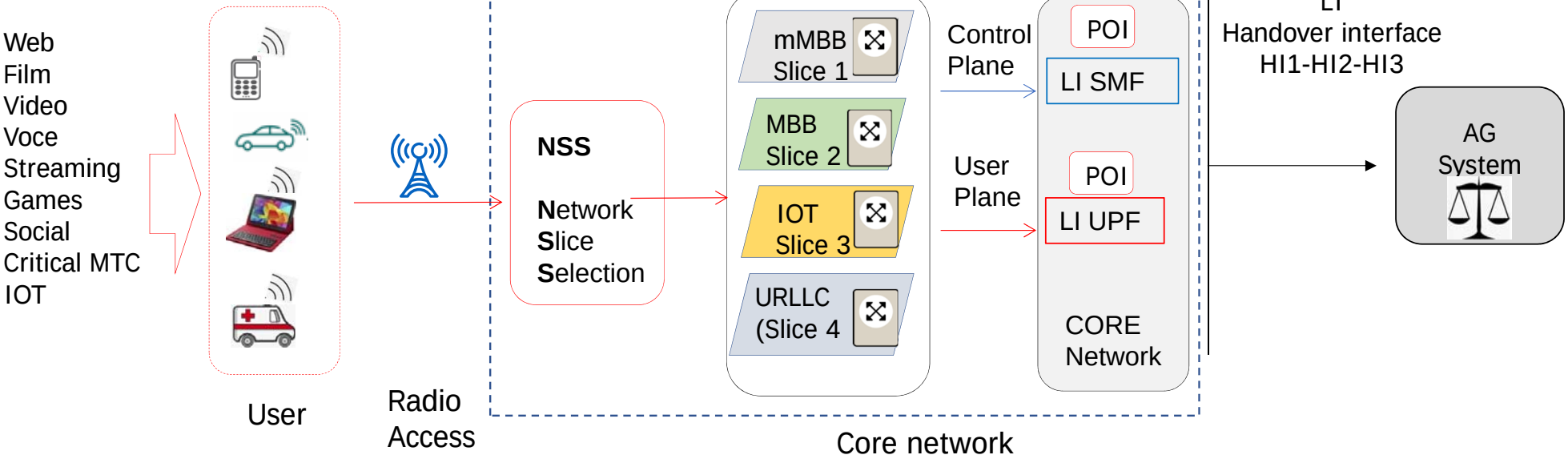
- Enhanced Mobile Broadband (eMBB): servizi broadband con trasmissioni a grande velocità. Sono comprese in questa categoria le comunicazioni ad altissima densità di connessioni contemporanee (mMBB - massive Mobile Broadband)
- Machine Type Communication, (MTC): servizi di comunicazione per dispositivi di ogni tipo. Sono compresi in questa categoria i servizi - HTM (Human To Machine) - MTM (Machine To Machine)
- Critical Communications: comunicazioni ultra-affidabili (reliability) a bassa latenza (latency) per servizi di connettività che richiedono elevati standard di sicurezza ed affidabilità

5G Network slicing - Lawful Interception

Slice utilizzata per servizi specifici.

POI (Point Of Interception)

SMF Session Management Function
User Plane Function



Slice utilizzata da terze parti

La gestione di Slicing di rete può essere applicata in diversi modelli architetturali:

- Slices utilizzate tutte all'interno di un unico CSP (Communication Service Provider)
- Slice fornita a terze parti come servizio: Network Slice as a Service (NSaaS).

Un CSP può offrire una slice ad un CSC (Communication Service Customer – (ad es. un MVNO) sotto forma di un servizio di comunicazione (NSaaS) che il CSC gestisce autonomamente come rete propria per offrire i servizi di comunicazione ai propri clienti

LI in Network slicing
Impatti con LI

La suddivisione della rete in slice non ha alcun impatto sulla intercettazione delle comunicazioni.

Il provisioning di LI si propaga a tutte le slices che forniscono i servizi richiesti dal target
L'architettura 5G include l'elemento NSSF (Nerwork Slice Selection Function) che identifica la lista di slices associate all'utente.

