PSN — Analisi dei Profili di Sovranità Digitale

Perché il Polo Strategico Nazionale non garantisce la sovranità digitale

Osservatorio Nazionale sulla Sovranità Digitale — progetto indipendente

05.08.2026

Documento generato automaticamente dalla pagina osservatorio.mxmap.it/psn/. Pagina e PDF hanno una sorgente unica: non possono divergere.

Analisi tecnica

La cifratura e il confidential computing sono misure di sicurezza reali e utili. Sono anche, da sole, incapaci di produrre sovranità su un cloud controllato da un'altra giurisdizione — e l'agenzia francese per la cybersicurezza lo mette per iscritto.

Il programma cloud pubblico italiano realizza **un consolidamento reale** e **ingegneria di sicurezza reale**. **Non** realizza la sovranità digitale, ed è presentato come se lo facesse.

Nel suo stesso manuale utente, l'etichetta formale **«sovranità del dato» è attribuita a una copia di backup periodica fuori sito** — replicata mensilmente. Una parola che porta un significato giuridico è usata per denominare un'opzione di storage.

In **161 pagine** di documenti contrattuali e operativi non compaiono né i termini (*CLOUD Act*, *extraterritoriale*, *nazionalità*, *controllo societario*, *paese terzo*, *immunità*) né le **clausole sostanziali di salvaguardia**: *articolo 48 GDPR*, *autorità giurisdizionale estera*, *ordine di un paese terzo*, *trasferimenti internazionali*, *assistenza giudiziaria* — tutte a **zero**. Non è una questione di gergo giuridico italiano: le salvaguardie mancano anche nella sostanza.

L'Italia ha applicato **il controllo societario dove la sua legge arriva** — golden power e consenso a ogni variazione di capitale, sul concessionario italiano. Lo strumento che raggiunge il **fornitore della tecnologia** non è il golden power, che non può: è il **requisito di gara** — e quello non è mai stato scritto.

Le misure tecniche su cui si fa affidamento — cifratura con chiavi esterne e confidential computing — sono dichiarate insufficienti proprio a questo scopo dall'**agenzia francese che ha scritto lo standard europeo di sovranità**.

Nessuno dei quattro fornitori usati possiede una qualificazione di sovranità. Nel catalogo ufficiale francese, **Microsoft, Google, Amazon e Oracle compaiono zero volte**.

Ciò che ne discende non è un rimedio tecnico. Le misure sono efficaci contro gli avversari per cui sono state progettate, e nessuna misura può essere progettata contro un ordine giuridico notificato al fornitore. La variabile che cambia la risposta è **dove il fornitore è stabilito, chi ne controlla il capitale, e da dove il servizio è amministrato** — e quella variabile si fissa scrivendo un requisito, non comprando una funzionalità. La Francia l'ha scritto. L'Italia lo ha co-firmato a Bruxelles nel 2021, l'ha perso nel 2024, e in casa propria non l'ha mai scritto.

Ogni affermazione qui sopra è documentata più avanti, con il rimando alla fonte primaria e, dove la fonte è un file, una copia archiviata. Chi vuole controllare invece di credere cominci da come verificare questa analisi.

La difesa più forte del programma, e perché non regge

Messo di fronte alla questione della sovranità, il programma cloud pubblico italiano risponde con **due misure tecniche**, e sono quelle che mette avanti per prime. Vale la pena enunciarle nella loro versione più forte, perché entrambe sono reali.

1. Le chiavi tenute dal Polo stesso

Chiavi di cifratura *«create e gestite dall'infrastruttura Thales presente on-premises nei datacenter del PSN, **escludendo così, dalla gestione delle chiavi di cifratura, il CSP**»*; e, sul livello managed, *«**il controllo della Root Key**»* della region.

2. Il confidential computing

*«Il confidential computing, **ove attivato**, rende impossibile agli operatori del cloud service provider di accedere anche al dato **durante l'elaborazione**.»*

Fonte: Manuale Utente Secure Public Cloud Azure, ed. 04/04/2025 (PDF, 64 pp.)
[https://www.polostrategiconazionale.it/app/uploads/2025/04/PSN-Manuale-Utente-SPC-Azure.pdf] · pagina servizi con Cloud Service Provider
[https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/]

Prese insieme, queste due sarebbero una risposta seria: le chiavi sono fuori dalle mani del fornitore, e il dato è illeggibile perfino mentre viene elaborato. **Se reggesse, la questione giurisdizionale si dissolverebbe in larga parte.**

L'agenzia nazionale francese per la cybersicurezza ha pubblicato il **17 ottobre 2025** un documento di posizione tecnica sul confidential computing. È la stessa agenzia che ha redatto la **sezione 19.6 di SecNumCloud** — la clausola che impone l'immunità dalle leggi extraterritoriali non europee. Quattro frasi di quel documento liquidano entrambe le misure.

*«Il Confidential Computing **non è abbastanza sicuro da proteggere l'integrità e la riservatezza dei dati contro un amministratore ostile che compia attacchi mirati e attivi**.»*

*«Il Confidential Computing **non è sufficiente, da solo**… **a soddisfare i requisiti descritti nella sezione 19.6 del referenziale SecNumCloud 3.2**.»*

*«Si noti che **gli approcci 'Bring Your Own Key' (BYOK) non risolvono il problema, perché il fornitore cloud deve comunque essere considerato affidabile per usare le chiavi fornite dall'utente**.»*

*«**Non fare affidamento sul Confidential Computing se il fornitore cloud è considerato non affidabile o potenzialmente ostile**… passare a un fornitore affidabile… **è un prerequisito**.»*

Fonte: ANSSI, *Technical Position Paper on Confidential Computing* v1.0, 17.10.2025 (PDF, 13 pp.) [https://cyber.gouv.fr/sites/default/files/document/anssi-technical-position-paper-coco-v1.0.pdf] · e il referenziale SecNumCloud 3.2 [https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf], la cui sezione 19.6 è citata

Le due misure su cui il programma fa affidamento sono, nelle parole dell'autorità che ha definito lo standard, **le due misure che non lo soddisfano**. E l'ordine dei fattori è rovesciato: un fornitore affidabile non è un'alternativa alla tecnologia — è **la precondizione senza la quale sulla tecnologia non ci si dovrebbe affidare affatto**.

E un dettaglio dai documenti del programma stesso. Il confidential computing è promosso sulla pagina commerciale con la riserva *«ove attivato»*. Nel **manuale utente di 64 pagine** del servizio su cui viene promosso, il termine *confidential computing* compare **zero volte**. Non sosteniamo che non sia disponibile — constatiamo che il manuale operativo del servizio non lo documenta, mentre la pagina di vendita lo rende condizionale. **E la condizione non è nelle mani del cliente.**

Le ragioni tecniche che stanno dietro a queste quattro frasi — perché un dato debba essere in chiaro per essere elaborato, perché la custodia esterna delle chiavi non possa impedirne l'uso imposto, e perché l'attestazione verifichi il software e non il luogo — sono esposte nella Parte II. Chi accetta le quattro citazioni può andare direttamente alla tabella delle cinque offerte.

Che cos'è il Polo Strategico Nazionale, e che cosa promette

Il **Polo Strategico Nazionale** è l'infrastruttura su cui le amministrazioni pubbliche italiane stanno spostando i propri sistemi, finanziata con i fondi europei per la ripresa. Esiste per portare in poche strutture presidiate i server sparsi in migliaia di enti pubblici.

Il consolidamento è un guadagno reale, e va detto per primo. Concentrare migliaia di sale server sparse e disomogeneamente manutenute in pochi data center presidiati migliora la sicurezza fisica, la continuità e la gestione — *qualunque software ci giri sopra*. Chi attacca questo programma ignorandolo perde il confronto nei primi trenta secondi, e merita di perderlo.

Ma il programma non è presentato solo come consolidamento. Le sue stesse pagine promettono che le amministrazioni accederanno ai servizi *«in piena sicurezza, **autonomia e sovranità**»*. Questa pagina esamina quella seconda parola — perché è quella che porta un significato giuridico, e perché nei documenti del programma stesso risulta significare altro.

*«Il primo requisito è legato alla **sovranità del dato**… la replica del dato su storage del PSN ha **frequenza mensile** e ne viene mantenuta solo una versione.»*

Fonte: Manuale Utente Secure Public Cloud Azure, ed. 04/04/2025, sezione sul servizio di backup
[https://www.polostrategiconazionale.it/app/uploads/2025/04/PSN-Manuale-Utente-SPC-Azure.pdf]

Letto con precisione, questo non è una definizione di sovranità — ed è proprio questo il punto. Il passaggio si trova nella sezione che descrive il servizio di backup, e afferma che uno dei due requisiti di quel servizio è *«legato alla sovranità del dato»*, soddisfatto da una replica mensile. Chi obiettasse che si tratta semplicemente di un obiettivo di punto di ripristino **avrebbe ragione sul meccanismo**.

Il reperto non è che un backup mensile sia una forma povera di sovranità. È che **«sovranità del dato» è il nome formale dato, nella documentazione operativa, a una misura di storage** — e che questo è **l'unico punto, nei documenti che abbiamo letto, in cui il termine viene attaccato a qualcosa di concreto**. Una parola che nel diritto europeo indica una condizione giurisdizionale svolge qui il lavoro di una politica di conservazione. Non è una carenza tecnica: è una carenza semantica, ed è ciò che rende necessario il resto di questa pagina.

Sul cloud pubblico italiano **numerose misure tecniche sono state realmente attivate**: dati cifrati a riposo, chiavi custodite in moduli hardware fuori dal perimetro del fornitore, segregazione di rete, region italiane, separazione operativa, confidential computing ove attivato.

Nessuna di esse è in grado di difendere da un attore statuale che possa obbligare il fornitore cloud con un ordine giuridico. Non è un'ipotesi: è la situazione creata dal **CLOUD Act** statunitense e dalla **Sezione 702 del FISA** nei confronti di Microsoft, Google e Amazon. E la ragione non è che quelle misure siano fatte male. È che **sono tutte misure contro un attaccante — e un ordine giuridico non è un attacco**.

La **Parte I** risponde alla domanda direttamente, con i documenti. La **Parte II** spiega le ragioni tecniche che stanno sotto — si può leggere per conto proprio, ed è ciò su cui la risposta poggia.

La difesa più forte del programma, e perché non regge — chiavi e confidential computing, a cui risponde l'agenzia che ha scritto lo standard.

Come verificare questa analisi — convenzioni, scansioni riproducibili, fonti archiviate.

PARTE I — Perché il PSN non garantisce la sovranità digitale

Perché questo riguarda l'Italia: che cosa dicono i documenti

«PSN Managed» sono due architetture diverse

Le cinque offerte, una accanto all'altra — la tabella principale

Requisito per requisito, contro lo standard francese

Perché la Francia è avanti — e non per la ragione che si dice

Oracle Alloy, con le parole di Oracle

Amazon: Nitro Enclaves, e dov'è davvero il confine

Chi ha una qualificazione di sovranità, e chi no

I quattro fornitori, e il punto in cui coincidono

PARTE II — Le misure tecniche, e perché non bastano

Un dato esiste in tre stati. La cifratura ne copre due.

Che cos'è il confidential computing, e che cosa ottiene

Quattro ragioni per cui non produce sovranità

E le chiavi? Lo stesso problema, un piano più sotto

Perché una misura tecnica non può risolvere un problema giuridico

Le obiezioni, una per una

Sette scenari, graduati

Le migliori argomentazioni a favore del programma

Che cosa si potrebbe fare — sei misure

La conclusione, detta con cura

Come verificare questa analisi

Questa pagina è scritta per essere **controllata, non creduta**. Ogni citazione proviene da un documento che abbiamo scaricato e letto per intero, non da resoconti di seconda mano. Chi lavora in sicurezza o infrastrutture deve poter riprodurre ogni reperto in autonomia, e questa sezione spiega come.

