La protezione dei dati nel futuro tecnologico

Nascita di una startup di scopo

IGF Italia 2018 – Roma, 6 novembre 2018

Ing. Iolanda Giallonardo

riferimenti in rete

Company website: www.digitalynn.com

Product website: www.nodrive.cloud

Facebook: https://www.facebook.com/digitalynn/

Twitter: @DGitalynn

Linkedin: https://www.linkedin.com/company/digitalynn/

Ing. Iolanda Giallonardo: https://www.linkedin.com/in/iolanda-giallonardo-1116127/

il valore dei dati

Risultati 2017

	Fatturato (BUSD)
Apple	787
Google	678
Microsoft	570
Amazon	491
Facebook	475

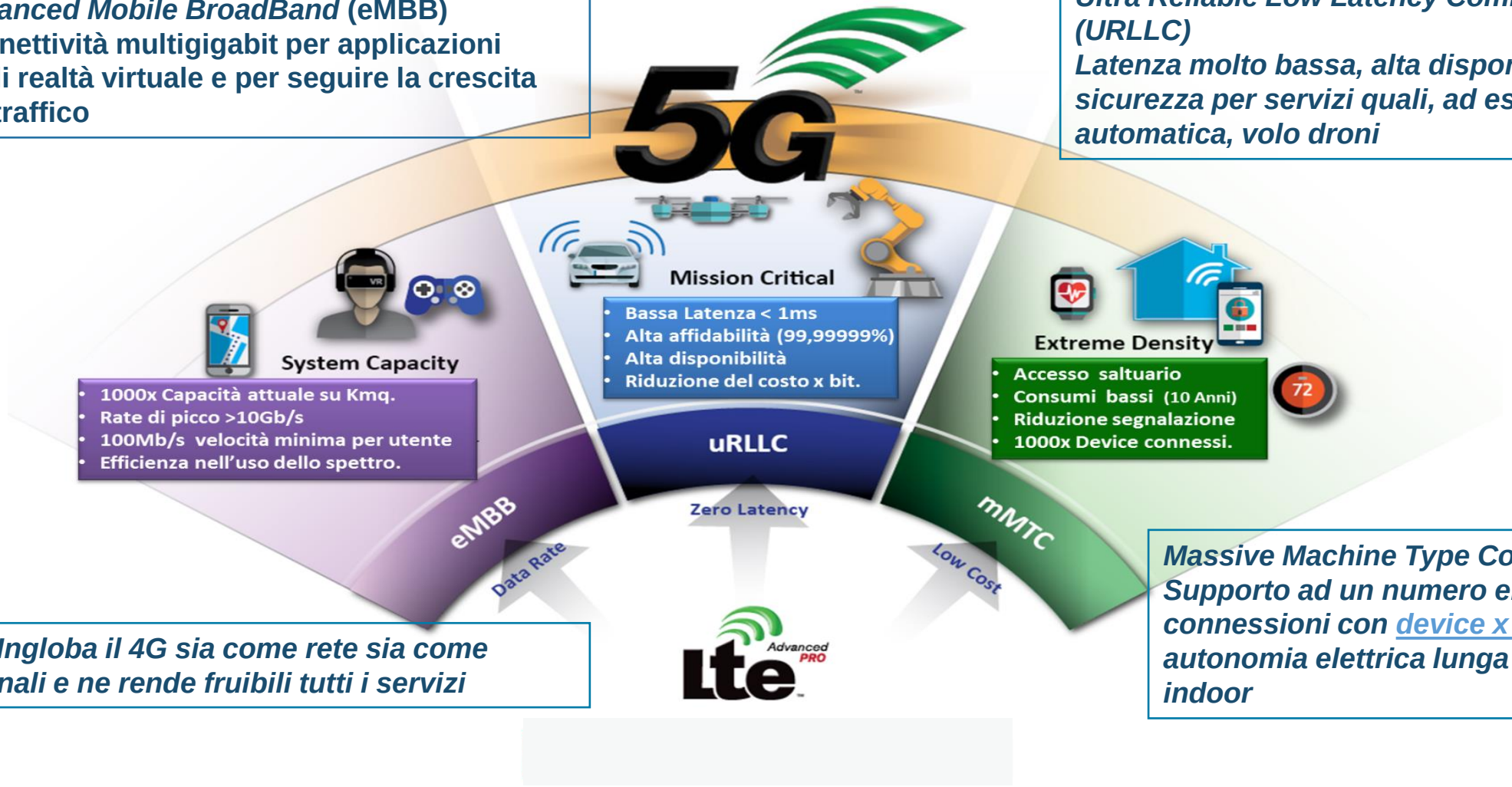
obiettivi del 5g

Source: Ericsson – 5G What is it? October 2014

il 5g - un sistema pensato per i servizi

***Enhanced Mobile BroadBand* (eMBB)**
Connettività multigigabit per applicazioni quali realtà virtuale e per seguire la crescita del traffico

Ultra Reliable Low Latency Communication (URLLC)
Latenza molto bassa, alta disponibilità, affidabilità e sicurezza per servizi quali, ad esempio, la guida automatica, volo droni

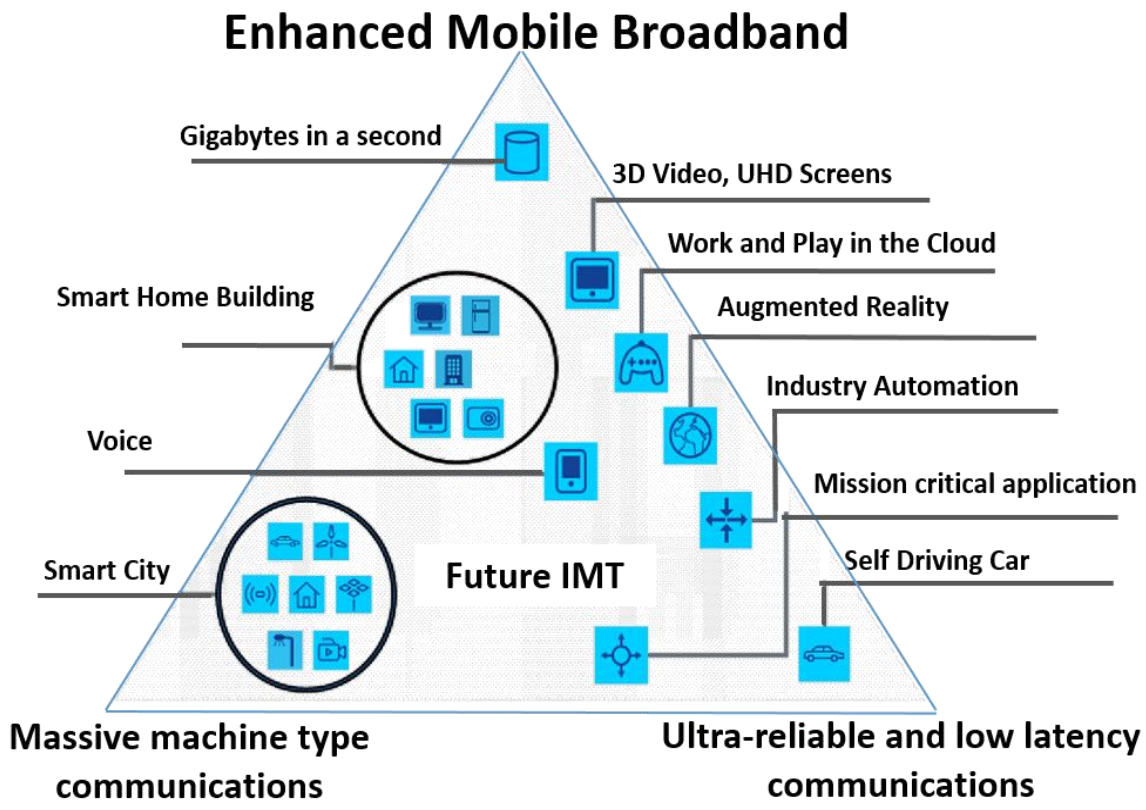


Il 5G Ingloba il 4G sia come rete sia come terminali e ne rende fruibili tutti i servizi

