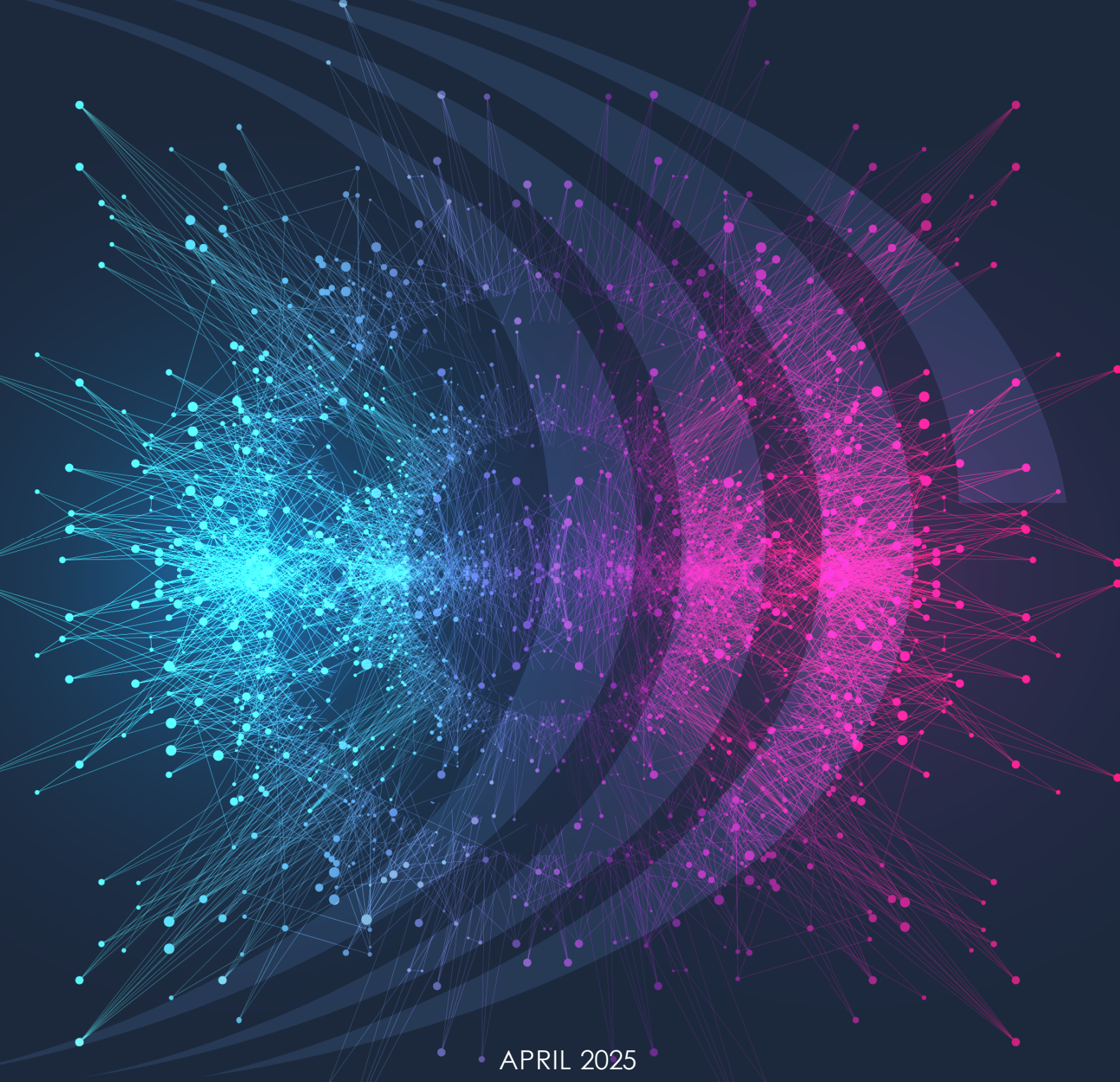


APRIL 2025

Preparing for a quantum secure future

Executive perspectives on the transition of cyber infrastructures and business practices to ensure security in the imminent quantum era

Featuring contributions from members of the Programme Committee of the 10th ETSI/IQC Quantum Safe Cryptography Conference

ETSI
The Standards People

In partnership with

IQC Institute for Quantum Computing

Introduction

The advent of large-scale quantum computing offers immense promise to science and society. Quantum computers will enable significant breakthroughs in areas from machine learning to climate modelling, drug discovery and the development of new materials. They will also accelerate better-informed decision making and risk management for financial institutions, governments and other organizations.

However this disruptive leap forward in computing capability brings with it a significant threat to our global information infrastructure.

The security and integrity of information travelling over the Internet today relies heavily on public-key cryptography. This exploits the difficulty in solving 'hard' mathematical problems, where today's classical computers are incapable of solving these problems – and decrypting the data they protect – in a timeframe that makes the interception and exploitation of this data worthwhile.

There is an existential danger that popular cryptographic schemes based on these tough problems will be easily broken by a quantum computer. This will rapidly accelerate the obsolescence of our currently deployed cryptographic techniques security systems. In turn, this will impact across every organization and industry where financial, scientific, medical, commercial, personal and governmental information needs to be kept secure.