Le specifiche 3GPP TS 33 127 e TS 33 128 includono il requisito d'inviare al LEMF:

- il contenuto della comunicazione (CC Payload)

- gli IRI con le informazioni di:
  - Registration type information.
  - Access type information.
  - Requested slice information.

Network Function Virtualization
NFV

Il sottogruppo di ETSI: Industry Specification Group (ISG) Network Functions Virtualisation (NFV) ha definito l'architettura, le funzioni ed i requisiti di sicurezza da applicare per la virtualizzazione della rete.

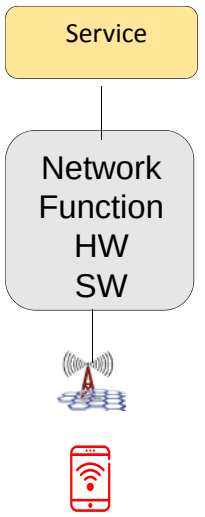
NFV si riferisce alla sostituzione di dispositivi hardware specializzati tradizionali con software che può essere installato su hardware standardizzato.

NFV è basato su software, cioè tutte le funzioni di un tradizionale elemento di rete (ad esempio uno"switch")sono gestite da una funzione di rete virtuale (VNF), simile un programma su un PC.

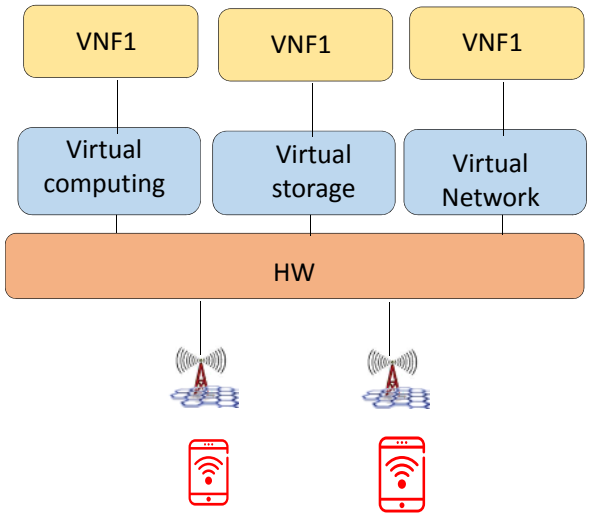
Le varie funzioni (VNF) sono gestite da un Hypervisor.

NFV

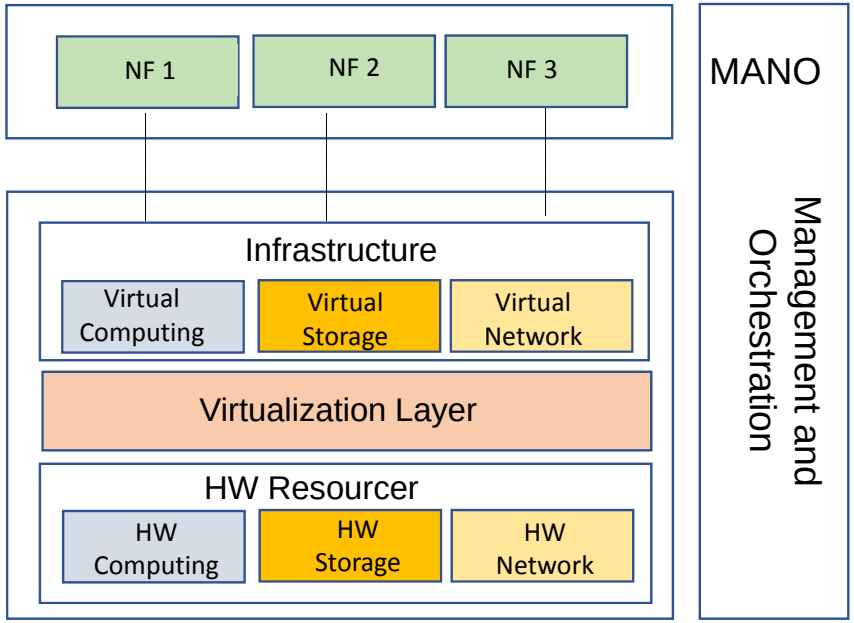
Network Function
In ogni NF risiede
HW e SW



Separazione HW e SW
Virtual Network Function
Un SW è utilizzato da più NF



NFV ETSI Model



Network Function Virtualization

Il sottogruppo di ETSI: Industry Specification Group (ISG) Network Functions Virtualisation (NFV) ha definite:

- l'architettura,
- le funzioni
- i requisiti di sicurezza.
- I requisiti per le funzioni d’intercettazione legale.

