Proyecto TSI-064100-2023-0024 financiado por MTDFP / dentro del programa UNICO I+D y por la Unión Europea Next GenerationEU/ PRTR

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES DEL CONTRATO DE SUMINISTRO DE SISTEMAS DE DISTRIBUCIÓN CUÁNTICA DE CLAVES (QKD) PARA SU INTEGRACIÓN EN LA INFRAESTRUCTURA DE EXPERIMENTACIÓN SN4E+"

0. ANTECEDENTES O CONTEXTO

El objetivo de este pliego de prescripciones es definir las características técnicas particulares de los **"Sistemas de Distribución Cuántica de Claves (QKD) para su integración en la infraestructura de experimentación SN4E+"** que se deben adquirir para el proyecto denominado SN4E+ (Enhanced Smart Networks for Everything) con referencia TSI-064100-2023-0024, financiado por el Ministerio de Asuntos Económicos y Transformación Digital. La financiación proviene del programa ÚNICO I+D 6G 2023, en el marco del Plan de Recuperación, Transformación y Resiliencia, Infraestructuras de investigación y equipamiento científico-técnico.

1. OBJETO

El presente pliego tiene por objeto la definición de las características técnicas que rigen la prestación consistente en el suministro de Sistemas de distribución cuántica de claves (QKD) para su integración en la infraestructura de experimentación SN4E+. Para adecuarse a las necesidades del proyecto, este suministro se divide en dos lotes:

- LOTE 1: Sistema QKD de variable continua, de aplicación I+D, con el canal cuántico en banda C y coexistencia DWDM.
- LOTE 2: Sistema QKD de tipo MDI-QKD (Measurement Device Independent) con 2 usuarios remotos.

2. CARACTERÍSTICAS TÉCNICAS QUE DEBEN REUNIR LOS BIENES A SUMINISTRAR

2.1. REQUERIMIENTOS TÉCNICOS

LOTE 1: Sistema QKD de variable continua, de aplicación I+D, con el canal cuántico en banda C y coexistencia DWDM (R.T.L1):

- **R.T.L1.1. Volumen de suministro.**

  El suministro debe constar de un par de dispositivos QKD formado por un módulo transmisor y un módulo receptor que operen de forma conjunta para generar la clave criptográfica entre ellos mediante un protocolo de QKD. En el caso de que los dispositivos requieran de sistemas adicionales como servidores o dispositivos de red, deberán ser suministrados sin ningún coste adicional. También se deben suministrar todos los conectores y latiguillos de fibra y SFPs bidireccionales necesarios para el funcionamiento completo del sistema.

  Asimismo, se deben suministrar todos los elementos software y licencias que permitan la operación del suministro durante la vida útil del equipamiento. Los equipos deben garantizar su funcionalidad una vez finalizado el contrato, no dependiendo de licencias con vigencia limitada a la duración del contrato.

- **R.T.L1.2. Tecnología QKD.**

  El suministro de dispositivos QKD deberá ser de tecnología *prepare-and-measure*, de forma que el módulo transmisor sea el responsable de preparar los fotones y transmitirlos por el canal cuántico, y el módulo receptor se encargue de detectar los fotones y medirlos. En cuanto a la forma de generar y detectar las señales cuánticas, la tecnología que implemente el suministro debe ser basada en variable continua (CV-QKD). Además, ambos módulos deberán implementar todas las fases del protocolo para destilar la clave criptográfica secreta.

- **R.T.L1.3. Desempeño mínimo.**

  El sistema QKD debe generar una tasa mínima de clave criptográfica simétrica sin errores de 0,5kbps para una atenuación de al menos 16dB extremo a extremo, midiendo las pérdidas en banda C (1530-1565 nm). Este desempeño debe darse con una QBER adecuada y segura en función del protocolo QKD que implemente el sistema.

- **R.T.L1.4. Operación óptica.**

El canal cuántico del sistema QKD debe operar en banda C (1530-1565 nm) y deberá utilizar una única fibra óptica. Este canal debe ser sintonizable dinámicamente a cualquier longitud de onda dentro de la banda C. El canal cuántico solo deberá utilizar una fibra óptica.