Massive Machine Type Communication (MMTC)
Supporto ad un numero elevatissimo di connessioni con device x IoT con una autonomia elettrica lunga e copertura anche indoor

use case 5g: una prospettiva

Use case previsti per lo sviluppo della tecnologia 5g



Molte applicazione si possono realizzare utilizzando le reti 4G. Il 5G amplia l'ambito delle applicazioni

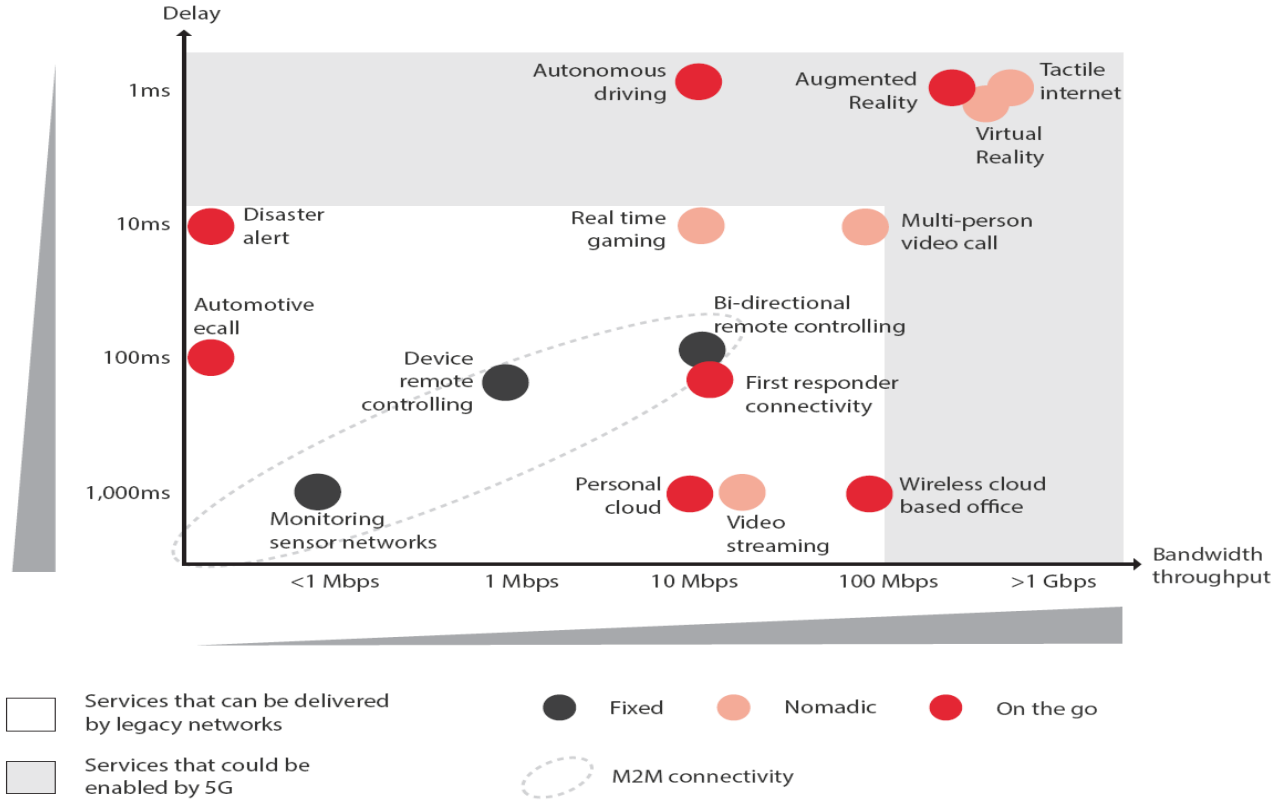


Figure 1: Bandwidth and latency requirements of potential 5G use cases

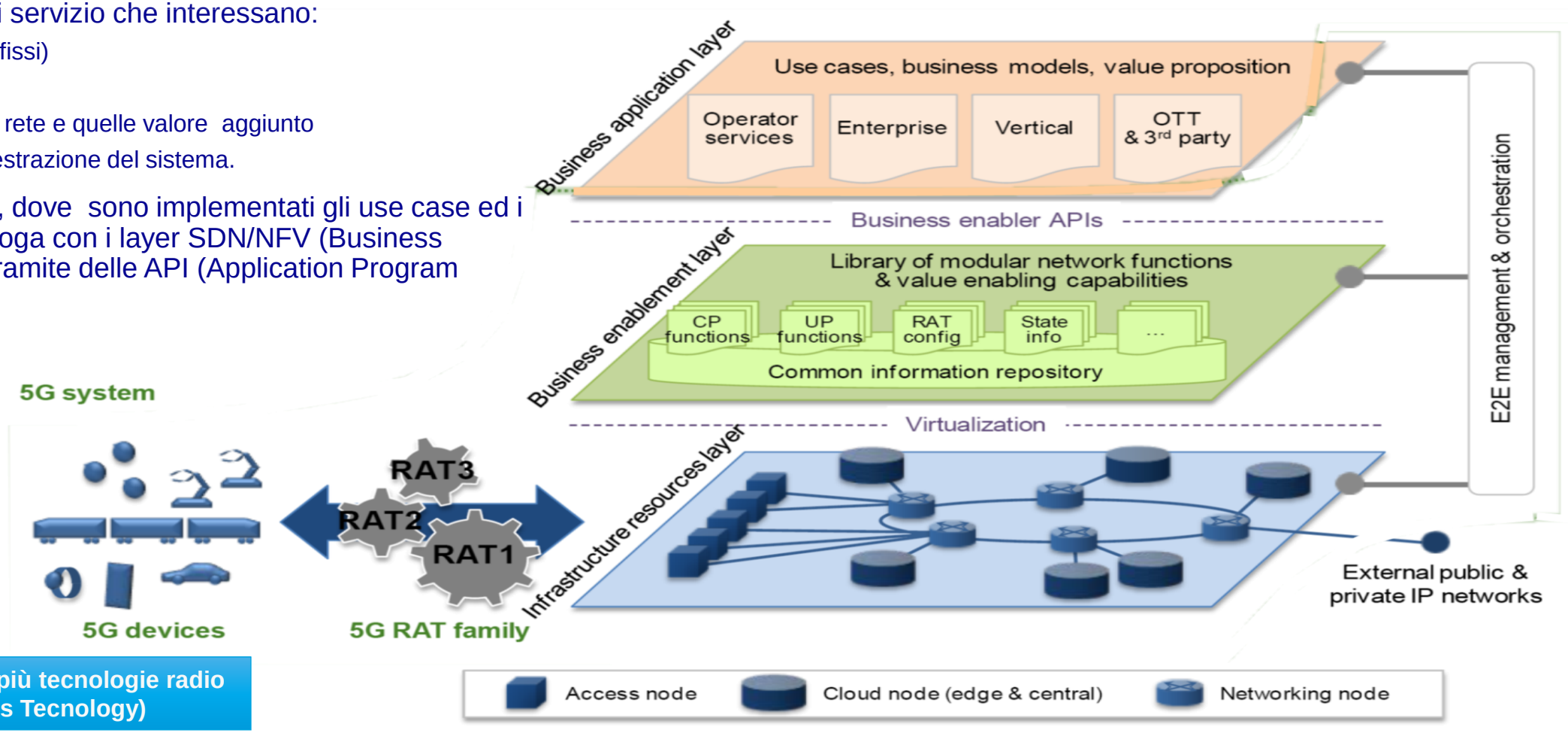
Source: GSMA Intelligence

