Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
UNICO I+D 6G
Universidad del País Vasco Euskal Herriko Unibertsitatea

Proyecto *TSI-064100-2022-22* 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 CUYO OBJETO ES SISTEMA QKD DE VARIABLE DISCRETA, DE APLICACIÓN I+D Y CON EL CANAL CUÁNTICO EN BANDA C Y DETECTORES SPD EXTERNOS

---

0. ANTECEDENTES O CONTEXTO

El objetivo de este pliego de prescripciones es definir las características técnicas particulares del **"Sistema QKD de variable discreta, de aplicación I+D y con el canal cuántico en banda C y detectores SPD externos"** que se debe adquirir para el proyecto denominado SN4E (Smart Networks for Everything) con referencia TSI-064100-2022-22, financiado por el Ministerio de Asuntos Económicos y Transformación Digital. La financiación proviene del programa ÚNICO I+D 6G 2022, 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 "Sistema QKD de variable discreta, de aplicación I+D y con el canal cuántico en banda C y detectores SPD externos"

2. CARACTERÍSTICAS TÉCNICAS QUE DEBEN REUNIR LOS BIENES A SUMINISTRAR

A continuación, se describen los **requisitos técnicos de obligado cumplimiento** para los bienes a suministrar:

- **R.T.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. Además de los elementos QKD, el suministro debe incluir detectores de fotones individuales externos (*external SPD*) que podrán ser utilizados como sustituto de los detectores internos, permitiendo además la realización de experimentos docentes y de investigación. También se deben suministrar todos los conectores y latiguillos de fibra y SFPs bidireccionales necesarios para el funcionamiento completo del sistema. Los equipos se suministrarán con todos los elementos de software y licencias necesarias para su funcionamiento, garantizándose su funcionalidad una vez finalizado el contrato.

- **R.T.2. Tecnología QKD.**
  El suministro de dispositivos QKD deberá ser de tecnología *prepare-and-measure*, de forma de 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 discreta (DV-QKD). Además, ambos módulos deberán implementar todas las fases del post-procesado para destilar la clave criptográfica secreta.

- **R.T.3. Desempeño mínimo.**
  El sistema QKD debe generar una tasa mínima de clave criptográfica simétrica sin errores de 1kbps ± 1% para una atenuación de al menos 24dB extremo a extremo, midiendo las pérdidas

en banda C (1530-1565 nm). Este desempeño debe darse con una QBER adecuada y segura (inferior al 10%) en función del protocolo QKD que implemente el sistema.

- **R.T.4. Operación óptica.**
  El canal cuántico del sistema QKD debe operar en banda C (1530-1565 nm). Los canales clásicos auxiliares (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.

- **R.T.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. Además, el KMS debe soportar la funcionalidad de *trusted relay* y rutado para proveer claves entre nodos que no están directamente conectados, soportando distintas topologías y permitiendo interoperar con equipamiento de múltiples fabricantes.

- **R.T.6. Interfaces de gestión y control estandarizadas.**
  El sistema QKD debe soportar las interfaces estandarizadas de ETSI ISG QKD relativas a la gestión y el control del sistema: ETSI GS QKD 015 para el control SDN, ETSI GS QKD 018 para la orquestación y ETSI GS QKD 020 para la comunicación entre KMS interoperables.

- **R.T.7. Mecanismo de reconfiguración.**
  El sistema QKD debe contar con un mecanismo de reconfiguración estándares como interfaces informáticas (APIs), bases de datos de gestión, etc. Además, también debe contar con un mecanismo de reconfiguración preparado para las tecnologías habituales en redes SDN, como Netconf, Restconf o SNMP. Se deberá garantizar la programabilidad de la red compatible con las redes SDN. No se entenderá por SDN la mera configuración de parámetros que no permiten ajustar las prestaciones del sistema como la configuración de nombres, identificadores o direcciones IP. La programabilidad debe garantizar una reconfiguración de las prestaciones del sistema para adaptarse a diferentes casos de uso. Los parámetros y funcionalidades reconfigurables o programables son los que permiten realizar lo siguiente, y deben ser soportados por el equipamiento suministrado:

    - Interoperación con otros elementos de control de red como controladores SDN u orquestadores.
    - Interoperación con elementos criptográficos: KMS externos, cifradores, HSM externos, etc.
    - Gestión de la calidad del servicio prestado en redes en producción.
    - Acceso y configuración de parámetros QKD.
    - Acceso a claves raw previas al post-procesado.

- **R.T.8. Posibilidad de operar con detectores internos o externos.**
  El sistema QKD en su funcionamiento estándar operará utilizando detectores de fotones individuales internos (*internal SPD*). Cuando se opera de esta forma, el desempeño mínimo del sistema debe ser el indicado en el R.T.3. Sin embargo, el sistema debe permitir su funcionamiento con el uso de detectores externos (*external SPD*) que permitan nuevas funcionalidades como aumentar el control y obtener acceso a parámetros de los detectores, permitir pérdidas más altas en el enlace o probar el desempeño de otros detectores.

