	COMANDO PER LE OPERAZIONI IN RETE	**n. 22/2025 di Reg.**
	UFFICIO AMMINISTRAZIONE	**del 03/07/2025**
	Via Stresa 31/b – 00135 ROMA	
	OBBLIGAZIONE COMMERCIALE	
	Per: **Gara 180 – Acquisizione di studi e di un sistema prototipale relativi a un**	
	device-independent quantum key distribution (DI-QKD) per le applicazioni	
	Difesa. CUP D87H24007090001 - Capitolo 7101 - E.F. 2025. -RDO 5335762 II	
	ESPERIMENTO.	
	L'anno duemilaventicinque addì 3 del mese di luglio,	
	PREMESSO CHE	
	il Comandante del Comando per le Operazioni in Rete con Determina a Contrarre	
	nr. **795 in data 19/12/2025** ha autorizzato il Capo del Servizio	
	Amministrativo/Responsabile Unico del Progetto in Fase Affidamento ad	
	effettuare la procedura in economia; che tramite Mercato Elettronico della	
	Pubblica Amministrazione con R.**D.O. n. 5335762 II ESP. in data 07/05/2025**, il	
	Capo del Servizio Amministrativo ha indetto un'indagine di mercato; che con il	
	verbale di Ricognizione offerta n. 23 datato 07/06/2025 l'offerta presentata dalla	
	Società FABARIS SPA - VIA DEL SERAFICO 200 - ROMA, è stata valutata	
	congrua e vantaggiosa per l'A.D. da apposita Commissione all'uopo nominata; si	
	conviene e si stipula quanto segue: ==========	
	ART. 1 (le parti)	
	La **Società FABARIS SPA**, nella persona della **Sig. Antonello Gagliardi** nato a	
	Roma il 23/01/1968**,** in qualità di Legale Rappresentante della Società predetta,	
	come si evince dalla documentazione custodita in copia agli atti, che nel seguito	
	della presente obbligazione sarà denominata semplicemente "la Società", si	

impegna con l'A.D. e per essa con il Comando per le Operazioni in Rete nella persona del **RESPONSABILE UNICO DEL PROGETTO IN FASE AFFIDAMENTO Brig. Gen. Maurizio LAMBIASE** che nel seguito della presente obbligazione sarà denominata "l'Amministrazione", ad effettuare la fornitura in oggetto, come da requisito tecnico operativo e dettaglio prezzi in allegato, che costituisce parte integrante della presente scrittura. ====

ART. 2 (condizioni)

La presenta commessa, per tutto quanto non previsto nella presente, si svolgerà sotto l'osservanza del **D.P.R. 13 marzo 2013, n. 49** (Regolamento per la disciplina delle attività del Ministero della difesa in materia di lavori, servizi e forniture militari, a norma dell'articolo 4, comma 1, del decreto legislativo 15 novembre 2011, n. 208, recante attuazione della direttiva 2009/81/CE;. ==========

ART. 3 (durata della prestazione)

La fornitura/prestazione ha efficacia a decorrere dalla data di accettazione della presente obbligazione commerciale e della discendente lettera di ordinazione e dovrà essere conclusa **entro il 30/9/2025**. La verifica di conformità sarà eseguita da apposita Commissione nominata dal Comandante del Comando per le Operazioni in Rete, la quale dovrà verificare accuratamente che la fornitura sia stata eseguita conformemente a quanto richiesto e provvederà a redigere il relativo verbale di verifica di conformità. ==========

ART. 4 (importo aggiudicato e garanzia)

Per l'esecuzione delle prestazioni di cui alla presente obbligazione alla Ditta sarà corrisposto l'importo di **€. 347.334,00 IVA INCLUSA.** La Ditta a garanzia degli obblighi assunti con la presente scrittura, presenta **polizza fideiussoria nr. 15002503 datata 10/6/2025 rilasciata dalla Società AXERIA IARD S.A. per**

un valore di € 14.235,00 ai sensi della Legge 10.06.1982 n. 348. La garanzia prestata con la predetta polizza sarà valida dalla data della stipula fino a quella di cessazione della presente obbligazione. L'importo suddetto si intende fisso e invariabile e la Ditta si impegna a non avanzare richieste di revisione di prezzo. ==========

ART. 5 (modalità di pagamento)

Il pagamento, detratte le eventuali penalità di cui la Società si sia resa passibile, sarà effettuato a cura dalla Tesoreria Provinciale dello Stato, a mezzo di bonifico on-line sul conto corrente bancario/postale dedicato, entro il termine massimo di gg. 60 (sessanta) dalla data di avvenuta verifica di conformità/data fattura qualora quest'ultima sia emessa successivamente dalla data di avvenuta verifica di conformità. ==========

Si precisa che la fattura elettronica dovrà essere obbligatoriamente emessa in data successiva all'ultimazione della fornitura/servizio e, comunque, successivamente agli esiti positivi delle procedure previste ai fini dell'accertamento della conformità della fornitura/servizio (verbale di verifica conformità ove previsto); dovrà essere compilata in maniera analitica nelle modalità richieste, come da dettaglio prezzi in allegato, e dovrà indicare il numero di protocollo della lettera di ordinazione, il numero di CIG, la causale come da oggetto della presente Obbligazione e l'annotazione "SCISSIONE DEI PAGAMENTI" (qualora in presenza di IVA da versare allo Stato). La stessa dovrà essere intestata ed inviata a: COMANDO PER LE OPERAZIONI IN RETE – SERVIZIO AMMINISTRATIVO - Via Stresa, n. 31/b – 00135 ROMA Codice Fiscale 96451060584. Codice Ufficio ai sensi dell'articolo 3, del Decreto MEF n. 55 del 3 aprile 2013 in materia di emissione, trasmissione e ricevimento della

fattura elettronica **2SR075.** Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 7101 dell'E.F. 2025.**

ART. 6 (flussi finanziari)

La società assicura e garantisce che il c/c "dedicato" e le persone delegate ad operare su di esso, sono come da dichiarazione presentata dalla società in fase di offerta ai sensi dell'art. 3 della L.136 del 13.8.2010. **Tale dichiarazione viene allegata alla presente scrittura e ne costituisce parte integrante**. Ogni variazione negli estremi del predetto conto o delle persone delegate ad operare su di esso deve essere immediatamente comunicata all'Ente Militare a mezzo lettera raccomandata A/R; in assenza di detta comunicazione, nessuna responsabilità può essere attribuita all'Ente Militare per pagamenti fatti in conformità a quanto sopra dichiarato. La Società inoltre assume su di sé tutti gli obblighi di tracciabilità dei flussi finanziari di cui alla predetta L.136/2010, impegnandosi a regolare tutti i pagamenti relativi al presente ordinativo esclusivamente tramite bonifico bancario o postale, altrimenti idonei a garantire la piena tracciabilità delle operazioni. Il mancato utilizzo dei suindicati strumenti comporta la risoluzione di diritto del presente atto negoziale. L'obbligo di tracciabilità si estende a tutti i subcontraenti della filiera delle imprese a qualsiasi titolo interessate alle attività oggetto del contratto. Per tutto quanto non espressamente previsto nella presente dichiarazione, si applicano le disposizioni della L. 136/2010 e successive modifiche. ==========

ART. 7 (affidamento a terzi)

Ove si verificassero i seguenti eventi: ==========

- Frode, grave negligenza, contravvenzione nella esecuzione degli obblighi e condizioni contrattuali; ==========

- Cessione dell'azienda, cessazione dell'attività, oppure di concordato preventivo di fallimento, di stato di moratoria e conseguenti atti di sequestro o pignoramento a carico della Società; ==========
- Morte dell'imprenditore, quanto la considerazione della sua persona sia motivo determinante della garanzia; ==========
- Inizio delle prestazioni non nel termine prefissato; ==========
- Interruzione, anche momentanea, del servizio per qualsiasi motivo non autorizzata da questo Comando; ==========

l'Amministrazione potrà affidare a terzi, sempre con l'applicazione delle procedure di sicurezza, il servizio o la parte rimanente di esso in danno della Società, nei limiti del valore della presente obbligazione commerciale. =======

L'addebito a carico della Società inadempiente sarà effettuato secondo le previsioni normative vigenti. ==========

ART. 8 (patti di integrità)

La Società si obbliga al rispetto dei "**Patti di integrità**" sottoscritti in sede di presentazione dell'offerta ai sensi dell'art. 1 comma 17 Legge 190/2012. Tali provvedimenti, allegati al presente atto, ne costituiscono parte integrante, sostanziale, e pattizia ed il mancato rispetto degli stessi determinerà la risoluzione del presente Atto Negoziale. ==========

ART. 9 (penalità)

In caso di inadempimento ai patti e agli obblighi contrattuali l'A.D., fatto salvo quanto previsto dall'art. 134 del D.P.R. 236/2012 in ordine all'esecuzione in danno e alla risoluzione del rapporto contrattuale, applicherà una penalità del 1 ‰ (uno per mille) dell'importo contrattuale netto per ogni giorno di ritardo, fino al raggiungimento della percentuale massima del 10% (dieci per cento) dell'importo

contrattuale netto. Le condizioni stesse, per quanto non allegate alla presente obbligazione, ne fanno parte integrante a tutti gli effetti di legge, ai sensi dell'art. 99 del R.C.G.S., approvato con R.D. 23/5/1925, n. 827. Inoltre, la presente scrittura sarà soggetta a risoluzione automatica, qualora, la Società non adegui le condizioni economiche del presente atto negoziale alle condizioni più favorevoli previste in una eventuale convenzione CONSIP stipulata successivamente al presente atto negoziale ed avente lo stesso contenuto negoziale ("clausola di recesso" ai sensi del D.L. 95/2012 – cd. spending review), senza che la Ditta abbia nulla a che pretendere per la parte del servizio non svolta. ==========

ART. 10 (infortuni e danni)

La Società dichiara di assumere in proprio ogni responsabilità in caso di infortuni ed in caso di danni arrecati, eventualmente, alle persone ed alle cose tanto dell'Amministrazione che a terzi, in dipendenza di manchevolezze o di trascuratezze nell'esecuzione delle prestazioni. ==========

ART. 11 (variazioni)

Per l'esecuzione della presente obbligazione la Società elegge il suo domicilio legale **in VIA DEL SERAFICO 200 - ROMA**, ove si conviene dovranno essere notificati tutti gli atti di qualsiasi natura che potessero o dovessero derivare dal presente rapporto. Qualora nel corso di svolgimento della presente obbligazione si verificassero variazioni nella denominazione della Società o nelle persone della Società stessa autorizzate ad esigere o quietanzare in nome e per conto di essa, dette variazioni dovranno essere debitamente ed immediatamente notificate all'Amministrazione.

