



Allegato A1

Ven-QCI

INFRASTRUTTURA QUANTISTICA VENETA PER LA CYBER SECURITY

Regione Veneto

CAV SpA

Università degli Studi di Padova, Centro QTech*

*Padua Quantum Technologies Research Center

Progetto v.02, 14/09/2023



Sintesi documento

Nel contesto della sicurezza delle comunicazioni si è definito un progetto di rete quantistica per il Veneto con **obiettivi ambiziosi a medio-lungo termine**.

La prima fase di tale percorso è costituita dalla **realizzazione nel breve termine di una rete pilota** tra **Regione Veneto, CAV SpA e Università degli Studi di Padova** (Vsix, Neutral Access Point del Nord Est) e dall'analisi degli scenari di governance di una futura rete quantistica regionale.

I tecnici delle tre organizzazioni hanno elaborato un piano di lavoro per questa prima fase che richiede quindici mesi di attività ed un budget di c.a. 472.000€.



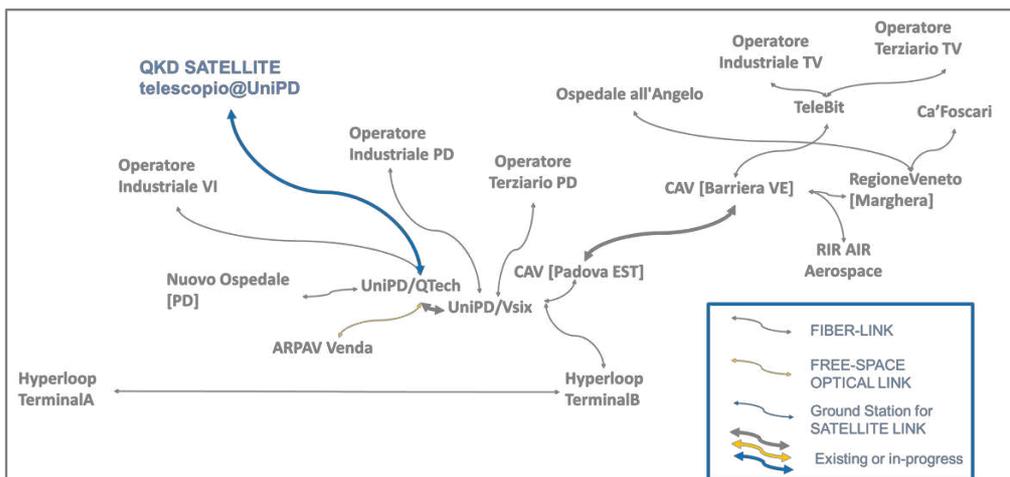
VEN-QCI: RETE QUANTISTICA VENETA per la CYBER SICUREZZA

Descrizione progetto complessivo a medio termine

Il contesto della sicurezza nelle comunicazioni costituisce un aspetto fondamentale dell'operatività di istituzioni e privati. L'atteso prossimo sviluppo di computer quantistici metterà a rischio gli attuali metodi crittografici, per i quali la sicurezza nella generazione e distribuzione di chiavi crittografiche risiede nella complessità computazionale.

Per risolvere tale criticità, l'uso di sistemi di crittografia quantistica comunemente indicati come 'distribuzione di chiave quantistica' (Quantum Key Distribution) consentirà di disporre sistemi robusti e sicuri. Nel contesto europeo sono avviati programmi per infrastrutture a terra (euroQCI, EU) integrate da costellazioni satellitari (programma SAGA, ESA). Regione Veneto intende promuovere la realizzazione di una rete per la distribuzione di chiavi quantistiche pronta a svilupparsi successivamente su scala nazionale, europea e intercontinentale. La rete costituirebbe un'infrastruttura per l'innalzamento dei livelli di cybersicurezza, partendo dalle esigenze prioritarie della parte istituzionale (Regione, Sanità) e come fattore abilitante di nuove applicazioni per industria e terziario del territorio regionale. Le maggiori criticità del progetto derivano dall'integrazione di tali nuove tecnologie nella rete esistente e dalla necessità di definire una visione consistente nel medio-lungo termine.

Il tessuto economico veneto distribuito nel territorio con le molte attività dislocate internazionalmente da un lato risulta un eccellente terreno di sviluppo e dall'altro può fare di una tale infrastruttura un fattore abilitante per la realizzazione di nuove applicazioni e opportunità imprenditoriali. Il territorio veneto vanta inoltre la presenza di importanti risorse operatori del settore, dall'Università degli studi di Padova attiva da circa vent'anni sui temi delle tecnologie quantistiche, alla presenza di operatori privati attivi nel settore cyber security e aerospazio.