5g: architettura di riferimento in cloud

L'architettura della rete 5G è nativa SDN/NFV. Essa copre gli aspetti funzionali e di servizio che interessano:

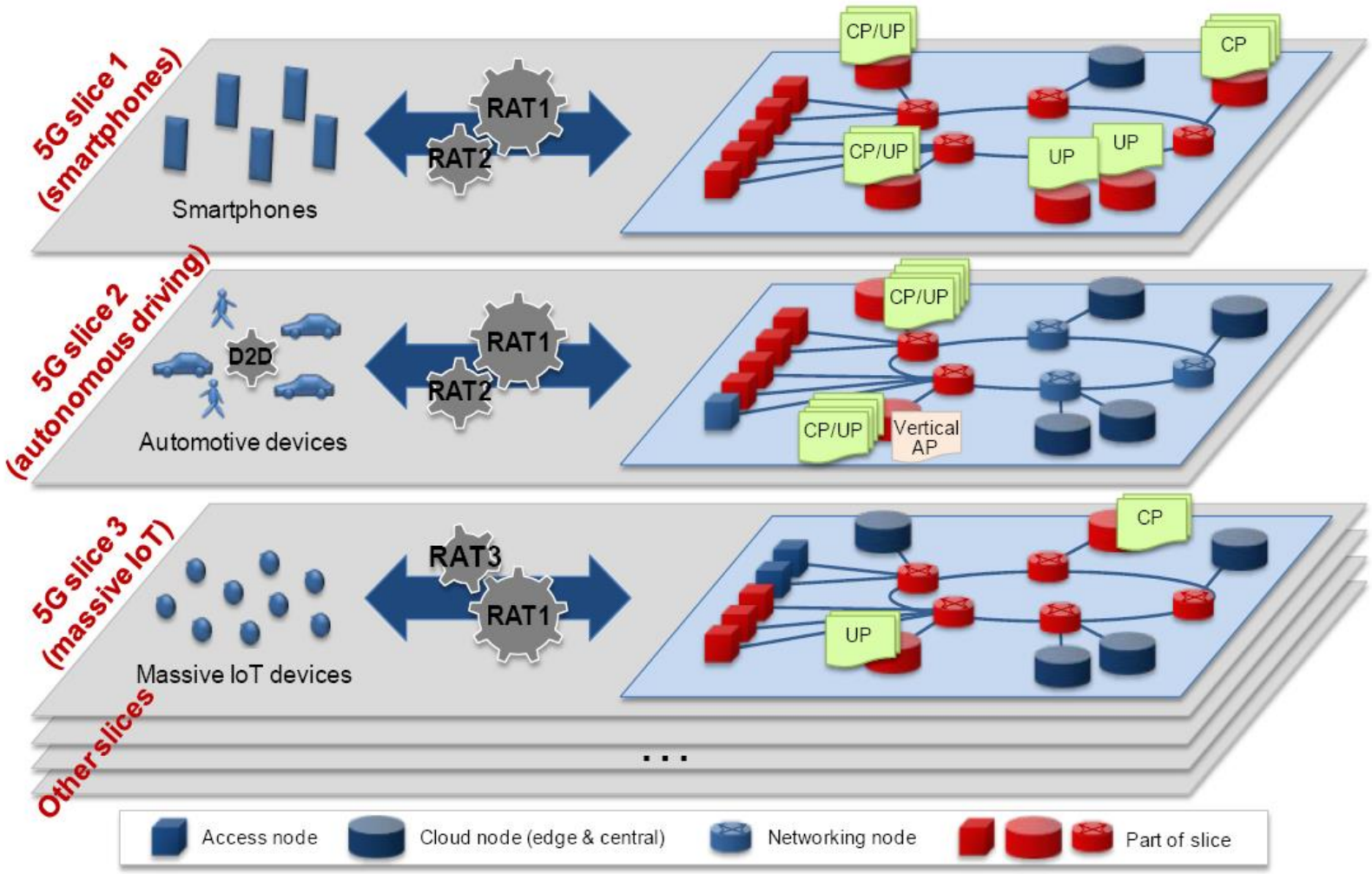
- device (mobili e fissi)
- le infrastrutture
- le funzionalità di rete e quelle valore aggiunto
- gestione e orchestrazione del sistema.

Il Layer di business, dove sono implementati gli use case ed i Business model, dialoga con i layer SDN/NFV (Business Enablement Layer) tramite delle API (Application Program Interface).



