EUSTEMA®

Making Innovation


CifrisCloud

**Daniele Ballo**

d.ballo@eustema.it

31 Maggio 2022

# Key Management System vs Homomorphic Encryption

EUSTEMA®
Making Innovation

- Introduzione
- Key Management System
- Modelli
- The three states of data
- Homomorphic Encryption

# Key Offering

## Big Data & AI

Data Governance, Big Data Architecture, Data Analytics & Visualization

## Digital Media

Customer Engagement, UX Design, Cloud & Headless Content Architecture

## Knowledge Engineering

Document & Process Automation, Enterprise Search


## Enterprise Architecture

Microservices & Serveless architecture, Continuous Integration, Cloud native design pattern

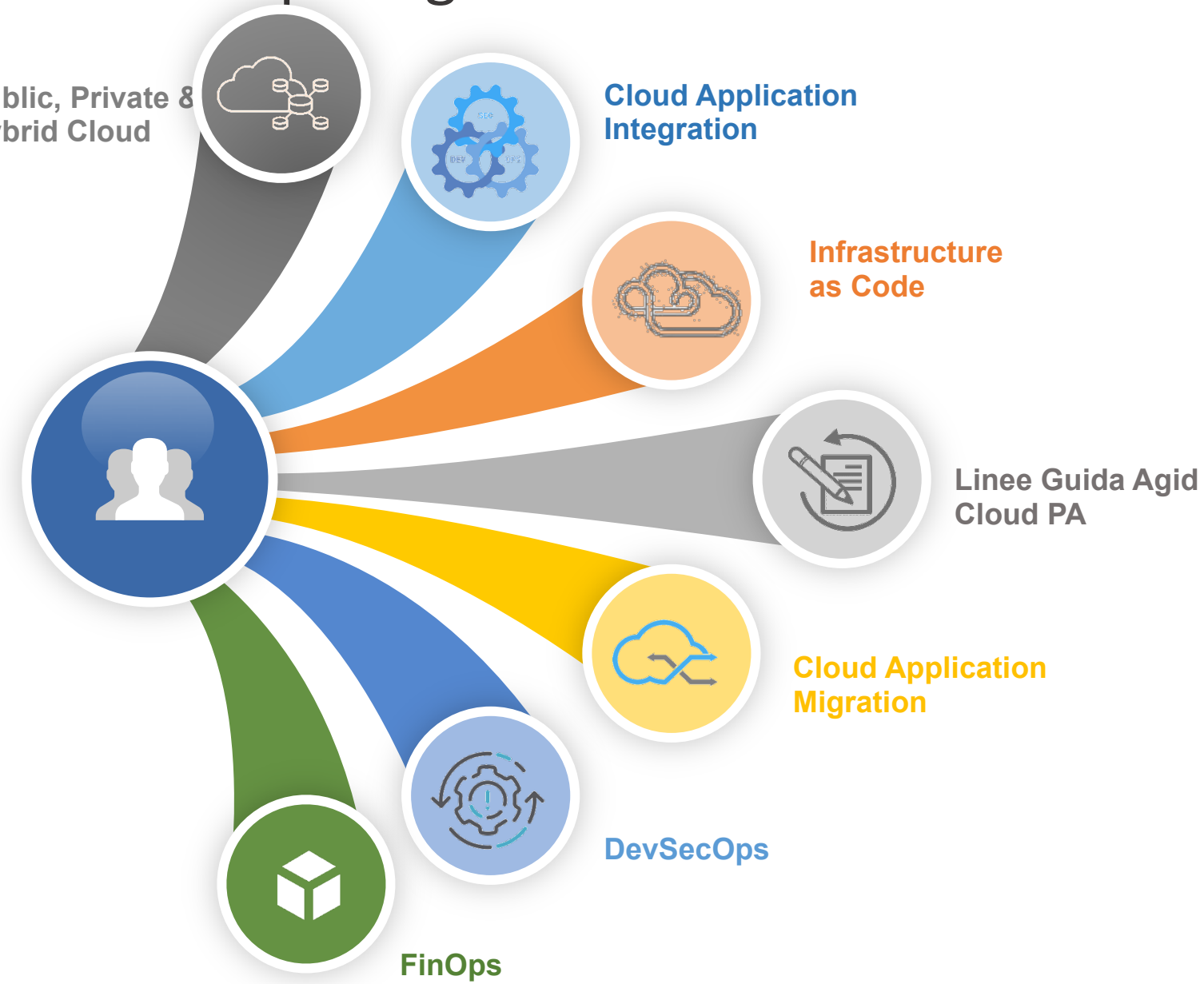
## Cloud Computing

Cloud Migration & Integration, Edge & Hybrid, DevOps

## ICT Consultancy

Innovation Management, Continuous Improvement, Change Management

# Cloud Computing




**Best Case**

- Poste Italiane
- FORTE
- RAI
- Poligrafico

## Principali tecnologie

- Amazon AWS
- Microsoft Azure
- Google CP
- Open Shift
- Kubernetes
- Terraform

Google Cloud Partner

Microsoft Partner
Gold Application Integration
Gold Data Analytics
Gold Application Development
Silver Windows and Devices

Soci Fondatori Gaia X

# Introduzione

# Cloud Computing

La distribuzione di servizi di calcolo, come server, risorse di archiviazione, database, rete, software, analisi e intelligence, tramite Internet.

Fornitore

Sicurezza

Velocità

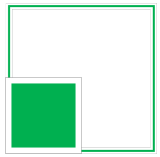
Affidabilità

Prestazioni

Costo

Perdita di controllo

Interruzione servizi



Scalabilità

Produttività

# Cloud Computing

La distribuzione di servizi di calcolo, come server, risorse di archiviazione, database, rete, software, analisi e intelligence, tramite Internet.

Fornitore

Sicurezza

Velocità

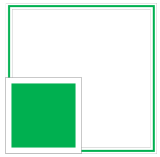
Affidabilità

Prestazioni

Costo

Perdita di controllo

Interruzione servizi



Scalabilità

Produttività

# Tipi di Cloud Computing

- Cloud pubblico

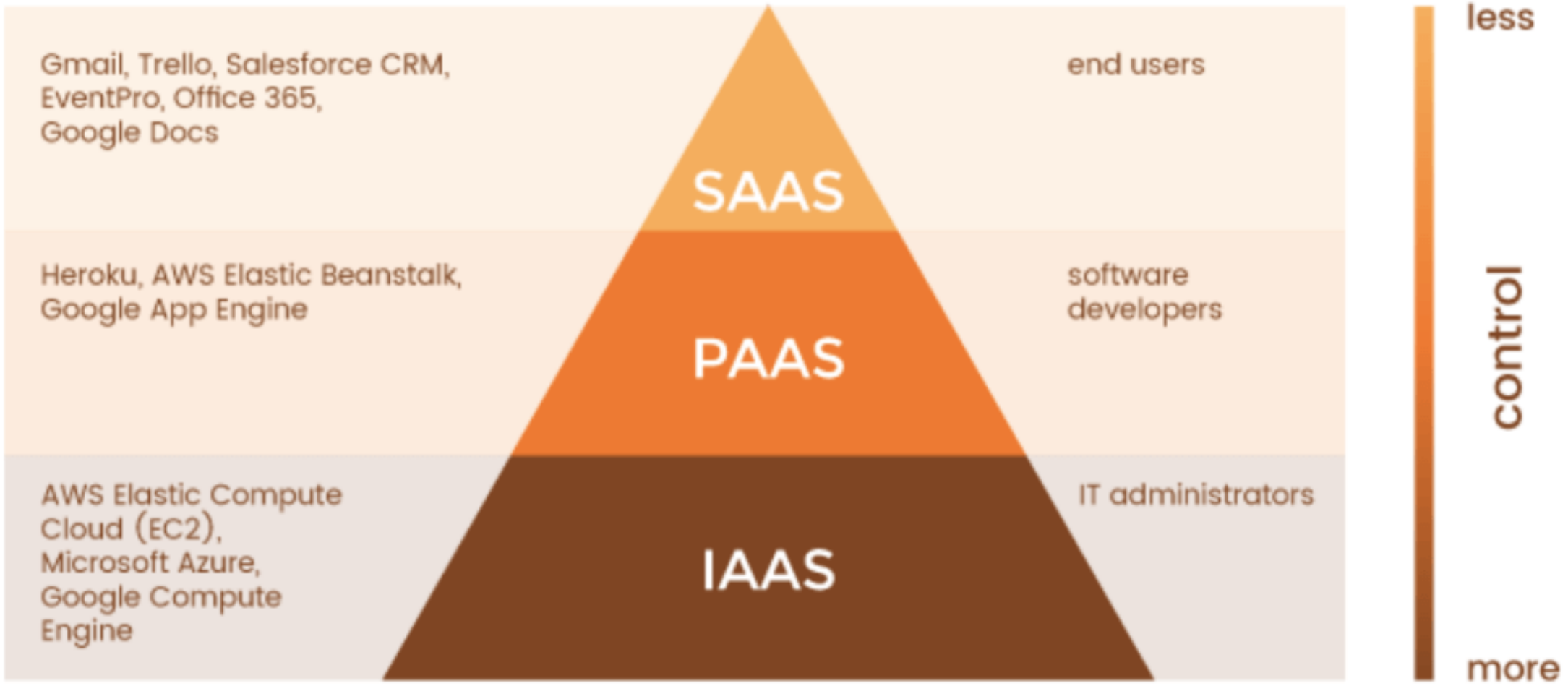
- Cloud privato

- Cloud ibrido

# Tipi di servizi

- Infrastruttura distribuita come servizio **(IaaS, Infrastructure as a service)**
- Piattaforma distribuita come servizio **(PaaS, Platform as a Service)**
    - Elaborazione serverless
- Software come un servizio **(SaaS, Software as a Service)**

# Tipi di servizi






*https://ncube.com/blog/saas-paas-iaas*

# Statistiche

## Utilizzo del cloud computing:

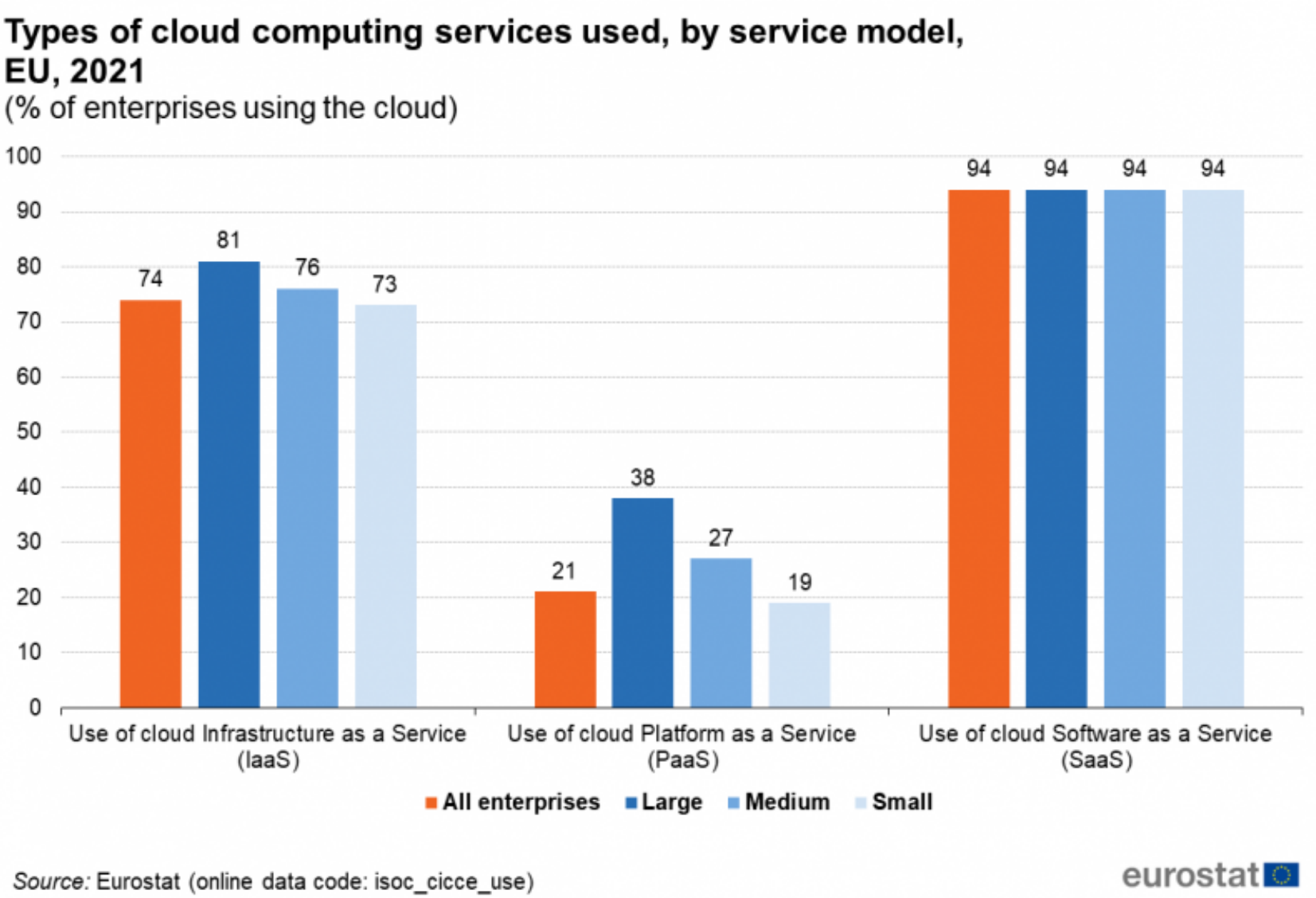
- Il 41% delle imprese dell'UE ha utilizzato il cloud computing nel 2021, soprattutto per ospitare i propri sistemi di posta elettronica e archiviare file in formato elettronico.

- Il 73% di queste imprese ha utilizzato servizi cloud sofisticati relativi alle applicazioni software di sicurezza, all'hosting dei database aziendali o alla piattaforma informatica per lo sviluppo, il test o la distribuzione delle applicazioni.

- Rispetto al 2020, l'uso del cloud computing è aumentato di 5 punti percentuali.

**https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises**

# Statistiche




**https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises**

# Key Management System

# KMS - Storia

- IV o V secolo a.C.
- 2006, Amazon, Elastic Compute (EC2)
- 2010, Key Management Interoperability Protocol

- prodotti di gestione delle chiavi legacy (non rimpiazzabili)
- opzioni di crittografia disponibili su una base di servizi in-the-cloud

- 2013, Amazon Key Management Service
- Microsoft, Azure Key Vault
- 2017, Google, Cloud Key Management

- soluzioni cloud native
- password, stringhe di connessione e altri secret

# KMS - Definizioni

## Cryptographic Module

È “un insieme di hardware, software, firmware, o una loro combinazione che implementa la logica o i processi crittografici, compresi gli algoritmi crittografici, ed è contenuto all'interno del *'confine crittografico*' del modulo, che è un perimetro contiguo esplicitamente definito che stabilisce i limiti fisici del modulo.” [RFC4949], [NIST FIPS 140-2].