Le tre convenzioni che usiamo, e che cosa significano

Formula	Che cosa afferma — esattamente
«zero occorrenze»	È stata eseguita una ricerca full-text sui documenti indicati e non ha restituito nulla. L'insieme dei documenti e i termini cercati sono sempre dichiarati, così la ricerca si può ripetere.
«non documentato»	Abbiamo letto il documento e non l'abbiamo trovato. **Non** è l'affermazione che la cosa non esista — solo che la fonte non la dichiara.
«non trovato»	Abbiamo cercato un documento o una dichiarazione e non siamo riusciti a individuarla. È la più debole delle tre, e viene sempre segnalata come tale.

Riprodurre le due scansioni

I due reperti quantitativi di questa pagina sono ricerche full-text, ed entrambe si possono rifare in pochi minuti.

1. **Le 161 pagine.** Si scarichino i quattro documenti collegati nella sezione 1 — convenzione di concessione, guida alla convenzione, caratteristiche tecniche dei servizi e manuale utente del livello su Azure — se ne estragga il testo e si cerchino: CLOUD Act, extraterritoriale, nazionalità, capogruppo, paese terzo, controllo societario, immunità, legge straniera. **Una trappola di metodo in cui siamo caduti, e in cui cadrete anche voi.** Lo strato testuale della guida alla convenzione si estrae *senza spazi*: una ricerca ingenua di software di base restituisce zero, falsamente. Si normalizzino via gli spazi bianchi dal testo estratto prima di cercare, altrimenti si riportano assenze che non esistono.
2. **Il catalogo francese.** Si scarichi il catalogo ufficiale dei prodotti e servizi qualificati collegato nella sezione 8 e vi si cerchino Oracle, Microsoft, Amazon, AWS, Polo Strategico.

Lo standard probatorio che applichiamo a noi stessi

Queste dodici regole governano ciò che su questa pagina si può e non si può concludere. Sono pubblicate perché un lettore possa controllare se le abbiamo rispettate.

1. Una pagina commerciale non dimostra una proprietà tecnica se non è accompagnata da specifiche, da un audit o da una clausola contrattuale.
2. Un documento generico del fornitore non dimostra l'implementazione concreta dentro questo programma.
3. **L'assenza di una parola non dimostra l'assenza di una regola.**
4. La presenza di una connessione o di una dipendenza non dimostra l'accesso ai contenuti.
5. La capacità di aggiornare il software è rilevante, ma è cosa distinta dalla capacità attuale di leggere i dati.
6. Una qualificazione non è una garanzia assoluta e va descritta nel suo perimetro.
7. **«Non documentato» non equivale a «inesistente».**
8. **«Mitigato» non equivale a «eliminato».**
9. «Tecnicamente possibile» non equivale né a «giuridicamente autorizzato» né a «effettivamente avvenuto».
10. «Giuridicamente ordinabile» non equivale a «tecnicamente eseguibile senza ulteriori modifiche».
11. Ogni affermazione temporale deve portare la propria data.
12. Ogni confronto deve dichiarare se gli oggetti confrontati siano realmente comparabili.

Due conseguenze che accettiamo. Primo: *«zero occorrenze»* significa esattamente e soltanto **«nessuna corrispondenza lessicale in questo corpus, con queste interrogazioni e questi limiti»** — non l'assenza del rischio, della regola o della discussione. Secondo: abbiamo **privilegiato** fonti primarie normative, contrattuali, tecniche e scientifiche; dove compare una fonte giornalistica è usata **per contesto o come strada verso il documento originale**, mai come prova.

Registro delle fonti — file, dimensioni e impronte

Ogni file qui sotto è archiviato nel repository del progetto. L'impronta SHA-256 consente a chiunque di verificare di stare esaminando **lo stesso documento che abbiamo esaminato noi**, e non una revisione successiva.

Documento	Dimensione	SHA-256
Convenzione di concessione Polo Strategico Nazionale · DTD	53 pp 172 KB	ae3e3b0f2a97a91e38cd9e9ca71b2ac07d42a5405fcf7ba7a93dd231d062e0bb
Guida alla Convenzione Polo Strategico Nazionale · 08/2025	11 pp 199 KB	8b7e7ef454cb4679a8737e77c441a72836b240332e5d49f090b25e75e54575f6
Caratteristiche tecniche dei Servizi Polo Strategico Nazionale · 08/2025	33 pp 1060 KB	b839c349eb8b4a3a0c2be4b0da758eeaade0834b62c7354e708d4cd57104c4c1
Manuale Utente Secure Public Cloud Azure Polo Strategico Nazionale · ed. 04/04/2025	64 pp 3155 KB	bba442bd4a5afa8fc1d247d3619c83451ccb2da8ceb8a85aceb4941b370c09ab
Presentazione servizi a listino Polo Strategico Nazionale · 04/2026	121 pp 9783 KB	70344b74f2eab896aeba2e26622ba0858f30fd17ef00f99b2c20291eca7461ef
Deck istituzionale v12 Polo Strategico Nazionale · 10/2025	109 pp 8754 KB	c386b4ad00f8461e30b636480e003494d01763be7d449fe261b2ad82ff9f1a9a

Documento	Dimensione	SHA-256
Technical Position Paper on Confidential Computing ANSSI · v1.0, 17/10/2025	13 pp 309 KB	12b17100973fc205937866405dc243b453fa6b6f1ad99323fa58eb1e4e7eb128
Catalogue produits et services qualifiés ANSSI · 2026	130 pp 3597 KB	5a4bb87cf9216ae3251f35227a447563aa8b783c2298a83134bbf3f8843a69d4
Elenco dei soci — AWS European Sovereign Cloud GmbH Registro delle imprese, Potsdam · HRB 40853 P · autenticato 20.10.2025	3 pp 87 KB	69c7ef33bcad326426e40b5c9121ec4bd97bec63fbda7857e279e16ba179d55f

Le **«161 pagine»** citate in tutta la pagina sono i quattro documenti contrattuali e operativi: **53 + 11 + 33 + 64**. Gli altri file del registro sostengono reperti specifici e sono citati dove vengono usati.

Documenti che non abbiamo letto, e che cosa cambierebbero

Il corpus esaminato è contrattuale e operativo. **Non** comprende i documenti di strategia cloud nazionale, che risultano riconoscere il rischio derivante da ordinamenti extra-UE. Quel riconoscimento non è in discussione qui, e questa pagina non sostiene che la domanda non sia mai stata posta in Italia — al contrario, l'Italia è coautrice dei criteri europei di immunità nel 2021.

La distinzione su cui questa pagina si regge. Riconoscere un rischio in un documento di strategia non è la stessa cosa che tradurlo in **requisiti vincolanti, criteri di esclusione, clausole contrattuali, verifiche tecniche o conseguenze in caso di inadempimento**. Il nostro reperto è limitato al corpus del registro qui sopra: **in quei documenti nessun requisito del genere è stato trovato**. Leggere i documenti di strategia affinerebbe il quadro delle intenzioni; non cambierebbe di per sé ciò che i contratti contengono.

Dove sono conservate le fonti

Le pagine commerciali cambiano e i PDF vengono ritirati. Ogni file citato qui è stato **archiviato nel repository del progetto**, perché la prova non dipenda dalla permanenza in rete dei siti dei fornitori. I collegamenti puntano all'originale; la copia archiviata è la riserva.

Chi scrive, e a che titolo. Questo Osservatorio è un **progetto indipendente**. **Non è un ente pubblico, non è un'autorità e non è un'agenzia**, e nulla di quanto scritto qui ha valore istituzionale: l'analisi vale esattamente quanto valgono le sue fonti, ed è per questo che sono elencate tutte con le rispettive impronte. Il nome descrive l'ampiezza della materia esaminata, non un mandato pubblico.

E un punto di coerenza che dobbiamo al lettore. Un sito che critica la dipendenza da infrastrutture non europee mentre carica i propri caratteri, fogli di stile e icone da server di terze parti argomenterebbe contro sé stesso. **Questa pagina non richiede nulla ad alcun soggetto terzo.** Carattere tipografico, foglio di stile, script e icone sono serviti da questo dominio: nessun indirizzo IP di chi legge parte verso un server fuori dal nostro controllo per leggere questa analisi. Si verifica in trenta secondi con il pannello di rete del browser — e vi invitiamo a farlo.

Questa analisi è per costruzione esposta alla contestazione: è fatta per essere attaccata. Se una citazione è inesatta, un documento è stato superato o una lettura tecnica è sbagliata, **vogliamo saperlo e correggeremo pubblicamente**. Diversi reperti di questa pagina esistono perché una versione precedente del nostro stesso ragionamento era sbagliata ed è stata corretta. È lo standard che applichiamo a noi stessi, e invitiamo allo stesso esame chiunque lavori professionalmente con questi sistemi.

Parte I

1. Perché questo riguarda l'Italia: il Polo Strategico Nazionale

Il programma cloud pubblico italiano — il Polo Strategico Nazionale, PSN — offre esattamente queste due misure come propria protezione, sul livello erogato dalle region pubbliche degli hyperscaler.

Che cosa dicono i documenti PSN	Che cosa ne consegue da questa pagina
Gestione delle chiavi *«create e gestite dall'infrastruttura Thales presente on-premises nei datacenter del PSN, escludendo così, dalla gestione delle chiavi di cifratura, il CSP»*	Reale e utile per il dato a riposo. Non risponde al dato in uso — si veda la sezione 13.
Il confidential computing *«ove attivato»* rende *«impossibile agli operatori del cloud service provider di accedere anche al dato durante l'elaborazione»* (pagina commerciale)	L'ANSSI afferma che questa tecnica non soddisfa SecNumCloud 19.6 e non protegge da un amministratore ostile. E la condizione — *ove attivato* — la decide chi gestisce il servizio.
Nel manuale utente di 64 pagine del livello su Azure, pubblicato in aprile 2025, il termine *confidential computing* compare **zero volte**.	Non sosteniamo che non sia disponibile. Constatiamo che il manuale utente del servizio non lo documenta, mentre la pagina commerciale lo qualifica con *ove attivato*.
In 161 pagine di documenti contrattuali e operativi del PSN, questi termini compaiono **zero volte**: CLOUD Act, extraterritoriale, nazionalità, capogruppo, paese terzo, controllo societario, immunità, legge straniera.	La questione giurisdizionale non riceve una risposta tecnica debole. **Non viene posta.**

2. «PSN Managed» sono due architetture diverse sotto un nome solo

Il livello più protetto del cloud pubblico italiano è presentato come un servizio unico. La sua stessa pagina dice altro, in una frase:

> *«Il servizio si basa su **due tecnologie: Google Assured Workload e Oracle Alloy**.» — «Queste infrastrutture sono ospitate in **region italiane oppure all'interno dei Data Center del Polo Strategico Nazionale**.»*

*«Il servizio si basa su **due tecnologie: Google Assured Workload e Oracle Alloy**.» — «Queste infrastrutture sono ospitate in **region italiane oppure all'interno dei Data Center del Polo Strategico Nazionale**.»*

Fonte: PSN, *PSN Managed Public Cloud* [https://www.polostrategiconazionale.it/en/solutions/cloud-services-with-csp/psn-managed-public-cloud/] · listino servizi, 04/2026 [https://www.polostrategiconazionale.it/app/uploads/2026/04/Presentazione-servizi-a-listino-Polo-Strategico-Nazionale.pdf] · Guida alla Convenzione, 08/2025 [https://www.polostrategiconazionale.it/app/uploads/2025/08/PSN_Guida-alla-Convenzione_.pdf]

Quell'**«oppure»** regge tutto il peso. Non sono due fornitori dentro un'architettura: sono **due architetture opposte**, e una sola delle due sta dentro i data center del PSN.

	Lato Google	Lato Oracle
Tecnologia	Assured Workloads	Oracle Alloy
Dove gira	Region italiane **di Google** — Milano europe-west8, Torino europe-west12	Dentro i Data Center del PSN
Che cos'è	Uno **strato di policy** su cloud pubblico	Un **realm separato**, hardware proprio

Il listino del PSN conferma entrambe le metà: sul versante Google riporta una voce di listino chiamata *«Sovereign Controls»*, descritta come la possibilità di *«impostare delle policy all'interno di GCP»*. **La sovranità come voce di listino, e come impostazione di policy.**

3. Le cinque offerte, una accanto all'altra

La prima colonna è il metro: l'unica delle cinque che possiede una qualificazione di sovranità. Tutto ciò che le sta a destra non ce l'ha.