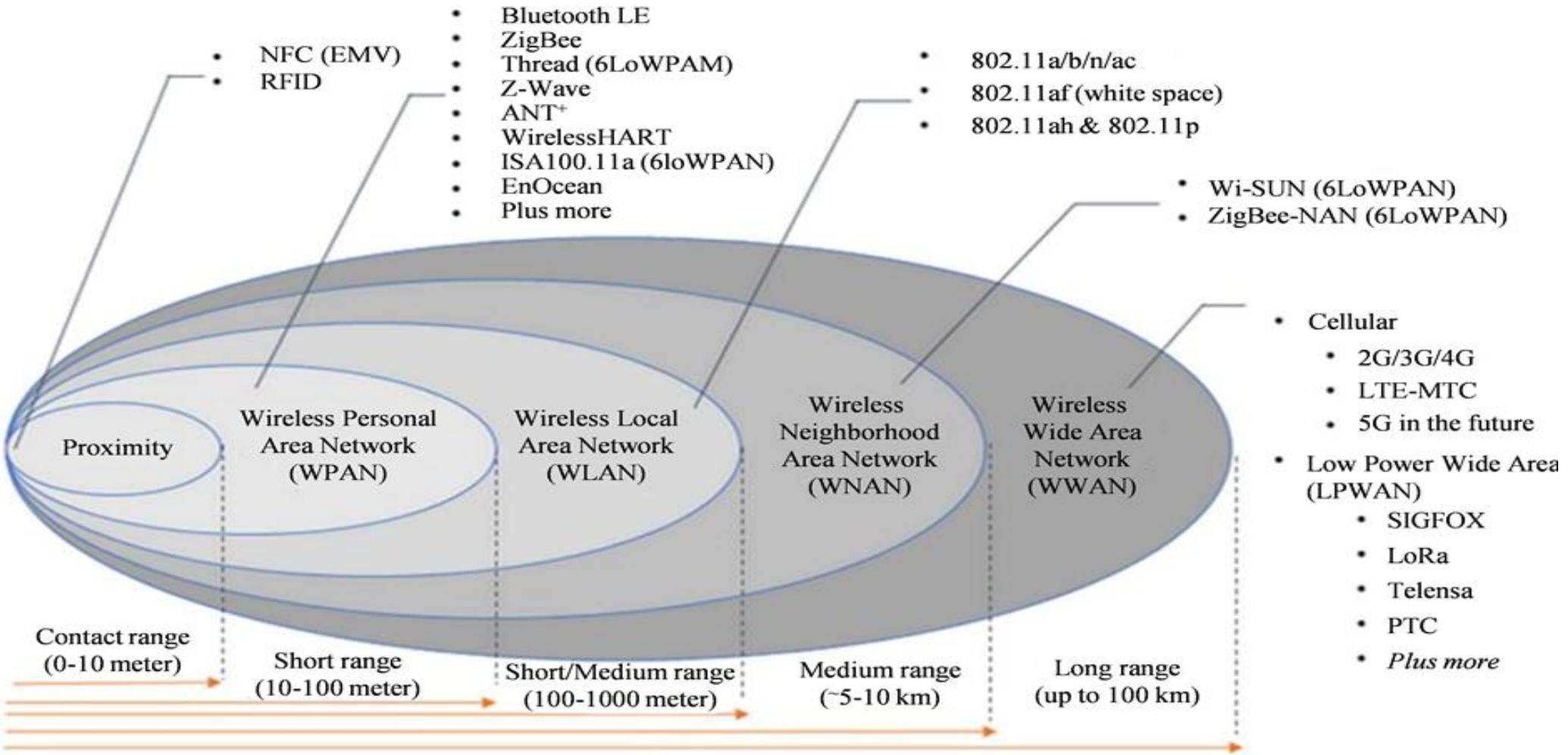
Sistema gestisce più tecnologie radio RAT (Radio Access Tecnology)

5g: lo slicing di rete

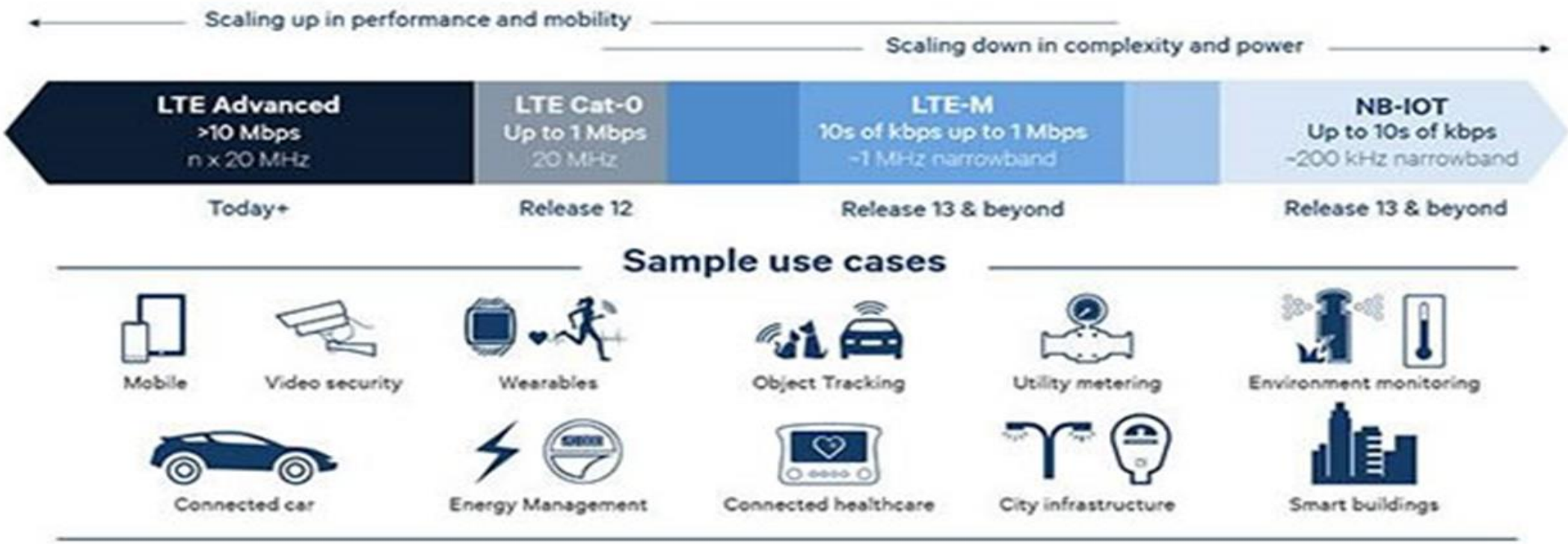


- La rete fisica è segmentata in tante sottoreti logiche.
- In figura tre casi che coprono, dall'alto verso il basso:
  - Mobile Broadband;(Video smart phone ecc.)
  - Mission critical (Automotive, smart grid ecc)
  - IoT. (metering, sensing ecc.)
- Sia la copertura che i nodi di cloud possono essere diversi tra uno slice ed un altro.
- Modello di Business Network as a Service

