Nota de prensa MWC 2025

Telefónica se adelanta a los desafíos cuánticos con una innovadora demo en el MWC

- Situada en el stand de Telefónica en el MWC, la demo 'Quantum-Safe Networks' muestra, a través de tres casos de uso, cómo Telefónica evoluciona sus redes para los retos actuales y los desafíos futuros que conlleva la computación cuántica. Lo hace de forma conjunta con partners líderes como: XRF, Idemia o Subsea Mechatronics.

- Los visitantes podrán entender cómo se puede añadir una capa extra de protección, con cifrado post-cuántico en redes privadas 5G, en un entorno altamente sensible y demandante de una latencia mínima como es la operación de un submarino ROV de vigilancia ubicado en Las Palmas de Gran Canaria que podrá ser operado en remoto desde Barcelona.

- Esta demostración también presenta las prestaciones que las tecnologías Quantum-Safe ofrecen para proteger redes públicas añadiendo una certificación extra a las eSIMs que llevan los contadores inteligentes de gas, agua o luz, preservando la privacidad y evitando las manipulaciones de los datos transferidos.

- El tercer caso de uso de la demo muestra que la criptografía post-cuántica de Telefónica refuerza la seguridad en dispositivos IoT en entornos críticos como sanidad, industria y minería a través de una solución gestionada mediante la plataforma Kite de Telefónica Tech.

Barcelona, 3 de marzo de 2025. – Telefónica presenta en el Mobile World Congress (MWC) que se celebra desde hoy hasta el jueves 6 de marzo en Barcelona una demo llamada 'Quantum-Safe Networks', una propuesta con tres casos de uso diseñada para proteger las comunicaciones y datos críticos frente a los desafíos que presenta la computación cuántica. 'Quantum-Safe Netwoks' no solo se anticipa a las amenazas futuras, sino que también refuerza la seguridad actual con una capa extra para prepararse para los retos que conllevará la irrupción de los futuros computadores cuánticos.

La computación cuántica promete revolucionar diversos sectores, lo que acelerará grandes avances en campos como la medicina o la investigación científica, entre otros, pero se prevé que también conlleve la capacidad de romper la criptografía que protege la seguridad actual. Ante esta amenaza, los actores maliciosos están intentando capturar en la actualidad datos confidenciales de larga duración, una práctica que se conoce como 'captura ahora, descifra después' (Store Now, Decrypt Later -SNDL-). En este contexto, Telefónica se adelanta a los desafíos emergentes y dota a las industrias

Telefónica, S.A.
Dirección de Comunicación Corporativa
email: prensatelefonica@telefonica.com
telefonica.com/es/sala-comunicacion/

de herramientas que no solo resuelven problemas actuales, sino que generan confianza en un futuro interconectado y protegido.

Redes privadas 5G más seguras, incluso en el mar

En la demo 'Quantum-Safe Networks' los visitantes podrán entender cómo se puede añadir una capa extra de protección, con cifrado post-cuántico en redes privadas 5G, en un entorno altamente sensible y demandante de una latencia mínima, como es la operación de un submarino de vigilancia. En concreto, se presenta un ejemplo de caso de uso de protección extra donde los usuarios que visiten el stand de Telefónica en el MWC podrán operar directamente en directo desde Barcelona a través de gafas de realidad virtual en la plataforma del partner XRF y mediante unos mandos un vehículo submarino ROV (Remotely Operated Vehicle) de Subsea Mechatronics ubicado en Las Palmas de Gran Canaria.

Este submarino será controlado en tiempo real para tareas de inspección y mantenimiento de infraestructuras, donde el usuario actuará como operario que podrá visualizar datos de telemetría mientras controla el vehículo. De esta forma, podrá comprobar que con la combinación de la conectividad 5G y el cifrado post cuántico se asegura la seguridad y la mínima latencia en el flujo de datos críticos necesarios para operaciones de mantenimiento del submarino, lográndolo incluso debajo del agua.

Redes abiertas protegidas cuánticamente

El segundo caso de uso evidencia que es necesario extender la seguridad a redes abiertas aplicando la criptografía post-cuántica en redes de utilities, como las utilizadas por contadores inteligentes de agua, gas y electricidad.

En colaboración con IDEMIA Secure Transaction, Telefónica muestra en esta demo la aplicación de tecnologías Quantum-Safe para proteger las comunicaciones móviles empleadas tanto para la provisión remota de tarjetas eSIM para los contadores como para el envío de las mediciones realizadas, preservando así la privacidad y evitando manipulaciones.

En concreto, se ha implementado una arquitectura eSIM en la que se han utilizado algoritmos Quantum-Safe para los certificados digitales que identifican al operador y para la firma del perfil eSIM que se provisiona remotamente en los contadores de una utility. Usando Crypto Agility (funcionalidad que permite cambiar la criptografía de forma ágil a medida que se identifiquen vulnerabilidades), es posible actualizar de manera remota los algoritmos Quantum-Safe para garantizar en todo momento la seguridad de las comunicaciones, especialmente importante en un entorno IoT. De este modo, no es posible suplantar al operador ni alterar el contenido de los perfiles eSIM por medios de computación cuántica, protegiendo así a la utility de un ataque que controle sus contadores o actuadores remotos.

Telefónica, S.A.
Dirección de Comunicación Corporativa
email: prensatelefonica@telefonica.com
telefonica.com/es/sala-comunicacion/

Adicionalmente, dicho perfil eSIM contiene librerías criptográficas que actualizan el sistema operativo del contador, para que a la hora de enviar datos de medición a la empresa utility, los cifre con protocolo TLS post-quantum, protegiendo así la privacidad.

Comunicaciones IoT con una capa extra de seguridad

El tercer caso de uso que muestra la demo 'Quantum-Safe Networks' en el stand de Telefónica en el MWC es el de cifrado post-cuántico aplicado a la conectividad de dispositivos IoT en entornos críticos. Como ejemplo, se muestran la comunicación entre dispositivos inteligentes de Halotech, en concreto los cascos conectados Halo I y el brazalete inteligente Halo III.

Telefónica ofrece conectividad mediante redes de bajo consumo de energía y amplio rango de cobertura, lo que garantiza una cobertura y fiabilidad óptimas incluso en zonas de difícil acceso. Toda la información crítica se cifra mediante algoritmos clásicos y post-cuánticos, mitigando así eficazmente las amenazas vigentes sobre el secreto de la información.

Esta solución de conectividad es gestionada a través de la plataforma Kite de Telefónica Tech, que permite a los usuarios monitorizar y controlar sus dispositivos en tiempo real y de forma remota desde cualquier lugar del mundo. Gracias a la incorporación de la criptografía post-cuántica, se añade además una capa extra de seguridad, protegiendo la información crítica contra futuras amenazas derivadas de la computación cuántica.

Para más información: Telefónica en el MWC 2025

Telefónica, S.A.
Dirección de Comunicación Corporativa
email: prensatelefonica@telefonica.com
telefonica.com/es/sala-comunicacion/