ART. 12 (tutela dei lavoratori)

La Società si obbliga a dimostrare in ogni tempo che adempie a tutti gli obblighi di

legge e di contratto relativi al lavoro ed alla tutela dei lavoratori riguardanti: ===

- le assicurazioni sociali , previdenziali e contributive derivanti da legge e da accordi salariali di lavoro (invalidità, vecchiaia, disoccupazione, tubercolosi, infortuni, malattia, ecc.); ==========

- quei rapporti in materia di lavoro che trovano la loro origine in accordi salariali, e prevedono, a favore dei lavoratori, assegni familiari, indennità ai richiami alle armi, contributi ex Ges.ca.l., ecc.; l'Amministrazione si riserva di operare una ritenuta sugli averi della società fino al 20% (ventipercento) dell'importo totale della prestazione, qualora l'ufficio competente denunci che la Società non ha adempiuto agli obblighi di cui sopra. ==========

La somma trattenuta sarà corrisposta soltanto quando l'ufficio denunciante avrà dichiarato di essersi la Società posta in regola, né la Società potrà prendere, per il ritardato pagamento del saldo, somma alcuna a qualsiasi titolo. L'Amministrazione si riserva, in presenza di un Documento Unico di Regolarità Contributiva (DURC) che evidenzi delle irregolarità nei versamenti dovuti agli Istituti e/o Casse Edili, di sostituirsi alla Società versando – in tutto o in parte – la somma dovuta in forza della presente obbligazione commerciale direttamente ai predetti Istituti e Casse in applicazione dell'art. 4 del D.P.R. n. 207/2010. La Società si obbliga, inoltre, a praticare verso i dipendenti lavoratori, condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro di categoria. Il mancato versamento dei contributi assicurativi e previdenziali nei riguardi degli operai impiegati potrà comportare a giudizio insindacabile dell'Amministrazione la sospensione dei pagamenti (art. 5 legge 25.01.94 n. 82) nonché la risoluzione dell'atto negoziale. ==========

ART. 13 (clausola risolutiva)

La presente obbligazione, in caso di accertamento di dichiarazioni non veritiere o mendaci, ai sensi del D.P.R. n. 445/00, sulla base delle autocertificazioni rese, secondo quanto richiesto dall'articolo 99 del D.LGS 36 del 31 marzo 2023, è da intendersi unilateralmente nulla e senza che la Società abbia nulla a pretendere. La Committente, senza bisogno di assegnare alcun termine per l'adempimento, potrà risolvere il presente contratto ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi all'Appaltatore tramite pec, nei casi previsti dagli art. 94 e 95 del D.Lgl. 36/2023, nell'ipotesi di irrogazione a carico dell'Appaltatore di sanzioni interdittive o misure cautelari di cui al D.Lgs. n. 231/2001, che impediscano all'Appaltatore di contrarre con la Pubblica Amministrazione. ==========

ART. 14 (clausola di riservatezza)

Ciascuna Parte si impegna a mantenere riservata, anche al termine del presente atto, qualsiasi informazione comunicata dall'altra Parte che desidera che sia mantenuta riservata ai documenti che: (1) risultano chiaramente evidenziati in forma scritta come riservati, o (2) siano stati dichiarati verbalmente confidenziali, con successiva conferma scritta entro 15 giorni dall'iniziale. La presente obbligazione di riservatezza non si applica alle informazioni che: (1) siano di dominio pubblico al momento della loro comunicazione; (2) siano state sviluppate autonomamente dalla Parte ricevente tali informazioni; (3) siano divenute di dominio pubblico senza alcuna responsabilità da parte della Parte ricevente tali informazioni, successivamente alla loro comunicazione da parte della Parte divulgante alla Parte ricevente; (4) siano già nella disponibilità della Parte ricevente al momento della loro comunicazione da parte della Parte divulgante e non siano gravate da alcun obbligo di riservatezza; (5) siano state comunicate a

terzi da parte della Parte divulgante senza alcun obbligo di riservatezza per i terzi; (6) siano state divulgate, per le quali la Parte divulgante ha espresso il suo consenso alla diffusione. In aggiunta a quanto sopra previsto, la Parte ricevente può liberamente comunicare le suddette informazioni in caso di richieste derivanti da un'autorità giudiziaria. L'Amministrazione è a conoscenza del fatto che la Ditta svolge la propria attività commerciale nella ricerca e nell'analisi dei servizi I.T. e la presente obbligazione di riservatezza non si applicherà ad ogni informazione ottenuta dalla Ditta attraverso ricerche, analisi, consulenze provenienti da fonti che siano diverse dai dipendenti che ricevono informazioni ai sensi del presente contratto. ==========

ART. 15 (clausola revisione dei prezzi)

Ai sensi dell'art. 60 e successive modifiche ed integrazioni, qualora nel corso di esecuzione del contratto al verificarsi di particolari condizioni di natura oggettiva, si determina una variazione, in aumento o in diminuzione, del costo del servizio superiore al cinque per cento, dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione, in relazione Pagina 3 di 3 alle prestazioni da eseguire. Ai fini del calcolo della variazione dei prezzi si utilizzano gli indici anche disaggregati dei prezzi al consumo, dei prezzi alla produzione dell'industria e dei servizi e gli indici delle retribuzioni contrattuali orarie. Gli indici di prezzo per le forniture di beni e servizi, sono pubblicati, unitamente alla relativa metodologia di calcolo, sul portale istituzionale dell'ISTAT in conformità alle pertinenti disposizioni normative europee e nazionali in materia di comunicazione e diffusione dell'informazione statistica ufficiale. ==========

ART. 16 (luogo di esecuzione fornitura e contatti)

La fornitura/prestazione deve essere realizzata a cura di codesta Società, secondo

le modalità riportate nel requisito tecnico operativo in allegato. Eventuale fornitura di materiali dovrà essere effettuata presso i Magazzini del Comando per le Operazioni in Rete - Viale del Castro Pretorio, 57 - 00184 Roma, **indicando i CODICI NATO dei materiali**, previo contatto telefonico con il **Mar.Ca. Alfredo MILITANO** al seguente numero di telefono 06.4691.4523 - e-mail: consegnatario2@cor.difesa.it. ==========

Direttore Esecuzione Contrattuale: S.T.V. BARTOCCI - mail: manolo.bartocci@difesanc.dom. ==========

ART. 17 – (rispetto norme trattamento dati personali) (GDPR)

Il Contraente dichiara di aver ricevuto prima della sottoscrizione del presente Contratto le informazioni di cui all'Art. 13 del Regolamento UE nr.2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), circa il trattamento dei dati personali, conferiti per la sottoscrizione e l'esecuzione del Contratto stesso e di essere a conoscenza dei diritti riconosciuti ai sensi della predetta normativa. ==========

Con la sottoscrizione del Contratto, il rappresentante legale del Contraente (o Procuratore munito di necessari poteri) acconsente espressamente al trattamento dei dati personali come sopra definito. In ragione dell'oggetto del presente Contratto, ove il Contraente sia chiamato ad eseguire attività di trattamento di dati personali, per conto dell'A.D. contraente, lo stesso potrà essere nominato "Responsabile del trattamento" o "sub-Responsabile del trattamento" ai sensi dell'Art. 28 del Regolamento UE; a tal fine, essa si impegna ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto di quanto disposto dall'Art. 5 del Regolamento UE, limitandosi ad

eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non incompatibili con le finalità per cui i dati sono stati raccolti. Il Contraente si impegna ad accettare la designazione a Responsabile/sub-Responsabile del trattamento ai sensi dell'Art. 28 del Regolamento UE, da parte dell'A.D., relativamente ai dati personali di cui la stessa è Titolare e che potranno essere trattati dal Contraente nell'ambito dell'erogazione dei servizi contrattualmente previsti. Con la sottoscrizione del Contratto il Contraente si obbliga ad adottare le misure di sicurezza di natura fisica, logica, tecnica e organizzativa idonee a garantire un livello di sicurezza adeguato al rischio e conformi a quanto previsto dalla normativa pro-tempore vigente e dalle istruzioni fornite dall'A.D., ivi comprese quelle specificate nel Contratto, unitamente ai suoi Allegati. Il Contraente si impegna ad osservare le vigenti disposizioni in materia di sicurezza e riservatezza e a farle osservare ai relativi dipendenti e collaboratori, anche quali incaricati del trattamento dei Dati personali. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti."

ART. 18 (sottoscrizioni)

La presente Obbligazione Commerciale consta di n. 12 pagine interamente scritte - allegati esclusi oltre le sottoscrizioni. ==========

Fatto, letto e sottoscritto alla data in epigrafe. ==========

PER L'AMMINISTRAZIONE DELLA DIFESA

IL RESPONSABILE UNICO DEL PROGETTO

IN FASE AFFIDAMENTO

Firmato Digitalmente da/Signed by:
MAURIZIO LAMBIASE
RUP AFFID
In Data/On Date:
venerdì 4 luglio 2025 09:23:06

Brig. Gen. Maurizio LAMBIASE

(documento firmato digitalmente)

IL RAPPRESENTANTE LEGALE DELLA SOCIETA'

Sig. Antonello GAGLIARDI (documento firmato digitalmente)

Firmato digitalmente da:
Antonello Gagliardi
Data: 07/07/2025 11:00:13

VISTO: APPROVO

IL COMANDANTE

Gen. D. Sandro SANASI (documento firmato digitalmente)

Firmato Digitalmente da/Signed by:
SANDRO SANASI
In Data/On Date:
lunedì 7 luglio 2025 19:18:32

Allegato all'Obbligazione Commerciale n. 22/2025 del 03/07/2025 (da citare in fattura)

Rife: Lettera di Ordinazione n. 76 del 03/07/2025 (da citare in fattura)

Oggetto: **Gara 180 – Acquisizione di studi e di un sistema prototipale relativi a un device-independent quantum key distribution (DI-QKD) per le applicazioni Difesa. CUP D87H24007090001 - Capitolo 7101 - E.F. 2025. -RDO 5335762 II ESPERIMENTO.**

PROSPETTO RIEPILOGATIVO

Descrizione	Quantità	Prezzo Unitario	Imponibile
Acquisizione di studi e di un sistema prototipale relativi a un device-independent quantum key distribution (DI-QKD) per le applicazioni Difesa, come da Requisito Tecnico Operativo e dettaglio prezzi in allegato.			€. 284.700,00
Totale Imponibile			€. 284.700,00
Iva 22%			€. 62.634,00
Totale			€. 347.334,00

COMANDO PER LE OPERAZIONI IN RETE

Reparto Operazioni Cibernetiche

REQUISITO

TECNICO OPERATIVO

RELATIVO A

Acquisizione di studi e di un sistema prototipale relativi a un Device-Independent Quantum Key Distribution (DI-QKD) per applicazioni Difesa. Fase unica

---

Edizione

Dicembre 2024

COMANDO PER LE OPERAZIONI IN RETE

Reparto Operazioni Cibernetiche

PREDISPOSIZIONE DEL DOCUMENTO

Redatto da	Data
Ufficio Tecnico Operativo	14/12/2024

LISTA REVISORI

Ufficio/Sezione/Nominativo

REGISTRO DELLE REVISIONI

Revisione	Data	Capitoli/paragrafi modificati	Osservazioni

QUESTO DOCUMENTO È COSTITUITO DA _____ PAGINE TOTALI

Sommario

1. OBIETTIVO

Lo Stato Maggiore delle Difesa, attraverso il Dipartimento Cyber Operations (ROC) del COR vuole prepararsi all'avvento sempre più invasivo di nuove soluzioni tecnologiche che risolvono il problema delle future esigenze dei sistemi crittografici. Mentre il mondo anticipa i prossimi standard di crittografia post-quantistica del NIST, è in essere lo sviluppo simultaneo di sistemi di distribuzione di chiavi quantistiche (QKD), con attori importanti come India, Cina, UE e Stati Uniti che ricercano e valutano attivamente gli standard per questo approccio crittografico emergente; la domanda cruciale rimane come la QKD potrebbe integrarsi in uno standard globale a prova di futuro per le comunicazioni digitali sicure oltre il 2030, anche se attualmente varie organizzazioni stanno perseguendo diverse implementazioni tecnologiche poiché non è emerso un chiaro leader in questo campo nascente.