iot: tecnologie e applicazioni



scenari di utilizzo



dispositivi wearable

iot della salute

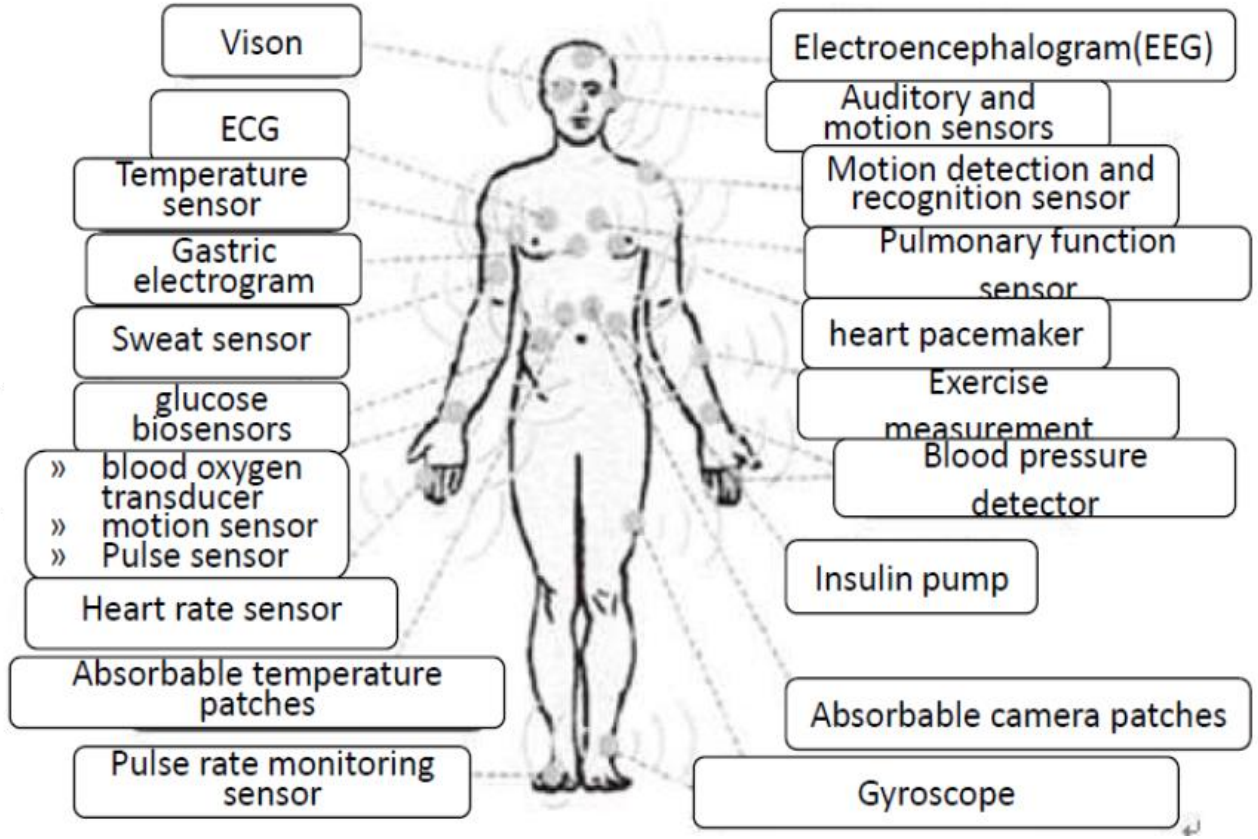
- Sono sensori che misurano le condizioni fisiologiche del paziente.

I sensori principali sono quelli che misurano;

  - **battito cardiaco, frequenza respiratoria , temperature corporea,**
  - **Parametri minimi sufficienti per determinare lo stato di salute.**

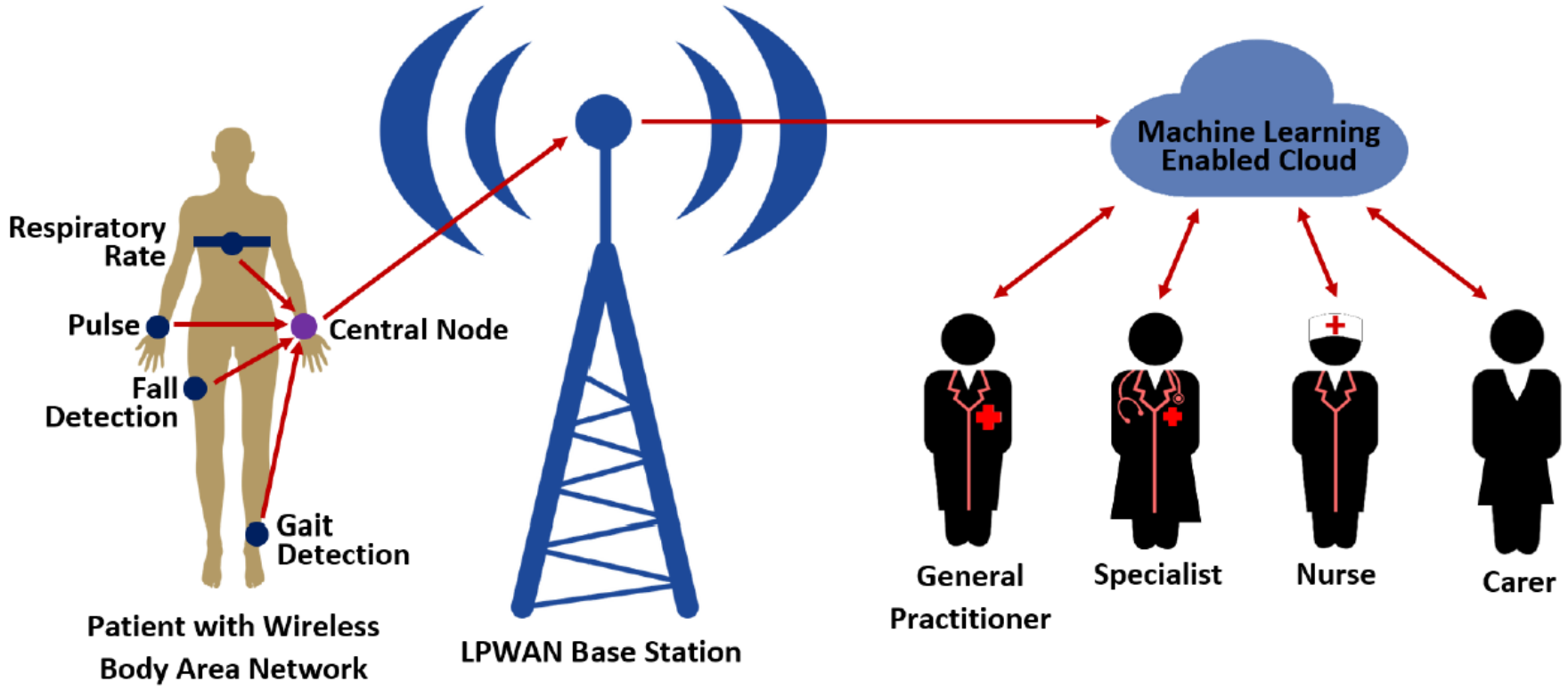
- Ulteriori sensori possono misurare la pressione l'ossigeno nel sangue.
- Sensori speciali come il glucosio nel sangue , rilevatori di caduta , l'angolazione del corpo possono essere aggiunti per pazienti specifici
- Un nodo centrale riceve i dati che sono disponibili per le

opportune valutazioni.



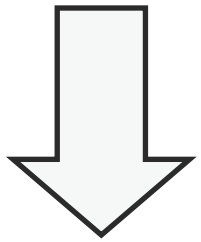
architettura iot

- Un nodo centrale raccoglie le misure dei sensori.
  - **Questo nodo può comunicare anche la posizione geografica del paziente**
- Questo nodo si interfaccia con una tecnologia LPWAN
- I dati sono inviati in un Cloud per essere accessibili da più enti
  - **Machine learning in cloud consente di identificare dei trend nei dati medici non noti fornendo un supporto alla definizione delle cure, diagnosi ed assistenza personalizzate.**



sicurezza in rete

Nello scenario tecnologico evolutivo descritto il problema della SICUREZZA ha acquisito e andrà assumendo sempre maggiore importanza: siamo infatti di fronte ad una crescita esponenziale della quantità di informazioni e di dati che gli utenti della rete si scambiano.