- **R.T.9. Detectores externos.**
  Se deben suministrar detectores de fotones individuales externos (*external SPD*) que permitan realizar una detección precisa y fiable de los fotones. El número de detectores externos dependerá de la implementación del protocolo QKD, pero se garantizará que se proporcionen tantos detectores externos como sean necesarios para su correcta implementación. La detección que realicen estos detectores debe ofrecer una alta eficiencia, bajo ruido y jitter bajo, de acuerdo a los siguientes valores:

  - Eficiencia de detección cuántica calibrable a 10%, 15%, 20%, 25%, 30% y 35%
  - Jitter máximo para la configuración de detección al 25%: 200 ps
  - Ruido bajo, cumpliendo con los siguientes "Dark Counts" máximos:
    - ‹0,8 kHz para una eficiencia del 10%
    - ‹1,5 kHz para una eficiencia del 15%
    - ‹3 kHz para una eficiencia del 20%
    - ‹6 kHz para una eficiencia del 25%

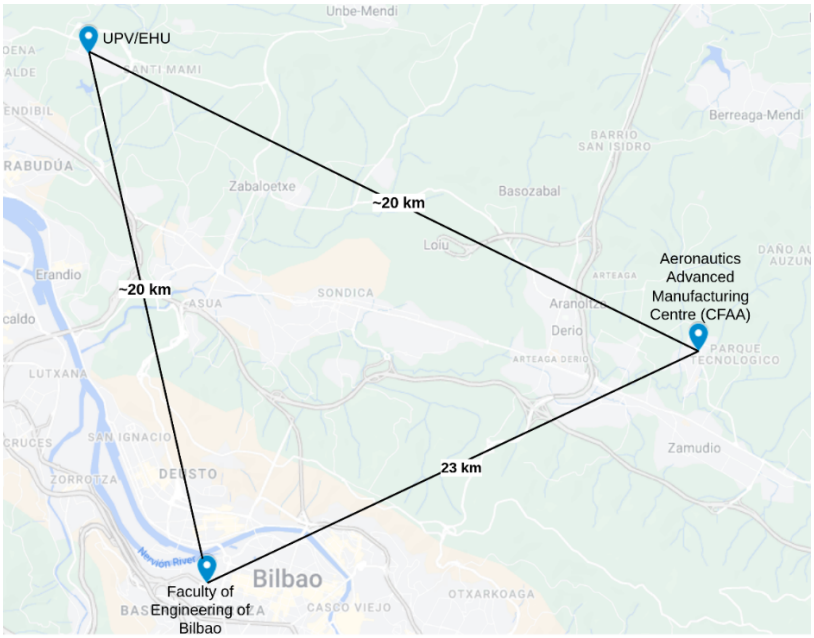
  Estos detectores podrán ser utilizados junto al sistema QKD que se suministra, como sustituto de los detectores internos que vienen integrados en el sistema. Por lo tanto, los detectores deben ser compatibles para aplicaciones de QKD. Los detectores deberán contar con una entrada para fibra óptica MMF62.5.

- **R.T.10. Alimentación y condiciones de funcionamiento.**
  Todos los equipos que se suministren, a excepción de los detectores externos, 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 deberá ocupar un máximo de 2U incluyendo todas las funcionalidades de gestión de claves. 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.

- **R.T.11. 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.12. Instalación, configuración y puesta en marcha.**
  El sistema QKD debe ser instalado, configurado y puesto en marcha en el emplazamiento que determine 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 realizarse por parte del personal de la UPV/EHU con un soporte de forma remota por parte del contratista, y 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 no se deben instalar elementos que imposibiliten el traslado de los equipos.

  Las tres posibles localizaciones de la infraestructura SN4E, así como las distancias aproximadas entre las mismas, se muestran en la siguiente figura.



- **R.T.13. 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, tanto de los QKD como de los detectores externos, de 14 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.14. Garantía y asistencia técnica.**
  El período mínimo de garantía será de TRES (3) años, contados desde la fecha del acta de recepción del suministro. Durante este período, la garantía comprenderá:
  1. La asistencia técnica para la resolución de incidencias. La Asistencia técnica se clasificará en base al mecanismo de valoración y escalado de incidencias en tres niveles, cumpliendo con los siguientes tiempos de respuesta:
     - 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 la 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.
  2. 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 ser completamente operativo en la versión en que se encuentre, manteniendo activas todas las funcionalidades disponibles en el momento de expiración de la garantía.

Firma:



Firmado digitalmente por JACOB TAQUET EDUARDO JUAN - 14602834L
Fecha: 2024.10.31 14:51:09 +01'00'