With the advent of large-scale quantum computers, all the information transmitted on public channels using traditional cryptography will be vulnerable to eavesdropping and modification. This will remove the security properties of confidentiality and message authenticity that we rely on today to ensure the security of our information technology and systems today.

'Quantum-safe cryptography' describes efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, with the objective of keeping information assets secure even after a large-scale quantum computer has been built.

In recent years we have seen significant progress in solving the challenges of building real quantum computers. Today, it is not known when cryptographically relevant quantum computers will be available with the ability to run algorithms that can break or weaken existing cryptography.

There are already quantum-safe cryptographic solutions in existence today. These use more bandwidth or may require additional hardware, and may not solve all deployment scenarios. Nevertheless this leaves some systems still at risk from current adversaries who can intercept and store data for later decryption once a practical quantum computer becomes available at a future date – the so-called 'harvest now, decrypt later' (HNDL) scenario.

The risk posed by a large scale quantum computer is undeniable. And today we already have quantum-safe technologies that can protect against this risk. Many organizations are currently preparing for the transition to quantum secure technologies. In parallel with this, there's a corresponding acceleration in efforts to standardize tools to mitigate quantum threats.

When ETSI held the first QSC (Quantum Safe Cryptography) Conference in 2013, there were no standards available for quantum-safe cryptography. In August 2024, NIST (the National Institute of Standards and Technology) announced finalization of its principal set of three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography. Specifying key establishment and digital signature schemes, these standards are intended to resist future attacks by quantum computers that pose a threat to the security of current standards.

Meanwhile working groups at ETSI – notably our TC CYBER Working Group for QSC and Industry Specification Group on Quantum Key Distribution (QKD) – are actively exploring how ongoing standardization initiatives will fit into existing protocols, applications and public-key infrastructures.

Jointly presented by ETSI and the Institute for Quantum Computing, this report presents the personal perspectives of several notable leaders in the fields of cybersecurity, quantum computing and technology standardization.

Intended to help organizations ready themselves for a post-quantum era, it highlights a number of key themes presented by members of the Programme Committee organizing the 10th ETSI/IQC Quantum Safe Cryptography Conference held in Singapore in May 2024.

Here you'll find discussion of a number of the issues that are relevant to a broad range of stakeholders in planning their timely migration to quantum resilience. As such this report is intended to be of value to governments, regulators, academic and research communities, standards bodies, telcos, IT and cloud providers, hardware and software vendors, data holders, corporate and public sector organizations, and financial institutions.

> Standardization provides a powerful platform to consolidate fragmented global research efforts in the development of quantum-safe algorithms. It also enables associated business practices that will protect the Internet and everyone who relies on it.

Jan Ellsberger
ETSI Director-General

> Quantum computers are poised to disrupt the technology landscape. There is an urgent necessity for business leaders worldwide to prepare for the quantum era by focusing on 'resilience by design' of their critical cyber systems, and on the integrity and confidentiality of their information assets.

Professor Michele Mosca
Programme Chair and co-founder of the ETSI/IQC Quantum Safe Cryptography Conference, Institute for Quantum Computing, University of Waterloo, evolutionQ

Acknowledgements

This report has been prepared with the additional assistance of Sarah McCarthy, evolutionQ, University of Waterloo.

A conversation that's about more than technology

Donna F Dodson, Senior Strategic Advisor, evolutionQ

Cryptography underpins all our cybersecurity efforts: it is a fundamental element of what creates trust in businesses and organizations. And today there's a realization that the work we're doing in preparation for quantum readiness in our cryptographic infrastructure isn't just a technical issue. It is about people and processes, too.

We've got over the hurdle of 'is this theory, or practice?' – now we understand that we're in the engineering phase of building cryptographically relevant quantum computers.

A survey prior to the 10th ETSI/IQC QSC Conference in 2024 confirmed that more organizations than ever are thinking about what they need to do in terms of quantum readiness. However there is underlying concern that they are still not really sure what their roadmap should be looking like.

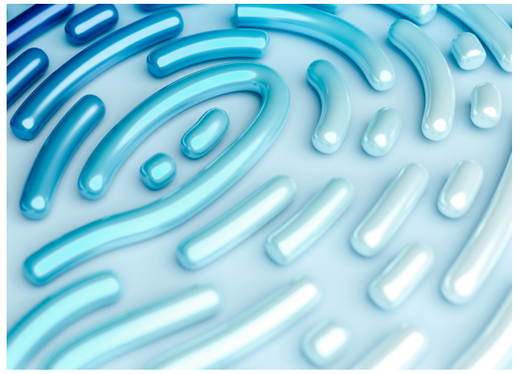
Business leaders are asking 'how can I build an agile cryptographic infrastructure that gives me the opportunity to be able to change algorithms when I need to – while ensuring I have a resilient infrastructure so I can keep my cryptographically dependent applications running, even if there's a change in the system?' This isn't just about algorithms. It is also about all the other functions and processes I need to have in place to ensure a strong cryptographic infrastructure.

This whole question around resilience also raises some other big questions for organizations planning their transition. How do I need to partner with my suppliers? How can I transition successfully with my cloud provider? What do I need to think about from a legal and regulatory perspective? How do I bring my different business units together? What kind of staff do I need to be hiring? And from a corporate perspective, how do I keep my senior leaders informed and involved?