Obiettivi e target di progetto a medio termine

Realizzazione rete QKD a livello regionale con il coinvolgimento pubblico e privato.

Il progetto si articola in fasi successive: realizzazione di una rete pilota e dello studio preliminare del sistema infrastruttura e sua gestione (stima dettagliata dei costi e scenari di governance); conseguente progettazione esecutiva e dispiegamento della rete di nodi regionali e collegamenti esterni extra-regionali a terra e satellitari in relazione agli sviluppi regionali, nazionali ed internazionali.

Effetti/Impatti a medio termine

Tra gli effetti/impatti attesi vi sono:

- formazione a istituzioni e privati sui temi legati alla cyber sicurezza e nuove tecnologie in prospettiva post-quantum;
- realizzazione rete, di seguito possibili kpi:
 - numero di nodi connessi (dettaglio di nodi pubblico/privato, nodi per settore merceologico);
 - numero di connessioni (a terra) con rete nazionale;
 - numero connessioni satellitari (ground-station);
 - budget k-rate (numero chiavi gestibili) complessivo regionale, per singolo collegamento, per collegamenti extra-regionali, per collegamenti satellitare;
- innalzamento dei livelli di cyber sicurezza nell'operatività ordinaria dei soggetti regionali pubbliche e delle aziende coinvolti (es. storage sicuro dei dati per Business Continuity & Disaster Recovery; es. autenticazione avanzata);
- nuove applicazioni e business model abilitati nel territorio.



Rete pilota Regione - CAV - Unipd

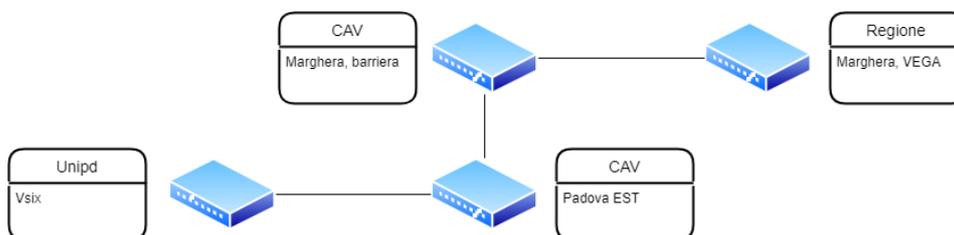
Al fine di avviare le attività e validare gli aspetti tecnico gestionali del progetto complessivo, si è ritenuto di procedere con una prima fase limitata alla realizzazione di una rete pilota tra i seguenti partner:

- Regione Veneto;
- CAV;
- Unipd.

In questa prima fase verranno affrontate tematiche tecnico gestionali quali:

- la realizzazione di una **rete pilota** per la distribuzione delle chiavi quantistiche tra i partner;
- la definizione dei **casi d'uso** di maggior interesse (utilizzo chiavi) e la messa in esercizio di un'applicazione pilota tra i partner;
- l'analisi dei possibili scenari di **governance** della rete così come ipotizzata nel progetto complessivo.

Tale fase, realizzazione rete pilota e svolgimento delle tematiche tecnico gestionali sopra descritte, è prevista della durata **15 mesi** e necessita di un **budget pari a** circa 472.000,00 euro. Realizzazione rete pilota



Nodi	Partner
1. Regione Veneto VEGA	Regione
2. CAV (Marghera)	CAV
3. CAV Padova EST	CAV
4. Unipd (Vsix)	Unipd

In relazione al collegamento Regione Veneto VEGA - CAV (Marghera) si intende utilizzare una fibra CAV, attualmente non utilizzata, che da Marghera giunge in prossimità del centro VEGA. L'ultima tratta di tale collegamento è attualmente in realizzazione da parte di CAV.

Il collegamento CAV (Marghera) - CAV (Padova EST) è presente e operativo, facente parte della rete di CAV.

Per il collegamento CAV (Padova EST) - Unipd (Vsix) si rende necessario il coinvolgimento di un operatore TLC in grado di fornire la connessione tra i due siti. Fattibilità e costi sono stati verificati e valutati attraverso una prima iterazione con operatori TLC commerciali.



Al fine di realizzare una rete pilota per la distribuzione delle chiavi quantistiche tra i partner, i nodi della rete dovranno essere opportunamente equipaggiati con sistemi quali:

- sistema QKD in trasmissione (“Alice”), di seguito indicato con **Q-TX**;
- sistema QKD in ricezione (Bob), indicato con **Q-RX**;
- Key management system per la gestione delle chiavi generate dai sistemi QKD, indicato **KMS**;
- eventuali interruttori ottici e relativo upgrade del software dei sistemi QKD (**SwitchPack**).