	■■ PREMI3NS (riferimento)	■■ France Data Boundary	■■ PSN Managed — Google	■■ PSN Managed — Oracle Alloy	■■ Secure Public Cloud Oracle
Dove girano i dati	Data center S3NS	Region Google	Region Google — Milano, Torino	Data center PSN	**Region pubblica Oracle**
Natura	Infrastruttura separata	Policy su cloud pubblico	Policy su cloud pubblico	Realm dedicato	Cloud pubblico
Chi opera i servizi	**Solo personale S3NS**	Google	Google	**Oracle** — «secure service operations»	Oracle
Aggiornamenti software	**Messi in quarantena, analizzati e validati da S3NS** prima del rilascio	Google	Google	Li produce Oracle; il PSN applica il patching standard; **Oracle esegue gli upgrade non standard**	Oracle

	■■ PREMI3NS (riferimento)	■■ France Data Boundary	■■ PSN Managed — Google	■■ PSN Managed — Oracle Alloy	■■ Secure Public Cloud Oracle
Controllo sugli aggiornamenti	**Approvazione**	—	—	**Solo visibilità** — una dashboard che elenca modifiche di emergenza, mitiganti, normali e di routine	—
Accesso del fornitore	«Il personale Google non ha accesso»	Split boundaries accessibili al personale Google	Identico	*Operator Access Control* — **ma non copre l'automazione root**	Standard OCI
Qualificazione di sovranità	**Sì — SecNumCloud 3.2**	No	No	No	No

Fonte: Google, *Italy Data Boundary by PSN* [https://docs.cloud.google.com/sovereign-controls-by-partners/docs/data-boundaries/italy-data-boundary-psn] · France Data Boundary by S3NS [https://docs.cloud.google.com/sovereign-controls-by-partners/docs/data-boundaries/france-data-boundary-s3ns] · listino PSN 04/2026 [https://www.polostrategiconazionale.it/app/uploads/2026/04/Presentazione-servizi-a-listino-Polo-Strategico-Nazionale.pdf]

Il listino del PSN introduce un ulteriore servizio, il *Secure Public Cloud Oracle*, con queste parole:

*«Disponibilità di servizi **non erogabili tramite tecnologia Alloy o non implementabili nei Data Center PSN**, grazie all'**utilizzo diretto della region pubblica Oracle**.» — «**Superamento dei limiti** Public Cloud PSN managed (Alloy): **Exadata di nuova generazione (X9M, X11M)**, nuove classi compute, Object Storage avanzato.»*

Per avere l'Exadata moderno si **esce dai data center PSN e si va nella region pubblica Oracle**. Il perimetro «sovrano» non è dove stanno i servizi migliori: è dove stanno quelli che Alloy riesce a erogare. E la mitigazione è di nuovo condizionale — *«utilizzo del modello BYOK **ove applicabile**»*.

4. Il confronto, requisito per requisito

Il cloud pubblico italiano è erogato in **tre livelli**, con tre gradi di controllo molto diversi — tutti promossi con la stessa parola. Questa tabella li mette a confronto con i requisiti che il quadro francese misura davvero. Ogni casella sul PSN viene da documenti scaricati e letti per intero: la convenzione di concessione, la guida alla convenzione, le caratteristiche tecniche dei servizi e il manuale utente del livello su Azure — 161 pagine.

Requisito	SecNumCloud 3.2 §19.6	PSN Managed Google — Assured Workloads	PSN Managed Oracle Alloy	Hybrid on PSN site	Secure Public Cloud
Sede del fornitore nell'UE	**Richiesto**	**Non richiesto in alcun punto.** Il termine non compare come requisito sui fornitori in nessuna delle 161 pagine.			
Controllo del capitale — tetto alla quota extra-UE	**Richiesto**, tetto al 24%	**Non richiesto.** Zero occorrenze di *nazionalità*, *capogruppo*, *controllo societario*, *paese terzo*. **Non perché lo strumento mancasse.** Golden power e consenso a ogni variazione di capitale ci sono — *sul concessionario italiano*, che è dove la legge italiana arriva. Lo strumento che raggiunge il **fornitore** è il requisito di gara, come nel referenziale francese. Non è stato scritto.			

Requisito	SecNumCloud 3.2 §19.6	PSN Managed Google — Assured Workloads	PSN Managed Oracle Alloy	Hybrid on PSN site	Secure Public Cloud
Amministrazione del servizio dall'UE	**Richiesto**	**No.** Gira sulle region italiane di Google (europe-west8, europe-west12); opera Google.	**In parte — ed è reale.** Hosting nei data center PSN, *«gestiti da personale PSN»*. Ma Oracle fornisce le *«operazioni di servizio sicure»* e il ciclo di vita del prodotto.	**No.** *«Un control plane unico con Microsoft Azure Arc»*.	**No.** Erogato dalle *region pubbliche* degli hyperscaler.
Immunità dichiarata dalle leggi extraterritoriali non UE	**È l'intera ragion d'essere del §19.6**	**Zero occorrenze in 161 pagine** di: CLOUD Act, extraterritoriale, immunità, legge straniera, autorità straniera, extra-UE. Le due occorrenze di *giurisdizione* riguardano il contenzioso sul concessionario, non i dati. **La domanda non riceve una risposta debole. Non viene posta.**			
Titolarità delle chiavi di cifratura	Necessaria ma, secondo l'agenzia francese, **non sufficiente**	CMEK obbligatoria su 23 servizi; Cloud EKM disponibile.	*«Il controllo della Root Key»*; gestione centralizzata tramite KMS/HSM del PSN. Reale.	Non documentato per questo livello.	BYOK su HSM Thales on-premises, *«escludendo il CSP dalla gestione delle chiavi»*. Reale — e l'agenzia francese afferma che il BYOK *«non risolve il problema»*.
Protezione del dato in uso	Il confidential computing **non soddisfa il §19.6**	Non documentato. Google dichiara che il perimetro *«non fornisce controlli di residenza per i dati in uso»*.	Non documentato.	Non documentato.	Promosso *«ove attivato»* sulla pagina commerciale. **Zero occorrenze nel manuale utente di 64 pagine.**
Come viene definita la «sovranità»	Una **condizione giuridica**: sede, capitale, amministrazione.	**Il termine è usato ma mai definito** per questi livelli, nei documenti che abbiamo letto.	**Una copia di backup mensile.** Manuale utente, verbatim: *«il primo requisito è legato alla **sovranità del dato**… la replica del dato su storage del PSN ha **frequenza mensile** e ne viene mantenuta solo una versione»*.		
Il requisito è scritto in un atto vincolante?	**Sì.** Un referenziale di qualificazione con effetti giuridici per i dati sensibili dello Stato.	**Nessun requisito del genere esiste nella normativa italiana né nel contratto PSN.** Non c'è quindi nulla a cui conformarsi, nulla da misurare, e nessun terreno su cui un fornitore possa risultare inadempiente.			

Fonte: Convenzione di concessione [https://www.polostrategiconazionale.it/app/uploads/2023/03/PSN-Concessione-Convenzione.pdf] · Guida alla Convenzione [https://www.polostrategiconazionale.it/app/uploads/2025/08/PSN_Guida-alla-Convenzione_.pdf] · Manuale Utente SPC Azure [https://www.polostrategiconazionale.it/app/uploads/2025/04/PSN-Manuale-Utente-SPC-Azure.pdf] · impronte nel registro delle fonti

Perché «PSN Managed» occupa due colonne. Come stabilito nella sezione 2, quel servizio è composto da due architetture diverse: sul lato Google uno strato di policy sulle region di Google, sul lato Oracle un realm dedicato dentro i data center del PSN. Comprimerle in una colonna sola nasconderebbe l'unico livello in cui il requisito di amministrazione è in parte soddisfatto — e attribuirebbe al lato Google una proprietà che non ha. **In questa pagina restano sempre distinte.**

Sul metodo. Dove una casella dice *«non documentato»* intendiamo esattamente questo: abbiamo letto i documenti e non l'abbiamo trovato — che è cosa diversa dall'affermare che non esista. Dove una casella dice *«zero occorrenze»*, abbiamo eseguito una ricerca full-text su tutti e quattro i documenti e ne riportiamo l'esito. La distinzione è voluta.

5. Perché la Francia è avanti — e non per la ragione che si dice

Prima, l'affermazione che *non* facciamo. Sarebbe facile, e sbagliato, dire «i cloud francesi sono sovrani e quelli italiani no». La Francia ha **Bleu**, costruito su tecnologia Microsoft, e **S3NS**, costruito su tecnologia Google. Chiunque può indicare quei due nomi e l'argomento crolla. Perciò non lo facciamo.

La differenza vera non sta nella purezza dei fornitori. Sta nel fatto che **la Francia ha scritto un requisito che si può misurare, e l'Italia non ne ha scritto alcuno**. Tre verifiche, ciascuna delle quali o è soddisfatta o non lo è: dove è stabilita l'azienda, chi ne controlla il capitale, da dove il servizio è amministrato.

Bleu e S3NS **esistono perché la regola esiste**. Nessuna azienda americana si è ristrutturata per benevolenza: lo ha fatto perché altrimenti non poteva vendere allo Stato francese. Tecnologia americana, in licenza; un operatore europeo; capitale extra-UE con tetto al 24%. S3NS ha ottenuto la qualificazione ANSSI il **17 dicembre 2025**. **Un fatto scomodo per la nostra tesi si rivela la prova che la regola funziona.**

In Francia un fornitore americano **ha dovuto cambiare struttura societaria** per poter vendere allo Stato.
In Italia **non gli è stato chiesto di cambiare nulla**.

È tutto qui il divario, e non è un divario di tecnologia, di bilancio o di competenza ingegneristica. L'Italia ha ottimi data center, operatori capaci e un vero programma di consolidamento. Ciò che non ha è **una frase in un documento vincolante** che dica che cosa un fornitore debba essere per custodire i dati più sensibili dello Stato. La Francia quella frase l'ha scritta. Scriverla non è costato nulla. Ha cambiato il mercato.

E c'è un dettaglio che rende il confronto ancora più netto. Non è che l'Italia non ci abbia pensato. **Nel 2021 l'Italia è coautrice, con Francia, Germania e Spagna, della proposta europea che introduceva l'immunità dalle leggi straniere nella certificazione cloud dell'Unione.** Quei requisiti sono stati rimossi nel marzo 2024. L'Italia ha chiesto la regola a Bruxelles — e negli stessi cinque anni non l'ha mai scritta in casa propria, nell'unico strumento che non dipendeva dal voto di nessun altro.

6. Oracle Alloy, con le parole di Oracle

Prima, ciò che va riconosciuto. Alloy è davvero un realm separato, con *«un proprio control plane»*, *«fisicamente e logicamente separato»* dal cloud pubblico Oracle. Il PSN dichiara due region, rete esclusiva senza internet pubblico, tutti i dati nei propri data center, cifratura secondo le specifiche dell'autorità nazionale. **Sul piano dell'infrastruttura è più di quanto offra il Data Boundary di Google.**

*«Oracle Alloy combina una **cloud foundation gestita da Oracle** con uno strato di business e customer experience gestito dall'operatore. **Oracle fornisce la piattaforma cloud, le operazioni di servizio sicure e la gestione continua del ciclo di vita del prodotto.** L'operatore fornisce **l'ambiente di hosting** ed esercita il business cloud rivolto al cliente su quella fondazione.»*

L'operatore mette il palazzo e il rapporto commerciale. **Le operazioni di servizio sono di Oracle.**

E il lessico che Oracle usa per il partner non lascia dubbi: l'operatore *«**rivende** servizi cloud Oracle»* e gestisce *«il ciclo di vita del proprio **business di rivendita cloud**»*. Un dettaglio che dice molto: il post Oracle intitolato *«Expanding Control & Flexibility»* per gli operatori Alloy riguarda **valute multiple e rinnovi contrattuali**. Il controllo che viene

ampliato è commerciale.