Donna Dodson is a senior strategic advisor at evolutionQ, working with the leadership team on the strategic direction of the company to help scale their technology offerings around quantum delivery networks. Donna has an extensive background in cybersecurity, standards, risk management and cryptography. She held technical and policy leadership positions at the National Institute of Standards and Technology and the US Department of Commerce. Donna led NIST's cybersecurity programme to develop standards, guidelines, best practices and resources. She was the inaugural director of the National Cybersecurity Center of Excellence. As the Commerce Department's cybersecurity advisor, Donna counselled the Secretary and represented the department in strategic policy decision-making forums.

Know thyself – the CISO perspective

Jaya Baloo, COO, Stealth Startup AI & Cybersecurity



Even now that quantum-resistant cryptographic standards exist, the real cybersecurity task being faced by a lot of businesses is centred around some fundamentals. The first command to Chief Information Security Officers (CISOs) is 'know thyself'. As networks and systems get larger and more complex, many organizations have no real idea about the scope and scale of the challenge. Asset management and inventory understanding is already a huge challenge: and that's before you even add further cryptographic complexity to the mix and start to understand which solution you want to use.

We already struggle with understanding what we need to protect and from whom. Understanding your assets and threats is a big challenge for pretty much everyone who's working in cybersecurity right now.

Another big issue is this notion we have from a post quantum perspective of 'defence in depth' is also a challenge to people working in security. One of the main reasons companies get exploited is because they're still poor at vulnerability management. There are tools out there to scan corporate networks and figure out where potential weaknesses lie in order to be able to prioritize and remediate. But we're still not really good at habitually practicing this. It's welcome that we have regulatory requirements in place that force companies to report on their vulnerabilities, in order to understand what that posture and position is. And that's a good thing for cryptography too. Where you can see organizations are weak in this overall vulnerability understanding, it's also an indicator where they are likely to be weak from a cryptographic perspective.

It's great we now have standards and best practices. But without a vendor implementation that's native to all of the things in the landscape of a particular organization, there's a danger that migration won't happen sufficiently quickly or efficiently. Let's take an example. If you look at the big security breaches that happened in 2023, the two biggest reasons these happened were poor vulnerability management and poor multi-factor authentication (MFA). And we still don't have an adequate containment of that problem. So the biggest lessons we can learn from a post-quantum perspective are to understand your cryptographic assets, be able to construct defence in depth solutions, and have some understanding of the vendor integration of the thing that you need – that best practice – in all of your system, and to have the knowledge that it's applied ubiquitously. It's not that companies don't have MFA – it's more the case that many don't apply it properly across their entire estate.

These same practices are what CISOs and cybersecurity teams need to do with an addition of the cryptographic piece. This is really about doing more of the good practices that we already do in cybersecurity… and bringing it to bear on the post-quantum challenges that we've now got to think about as well.

Jaya Baloo is the COO of Stealth Startup AI & Cybersecurity, and has been working in the field of information security with a focus on secure network architecture for over twenty years. She is the former CSO of Rapid7, CISO of Avast, and prior to that was CISO at KPN, the largest telecommunications carrier in the Netherlands. Jaya serves on boards of the NL's National Cyber Security Centre, TIIN Capital, the NOS, and was the former Vice Chair of the EU Quantum flagship. She is also on the faculty at Singularity University.

Jaya is recognized as a top 100 global CISO and ranks among the top 100 security influencers worldwide. In 2019, she was selected as one of the 50 most inspiring women in the Netherlands by Inspiring Fifty. In 2022 she received an honorary doctorate from the University of Twente for her contributions to the field of Cybersecurity.

The value of standards: a cloud providers' viewpoint

Matthew Campagna, Chair, ETSI Technical Committee Cyber QSC, AWS

Standards, early legislation and clear migration timelines are enabling organizations to start building solutions that meet both future regulatory requirements and emerging best industry standards. Having accepted standards and adoption timelines for post-quantum cryptography enables some other important things to happen. Other downstream standards – like the protocols coming from IETF – will define how we can actually use these new NIST algorithms. And for implementers and technology providers, it gives them a framework to start building and deploying interoperable solutions for the larger ecosystem where they are doing business.

From the perspective of cloud providers you can expect them to start offering post-quantum cryptography (PQC) and hybrid key establishment mechanisms. These are where you're combining the classical key establishment methods we use today with one of the new post-quantum key encapsulation mechanisms. I think this is going to happen relatively quickly. Indeed cloud providers including AWS have been deploying these hybrid solutions in their infrastructures since 2018.

It is great that standardization work is underway that will enable customers to connect securely to the cloud. However this is only half of the story. Cloud users must also adopt these standardized tools and protocols. PQC is going to be part of the basic security offering of cloud providers to their customers as part of their shared responsibility model. This is an idea that's reflected in ETSI's technical recommendation on cloud controls. In parallel with this ETSI's QSC working group is updating its current hybrid quantum safe key exchange specifications to align with NIST's new algorithms.

We've seen recommendations from the EC for member states to adopt interoperable standardized solutions – but so far there's been less guidance on timelines for adoption. ETSI's QSC working group and Industry Specification Group on QKD are collectively addressing some of these gaps so we can get towards harmonized standards that make sense for Europe.

