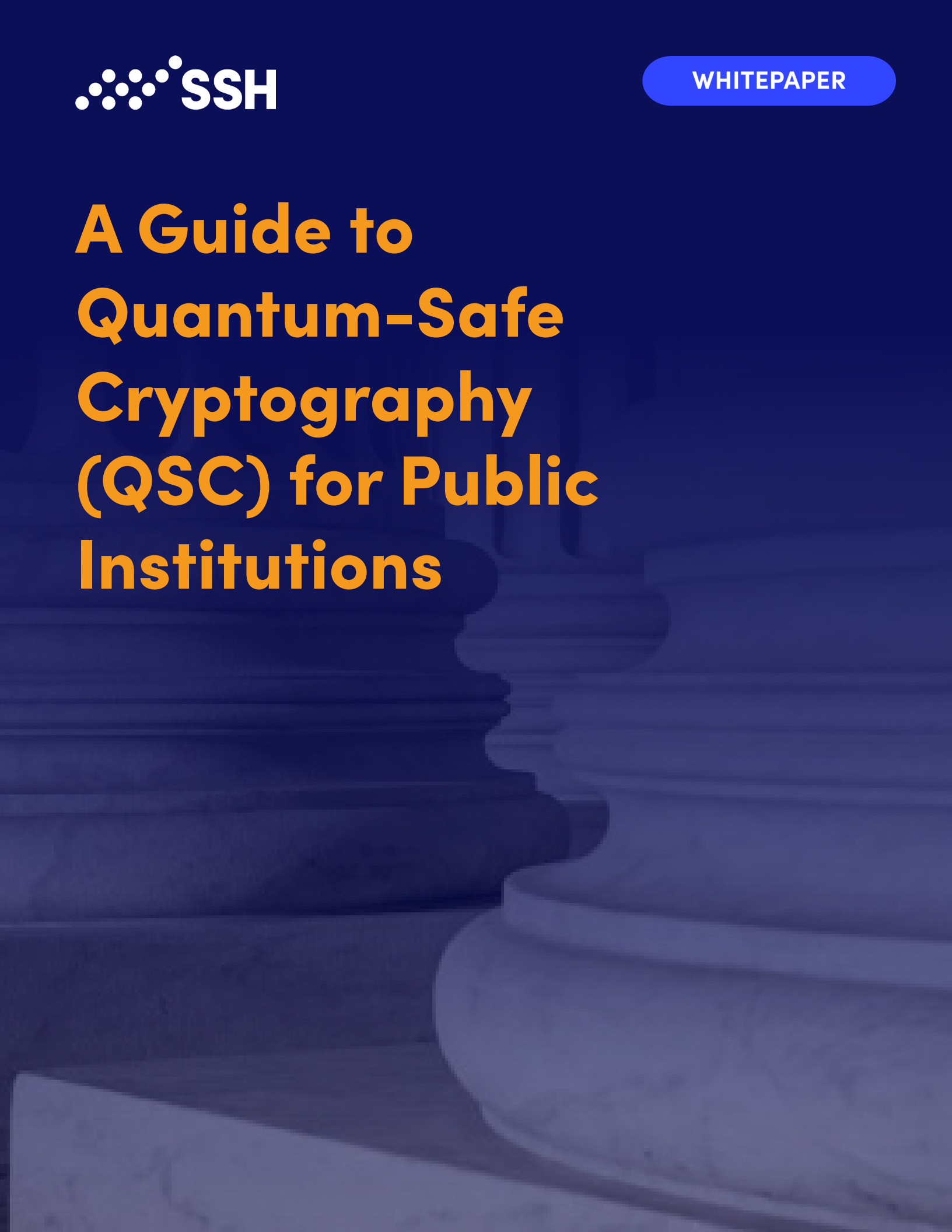
SSH

WHITEPAPER

A Guide to Quantum-Safe Cryptography (QSC) for Public Institutions



Mitigating threats and risks of quantum computing

The age of quantum computers has been looming on the horizon for some time now, and it can still take years until their large-scale use is viable. However, there are already implications, which affect every organization that handles data, and defensive actions that need to be considered.

In the 1960s, personal computers did not exist yet, but computers were already important in military and scientific use. In a similar fashion, it is likely that quantum computers will be first adopted by the military and national security organizations of various countries. It can be said that there is a virtual arms race going on with high stakes. As an example: in 2021, Biden administration announced a new strategic partnership with Australia and the UK, with the following emphasis:

"AUKUS will bring together our sailors, our scientists, and our industries to maintain and expand our edge in military capabilities and critical technologies, such as cyber, artificial intelligence, quantum technologies, and undersea domains."

At the same time, China is ramping up its quantum capability, raising fears of a "quantum gap". The response by the Biden administration is the Quantum Computing Cybersecurity Preparedness Act, which mandates all US government organizations to take defensive measures and adopt quantum-resistant cryptographic solutions as soon as possible. Other governments in the Western world already have similar initiatives, or they are likely to soon follow suit.