Le implicazioni per gli aspetti di LI sono descriiti nei due report:

- ETSI GS NFV-SEC 004 V1.1.1 Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implication

- ETSI GS NFV-SEC 011 V1.1.1 Network Functions Virtualisation (NFV);Security; Report on NFV LI Architecture

Network Function Virtualization

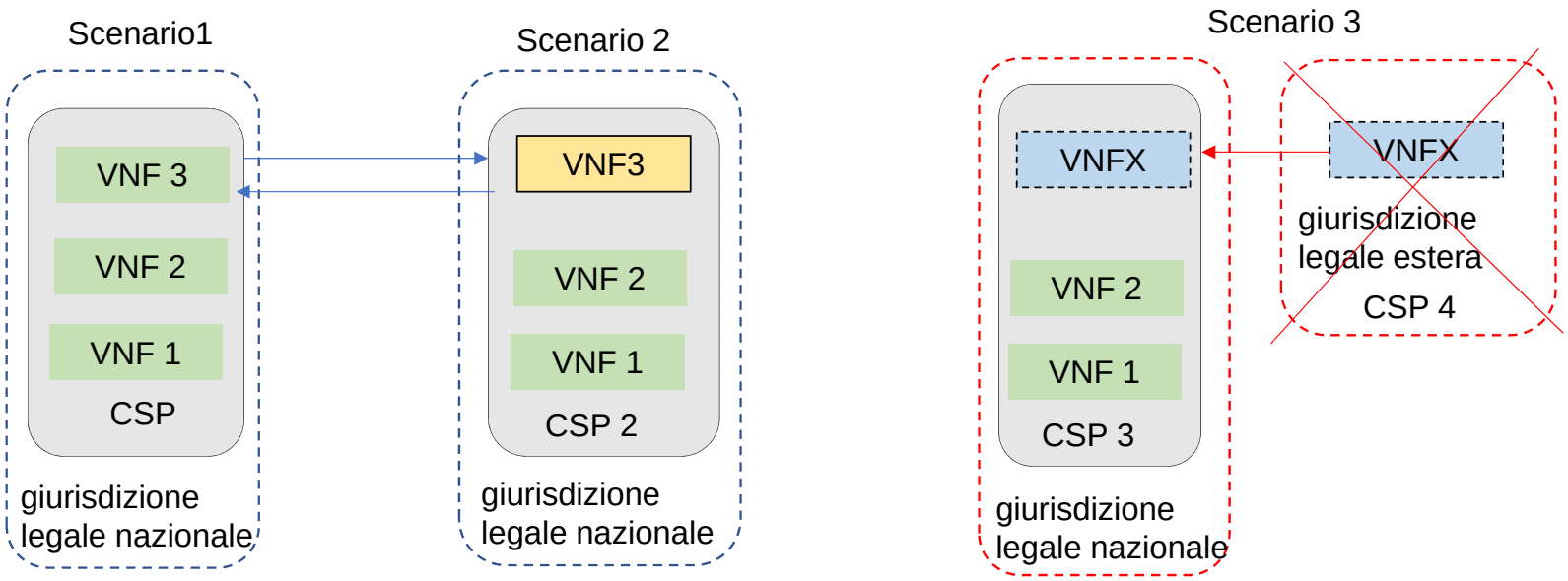
La ETSI GS NFV-SEC 004
definisce le informazioni (CC payload , IRI) che devono essere inviate al LEMF attraverso le interfacci HI 1, 2, 3.
Di fatto conferma i requisiti LI già specificati nelle TS 33 106, TS 33 107, TS 33 108 applicate fino al 4G