QKD is maturing as an important technology for specific use cases, and it will be part of security-in-depth strategies for some organizations building quantum resistant infrastructures.

There are still some engineering concerns to be addressed, but nonetheless we expect QKD to become a very important part of cloud providers' security-in-depth strategies for how they manage their own infrastructures. It may well play a less significant role for how end users connect to the cloud, which is largely over wireless and switched networks. However there are direct connection use cases for where QKD is definitely going to be a relevant security-in-depth technology.

Matthew Campagna is a Senior Principal Engineer and Cryptographer at Amazon Web Services Inc. He oversees the design and analysis of cryptographic solutions across AWS. He is a member of the ETSI Security Algorithms Group Experts (SAGE), and Chair of ETSI TC CYBER's Quantum Safe Cryptography group. Previously he managed Certicom/BlackBerry's Cryptography Research Group focused on the development of intellectual property and standardization for elliptic curve cryptography. Matt holds a doctorate in Mathematics from Wesleyan University.

Quantum computing and cryptographic risk: a strategic imperative for the financial sector

Jaime Gomez Garcia, Global Head of Quantum Threat Program, Banco Santander

Opinions expressed are those of the author and do not necessarily reflect the official view of Banco Santander.

The transition to quantum-safe cryptography is a global challenge that demands strong focus and coordination, particularly in the financial sector. Despite increasing awareness, most organizations have yet to define and resource quantum-safety projects adequately. This delay – what we call crypto-procrastination – threatens the overall migration roadmap by compressing future implementation tasks into an impractically short timeframe. Three key factors contribute to this inaction:

Underestimating the impact

Cryptography is foundational to the digital economy. Without the guarantees of confidentiality, authentication, and integrity, global business operations over untrusted networks would not be possible. Digital signatures, for example, are essential for interacting securely with governments and private organizations.

Quantum computers pose a fundamental threat to the digital economy in these distinct dimensions:

- **Confidentiality:** Encrypted financial data could be retroactively decrypted, exposing sensitive information.
- **Authentication:** Customers and organizations may no longer be able to verify their peers securely, leading to unreliable identity verification and supply chain risks.
- **Legal history:** Digital signatures could be forged, rendering digital contracts at risk retroactively.

Misunderstanding the challenges of migration

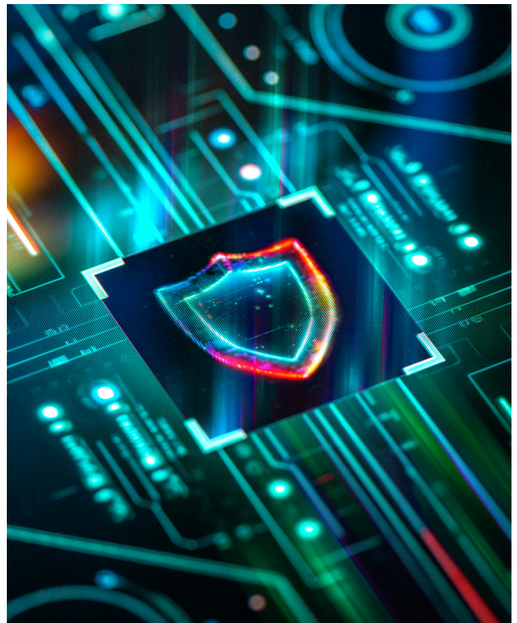
The deadline for transitioning is not determined by the arrival of a large-scale quantum computer. NIST has already signalled the phase-out of current cryptographic standards between 2030 and 2035. In the financial sector, where compliance with strict cybersecurity regulations is mandatory, these dates are effectively hard deadlines.

Historically, cryptographic transitions have been slow and complex, often taking years or even decades. The shift to quantum-safe cryptography will be also challenging, requiring years of planning and execution. Backward compatibility is particularly tough in finance, where legacy systems and diverse environments create barriers to rapid change.

Treating the quantum threat as a long-term risk

While 2024 and 2025 have seen the quantum threat included in several cybersecurity forecasts for the first time, many organizations still do not address it in their risk management frameworks. This is due to a fundamental misconception: the impact feels distant, leading to consider it a long-term risk. However, the risk response – migrating global cryptographic infrastructure – will take several years. Since the transition is a multi-year endeavour, failing to act today can cause future disruption and crisis-driven migration.

Quantum security must be treated as an emerging risk requiring immediate action. But despite growing concern among subject matter experts, many organizations still lack concrete action plans. Cybersecurity leaders are already stretched thin by other urgent priorities – ransomware threats, AI security, cost constraints – making it easy for quantum risks to fall by the wayside.