### Esempi

- Trusted Platform Module (TPM)
- Smartcard
- Hardware Security Modules (HSM)

# KMS - Definizioni

**FIPS (Federal Information Processing Standard) 140-2** e
**ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation** (Common Criteria o CC) sono standard internazionali per certificare i livelli di protezione dei moduli crittografici.

**Nota:**
I regolatori di varie industrie (in particolare il settore finanziario) richiedono che solo i moduli crittografici certificati FIPS 140-2 siano usati per proteggere dati e processi critici.
Il livello di protezione dipende dall'uso del modulo crittografico.

Questi moduli sono spesso sotto forma dei cosiddetti moduli di sicurezza hardware (HSM) usati per gestire, generare e conservare in modo sicuro le chiavi crittografiche.

# KMS - Definizioni

## KMS

Un sistema di gestione delle chiavi è un sistema che è costruito intorno a un modulo crittografico e sfrutta la funzionalità crittografica e la gestione del ciclo di vita delle chiavi per collegare applicazioni e servizi.

Il NIST[1] definisce il KMS come ***"a system for the management of cryptographic keys and their metadata"*** (ad esempio generazione, distribuzione, memorizzazione, backup, archivio, recupero, uso, revoca e distruzione).

1 - [NIST SP [800-57] Part1]

# KMS – *YOK

- **BYOK (Bring Your Own Key)**
- **HYOK (Hold Your Own Key)**
- **CYOK (Control Your Own Key)**

# Modelli

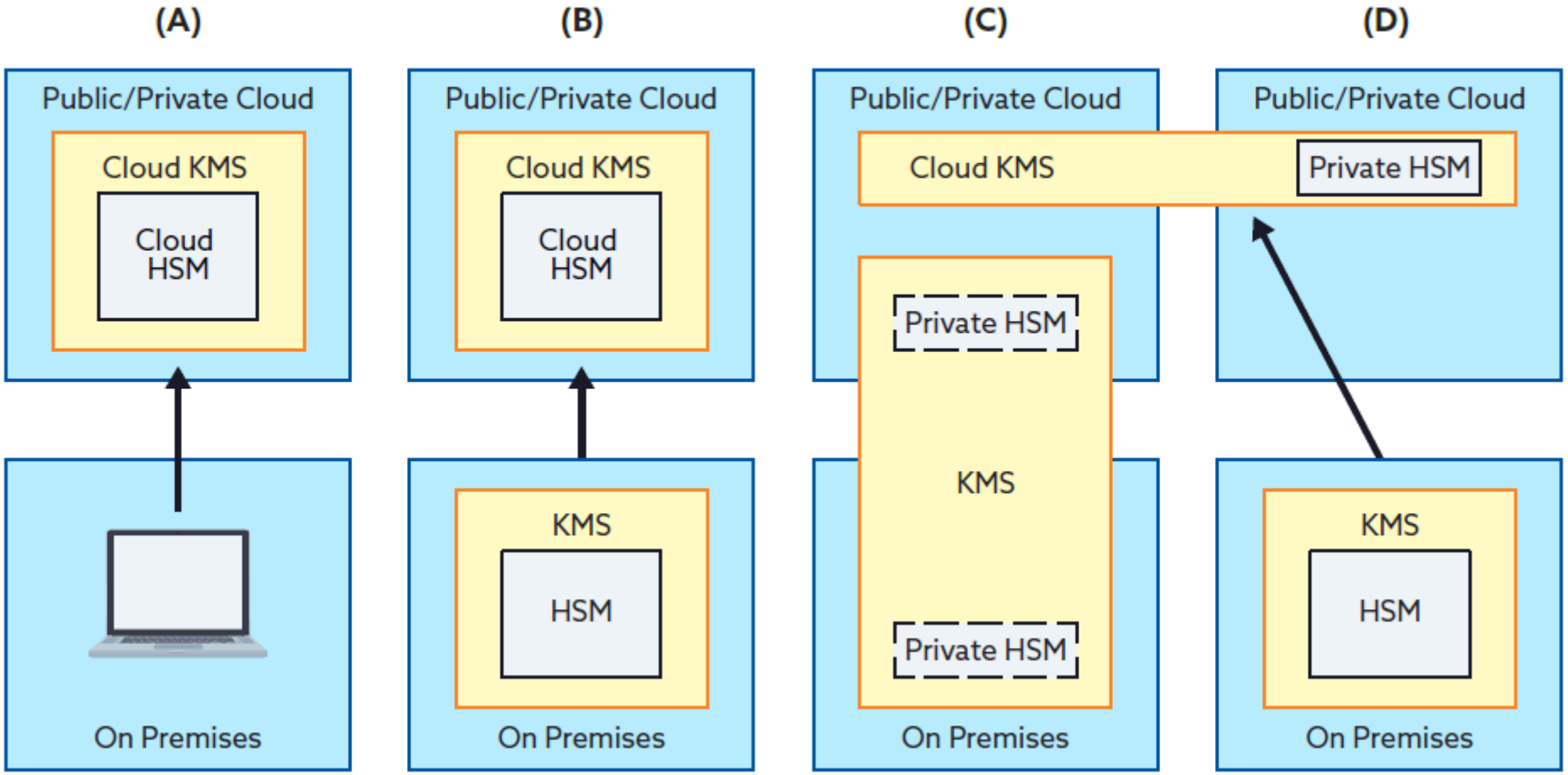
# MODELLI

1. **Quali sistemi KMS sono già in uso nell'organizzazione?**

2. **Quali sono i risultati funzionali, operativi e di business desiderati per l'uso del servizio cloud?**

# MODELLI

## Servizi cloud e schemi KMS



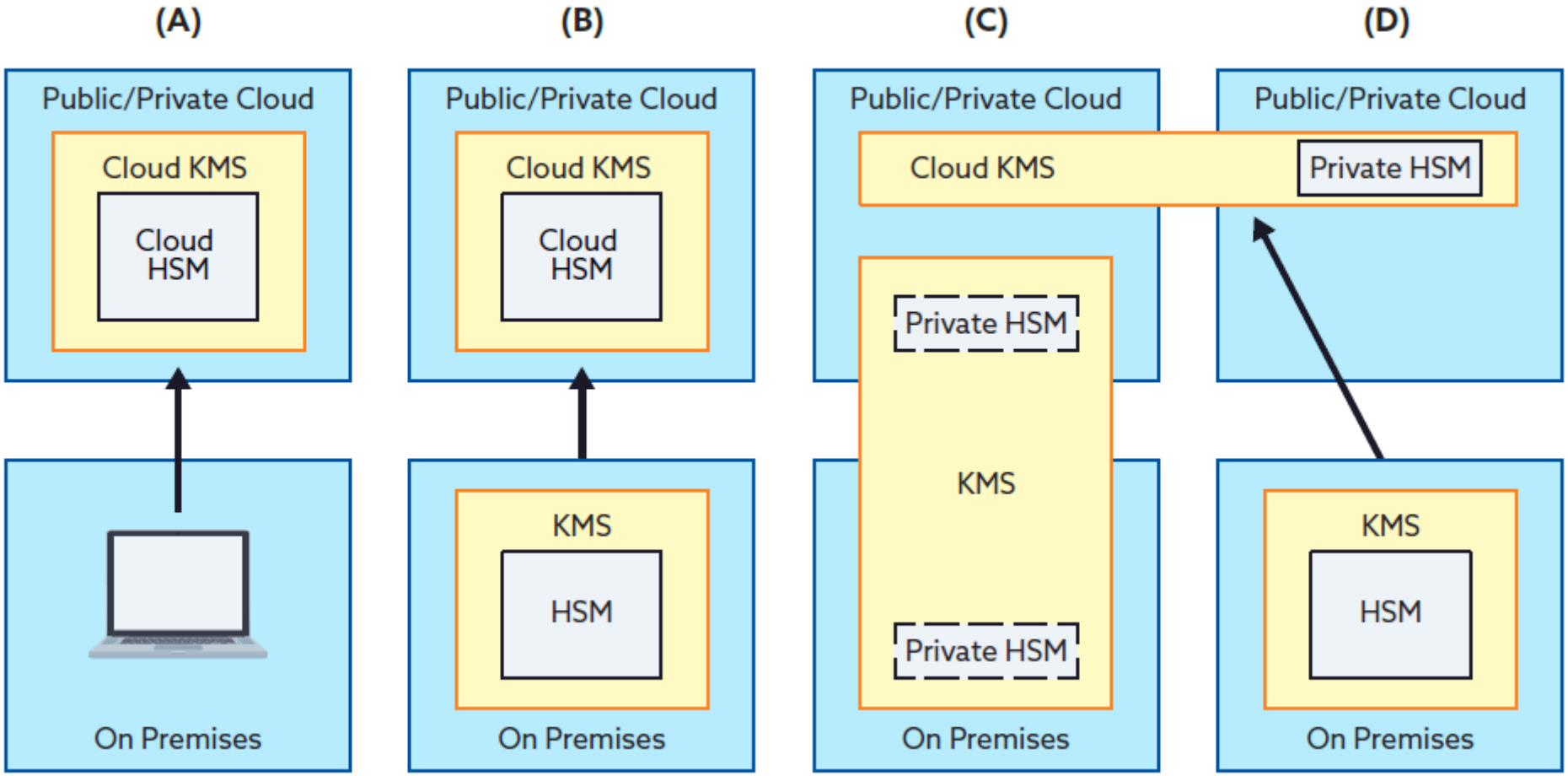

CSA – Cloud Security Alliance

**(A) è un servizio cloud che sfrutta un KMS (incluso HSM) all'interno dello stesso cloud;**

**(B) espande il modello (A) per permettere di importare elementi chiave da un KMS esterno;**

# MODELLI

## Servizi cloud e schemi KMS

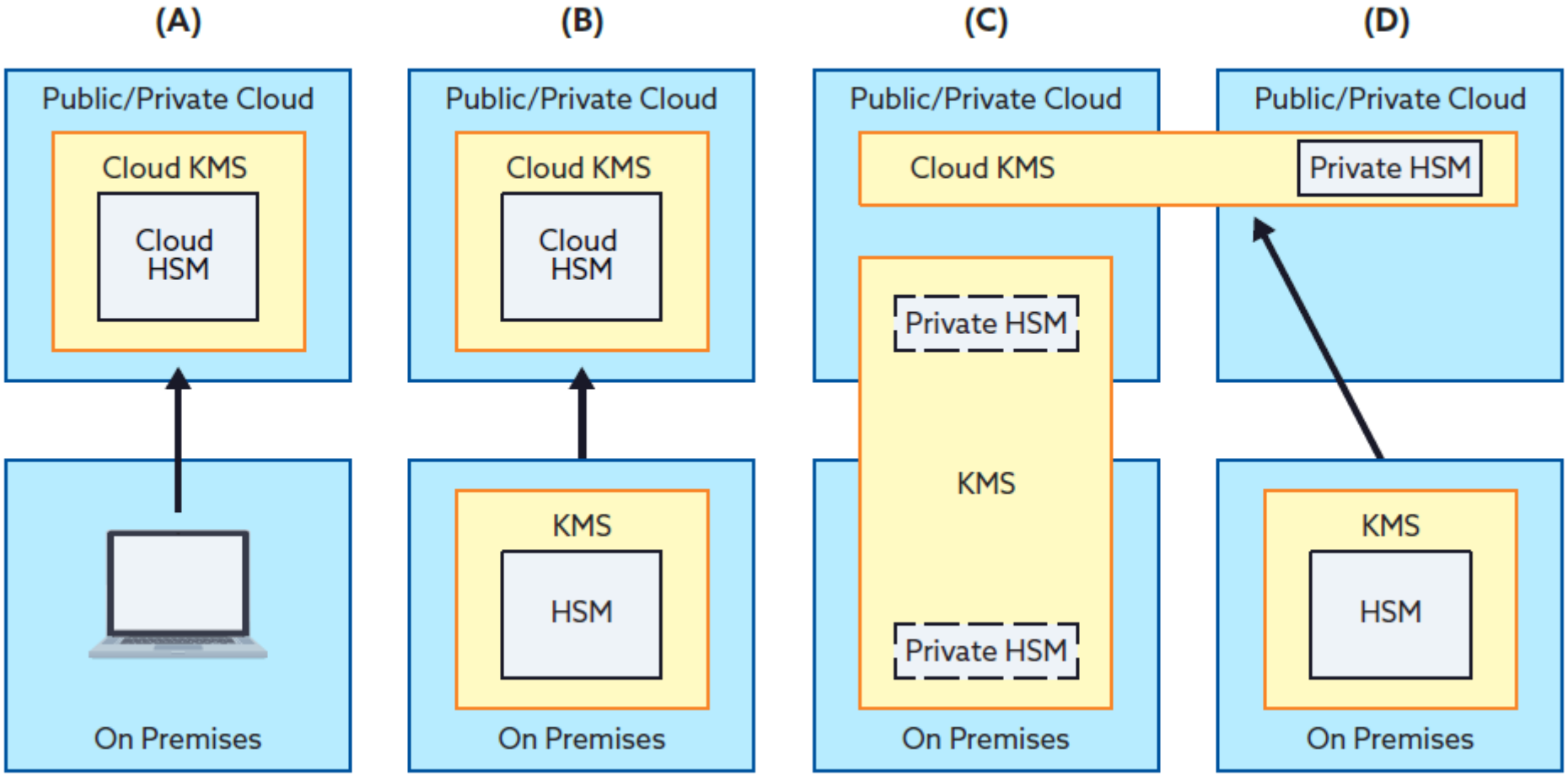



CSA – Cloud Security Alliance

**(C) è un KMS in-the-cloud con un HSM dedicato (privato) che è sotto il controllo del proprietario organizzazione, ma è fisicamente ospitato all'interno dei centri dati del fornitore di cloud;**