La ETSI GS NFV-SEC 011
elenca le raccomandazioni per LI che devono essere applicate dal CSP nella definizione dell'architettura NFV.
Di seguito i principi generali:

- Le funzioni di LI devono essere gestite completamente all'interno di un unico CSP
- Le funzioni di LI devono essere gestite completamente all'interno di un'unica giurisdizione legale
- Le funzioni di LI non devono essere visibili da soggetti non autorizzati (sistemi, o persone) esterni al CSP
- Le funzioni di LI non devono essere condivise tra CSP e tra giurisdizioni legali diverse
- Le funzioni di LI non possono essere implementate da un CSP di un paese per fornire la capacità di LI ad un CSP di un altro paese

Network Function Virtualization
esempi di scenari architetturali

- **Scenario 1**
  il CSP ha il controllo totale di tutte le funzioni di rete virtualizzate e quindi unico soggetto responsabile per la fornitura delle intercettazioni all'AG come prevede la regolamentazione nazionale
- **Scenario 2**
  il CSP1 fornisce VFN a CSP2, oppure CSP2 fornisce VFN a CSP. In entrambi i casi i CSP sono Operatori nazionali e quindi ciascuno è responsabile delle funzioni d' intercettazioni per l'AG
- **Scenario 3**
  Il CSP 3 fornisce ai propri clienti i servizi di una VFN localizzata in un paese estero. Il CSP 4 non garantisce le intercettazioni e il trattamento delle informazioni sensibili sono a rischi.



MEC

ETSI ISG MEC (Industry Specification Group for Multi-access Edge Computing)

Il MEC è una architettura che abilita un servizio ai margini (Edge) della rete per eseguire applicazioni in prossimità del dispositivo mobile con lo scopo evitare congestioni e minimizzare la latenza per tutti i servizi che richiedono una elevata e larghezza di banda e bassissima latenza (max 1 ms).

Spostando i contenuti critici ai margini della rete, diminuisce il carico della Core network

MEC Consente alle applicazioni software di accedere al contenuto dei servizi (es video 4K) e alle informazioni in tempo reale sulle condizioni della rete di accesso radio per ottimizzare la qualità della trasmissione.

Tipicamente MEC è utilizzata per

- Applicativi per veicoli a guida autonoma o altamente autonoma
- servizi video 4K con codifica video adattata alla capacità di downlink instantanea disponibile
- Video game
- servizi di localizzazione
- Internet-of-Things (IoT)
- realtà virtuale
- LAN aziendali
- ……

Requisiti minimi e parametri di qualità per i servizi 5G

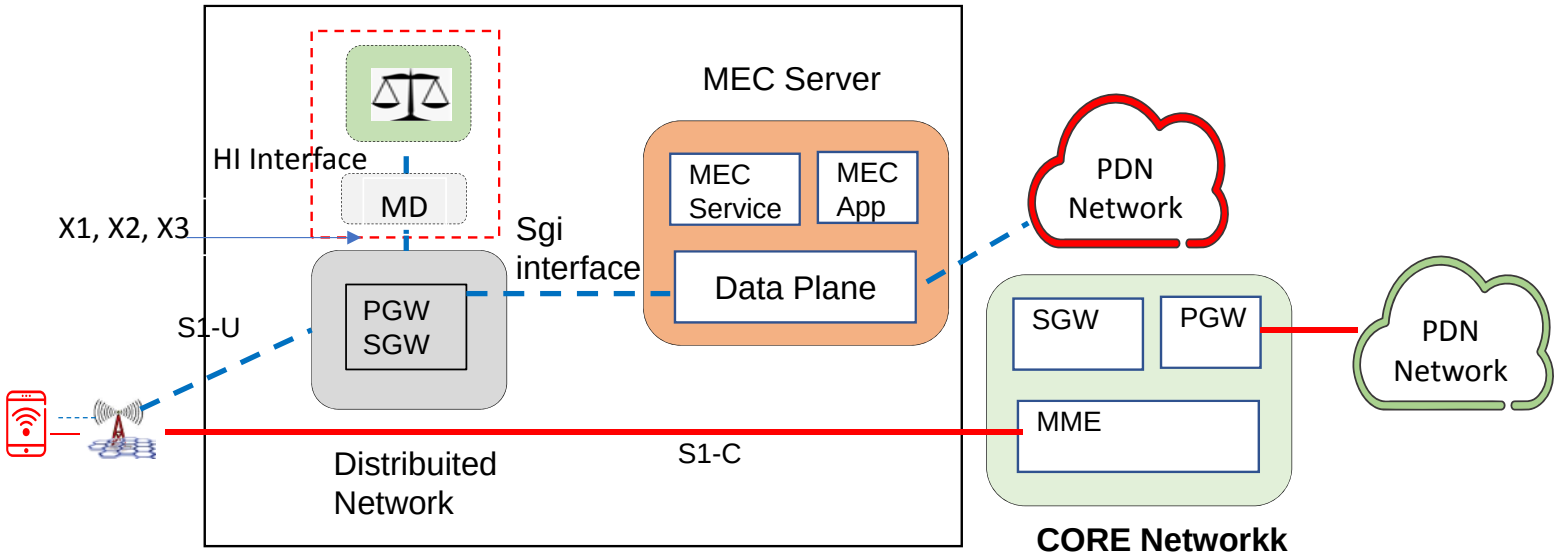
Source ITU Minimum Technical Performance Requirements for IMT-2020 radio interface