Los canales clásicos auxiliares s (también llamados canales de servicio) también deben operar en banda C (1530-1565nm). El contratista podrá determinar el número de canales auxiliares necesarios para el procesado clásico del protocolo QKD, siempre que se garantice que operan dentro de la banca C. Además, el equipamiento debe tener la capacidad de copropagar el canal cuántico con otras señales clásicas en banda C, garantizando por tanto una capacidad para la coexistencia con DWDM. La transmisión del canal clásico o de post-procesado también podrá llevarse a cabo co-propagando sobre la misma fibra óptica.

- **R.T.L1.5. Gestión de claves.**

  El sistema QKD debe contar con un sistema integrado para proveer claves criptográficas de forma estandarizada (KMS), siguiendo al menos uno de los siguientes estándares de ETSI ISG QKD: ETSI GS QKD 004 o ETSI GS QKD 014.

- **R.T.L1.6. Receptores conmutables**

  El transmisor y el receptor del sistema QKD no deben estar emparejados, por lo que cualquier transmisor debe ser compatible con cualquier receptor. Eso permite desplegar topologías más complejas en el futuro como las P2MP, con un transmisor conectado a varios receptores.

- **R.T.L1.7. Monitorización y reconfiguración**

  El sistema QKD debe contar con un mecanismo de monitorización y reconfiguración estándares como interfaces informáticas (APIs), bases de datos de gestión, SNMP, SSH, REST API HTTPS, etc. Además, el sistema QKD debe permitir el acceso a varios parámetros y funcionalidades:

  - Interoperación con elementos criptográficos: KMS externos, cifradores, HSM externos, etc.
  - Acceso y configuración de parámetros QKD: ruido, correlaciones, pérdidas, tasa de generación de claves, etc.
  - Acceso a claves raw previas al post-procesado.

- **R.T.L1.8. Alimentación y condiciones de funcionamiento.**

  Todos los equipos que se suministren deben tener un diseño que permita colocarlo en racks de 19". El contratista debe suministrar todos los elementos necesarios para lograrlo, como los raíles adecuados. El sistema QKD que consiste en los equipos de emisión y transmisión deberá ocupar un máximo de 3U cada equipo. Estos equipos podrán ir acompañados de otros dos dispositivos adicionales necesarios para su funcionamiento, como servidores, que ocuparán un máximo de 1U adicional cada uno. El suministro debe poder operar en entornos industriales o profesionales. Además, los equipos deben funcionar entre 10-40ºC y de acuerdo con los estándares europeos de alimentación eléctrica.

- **R.T.L1.9. Inventario y etiquetado.**

  Todos los equipos que se suministren deben ser identificados con la información suficiente que permita su inventariado: referencia de modelo y número de serie como mínimo.

- **R.T.L1.10. Instalación, configuración y puesta en marcha.**

  El sistema QKD debe ser instalado, configurado y puesto en marcha en el emplazamiento determinado por la UPV/EHU, que estará en algunas de las tres localizaciones de la infraestructura SN4E+ (en la Escuela de Ingeniería de Bilbao (EIB); en el Centro de Fabricación Avanzada Aeronáutica (CFAA) o en el de Leioa). La instalación, configuración y puesta en marcha debe llevarse a cabo por parte del personal de la UPV/EHU sin alterar de forma significativa la funcionalidad de la infraestructura ni de otros equipos. Tras la puesta en marcha inicial, debe ser posible reubicar los equipos por parte del personal de la UPV/EHU en cualquier otra localización, por lo que se deben evitar instalar elementos que imposibiliten el traslado de los equipos.

- **R.T.L1.11. Documentación y formación.**

El sistema QKD se suministrará con toda la documentación y manuales necesarios para operar los equipos con seguridad. Esto incluirá:

- Instrucciones detalladas para la instalación y puesta en marcha de los equipos.
- Guías de uso para el correcto funcionamiento de los equipos.
- Instrucciones para reubicar los equipos de manera segura.
- Instrucciones para la reconfiguración de los equipos.