Fonte: Oracle, *Alloy Overview* [https://docs.oracle.com/en-us/iaas/Content/dedicated/alloy/oracle-alloy-overview.htm] · oracle.com/cloud/alloy [https://www.oracle.com/cloud/alloy/] · Alloy Business Reporting [https://docs.oracle.com/en-us/iaas/Content/dedicated/alloy/alloy-business-reporting.htm]

Aggiornamenti: chi fa che cosa, detto con precisione

La pagina prodotto Oracle dice che l'operatore *«può gestire in autonomia **tutte le attività operative standard, come il patching di base e gli aggiornamenti dei servizi**»*, e può contare sui *«team Oracle per troubleshooting, **upgrade non standard**, risoluzione dei disservizi ed escalation»*. Il VP Dedicated Cloud di Oracle lo sintetizza: è *«di fatto un'intera region OCI che il team dell'operatore può gestire, mantenere e potenziare in autonomia, **assistito dagli upgrade e dal supporto di Oracle**»*.

E ciò che l'operatore ottiene sulle modifiche è una dashboard che *«fornisce **visibilità** sui cambiamenti di servizio OCI schedulati e completati, inclusi quelli **di emergenza**, mitiganti, normali e di routine»*. I verbi sono osservativi dall'inizio alla fine. **Nessuna approvazione, nessun rifiuto, nessun differimento risulta documentato.**

Operator Access Control — reale, e con tre buchi dichiarati

Oracle offre un meccanismo davvero più forte di qualunque cosa ci sia nel pacchetto Google: il cliente **può approvare o negare l'accesso dei dipendenti Oracle**, con limiti di tempo, registrazione di tutti i comandi e, se richiesto, dei tasti premuti. Va riconosciuto.

Le tre esclusioni, con le parole di Oracle:

*«non controlla le **azioni di automazione**, incluse quelle eseguite come **root**, o da altri utenti di automazione ad alto privilegio, compreso l'**accesso di automazione basato su proxy**»*

*«non offre controlli su entità esterne di Oracle Cloud Infrastructure, come gli switch, **o altro software del control plane**»*

*«è una soluzione progettata per l'audit e la conformità dell'accesso Oracle, **non una soluzione di conformità generale**»*

Fonte: Oracle, *Operator Access Control* — overview [https://docs.oracle.com/en-us/iaas/operator-access-control/doc/overview-of-operator-access-control.html]

Il cancello controlla le persone. Non controlla l'automazione che gira come root.

Due riserve oneste. L'Operator Access Control è documentato per Exadata Cloud@Customer e Compute Cloud@Customer, non per Alloy nel suo insieme — il PSN usa Exadata sulla piattaforma Alloy, quindi è pertinente, ma non sosteniamo che copra tutto. E l'affermazione più forte di Oracle — *«un operatore Oracle Alloy mantiene il pieno controllo dei dati e delle applicazioni»* — è una **dichiarazione aziendale che non abbiamo potuto verificare**, della stessa natura del «non è mai successo» di Microsoft.

7. Amazon: Nitro Enclaves, e dov'è davvero il confine

Amazon è il **quarto fornitore cloud** integrato nel cloud pubblico italiano: il listino del PSN registra l'*«integrazione 4° cloud service provider AWS»* nel 2024, e descrive il *Secure Public Cloud* come basato sui servizi pubblici *«degli hyperscaler Microsoft Azure, Google Cloud, AWS e Oracle, con region in territorio italiano»*. La domanda vale quindi anche qui.

Da che cosa protegge Nitro Enclaves — nella documentazione di AWS

Nitro Enclaves è una tecnologia di isolamento davvero ben costruita. Il suo modello di minaccia documentato è enunciato con precisione, e vale la pena leggerlo due volte:

> *«i dati e le applicazioni dentro l'enclave non possono essere acceduti da processi, applicazioni o utenti (**root o admin**) **dell'istanza padre**» — «Il Nitro Hypervisor garantisce che **l'istanza padre** non abbia accesso alle vCPU e alla memoria isolate dell'enclave.»*

*«i dati e le applicazioni dentro l'enclave non possono essere acceduti da processi, applicazioni o utenti (**root o admin**) **dell'istanza padre**» — «Il Nitro Hypervisor garantisce che **l'istanza padre** non abbia accesso alle vCPU e alla memoria isolate dell'enclave.»*

Il soggetto escluso dall'enclave è **l'istanza del cliente stesso** — il proprio root, il proprio amministratore, il proprio codice compromesso. **AWS non è nominata.** È una difesa contro sé stessi, ed è una buona difesa. Non è quella di cui parla il dibattito sulla sovranità.

Due dettagli ulteriori, dalla stessa pagina. La vita dell'enclave è legata all'istanza: *«Le enclave sono attive solo mentre l'istanza padre è in stato running. Se l'istanza padre viene **arrestata o terminata**, le sue enclave sono terminate.»* Chi controlla l'hypervisor controlla l'interruttore. E l'attestazione è integrata con **AWS KMS** — il servizio di chiavi gestito da AWS.

Fonte: AWS, *What is Nitro Enclaves?* [https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html] · European digital sovereignty [https://aws.amazon.com/compliance/europe-digital-sovereignty/]

Sono due cose diverse, e non vanno confuse. *Nitro Enclaves* è una funzionalità di EC2 che isola un'enclave dalla propria **istanza padre** — è il modello di minaccia citato sopra, e riguarda l'ambiente del cliente. Il *sistema Nitro* è l'architettura di piattaforma sottostante, ed è l'oggetto dell'affermazione molto più ampia esaminata qui di seguito. Rispondere a un'affermazione sul sistema con la documentazione delle enclave sarebbe un errore di categoria, e per questo i due piani sono tenuti distinti.

Il sistema Nitro: la dichiarazione più forte dei quattro fornitori, e ciò che la sostiene

AWS afferma che il sistema Nitro *«fornisce un confine di sicurezza fisico e logico tale che **nessuno, inclusi i dipendenti AWS, può accedere ai carichi di lavoro o ai dati dei clienti**»*. È la dichiarazione più netta fra quelle dei tre fornitori, e merita di essere affrontata con le prove, non con una smentita.

La dichiarazione poggia su un audit esterno del sistema Nitro. Quell'audit dichiara **quattro limiti propri**:

- l'auditor è stato **pagato da AWS**;
- è una **revisione del progetto senza test** — l'auditor dichiara di non poter attestare che l'implementazione corrisponda al progetto;
- mette **fuori dal proprio perimetro** il piano di controllo EC2, l'hypervisor, il firmware e le Nitro Card;
- e non fornisce **alcuna garanzia rispetto a modifiche tecniche future «scelte o *imposte*»**.

La parola è dell'auditor: ***imposte***.
La dichiarazione descrive un progetto. **L'audit di quel progetto esclude espressamente lo scenario di cui si discute.**

Una valutazione indipendente non finanziata da AWS — Trail of Bits — formula il residuo senza giri di parole: *«devi fidarti completamente di AWS»*.

La struttura europea, e che cosa dice il registro delle imprese

Sul piano societario Amazon ha fatto **più di Google e Oracle in Italia**, e va riconosciuto. AWS ha annunciato *«una nuova capogruppo e tre controllate costituite in Germania»*, una direzione composta da *«cittadini UE residenti nell'UE»* e un consiglio consultivo di quattro cittadini UE *«fra cui almeno un membro indipendente non affiliato ad Amazon»*, *«legalmente obbligato ad agire nell'interesse dell'AWS European Sovereign Cloud»*. Prima region: Brandeburgo.

Siamo poi andati a cercare quella società nel registro delle imprese tedesco, su due servizi di registro indipendenti. L'iscrizione è **Amtsgericht Potsdam, HRB 40853**:

Data	Iscrizione a registro
12–13.08.2021	Costituita come **SCUR-Alpha 1391 GmbH**. Capitale sociale **25.000 €**.
21.10.2021	Cambio di denominazione: **Amazon Germany Holdco 1 GmbH**.
23.07.2025	Cambio di denominazione: **AWS European Sovereign Cloud GmbH**, sede spostata a Potsdam.
17.06.2025 → 03.12.2025	**Kathrin Renz** — l'amministratrice delegata indicata nell'annuncio — nominata e poi **non più amministratrice**.
Oggi	Amministratori: **Stephane Israel** (14.11.2025) e **Stefan A. Höchbauer** (21.01.2026).
Socio unico	**A100 ROW, Inc.**, Wilmington, **Delaware, Stati Uniti** — State File no. 4517940. **25.000 quote da 1,00 € — somma della partecipazione: 100%.** Elenco notarile, autenticato a Monaco il 20.10.2025.
Oggetto sociale	*«Die Beteiligung an Gesellschaften, die durch den Betrieb europäischer Rechenzentren die Bereitstellung von Datenhosting-Diensten unterstützen»* — la partecipazione in società che supportano servizi di hosting di dati.

Fonte: Registro delle imprese — Amtsgericht Potsdam, HRB 40853 [https://openregister.de/company/DE-HRB-G1312-40853] · annuncio AWS sulla governance [https://www.aboutamazon.eu/news/aws/built-operated-controlled-and-secured-in-europe-aws-unveils-new-sovereign-controls-and-governance-structure-for-the-aws-european-sovereign-cloud]

In precedenza ci eravamo rifiutati di indicare una percentuale di proprietà, perché l'elenco dei soci è un documento a pagamento che non avevamo letto. **Ora lo abbiamo letto.** La *Liste der Gesellschafter* di HRB 40853 P registra un **socio unico**:

A100 ROW, Inc. — Wilmington, Delaware, Stati Uniti
25.000 quote da 1,00 € · **somma della partecipazione: 100%** · autenticato da notaio a Monaco, 20.10.2025

La società presentata come capogruppo **europea** del cloud sovrano è **interamente posseduta da una società del Delaware**. Non in parte, non insieme a un socio europeo: **un socio, cento per cento** — e non è in Europa.

Dove la catena si ferma, e perché conta. Il registro tedesco prova il **primo anello** con un documento notarile. Il secondo — chi possieda A100 ROW, Inc. — non è provabile allo stesso modo: **il Delaware non pubblica le informazioni sui soci**, il che è fra le ragioni per cui vi si costituiscono società. Fonti secondarie convergenti indicano Amazon.com, Inc.; lo riportiamo come tale, non come prova. **Il punto non ne dipende:** la capogruppo del cloud sovrano è già, su prova primaria, interamente posseduta fuori dall'Unione — e la catena prosegue poi in una giurisdizione dove la proprietà non viene divulgata affatto.

La «nuova capogruppo europea» è un veicolo societario preesistente, costituito nel 2021 e denominato *Amazon Germany Holdco 1 GmbH* fino al luglio 2025, con il capitale minimo di legge di 25.000 euro e un oggetto sociale di partecipazione in altre società. E l'amministratrice presentata come il volto della governance europea **ha cessato la carica nel giro di circa sei mesi**.

Detto con equità. Usare un veicolo societario già registrato e il capitale minimo di legge è **prassi societaria del tutto ordinaria** in Germania, e non prova alcuna malafede. Per sostenere un giudizio più forte servirebbero statuto, patti parasociali, diritti di veto, composizione del consiglio e le dipendenze di licenza e operative — **nulla di tutto ciò l'abbiamo letto**. Il punto non è la prassi: è la **distanza fra quella prassi e il linguaggio dell'annuncio**. Il giudizio non riguarda il veicolo: riguarda la **distanza fra quella prassi ordinaria e il linguaggio dell'annuncio**, e la proprietà registrata qui sopra.

E la frase sul non essere mai successo — scritta meglio di quella di Microsoft

La formulazione di Amazon è che dal 2020 *«non ci sono state richieste di dati ad AWS che **abbiano portato alla divulgazione** di contenuti **archiviati fuori dagli Stati Uniti** da clienti **aziendali o governativi** al governo statunitense»*.