Technical Performance Requirement				
Technical requirement	Usage scenario applicability			Target value
	eMBB	mMTC	URLLC	
Peak date rate	X			• DL: 20 Gbps • UL: 10 Gbps
Connection density	X	X		• 1,000,000 devices /km2
Mobility interruption time	X		X	• 0 ms
Area traffic capacity	X			10 Mbit/ms
User plane latency	X		X	• URLLC: 1ms Ultra Reliability low Latency Communication • eMBB : 4ms
Control Plane Latency	X		X	• 20ms
User Plane Reliability			X	• $1^{10 - 5}$ • Success Probability for Tx 32Bytes in 1ms
Mobility	X		X	• Pedestrian: 0 km/h to 10 km/h • Vehicular: 10 km/h to 120 km/h • High speed vehicular: 120 to 500 km/h
User experienced data rate	X			• DL 100 Mbps • UL 50 Mbps

- DL downlink - UL uplink -
- eMBB (enhanced Mobile Broadband
- URLLC (Ultra Reliable Low Latency Communication)
- mMTC (massive Machine Type)

MEC deployment option on SGi interface

MEC può essere implementato con diverse architetture
In ogni caso, ai fini di LI, qualunque soluzione sia adottata, le architetture MEC che includono un gateway EPC, (SGW + PGW) e CUPS (Control Plane e User Plane Separation) sono conformi ai requisiti LI in quanto supportano nativamente le interfacce X1, X2, X3 per connettersi al MD responsabile della connessione con il LEMF per il trasferimento del traffico del target. Come esempio è riportata l'architettura di MEC sulla interfaccia SGi standardizzata da 3GPP, quindi è possibile il supporto per Lawful Interception (LI) e Data Retention (RD)



Source : ETSI GS MEC 026 V2.1.1 (2019-01) Multi-access Edge Computing(MEC);
Support for regulatory requirement

5G Security

5G Security - Le tecnologie 2, 3, 4 G hanno evidenziato importanti criticità su:

- Sicurezza dell’accesso radio (RAN).

Mancanza di riservatezza in alcuni messaggi di segnalazione, e violazione della identità dell’utente. Trasmissione dell'IMSI in chiaro durante le procedure di location update

- Criticità su procedure di mobilità (Mobility Management - MM) e scenari di roaming.

Nelle procedure di mobility management o di riautenticazione i parametri che identificano l’utente non sono crittografate, di conseguenza può essere rilevato il parametro IMSI con strumentazioni esterne alla rete.