Toda la documentación estará disponible en inglés y/o castellano.

El contratista también debe impartir una formación específica en el manejo y operación de los equipos de 8 horas a 5 personas determinadas por la UPV/EHU. El formato, el calendario y los horarios se acordarán entre la UPV/EHU y el contratista para seleccionar la opción más adecuada.

- **R.T.L1.12. Garantía y asistencia técnica.**

  El contratista debe ofrecer asistencia técnica sobre el suministro durante un mínimo de DOS (2) años contando desde la recepción del mismo. Durante este periodo, la garantía comprenderá:

  - La asistencia técnica para la resolución de incidencias. Se clasificará en base al mecanismo de valoración y escalado de incidencias en 3 niveles, cumpliendo lo siguiente:
    - Respuesta inicial: máximo OCHO (8) horas hábiles tras abrir la incidencia.
    - Clasificación, diagnóstico y previsión de solución o alternativa: máximo SETENTA Y DOS (72) horas naturales tras abrir incidencia.
    - Solución o alternativa: máximo QUINCE (15) días hábiles tras abrir la incidencia, ampliables a TREINTA (30) días si se requiere envío o traslado de piezas desde o hasta el extranjero.
  - Actualización de Software: la inclusión de todas las actualizaciones necesarias para el correcto funcionamiento del equipo.

  Una vez finalizado el periodo de garantía, el equipo debe seguir completamente operativo en la versión en que se encuentre, manteniendo activas todas las funcionalidades disponibles en el momento de expiración de garantía.

LOTE 2: Sistema QKD de tipo MDI-QKD (Measurement Device Independent) con 2 usuarios remotos. (R.T.L2):

- **R.T.L2.1. Volumen de suministro.**

  El suministro debe constar de un nodo central o receptor y 2 nodos finales o emisores que operen de forma conjunta para generar la clave criptográfica entre ellos mediante un protocolo MDI-QKD en esa topología. En el caso de que los dispositivos requieran de sistemas adicionales como servidores o dispositivos de red, deberán ser suministrados sin ningún coste adicional. También se deben suministrar todos los conectores y latiguillos de fibra y SFPs bidireccionales necesarios para el funcionamiento completo del sistema.

  Asimismo, se deben suministrar todos los elementos software y licencias que permitan la operación del suministro durante la vida útil del equipamiento. Los equipos deben garantizar su funcionalidad una vez finalizado el contrato, no dependiendo de licencias con vigencia limitada a la duración del contrato.

- **R.T.L2.2. Tecnología QKD.**

  El suministro de dispositivos QKD deberá ser de tecnología independiente del dispositivo de medida o *Measurement Device Independent* (MDI-QKD). En ningún caso se entenderá como sistema MDI-QKD las asociaciones de clave que no se generen directamente de las correlaciones cuánticas y los protocolos QKD. Por ejemplo, no se entenderá como MDI-QKD el resultado de ejecutar protocolos de reenvío de clave mediante cifrado o al resultado de ejecutar algoritmos PQC. Por lo tanto, los equipos suministrados deberán implementar todas las fases del protocolo QKD para transmitir y medir fotones, así como destilar la clave criptográfica secreta.

- **R.T.L2.3. Desempeño mínimo.**

El sistema MDI-QKD debe generar una tasa mínima de clave criptográfica simétrica sin errores de 0,5kbps para una atenuación de al menos 25dB extremo a extremo sin contar el nodo central, midiendo las pérdidas en banda C (1530-1565 nm). Este desempeño debe darse con una QBER adecuada y segura en función del protocolo QKD que implemente el sistema. Este desempeño corresponde a la configuración de QKD sobre fibra oscura dedicada, sin co-propagación de canales clásicos.