# MODELLI

## Servizi cloud e schemi KMS




**CSA – Cloud Security Alliance**

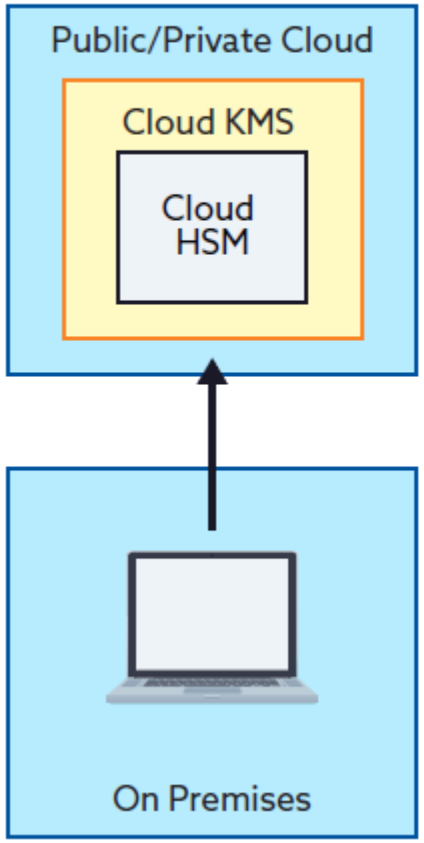
**(D) descrive un KMS on-premises che viene utilizzato per l'integrazione/gestione KMS multi-cloud che può essere ospitato in sede o nel cloud ed è collegato a un modulo crittografico in sede come un HSM o una crypto card.**

# MODELLI

**Sistemi KMS cloud considerati per questo studio:**

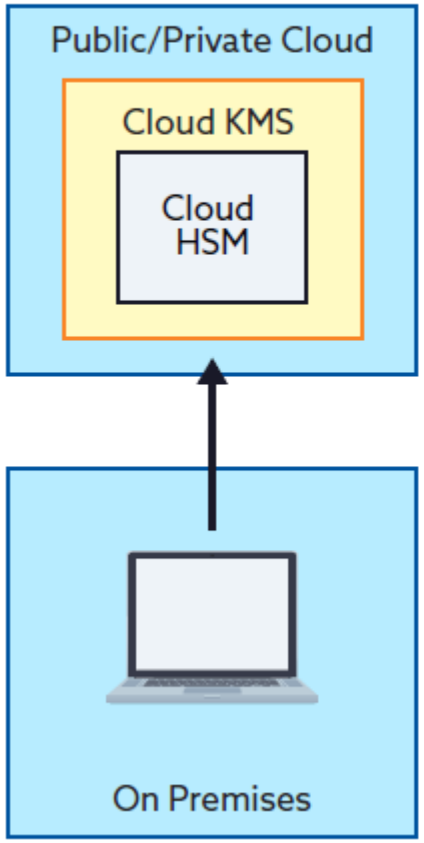
- Alibaba Cloud
- AWS
- Azure
- Google Cloud
- IBM

# Cloud Native KMS




- **KMS costruito e di proprietà del fornitore del servizio**
- **KMS è parte integrante del servizio oppure può essere fornito separatamente all'interno dello stesso fornitore di servizi cloud**
- **Algoritmi e moduli crittografici scelti e gestiti dal fornitore del cloud**

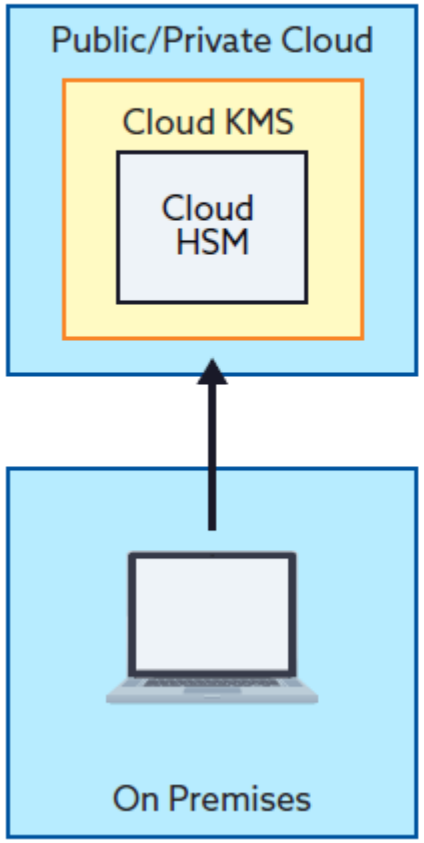
# Cloud Native KMS




**Proprietà**

- Tutti i componenti hardware e software sono sotto il controllo del fornitore, e il KMS è tipicamente una "scatola nera" per il cliente, a parte la documentazione pubblica
- In genere, ha una separazione dei compiti limitata o assente tra il servizio cloud e le caratteristiche del KMS
- Modello meno distruttivo per l'applicazione degli SLA (Service Level Agreement)
- L'ambiente cloud ha, o può avere, accesso ai dati in chiaro del cliente
- Questo modello può avere una bassa estensibilità delle funzioni KMS al di fuori del provider, anche se spesso fornisce una facile estensione ad altri servizi all'interno dello stesso
- Il costo è comunemente incorporato nel servizio cloud che il cliente acquista, ed è quindi nascosto, difficile da discernere, o assunto come zero

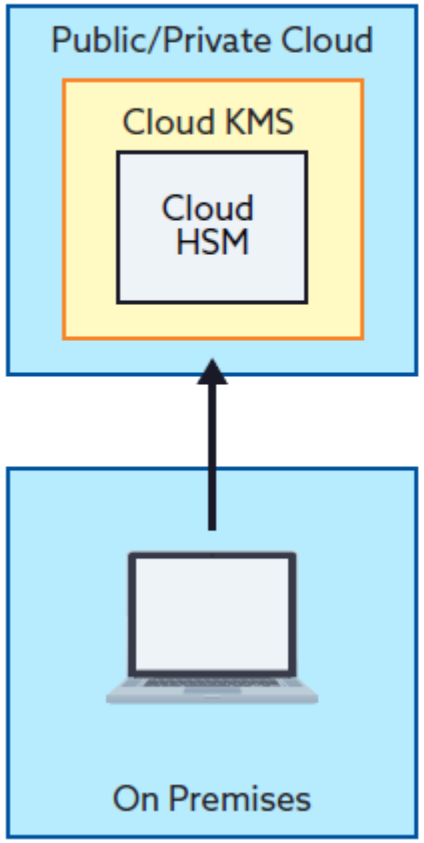
# Cloud Native KMS




**Proprietà**

- Il costo è guidato dalla competenza tecnica necessaria per amministrare e far funzionare le funzioni KMS
- Tempo di implementazione più veloce
- Tipicamente, alte prestazioni
- Tipicamente, alta scalabilità
- Non sensibile alla latenza
- Può supportare l'evoluzione verso altri modelli KMS del cloud
- Il supporto FIPS è limitato dal KMS del cloud
- In genere, non può supportare i requisiti per *key ceremony*

# Cloud Native KMS




## Sfide

Differenze di progettazione tra i fornitori di cloud → conoscenze e competenze tecniche per ogni fornitore di cloud

Spesso il modello amministrativo non distingue tra l'amministratore del servizio e l'amministratore del KMS → scarsa separazione dei compiti

La semplicità di implementazione e il set di funzioni disponibili per il consumatore possono mitigare la necessità di sviluppare molta conoscenza tecnica del dominio e carico amministrativo

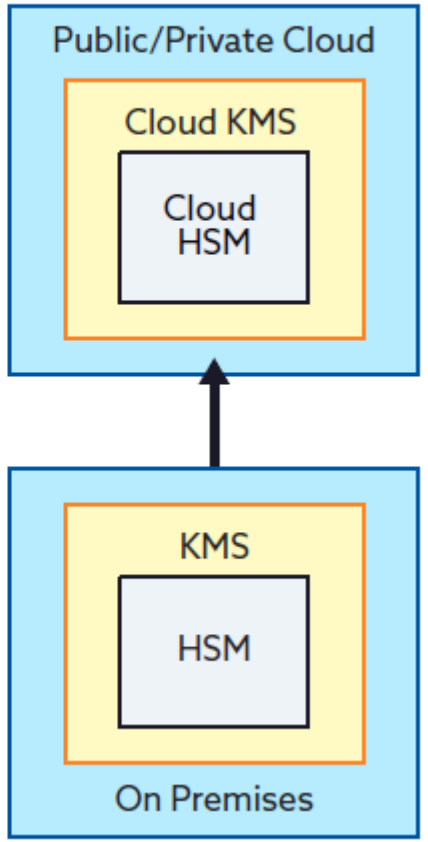
I dettagli su algoritmi e protocolli specifici non sono visibili all'utente → documentazione

Si ha poco o nessun controllo sulla configurazione o sulle azioni del KMS, → non soddisfa i requisiti di conformità come il periodo di rotazione delle chiavi o la revoca e il recupero

**Questo modello non garantisce la totale privacy dei dati del cliente dal fornitore di cloud provider, poiché il CSP (Cloud Service Provider) ha le chiavi**

# External Key Origination

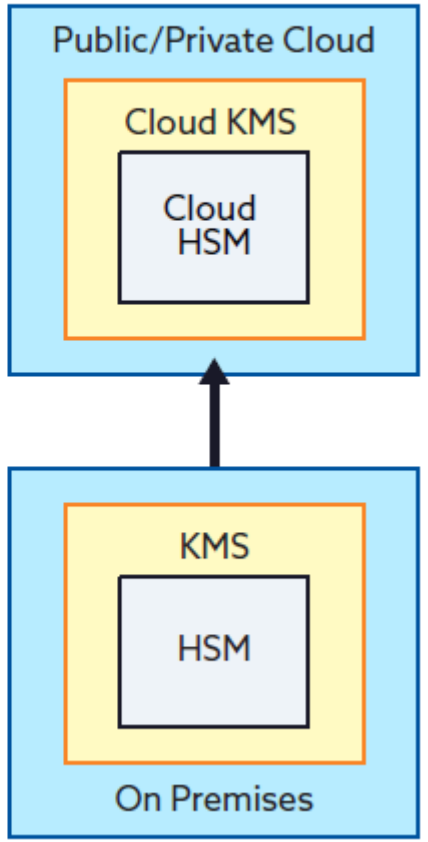
- **Cloud Native → generazione di chiavi (root) che hanno origine con un KMS esterno**
- **Si ha una "proprietà" delle chiavi**
- **No integrazione del KMS esterno con il KMS del cloud → il KMS esterno agisce solo come una struttura di generazione di chiavi**
  - In alcuni casi d'uso il provider può essere costretto a fare chiamate al KSM esterno → potenziali implicazioni per la gestione degli incidenti e impatto della latenza sulle prestazioni



# External Key Origination

**Proprietà**

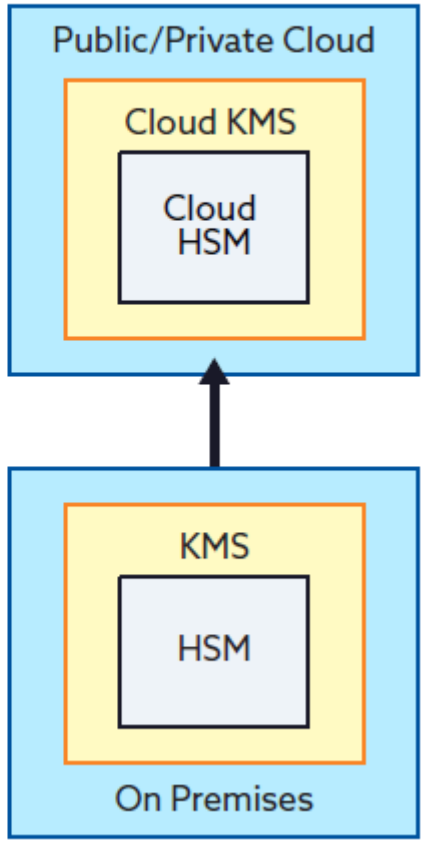
- I componenti hardware e software del cloud sono sotto il controllo del fornitore; il cliente controlla un KMS esterno al cloud e tipicamente lo usa per la generazione della chiave root e l'importazione nel KMS del cloud
- Chiara separazione dei compiti per la generazione della chiave root
- Minimo potenziale di impatto sugli SLA del cloud, sebbene il processo di importazione della chiave esterna possa avere un impatto sulle operazioni di recupero
- **L'ambiente in-the-cloud ha, o può avere, accesso ai dati in chiaro del cliente**
- Questo modello può avere una bassa estensibilità delle funzioni KMS al di fuori del fornitore, sebbene spesso fornisce una facile estensione ad altri servizi all'interno dello stesso provider



# External Key Origination

**Proprietà**

- Costo determinato dal prezzo delle licenze per la funzionalità di importazione delle chiavi, dal numero di chiavi importate e dalla gestione del KMS esterno da cui vengono importate le chiavi
- Il tempo di implementazione è tipicamente determinato dall'acquisizione e dalla configurazione del KMS esterno che sarà utilizzato per la generazione e l'importazione delle chiavi.
- Le prestazioni sono tipicamente le stesse del modello KMS nativo
- La scalabilità è tipicamente la stessa del modello KMS nativo
- La sensibilità alla latenza è tipicamente la stessa del modello KMS nativo
- Soddisfa i *key ceremony* del cliente per le chiavi root