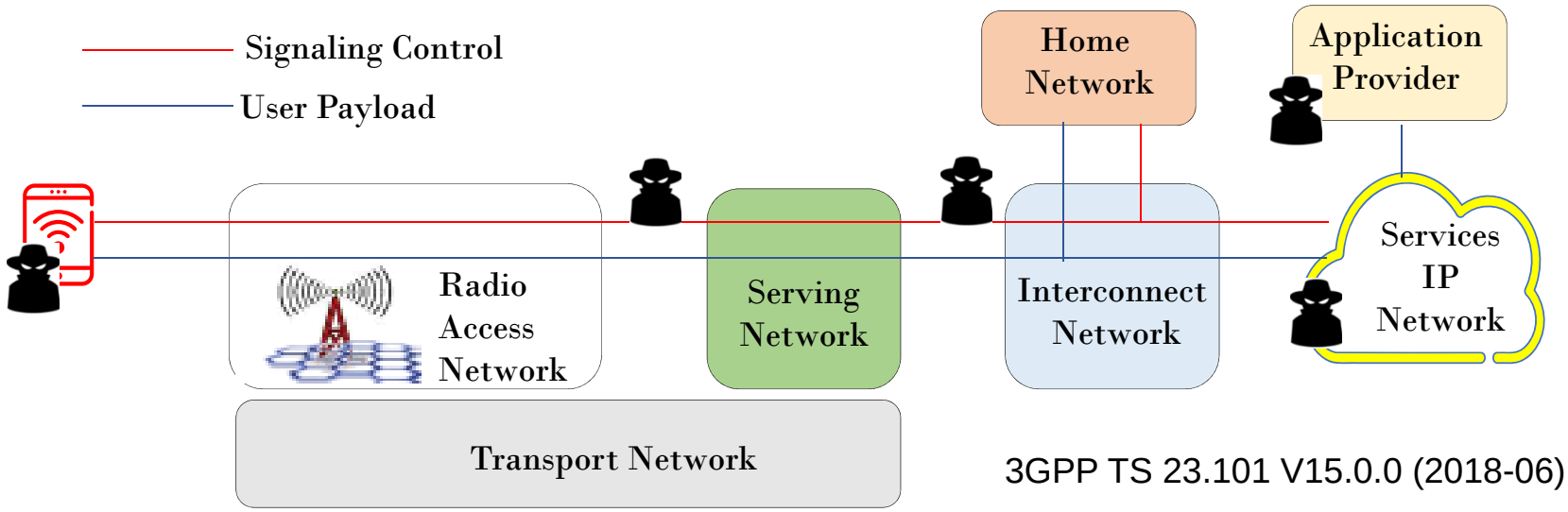
- Mancanza di autenticazione trusted reciproca tra rete e terminale con conseguenti attacchi come lo spoofing di rete

- Nessuna misura di sicurezza per i sistemi operativi, applicazioni e dati di configurazione presenti nei dispositivi d’utente

Mobile Network Model

In sintesi il modello di riferimento di una rete mofile è costituito dai seguenti elementi logici:

- Il terminale utente (UE), contenente il modulo (USIM)
- la Rete Home (HN) contenente il data base degli utenti dei servizi, certifica le credenziali dell'utente per la loro autenticazione, partecipa alle procedure di location update
- La serving network è la rete in cui l'utente è temporaneamente registrato. ha le funzioni di di mobility management, routing delle chiamate e del trasporto dei dati. Può appartenere alla stessa Home Network o ad un'altra rete nei casi di roaming.
- Application Provider