The need for a global action plan

Given the financial sector's high level of interconnectivity, a synchronized migration strategy would streamline the transition by addressing key bottlenecks, including:

- **Fragmentation:** Misaligned strategies due to organizations adopting different approaches.
- **Prolonged reliance on outdated cryptography:** The need to maintain legacy cryptography to accommodate slower adopters.
- **Duplicated effort:** Wasted resources as companies independently solve the same challenges without knowledge sharing

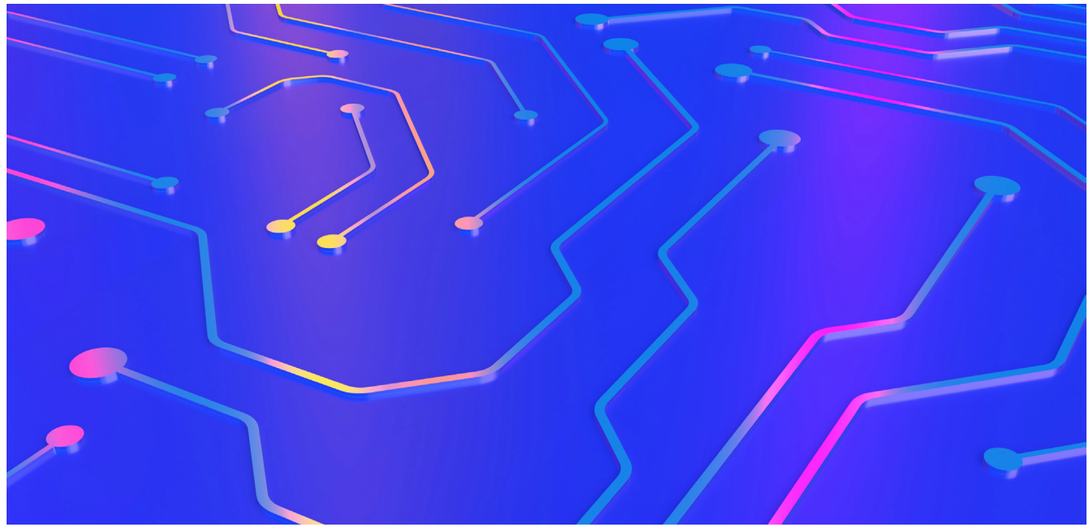
The global, interconnected and interoperable nature of the financial ecosystem sets the need for a strong global alignment in the sector at large on the priorities and timeline to implement the transition. Existing regulations, such as DORA or PCI-DSS, require organizations to prevent future challenges to cryptography. However, a global action plan is essential to prevent crypto-procrastination and ensure an orderly transition. The global financial system must act now to build a cohesive, strategic roadmap: arguably the most urgent step toward a quantum-secure economy today.

Jaime Gómez García is a recognized expert in telecommunications, blockchain, and quantum technologies, with an extensive professional background within the financial sector. His contributions as a disseminator of quantum technologies and their consequential influence on enterprises, notably within the financial domain, have garnered him recognition as a LinkedIn Top Voice and Quantum Top Voices in 2022-2024, and the 2025 Keyfactor Quantum Leap Award.

Currently, Jaime serves as the Global Head of the Santander Quantum Threat Programme, addressing the transition to a quantum-safe economy. Additionally, he holds the role of Chair of the Europol Quantum Safe Financial Forum, working to facilitate collaboration and coordinate the transition to quantum-safe cryptography within the financial sector.

Delivering certainty through standards

Colin Whorlow, Head of International Standards, National Cyber Security Centre



Members of ETSI's Quantum Safe Cryptography (QSC) Working Group have been involved on an individual basis in the NIST standardization process as co-authors of some of the candidates. The group itself has produced documents describing the algorithms which progressed to the final stages and provided security comments.

The group's wider role addresses all aspects of post-quantum cryptography other than the algorithms themselves, which is where NIST leads. Documents have been delivered on subjects including quantum-safe VPNs, hybrid key exchanges, the impact on symmetric cryptography, as well as general advice on migration.

The group has published a document on deployment considerations for hybrid security schemes. There's a big conversation at the moment around the possibility of organizations using a quantum safe algorithm, and also a classical algorithm to provide 'belt and braces' protection. Balancing the attractions of this hybrid strategy, there are other factors to consider like the additional cost and complexity of implementing such a scheme. These arguments may also have different importance in the context of different use cases and deployment scenarios.

To be ready for the post-quantum era organizations should start off by working out what encryption they're currently using by performing an inventory. NCSC advice on migration is that organizations should not rush headlong into doing something without thinking it through very carefully. It's better to go cautiously and get it right – rather than going too fast and paying the price of getting it wrong.

Colin Whorlow has worked in the UK National Cyber Security Centre (NCSC), and its predecessor CESG, for over 20 years. As Head of International Standards he has spearheaded NCSC's active involvement in global security standards work including within ETSI and 3GPP. He convened the ETSI Quantum Safe Cryptography Industry Specification Group (ISG) – now a Working Group within TC Cyber – and has also chaired the group. He also convened the ETSI ISG on Securing AI, now TC SAI. Colin was a long-time member of the Management Board of ENISA, and is a former chair of the CCRA Management Committee. In previous roles he led CESG's engagement on EU and NATO information assurance issues. Colin also chaired the Information Security Technical Working Group at the Wassenaar Arrangement for some years. Colin was awarded an OBE for services to National Security in 2024.

Standardization underpins acceleration in quantum-secure network deployments

Martin Ward, Chair, ETSI Industry Specification Group QKD, Toshiba Europe

The development of large-scale quantum computers represents a potential threat to the majority of public-key cryptography systems in use today. Complementing the security offered by post-quantum cryptographic (PQC) algorithms, Quantum Key Distribution (QKD) is a quantum-safe security technique where shared random secret keys are generated by using the quantum properties of optical signals.