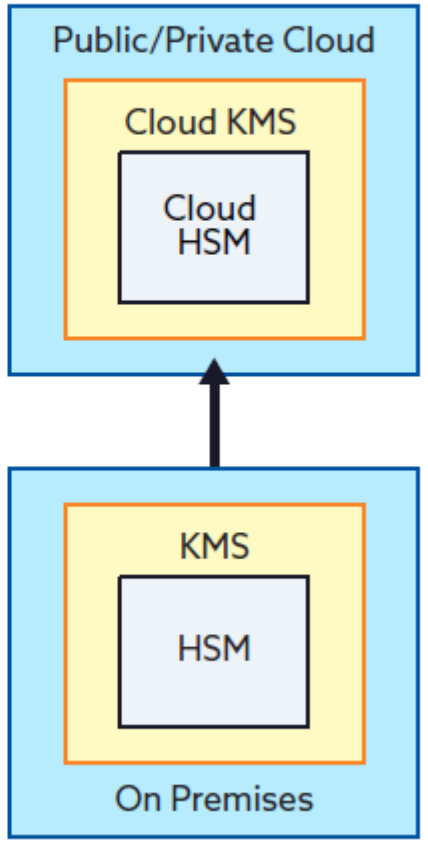
# External Key Origination

## Sfide

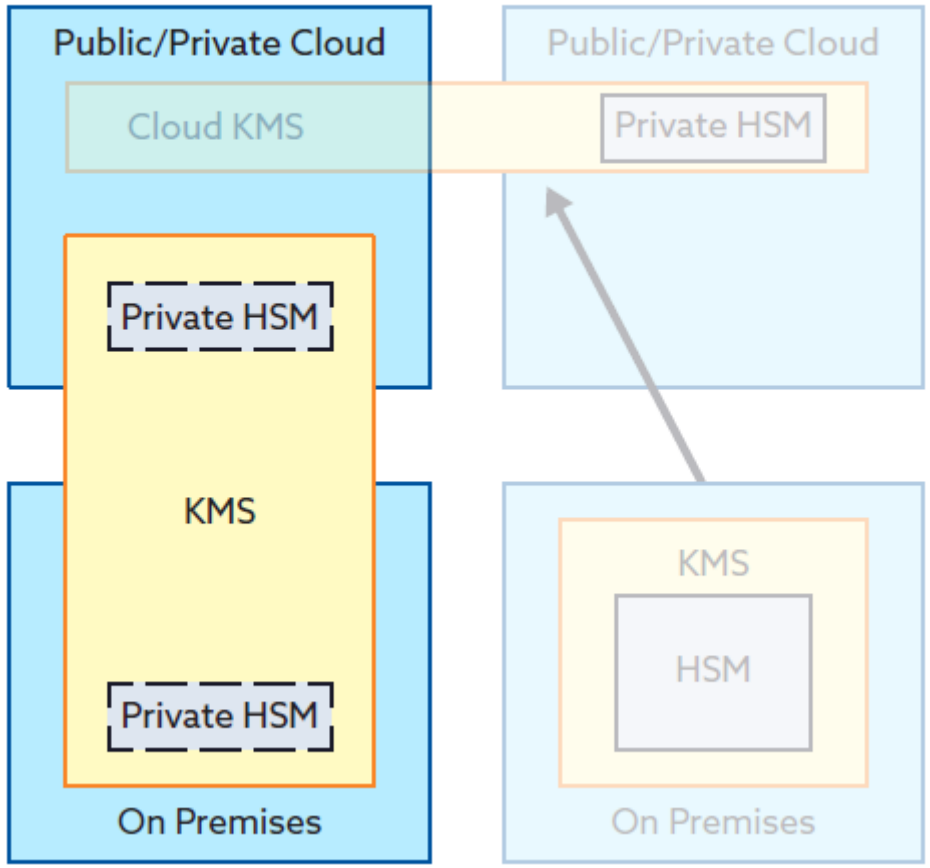
- **Tutte le sfide del modello Cloud Native si applicano**

- Il fornitore di cloud potrebbe supportare solo un insieme limitato di produttori di hardware per la generazione di chiavi esterne → può essere necessario acquisire hardware/software KMS compatibili → tempi di implementazione maggiori

- Le chiavi generate utilizzando il KMS esterno potrebbero non essere utili come copie di backup. I fornitori possono aggiungere metadati critici alle chiavi che il consumatore ha importato, rendendo le chiavi originali inutili per le operazioni di ripristino.

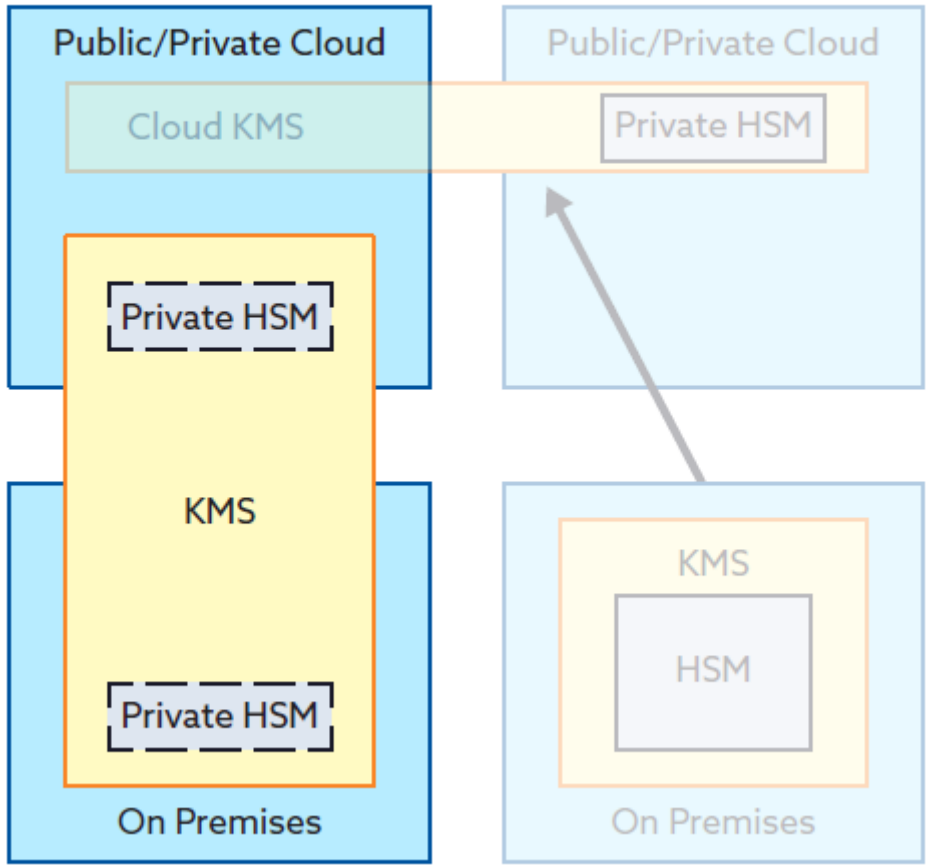


# Cloud Service con External Key Management System




- **KMS è esterno al servizio cloud**
- **Hardware (di proprietà dell'utente o del provider) è fornito esclusivamente per l'uso da parte dell'utente**
- **Servizi HSM cloud dedicato o co-locazione**
- **Gestione del KMS da parte dell'utente**
- **Total privacy ↔ no *key wrapping* o *unwrapping* dal CSP**

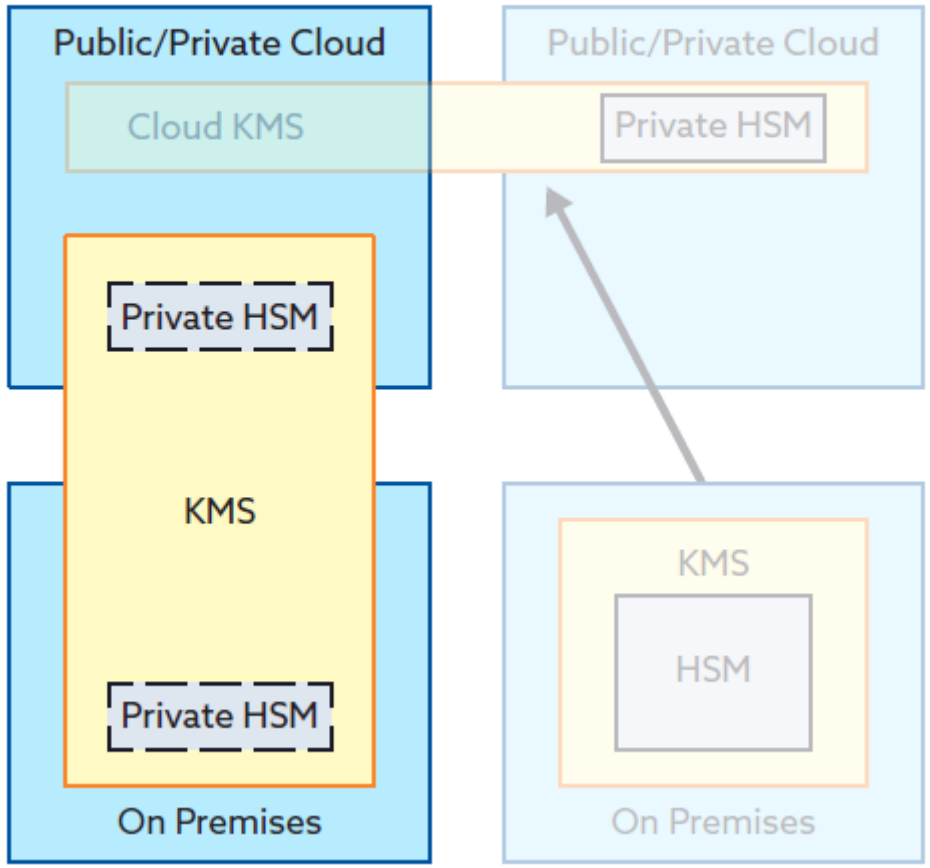
# Cloud Service con External Key Management System




**Proprietà**

- Alto grado di controllo e configurazione del cliente
- Separazione dei compiti per le attività del KMS e del servizio cloud, così come all'interno del KMS
- Può supportare l'unificazione del KMS in un unico punto di gestione
- **Key non condivise → nessun dato in chiaro del consumatore è esposto al provider**
- Massima portabilità poiché la maggior parte o tutte le funzioni KMS sono implementate al di fuori del servizio in-the-cloud

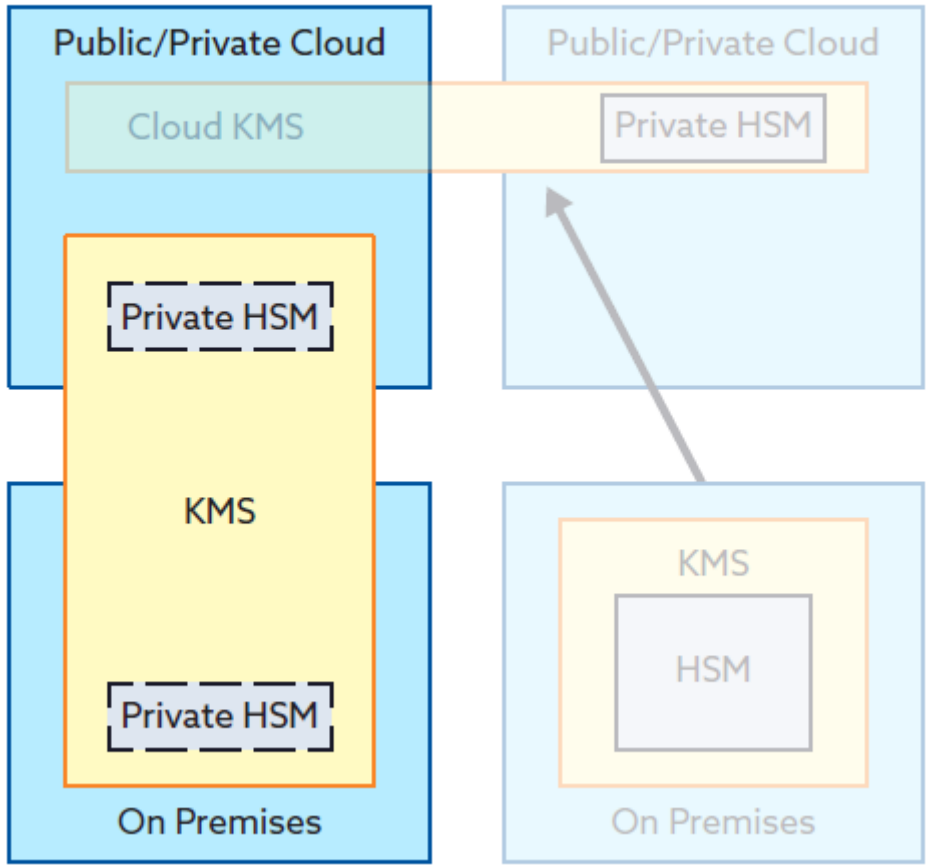
# Cloud Service con External Key Management System




**Proprietà**

- Costo più alto spesso determinato dalla scelta del KMS
- Lunghi tempi di implementazione
- Limitazioni delle prestazioni
- Limitazioni di scalabilità
- Impatto di latenza
- Conformità FIPS guidata dal cliente per tutte le chiavi
- Key ceremony

# Cloud Service con External Key Management System




**Sfide**

- Modello poco comune → disponibilità non garantita
- Implicazioni livello di servizio → malfunzionamenti
- **Garantisce la segretezza → incompatibile con SaaS o con sistemi che elaborano i dati**
- Richieste competenze per la gestione del KMS

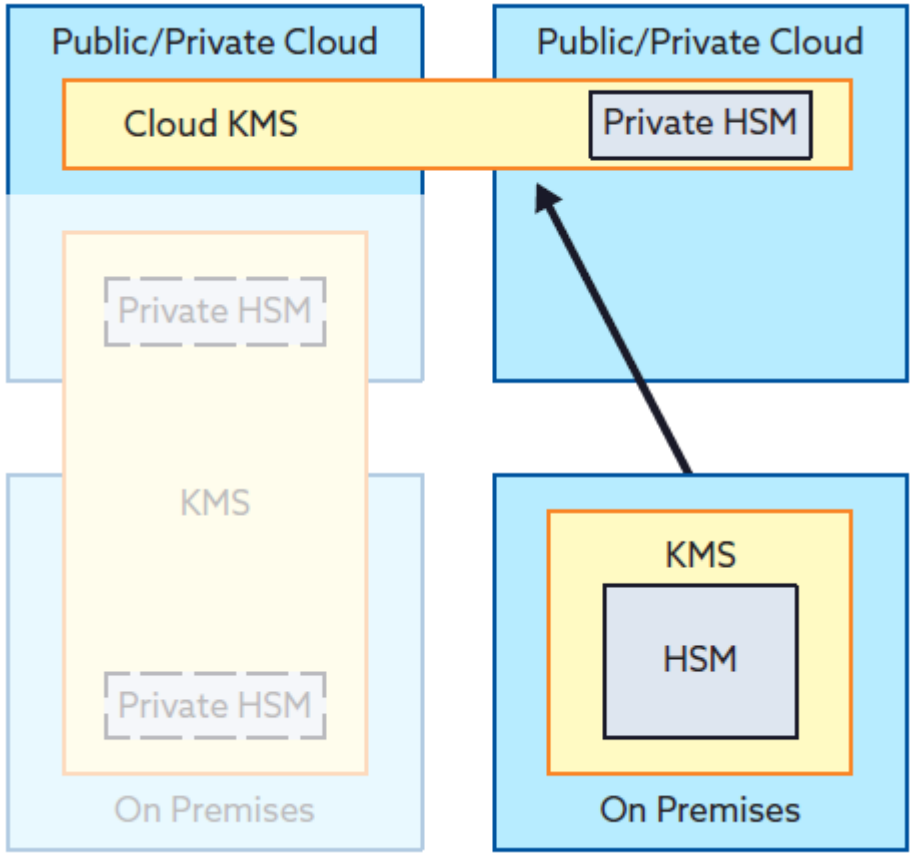
# Multi-Cloud Key Management Systems (MCKMS)

- **Capacità di fondere approcci per implementazioni KMS e servizi cloud**

- **Ci sono servizi cloud esistenti che supportano un KMS esterno, quindi è possibile**