Tre restrizioni in una riga sola. Non dice che non ci siano state *richieste*: dice che nessuna *ha portato alla divulgazione*. Copre solo i contenuti *fuori dagli Stati Uniti*. E solo i clienti *aziendali o governativi*. È la stessa classe di affermazione esaminata nella sezione 12 — ed è inverificabile per la stessa ragione: il divieto di dirlo è esso stesso legge.

Due reperti ulteriori, per completezza. L'annuncio AWS sulla governance dell'European Sovereign Cloud **non tratta in alcun punto il CLOUD Act**: come nei documenti italiani, la questione giurisdizionale non riceve una risposta debole — non viene posta. E nel catalogo ufficiale dei prodotti qualificati dell'agenzia francese, **Amazon e AWS compaiono zero volte**: né qualificati né in istruttoria. Microsoft ha costituito Bleu ed è entrata in istruttoria; Google ha costituito S3NS ed è arrivata alla qualificazione. **Amazon ha costituito una GmbH tedesca e non l'ha portata alla qualificazione francese.**

8. Chi ha una qualificazione di sovranità, e chi no

L'agenzia francese pubblica un catalogo ufficiale dei prodotti e servizi qualificati. Lo abbiamo letto per intero — 130 pagine — e vi abbiamo cercato.

Oracle 0 · Microsoft 0 · Amazon 0 · AWS 0 · Polo Strategico Nazionale 0

Fonte: ANSSI, catalogo dei prodotti e servizi qualificati (PDF, 130 pp.) [https://messervices.cyber.gouv.fr/visas/catalogue-produits-services-profils-de-protection-sites-certifies-qualifies-agrees-anssi.pdf] · elenco dei prestatori in istruttoria [https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/services-de-securite-evalue/solutions-en-cours-de-qualification/prestataires-secnumcloud/]

Che cosa significa e che cosa non significa questo conteggio — ed è un punto che conta. La qualificazione francese si attacca a una **offerta specifica**, non a un'azienda né a una tecnologia. Un'offerta *costruita su* tecnologia di un fornitore ma **operata da un soggetto europeo** può essere qualificata: è esattamente il caso di **S3NS**, che gira su tecnologia Google ed **è qualificata**, e di **Bleu**, che gira su tecnologia Microsoft ed è **in istruttoria**. La lettura corretta del conteggio è quindi stretta: **nessuna offerta usata dal programma italiano possiede una qualificazione del genere, e nessuna è in istruttoria** — non che le tecnologie di quei fornitori siano incapaci di sostenerne una. I casi francesi dimostrano il contrario.

Le **sedici** offerte attualmente in istruttoria dicono altrettanto: Adista, **Bleu SAS**, BLUE, Cegedim, Cloud Temple, Ecritel, Free Pro, GIP Mipih, ITS Integra, NumSpot, NRB, Orange Business, OVH, Prolival, Scaleway, Scalingo. **Bleu — l'impresa di Microsoft, Orange e Capgemini — è in quell'elenco. Oracle no.**

Il **9 febbraio 2021**, davanti all'Assemblea nazionale francese, la direttrice generale di Oracle France annunciava che l'azienda era *«in discussione con l'agenzia»*.
Cinque anni e mezzo dopo, Oracle non compare né fra i qualificati né fra quelli in istruttoria.

Microsoft, sulla stessa strada, ha costituito **Bleu** — capitale francese di controllo — ed è entrata in istruttoria. Google ha costituito **S3NS** con Thales ed è arrivata alla qualificazione, intestata a **Thales Cloud Sécurisé**: il titolare è il socio europeo di controllo. **Oracle ha annunciato una discussione.**

Che cosa questo reperto non dimostra. L'assenza di una qualificazione non è la prova che Alloy sia inadeguato. Significa una cosa più precisa e più difendibile: **Alloy non è mai stato misurato con quel metro** — e il programma cloud pubblico italiano, che su Alloy costruisce il proprio livello più protetto, **non ha chiesto a nessuno di misurarlo**. Non abbiamo trovato **alcuna analisi dell'agenzia francese dedicata a Oracle Alloy**: non trovata non significa inesistente.

9. I quattro fornitori, e il punto in cui coincidono

Ciascuno dei quattro fornitori usati dal cloud pubblico italiano ha costruito qualcosa di reale, e ciascuno ha tracciato un confine di sicurezza. Letti uno per volta i quattro sembrano diversi. Letti uno accanto all'altro, **escludono quattro soggetti diversi — e nessuno dei quattro esclude lo stesso**.

Fornitore	La sua misura più forte	Chi esclude davvero	Chi non esclude
Microsoft	Region italiana, chiavi del PSN, ibrido nei locali del PSN	Gli altri clienti, il furto dei dischi, l'ispezione occasionale del personale	Chi tiene il piano di controllo — dichiarato **Azure Arc** nella guida contrattuale del PSN
Google	Assured Workloads — policy di residenza e accesso	La creazione di risorse fuori dalle region scelte, i servizi senza CMEK	Chi può cambiare la policy — la modifica è **registrata, non impedita**, e può ricevere un'eccezione
Amazon	Nitro Enclaves — esecuzione isolata e cifrata	**L'istanza padre del cliente stesso** — il suo root, il suo amministratore, il suo codice compromesso	Chi esegue l'hypervisor e può arrestare l'istanza — e firma l'attestazione
Oracle	Alloy — realm separato nei data center del PSN, più l'*Operator Access Control*	**I dipendenti Oracle** — davvero: approvazione, limiti di tempo, log dei comandi e dei tasti	**L'automazione che gira come root** — esclusa dalla documentazione di Oracle stessa — e il canale degli aggiornamenti

Si legga l'ultima colonna dall'alto in basso. Ognuno di quei soggetti è **il fornitore stesso**, in una veste tecnica diversa: il piano di controllo, il motore delle policy, l'hypervisor, l'automazione. **Quattro misure diverse, e ciascuna si ferma allo stesso muro.**

9.1 Come le mitigazioni stesse creano l'esposizione

È la parte che sfugge più facilmente, ed è il punto più affilato di questa pagina. La legge statunitense raggiunge i dati che si trovano in **possesso, custodia o controllo** del fornitore. Ognuna di queste mitigazioni, per funzionare, deve **creare un nuovo oggetto** — e quell'oggetto finisce esattamente in quella condizione.

La mitigazione	L'oggetto che deve creare	Dove sta quell'oggetto
Cifratura a riposo	Una chiave che la piattaforma deve poter *usare*	Nel servizio di chiavi, o raggiungibile da esso
Confidential computing	Un'attestazione, firmata da una radice di fiducia	Nella catena del produttore e del fornitore
Enclave isolata	Un hypervisor che applica l'isolamento e un'istanza che lo ospita	Interamente presso il fornitore
Region sovrana / data boundary	Un piano di controllo che applica e verifica le regole	Presso il fornitore — e, sul livello ibrido, **nominato nel contratto**
Realm operato dal partner	Un canale di aggiornamento attraverso cui la piattaforma resta viva	Presso il fornitore, che produce gli aggiornamenti
Controllata europea	Una catena di controllo societario	Che termina in una capogruppo fuori dall'Unione

Una mitigazione non elimina l'appiglio giuridico. **Lo sposta, e gli dà un nome nuovo.** Il dato diventa illeggibile e diventa raggiungibile la *chiave*; la memoria diventa opaca e diventa firmabile l'*attestazione*; la region diventa nazionale e il *piano di controllo* resta all'estero. È per questo che aggiungere misure non converge verso la sovranità: ogni misura nuova aggiunge un oggetto in più all'elenco di ciò che il fornitore detiene.

9.2 Che cosa hanno in comune i quattro quando parlano

Lo schema si ripete anche nel linguaggio. Ogni fornitore fa un'affermazione forte, e ogni affermazione è **vera come è scritta** — e più stretta di come suona.

- **Microsoft**, sotto giuramento: *«No, non posso garantirlo, ma, ancora una volta, ciò non si è ancora mai verificato.»* La prima metà è l'ammissione; la seconda è inverificabile per costruzione.
- **Amazon**: *«nessuna richiesta di dati che **abbia portato alla divulgazione** di contenuti **archiviati fuori dagli Stati Uniti** da clienti **aziendali o governativi**»*. Tre restrizioni in una riga.
- **Oracle**: *«un operatore Oracle Alloy mantiene il pieno controllo dei dati e delle applicazioni»* — una dichiarazione aziendale, accanto a una pagina di documentazione che esclude l'automazione root dai controlli di accesso.
- **Google**, in un documento scritto per le scuole: *«esaminiamo **con attenzione** ciascuna richiesta»*. Esaminiamo con attenzione. **Non: rifiutiamo.**

E un silenzio che pure condividono: nell'annuncio ufficiale sulla governance dell'AWS European Sovereign Cloud, nelle pagine Google sui data boundary e in 161 pagine di documenti contrattuali italiani, **la legge statunitense non viene mai discussa**. La questione giurisdizionale non riceve una risposta debole. Non viene posta.

Che cosa niente di tutto questo dimostra. Non dimostra che alcun fornitore abbia agito scorrettamente, né che dati pubblici italiani siano stati divulgati. Non ne abbiamo prova, e lo diciamo. Ciò che le quattro analisi stabiliscono è più stretto e più solido: **le misure attivate sono efficaci contro gli avversari per cui sono state progettate, e nessuna di esse è stata progettata per un ordine giuridico notificato al fornitore**. Non è un difetto dell'ingegneria. È il confine di ciò che l'ingegneria può fare.

Una risposta tecnica a una domanda giuridica

I fornitori soggetti al CLOUD Act — Microsoft, Google, Amazon — non sono rimasti fermi. Hanno investito molto, e in modo visibile, in ciò che viene messo sul mercato come *sovranità*: entità giuridiche europee, region nazionali, personale operativo locale, gestione esterna delle chiavi, enclave cifrate, perimetri dedicati ai dati dell'Unione. Alcune di queste cose sono ingegneria seria, fatta da persone competenti, e in questa pagina ciascuna verrà riconosciuta per quello che vale.

Vale la pena essere chiari sul perché stia accadendo. Non è un ripensamento: è una **risposta commerciale a un'esposizione giuridica**. Le amministrazioni pubbliche europee hanno cominciato a fare una domanda scomoda, la Francia l'ha scritta dentro un referenziale di certificazione, e il mercato ha prodotto delle risposte. È un fatto sano — ed è anche il punto in cui nasce il problema.

Ognuna di queste misure è **costruita, configurata e amministrata proprio dal soggetto da cui dovrebbe proteggervi**. Non è un difetto di questo o quel prodotto: è una proprietà strutturale del comprare un servizio da qualcuno. E significa che ogni misura ha un punto preciso in cui restituisce il controllo — un punto in cui, per continuare a funzionare, deve tornare a fidarsi del fornitore.

La tabella qui sotto è la mappa di questa pagina. A sinistra ogni misura e ciò che risolve davvero — perché ciascuna risolve qualcosa di reale. A destra **il punto in cui si richiude su sé stessa**, con il rimando alla sezione che la esamina. Si legga la colonna di destra dall'alto in basso: ci si accorge che la ragione è sempre la stessa, detta in sei modi diversi.