European Union Agency for Cybersecurity (ENISA), has published a report called 'Post-Quantum Cryptography: Anticipating Threats and Preparing the Future'. In this report, the agency outlines why Europe needs to take measures now in anticipation of the rise of quantum technology.

This white paper explores how the shift to quantum computing will affect cybersecurity in the public sector, putting special emphasis on encryption, secure file transfer, and quantum-safe algorithms. It also highlights why public institutions should start planning for the migration to quantum-safe cryptography (QSC) already today and how organizations will benefit from this move, both now and in the future.

SSH

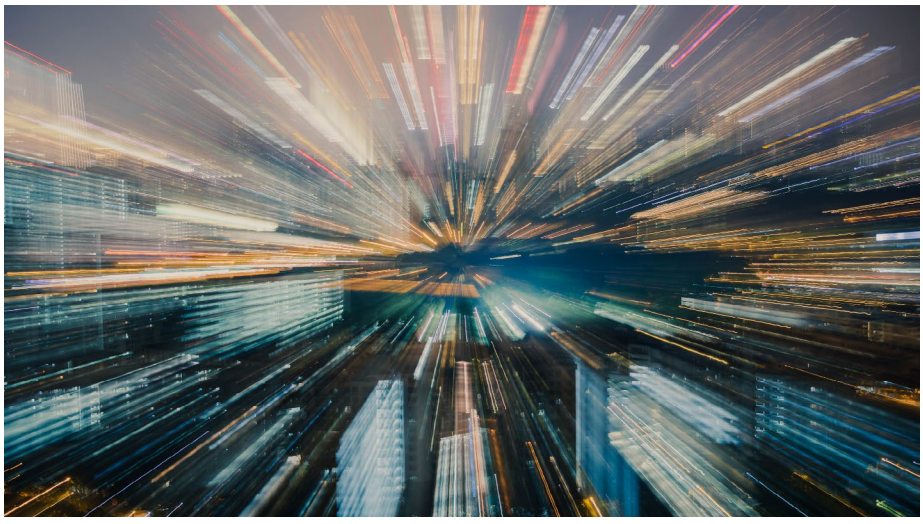
How to prevail around a virtual arms race

Cyberspace is the new “final frontier”. Cyberattacks are a method of power projection that is different from any of the more traditional forms. They can be executed extremely quickly and with extreme precision. They also make physical location completely irrelevant and can be easily covered up to claim plausible deniability. Cyberattacks have already been used as important components in the “hybrid warfare” agenda, and in all likelihood, the future will see more hostile cyberspace actions.

The advanced decryption capability provided by quantum computers will eventually add one more punch to the offensive arsenal of the hostile cyber actors. Unlike the more traditional attack vectors that exploit, for example, user credentials and privileges, quantum decryption will be able to target any data in transit that is not protected well enough.

The first hostile actors to wield the power of quantum decryption will likely be large state actors with their practically unlimited resources. However, eventually, these tools will find their way to the hands of rogue states, terrorist organizations, or criminals operating solely for profit. As an example, according to experts in Cyber Security Ventures, the annual global losses to cybercrime by 2025 might reach $10.5 trillion, making it the most profitable criminal segment – more than the illegal trade of all major drugs combined. The first potential victims will likely be government organizations and businesses, followed by vital infrastructure and economy.

We are living in a period of a constant virtual arms race, where the development of more sophisticated offensive systems requires more advanced defensive systems to be deployed. While the offensive capability can and should be left in the hands of militaries and national security organizations, maintaining defensive systems is the responsibility of every organization that handles data. Following the development of quantum computers, fortunately, there are defensive measures already in existence.



SSH

How will quantum computing break cryptography as we know it?

Encryption is a necessary component of protecting data, both in transit and at rest. For any kind of encryption to be efficient, there is a trade-off between convenience (the time and computing resources required to encrypt/decrypt) and security (the time and computing resources required to break the encryption). When processing power increases and eventually becomes commonplace, the level of encryption that was previously considered secure enough will become easier and cheaper to crack, and it will eventually need to be replaced with a more secure encryption.

So far, improving the strength of encryption has been mostly achieved by adjusting the length of the secret key used to encrypt the data, as longer keys are usually significantly harder to crack. For example, the formerly widely used 512-bit RSA is no longer used and was replaced by its 2048-bit counterpart, which should be, according to NIST, secure until 2030.

And after that, we can just add more bits, right?

Unfortunately, this is where quantum computing breaks the tried-and-true methods. The current classical encryption algorithms were devised in the 1970's, whereas the quantum computer as a concept dates back to the 1990's – because of this, there is now a fatal weakness in classical encryption algorithms.

All currently widely used encryption algorithms are vulnerable to an attack called *prime factoring*, which a powerful-enough quantum computer will do very well. While current quantum computers are too weak to perform prime factoring attack well, this will change rapidly. According to Google's CEO, Sundar Pichai, quantum cryptography will break cryptography as we know it in five to ten years from now (quote from 2021).