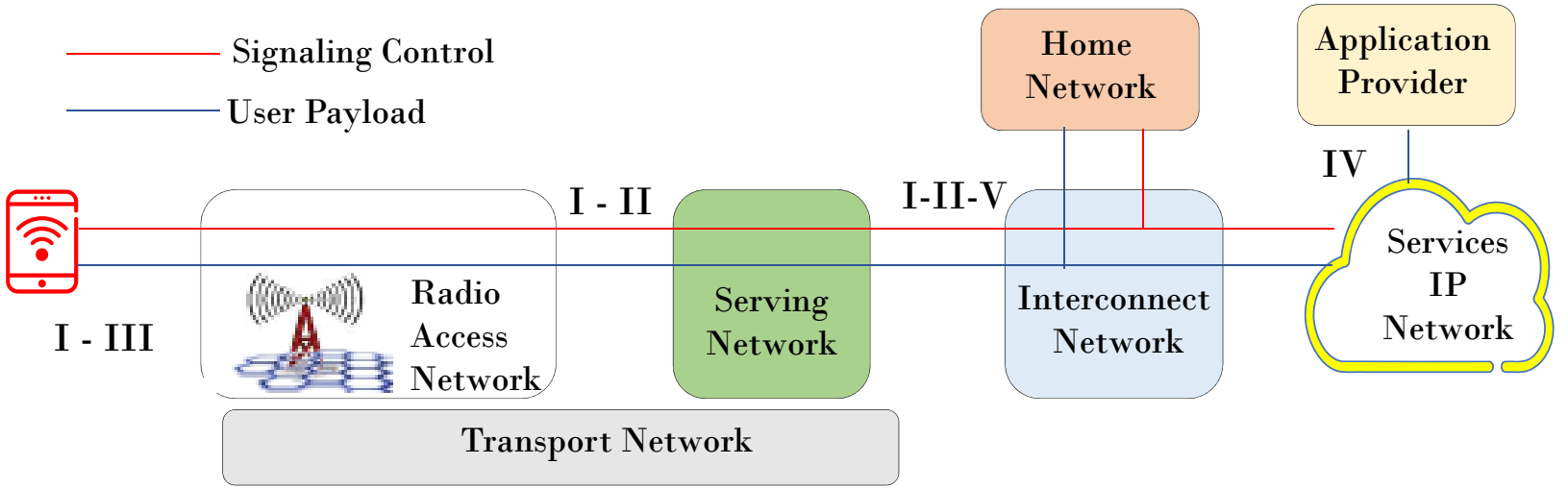


3GPP TS 23.101 V15.0.0 (2018-06)

3GPP Security framework

3GPP TS 33 501 V15.1.0 (2018-07) 5G; Security architecture and procedures for 5G System

- **(I)** Network access security: funzionalità che consentono a una UE (User Equipment) di autenticarsi ed accedere ai servizi in modo sicuro, sia da accessi 3GPP sia da accessi non 3GPP.
- **(II)** Network domain security: requisiti che consentono ai nodi di rete di scambiare dati in modo sicuro sia nello User Plane sia nel Control Plane.
- **(III)** User domain security: funzionalità per proteggere il dispositivo mobile da attacchi impropri o intrusioni.
- **(IV)** Application domain security: funzionalità che consentono alle applicazioni nel dominio dell'utente e del Provider di scambiare messaggi in modo sicuro.
- **(V)** Sicurezza del dominio SBA (Security Based Architecture): insieme delle funzionalità relative alla sicurezza per la fornitura dei servizi.



5G user identity

Nel 5G all'utente sono state assegnate nuove identità per coprire in modo sicuro ogni scenario di accesso radio e procedure di roaming.

- **SUPI** (Subscriber Permanent Identifier) Identificativo permanente assegnato a ciascun utente. Il formato può essere come l'IMSI (ETSI 23 003) o NAI (Network Access Identity) (RFC 4282).
- Il SUPI (IMSI) contiene l'indirizzo della HN (MCC) e Network ID (MNC) in chiaro e MSIN (Mobile Subscriber Identity Number) che rimane crittografato. Il SUPI non viene mai trasmesso in chiaro attravero l'accesso radio.
- **SUCI** (Subscription Concealed Identifier). Per preservare la privacy invece di trasmettere il SUPI in chiaro viene utilizzato il SUCI fino a quando il dispositivo non viene autenticato dalla rete. Solo allora la HN comunica il SUPI alla Serving Network.
- **GPSI** (Generic Permanent Subscriber Identity). Sostituisce l'MSISDN.
- **PEI** (Permanent Equipment Identity). Ad ogni UE (User Equipment) un identificativo permanente
- **5G GUTI** (Globally Unique Temporary UE Identity): il 5G-GUTI fornisce un identificativo unico all'UE mantenendo riservato il PEI. Consente l'identificazione del dispositivo mobile alla *AMF* (Mobility Management Function).
-

Grazie per l'attenzione

Relatore

Armando Frallicciardi