  **→ per il KMS estendersi su molti cloud**

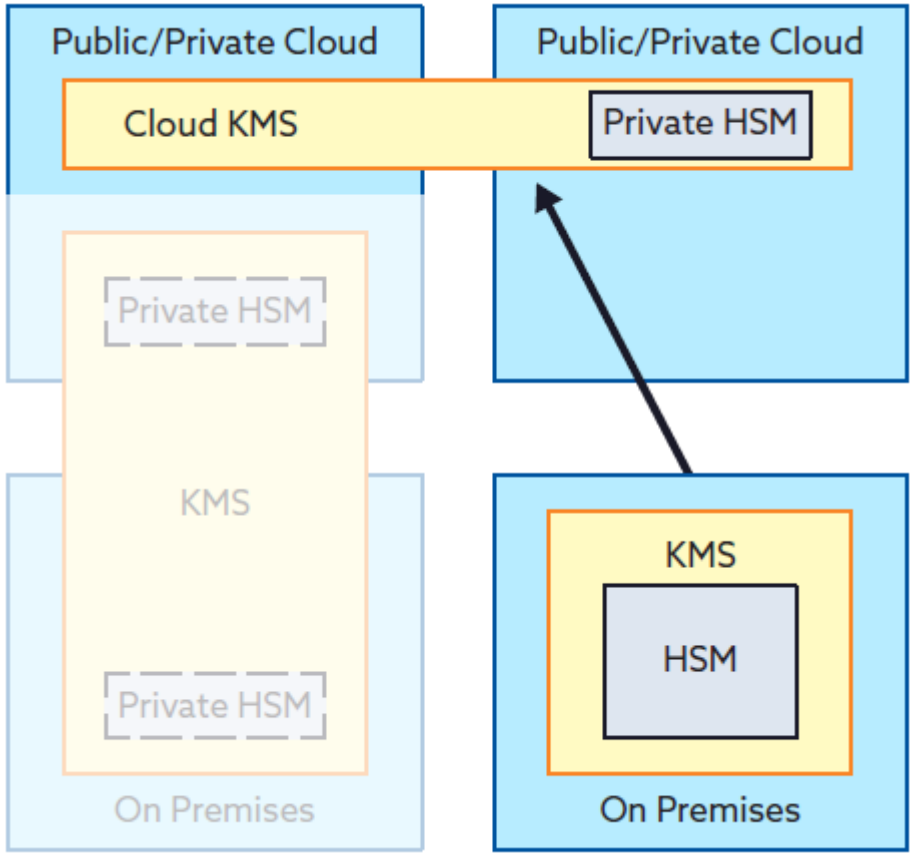
  **→ per il cloud estendersi su molte scelte di KMS**



# Multi-Cloud Key Management Systems (MCKMS)

**Proprietà**

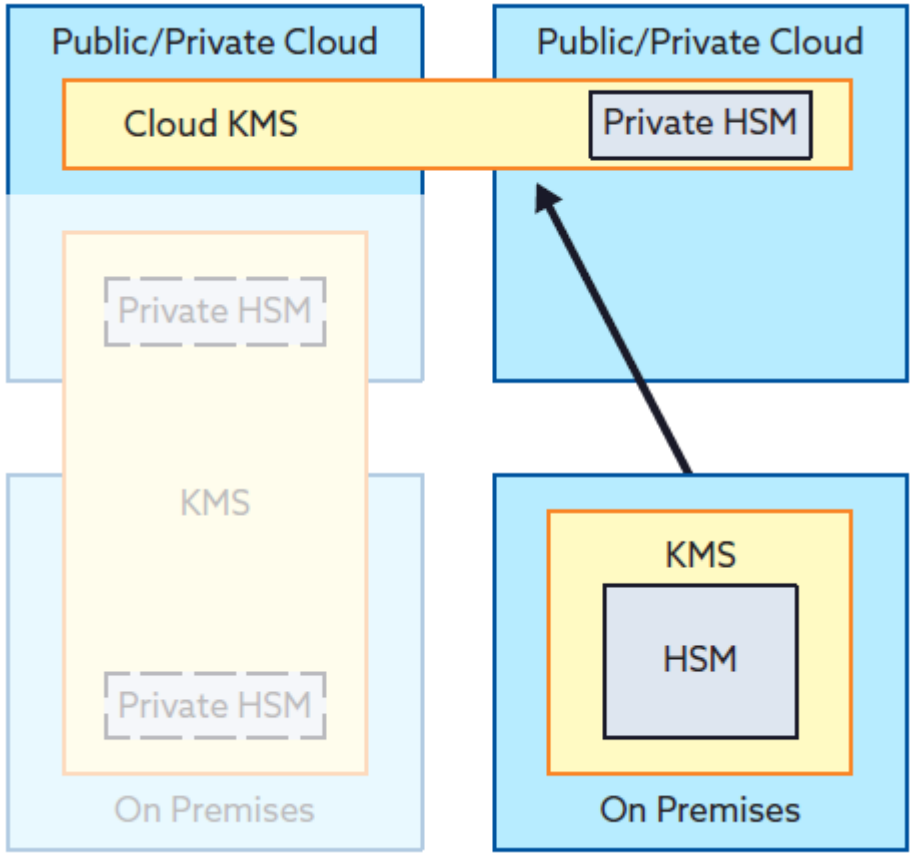
- Costo, complessità, controllo, tempo di implementazione, scala, prestazioni e interoperabilità sono in funzione degli altri modelli KMS nel cloud implementati
- Tolleranza agli errori grazie alla capacità di sfruttare un KMS cloud come backup di un altro KMS nel cloud
- Può avere l'effetto collaterale di accelerare l'adozione di ulteriori servizi in-the-cloud grazie agli investimenti in competenze e risorse



# Multi-Cloud Key Management Systems (MCKMS)

**Sfide**

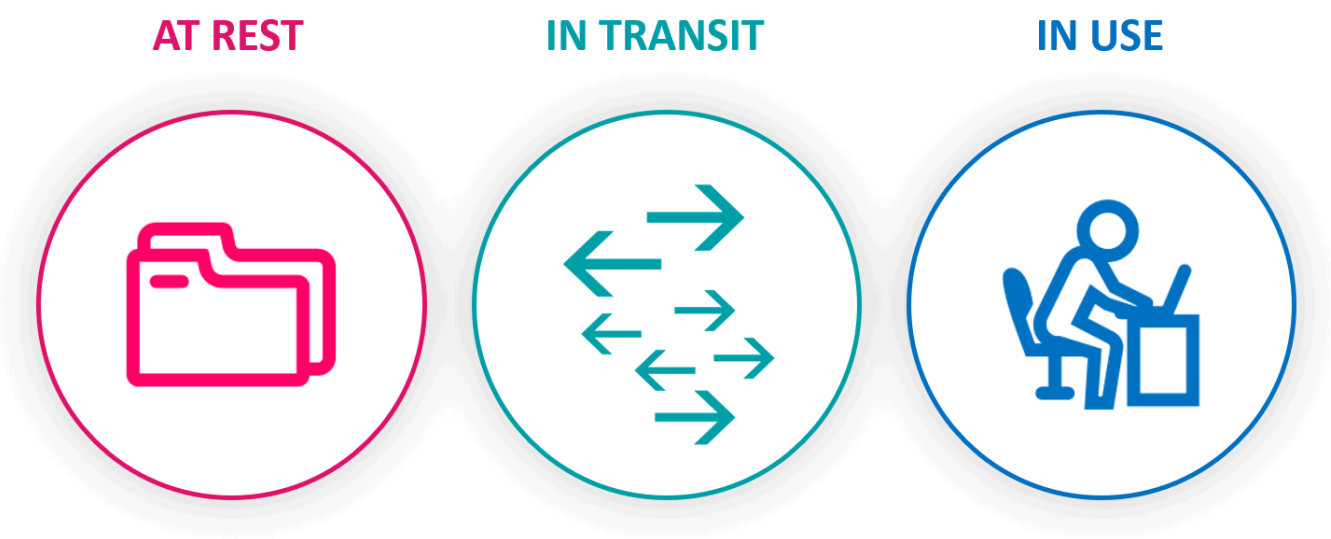
- Modello generalmente riservato a un approccio strategico alla gestione delle chiavi
- Richiede la più ampia gamma di competenze, il più tempo per la progettazione e l'implementazione, e il più alto costo in capitale (licenze) e/o costi operativi
- Fornisce il maggior grado di portabilità, tolleranza agli errori e scalabilità grazie allo sfruttamento di più fornitori di cloud pubblici



# The three states of data

# The three states of data

## Analisi sugli scenari di crittografia (at Rest, in Motion, in Use)




*5. https://www.sealpath.com*

# The three states of data

## Analisi sugli scenari di crittografia (at Rest, in Motion, in Use)


*5. https://www.sealpath.com*

# The three states of data

## Analisi sugli scenari di crittografia (at Rest, in Motion, in Use)


*5. https://www.sealpath.com*

# The three states of data

## Analisi sugli scenari di crittografia (at Rest, in Motion, in Use)

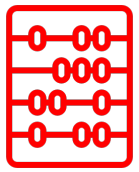

*5. https://www.sealpath.com*

# Homomorphic Encryption

# Perché Homomorphic Encryption?

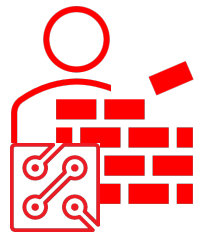
**Come garantire la privacy?**

- affidarsi a hardware fidato sul lato server (Goldreich e Ostrovsky, 1996)



- hardware sicuro limita la capacità di calcolo del server cloud (Sahai, 2008)

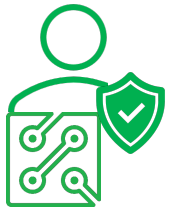
- GC (*garbled circuits*) per una secure two-party computation (Yao 1982; Kolesnikov et al. 2009; Goldwasser et al. 2013)

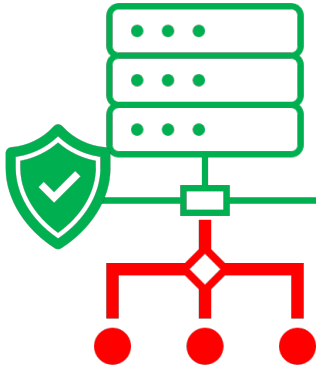


# Homomorphic Encryption

**Come garantire la privacy?**

- GC + FHE
  (Gennaro et al. 2010)





- Twin Cloud
  (Bugiel et al 2011)

- Cloud computing basato su token
  (reza Sadeghi et al. 2010)

# Homomorphic Encryption - Definizioni

**Gruppo:**

Sia G un insieme non vuoto su cui è definita una operazione binaria, cioè un'applicazione $\bullet : G \times G \rightarrow G$. Allora $(G, \bullet)$ risulta un *gruppo* se:

i. l'applicazione $\bullet$ è associativa;

ii. esiste elemento neutro;

iii. esiste elemento inverso.

# Homomorphic Encryption - Definizioni

**Omomorfismo:**

Siano (G, •) e (H, *) due gruppi muniti di due distinti operazioni binarie.
Un'applicazione f : G → H è detta *omomorfismo* di gruppi se:

$$f(a \bullet b) = f(a) * f(b)$$

# Homomorphic Encryption - Definizioni

**Schema di HE:**

Uno schema crittografico a chiave pubblica che calcola un'operazione sui testi cifrati che è equivalente a qualche operazione binaria sui corrispondenti testi in chiaro.

Se $\mathbf{M} \in (\mathbf{H}, \bullet)$ è l'insieme dei testi in chiaro da crittografare con una chiave pubblica *pk* in uno spazio di cifratura $(\mathbf{C}, \otimes)$, si ha che $\forall\ m_1, m_2 \in \mathbf{M}$:

$$\text{Encrypt}(m_1 \bullet m_2, pk) = \text{Encrypt}(m_1, pk) \otimes \text{Encrypt}(m_2, pk) = c_1 \otimes c_2.$$

Inoltre, per qualsiasi coppia di testi cifrati

$$c_1 = \text{Encrypt}(m_1, pk), \qquad c_2 = \text{Encrypt}(m_2, pk)$$

chiave segreta *sk* e chiave pubblica *pk*

$$\text{Decrypt}(c_1 \otimes c_2, sk) = m_1 \bullet m_2$$

# Homomorphic Encryption - PHE

## RSA

$$\mathbf{E}(x) = x^e \bmod m$$

$$\mathbf{E}(x_1) \cdot \mathbf{E}(x_2) = x_1^e\, x_2^e \bmod m = (x_1 x_2)^e \bmod m = \mathbf{E}\,(x_1 \cdot x_2)$$

# Homomorphic Encryption - PHE

## Paillier

$pk = (n, g)$, $r \in \mathbf{Z}^*$ (casuale), $m \in \mathbf{Z}$

$$\text{Encrypt}(m, pk) = g^m r^n \pmod{n^2}$$

$$c_1 = \text{Encrypt}(m_1, pk) = g^{m1}\, r_1^{\,n} \bmod n^2$$
$$c_2 = \text{Encrypt}(m_2, pk) = g^{m2}\, r_2^{\,n} \bmod n^2$$

$$c_1 c_2 = g^{m1}\, r_1^{\,n}\, g^{m2}\, r_2^{\,n} = g^{m1+m2}\,(r_1 r_2)^n \bmod n^2 = c_3$$

# Homomorphic Encryption - PHE

## **ElGamal** (p = 2q + 1)

*e-voting protocal (UniCrypt, 2017)*

$$\mathbf{E} : G_q \rightarrow G_q \times G_q$$

$$\mathbf{E}(m) = (g^r, m * h^r)$$

x: chiave segreta
h: chiave pubblica
g: generatore
m: messaggio
r : num casuale

$$\mathbf{E} : (G_q, *) \rightarrow (G_q \times G_q, *)$$

$$\mathbf{E}(m_1) * \mathbf{E}(m_2) = (g^{r1}, m_1 * h^{r1})(g^{r2}, m_2 * h^{r2})$$
$$= (g^{r1+r2}, m_1 * m_2 * h^{r1+r2})$$
$$= \mathbf{E}(m_1 * m_2)$$

# Homomorphic Encryption - PHE

## **ElGamal** ($p = 2q + 1$)

$$\mathbf{E} : Z_q \rightarrow G_q \times G_q$$

$$E(m_1) * E(m_2) = (g^{r1}, g^{m1} * h^{r1})(g^{r2}, g^{m2} * h^{r2})$$
$$= (g^{r1+r2}, g^{m1}g^{m2} * h^{r1+r2})$$
$$= E(m_1 + m_2)$$

# Homomorphic Encryption - SHE

- **Sander, 1999**
- **Boneh–Goh–Nissim (BGN), 2005**
- **Melchor, 2008**
- **Gentry, 2009**