Aumenta quindi l'esigenza di proteggere le informazioni da tutti coloro che cercano di impossessarsene abusivamente tramite attacchi al sistema di comunicazione: sicurezza di una rete, che implica l'introduzione di un insieme di misure necessarie a scoraggiare, prevenire, rilevare e correggere le violazioni della sicurezza di una trasmissione di dati

privacy e web

- L’esigenza di mettere in sicurezza gli apparati informatici nasce dall’impatto invasivo della diffusione del web e delle sue applicazioni sulla sfera della privacy

- La sicurezza informatica, cioè la tutela dei sistemi da potenziali rischi e/o violazioni dei dati sensibili custoditi negli archivi digitali è diventata una condizione necessaria per la protezione della privacy

il nuovo regolamento (gdpr)

si rimanda a presentazione realizzata dal Garante
www.garanteprivacy.it/regolamentoue

PDF
Adobe Acrobat Document

cosa deve garantire la sicurezza

- La RISERVATEZZA dei dati (cioè la riduzione del rischio che si possa accedere alle informazioni senza autorizzazione)

- L'INTEGRITA' dei dati (cioè la riduzione del rischio che possano essere modificati i cancellati da chi non è autorizzato)

- La DISPONIBILITA' (cioè la riduzione del rischio che i dati vengano cancellati o che non vi si possa accedere)

i dati personali

Dati SENSIBILI:

- Razza
- Religione
- Politica
- Salute
- Vita sessuale
- Interessi
- Relazioni sociali

Dati SEMISENSIBILI:

- Tutti i dati la cui diffusione può causare un danno all'interessato

Dati COMUNI:

- Consentono l'individuazione di una persona fisica o giuridica

Dati GIUDIZIARI:

- dati idonei a rivelare taluni provvedimenti giudiziari

esempi di reati contro la privacy

- Violazione, sottrazione o soppressione di email
- Rivelazione di contenuto di email
- Intercettazione di comunicazioni informatiche e telematiche
- Installazioni abusive di apparecchiature per intercettazioni informatiche
- Falsificazione, alterazione e/o sottrazione di comunicazioni informatiche
- Rilevazione di contenuto di documenti segreti
- Accesso non autorizzato a un sito
- Spionaggio informatico
- Frode informatica

gli attacchi alla sicurezza

- SPYWARE, software che raccoglie informazioni sull'attività online dell'utente senza consenso. I dati raccolti vengono ceduti a società di marketing
- SOCIAL ENGINEERING, software che estorce informazioni personali agli utenti ottenendo il rilascio di propri dai personali
- PHISHING, i siti-copia di banche o finanziarie "catturano" user e pw di accesso ai veri siti
- COOKIES, piccoli file di testo che raccolgono info sulla navigazione di un sito. Possono essere utilizzati impropriamente
- MALWARE, insieme di codici che comprendono worm, virus, virus, trojan horse
- RANSOMWARE, un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (*ransom* in Inglese) da pagare per rimuovere la limitazione

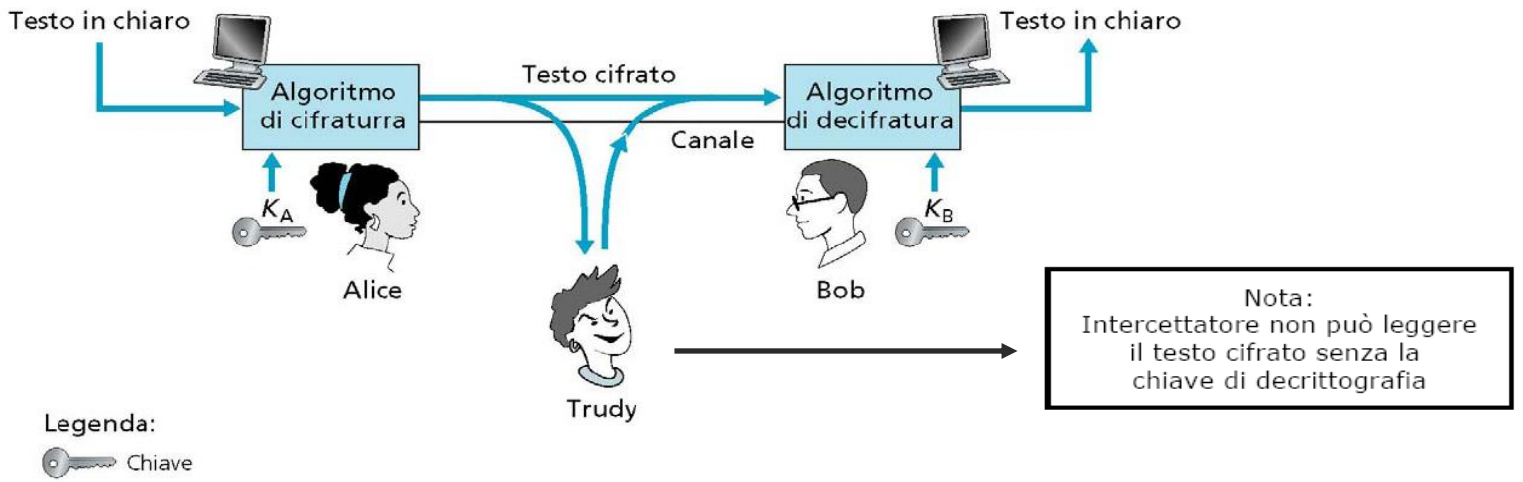
Le armi degli utenti

- PASSWORD: utilizzo di codici alfanumerici che aumenta la sicurezza
- FIREWALL, ANTIVIRUS, ANTISPYWARE: sempre aggiornati
- COOKIES: è possibile controllarli, limitarli, cancellarli
- EMAIL: diffidare di quelle provenienti da utenti sconosciuti, evitare di utilizzare link in esse contenute

sistemi sicuri

- Il termine Sistema Sicuro non implica che il sistema sia inviolabile
- Ogni sistema può essere violato, avendo sufficiente tempo e denaro
- La sicurezza di un sistema deve essere proporzionale alle risorse che esso protegge
- Proprietà di un sistema sicuro:
  - Ogni entità è sicura dell'identità dell'altra
  - L'informazione è privata e protetta contro il tampering
  - Protezione contro la ripetizione ed il riordino dei dati
- Impiego della crittografia
  - La segretezza è basata sul concetto di crittografia
  - L'autenticazione è basata sulla dimostrazione di un segreto