QKD can be included in layered cybersecurity strategies for organizations that are looking to protect their infrastructure with truly quantum safe solutions that aren't solely reliant on public key infrastructures. Diversification with such a complimentary technique based on a fundamentally different operating principle can add protection against residual risks in post-quantum public key solutions.

Right now, there is rapid progress worldwide by telecom operators and QKD module vendors in the development, deployment and testing of QKD networks. QKD's integration with PQC can address use cases in areas including governmental, healthcare, finance and more.

China has constructed a QKD network with over 10,000 km of links, while Singapore's geography is allowing it to explore the provision of national coverage. Other countries from South Korea to the United Kingdom are trialling commercial networks. Meanwhile most EU member states have projects underway to build fibre- and satellite-based QKD networks under the EuroQCI (European Quantum Communication Infrastructure) initiative, with the eventual objective of conjoining these to build a pan-European quantum communications infrastructure.

In ETSI's Industry Specification Group (ISG) on QKD we are creating specifications to enable the development of robust security solutions to protect next-generation telecommunications. Complementing other global standardization activities, the group's work spans the development of technical specifications that variously address QKD system interfaces, implementation of security requirements and optical characterization of QKD systems and their constituent elements.

Published in 2024 and certified by BSI, the German Federal Office for Information Security, ETSI's Protection Profile (PP) for the security evaluation of QKD modules can help manufacturers submit pairs of QKD modules for evaluation under a security certification process.

A foundational step in the journey towards security certification of QKD modules, this initial Protection Profile is an important step to help certify QKD modules under the widely recognized security certification scheme of the Common Criteria for Information Technology Security Evaluation.

Martin Ward is a Senior Research Scientist at Toshiba Europe's Cambridge Research Laboratory in the UK. He has developed semiconductor quantum devices, including single and entangled photon pair sources at telecom wavelengths, and works on schemes for the security evaluation of quantum key distribution (QKD). He leads Toshiba Europe's standardization activities on quantum technologies and is Chair of ETSI's Industry Specification Group on QKD. Martin holds a doctorate in Physics from the University of Oxford.

A networking perspective

Vicente Martin, Vice Chair, ETSI Industry Specification Group QKD, Universidad Politécnica de Madrid

ETSI's Industry Specification Group on Quantum Key Distribution was created in 2008. The founding members were primarily QKD companies and research institutions developing QKD devices. Naturally, the focus was on addressing the changes of an emerging technology. At the time, more attention was given to developing the interface for extracting keys from QKD devices and to broader topics such as security, use cases, and terminology. The typical setup involved a single point-to-point link, meaning that the network aspects of QKD took a back seat.

Until a few years ago, little attention was paid to QKD network architecture. However with real networks being built and deployed, this aspect is now very important. There are currently several European projects that are focused on deploying QKD networks and the transition to quantum safe networks: things are moving quicker than ever before.

With regard to the network architecture, now we have a clear understanding of what the actual components are. And once you know those components and the relation between them, you know what the interfaces are because you know what the flow of information is. Several interfaces have been developed at ETSI, making the construction of QKD networks much easier.

Security in view of future certification is also a very active field. ETSI has developed the first protection profile for QKD, which is the first step on the ladder towards Common Criteria certification. In the broader context of transitioning to quantum safe networks, one of the research areas that's being looked at right now is hybridization of keys between QKD and post quantum algorithms. This will also need standards.

In terms of pre-standardization activity we're seeing more participation in ETSI meetings, and also in the IQC meetings, with more organizations coming including people from established companies in the networking area. We have more network manufacturers and suppliers than ever. There's also a fast growing presence from Tier-1 telcos, and we also have very good attendance from academics and research institutes.

The needs for security are quite different in each use case or application, whether you're talking about a telco, or a bank, or a hospital. With banking, for example, you could want to have a replica of their central systems, so if one fails then there's an immediate copy available so that the banking infrastructure is always working.

Contrast that with the example of healthcare, where you are essentially connecting hospitals and doing some transfer of information between them. In that instance a wait of a few seconds isn't a big problem. However, you need to think about long-term security, because the clinical history of an individual has to be secure by law during their lifetime. This requires cryptographic technology that can guarantee secrecy for a very long time, something that QKD can currently provide.

We don't know what's going to happen in the future, when we have fully developed quantum computers and people have learned to write efficient programme for them and developed new algorithms. Current quantum-resistant algorithms are robust against a quantum computer running Shor's algorithm for finding the prime factors of an integer – but we do not yet know for sure whether they will remain secure against other potential quantum-based attacks.

What these quantum-resistant algorithms do is they buy us some more time for organizations to strengthen their defences. Given the speed of advances in quantum computers and the complexity of doing an in-depth change to our current security infrastructure, transitioning to a quantum-safe network as quickly as possible is essential.

Vicente Martin is Full Professor at the Technical University of Madrid, Deputy Director of the Center of Computational Simulation, coordinates the Research Group on Quantum Information and the DIANA NATO Test Centre on Quantum Communications at Madrid, the current Madrid Quantum Communications Infrastructure and Spanish national program on quantum communications. He also works in standards on QKD as co-founder of the Industry Specification Group on Quantum Key Distribution and its Vice Chair at ETSI. Vicente is Convener of the Quantum cryptography and Communications Workgroup of the JTC-22 at CEN. His main research interest is the integration of Quantum Communications in Telecommunications Networks and security infrastructure.