# Homomorphic Encryption - SHE

Per criptare **m**, si scelgono a caso **q** (grande) e **r** (piccolo).

$$c = pq + 2r + m$$

$$m = (c \bmod p) \bmod 2$$

$$c_1 = q_1 p + 2r_1 + m_1 \quad \text{e} \quad c_2 = q_2 p + 2r_2 + m_2$$

**Somma:**

$$c_1 + c_2 = (q_1 + q_2)p + 2(r_1 + r_2) + (m_1 + m_2)$$

$$c_1 + c_2 \bmod p = 2(r_1 + r_2) + (m_1 + m_2)$$

**Molt:**

$$c_1 * c_2 = (c_1 q_2 + q_1 c_2 - q_1 q_2)p + 2(2r_1 r_2 + r_1 m_2 + m_1 r_2) + m_1 * m_2$$

$$c_1 * c_2 \bmod p = 2(2r_1 r_2 + \ldots) + m_1 * m_2$$

# Homomorphic Encryption - FHE

**Zhang** – 2014

$KeyGen_{\varepsilon}(\lambda) \rightarrow (pk, sk)$

$Encrypt_{\varepsilon}(m, pk) \rightarrow c = Encrypt_{\varepsilon}(m, pk)$

$Decrypt_{\varepsilon}(c, sk) \rightarrow m = Decrypt_{\varepsilon}(c, sk)$

$Evaluate_{\varepsilon}(f, c_1, \ldots, c_t, pk) \rightarrow \boldsymbol{C}^{n}(c_1, c_2 \ldots, c_n)$

$$Decrypt_{\varepsilon}(Evaluate_{\varepsilon}(\boldsymbol{C}, c_i, pk), sk) = C(m_1, \ldots, m_t)$$

# Homomorphic Encryption - FHE

$$\text{Decrypt}_{\varepsilon}(\text{Evaluate}_{\varepsilon}(\boldsymbol{C}, c_i , pk), sk) = C(m_1, \ldots, m_t)$$

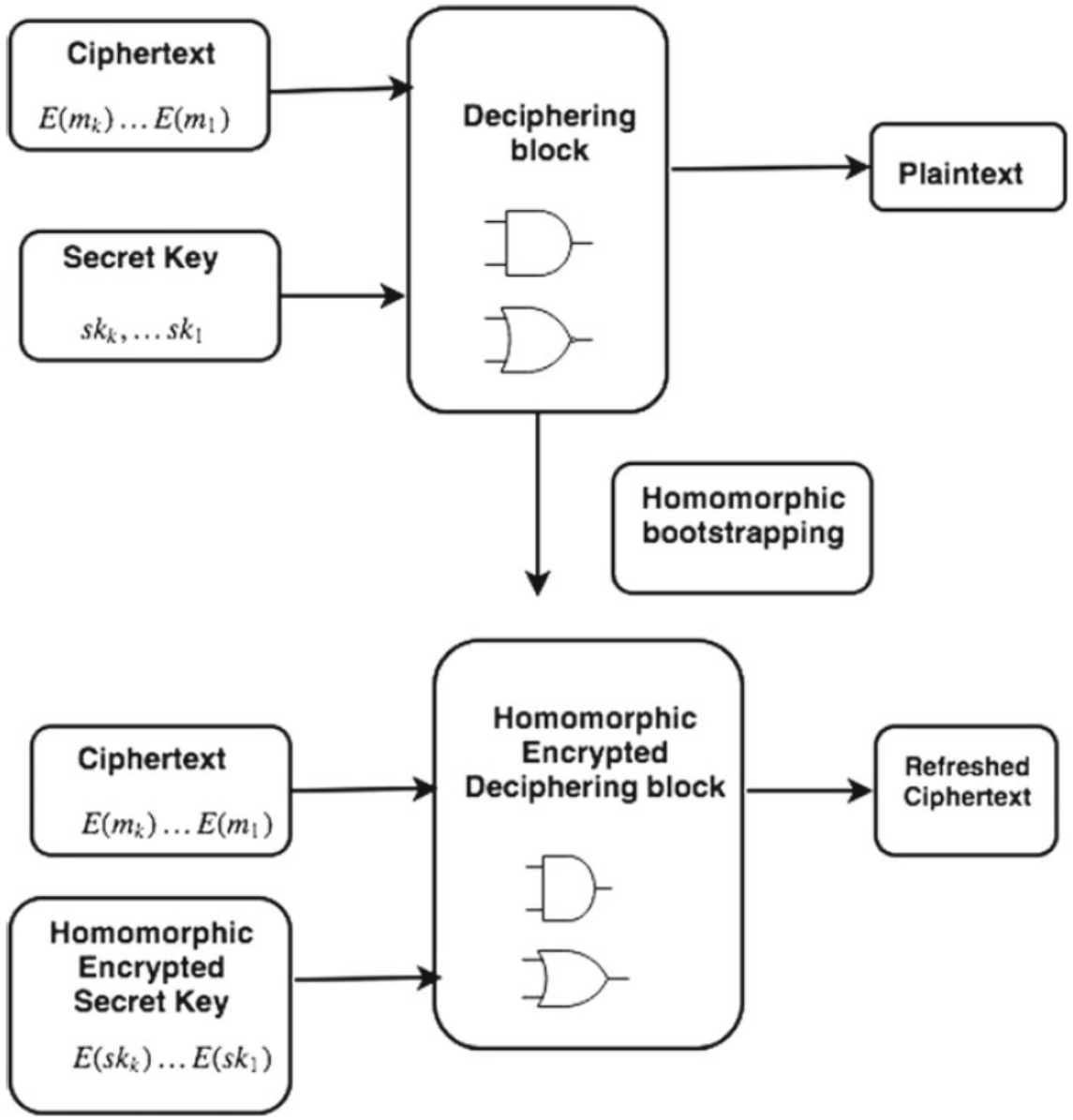
**Definizione:**

Lo schema **ζ = (KeyGen, Encrypt, Decrypt, Evaluate)** è omomorfico per una classe ***C*** di circuiti se è corretto secondo l'eq. in verde per tutti i circuiti $C \in \boldsymbol{C}$.
**ζ** è completamente omomorfo se è corretto per tutti i circuiti booleani.

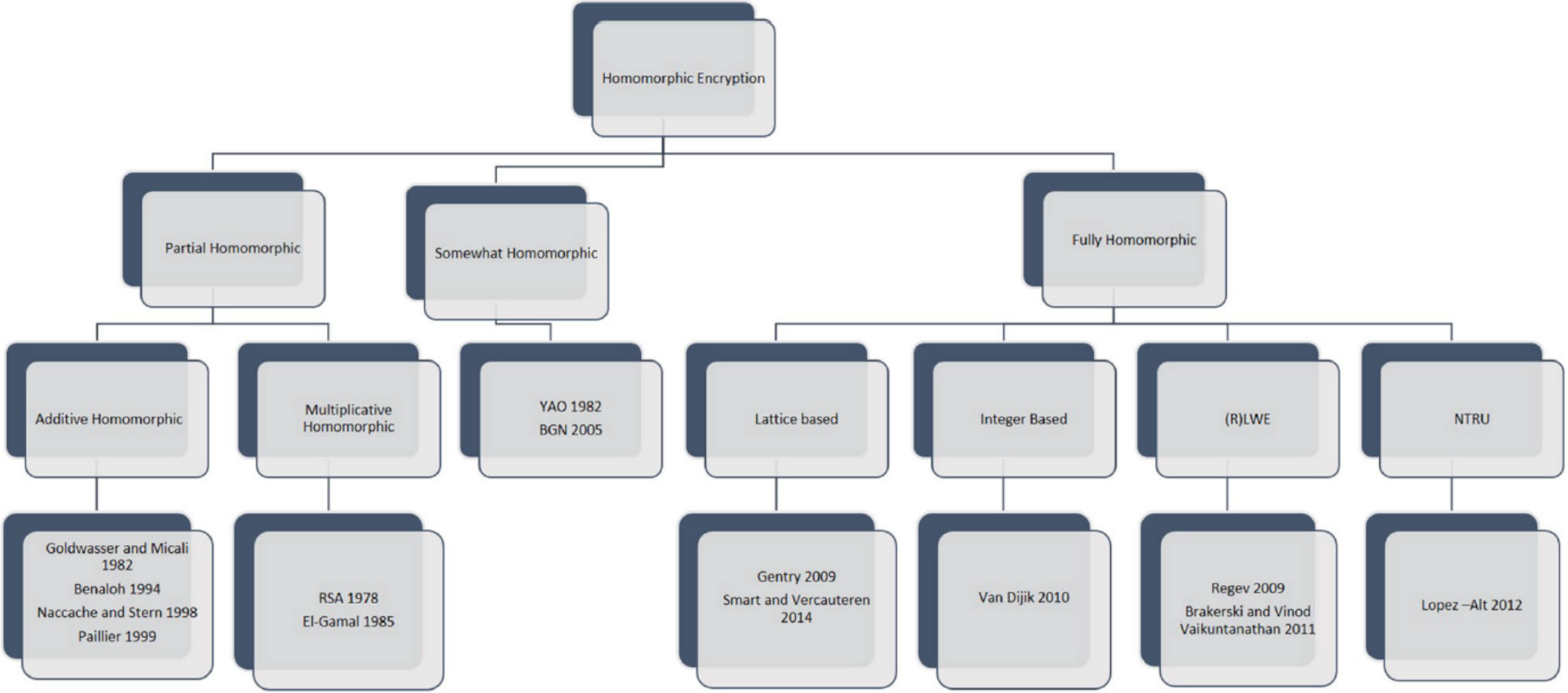
# Homomorphic Encryption - FHE

**Gentry:**

- SHE su polinomi a *l*-variabili
- bootstrapping
  - recrypt



# Homomorphic Encryption - Overview

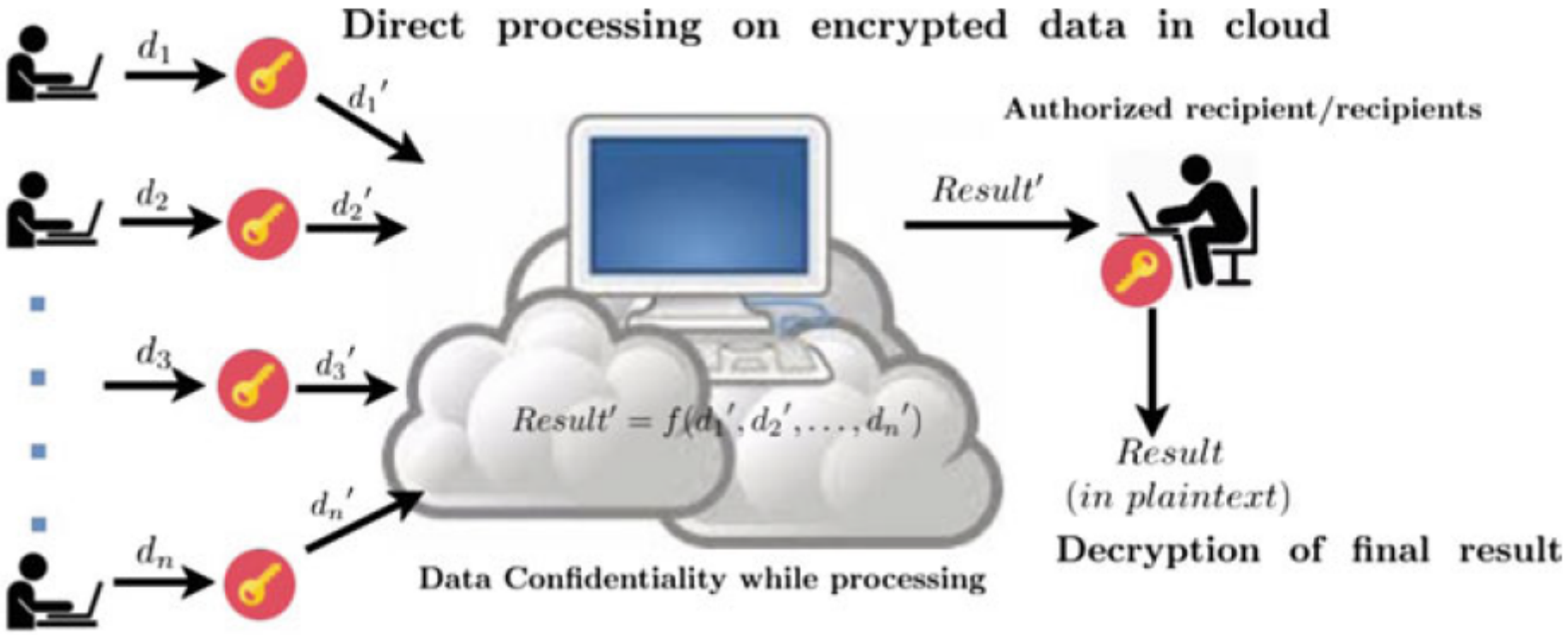



Kundan Munjal, Rekha Bhatia, A systematic review of homomorphic encryption and its contributions in healthcare industry, Springer, Aprile 2022