La misura	Che cosa risolve davvero	Dove si richiude su sé stessa
Cifratura a riposo con chiavi esterne	Furto dei dischi, altri clienti sulla stessa macchina, ispezione occasionale di un archivio. **Protezione vera.**	Per elaborare un record bisogna decifrarlo, e il testo in chiaro compare nella memoria del fornitore. → §13
Region nazionale — residenza del dato	Latenza, continuità, e una serie di obblighi reali sui trasferimenti in materia di protezione dei dati.	La giurisdizione segue l'azienda, non il disco: la legge raggiunge i dati in *possesso, custodia o controllo* del fornitore, ovunque si trovino. → §15
Personale locale e separazione operativa	L'accesso quotidiano di personale estero, e il supporto svolto dall'estero. **Una proprietà seria.**	Un ordine non viene notificato alla squadra operativa locale: viene notificato alla casa madre. → §1
Confidential computing	I clienti vicini di macchina e la lettura passiva della memoria da parte dell'host. **Vera difesa in profondità**, con le parole dell'ANSSI.	Non regge contro un amministratore *attivo* — ed è chi gestisce la piattaforma a decidere se sia acceso. → §12
Attestazione remota	La verifica crittografica che il carico di lavoro in esecuzione sia quello atteso.	Verifica *che cosa* gira, non *dove* — e il meccanismo stesso è stato rotto nel 2026. → §12.4
Entità giuridica europea del fornitore	Il contratto, la fatturazione, la giurisdizione civile e un punto di responsabilità locale.	Una controllata europea di un gruppo extra-europeo non è un gruppo europeo — principio enunciato sotto giuramento da uno dei fornitori stessi. → §12
Backup «sovrano» nel perimetro nazionale	La continuità e il recupero, se il servizio diventa indisponibile.	Una copia non è una limitazione d'accesso. Avere un duplicato non impedisce a nessuno di leggere l'originale. → §4

Ogni riga della colonna di destra è un modo diverso di scrivere: **la misura dipende dal fornitore**. È per questo che aggiungerne altre non aiuta, ed è per questo che la risposta non è una misura migliore. La sezione 14 spiega perché non sia affatto un problema di ingegneria; la sezione 15 affronta le obiezioni una per una; la sezione 1 applica tutto questo al cloud pubblico italiano.

> *«Il Confidential Computing **non è abbastanza sicuro da proteggere l'integrità e la riservatezza dei dati contro un amministratore ostile che compia attacchi mirati e attivi**.»*
>
> — **ANSSI**, l'agenzia nazionale francese per la cybersicurezza, *Technical Position Paper on Confidential Computing*, 17 ottobre 2025

Si rilegga il modello di minaccia: **un amministratore ostile**. Non un attaccante esterno, non un altro cliente sulla stessa macchina — chi gestisce la piattaforma. È esattamente la situazione che crea un ordine giudiziario emesso sotto una giurisdizione straniera: un fornitore che non è malintenzionato, ma è *obbligato* — e a cui è vietato dirlo.

10. Un dato esiste in tre stati. La cifratura ne copre due.

È tutto qui l'argomento tecnico, e sta in una tabella. Non è materia controversa: è il modo in cui funzionano i computer.

Stato	Protezione	Funziona?
A riposo sul disco	Cifratura con chiavi esterne	**Sì.** Realmente efficace. Protegge i blocchi memorizzati dal furto dei dischi, dagli altri clienti e dall'ispezione occasionale del personale.
In transito sulla rete	TLS	**Sì.** Matura, standard, efficace.

Stato	Protezione	Funziona?
In uso nella RAM, nella CPU	Confidential computing	**In parte, e non contro chi gestisce la piattaforma.** È l'argomento di tutto il resto di questa pagina.

Nei **normali carichi di lavoro cloud general purpose** — un database, un server di posta, un applicativo — un dato dev'essere **in chiaro** dentro un contesto di esecuzione per poter essere elaborato. Ogni interrogazione, ogni ricerca, ogni report, ogni accesso comporta un istante in cui il dato è in chiaro nella RAM di una macchina che appartiene a qualcuno e che qualcuno amministra.

Una precisazione che conta, perché spesso si scrive il contrario. *Non* è vero in generale che un processore non possa calcolare su dati cifrati: la **crittografia omomorfica**, il **calcolo multiparte sicuro** e le tecniche di *privacy-preserving computation* fanno esattamente questo. Hanno ambiti, prestazioni e maturità molto diversi e — per quanto risulta — **non sono la base delle architetture descritte in questa pagina**. L'affermazione qui è quindi più stretta e verificabile: nei carichi di lavoro ordinari che questi programmi effettivamente eseguono, il dato viene decifrato dentro un contesto di esecuzione.

Chi controlla l'hypervisor e la macchina fisica controlla quell'istante. Può sospendere una macchina virtuale e riversarne la memoria su disco; può farne uno snapshot; può leggere i registri della CPU. Nulla di esotico: è **ordinaria amministrazione della piattaforma**, la stessa capacità che si usa ogni giorno per la migrazione a caldo, il debug e i backup.

11. Che cos'è il confidential computing — e che cosa ottiene davvero

Il confidential computing è la risposta dell'industria alla terza riga di quella tabella. Il processore crea un'enclave cifrata e isolata — un *Trusted Execution Environment* — la cui memoria è cifrata con una chiave custodita nel silicio e, in linea di principio, non disponibile all'hypervisor. Le implementazioni principali sono **Intel TDX**, **AMD SEV-SNP** e **ARM CCA**. Un meccanismo chiamato **attestazione remota** dovrebbe permettere al cliente di verificare crittograficamente che il proprio carico di lavoro giri davvero dentro una di queste enclave.

L'ANSSI — la stessa agenzia citata in apertura — è esplicita: la tecnologia *«completa efficacemente la cifratura a riposo e in transito cifrando i dati in uso»* e *«fornisce comunque una difesa in profondità significativa»*. Usata correttamente *«può aumentare la complessità degli attacchi provenienti dall'host o da altri clienti sulla stessa macchina fisica, e ridurre la dimensione della Trusted Computing Base»*. **Non è una cattiva tecnologia.** Chi sostiene il contrario esagera, e perde il confronto con qualunque ingegnere competente.

12. Quattro ragioni per cui non produce sovranità

12.1 Il modello di minaccia esclude proprio la nostra minaccia

Il confidential computing è progettato contro un operatore *curioso* e contro i clienti vicini di macchina. Non è progettato contro un operatore *determinato*, che controlla il firmware e la catena di fornitura e che ha tempo. La conclusione dell'ANSSI su quello scenario è la frase in cima a questa pagina. E l'ANSSI aggiunge che cosa fare invece: gli utenti *«devono evitare di girare su infrastrutture condivise gestite da fornitori di cui non possono fidarsi»*.

Un ordine giudiziario non rende malintenzionato un fornitore. Lo rende obbligato — che, nel modello di minaccia, è la stessa cosa.

*«**Non fare affidamento sul Confidential Computing se il fornitore cloud è considerato non affidabile o potenzialmente ostile**: contro un attaccante attivo esistono **troppe vulnerabilità note per potersene difendere efficacemente**. In tali situazioni, **passare a un fornitore affidabile o usare hardware dedicato bare-metal in un ambiente fisico controllato è un prerequisito**.»*

Non è una riserva sepolta in un allegato. È una raccomandazione agli utenti, numerata, nel documento di posizione dell'agenzia.

Si noti la parola **prerequisito**. L'ANSSI non presenta il fornitore affidabile come un'alternativa alla tecnologia: lo presenta come la *precondizione* senza la quale sulla tecnologia non ci si dovrebbe affidare affatto. L'ordine dei fattori è l'opposto di quello implicito in ogni offerta di «cloud sovrano» costruita su un fornitore a controllo estero.

12.2 Non soddisfa lo standard di sovranità — secondo l'agenzia che lo ha scritto

> *«L'analisi condotta mostra che il Confidential Computing* ***non è sufficiente, da solo, a mettere in sicurezza un intero sistema, né a soddisfare i requisiti descritti nella sezione 19.6 del referenziale SecNumCloud 3.2****.»*

La sezione **19.6** di SecNumCloud è *la* clausola di immunità: il requisito che un fornitore qualificato sia al riparo dalle leggi extraterritoriali non europee — attraverso la sede, il controllo del capitale e il luogo da cui il servizio è amministrato. **Quella clausola l'ha scritta l'ANSSI. Ed è l'ANSSI a dire che il confidential computing non la soddisfa.**

È il fatto più importante di questa pagina. Ogni argomento che proponga il confidential computing *in sostituzione* dei requisiti giurisdizionali è già smentito dall'autorità che quei requisiti li ha inventati.

Che cosa l'ANSSI dice e che cosa non dice — perché la distinzione conta. Le parole *sovranità*, *attore statuale*, *extraterritoriale*, *giurisdizione* e *legge* compaiono **zero volte** nelle tredici pagine del documento. Lo abbiamo verificato. L'ANSSI non imposta la propria analisi in termini politici.

Ciò che fa è più utile. Descrive l'avversario **per funzione** — un *«amministratore malintenzionato»* che *«può controllare la creazione e l'esecuzione dei carichi di lavoro, compreso modificarli prima dell'avvio, e* ***leggerne o scriverne la memoria durante l'esecuzione****»*; e, fra gli attori contro cui il modello non regge, *«attaccanti con un* ***altissimo potere di coercizione sui fornitori****»*. Poi dichiara la tecnica insufficiente per la clausola che esiste proprio per contrastare l'accesso di uno Stato estero. **La conclusione politica è nostra; le premesse tecniche sono interamente dell'ANSSI.**

12.3 Chi gestisce la piattaforma decide se è acceso

Il confidential computing non è una proprietà del dato. È una *configurazione della piattaforma*: un tipo di macchina da selezionare, una funzionalità da abilitare, un firmware da tenere aggiornato. Il soggetto che decide se l'enclave è attiva, per quali carichi di lavoro e dopo quale aggiornamento, è lo stesso soggetto da cui l'enclave dovrebbe proteggere.

È per questo che le formule usate dai fornitori pesano tanto. Quando un servizio è descritto come dotato di confidential computing **«ove attivato»**, la protezione è stata resa condizionale — e la condizione non è nelle mani del cliente.

12.4 Una debolezza trovata nel modo in cui l'attestazione viene legata al canale

L'intera costruzione poggia sull'attestazione remota: senza, il cliente non ha modo di sapere se l'enclave è reale. Il reperto che segue **non invalida l'attestazione in generale** — riguarda un modo molto diffuso di legare l'evidenza di attestazione a un canale TLS. Nel 2026 un gruppo guidato da **Muhammad Usama Sardar** (TU Dresden), con Mariam Moustafa e Tuomas Aura, ha dimostrato che l'attestazione eseguita dentro l'handshake TLS può essere sconfitta con un attacco di inoltro. Nella sintesi che ne ha dato The Register:

> *«Una connessione destinata a un server può essere* ***silenziosamente reindirizzata verso una macchina diversa e compromessa che esegue software identico, ovunque nel mondo****, senza che il client se ne accorga mai.»*

«Una connessione destinata a un server può essere ***silenziosamente reindirizzata verso una macchina diversa e compromessa che esegue software identico, ovunque nel mondo****, senza che il client se ne accorga mai.»*

Il protocollo *verifica l'integrità del software, non la sua collocazione*. La vulnerabilità è registrata come **CVE-2026-33697** (CVSS 7.5) e ha riguardato sistemi già in produzione. La ricerca è pubblicata come *Identity Crisis in Confidential Computing* (AsiaCCS 2026) e *Intra-handshake.fail* (ESORICS 2026). E sulla possibilità di correggerla, il lavoro conclude che la protezione piena *«potrebbe non essere possibile»* con l'attestazione dentro l'handshake così com'è oggi progettata, senza rompere proprietà del TLS 1.3.

Detto con precisione. È un difetto in un *modo* molto diffuso di fare attestazione, non la prova che ogni installazione di confidential computing sia compromessa; esistono mitigazioni e vengono adottate. Ciò che dimostra è che l'attestazione è un campo di ricerca attivo con problemi irrisolti — il che è una base fragile su cui fondare un'affermazione di sovranità.

12.5 E l'affermazione commerciale che l'ANSSI corregge di persona

L'ANSSI osserva che la tecnologia *«è spesso presentata dai fornitori commerciali come una soluzione per eseguire carichi di lavoro remoti con lo stesso livello di riservatezza e integrità di un'installazione locale, cioè resistente a un attacco fisico»* — e poi afferma senza giri di parole: ***«gli attacchi fisici sono esplicitamente fuori dal perimetro del modello di sicurezza»***.

Chi possiede l'edificio ha accesso fisico alle macchine. Il modello di sicurezza del confidential computing non copre quel caso, e lo dichiara.

13. E le chiavi? Lo stesso problema, un piano più sotto

La seconda risposta tecnica che viene di solito offerta è la gestione delle chiavi: il cliente custodisce le chiavi di cifratura fuori dal perimetro del fornitore, tipicamente in un modulo hardware di sicurezza. I modelli hanno un nome — **BYOK** (*bring your own key*), **HYOK** e gestione esterna delle chiavi — e differiscono per quanto la chiave resti lontana dalla piattaforma.