In a good place: strategies for ensuring quantum readiness

Professor Michele Mosca, Programme Chair and co-founder of the ETSI/IQC Quantum Safe Cryptography Conference, Institute for Quantum Computing, University of Waterloo, evolutionQ

There's a growing acknowledgement of the need to get ready with respect to the threat timeline and the migration timeline, taking into account the shelf life of the information asset. This is the fundamental equation of quantum risk management that's being studied around the world.

We're no longer talking about a timeframe of 15 or 20 years for the quantum threat to be realized. It's within the next 5-10 years when it starts to become a significant risk for any reasonably sized organization. So we are now in the realm where it's going to be challenging for organizations to achieve readiness if they haven't started already.

From a quantum computing point of view we're in a new era. Over the last couple of years we've seen progressive acceleration in the number of well-controlled fault tolerant logical qubits. And we can expect to see this increase in pace factored into other people's risk assessments.

For the last five years or more a number of large organizations around the world have already known that they must be prepared to be safe against known quantum attacks that we can see getting steadily closer. The more daunting question, however, is 'but what about the next time?' – when we might not be so lucky to have a 10-30 year start on preparing for the next existential cybersecurity challenge posed by future advances in code breaking.

Constructing an effective defence against the cybersecurity risks posed by quantum computers represents a significant commitment of time and resources. However there are practical steps that organizations can take right now to help ensure the successful implementation of quantum-secure cryptography and mitigate the threats posed by quantum computing.

Mitigating the risks quantum computers pose to our cybersecurity infrastructure will require organizations to implement quantum-secure cryptography frameworks. Central to this are algorithms standardized by the National Institute of Standards and Technology (NIST), complemented by other encryption tools and methods – including quantum key distribution – that are being developed by ETSI and other organizations worldwide.

Cryptography is typically deeply embedded in organizations' networks and information systems with multiple dependencies, including from third parties through the supply chain. Nevertheless, there are several steps leaders can take now before in preparation for a more significant transition.

Assign responsibility. An essential first step is to nominate an individual or team, with the sufficient mandate and resources to manage quantum risk and help ensure that preparatory steps are taken.

Know what needs protecting. Creating and managing an up-to-date inventory of sensitive information assets and security tools will make it easier to take action to understand and address potential threats to your estate.

Quantify your quantum risk. Define to what extent your organization is reliant on vulnerable cryptography – and to what extent it can effectively manage this cryptography – as a guide to building awareness across the organization.

Put basic cyber hygiene first. Cryptography is just one of many protection mechanisms that modern organizations have at their disposal. Ensuring that other cybersecurity measures are in place can provide some level of protection against quantum risks now, while ensuring that these measures effectively complement cryptographic solutions.

Cryptography's crucial role as a security control in many places throughout systems in organizations, the scope of the transition will be broad and with many dependencies. It is, therefore, essential to start today.

Clear leadership at board level is needed to help executives develop and implement an effective quantum cyber strategy. This engagement should include a consistent review of meaningful key performance indicators to track progress.

Here are three transition approaches that are likely to be adopted by most organizations. The first approach may be combined with either of the other two.

1. Introduce parallel quantum solutions

Managing a parallel implementation is suitable for most organizations if they have sufficient resources. Various publicly available cryptographic algorithms are already potentially quantum-safe. Organizations can start using these solutions today in addition to existing classical cryptography, combining their powers.

There are two major benefits to this approach. First, it provides organizations with a low-barrier opportunity to experiment with implementing quantum-secure cryptography to see what expected and unexpected consequences it may have for their IT systems. This prepares them for when they eventually embark on their complete migration. Secondly, combining quantum-secure and classical cryptography offers a double-layered defence that may protect against today's and tomorrow's threats.

2. Follow a phased approach

Organizations with more complex infrastructure or resource limitations may transition in distinct phases. That means starting with migrating groups of systems to quantum-secure cryptography and having interim "cool-off" periods to define lessons learned to incorporate in the next phase.

Phase-based transformations allow for investments and milestones to be spread, which can help leaders create support for the migration throughout affected business functions due to less downtime of affected systems. In addition, the continuous adoption of lessons learned from the previous phases and new industry insights (such as developments in the standardization of quantum-secure algorithms) allows for a constant improvement of the quality of the migration.

3. Complete migration in one go

Some organizations, especially smaller or emerging ones, have smaller infrastructure deployments or have limited business needs to communicate sensitive information. These might consider a full overhaul, in which the goal is to become quantum-secure as soon as possible with the knowledge and experience that is currently at hand. Such an approach applies to projects in the early stages of development or deployment of new capabilities.

A complete 'big bang' approach can theoretically provide immediate protection and safeguard against HNDL (Harvest Now, Decrypt Later) attacks, which can be valuable for organizations that process sensitive data and may be specifically at risk of HNDL attacks. However, limited preparation and lack of intermittent learning may result in implementation challenges and hamper the longer-term utility of the solution.

Irrespective of the chosen transition scenario, organizations must act now to embrace the quantum era and confidently reap its benefits.

Quantum resilient cryptographic standards and regulatory requirements will be commonplace sooner rather than later. Digital encryption may not yet be broken today: but will your own organization be ready when it is?