# Homomorphic Encryption in Cloud

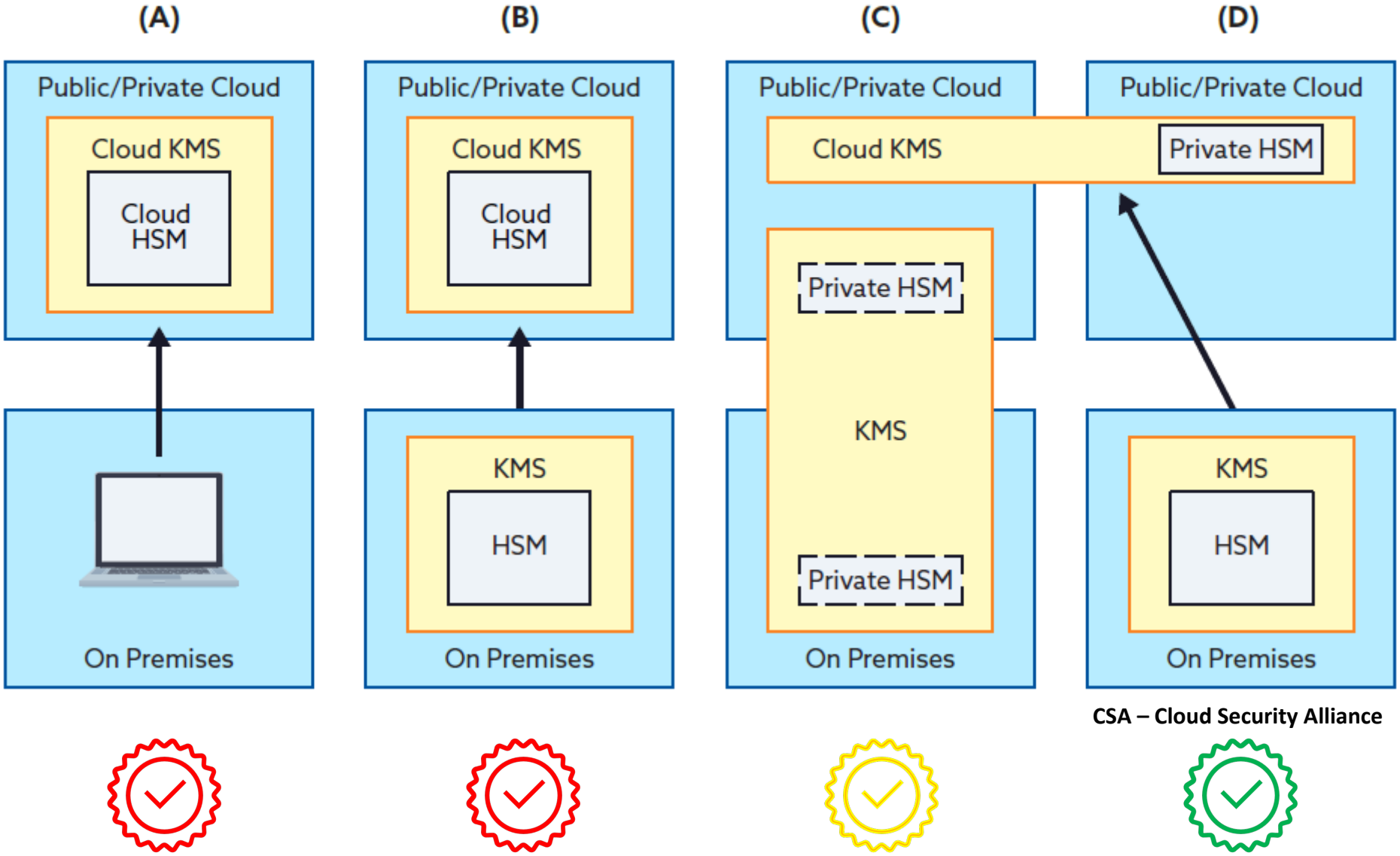
# Homomorphic Encryption - FHE

## FHE su cloud



# Homomorphic Encryption - FHE

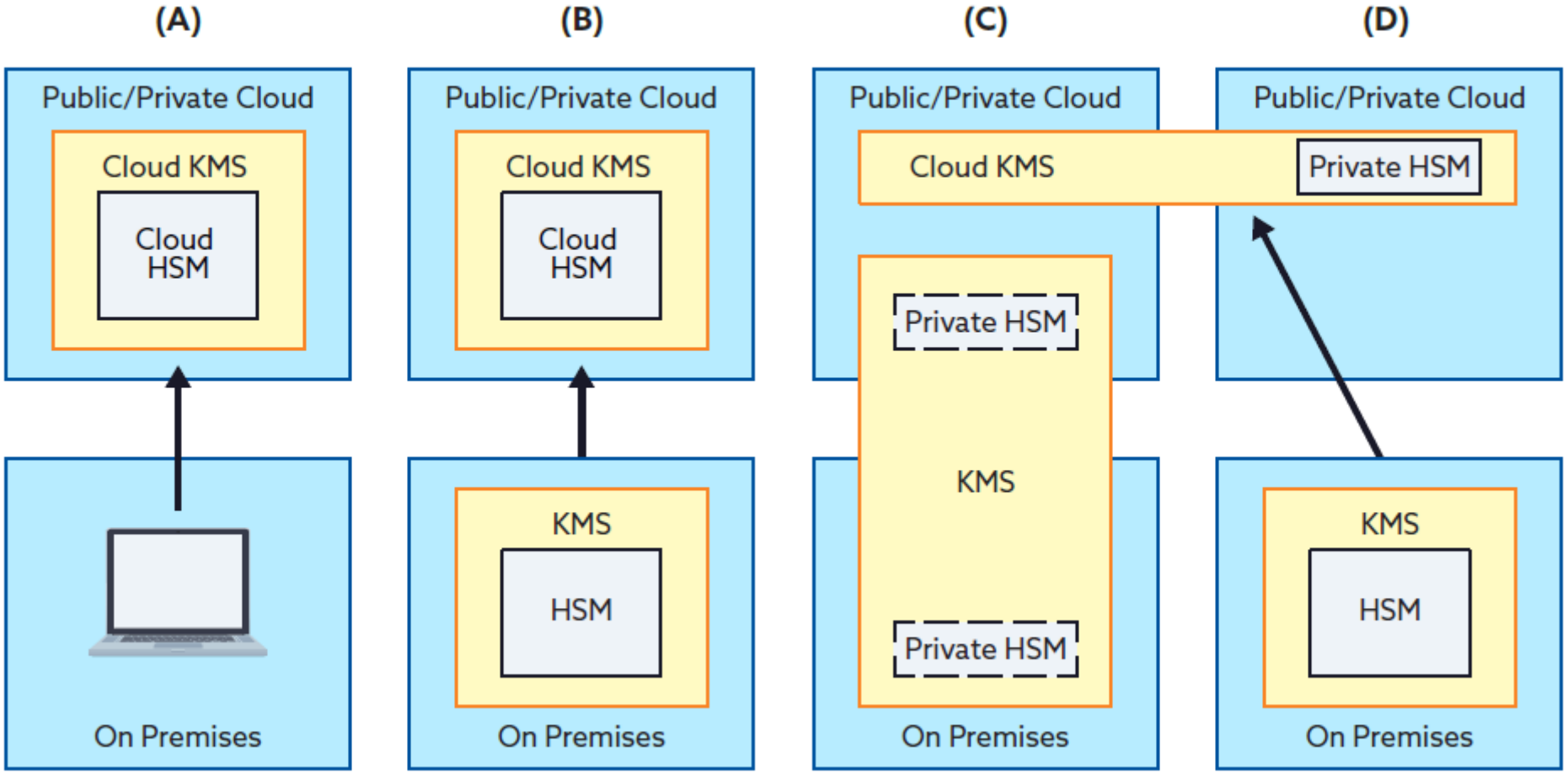
## Servizi cloud e schemi KMS - Trust




**CSA – Cloud Security Alliance**

# Homomorphic Encryption - FHE

## Servizi cloud e schemi KMS - Trust

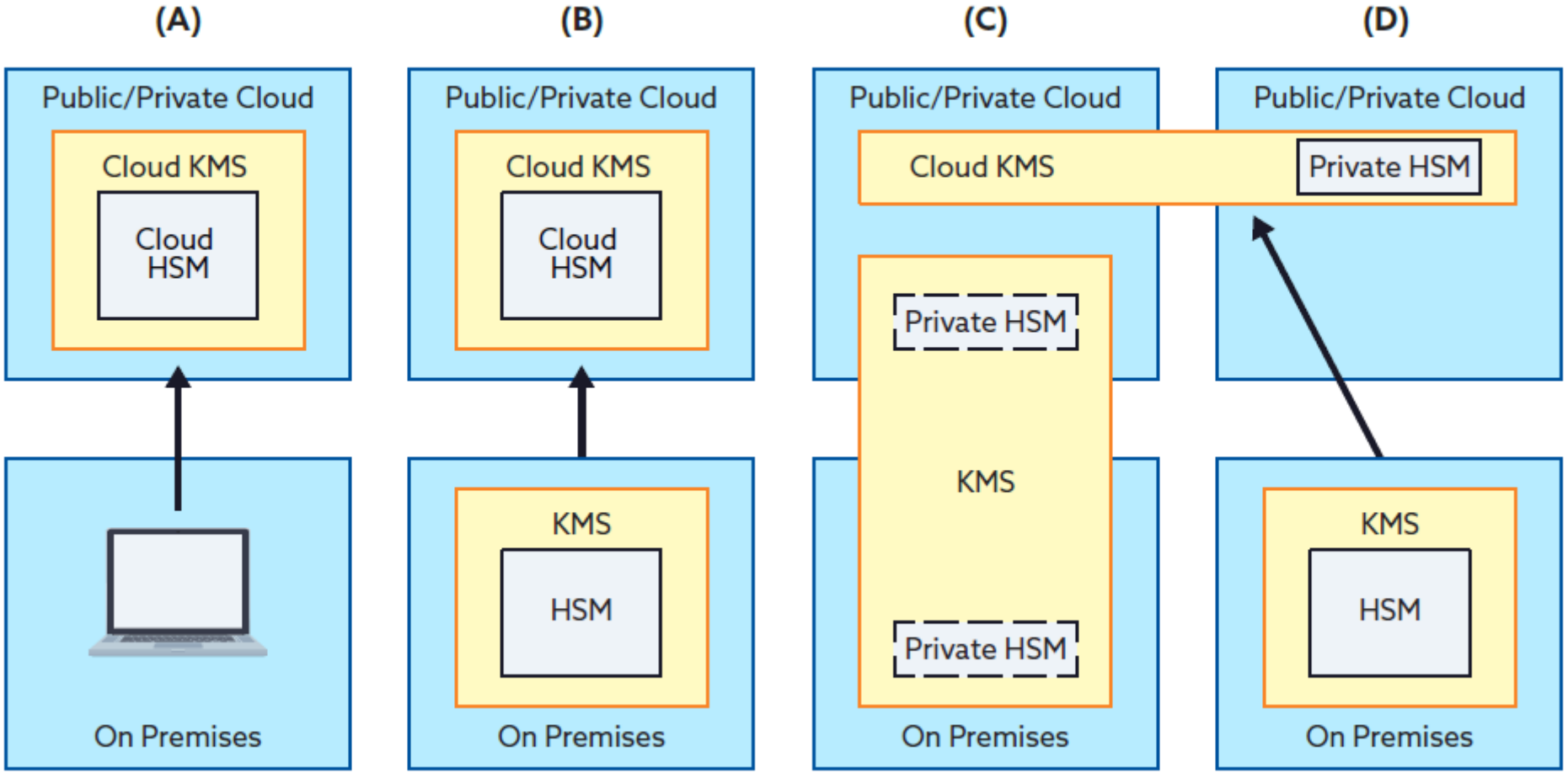



**CSA – Cloud Security Alliance**

# at Rest/in Motion

# Homomorphic Encryption - FHE

## Servizi cloud e schemi KMS - Trust

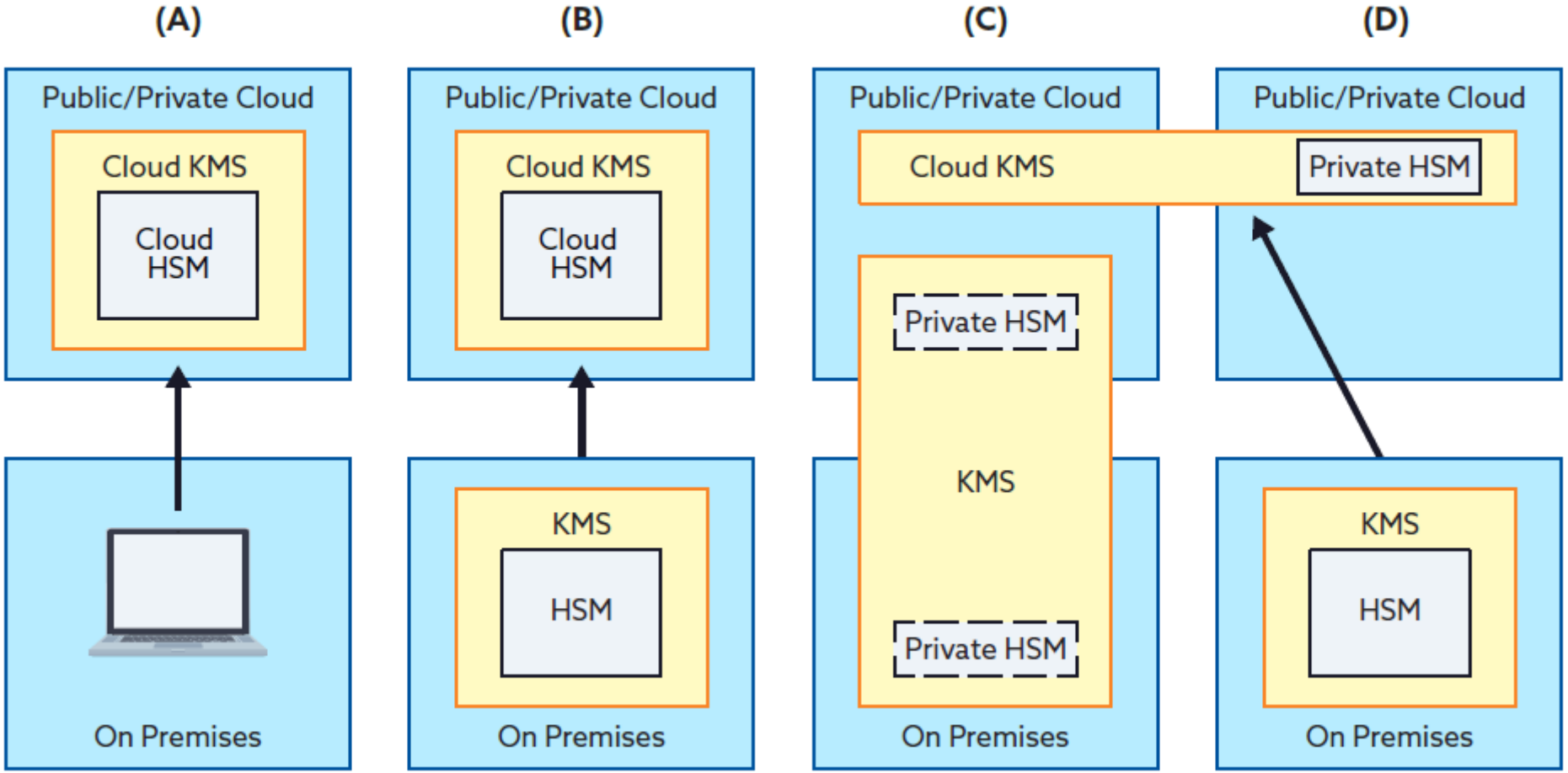



**CSA – Cloud Security Alliance**

**in Use:**

# Homomorphic Encryption - FHE

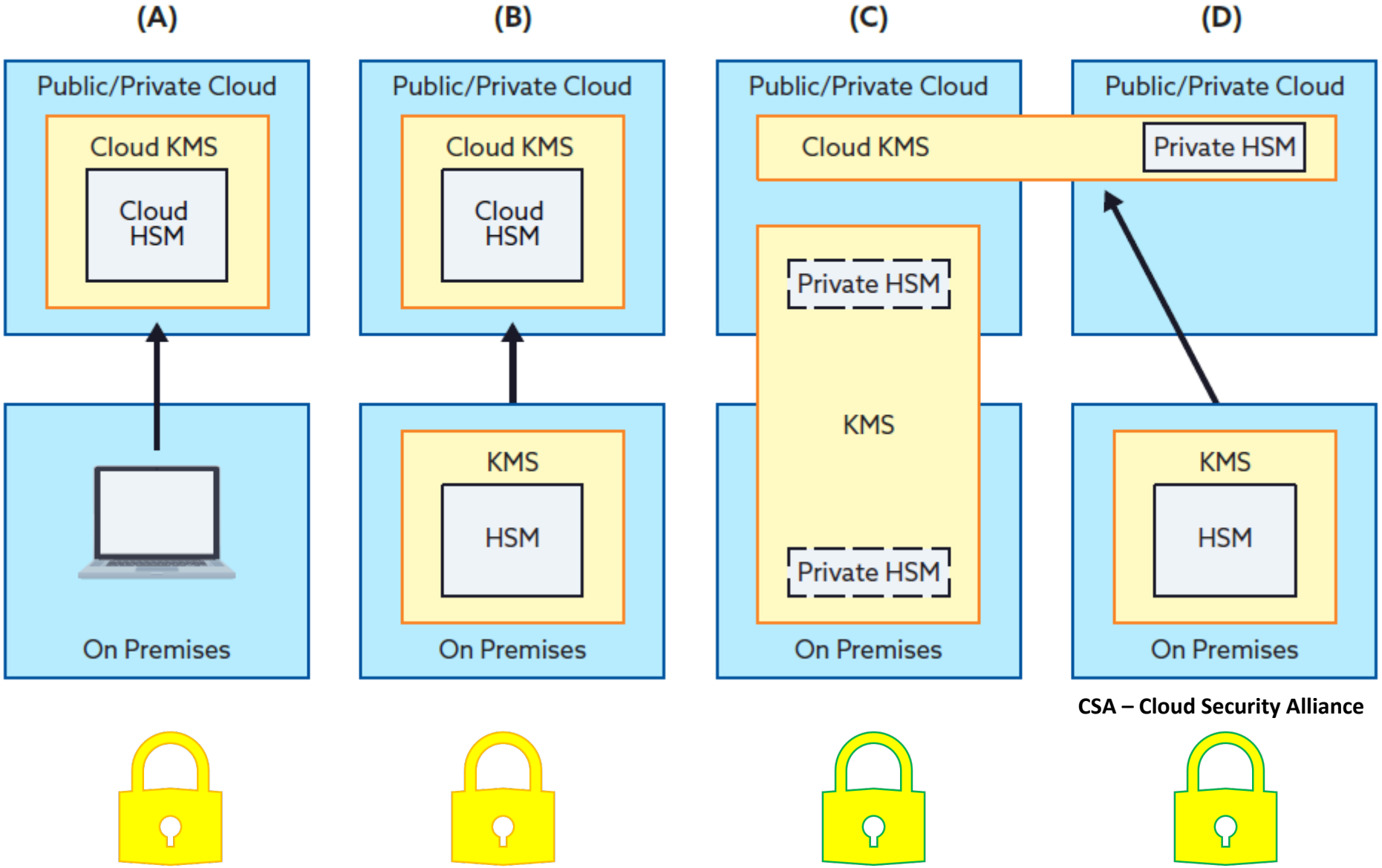
## Servizi cloud e schemi KMS - Trust




**CSA – Cloud Security Alliance**

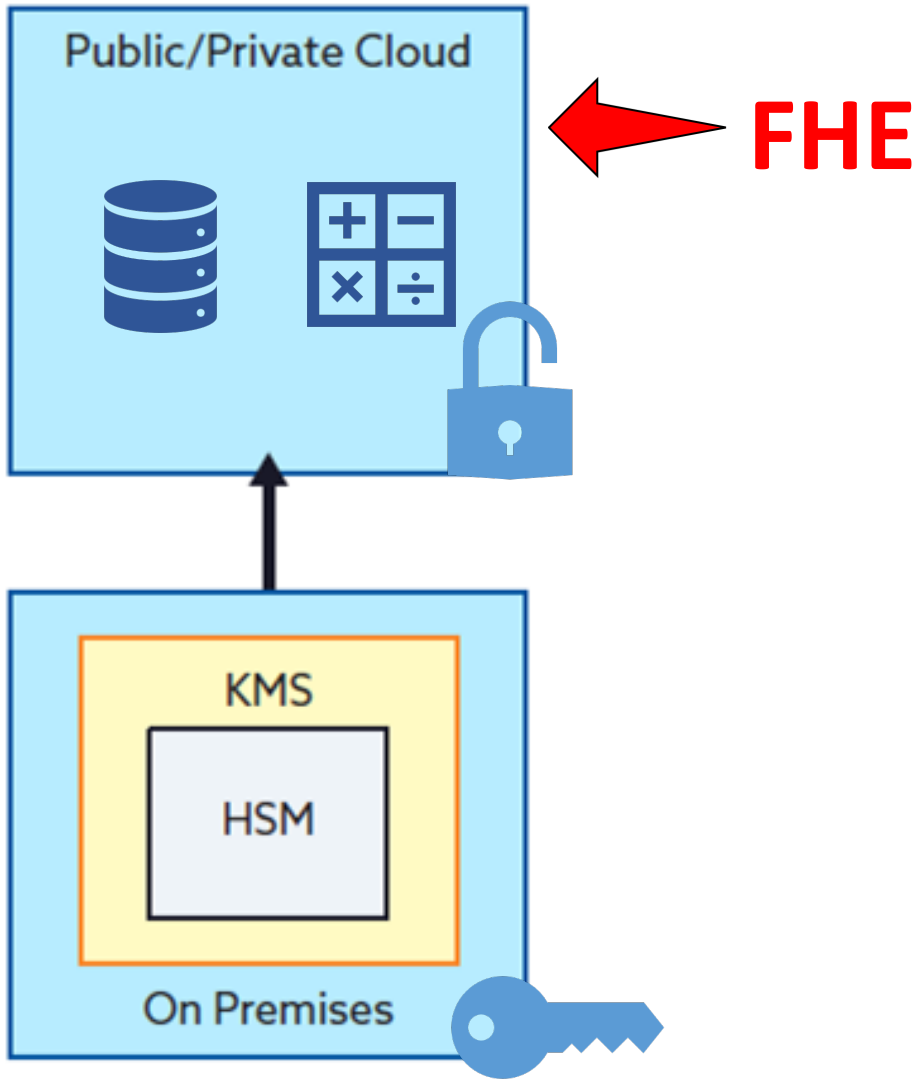
# Homomorphic Encryption - FHE

## Servizi cloud e schemi KMS - Trust




**CSA – Cloud Security Alliance**

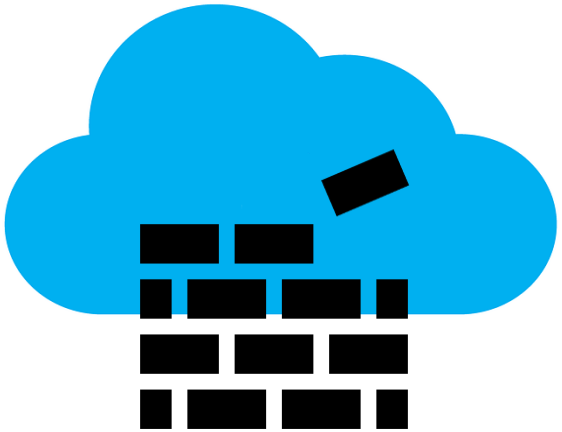
# Homomorphic Encryption - FHE




**“home” KMS**

# Homomorphic Encryption - Sfide

## 1 – Riprogettazione del Cloud



# Homomorphic Encryption - Sfide

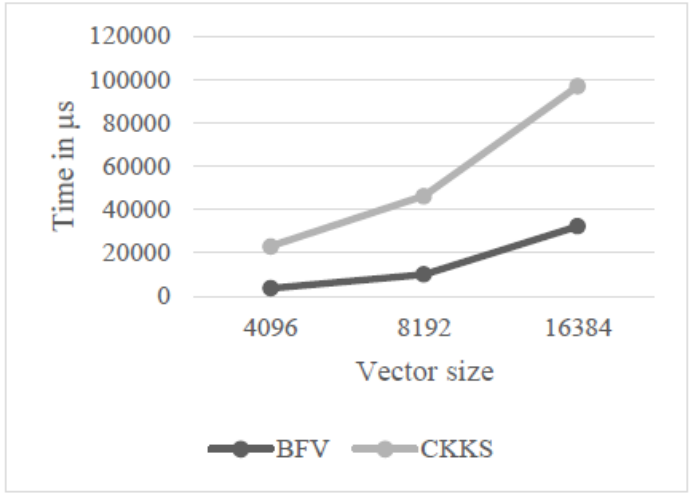



**Figure 1.**Addition Time in BFV vs CKKS

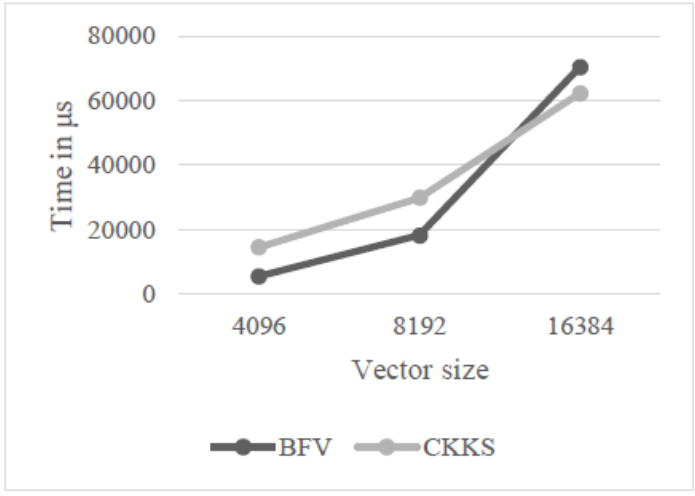



**Figure 2.** Squaring Time in BFV vs CKKS

## 2 – Costo Computazionale

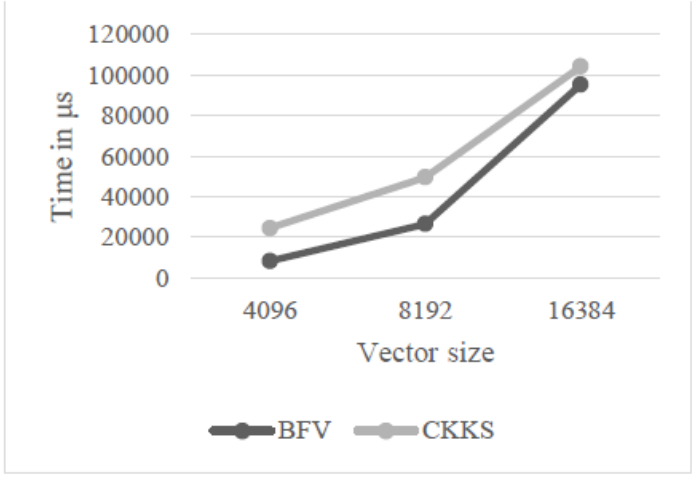



