

QKDPQC - Criptografía Avanzada resistentes a ataques cuánticos (Reto 02)

Consortio: UTE Ayesa Ibermatica-ITS; i3B

Tecnología: Industria & Consumo; Quantum Computing; Ciberseguridad

Descripción general:

El objetivo principal de este proyecto es generar una plataforma de software y servicios conexos que permitan inventariar, evaluar, planificar, desplegar y validar la migración ágil de los actuales sistemas de seguridad pre-cuánticos a escenarios post-cuánticos realistas, en concreto, en un escenario industrial.

Para ello, el objetivo funcional principal es el desarrollo, integración y despliegue de un conjunto de herramientas de gestión de claves y algoritmos de resistencia cuántica para facilitar la migración a un contexto protegido de posibles ataques cuánticos. Para lograr este objetivo principal se plantean los siguientes objetivos funcionales:

- OF1. Análisis de vulnerabilidad, adaptación y parametrización de los sistemas PQC/QKD disponibles.
- OF2. Gestión de claves.
- OF3. Mecanismos criptográficos PQC/QKD.
- OF4. Despliegue híbrido, ágil y progresivo.
- OF5. Industrialización de la migración post-cuántica.

Programa: Iniciativa Estratégica de Compra Pública de Innovación (IECPI)

Duración: 34 meses (2023-2026)

Presupuesto global proyecto: 673.950,00 €

Presupuesto Grupo Ayesa: 673.950,00 €

Proyecto financiado con fondos europeos Next Generation



QKDPQC - Criptografía Avanzada resistentes a ataques cuánticos (Reto 02)

Consortio: UTE Ayesa Ibermatica-ITS; i3B

Tecnología: Industria & Consumo; Quantum Computing; Ciberseguridad

Rol de Ayesa:

La solución incluye el desarrollo de herramientas para entornos IT/OT que integren criptografía post-cuántica, QKD y sistemas híbridos, con funciones de gestión de claves, detección de anomalías y despliegue en entornos industriales y en la nube. También se contempla la virtualización de QKD para reducir la dependencia del hardware físico.

Se incorporan innovaciones como la combinación de criptografía clásica y cuántica, la virtualización de generación de claves, la adaptación de protocolos industriales y el uso de técnicas cuánticas para la detección de ataques y anomalías en tiempo real.