La sicurezza delle informazioni digitali si basa sulla crittografia, utilizzata per la cifratura dei dati memorizzati su dischi e trasmessi in *streaming* su fibre ottiche o collegamenti "*free-space*" (spettro elettromagnetico). La base dei moderni sistemi di crittografia è data dai cifrari simmetrici, come Rijndael/AES, RC5 o SNOW, che garantiscono la riservatezza e l'integrità delle informazioni nelle reti Internet e 5G/6G distribuite. Questi algoritmi, in particolare Rijndael/AES, sono raccomandati da organizzazioni quali NATO, NIST, NSA negli Stati Uniti e dalle direttive eIDAS2/NIS2 dell'UE per la sicurezza delle informazioni fino al livello top-secret [NIST Federal Inf. Process. Stds. 197 (2001)]; nello specifico questi algoritmi utilizzano operazioni a bassa latenza e ad alte prestazioni per codificare e decodificare i *byte* in modo tale da rendere impossibili gli attacchi. Tuttavia, questi metodi richiedono l'utilizzo della stessa chiave segreta da parte di entrambi gli interlocutori.

Un'opzione, ampiamente utilizzata nelle infrastrutture critiche come le stazioni base 5G o i sistemi di controllo satellitare, è quella di salvare manualmente la chiave nel dispositivo *endpoint* (*pre-shared key*, PSK), ma questo comporta dei rischi quando il dispositivo viene catturato da un nemico o violato da un *hacker*. Attualmente, il problema della condivisione delle chiavi è risolto dall'infrastruttura a chiave pubblica (PKI) utilizzata per la generazione e la distribuzione di chiavi crittografiche con algoritmi asimmetrici. Tale soluzione è adeguata perché consente alle parti comunicanti di scambiare i dati senza una precedente interazione, basandosi solo sulla fiducia in un'autorità di certificazione (CA), solitamente fornita da un ente governativo o da un fornitore autorizzato. Tuttavia, le comuni PKI basate su Rivest-Shamir-Adleman (RSA) o sulla crittografia a curva ellittica (ECC) sono notoriamente violabili non solo da computer quantistici, ma anche da potenti computer convenzionali, e rappresentano il punto più debole del processo di scambio sicuro dei dati. Anche gli algoritmi asimmetrici di nuova generazione, ad esempio CRYSTALS-Kyber, che appartengono alla classe della crittografia post-quantistica (PQC) e che ora sono in fase di standardizzazione da parte del NIST, non offrono prove di sicurezza concrete e alcuni di essi hanno già dimostrato di poter essere violati nonostante anni di sviluppo. Pertanto, è urgente trovare nuove soluzioni per lo scambio di chiavi segrete che rispondano alle esigenze del moderno scenario sia in ambito

warfare, delle infrastrutture critiche e delle applicazioni commerciali ad alto valore economico e sociale.

Si intende sostituire la crittografia asimmetrica e l'infrastruttura a chiave pubblica con una tecnologia di distribuzione di chiavi quantistiche (QKD) che utilizzi l'*entanglement*, fornisca un'elevata sicurezza di creazione e distribuzione delle chiavi nonché un monitoraggio in tempo reale. La soluzione sarà dimostrata matematicamente e implementata sulla rete di test del COR-ROC e sarà sottoposta a collaudo al fine di verificarne la resistenza sia agli attacchi convenzionali che quantistici attraverso un protocollo che dovrà essere proposto dalla Ditta e validato da A.D.

2. SCENARIO ED ARTICOLAZIONE DEL PROGETTO

L'obiettivo di questo requisito tecnico operativo (RTO), redatto nell'ambito del PNRM di cui al titolo in copertina, è quello di definire i requisiti per una soluzione alternativa di crittografia quantistica indipendente dal dispositivo (DI) / distribuzione di chiavi quantistiche (QKD) che fornirà uno scambio sicuro di chiavi utilizzando la tecnologia fotonica quantistica più avanzata.

Lo scenario che si vuole realizzare si basa sull'ipotesi di un *entanglement* quantistico fotonico distribuito tra due terminali elettronico-ottici collegati mediante fibre ottiche in un modo che consenta loro di eseguire un *test* di Bell, e quindi estrarre i *bit* casuali correlati della chiave segreta senza inviarla fisicamente in alcuna forma tra gli *endpoint*. I terminali, che realizzeranno un protocollo ibrido quantistico-classico, eseguiranno un'ulteriore post-elaborazione crittografica dei *bit* estratti per garantirne l'utilità per le attività crittografiche, migliorare la loro *privacy* e fornirne l'utilizzo per le operazioni di rete. Inoltre, la velocità prevista con cui vengono generati i *bit* segreti sarà in rapporto con la radice quadrata della lunghezza della fibra ottica, consentendo lo scambio di informazioni a distanze molto lunghe, in modo simile al noto protocollo di distribuzione della chiave quantistica a doppio campo (TF), ma utilizzerà l' *entanglement* quantistico e un approccio completamente indipendente dal dispositivo, in cui il *test* di *entanglement* con risultato positivo informerà ulteriormente gli operatori di rete sull'assoluta sicurezza della chiave.

Quale *baseline* storica si tenga in considerazione che un sistema crittografico QKD è stato teoricamente descritto nel 1998, quindi le prove di sicurezza sono state sviluppate nel 2009 [https://iopscience.iop.org/article/10.1088/1367-2630/11/4/045021/meta], mentre le prime realizzazioni sperimentali sono state effettuate nel 2022 [https://www.nature.com/articles/s41534-023-00684-x].

Il progetto dovrà concretizzarsi con la realizzazione di un dimostratore per una soluzione DI-QKD da convalidare nell'infrastruttura di test del COR. Il sistema, composto da due terminali quantistici che utilizzano l'*entanglement* del numero di fotoni e da un nodo centrale, tutti ottimizzati per le operazioni nella lunghezza d'onda delle telecomunicazioni (1550 nm), potrà/dovrà prevedere eventuali personalizzazioni per le esigenze del settore della Difesa,

aggiungendo le opzioni di connettività necessarie e valutato per potenziali casi d'uso in diversi scenari.

Il progetto dovrà articolarsi nei seguenti *step*:

S1. Definire i casi di *test* e i criteri di successo;

S2. Realizzare un'installazione pilota DI-QKD basata su *entanglement*, collegando due terminali a una linea di test in fibra spenta ed eseguendo *test* delle prestazioni del sistema in scenari realistici, raggiungendo una velocità di trasmissione di almeno 10^4 *bit*/s su 15 km di fibra e allo stesso tempo soddisfacendo i criteri del *test* di Bell.

S3. Integrare e personalizzare il sistema per le esigenze del COR e del settore della Difesa, secondo le specifiche delle interfacce e degli standard utilizzati nella NATO e nelle Forze Armate italiane (queste ultime definite in S1).

S4. Eseguire *test* approfonditi di accettazione da parte dell'utente del funzionamento QKD in un collegamento tra due *data center* COR (da identificare nel corso di S1).

Il progetto si concluderà con un rapporto dettagliato sulla tecnologia QKD, le sue prestazioni, l'utilità per la Difesa e la robustezza nei diversi scenari definiti in S1.

3. OGGETTO DELLA DI FORNITURA

L'obiettivo è quello di acquisire un nuovo livello di conoscenza nel campo delle più avanzate soluzioni di crittografia quantistica che utilizzano l'*entanglement* quantistico e forniscono un livello di sicurezza delle informazioni indipendente dal dispositivo.

[R1] Per risolvere il problema dello scambio sicuro di chiavi, si propone di testare la sostituzione della crittografia asimmetrica *software-defined* e delle soluzioni PKI attualmente utilizzate con una nuova tecnologia di distribuzione di chiavi quantistiche (QKD) basata sull'*entanglement* quantistico multi-fotonico a lunga distanza, certificata da un test di Bell.

Il test di Bell è un concetto importante nell'ambito dell'informazione quantistica: è una misurazione congiunta di due stati quantistici che ne misura la correlazione. Questa tecnologia fornirà inoltre alla Difesa la possibilità di scambiare chiavi crittografiche realmente casuali, in modo incondizionatamente sicuro, superando il limite di distanza di circa 100 km [R2] imposto dalle precedenti soluzioni QKD.

[R3] Nella soluzione QKD ipotizzata, due parti comunicanti, "A" e "B", utilizzano cristalli SPDC (*Spontaneous Parametric Down-Conversion*) per produrre una coppia di impulsi quantistici multi-fotonici ciascuno, 10^5 - 10^8 volte al secondo. Quindi, uno degli impulsi di "A" e uno di "B" vengono inviati ad un nodo centrale, "C", che esegue lo scambio di *entanglement* per mezzo di una misura di Bell con "*heralding*" e crea di fatto un "*entanglement*" a lungo raggio tra i fotoni di "A" e "B". Questi fotoni *entangled* vengono

interferiti con impulsi coerenti sincronizzati su divisori di fascio variabili e misurati con rivelatori di nanofili superconduttori ad alta efficienza. L'*entanglement* è una fonte di casualità correlata: le letture di "A" e "B" sono davvero casuali, ma sono correlate nonostante la distanza, il che fornisce una base per produrre a distanza due chiavi segrete identiche, senza inviarle fisicamente attraverso il collegamento. L'esecuzione del *test* di Bell certifica la sicurezza e la casualità delle chiavi segrete prodotte in modo inconfutabile: permette alle parti di monitorare in tempo reale la sicurezza della connessione e di evidenziare immediatamente qualsiasi tentativo di intercettazione o manomissione delle informazioni scambiate, certificandone così l'integrità. Una volta che il *test* è positivo, le chiavi vengono post-elaborate e fornite agli utenti finali. Questa soluzione fornisce quindi un livello di sicurezza indipendente dal dispositivo (DI), che non dipende dalla sicurezza interna di alcun nodo o supporto fisico.

[R5] La soluzione QKD proposta sarà arricchita da un livello *software* che fornirà un'efficiente gestione delle chiavi segrete per ambienti multiutente, interfacce di programmazione delle applicazioni (API), connettori e *plug-in* per una perfetta integrazione con l'infrastruttura IT, un'interfaccia *user-friendly* per il controllo e l'amministrazione, il monitoraggio in tempo reale (osservabilità) e il funzionamento *cloud-native*.

