Making rapid quantum security leaps to keep Q-Day a myth

Antonella Sanguineti explains how Sparkle's efforts can avert looming threats from quantum computing

Wide-scale quantum computing could finally be on the verge of becoming more than just a distant dream. Excitement in the field has built over the past two years, as companies like Amazon, Google, IBM and Microsoft have announced developments and breakthroughs.

Many predictions have suggested we could see fully functioning quantum computers in 2030, with McKinsey & Company forecasting that faster-than-expected innovation may drive the global quantum technology market towards revenues of nearly $100 billion by 2035 and double that figure by 2040.

Among those taking a keen interest in these developments is Antonella Sanguineti, head of marketing and product management for networking, cloud, security and identity services at Sparkle. Although she points to the perils of potential hype, she believes the onset of the quantum age could come even sooner than 2030 given the rate of innovation.

"We see a lot of speed in the market in terms of investment and acceleration of quantum technology," says Sanguineti. "Big players have been active in driving that and it may arrive earlier than the end of the decade."

Antonella Sanguineti, head of marketing and product management for networking, cloud, security and identity services, Sparkle

GETTING SAFE EARLY

While quantum computing looks set to eventually deliver major benefits in industries from finance to the automotive and healthcare sectors, much of Sanguineti's interest is from the security side. With telcos and other organisations already facing a challenge to keep pace with increasingly sophisticated cyberattacks as technologies like IoT and AI proliferate, the rise of quantum computing adds an extra dimension.

Cybersecurity analysts have warned of so-called 'Q-Day', when a quantum computer powerful enough to crack widely used encryption methods arrives.

Sparkle sees itself as having a duty to provide not only a full set of security services for dealing with today's issues, but also a roadmap for averting potential new threats as a result of these quantum developments.

BIG RESPONSIBILITY

"We have a big responsibility," says Sanguineti. "It's essential that we protect customer data, provide business continuity and ensure our infrastructure is not attacked for the long term."

Sanguineti notes that much groundwork needs doing to put systems in place. "When we started investigating quantum security, we realised it's a long path – first of all, in terms of skills, and then in terms of preparation," she says.

"We want our customers to be protected today against 'store now, decrypt later' attacks, through which hackers steal data today to be able to decrypt it when quantum computers arrive. Furthermore, we want to help them in their post-quantum migration journey."

That pathway towards quantum security includes understanding all the different types of encryption methods being explored to gain comprehensive insight of the landscape. These cover the likes of post-quantum cryptography – involving the development of cryptographic algorithms – and quantum key distribution (QKD), which comprises secure sharing of cryptographic keys using quantum mechanics.

"We started with an internal skill-up, and then did lots of proofs-of-concept and technical investigations to find the best initial solution we should launch," says Sanguineti.

AUTOMATED SAFETY

The result of these efforts was Sparkle's launch last October of Quantum Safe over Internet (QSI), which offers secure VPN connectivity end-to-end between customer sites. It integrates post-quantum cryptography, cloud-based orchestration and deployment of universal CPE devices at customer premises to aid edge-based security tailored to their environments.

Sanguineti says the service is well-geared towards an operator like Sparkle, possessing an extensive 600,000km global backbone that requires protection for a huge number of customer endpoints. "QSI is a very flexible, agile solution that can scale for the enterprise market," she says.

Furthermore, the product has been fused with network-as-a-service (NaaS) from launch, giving customers the opportunity to use the service through a dedicated portal or via an API in a fully automated way. Indeed, QSI was the first product in Sparkle's new suite of NaaS services in accordance with the standards of the global Mplify Alliance. The company plans to later expand this suite to other applications, from edge devices to cloud infrastructure.

Sanguineti explains that the launch ushers in a fresh phase in Sparkle's strategy, whereby the company ultimately wants NaaS integrated with any new product, aside from being combined with existing ones.

"We wanted to start from day zero with the NaaS approach for QSI, so we combined the two innovations," says Sanguineti. "We're super-motivated about that because NaaS is something that will be needed in general for connectivity. More agility will be needed by businesses in future if, for instance, they're applying QSI to an IoT device or to agentic AI."

AWS ON BOARD

With QSI, Sanguineti believes Sparkle is at the forefront among carriers worldwide in introducing this type of commercial quantum security product at such scale. "There's been a lot of interest in the service from different players," she adds.

One of the key customers so far has been AWS, with which Sparkle announced a deal this June to make QSI available via AWS Marketplace. This has given the offering validation from a major player and interest is growing among other potential customers, with some further deals currently being finalised.

"For a company like AWS, securing everything to the very endpoint in the cloud is paramount," says Sanguineti. "It's also a big step because it enables a lot of use cases."

She points to AWS via Sparkle being selected as a preferred provider of cloud services last year in a Europe-wide framework aimed at easing cloud procurement for research and education institutions. "Being able not only to facilitate access to cloud services for such institutions, but also potentially provide robust security on top is a big plus for us," says Sanguineti.

> "It's essential that we protect customer data and provide business continuity for the long term"

'MULTI-QUANTUM' STRATEGY

But QSI is just one example of what Sparkle plans in the quantum security realm, being keen to cover a whole host of customer needs as its offering evolves over time. Last year, for instance, it also tested QKD with Telsy, a TIM Group company that operates in the security field.

"Our strategy is to be a leader in quantum protection, with a multi-quantum solution, because one lesson we have learned is that no one solution fits all," says Sanguineti. "We're adopting a step-by-step approach, whereby we'll implement one type of offering, learn, and then implement another."

Getting ahead in the realm of quantum security is also important for another reason, as it puts Sparkle in a strong position when it comes to meeting EU guidelines and regulations for security. For example, EU recommendations published in the last 18 months have urged a transition to post-quantum cryptography in member states by the early 2030s.

"Guidelines and regulations are coming in, so the solutions we put out must be agile and future-proof to meet requirements as the market matures," says Sanguineti.

She adds that different actors in the industry need to collaborate on defining standards for alignment on quantum security, ensuring services are safe for all. "The more we align on governance and ways of doing things, the better it will be," she says. "We also need to speed up as a community, considering everything that needs to be done when we're already nearing the end of 2025."

Sanguineti points to Sparkle closely following work on standards in the industry, such as those of ETSI, as well as the Mplify Alliance.

HARNESSING EXPERIENCE

Meanwhile, Sanguineti notes that the company's ability to move forward in the quantum world has been helped by Sparkle's team having a strong track record on security, giving its members invaluable experience for future realities.

"Our task has been simplified because Sparkle was advanced in security before the advent of quantum technology," she says. "This has helped in areas like designing the architecture for QSI, identifying use cases and integrating features in a virtual environment."

She highlights the company's well-established security operations centre, and services like SASE Connect and proactive DDoS protection services. Sparkle also has significant experience supporting enterprises in general, via services including SD-WAN, Cloud Connect, IP VPN and eSIM travel services.

At this early stage of the quantum security journey, Sanguineti refers to some "procrastination" in the market due to challenges in finding the right approach. That underscores the benefit of a major carrier already doing the groundwork to put foundations in place.

"The role of a service provider like Sparkle is super-important because we will have the knowledge to aid others when they need it," says Sanguineti. "We'll be there to support when the time comes."