For further reading:

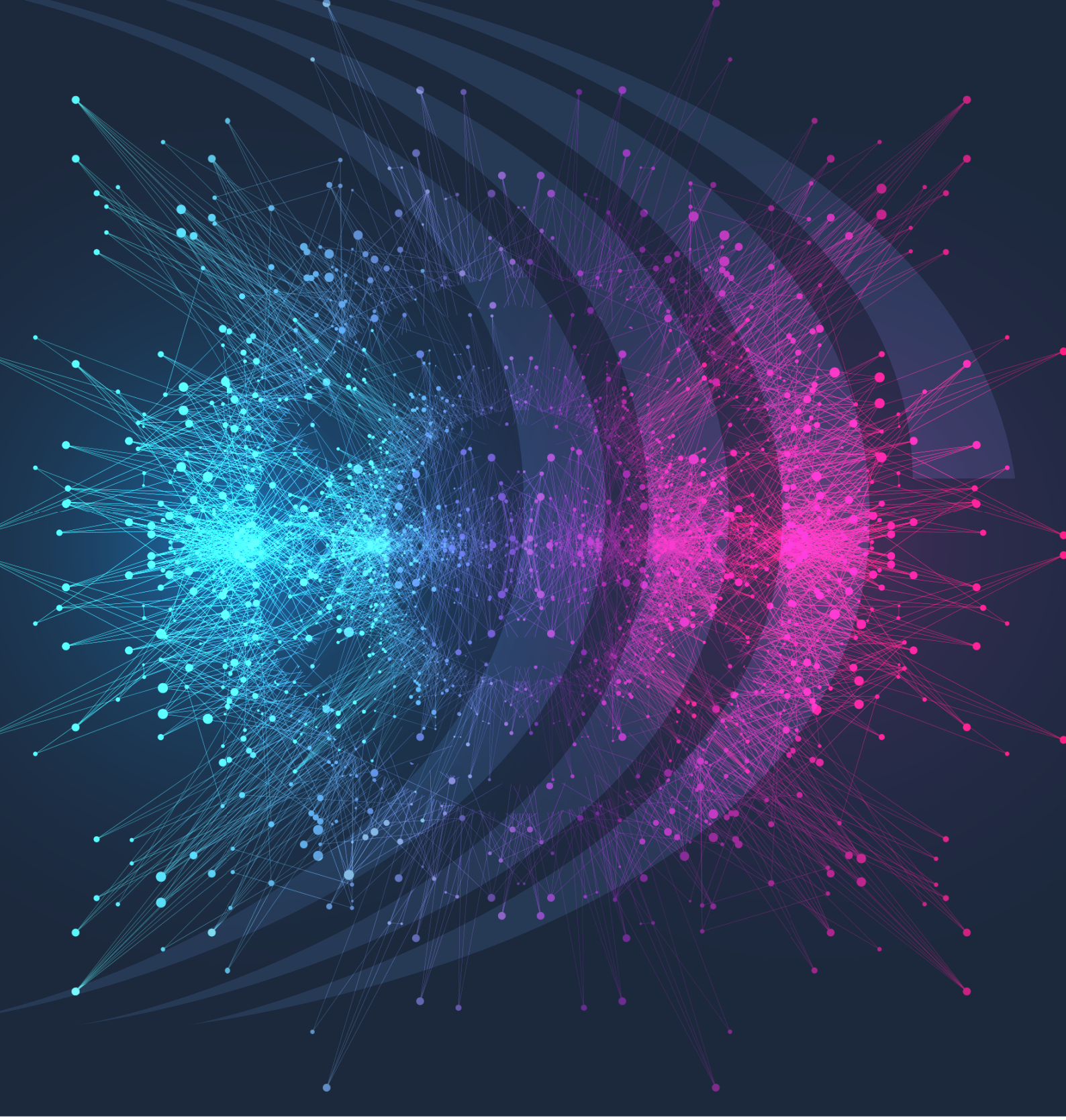
The quantum security era is coming – here's how leaders can prepare for it.

Michele Mosca is co-founder of the Institute for Quantum Computing at the University of Waterloo, a Professor in the Department of Combinatorics & Optimization of the Faculty of Mathematics, and a founding member of Waterloo's Perimeter Institute for Theoretical Physics. He is co-founder and CEO of the quantum-safe cybersecurity company, evolutionQ, and co-founder of the quantum software and applications company, softwareQ. He serves as Chair of the board of Quantum Industry Canada.

Michele started working in cryptography during his undergraduate studies and obtained his doctorate in Mathematics in 1999 from the University of Oxford on the topic of Quantum Computer Algorithms. His research interests include algorithms and software for quantum computers, and cryptographic tools designed to be safe against quantum technologies.

He co-founded the not-for-profit Quantum-Safe Canada, and the ETSI-IQC workshop series in quantum-safe cryptography and is globally recognized for his drive to help academia, industry and government prepare our cyber systems to be safe in an era with quantum computers.

Michele's awards and honours include 2010 Canada's Top 40 Under 40, Queen Elizabeth II Diamond Jubilee Medal (2013), SJU Fr. Norm Choate Lifetime Achievement Award (2017), and a Knighthood (Cavaliere) in the Order of Merit of the Italian Republic (2018).



ETSI
650 Route des Lucioles
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org

www.etsi.org

The Standards People