4. PIANO DI ATTUAZIONE

L'implementazione del sistema complessivo, costituito da due terminali e da un nodo centrale, sarà realizzata nelle seguenti fasi:

1. Due terminali QKD saranno assemblati e consegnati da un fornitore di tecnologia a livello industriale, scelto dopo una selezione competitiva per le competenze nello specifico campo scientifico, così come i dispositivi *stand-alone* contenuti in *rack standard* 19''. [R6] Ognuno di essi sarà costituito da un sistema laser pulsato da 1550 nm, un cristallo SPDC, modulatori di luce, un rivelatore di nanofili superconduttori in un criostato, un computer e componenti fotonici passivi. I terminali saranno testati, caratterizzati per le loro prestazioni e convalidati dal personale del Comando per le Operazioni in Rete (COR) e dai ricercatori della parte fornitrice.
2. I terminali saranno installati in *data center* di proprietà del COR, separati e collegati con una coppia di fibre a bassissima perdita (a cura fornitore), dove una fibra sarà utilizzata esclusivamente per le comunicazioni quantistiche e l'altra per il trasferimento convenzionale dei dati. Il fornitore caratterizzerà i canali e testerà l'interferenza quantistica misurandone la visibilità. Se necessario, migliorerà l'installazione.
3. Verrà implementato il protocollo di distribuzione dell'*entanglement* a lungo raggio e i risultati saranno poi confrontati con il modello numerico definito in S1. Successivamente, verrà eseguito un *test* di Bell mediante interferenza locale di fotoni con impulsi coerenti di intensità variabile. Il sistema DI-QKD sarà collegato a una piattaforma di osservabilità, come Observium o Grafana (a cura fornitore).
4. IL COR, insieme al fornitore, concorrerà alla definizione del piano *test* e dei criteri di successo di S1. Al termine del progetto, verrà prodotta una documentazione che illustrerà i metodi di caratterizzazione e i risultati di robustezza del PoC.

5. NECESSITÀ FINANZIARIA

Nella tabella seguente sono riportate le forniture e le relative stime economiche di massima.

Elementi di alimentazione di base	**Costo stimato (IVA esclusa)**
Fornitura di S1 + S2 + S3 + S4 (Fase Unica)	
COSTO TOTALE STIMATO	

Tabella 1 – Requisiti Tecnico-Funzionali

6. TABELLA DEL CRONOPROGRAMMA

ITEM	DATA DI CONSEGNA
S1	T1 = T0 + 2 MESI
S2	T2 = T1 + 3 MESI
S3	T3 = T2 + 3 MESI
S4	T4 = T3 + 1 MESE

Tabella 2 – Piano Attuativo

Note:

- la fornitura di ogni articolo previsto dal presente requisito dovrà essere completata **entro il 30 settembre 2025** al fine di permettere all'Amministrazione Difesa di effettuare i pagamenti dovuti entro il medesimo esercizio finanziario a seguito di ricezione di regolare fattura.

Antonello Soffiardi

FABARIS S.P.A
Via del Serafico, 200
00142 Roma (Rm)
P.I. e C.F. 00844040576

F A B A R I S

Proposta tecnica

"Gara 180 – Acquisizione di studi e di un sistema prototipale relativi a un device-independent quantum key distribution (DI-QKD) per le applicazioni Difesa"

CUP D87H24007090001
Capitolo 7101
E.F. 2025

Sommario

Indice delle figure

1 Premessa

Il presente documento costituisce la Proposta Tecnica risposta alla procedura negoziata sotto soglia previa Richiesta di Offerta (RdO Aperta) per l'"Acquisizione di studi e di un sistema prototipale relativi a un device-independent quantum key distribution (DI-QKD) per le applicazioni Difesa", secondo le condizioni dettagliatamente descritte nel RTO allegato al Capitolato Tecnico della "Gara 180 – Acquisizione di studi e di un sistema prototipale relativi a un device-independent quantum key distribution (DI-QKD) per le applicazioni Difesa. CUP D87H24007090001 - Capitolo 7101 - E.F. 2025".

L'offerente intende soddisfare tutti i requisiti obbligatori enunciati nel Capitolato relativo alla Procedura in oggetto e propone una soluzione tecnologica in grado di soddisfare pienamente le qualità e le caratteristiche richieste per il successo dell'iniziativa, non solo per gli attuali, dichiarati, scopi sperimentali, ma anche per le prospettive relative ad auspicabili implementazioni di architetture di comunicazione in regime di produzione su scala nazionale.

La soluzione proposta e il sistema offerto si basano principalmente sulla tecnologia del partner Quantum2pi, azienda italiana che incarna lo spirito imprenditoriale proiettato verso l'innovazione e che contribuisce ad espandere la portata di quanto offrono gli incubatori del mondo universitario italiano.

Il documento prosegue con le seguenti sezioni:

- **Capitolo 2**: breve profilo dell'azienda offerente, Fabaris;
- **Capitolo 3**: breve profilo del partner Quantum2pi;
- **Capitolo 4**: descrizione del sistema proposto;
- **Capitolo 5**: componenti HW e SW offerti;
- **Capitolo 6**: matrice di tracciabilità;
- **Capitolo 7**: piano di implementazione;
- **Capitolo 8:** pianificazione dei test.

2 Fabaris S.p.A.

Fabaris, fondata nel 1996, trae origine dal settore Difesa, nel quale ha maturato significative esperienze e referenze che ne valorizzano l'offerta di tecnologie e servizi specialistici.

Negli anni Fabaris ha investito in capacità che si adattano alle esigenze della clientela, in particolare delle FF.AA. e delle organizzazioni che presidiano punti nevralgici delle reti e delle infrastrutture della Difesa. L'intento è realizzare progetti innovativi di alto valore e contenuto tecnologico. L'approccio concreto e orientato consente a Fabaris di affiancare con fiducia il cliente nelle sfide che il settore Difesa affronta per l'evoluzione tecnologica, della sicurezza informatica e per il consolidamento di reti e sistemi.

Fabaris attinge al proprio bagaglio di competenze specialistiche per supportare i clienti nei servizi e nello sviluppo di soluzioni fortemente integrate, per dare dinamicità all'intera catena del valore, fornendo un servizio ad alto contenuto tecnologico e d'innovazione.

Fabaris vanta numerose partnership con vendor di primaria importanza. Le certificazioni specialistiche dell'azienda e del proprio personale rappresentano un elemento certo di garanzia per clienti e partner, per il sicuro successo delle proprie iniziative.

In relazione all'oggetto di gara, le prospettive della sperimentazione s'incastonano nel medesimo strato tecnologico di ICT & Security che Fabaris ha contribuito a far crescere notevolmente negli ultimi 25 anni; ciò rappresenta un fattore di successo nelle auspicabili future iniziative d'integrazione della soluzione in oggetto con le apparecchiature dispiegate in esercizio; un esempio per tutti, HashiCorp, partner Fabaris, così come lo è IBM, che ha recentemente acquisito HashiCorp.

2.1 Partnership e Certificazioni aziendali

Il sistema di gestione di Fabaris è certificato ed è conforme ai requisiti della norma UNI EN ISO 9001:2015 nel settore IAF di attività 33, per la progettazione, sviluppo e manutenzione di sistemi e prodotti software e per i servizi di consulenza e assistenza informatica specialistica.

Fabaris è certificata ISO/IEC 27001:2013 - UNI CEI EN ISO/IEC 27001:2017 e applica i dettami della Norma al proprio Sistema di Gestione della Sicurezza delle Informazioni in conformità, per il campo di applicazione "Progettazione, sviluppo e manutenzione di sistemi informatici e prodotti software. Servizi di consulenza e assistenza informatica in relazione alle soluzioni di sicurezza

logica, fisica ed applicativa, compresa fornitura di apparati hardware".

Fabaris vanta numerose esperienze e referenze relative a progetti realizzativi e servizi basati su architetture complesse che le consentono di giocare un ruolo consulenziale presso numerosi Enti della Difesa, ministeri e FF.AA. Fabaris è oggi presente presso i principali Enti/Reparti: Ministero della Difesa e Direzioni Generali, Stato Maggiore della Difesa, Comando C4 Difesa, Stati Maggiore di Forza Armata (Esercito, Marina, Aeronautica), Comando Generale dell'Arma dei Carabinieri.

3 Quantum2pi

Quantum2pi è una startup innovativa italiana la cui missione è sviluppare e implementare soluzioni di Quantum Computing all'avanguardia che superino le attuali barriere tecnologiche, attraverso l'uso pionieristico del Quantum Computing. La visione di Quantum2pi è un futuro in cui i progressi nel Quantum Computing rivoluzioneranno la sicurezza informatica e sbloccheranno una potenza di calcolo senza precedenti, aprendo nuove opportunità per tutta l'umanità. I quattro pilastri dell'orizzonte tecnologico di Quantup2pi sono:

Crittografia post-quantistica	QKD	Intelligenza artificiale quantistica
Sviluppo di algoritmi di sicurezza robusti per proteggere i dati da future minacce quantistiche, assicurando la longevità e la robustezza dei sistemi crittografici. Creazione di algoritmi quantum-safe e utilizzo di computer quantistici per simulare scenari di attacco complicati per l'ottimizzazione della sicurezza	Progettazione sistemi di comunicazione impenetrabili, attraverso la distribuzione di chiavi quantistiche (QKD) e l'entanglement quantistico, per garantire i massimi livelli di sicurezza dei dati.	Sfruttamento del calcolo quantistico per il potenziamento dell'apprendimento automatico, fornendo capacità analitiche senza pari e migliorando i modelli predittivi. Utilizzo dell'apprendimento di rinforzo potenziato quantisticamente e algoritmi quantistici variazionali per affrontare problemi del mondo reale, in contesti critici.

Le soluzioni Quantum2pi sono conformi alle direttive del NIST e soddisfano e superano gli standard ETSI QKD, offrendo una sicurezza superiore rispetto agli approcci crittografici tradizionali.

3.1 Referenze

I fondatori, Dr. Ugo Chirico e il Prof. Salvatore Cuomo, collaborano con il team di ricerca del dipartimento di Fisica dell'Università di Napoli Federico II, che ha realizzato il sistema di QKD della rete di comunicazione quantistica multi-nodi metropolitana (https://www.automazionenews.it/a-napoli-la-prima-rete-di-comunicazione-quantistica/).

La rete di comunicazione quantistica multi-nodo metropolitana inaugurata a Napoli rappresenta un traguardo pionieristico per l'Italia, essendo la prima infrastruttura permanente di questo tipo nel Paese. Il cuore tecnologico del sistema è basato sulla Quantum Key Distribution (QKD), una tecnica di distribuzione di chiavi crittografiche che sfrutta le proprietà fondamentali della meccanica quantistica per garantire la sicurezza delle comunicazioni.

Il progetto è il risultato di una collaborazione tra istituzioni pubbliche, università e aziende italiane, sotto il coordinamento del Ministero per le Imprese e del Made in Italy (MIMIT) e del Competence Center Meditech 4.0. Tra i partner figurano l'Università di Napoli Federico II, il CNR-INO, l'Istituto Nazionale di Ricerca Metrologica (INRiM), Leonardo, QTI, TIM, Telsy, ThinkQuantum, Cisco ed Exprivia.