Anche questo è reale, e anche questo va riconosciuto prima di criticarlo. Chiavi custodite in un HSM controllato dal cliente eliminano davvero una classe di esposizione: i blocchi memorizzati non si leggono copiando un disco, un operatore non può curiosare in un archivio, e una chiave si può revocare.

> Perché un carico di lavoro giri, il dato dev'essere decifrato. La decifratura avviene **dentro l'ambiente di esecuzione del fornitore**, perché è lì che sta la CPU. Per quanto lontano si tenga la chiave, nel momento dell'uso o la chiave o il testo in chiaro — e di solito entrambi — si trovano nella memoria di una macchina che il fornitore amministra.

Un paragone che regge: potete tenere la chiave della cassaforte in tasca vostra, in un altro Paese. Ma se la cassaforte è nel palazzo di qualcun altro, e chiedete al suo personale di aprirla e leggervi il documento, **il luogo in cui sta la chiave non è ciò che determina chi può leggere quel documento**. La gestione esterna delle chiavi cambia *chi deve essere obbligato*, e quanto la cosa sia visibile. Non cambia *se* il testo in chiaro esista dentro il perimetro del fornitore.

> *«Si noti che **gli approcci 'Bring Your Own Key' (BYOK) non risolvono il problema, perché il fornitore cloud deve comunque essere considerato affidabile per usare le chiavi fornite dall'utente**.»*
>
> — ANSSI, stesso documento, nella sezione su disponibilità e gestione delle chiavi

Quella sola frase liquida l'argomento secondo cui la custodia esterna delle chiavi produrrebbe sovranità. La chiave è vostra; **le mani che la usano no**. La fiducia nel fornitore non viene eliminata dall'architettura: viene spostata da «fidarsi che custodisca il dato» a «fidarsi che usi la chiave solo come richiesto». Per un fornitore che ha il dovere giuridico di ottemperare a un ordine straniero, è la stessa fiducia.

13.1 Dove esattamente il BYOK smette di funzionare, passo per passo

Vale la pena seguire la chiave lungo un'operazione ordinaria, perché il punto non è sottile una volta vista la sequenza. Si supponga che un'amministrazione tenga un archivio cifrato nel cloud del fornitore, con la chiave in un proprio modulo hardware.

#	Che cosa accade	Chi vede che cosa
1	Il dato sta sul disco, cifrato.	**Nessuno**, senza la chiave. Il BYOK funziona. È protezione vera.
2	Un funzionario esegue una ricerca.	La piattaforma deve decifrare. Richiede la chiave, oppure chiede al modulo esterno di eseguire l'operazione.
3	Il modulo esterno autorizza. È l'istante su cui l'intera architettura si regge.	Il modulo non può sapere *perché* la richiesta sia stata fatta, ma solo che è ben formata e proviene dalla piattaforma attesa. **Non può distinguere un'interrogazione legittima da una eseguita in esecuzione di un ordine.**
4	Il record viene decifrato ed elaborato.	Il testo in chiaro è **nella RAM di una macchina che il fornitore amministra**. È inevitabile: è lì che sta la CPU.

#	Che cosa accade	Chi vede che cosa
5	Il risultato viene restituito.	Chiunque possa fare uno snapshot della memoria di quella macchina ha il dato **in chiaro** — indipendentemente da dove risieda la chiave.

Il modulo esterno delle chiavi non è quindi una barriera alla lettura del dato. È **un interruttore che decide se il sistema funziona**. Il suo potere reale è fermare tutto — che è una proprietà vera e preziosa, e anche molto grossolana: un'amministrazione non può revocare la propria chiave ogni volta che sospetta qualcosa, perché revocarla significa spegnere il servizio.

E l'ANSSI segnala la stessa trappola dal lato opposto, quello della disponibilità: far dipendere la piattaforma da una chiave esterna introduce un modo di guasto che *«può causare l'indisponibilità dell'intero sistema»*. L'esternalizzazione delle chiavi compra un interruttore d'emergenza e lo paga in fragilità — ma non compra riservatezza nei confronti di chi gestisce la piattaforma.

Un beneficio reale, che va nominato perché è l'argomento più forte della parte avversa, esiste: revocare una chiave esterna è un atto *osservabile*. Il cliente che ritira la chiave si accorge che l'accesso si è fermato. È una proprietà vera — ma è una proprietà sugli accessi **futuri**, e non serve a nulla contro un'acquisizione già avvenuta e che un ordine di riservatezza vieta a chiunque di menzionare.

14. Perché una misura tecnica non può risolvere un problema giuridico

È la parte che vale la pena capire anche saltando tutto il resto di questa pagina, e richiede circa un minuto.

Ogni misura di sicurezza mai costruita presuppone un **avversario che deve aggirare qualcosa**. La cifratura presuppone qualcuno che non ha la chiave. Il controllo degli accessi presuppone qualcuno senza credenziali. La segregazione di rete presuppone qualcuno dalla parte sbagliata di un confine. Il confidential computing presuppone qualcuno che deve evadere da un'enclave. Tutte funzionano *alzando il costo di aggirare le regole del sistema*.

> Un ordine giudiziario non aggira nulla. **Viene eseguito dall'amministratore, usando i poteri legittimi dell'amministratore, dentro le regole del sistema.** Nessun confine viene attraversato, nessuna credenziale rubata, nessuna enclave forzata. Il fornitore fa ciò che ha titolo di fare sulla propria piattaforma — e lo fa perché un giudice glielo ha ordinato.

Fonte: Google, *Monitor an Assured Workloads folder for violations* [https://docs.cloud.google.com/assured-workloads/docs/monitor-folder]

È per questo che la domanda *«quale misura tecnica protegge dal CLOUD Act?»* non ha risposta. È come chiedere quale serratura protegga dalla chiave del padrone di casa. La serratura non è difettosa. **La domanda è puntata sullo strato sbagliato.**

E spiega perché sommare misure non aiuta. La difesa in profondità moltiplica il lavoro di un attaccante che deve sconfiggere ogni strato a turno. Non produce nulla quando **tutti gli strati sono amministrati dallo stesso soggetto**, perché quel soggetto non deve sconfiggerli: li configura.

15. Le obiezioni, una per una

Sono le risposte che un fornitore o un programma di cloud pubblico può legittimamente dare. Ognuna è riportata nella forma più forte che sappiamo darle, e poi affrontata. Dove l'obiezione ha in parte ragione, lo diciamo.

«Il confidential computing cifra la memoria. Non possiamo leggerla nemmeno noi.»

Sì — e però: Vero per la lettura passiva, ed è cosa buona. Ma la cifratura della memoria protegge il *contenuto* di una macchina, non la *catena di comando che decide come quella macchina viene avviata*. Chi gestisce la piattaforma può non attivare la funzione, disattivarla, alterare l'immagine prima dell'avvio, aggiornare il firmware, o riavviare il carico di lavoro in una configurazione senza enclave. L'ANSSI è esplicita: la tecnologia non regge contro un amministratore che compia attacchi **attivi**.

«C'è l'attestazione remota. Il cliente verifica crittograficamente.»

Sì — e però: L'attestazione verifica *che cosa* sta girando, non *dove*. Nel 2026 è stato dimostrato un attacco di inoltro — CVE-2026-33697 — in cui una connessione viene silenziosamente reindirizzata verso un'altra macchina che esegue software identico, ovunque nel mondo. E la radice di fiducia è la catena del produttore: l'ANSSI elenca fra gli

avversari rilevanti *«attaccanti con un altissimo potere di coercizione sui fornitori»*, in grado di ottenere copia delle chiavi private custodite nell'hardware.

«Le chiavi di cifratura sono vostre, in un modulo hardware fuori dal nostro perimetro.»

Sì — e però: L'ANSSI, verbatim: *«gli approcci BYOK non risolvono il problema, perché il fornitore deve comunque essere ritenuto affidabile per usare le chiavi fornite dall'utente»*. Custodire non è usare. Per elaborare un record la piattaforma deve ottenere una chiave utilizzabile o il testo in chiaro, e il modulo esterno non può distinguere una richiesta legittima da una eseguita in esecuzione di un ordine.

«Il dato non esce dall'Italia. La region è italiana.»

Sì — e però: La giurisdizione segue la nazionalità dell'azienda, non la posizione del disco. Il CLOUD Act raggiunge i dati in *possesso, custodia o controllo* del fornitore, ovunque si trovino — compreso un data center italiano. Non è una nostra lettura: è la ragione per cui quella legge fu scritta dopo che Microsoft aveva vinto proprio sull'argomento della collocazione, nel caso irlandese.

«Il personale che opera il servizio è italiano.»

Sì — e però: È una proprietà reale e preziosa sul piano operativo, e va riconosciuta. Ma un ordine non viene notificato al personale operativo italiano: viene notificato alla casa madre. E dove esiste un piano di controllo ibrido, quel piano è del fornitore — la guida contrattuale del PSN descrive *«un control plane unico con Microsoft Azure Arc»*.

«Combiniamo più misure. È difesa in profondità.»

Sì — e però: La difesa in profondità moltiplica lo sforzo di un attaccante che deve sconfiggere ogni strato. Non aggiunge nulla quando tutti gli strati condividono lo stesso punto di fiducia, perché quel soggetto non li sconfigge: li configura. Due serrature sulla stessa porta non servono, se le due chiavi sono nelle stesse mani.

«Potete revocare la vostra chiave in qualunque momento.»

Sì — e però: Vero, ed è l'argomento più forte di questo elenco: la revoca è *osservabile*, e il cliente si accorge che l'accesso si è fermato. Ma governa i soli accessi **futuri**. Non serve a nulla contro un'acquisizione già avvenuta — e che un ordine di riservatezza vieta a chiunque di menzionare.

«Non è mai successo.»

Sì — e però: Non è verificabile fino in fondo, né da noi né da chi lo afferma. Un ordine di riservatezza — dove viene emesso, e non ogni ordine ne porta uno — rende il fatto indicibile per legge, e la norma italiana che impone ai fornitori di segnalare le richieste di accesso extra-europee chiede esattamente la comunicazione che quella legge straniera proibisce. La frase non è una rassicurazione: descrive un silenzio garantito per legge.

«Il servizio è certificato e qualificato dall'autorità nazionale.»

Sì — e però: Il quadro di qualificazione italiano non contiene requisiti su nazionalità, controllo societario, capogruppo o legge di paesi terzi. In 161 pagine di documenti contrattuali e operativi del PSN quei termini compaiono zero volte. La questione giurisdizionale non riceve una risposta debole: non viene posta.

«Il confidential computing è uno standard di settore.»

Sì — e però: L'ANSSI osserva che *«manca di certificazioni di sicurezza»*, che l'ecosistema *«manca attualmente di stack software maturi che integrino l'attestazione con la consegna dei segreti»* e che realizzarlo correttamente *«richiede competenze profonde per garantire l'integrità dell'intera TCB»*. È un campo in movimento con problemi irrisolti, non una garanzia consolidata.

> Ogni obiezione riguarda una **capacità tecnica**: cifratura, attestazione, custodia delle chiavi, collocazione, personale, certificazione. Nessuna riguarda **chi possa ricevere l'ordine di agire, da parte di chi, e sotto quale legge**. È l'unica variabile che cambia la risposta — e non è una variabile tecnica.

16. Sette scenari, graduati

Un verdetto binario — sovrano o non sovrano — è più facile da scrivere e più facile da confutare. Segue la stessa evidenza organizzata per **scenario di minaccia**, perché il programma si comporta in modo molto diverso da uno all'altro. **In tre dei sette si comporta bene**: non è una concessione, è il risultato.