A. Casi d’uso

All’interno di questa prima fase si intende analizzare i possibili casi d’uso nel contesto del progetto, ovvero le diverse modalità di utilizzo delle chiavi quantistiche generate. Si cita ad esempio l’uso delle chiavi per la cifratura delle comunicazioni ai diversi livelli (layer). Tra i casi d’uso analizzati ne verranno selezionati alcuni da mettere in esercizio nella rete pilota tra i partner.

Ai fini della redazione del progetto pilota e definizione del budget preliminare, se è fatto riferimento all’implementazione di:

- cifratura (es. layer 2) mediante l’impiego di dispositivi commerciali per il collegamento Regione Veneto VEGA - CAV (Marghera);
- cifratura (es. layer 3) mediante l’impiego di dispositivi commerciali per il collegamento Regione Veneto VEGA – Vsix;
- cifratura (es. layer 2) mediante l’impiego di dispositivi commerciali per il collegamento CAV (Marghera) – CAV (Padova Est);

Essendo l’approfondimento e la definizione dei caso d’uso parte integrante del progetto, tale stima ha quindi valore indicativo.

B. Governance

Nell’ambito del progetto di sviluppo di una infrastruttura quantistica regionale si prevede di svolgere attività dedicate all’approfondimento inerente la tematica della governance dell’infrastruttura al fine di definire le condizioni per l’avvio e la gestione nella fase progettuale e per una sua sostenibilità nel tempo (crescita e consolidamento).

Gli aspetti che verranno presi in considerazione riguarderanno molteplici livelli:

1. Assetti istituzionali di proprietà e controllo dell’infrastruttura, forme giuridiche di governo. In quest’ambito si prevede inoltre di valutare e definire proposte inerenti
 - modalità di accesso e validazione di nuovi attori della rete
 - procedure per definire l’inclusione / l’ampliamento delle organizzazioni coinvolte (criteri di accesso richiesto, profilo dei richiedenti, ecc.) in relazione alla specificità della nuova infrastruttura (produzione, gestione e utilizzo delle chiavi) e in relazione alla distinzione eventuale tra fruizione del servizio vs. accesso al partenariato
 - gestione informativa per il controllo e monitoraggio dell’infrastruttura distribuita
2. Aspetti economici – coerenti con il punto 1 – connessi a
 - processi di erogazione del servizio e relativo sistema di produzione e distribuzione del valore generato (valutazione di modelli di business alternativi e processi di gestione economico-finanziaria che coniughino il contributo di ciascun membro e l’utilizzo del servizio (consumo di chiavi)).



- analisi tema non linearità del consumo risorse (chiavi) a fronte dello stesso servizio fruito
 - individuazione del supporto pubblico necessario ad avviare e mantenere l'operatività;
 - interfaccia con eventuali reti future connesse (connessione a terra, via fibra, o satellitare)
3. Aspetti tecnici inerenti la gestione dell'infrastruttura coerenti con il punto 1:
- necessità di un sistema ICT/TLC di gestione delle chiavi (*key management system*) che includa anche il monitoraggio dell'attività ovvero misure della fornitura di servizi e del consumo chiave da parte di ciascun partner (consistenti con il modello economico prescelto);

Coerentemente con la durata complessiva del progetto si prevede una durata per queste attività di 3-6 mesi (attività di analisi da svilupparsi in sinergia con la sperimentazione tecnologica). VSIX potrà contribuire a dare un supporto al gruppo di progetto per quanto attiene alle attività sopra indicate nell'ambito delle proprie competenze ed esperienze inerenti progetti di innovazione tecnologica e gestione delle infrastrutture di rete.

Responsabile delle attività in ambito governance: professoressa Eleonora Di Maria.

Effetti/Impatti progetto pilota

Tra gli effetti/impatti attesi per la fase 0:

- formazione a Regione e CAV su temi legati alla cyber sicurezza e nuove tecnologie in prospettiva post-quantum;
- realizzazione prima rete con 3 Istituzioni di rilevanza regionale :
 - numero di partner connessi: 3;
 - numero nodi: 4;
- messa in opera di casi d'uso legato alla sicurezza delle comunicazioni per i tre partners e monitoraggio attività post installazione;
- scenari di governance;
- sviluppi futuri: coinvolgimento nuovi partner pubblici e privati per fasi successive in linea con gli scenari di governance;
- scenari di estensione ad infrastrutture critiche e/o progetti strategici (collegamenti con PSN - polo strategico nazionale- , rete nazionali o europea euroQCI, progetto Hypertransfer, infrastruttura MOSE, infrastruttura Porto, infrastruttura Aeroporto/Vertiporto, tbd).