Questa iniziativa rappresenta un passo significativo verso lo sviluppo di un'infrastruttura nazionale di comunicazione quantistica, con l'obiettivo di estendere la rete a livello intercontinentale e di integrarla con altre tecnologie emergenti, come quelle spaziali.

La rete collega tre nodi principali:

- **CNR-INO** a Pozzuoli, parte dell'Italian Quantum Backbone (IQB);
- **Università di Napoli Federico II** nel campus di San Giovanni a Teduccio, sede del Competence Center Meditech 4.0;
- **Leonardo Labs** presso l'Aerotech Campus di Pomigliano d'Arco.

I nodi sono interconnessi tramite una rete in fibra ottica che integra componenti quantistici forniti da QTI e ThinkQuantum, oltre a sistemi di cifratura classica sviluppati da Telsy e Cisco. L'infrastruttura è progettata per essere compatibile con le soluzioni di cybersecurity di Leonardo.

4 Descrizione del Sistema proposto

Il sistema proposto è una soluzione avanzata per la **Quantum Key Distribution (QKD)** in regime **Device-Independent (DI)**, basata sull'utilizzo dell'entanglement quantistico per garantire la massima sicurezza nella trasmissione di chiavi crittografiche. La principale innovazione risiede nell'architettura che prevede due terminali stand-alone, collegati a un nodo centrale tramite fibra ottica single-mode a bassissima perdita, estesa per 15 km.

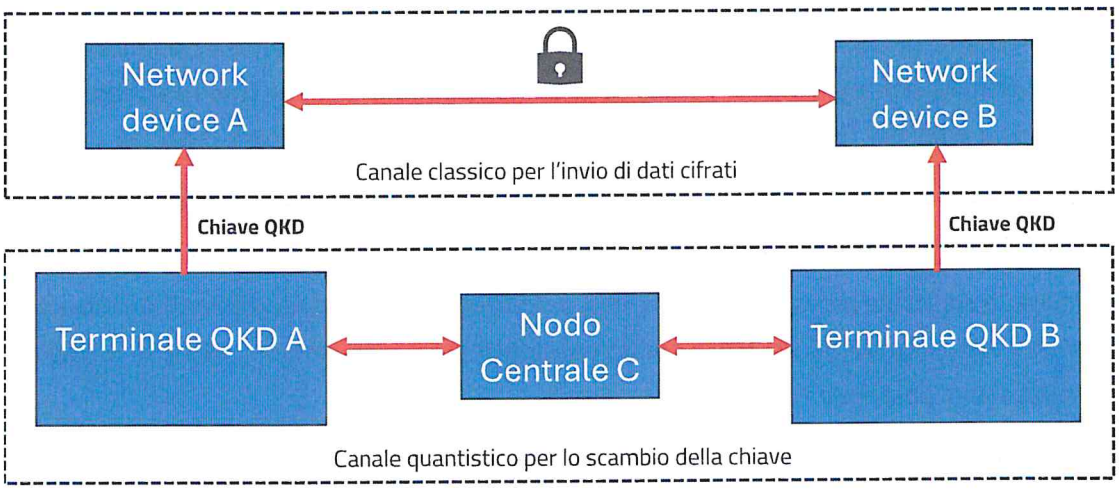

Figura 1: schema logico della soluzione proposta

Il DI-QKD consente di creare chiavi segrete condivise senza trasmetterle fisicamente, garantendo la sicurezza anche in presenza di dispositivi compromessi o canali insicuri. La sicurezza del sistema è certificata attraverso il test di Bell (CHSH), che verifica l'assenza di intercettazioni misurando la violazione della disuguaglianza di Bell. Un valore di S>2 conferma l'integrità del canale quantistico.

Il DI-QKD offre il massimo livello di sicurezza crittografica, basandosi esclusivamente sulla violazione delle disuguaglianze di Bell per garantire la sicurezza anche in caso di hardware non attendibile. Sebbene la letteratura recente (si veda articolo pubblicato su Nature nel 2023), abbia

convalidato sperimentalmente la fattibilità della DI-QKD, l'implementazione pratica in un ambiente operativo è un'attività complessa e sfidante.

Per rispondere ai requisiti quindi si delinea di seguito una roadmap ingegneristica completa, inclusi architettura, componenti e metodologia di deployment, per la costruzione di un sistema DI-QKD basato su coppie di fotoni entangled e central-node heralding.

Per il monitoraggio continuo delle prestazioni e della sicurezza, il sistema è integrato con piattaforme come **Grafana** e **Prometheus**, che offrono dashboard personalizzate per visualizzare il key-rate, il QBER (Quantum Bit Error Rate) e altre metriche critiche.

Tutta la soluzione destinata alla sperimentazione in oggetto è basata su software open-source. Le interfacce API RESTful consentono inoltre una facile integrazione con le infrastrutture IT esistenti e la conformità agli standard NATO, inclusi IPsec e TLS 1.3. Il sistema sarà realizzato rispettando gli standard ETSI GS QKD 002 - 014 e le raccomandazioni ITU-T Y.3800-Y.3805 per reti QKD.

La gestione sicura delle chiavi è affidata a soluzioni come **HashiCorp Vault**, che garantiscono la rotazione automatica e la crittografia end-to-end.

Infine, la soluzione prevede un piano di test articolato per verificare le prestazioni in scenari realistici, inclusi test operativi, di sicurezza contro attacchi come il man-in-the-middle e di robustezza contro variazioni di potenza e rumore.

Questa architettura non solo garantisce un key-rate minimo di 10 kbps su 15 km, ma offre anche rate di picco teorici di 40 kbps, rendendo il sistema una scelta ideale per applicazioni militari e governative ad alta sicurezza.

4.1 Generazione dello Shared Secret

Di seguito si riportano le fasi della generazione della chiave segreta:

1. **Generazione di coppie di fotoni entangled**
   Ogni terminale (**Alice** e **Bob**) contiene un **laser DFB** che pompa un **cristallo SPDC**, generando una coppia di fotoni entangled:
   - **Uno dei due fotoni** rimane localmente nel terminale in un optical delay line passiva
   - **L'altro viene inviato** al **nodo centrale (Charlie)**;

2. **Interferenza quantistica al nodo centrale (Charlie)**
   I due fotoni provenienti da Alice e Bob arrivano **simultaneamente** al **beam splitter di Charlie**, dove possono **interferire**;
   Due rivelatori SNSPD nel nodo centrale registrano gli eventi di **coincidenza**: se entrambi rivelano un fotone contemporaneamente, viene segnalato un evento **heralded**, che implica che **i due fotoni remoti (rimasti ad Alice e Bob)** sono ora **entangled** tra loro;

3. **Heralding: il segnale di conferma**
   Quando Charlie rileva una coincidenza valida, invia ad **Alice e Bob** un **messaggio classico**: "questo round è valido";
   Solo questi round vengono **considerati per la generazione della chiave**;

4. **Misura da parte di Alice e Bob**
   Per ogni evento heralded, che indica che i due fotoni inviati da Alice e Bob sono entangled, **Alice e Bob misurano i fotoni** che hanno trattenuto temporaneamente nell'optical delay line, in una **base scelta casualmente** (tipicamente due o tre basi diverse). Tali misure producono **bit classici (0 o 1),** ma poiché i fotoni posseduti da Alice e Bob sono correlati grazie all'entanglement, le due misurazioni produrranno gli stessi risultati con alta probabilità e pertanto entrambi avranno a disposizione una stringa di bit condivisa (il cosiddetto shared secret);

5. **Violazione della disuguaglianza di Bell**
   Alice e Bob confrontano **un sottoinsieme pubblico delle misure** per verificare la **violazione della disuguaglianza CHSH**;
   Se la violazione è significativa (es. > 5σ), la sicurezza **device-independent** è **certificata**;

6. **Sifting e correzione**
   I round in cui Alice e Bob hanno usato **basi compatibili** vengono **mantenuti**;
   Viene eseguita una **correzione di errore** per allineare i bit (classical error correction);
   Si esegue una **privacy amplification** (es. hashing universale) per **eliminare qualsiasi informazione residua** eventualmente nota a un eavesdropper;

7. **Risultato: Chiave segreta condivisa**
   Alla fine del processo:
   - Alice possiede una stringa di bit KA;
   - Bob possiede una stringa di bit KB;
   - Con **elevatissima probabilità**, KA = KB;
   - Nessun dispositivo (neanche compromesso) né un eavesdropper può conoscere questa chiave → sicurezza device-independent.

4.2 Architettura del Sistema

Ispirata al setup sperimentale proposto nell'articolo pubblica su Nature, la nostra implementazione consiste nei seguenti componenti hardware:

- Due terminali quantistici (Alice e Bob), ciascuno dotato di sorgenti SPDC, (Spontaneous Parametric Down-Conversion) per la generazione di coppie di fotoni entangled azionate da laser DFB a 1550 nm;
- Un nodo centrale (Charlie) che esegue Misure di Stati di Bell (BSM) utilizzando divisori di fascio e SNSPD (Superconducting Nanowire Single-Photon Detector) e comunica ad Alice e Bob gli eventi di entanglement annunciati con successo tramite un canale autenticato classico;
- Laser DFB a 1550 nm: sorgenti a larghezza di riga stretta utilizzate per pompare cristalli PPLN;
- Cristalli SPDC PPLN: generano coppie di fotoni entangled con elevata luminosità spettrale;
- Divisori di fascio (50:50): per il routing ottico;
- Rivelatori SNSPD con criostato integrato: posizionati esclusivamente nel nodo centrale, ottimizzati per un basso jitter (<50 ps) e un'elevata efficienza di rivelazione (>80%);
- Contatore di coincidenza (quTAG): esegue la correlazione temporale tra le rilevazioni di fotoni;
- Moduli FPGA: eseguono l'elaborazione del segnale in tempo reale e la valutazione del test di Bell;
- OTDR ed EOM: rispettivamente per la calibrazione del canale e la modulazione di fase;
- Canali Quantistici e Classici basati su fibra ottica single-mode (15 km) con attenuazione <0,2 dB/km.

Lo stack software è progettato per l'osservabilità, la gestione delle chiavi basata su API e il monitoraggio in tempo reale:

- Controllo e visualizzazione tramite Grafana e Prometheus;
- Integrazione con reti classiche tramite API RESTful e archiviazione sicura delle chiavi basata su vault;
- Valutazione dei test Bell in tempo reale e filtraggio dei dati tramite logica FPGA e post-elaborazione.

4.3 Rivelatore SNSPD

Il **rivelatore SNSPD (Superconducting Nanowire Single-Photon Detector)** è un componente chiave per il sistema DI-QKD, progettato per rilevare singoli fotoni con un'altissima efficienza e un tempo di risposta estremamente rapido. Questo tipo di rivelatore sfrutta le proprietà di superconduttività di nanofili sottilissimi (spessi pochi nanometri), generalmente realizzati in Nitrato di Niobio **(NbN)** o in Siliciuro di Molibdeno **(MoSi)**, mantenuti a temperature criogeniche inferiori ai **3 K** all'interno di un **criostato a ciclo chiuso**.