Scenario	Misura dichiarata	Prova pubblica	Rischio residuo
A — Accesso ordinario di un amministratore del servizio	Personale operativo italiano sul livello managed; *Operator Access Control* di Oracle con approvazione, limiti di tempo e log dei comandi.	Documentata in fonti del fornitore e del programma.	**Basso.** L'automazione root è esclusa da quei controlli, per dichiarazione di Oracle.
B — Compromissione o vulnerabilità del fornitore	Segmentazione, cifratura a riposo con chiavi in HSM controllato dal cliente, isolamento Nitro, Zero Trust, rete senza internet pubblico.	Documentate, e tecnicamente valide.	**Realmente ridotto.** È ciò per cui queste misure sono costruite, e funzionano.
C — Ordine giuridico al soggetto italiano	Legge italiana ed europea, vigilanza nazionale, golden power sul concessionario.	Documentata nella convenzione di concessione.	**Non è l'oggetto di questa analisi.** Un ordine di diritto italiano o europeo segue garanzie italiane o europee. Nulla qui lo contesta.
D — Ordine giuridico a una società statunitense collegata	Cifratura con chiavi proprie; confidential computing *«ove attivato»*.	L'agenzia francese dichiara entrambe **insufficienti** a questo scopo, e nessuna clausola contrattuale sul punto è stata trovata.	**Non affrontato.** Se il destinatario abbia possesso, custodia o controllo va accertato caso per caso — ma nulla lo esclude, e nulla è scritto in proposito.
E — Aggiornamento imposto o malevolo	Sul livello Oracle, patching standard a cura dell'operatore. Sui livelli Google, aggiornamenti a cura del fornitore.	L'operatore ha **visibilità** sulle modifiche, incluse quelle di emergenza. **Nessuna approvazione o rifiuto risulta documentato.**	**Aperto.** L'audit Nitro non fornisce espressamente garanzie contro modifiche *«scelte o imposte»*. È un rischio di **controllo del software**, e non va confuso con la prova di un accesso ai dati.
F — Interruzione geopolitica o commerciale	Backup sovrano nel perimetro nazionale; due region Alloy; rete esclusiva.	Una copia esiste. Se la piattaforma possa operare **disconnessa dal fornitore**, e per quanto, **non risulta documentato in nessuna fonte esaminata**.	**Non quantificato.** Licenze, supporto, aggiornamenti e sostituzione hardware passano tutti da soggetti extra-UE. Un backup non è continuità.
G — Richiesta di metadati	La cifratura protegge il contenuto. Configurazioni, log, identità, fatturazione, telemetria e grafo delle risorse sono un'altra questione.	**Non affrontato nei documenti esaminati.** Non abbiamo trovato alcuna mappatura di quali componenti trasmettano telemetria fuori dal perimetro.	**Indeterminato, e probabilmente sottovalutato.** I metadati sono spesso rivelatori quanto il contenuto, e raramente sono cifrati punto a punto.

Lo schema non è che il programma sia debole ovunque. In **A, B e C** fa ciò per cui è stato costruito, e lo fa bene. L'esposizione si concentra in **D, E, F e G** — ordine giuridico estero, controllo del software, continuità senza il fornitore, metadati — e quei quattro condividono un tratto: **nessuno è un problema di sicurezza. Sono tutte domande su chi detiene che cosa, e sotto quale legge.**

17. Le migliori argomentazioni a favore del programma

Un'analisi che presenta solo la propria tesi non è un'analisi. Seguono le argomentazioni più forti che un difensore competente del cloud pubblico italiano potrebbe portare, enunciate **nel modo migliore che sappiamo** — e poi affrontate con ciò che le prove sostengono, e soltanto quello.

L'argomento, nella sua forma migliore	Che cosa le prove sostengono in risposta
Il consolidamento è un guadagno di sicurezza reale. Migliaia di sale server manutenute in modo disomogeneo sostituite da data center presidiati migliorano sicurezza fisica, continuità e aggiornamenti — probabilmente più di qualunque clausola di sovranità.	**Siamo d'accordo, senza riserve.** Nulla in questa pagina lo contesta, e questa analisi sarebbe disonesta se lo facesse.
Il soggetto contraente e operativo può essere italiano anche dove la tecnologia è americana. Governance, personale e responsabilità stanno davvero in Italia.	Vero, e documentato per un livello. Riguarda la sovranità *operativa*. Non riguarda a chi venga notificato l'ordine giuridico, che è una domanda diversa.
Localizzazione, segmentazione, cifratura, logging e controllo accessi riducono rischi reali. La maggior parte degli incidenti veri non sono ordini statuali.	**Corretto, e importante.** La nostra tesi non è che queste misure siano inutili — è che rispondono a una domanda diversa da quella che la parola «sovranità» solleva.

L'argomento, nella sua forma migliore	Che cosa le prove sostengono in risposta
La nazionalità di un fornitore non dimostra possesso, custodia o controllo su ogni dato. Va accertato caso per caso.	**Corretto, e lo diciamo noi stessi.** Non sosteniamo che alcun dato sia stato divulgato, né che l'assoggettamento discenda automaticamente dalla proprietà. Ciò che documentiamo è che *nessuna clausola contrattuale lo esclude*.
Confidential computing e gestione esterna delle chiavi possono limitare l'accesso perfino del fornitore. È il loro scopo dichiarato.	Possono, e riducono davvero diversi scenari. Ma l'agenzia che ha scritto lo standard europeo di sovranità afferma che **non lo soddisfano** e che non reggono contro un amministratore ostile *attivo*. Non è un nostro giudizio.
SecNumCloud non è l'unico modello legittimo di sovranità. Un Paese può ragionevolmente scegliere un equilibrio diverso.	**Del tutto vero.** La nostra obiezione non è che l'Italia non abbia adottato il modello francese — è che **nessun requisito equivalente, di alcun tipo**, è stato trovato nel corpus esaminato. Anche un modello diverso andrebbe scritto.
La piena autonomia tecnologica ha costi, tempi e rischi operativi propri. Una soluzione pragmatica può accettare un rischio residuo.	**Concordiamo — purché il rischio residuo sia misurato e dichiarato.** È tutto lì il punto: un rischio accettato apertamente è una scelta politica; un rischio descritto come inesistente è un'altra cosa.

Delle sette argomentazioni qui sopra, **ne accettiamo tre per intero e ne qualifichiamo altre tre**. Il disaccordo si restringe a una sola proposizione, ed è falsificabile: **che nei documenti esaminati esista un requisito, di qualunque modello, che vincoli un fornitore su sede, proprietà o amministrazione.** Si produca quella clausola e questa analisi è sbagliata.

18. Che cosa si potrebbe fare — sei misure, in ordine di praticabilità

Una critica che non offre alternative è commento. Quel che segue è ordinato per quanto presto ciascuna misura potrebbe essere adottata, e ognuna poggia su uno strumento che **esiste già**. Nessuna richiede di abbandonare i fornitori attuali.

#	Misura	Strumento che esiste già
1	**Pubblicare quale livello usa ciascuna amministrazione.**	Non costa nulla e non richiede negoziato. È il dato la cui assenza impedisce a chiunque — Parlamento compreso — di misurare l'esposizione. **La sua assenza è la terza occorrenza dello stesso schema documentato su questo sito.**
2	**Usare la scadenza del 12 gennaio 2027.**	Da quella data, una legge europea già in vigore vieta di far pagare a un cliente il costo di uscire da un cloud. È l'unica data certa dell'intero quadro, e trasforma *«cambiare costa troppo»* da argomento in domanda.
3	**Mappare e pubblicare la telemetria.**	Quali componenti trasmettono fuori dal perimetro, verso quali endpoint, con quali metadati. Lo scenario G è indeterminato proprio perché questa mappa non esiste pubblicamente — e produrla è un compito ingegneristico, non politico.
4	**Pretendere l'approvazione, non la visibilità, sulle modifiche di piattaforma.**	Oggi l'operatore vede le modifiche, comprese quelle di emergenza, su una dashboard. Un requisito contrattuale di approvazione preventiva — e di quarantena e validazione prima del rilascio, come già fa un fornitore francese — trasforma lo scenario E da aperto a delimitato.
5	**Scrivere un requisito di sede, proprietà e amministrazione per la classificazione più alta dei dati.**	Tre verifiche binarie, applicate solo ai dati che le meritano. Non deve essere il modello francese — ma dev'essere **scritto**, perché a un requisito che non esiste in alcun documento non ci si può conformare, non lo si può misurare e non lo si può violare.
6	**Aderire alla centrale d'acquisto europea, senza aspettare.**	La proposta di regolamento europeo consente a un ente locale di aderire **anche se il proprio Stato non aderisce**, ed essere per ciò stesso in regola con il diritto UE degli appalti. **Non è ancora in vigore** — manca l'approvazione, manca l'accordo fra la Commissione e almeno due Stati membri, e la piattaforma non esiste. Il punto non è che la porta sia aperta: è **dov'è la porta**.

Che cosa non stiamo raccomandando. Non di abbandonare questi fornitori, il che non sarebbe né praticabile né evidentemente saggio; non la piena autonomia tecnologica, che ha costi, tempi e rischi operativi propri; e non il referenziale francese come unico modello legittimo. **Accettare un rischio residuo è una scelta politica legittima.** Descrivere quel rischio come inesistente è un'altra cosa, ed è l'unica contro cui questa pagina argomenta.

19. La conclusione, detta con cura

La cifratura e il confidential computing sono **buona ingegneria**. Sconfiggono una gamma ampia di attaccanti reali: gli altri clienti sulla stessa macchina, gli intrusi, i ladri, il singolo dipendente infedele. Vanno usati, e un fornitore che li offre sta facendo qualcosa di utile.

Ma sono tutte misure che proteggono *da qualcun altro* mentre si è dentro una casa che appartiene a un terzo. **Nessuna di esse risponde alla domanda su che cosa accade quando al padrone di casa viene notificato un ordine — e gli è vietato dirvelo.** Non è una domanda di ingegneria. È una domanda su quale legge si applichi, e gli unici modi noti di cambiare la risposta sono quelli scritti in SecNumCloud e nelle lettere che chiedono l'EUCS High+: dove l'azienda è stabilita, chi ne controlla il capitale, e da dove il servizio è amministrato.

Numerose misure tecniche sono state realmente attivate. Nessuna di esse è in grado di difendere da un attore statuale che possa obbligare il fornitore cloud con un ordine giuridico — che è la posizione degli Stati Uniti, attraverso il CLOUD Act e la Sezione 702 del FISA, nei confronti di Microsoft, Google e Amazon. Le misure sono buone. Sono rivolte agli attaccanti. **L'ordine non è un attacco: è l'amministratore che fa ciò che all'amministratore è consentito fare.**

Presentare queste misure come sovranità non è un errore tecnico. È un **errore di categoria**: rispondere a una domanda giuridica con un manufatto ingegneristico. Quelle misure sono una mitigazione. Non sono un'immunità — e l'agenzia che l'immunità l'ha definita lo ha messo per iscritto.

Fonti

- ANSSI — *Technical Position Paper on Confidential Computing* v1.0, 17.10.2025 [https://messervices.cyber.gouv.fr/guides/en-technical-position-paper-confidential-computing] La fonte primaria di ogni citazione ANSSI di questa pagina. **Il PDF integrale di 13 pagine è stato scaricato e letto per intero**, non la pagina di presentazione. Link diretto al PDF [https://cyber.gouv.fr/sites/default/files/document/anssi-technical-position-paper-coco-v1.0.pdf] · SecNumCloud 3.2, il referenziale la cui sezione 19.6 è citata [https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf]
- The Register — sull'attacco di inoltro all'attestazione, 04.07.2026 [https://www.theregister.com/security/2026/07/04/confidential-computings-trust-mechanism-is-broken-the-fix-may-not-exist/5266056] Resoconto del lavoro di Sardar, Moustafa e Aura. Lavori primari: AsiaCCS 2026 ed ESORICS 2026; CVE-2026-33697.
- PSN — servizi con Cloud Service Provider [https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/] La pagina commerciale. I documenti contrattuali e operativi qui citati (161 pagine) sono stati scaricati dal sito PSN e letti per intero.

Ogni citazione di questa pagina è stata letta alla fonte primaria, non ripresa da resoconti di seconda mano. Dove non abbiamo potuto verificare un'affermazione, lo diciamo nella pagina stessa.