**Figure 3.** Multiplication Time in BFV vs CKKS

Shereen Mohamed Fawaz et al 2021 J. Phys.: Conf. Ser. 2128 012021

# Homomorphic Encryption - Sfide

## 3 – Limiti sulle operazioni

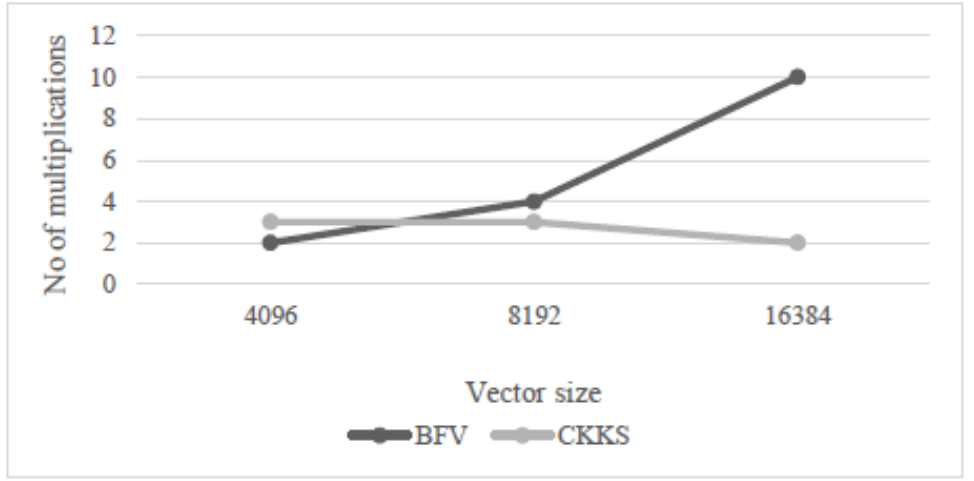



**Figure 4.** Maximum Number of Sequential Multiplications in BFV and CKKS Scheme

Shereen Mohamed Fawaz et al 2021 J. Phys.: Conf. Ser. 2128 012021

# Riferimenti


- A. Chatterjee, K. Aung, *Fully Homomorphic Encryption in Real World Applications*, Springer, 2019
- Cloude Security Alliance, *Key Management in Cloud Services: Understanding Encryption's Desired Outcomes and Limitations*, 2020
- S. M. Fawaz et al 2021 J. Phys.: Conf. Ser. 2128 012021
- K. Munjal, R. Bhatia, *A systematic review of homomorphic encryption and its contributions in healthcare industry*, Springer, 2022
- NISTIR 7956, *Cryptographic Key Management Issues & Challenges in Cloud Services*, NIST, 2013


EUSTEMA®

Making Innovation

# Grazie per l'attenzione


**ROMA**
Via Carlo Mirabello, 7
00195 – Roma
Tel.: +39 06372721
+39 06374931
Fax:+39 0637351735

**NAPOLI**
Centro Direzionale Via G.
Porzio, 4 - Isola C/2
80143 - Napoli
Tel.: +39 0816586610
Fax: +39 0816586611

**MILANO**
Via Roberto Lepetit, 8/10
20124 - Milano
Tel.: +39 0200696431


AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO
AGCM
RATING LEGALITA'

AZIENDA CON SISTEMA INTEGRATO
CERTIFICATO DA RINA
**ISO 9001 – ISO 14000 – SA 8000 – ISO 20000 – ISO 27001**

**www.eustema.it**