4.3.1 Caratteristiche tecniche

- **Efficienza quantistica:** >80% a lunghezza d'onda di 1550 nm (80-85% dichiarati dal produttore), garantendo un'alta probabilità di rilevare ogni fotone trasmesso;
- **Jitter temporale:** <50 picosecondi, permettendo misure estremamente precise nella sincronizzazione tra i terminali QKD;
- **Dark count rate:** inferiore a 100 Hz, riducendo al minimo i falsi positivi dovuti a rumore termico o a radiazione di fondo;
- **Tempo di reset:** inferiore a 50 ns, consentendo l'elaborazione di milioni di fotoni al secondo.

4.3.2 Vantaggi degli SNSPD rispetto ad altri rivelatori

- **Altissima efficienza:** Superiore rispetto ai rivelatori APD (Avalanche Photodiode), che solitamente non superano il 60-70% a 1550 nm;
- **Bassissimo rumore:** La ridotta dark count rate permette di distinguere con precisione i fotoni trasmessi da eventuali interferenze;
- **Precisione nella temporizzazione:** Il jitter ridottissimo consente di eseguire test di Bell e misure di entanglement con accuratezza estrema.

4.3.3 Integrazione nel sistema DI-QKD:

I rivelatori SNSPD sono presenti nel nodo centrale, permettendo di rilevare con alta precisione gli eventi di coincidenza necessari per verificare l'entanglement attraverso la misura di Bell. Inoltre, grazie alla bassa dark count rate, contribuiscono a mantenere il **Quantum Bit Error Rate (QBER)** al di sotto del 5%, garantendo la sicurezza delle chiavi generate. In sintesi, l'impiego dei rivelatori

SNSPD è essenziale per assicurare le prestazioni richieste dal sistema DI-QKD, sia in termini di efficienza che di sicurezza contro possibili intercettazioni.

4.4 Sorgenti SPDC (Spontaneous Parametric Down-Conversion)

Le sorgenti SPDC utilizzate nei terminali QKD impiegano cristalli PPLN (Periodically Poled Lithium Niobate) ottimizzati per la lunghezza d'onda di 1550 nm. Questi cristalli consentono la generazione di coppie di fotoni entangled con un rate regolabile tra 10^5 e 10^8 coppie al secondo. La scelta di operare a 1550 nm, tipica delle telecomunicazioni, è strategica per minimizzare le perdite durante la trasmissione su lunghe distanze attraverso fibra ottica, garantendo un'attenuazione inferiore a 0,2 dB/km. L'uso di filtri ottici a banda stretta permette inoltre di migliorare la purezza degli stati quantistici, riducendo la probabilità di interferenze indesiderate.

4.5 Sicurezza Quantistica: Test di Bell e Privacy Amplification

La sicurezza del sistema è basata sulla violazione della **disuguaglianza di Bell (CHSH)**, che certifica l'entanglement e impedisce qualsiasi forma di intercettazione non rilevata. Il test di Bell viene eseguito nel nodo centrale attraverso misure di coincidenza tra fotoni inviati dai terminali. Un valore della quantità S>2 conferma la sicurezza DI (Device-Independent) del sistema, indipendentemente dall'affidabilità dei dispositivi utilizzati.

Per garantire ulteriormente la sicurezza delle chiavi generate, il sistema impiega tecniche di **Privacy Amplification** basate su funzioni hash universali (come matrici di Toeplitz). Questo processo elimina ogni informazione residua che potrebbe essere stata acquisita da un potenziale attaccante, assicurando che le chiavi finali siano intrinsecamente sicure.

4.6 Scalabilità e adattabilità

L'integrazione di componenti avanzati come rivelatori SNSPD, sorgenti SPDC ottimizzate, infrastrutture di rete a bassa perdita e piattaforme di monitoraggio in tempo reale garantisce che il sistema DI-QKD proposto non solo soddisfi i requisiti minimi di sicurezza e prestazioni, ma rappresenti anche una soluzione scalabile per applicazioni governative e militari. La conformità agli standard NATO e la capacità di integrare API personalizzate assicurano inoltre che il sistema possa essere facilmente adattato a scenari operativi complessi.

4.7 Disegno del Sistema

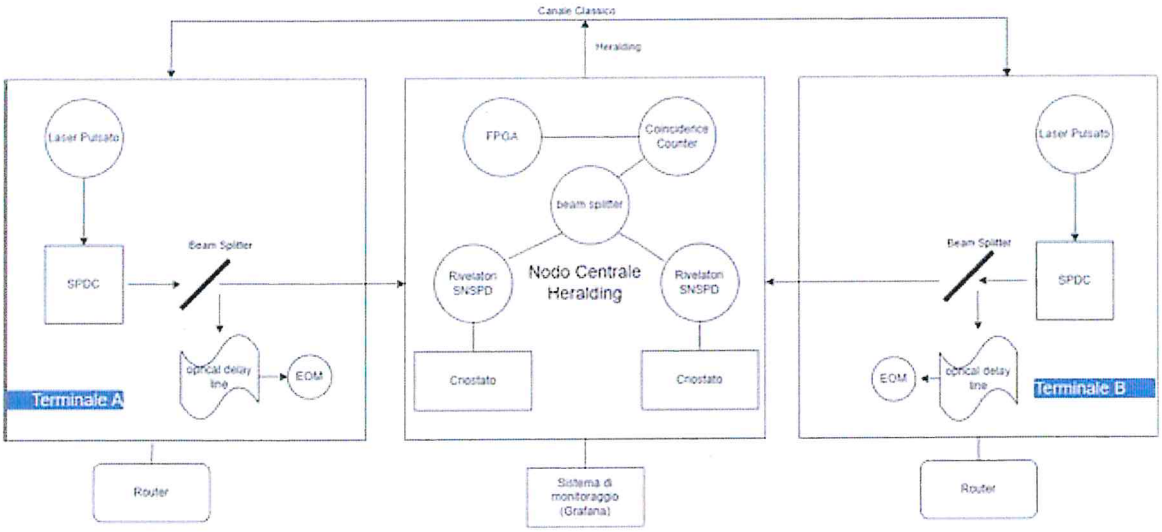

Figura 2: schema logico del sistema proposto

5 Componenti Hardware e Software Offerti

5.1 Componenti Hardware

Componente	Descrizione	Quantità
Laser DFB (1550 nm)	Potenza: 100 mW, jitter < 50 ps	4
Cristallo PPLN (SPDC a 1550 nm)	Periodically Poled Lithium Niobate	4
Rivelatori SNSPD (Superconducting) con criostato a ciclo chiuso	Efficienza >80% (80-85% dichiarati) jitter < 50 ps	4
Beam Splitter	50:50	4
Modulatori Elettro-Ottici (EOM)	Elettro-ottici per cambiamento basi	4
Computer di controllo	Tower CPU Xeon, 32 GB RAM, GPU (per calcoli rapidi)	1
OTDR (Optical Time-Domain Reflectometer)	Misura attenuazione e riflessioni	2

Componente	Descrizione	Quantità
Coincidence Counter (quTAG)	Precisione <50 ps	2
Moduli FPGA (Xilinx)	Privacy amplification + LDPC	3

5.2 Componenti Software

Software	Funzione	Fornitore
Qiskit (IBM)	Implementazione dei protocolli QKD e test di Bell	IBM
Prometheus + Grafana	Monitoraggio in tempo reale delle metriche QKD	Grafana Labs
HashiCorp Vault	Gestione sicura delle chiavi e rotazione automatica	HashiCorp
API Gateway (Kong)	Gestione e autenticazione delle API RESTful	Kong
OpenDaylight SDN	Orchestrazione dinamica dei percorsi di rete	OpenDaylight Foundation
Elastic Stack (ELK)	Analisi dei log e rilevazione di anomalie	Elastic.co
Librerie Python (Scipy, NumPy, PyQT)	Analisi dati, calcoli statistici e gestione GUI	Python.org

6 Matrice di tracciabilità

6.1 S1: Definizione casi e test

La soluzione proposta soddisfa i requisiti S1 attraverso l'implementazione di test approfonditi, inclusi:

- Test di Bell (CHSH): Per certificare l'entanglement e garantire sicurezza DI (Device-Independent);
- Test con Spia Simulata: Simulazioni di attacchi per verificare l'immunità contro eavesdropping, garantendo che il QBER rimanga sotto il 5%;
- Test di Privacy Amplification: Assicurano che le informazioni residue non possano essere sfruttate da eventuali attaccanti;
- Criteri di successo: Key-rate > 10 kbps, visibilità > 90%, S > 2 per il test di Bell.

6.2 S2: Velocità di TX

La soluzione soddisfa il requisito S2 implementando:

- Fibra ottica single-mode ITU-T G.652.D: Garantisce attenuazione <0,2 dB/km su 15 km;
- Key-rate garantito: Almeno 10 kbps tramite ottimizzazione delle sorgenti SPDC e rivelatori SNSPD;
- Test di visibilità: Misurazioni necessarie per verificare la qualità degli stati entangled.

Si rimanda al capitolo 4, dove sono forniti ulteriori dettagli sulla descrizione del sistema DI-QKD e al capitolo 7, relativo al piano di implementazione della soluzione.

6.3 S3: Integrazione sistema

Il sistema risponde a S3 attraverso:

- API RESTful personalizzabili: Per interoperabilità con infrastrutture NATO;
- Sicurezza avanzata: Compatibilità con IPsec, TLS 1.3 per gestione sicura delle chiavi;
- Monitoraggio: Integrazione con Grafana e Prometheus per dashboard personalizzate e alert;
- Il sistema sarà realizzato rispettando gli standard ETSI GS QKD 002 - 014 e le raccomandazioni ITU-T Y.3800-Y.3805 per QKD.

6.4 S4: Esecuzione test

Per soddisfare S4, verranno condotti:

- Test tra data center: Verifica di key-rate, attenuazione e robustezza in scenari operativi;
- Simulazione di attacchi avanzati: Man-in-the-middle, Photon Number Splitting per testare la sicurezza quantistica;
- Documentazione completa: Report tecnico con risultati, conformità ai requisiti e raccomandazioni.

Si rimanda al capitolo 8, dove sono forniti ulteriori dettagli in merito alla pianificazione e implementazione dei test.

6.5 S2/1: Incremento velocità di TX

Key-Rate teorico di picco:

Calcolo teorico:

- Tasso di generazione di coppie di fotoni (G): 10^5 coppie/s
- Efficienza dei rivelatori (η): 0.85
- Probabilità di coincidenza (P_c): $\eta^2 = 0.85 \times 0.85 = 0.7225$
- Key rate stimato (R): $G \times P_c = 10^5 \times 0.7225 = 72.250$ bps

Questa stima rappresenta il numero di bit di chiave segreta generati al secondo, assumendo condizioni ideali senza perdite nel canale o errori di trasmissione.

