

PLEC DE PRESCRIPCIONS TÈCNIQUES

SUBMINISTRAMENT, INSTAL·LACIÓ I ENCESA DE “QUANTUM KEY DISTRIBUTION AND KEY MANAGER SYSTEMS FOR FIELD TESTS OF QUANTUM-SECURED COMMUNICATIONS”, MITJANÇANT UN PROCEDIMENT OBERT SUBJECTE A REGULACIÓ HARMONITZADA

NÚMERO D'EXPEDIENT: 2024.SU.012

Fons

Els sistemes de distribució de claus quàntiques (QKD) i els sistemes de gestor de claus compatibles amb QKD (QC-KM) són components fonamentals per al desplegament de la infraestructura de comunicació quàntica (QCI). En particular, la comunicació segura habilitada per QKD és l'aplicació més rellevant de QCI. QKD va arribar a tal grau de maduresa que ara els dispositius clau en mà per a implementacions de camp estan disponibles comercialment, ja que són compatibles amb la infraestructura de telecomunicacions existent. Com a part del capítol espanyol de la iniciativa europea "Quantum Communication Infrastructure", es preveuen diferents demostracions de camp de comunicacions segures amb QKD a l'àrea de Barcelona. ICFO liderarà la fase d'implementació d'aquesta iniciativa i coordinarà els casos d'ús per als quals es requereixin aquests dispositius.

1. Necessitats a satisfer

Es demana el requisit dels sistemes QKD juntament amb el dispositiu Key Manager corresponent per implementar una demostració de Comunicació Segura habilitada per QKD a l'àrea de Barcelona. La demostració de camp s'ha de realitzar utilitzant dispositius comercials clau en mà que requereixin un servei de manteniment mínim durant el seu funcionament. El dispositiu ha d'adherir-se als estàndards criptogràfics (ETSI 004 i 014) que garanteixin la seva compatibilitat amb els sistemes de xifratge actuals utilitzats pels usuaris finals (és a dir, empreses, institucions públiques i privades), així com amb altres dispositius QKD. Els sistemes QKD necessaris haurien de poder funcionar utilitzant enllaços de fibra estàndard amb característiques d'atenuació específiques i proporcionar una taxa de clau prou alta per donar suport a les implementacions detallades en aquest document. Com que els llocs de desplegament dels dispositius QKD i Key manager són Data Centers, la robustesa dels dispositius, les seves característiques constitutives, l'autonomia i les condicions de funcionament acceptables han de ser compatibles amb aquest tipus d'entorn al qual no és possible accedir-hi físicament de forma recurrent.

Per tal d'implementar una prova de camp amb terminals col·locats en ubicacions reals d'usuari final, el grup d'Optoelectrònica necessitarà el sistema QKD (transmissors i receptors) juntament amb els corresponents dispositius de gestió de claus per al funcionament plug-and-play en dos escenaris (enllaç únic i node de confiança).

2. Especificacions tècniques:

Els dispositius QKD i QC-KM candidats han de complir els següents criteris:

Un sistema QKD amb sistemes KM per a QKD basat en entrellaçament amb les característiques següents:

1. El sistema hauria d'implementar un protocol de distribució de claus quàntiques (QKD) basat en BBM92 [<https://doi.org/10.1103/2FPhysRevLett.68.557>] utilitzant la polarització com a grau de llibertat.
2. El sistema hauria de permetre l'establiment de claus secretes entre dos punts utilitzant una fibra estàndard de mode únic (SMF-28), operant a la banda C. Els serveis auxiliars haurien de poder funcionar amb la mateixa fibra.
3. El sistema hauria d'incloure tots els elements necessaris per a la distribució de claus secretes (font de fotons entrellaçats, detectors, controladors...).

4. El sistema hauria de tenir la capacitat de generar claus criptogràfiques en temps real mitjançant canals de fibra òptica amb pèrdues de fins a 8 dB com a mínim. En aquesta condició d'atenuació, hauria d'oferir una taxa de clau segura per sobre de 4.000 claus segures AES-256 per hora, utilitzant paràmetres de seguretat d'última generació per als sistemes de distribució de claus quàntiques (QKD).
5. El sistema hauria de permetre l'accés a la clau generada en diferents etapes del postprocessament (clau en brut, clau tamisada, clau corregida d'errors) almenys en un mode de prova.
6. La font i els receptors del sistema QKD, així com el KM, haurien de ser totalment controlables de manera segura des d'una estació llunyana.
7. El sistema QKD ha de ser resistent a les pertorbacions mecàniques i als canvis de polarització amb temps característics de l'ordre d'un segon sobre el canal quàntic.
8. El rang de temperatura de funcionament ha d'estar entre 10°C i 40°C. Si hi ha canvis en el rendiment del dispositiu, haurien de ser inferiors al 20% per a la taxa de generació de clau segura del que s'esperava a la temperatura òptima en un canal quàntic de 8 dB.
9. La gestió de les claus i el funcionament del dispositiu s'han d'adherir als estàndards ETSI GS QKD 004/014.
10. El sistema de gestió de claus hauria de ser capaç de gestionar les claus en dos escenaris d'una manera plug-and-play: un enllaç punt a punt únic i un node de confiança.
11. Tant el transmissor com el receptor han d'encaixar en bastidors estàndard de 19", cadascun amb un volum màxim de 4U.
12. El pes de les unitats individuals no ha de ser superior a 30 kg

Els sistemes QKD i KM oferts han de complir amb les característiques esmentades anteriorment per poder ser considerats.

3. Enviament, transport

Llista de requisits essencials:

1. La proposta ha d'incloure el transport a les instal·lacions d'ICFO i tots els drets d'exportació/importació i de duana.
2. L'equip s'ha de col·locar als llocs seleccionats per ICFO. El guanyador del contracte ha de cobrir tots els costos, l'organització i la coordinació de la col·locació dels dispositius.
3. Suport per a la instal·lació i posada en marxa del sistema, inclosa la comprovació del sistema, les proves funcionals i la qualificació del procés (preferiblement en persona)

4. Enviament, transport

Cal incloure l'enviament i el transport als laboratoris del Prof. Valerio Pruneri de l'ICFO.

5. Garantia i Suport

Garantia mínima de 2 anys.

La garantia inclourà la substitució de qualsevol peça defectuosa o danyada en el moment del lliurament durant l'ús normal del sistema, independentment del fabricant dels components. Cobrirà qualsevol cost relacionat amb el desmuntatge, el transport, la reparació i el muntatge dels components danyats, inclosos tots els costos de viatge i manteniment dels enginyers de servei requerits. Una reparació in situ, o una alternativa justificada per reduir el temps d'inactivitat del sistema al mínim, sempre serà la primera opció de servei. Caldrà disposar d'un equip d'enginyers de servei degudament qualificats i qualificats.

6. MARCAT CE

7. Pressupost de licitació

- El preu objectiu és de 300.000,00 EUR (IVA exclòs).
- Condicions de pagament:
 - 30% amb l'emissió de l'ordre de compra.
 - 40% a l'entrega.
 - 30% després de la formació i acceptació de la instal·lació.

8. Hora d'entrega

Termini de lliurament màxim 16 setmanes:

- El termini de lliurament es defineix com el temps transcorregut des de la signatura del contracte fins al lliurament del sistema a les instal·lacions de l'ICFO. Inclou la fabricació del sistema, la prova d'acceptació a les instal·lacions de l'empresa i el transport.

Castelldefels, 9 de maig de 2024

Dr. Valerio Pruneri

GL Optoelectrònica