Telefónica anticipates quantum challenges with an innovative demo at MWC

PUBLISHED MAR 3, 2025
BY TELEFÓNICA

At Mobile World Congress (MWC), which runs from today until Thursday 6 March in Barcelona, Telefónica is presenting a demo called ‘ Quantum-Safe Networks‘, a proposal with three use cases designed to protect critical communications and data from the challenges posed by quantum computing. Quantum-Safe Networks not only anticipates future threats, but also reinforces current security with an extra layer to prepare for the challenges that will come with the emergence of future quantum computers.

Quantum computing promises to revolutionise many sectors, accelerating major advances in fields such as medicine and scientific research, but it is also expected to have the ability to break the cryptography that protects current security. Faced with this threat, malicious actors are currently trying to capture confidential data in the long term, a practice known as ‘store now, decrypt later’ (SNDL). In this context, Telefónica is anticipating new challenges and providing industries with tools that not only solve today’s problems, but also build confidence in a connected and protected future.

Safer private 5G networks, even at sea

In the ‘Quantum-Safe Networks’ demo, visitors will be able to understand how an extra layer of protection can be added with post-quantum encryption in private 5G networks in a highly sensitive environment that requires minimal latency, such as the operation of a surveillance submarine. Specifically, an example of an extra layer of protection use case will be presented where users visiting the Telefónica stand at MWC will be able to operate a Subsea Mechatronics ROV (Remotely Operated Vehicle) located in Las Palmas de Gran Canaria, live from Barcelona, through virtual reality goggles on the partner XRF platform and using a remote control.

This submarine will be controlled in real time for infrastructure inspection and maintenance tasks, with the user acting as an operator who can view telemetry data while controlling the vehicle. In this way, it will be possible to verify that the combination of 5G connectivity and post-quantum encryption ensures security and minimal latency in the flow of critical data required for submarine maintenance operations, even underwater.

Quantum-protected open networks

The second use case demonstrates the need to extend security to open networks by applying post-quantum cryptography to utility networks, such as those used by smart water, gas and electricity meters.

In this demo, Telefónica, in collaboration with IDEMIA Secure Transaction, shows the application of quantum-safe technologies to protect the mobile communications used both for the remote provisioning of eSIM cards for the meters and for the transmission of the readings taken, thus preserving privacy and preventing tampering.

Specifically, an eSIM architecture has been implemented using Quantum-Safe algorithms for the digital certificates that identify the operator and for signing the eSIM profile that is remotely deployed in a utility's meters. Thanks to Crypto Agility (a feature that allows cryptography to be changed quickly when vulnerabilities are identified), the Quantum-Safe algorithms can be updated remotely to guarantee the security of communications at all times, which is particularly important in an IoT environment. In this way, it is not possible to use quantum computing to impersonate the operator or change the content of eSIM profiles, thus protecting the utility against an attack that would allow control of its meters or remote actuators.

In addition, this eSIM profile includes cryptographic libraries that update the meter's operating system so that when meter data is sent to the utility, it is encrypted using the post-quantum TLS protocol to protect privacy.

IoT communication with an extra layer of security

The third use case demonstrated in the 'Quantum-Safe Networks' demo at the Telefónica stand at MWC is that of post-quantum encryption applied to the connectivity of IoT devices in critical

environments. An example of this is the communication between Halotech smart devices, specifically the Halo I connected helmets and the Halo III smart armband.

Telefónica offers connectivity through low power networks with wide coverage, guaranteeing optimal coverage and reliability even in areas that are difficult to access. All critical information is encrypted using classical and post-quantum algorithms, effectively mitigating current threats to information confidentiality.

This connectivity solution is managed by Telefónica Tech's Kite platform, which allows users to monitor and control their devices in real time and remotely from anywhere in the world. The incorporation of post-quantum cryptography adds an extra layer of security to protect critical information from future quantum computing threats.

Press release distributed by Wire Association on behalf of Telefónica, on Mar 3, 2025. For more information subscribe and follow us.

Media Assets

Embedded Media

Visit the online press release to interact with the embedded media.

https://wireassociation.eu/newsroom/telefonica/releases/en/telefonica-anticipates-quantum-challenges-with-an-innovative-demo-at-mwc-2399

Telefónica

Newsroom: https://wireassociation.eu/newsroom/telefonica
Website: https://www.telefonica.com/
Primary Email: contacto@fundaciontelefonica.com

Social Media

Facebook - https://www.facebook.com/telefonica
Linkedin - https://www.linkedin.com/company/telef%C3%B3nica
Twitter - https://twitter.com/telefonica/
Instagram - https://www.instagram.com/telefonica/
Youtube - https://www.youtube.com/user/telefonica