Considerando una distanza di 15 km, **il key rate netto si attesta intorno ai 40 kbps**, come riportato nel grafico seguente:

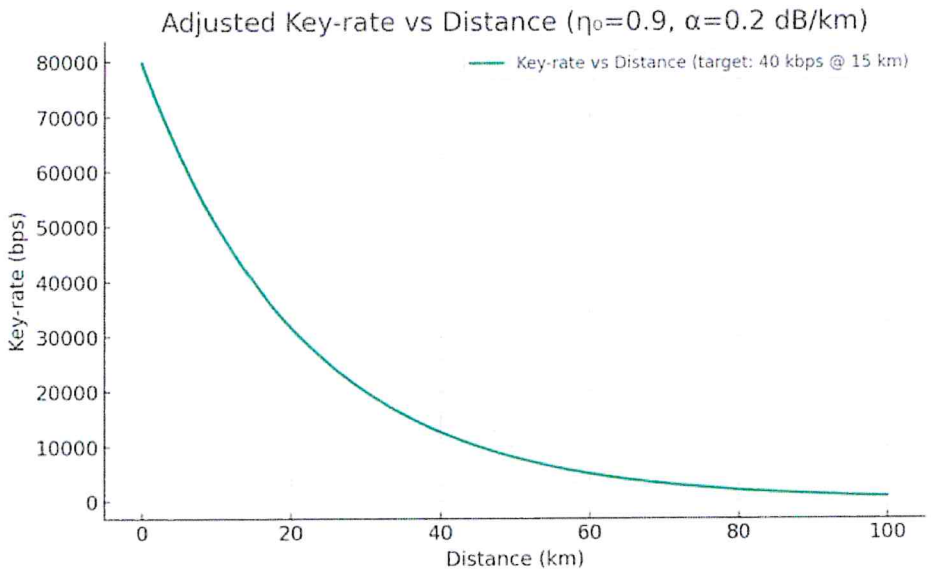

Figura 3: key-rate vs distanza

7 Piano di Implementazione

Il piano di implementazione prevede 4 fasi principali:

1. Assemblaggio e collaudo dei terminali QKD;
2. Installazione e caratterizzazione dei canali ottici nei data center;
3. Implementazione del protocollo di entanglement e test di Bell;
4. Definizione del piano test e documentazione finale.

7.1 Fase 1: Assemblaggio e Collaudo dei Terminali QKD

7.1.1 Obiettivi:

- Assemblaggio dei due terminali QKD e di un nodo centrale in rack standard 19".
- Integrazione:
  - Sistema laser pulsato (1550 nm);
  - Cristalli SPDC;

- Modulatori di luce;
- Rivelatori SNSPD in criostato;
- Computer per gestione e controllo.

7.2 Fase 2: Installazione nei Data Center e Caratterizzazione dei Canali

7.2.1 Obiettivi:

- Installazione dei terminali QKD nei data center.
- Collegamento tramite:
  - Coppia di fibre a bassissima perdita:
    - 1 fibra per comunicazioni quantistiche. (2 fibre da 7,5 km ciascuna);
    - 1 fibra per trasferimento dati convenzionale;
- Caratterizzazione:
  - Misura di attenuazione (<0,2 dB/km);
  - Test di interferenza quantistica (visibilità > 90%).

7.3 Fase 3: Protocollo di Entanglement e Test di Bell

7.3.1 Obiettivi:

- Implementazione del protocollo di distribuzione dell'entanglement.
- Esecuzione dei test di Bell:
  - Interferenza locale: Fotoni con impulsi coerenti;
  - Misure di Bell con heralding: Verifica correlazione;
- Collegamento a piattaforme di osservabilità (Observium, Grafana).

7.4 Fase 4: Piano Test, Criteri di Successo e Documentazione

7.4.1 Obiettivi:

- Definizione del piano di test finale:
  - Metriche: Key-rate, QBER (Quantum Bit Error Rate);

- Criteri di successo: Visibilità >90%, key-rate >10 kbps;

- Produzione della documentazione finale:
  - Metodi di caratterizzazione;
  - Risultati di robustezza.

8 Pianificazione dei Test

8.1 Obiettivi del Piano di Test

- Verificare la conformità della soluzione DI-QKD ai requisiti S1 - S4;
- Garantire la sicurezza quantistica contro attacchi convenzionali e quantistici;
- Validare le prestazioni (key-rate, QBER, visibilità) su 15 km di fibra ottica.

8.2 Categorie di Test

8.2.1 Test di Configurazione

Verificare l'installazione corretta dei terminali QKD e del nodo centrale.

- Test di sincronizzazione tra terminali (precisione <50 ps);
- Verifica connessioni in fibra ottica (attenuazione <0,2 dB/km);
- Configurazione API RESTful per monitoraggio remoto.

8.2.2 Test Operativi

Valutare il funzionamento sotto carico reale.

- Test di key-rate: Garantire almeno 10 kbps;
- Test di visibilità: Misura della coerenza (>90%);
- Test di Bit Error Rate (BER): Obiettivo <0,1%.

8.2.3 Test di Sicurezza

Validare la resistenza contro attacchi.

- Simulazione di attacco Man-in-the-Middle su canale classico;

- Test con spia simulata per monitoraggio del QBER;
- Test di Privacy Amplification: Validare rimozione di informazioni residue.

8.2.4 Test di Robustezza

Garantire la stabilità in condizioni critiche.

- Test di variazione di potenza dei laser (+/- 10%);
- Test di interferenza: Misura della visibilità in presenza di rumore.

8.3 Criteri di Successo

- Key-rate: >10 kbps garantito;
- QBER: <5%;
- Visibilità: >90%;
- Test di Bell (CHSH): S > 2.

8.4 Documentazione dei Risultati

- Rapporto Tecnico: Dettagli sui risultati, conformità ai requisiti e raccomandazioni;
- Dashboard Grafana: Visualizzazione delle metriche principali.

8.5 Pianificazione Temporale

Il piano di test prevede tre fasi:

- Fase 1: Configurazione e test preliminari (2 settimane);
- Fase 2: Test operativi e sicurezza (3 settimane);
- Fase 3: Test di robustezza e accettazione (2 settimane).

Alcune delle attività delle fasi sopra elencate verranno svolte in parallelo nell'ambito di cicli di verifica ed esecuzione di test, in modo che i test vengano completati nell'arco di un mese solare.

MINISTERO DELLA DIFESA
COMANDO PER LE OPERAZIONI IN RETE
PATTO DI INTEGRITA'

OGGETTO: Gara 180 – Acquisizione di studi e di un sistema prototipale relativi a un device-independent quantum key distribution (DI-QKD) per le applicazioni Difesa. CUP D87H24007090001 - Capitolo 7101 - E.F. 2025.

tra

il Comando per le Operazioni in Rete - Ufficio Amministrazione

e

la Ditta Fabaris S.p.A. (di seguito denominata Ditta), sede legale in Roma (RM), via Via Del Serafico n. 200 codice fiscale/P.IVA 00844040576, rappresentata da Antonello Gagliardi in qualità di Legale Rappresentante e Amministratore Delegato

Il presente documento deve essere obbligatoriamente sottoscritto e presentato insieme all'offerta da ciascun partecipante alla gara in oggetto. La mancata consegna del presente documento, debitamente sottoscritto, comporterà l'esclusione automatica dalla gara.

VISTO

- la legge 6 novembre 2012 n. 190, art. 1, comma 17 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- il decreto legislativo 14 marzo 2013, n. 33 avente per oggetto il "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- il decreto del Presidente della Repubblica 16 aprile 2013, n. 62 con il quale è stato emanato il "Regolamento recante il codice di comportamento dei dipendenti pubblici";
- il Protocollo d'intesa siglato tra il Ministero dell'Interno e l'Autorità Nazionale Anticorruzione il 15 luglio 2014;
- il decreto-legge 24 giugno 2014, n. 90 recante "Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari" convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114;
- il Protocollo d'intesa siglato tra il Ministero dell'Interno e l'Autorità Nazionale Anticorruzione il 15 luglio 2014;
- il "Regolamento in materia di esercizio del potere sanzionatorio dell'Autorità Nazionale Anticorruzione per l'omessa adozione dei Piani triennali di prevenzione della corruzione, dei

Antonello Gagliardi

FABARIS S.P.A.
Via del Serafico, 200
00142 Roma (Rm)
P.I. e C.F. 00844040576

Programmi triennali di trasparenza, dei Codici di comportamento" emanato dall'Autorità Nazionale Anticorruzione con delibera del 9 settembre 2014;

- il "Codice di comportamento dei dipendenti del Ministero della Difesa" approvato dal Ministro della Difesa il 22 marzo 2018;
- il Piano Nazionale Anticorruzione (P.N.A.) emanato dall'Autorità Nazionale Anticorruzione approvato con Delibera n. 1064 del 13 novembre 2019, e relativi allegati;
- il Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) 2025-2027 del Ministero della Difesa;

SI CONVIENE QUANTO SEGUE

Art. 1 - Il presente Patto d'integrità stabilisce la formale obbligazione della Ditta che, ai fini della partecipazione alla gara in oggetto, si impegna:

- a conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, a non offrire, accettare o richiedere somme di denaro o qualsiasi altra ricompensa, vantaggio o beneficio, sia direttamente che indirettamente tramite intermediari, al fine dell'assegnazione del contratto e/o al fine di distorcerne la relativa corretta esecuzione;
- a segnalare alla stazione appaltante qualsiasi tentativo di turbativa, irregolarità o distorsione nelle fasi di svolgimento della gara e/o durante l'esecuzione dei contratti, da parte di ogni interessato o addetto o di chiunque possa influenzare le decisioni relative alla gara in oggetto;
- ad assicurare che non si è accordata e non si accorderà con altri partecipanti alla gara per limitare o eludere la concorrenza e, comunque, di non trovarsi in altre situazioni ritenute incompatibili con la partecipazione alle gare dal Codice degli Appalti, dal Codice Civile o dalle altre disposizioni normative vigenti;
- ad informare puntualmente tutto il personale, di cui si avvale, del presente Patto di integrità e degli obblighi in esso contenuti;
- a vigilare affinché gli impegni sopra indicati siano osservati da tutti i collaboratori e dipendenti nell'esercizio dei compiti loro assegnati;
- a denunciare alla Pubblica Autorità competente ogni irregolarità o distorsione di cui sia venuta a conoscenza per quanto attiene l'attività di cui all'oggetto della gara in causa.

Il legale rappresentante della Ditta, inoltre, dichiara: - di non aver conferito incarichi ai soggetti di cui all'art. 53, comma 16- ter, del D.Lgs.. n. 165 del 30 marzo 2001, così come integrato dall'art. 21 del D.Lgs. 8 aprile 2013 n. 39 e di non aver stipulato contratti di lavoro subordinato o autonomo con i medesimi soggetti; - di essere consapevole che, qualora emerga la violazione del suddetto divieto verrà disposta l'immediata esclusione dalla partecipazione alla procedura di affidamento.

Art. 2 - La Ditta prende nota e accetta che nel caso di mancato rispetto degli impegni anticorruzione assunti con il presente Patto di integrità, comunque accertato dall'Amministrazione, potranno essere applicate le seguenti sanzioni:

- esclusione del concorrente dalla gara;
- escussione della cauzione di validità dell'offerta;
- risoluzione del contratto;
- escussione della cauzione di buona esecuzione del contratto;
- esclusione del concorrente dalle gare indette dalla stazione appaltante per 5 anni.