crittografia

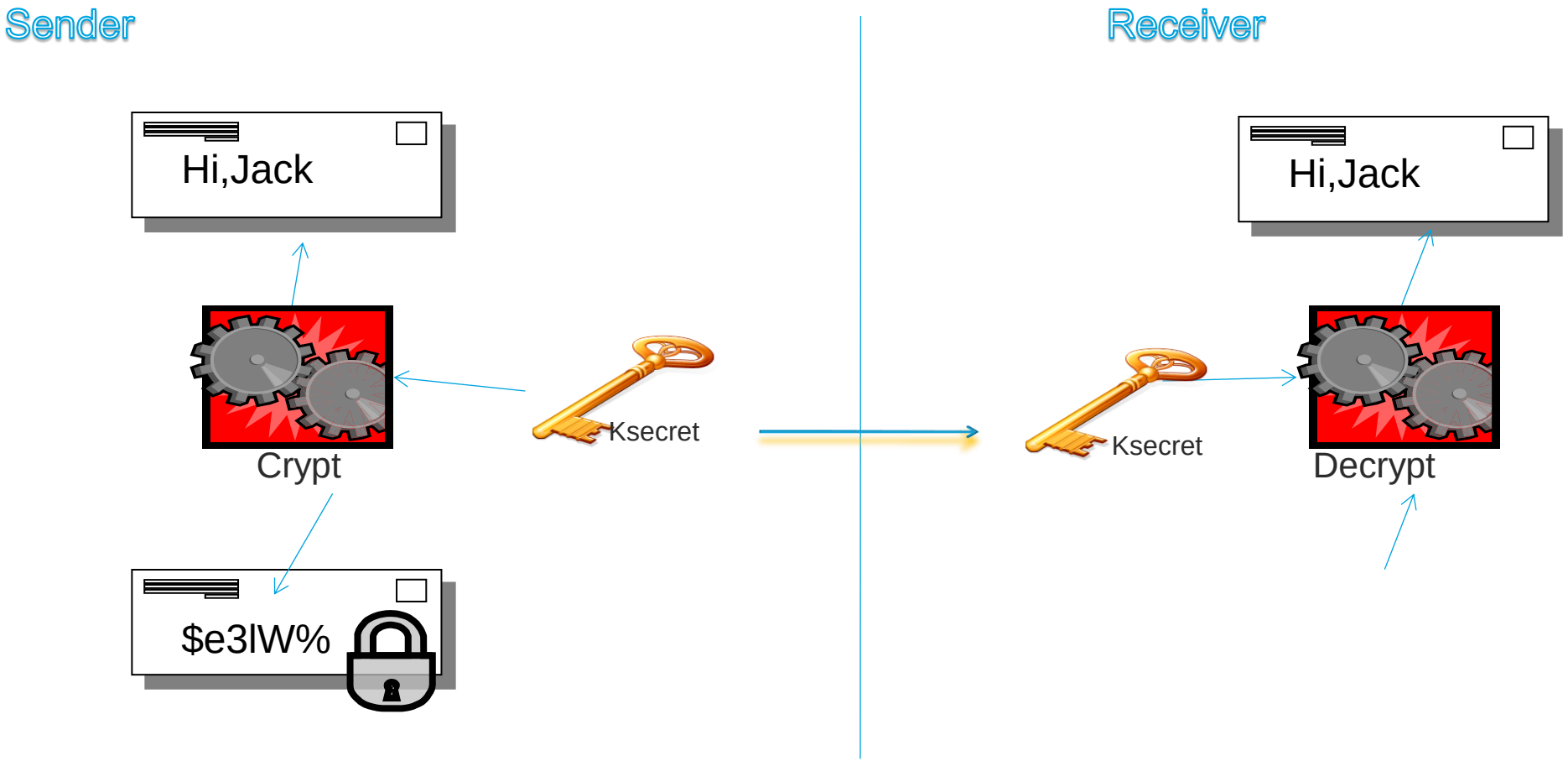


- Principio di Kerckhoffs: “La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione.”

tipi di crittografia

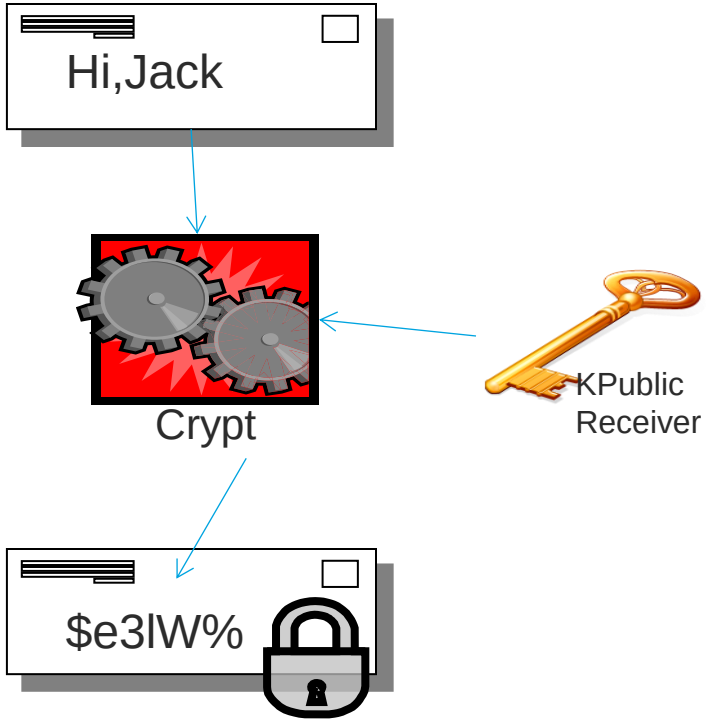
- Crittografia a chiave privata
  - Il sender e il receiver usano la stessa chiave (è anche detto crittografia a chiave singola, segreta o simmetrica)
- Crittografia a chiave pubblica
  - Il sender e il receiver usano differenti chiavi (è anche detto crittografia a due chiavi o a chiave asimmetrica)