- **R.T.L2.4. Operación óptica.**

  El canal cuántico del sistema QKD debe operar en banda C (1530-1565 nm). Los canales clásicos auxiliares también deben operar en banda C (1530-1565nm). Estos canales auxiliares específicos podrán acordarse entre el contratista y la UPV/EHU llegado el momento. Además, el equipamiento debe tener la capacidad de co-propagar el canal cuántico con otras señales clásicas en banda C, garantizando por tanto una capacidad para la coexistencia con DWDM. Los canales específicos de DWDM y las potencias de transmisión se acordarán con el contratista en el momento de la firma del contrato.

- **R.T.L2.5. Gestión de claves.**

  El sistema QKD debe contar con un sistema integrado para proveer claves criptográficas de forma estandarizada (KMS), siguiendo al menos uno de los siguientes estándares de ETSI ISG QKD: ETSI GS QKD 004 o ETSI GS QKD 014. Se valorará positivamente que los sistemas soporten el uso de ambos estándares.

- **R.T.L2.6. Alimentación y condiciones de funcionamiento.**

  Todos los equipos que se suministren deben tener un diseño que permita colocarlo en racks de 19". El contratista debe suministrar todos los elementos necesarios para lograrlo, como los raíles adecuados. El suministro debe poder operar en entornos industriales o profesionales. Además, los equipos deben funcionar en las condiciones típicas de temperatura y humedad de los CPDs y de acuerdo con los estándares europeos de alimentación eléctrica.

- **R.T.L2.7. Inventario y etiquetado.**

  Todos los equipos que se suministren deben ser identificados con la información suficiente que permita su inventariado: referencia de modelo y número de serie como mínimo.

- **R.T.L2.8. Instalación, configuración y puesta en marcha.**

  El sistema QKD debe ser instalado, configurado y puesto en marcha por parte del contratista en el emplazamiento determinado por la UPV/EHU, que estará en algunas de las tres localizaciones de la infraestructura SN4E+. La instalación, configuración y puesta en marcha debe llevarse a cabo sin alterar de forma significativa la funcionalidad de la infraestructura ni de otros equipos. Tras la puesta en marcha inicial, debe ser posible reubicar los equipos por parte del personal de la UPV/EHU en cualquier otra localización, por lo que se deben evitar instalar elementos que imposibiliten el traslado de los equipos.

- **R.T.L2.9. Documentación y formación.**

  El sistema QKD se suministrará con toda la documentación requerida en la normativa y con la documentación necesaria para operar los equipos con seguridad: instrucciones para reubicar los equipos, instrucciones para reconfigurar los equipos, etc. El contratista también debe impartir una formación específica en el manejo y operación de los equipos de 8 horas a 5 personas determinadas por la UPV/EHU. El formato, el calendario y los horarios se acordarán entre la UPV/EHU y el contratista para seleccionar la opción más adecuada.

- **R.T.L2.10. Garantía y asistencia técnica.**

  El contratista debe ofrecer asistencia técnica sobre el suministro durante un mínimo de DOS (2) años contando desde la recepción del mismo. Durante este periodo, la garantía comprenderá:

  - La asistencia técnica para la resolución de incidencias. Se clasificará en base al mecanismo de valoración y escalado de incidencias en 3 niveles, cumpliendo lo siguiente:
    - Respuesta inicial: máximo OCHO (8) horas hábiles tras abrir la incidencia.
    - Clasificación, diagnóstico y previsión de solución o alternativa: máximo SETENTA Y DOS (72) horas naturales tras abrir incidencia.

- Solución o alternativa: máximo QUINCE (15) días hábiles tras abrir la incidencia, ampliables a TREINTA (30) días si se requiere envío o traslado de piezas desde o hasta el extranjero.

- Actualización de Software: la inclusión de todas las actualizaciones necesarias para el correcto funcionamiento del equipo.

Una vez finalizado el periodo de garantía, el equipo debe seguir completamente operativo en la versión en que se encuentre, manteniendo activas todas las funcionalidades disponibles en el momento de expiración de garantía.



JACOB TAQUET EDUARDO JUAN - 14602834L
2025.05.19 10:29:42 +02'00'