Art. 3 – Fermo restando quanto previsto dai precedenti articoli 1 e 2, in aderenza alle prescrizioni in materia di anticorruzione contenute nel d.l. 90/2014 convertito dalla l. 114/2014 e ss.mm.ii.:

- la Ditta si impegna a dare comunicazione tempestiva alla Stazione appaltante di tentativi di concussione che si siano, in qualsiasi modo, manifestati nei confronti dell'imprenditore, degli

Antonello Fabaris

FABARIS S.P.A.
Via del Serafico, 200
00142 Roma (Rm)
P.I. e C.F. 00844040576

organi sociali o dei dirigenti di impresa. Il predetto adempimento ha natura essenziale ai fini della esecuzione del contratto. Ne consegue, pertanto, che il relativo inadempimento darà luogo alla risoluzione espressa del contratto stesso, ai sensi dell'art. 1456 c.c., qualora la mancata comunicazione del tentativo di concussione subito risulti da una misura cautelare o dal disposto rinvio a giudizio, nei confronti di pubblici amministratori che abbiano esercitato funzioni relative alla stipula ed esecuzione del contratto, per il delitto previsto dall'art. 317 c.p.;

- la Stazione appaltante si impegna ad avvalersi della clausola risolutiva espressa, di cui all'art. 1456 c.c., ogni qualvolta nei confronti dell'imprenditore o dei componenti la compagine sociale, o dei dirigenti dell'impresa, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli arti. 317 c.p., 318 c.p., 319 c.p., 319-bis c.p., 319- ter c.p., 319-quater c.p., 320 c.p., 322 c.p., 322-bis c.p., 346-bis c.p., 353 c.p. e 353-bis c.p..

Nei casi di cui al presente articolo, l'esercizio della potestà risolutoria da parte della Stazione appaltante è subordinato alla previa intesa con l'Autorità Nazionale Anticorruzione. La Stazione appaltante, pertanto, comunicherà la propria volontà di avvalersi della clausola risolutiva espressa al Responsabile per la prevenzione della corruzione che ne darà comunicazione all'Autorità Nazionale Anticorruzione. Quest'ultima potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto contrattuale tra Stazione appaltante ed impresa aggiudicataria, alle condizioni di cui al d.l. 90/2014.

Art. 4 - Il contenuto del Patto di integrità e le relative sanzioni applicabili resteranno in vigore sino alla completa esecuzione del contratto. Il presente Patto dovrà essere richiamato dal contratto quale allegato allo stesso onde formarne parte integrante, sostanziale e pattizia.

Art. 5 - Il presente Patto deve essere obbligatoriamente sottoscritto in calce ed in ogni sua pagina, dal legale rappresentante della Ditta partecipante ovvero, in caso di consorzi o raggruppamenti temporanei di imprese, dal rappresentante degli stessi e deve essere presentato unitamente all'offerta. La mancata consegna di tale Patto debitamente sottoscritto comporterà l'esclusione dalla gara.

Art. 6 - Ogni controversia relativa all'interpretazione ed esecuzione del Patto d'integrità fra la Stazione appaltante ed i concorrenti e tra gli stessi concorrenti sarà risolta dall'Autorità Giudiziaria competente.

Luogo e data Roma lì, 14/05/2025

Per la Ditta:

Il legale rappresentante
(sottoscrizione digitale)

FABARIS S.P.A
Via del Serafico, 200
00142 Roma (Rm)
P.I. e C.F. 00844040576

OGGETTO: Tracciabilità dei flussi finanziari - L. 136 del 13 agosto 2010, art. 3 (GURI n. 196 del 23 agosto 2010).

DICHIARAZIONE
(ex D.P.R. N.445 del 28 dicembre 2000)

In relazione a quanto in oggetto, il sottoscritto Antonello Gagliardi, nato a Roma il 23/01/1968, residente a Roma in via Umberti Ricci n. 49, in qualità di Amministratore Delegato e Legale Rappresentante della Fabaris S.p.A., sede legale in Roma, Via del Serafico, 200 , Partita IVA/C.F.00844040576

DICHIARA

- di assumere gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3, commi 7 e 8, della legge 13 agosto 2010, n. 136;

- di assumere gli obblighi connessi con l'identificazione dei lavoratori previsti dall'art. 18, comma 1, lettera n), del D.Lgs. 81/2008, così come integrato dall'art. 5 della legge n. 136/2010.

Il C/C n. 10348897 (cod. IBAN IT34Q0200873731000010348897) della banca UNICREDIT SpA filiale di Poggio Mirteto (RI) è un conto "dedicato" ai sensi dell'Art. 3 della L. 136 del 13.08.2010 e dichiara che le persone delegate ad operare su di esso sono:

- **ANTONELLO GAGLIARDI, SIMONA SAVI, STEFANO DI ZIO.**

Il C/C n. 42129648 (cod. IBAN IT28V0538773730000042129648) della BPER di Poggio Mirteto (RI) è un conto "dedicato" ai sensi dell'Art. 3 della L. 136 del 13.08.2010 e dichiara che le persone delegate ad operare su di esso sono:

- **ANTONELLO GAGLIARDI, SIMONA SAVI, STEFANO DI ZIO.**

Il C/C n. 001614 (cod. IBAN IT10V0306973730100000001614) della banca Intesa San Paolo S.p.A. - filiale di Poggio Mirteto (RI) è un conto "dedicato" ai sensi dell'Art. 3 della L. 136 del 13.08.2010 e dichiara che le persone delegate ad operare su di esso sono:

- **ANTONELLO GAGLIARDI.**

Il C/C n. 3802 (cod. IBAN IT71Y0303203204010000003802) della banca CREDITO EMILIANO S.p.A. Roma Ag. 6, è un conto "dedicato" ai sensi dell'Art. 3 della L. 136 del 13.08.2010 e dichiara che la persona delegata ad operare su di esso è:

ANTONELLO GAGLIARDI

Fabaris S.p.A.
Socio unico
www.fabaris.it
info@fabaris.it

Sede Legale ed Operativa:
Via del Serafico, 200
00142 - Roma (RM)

Amministrazione:
Via Roma, 82
02047 - Poggio Mirteto (RI)
Tel. +39 0765.22181
Fax +39 0765.410100

P. Iva, C.F. e C.C.I.A.A. Roma: 00844040576 - Numero REA: 1204394 - Cap. Sociale: € 500.000,00 i.v. - Fatturazione Elettronica: Cod.Destinatario: W7YVJK9 - PEC: fabaris@legalmail.it
Società sottoposta all'attività di direzione e coordinamento della S3K SECURITY OF THE THIRD MILLENNIUM S.P.A. – P.Iva/Cod.Fisc. 15379561002 – N. REA RM - 15887

Il C/C n. 000000006004 (cod. IBAN IT62B0100503203000000006004) della banca BNL Gruppo BNP PARIBAS sede di Roma (RM) è un conto "dedicato" ai sensi dell'Art. 3 della L. 136 del 13.08.2010 e dichiara che la persona delegata ad operare su di esso sono:

- **ANTONELLO GAGLIARDI, STEFANO DI ZIO.**

Nome Cognome	**ANTONELLO GAGLIARDI**
Codice Fiscale	GGLNNL68A23H501S
Luogo e data di nascita	ROMA (RM) IL 23/01/1968
Residente	VIA UMBERTO RICCI N. 49 ROMA

Nome Cognome	**STEFANO DI ZIO**
Codice Fiscale	DZISFN85M17A488J
Luogo e data di nascita	ATRI (TE), IL 17/08/1985
Residente	VIA PALERMO N. 15, PESCARA (PE)

Nome Cognome	**SIMONA SAVI**
Codice Fiscale	SVASMN73C58H282B
Luogo e data di nascita	RIETI (RI), IL 18/03/1973
Residente	VIALE VERDI, 23 CAP. 02040 CANTALUPO IN SABINA (RI)

La società si impegna a comunicare all'Ente ogni eventuale variazione relativa ai predetti conti correnti e ai soggetti autorizzati ad operare su di essi.
La società accetta che l'Ente provveda alla liquidazione del corrispettivo contrattuale, a mezzo bonifico bancario sull'Istituto di credito o su Poste Italiane S.p.A. e sul numero di conto corrente dedicato indicato nella presente clausola, secondo quanto disposto dal contratto in questione, sulla base della consuntivazione dei servizi/forniture effettivamente prestati.

Roma, lì 13/05/2025

Fabaris S.p.A.

FABARIS S.P.A.
Via del Serafico, 200
00142 Roma (Rm)
P.I. e C.F. 00844040576

Fabaris S.p.A.
Socio unico
www.fabaris.it
info@fabaris.it

Sede Legale ed Operativa:
Via del Serafico, 200
00142 - Roma (RM)

Amministrazione:
Via Roma, 62
02047 - Poggio Mirteto (RI)
Tel. +39 0765 22181
Fax +39 0765 410100

RESIDENZA / RESIDENCE / DOMICILE (11)

ROMA (RM)

RESIDENZA / RESIDENCE / DOMICILE (11)

RESIDENZA / RESIDENCE / DOMICILE (11)

STATURA / HEIGHT / TAILLE (12)

178

COLORE DEGLI OCCHI / COLOUR OF EYES / COULEUR DES YEUX (13)

AZZURRI

PASSAPORTO
PASSPORT
PASSEPORT

REPUBBLICA ITALIANA
Tipo. Type. Type. Codice Paese. Code of issuing State. Code du Pays émetteur. Passaporto N. Passport No. Passeport N°.

P ITA YB2694351

Cognome. Surname. Nom. (1)
GAGLIARDI

Nome. Given Names. Prénoms. (2)
ANTONELLO

Cittadinanza. Nationality. Nationalité. (3)
ITALIANA

Data di nascita. Date of birth. Date de naissance. (4)
23 GEN/JAN 1968

Sesso. Sex. Sexe. (5) Luogo di nascita. Place of birth. Lieu de naissance. (6)
M ROMA (RM)

Data di rilascio. Date of issue. Date de délivrance. (7)
28 FEB/FEB 2018

Autorità. Authority. Autorité. (9)
MINISTRO AFFARI ESTERI
E COOPERAZIONE INTERNAZIONALE

Data di scadenza. Date of expiry. Date d'expiration. (8)
27 FEB/FEB 2028

Firma del titolare. (10)
Holder's signature / Signature du titulaire

P<ITAGAGLIARDI<<ANTONELLO<<<<<<<<<<<<<<<<<<<<

Fabaris S.p.A.
Socio unico

www.fabaris.it
info@fabaris.it

Sede Legale ed Operativa:
Via del Serafico 200
00142 - Roma (RM)

Amministrazione:
Via Roma, 62
02047 - Poggio Mirteto (RI)
Tel. +39 0765 22181
Fax. +39 0765 410100

P. Iva, C.F. e C.C.I.A.A. Roma: 00844040576 - Numero REA: 1204394 - Cap. Sociale: € 500.000,00 i.v. - Fatturazione Elettronica: Cod.Destinatario: W7YVJK9 - PEC: fabaris@legalmail.it
Società sottoposta all'attività di direzione e coordinamento della S3K SECURITY OF THE THIRD MILLENNIUM S.P.A. – P.Iva/Cod.Fisc. 15379561002 – N. REA RM - 1583?