crittografia simmetrica

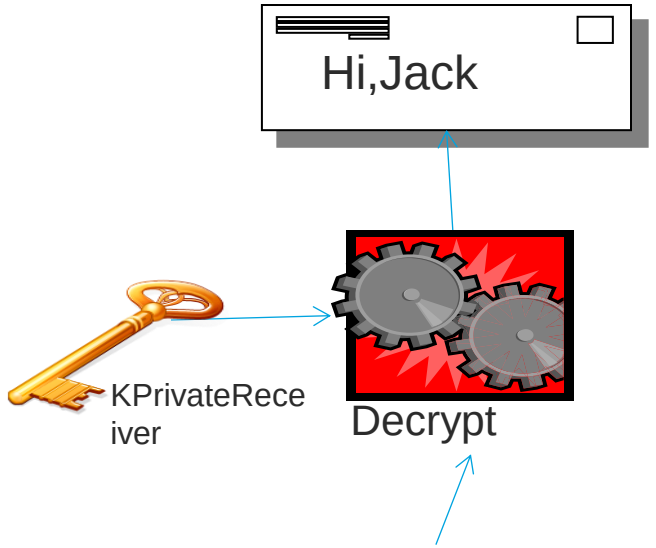


crittografia asimmetrica

Sender



Receiver



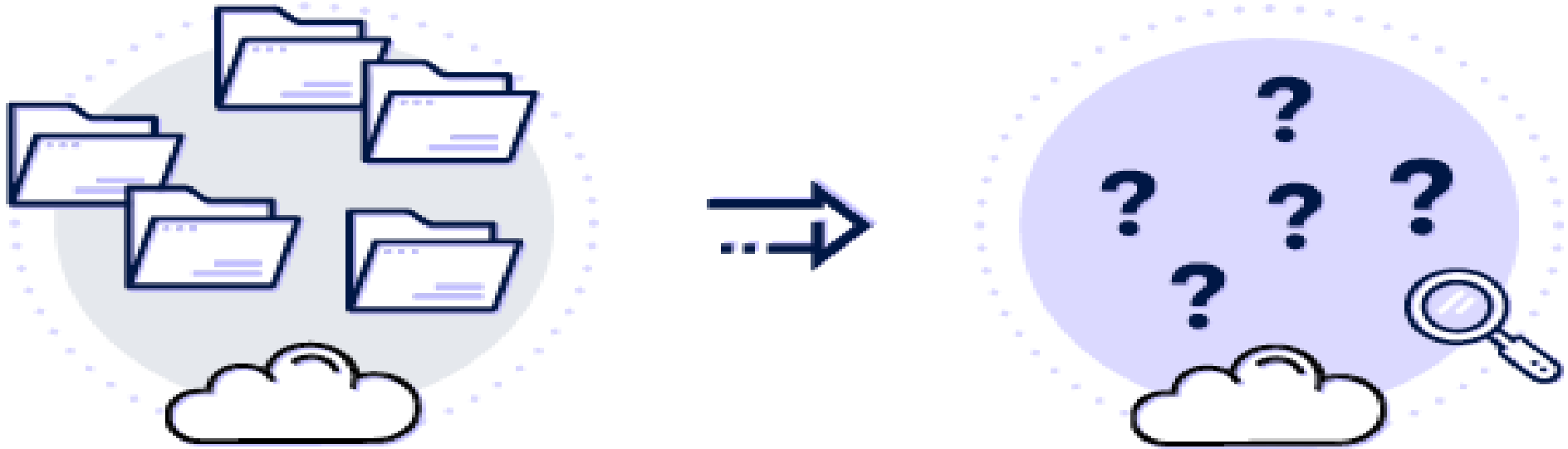
nomenclature: crittografia, cifratura e codifica

L'italiano ha "importato" la parola *cifra* dall'arabo *cifr*, in origine *vuoto*, *zero*. in seguito il termine venne utilizzato per qualunque *segno di numerazione* ed è presente in diverse lingue (in francese *chiffre*, in inglese *cipher*). In effetti i numeri sono stati portati in Europa dagli Arabi, che a loro volta li avevano conosciuti in India.
Le origini della parola *cripta* sono invece più semplici in quanto si rifanno al greco, attraverso il latino, significando *luogo nascosto*.

Cifrare e decifrare si usano quando il messaggio sia stato offuscato in cifra, tramite numeri, mentre un testo viene criptato quando è semplicemente nascosto, magari utilizzando un alfabeto arbitrario. Per la *codifica* infine mi limiterei a pensare ad un codice, un *sistema di corrispondenze*

il software NODRIVE

Un **software** di semplice installazione che **protegge i dati archiviati** su qualsiasi dispositivo fisico e/o virtuale da attacchi informatici o **limita gli accessi** solo ad utenti autorizzati.
Nodrive si affianca in maniera trasparente a tutti i sistemi di sicurezza pre-esistenti ed elimina in maniera radicale il problema della protezione del dato, eliminando il dato stesso.
Nodrive implementa le misure di sicurezza informatica richieste dal nuovo regolamento europeo per la tutela della privacy (**GDPR compliant**) rispettando qualsiasi configurazione informatica preesistente di archiviazione dati su dispositivi informatici locali e/o virtuali.



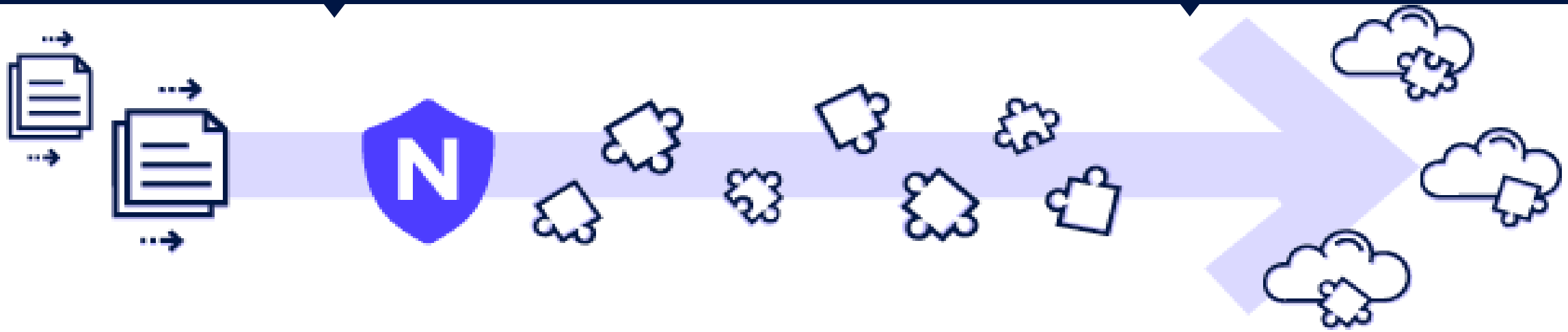
Un qualsiasi utente, anche non esperto, può installare Nodrive

www.nodrive.cloud

cosa fa NODRIVE (1/2)

I file vengono immediatamente cifrati, offuscati e spezzettati

I pezzi dei file vengono distribuiti casualmente su un numero variabile di server



Sul tuo PC:

I file non sono mai in chiaro

Con la tecnologia di **offuscamento** di Nodrive il disco è protetto da accessi indesiderati.

Sul cloud:

I file non sono mai in chiaro

Con la tecnologia di **spezzettamento**, **occultamento** ed **anonimizzazione** di Nodrive è impossibile accedere al contenuto dei file anche accedendo ai server che li ospitano.

Nodrive mette al sicuro i dati, ovunque si trovino

cosa fa NODRIVE (2/2)

1

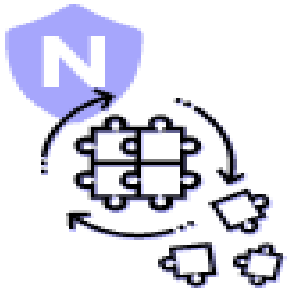
Dati in ingresso

Qualunque informazione può essere inviata al
motore Nodrive per la **cifratura**,
randomizzazione e
spezzettamento.

2

Algoritmo Nodrive

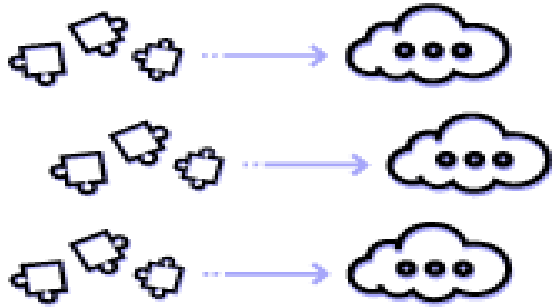
Nodrive attraverso un algoritmo proprietario (**patent pending**) acquisisce le informazioni in ingresso, le randomizza e le spezzetta



3

Dati in uscita

I pezzetti di informazioni prodotti da Nodrive
vengono distribuiti
casualmente su un
numero indeterminato di server.



Nodrive è compatibile con qualsiasi ambiente cloud

Contacts

(+39) 06 9456057

info@digitalynn.com

www.digitalynn.com

Locations

Via M.G. dell’Unità, 14
00046 Grottaferrata (Roma)

Via Morrone, 89
67039 Sulmona (AQ)