That still gives you five or ten years to upgrade your systems, right?

In the following sections we will outline the reasons why this isn't the case.

Confidential data at risk

1 Recording sessions for later abuse

Every organization has data that needs to remain secret or protected for a long period of time. Consider any important secret that will remain relevant for 5-10 years: health information, personal ID codes, confidential discussions, diplomatic or military secrets.

By recording and storing encrypted communications now, even if the technology is not available today, it will be possible to crack the message when the quantum processing power becomes available. In our example case, this means that the attacker can open the stash of encrypted files recorded in 2023, break the encryption, and have access to, for example, secret diplomatic correspondence. This will give the attacker the potential for blackmailing nations by threatening to divulge the information, leading to a scandal, propaganda opportunities, or threat to national security.

This process is certainly too slow for ordinary criminal groups looking for a "quick cash". However, nation states tend to play the "long game", and they certainly have the resources for these kinds of operations.

This is why the quantum threat is in fact affecting organizations now, even if it doesn't exist yet as a serious threat factor per se.

Do you have any data in your organization that will be sensitive even five to ten years in the future?

2 You don't need a quantum physicist on your team to be quantum-safe

When people talk about becoming quantum-safe, they often think about QSC (quantum-safe cryptography) and QSC algorithms. Utilizing novel quantum mechanical phenomena and requiring heavy infrastructure investment, like dedicated fiber cables, QSC sounds like science fiction. Mostly, it still is. The current QSC algorithms are not widely in use due to their prevailing technological limitations.

Eventually, QSC will be used to safeguard carefully selected data, but the prohibitive cost will make it hard to secure an entire network. Thus, most parts of your network will still be vulnerable.

In contrast, post-quantum cryptography (PQC) is not science fiction.

Utilizing existing data communication networks and protocols, PQC focuses on replacing the most vulnerable key exchange algorithms with more robust alternatives.

SSH

3 Preparation needs to start sooner than organizations typically think

Even if quantum computing may seem like a far-fetched future threat, a full-scale implementation of new technology often takes longer than companies think. Just think about the current public key cryptography infrastructure: one of the key technologies behind it, the Secure Shell protocol, was invented 27 years ago. At first, its use was rather small-scale but once the wheels started spinning, it fast became the de facto method to encrypt interactive and automated file transfers – and it still is today.

However, it has taken almost 20 years to deploy the modern public key cryptography infrastructure as we know it. Even if it would take 15-20 years for quantum computing to be a serious threat, the preparations for its arrival need to start now.

Waiting until the technology is close to implementation or reacting after it's available is already too late.

4 Post-quantum cryptography (PQC) can exist side by side with classic cryptography

Technologies to mitigate quantum risks already exist. As mentioned above, PQC can replace existing and quantum-vulnerable algorithms used in current cryptography with an upgraded version that can resist the threat posed by both classical and quantum computers. Both key agreement and digital signatures can be made quantum-safe, and PQC can be implemented in both software and hardware.

As such, PQC is an easy, fast, straightforward, and affordable response to the quantum threat, and it should be on the to-do list of every organization that handles data. It should be on a higher-priority level than any of the heavier and more expensive means (like QSC).

For example, the National Cybersecurity Center (NCSC) is a firm believer that adoption of PQC provides the most effective mitigation for the quantum computing threat right now. Additionally, the Department of Homeland Security (DHS) also recommends the co-existence of classical and PQC algorithms.

Making future-proof encryption easy with quantum-safe communications

The vast majority of organizations, probably including yours, are already using the SSH or SFTP protocols for secure communications or running mainframe communications.

If so, then you are in luck, as SSH launched the Tectia Quantum-Safe family for secure communications.

SSH's Secure Shell client/server application, Tectia Client/Server Quantum-Safe Edition, implements the most advanced algorithms recommended by NIST and other agencies, like BSI in Germany. It can also be run in an optional FIPS compliance mode. Tectia Quantum-Safe Edition provides secure remote access (with the SSH protocol), file transfers (with the SFTP protocol), and any type of tunneled TCP connection.

Tectia Quantum-Safe Edition uses a hybrid approach, combining the security of traditional encryption algorithms (against traditional attacks) and the security of PQC algorithms (against quantum attacks) – without compromising efficiency of the product. The solution is also fully backward-compatible with earlier Tectia versions and third-party SSH clients and servers.

The Tectia technology also comes in a quantum-safe edition for IBM z/OS mainframe communications, protecting data flowing in and out of mainframes. It supports the same hybrid approach as the client/server edition and makes migration from either FTP- or SFTP–based communications to quantum-safety smooth and painless.

SSH

Conclusion

There is no need to delay quantum adoption. In fact, quite the opposite - you should start your journey toward quantum safety as soon as possible. With nation states and private businesses racing to develop quantum computers, their serious adoption is more and more realistic every day.

Once viable quantum computers are available, it's only a question of time when they will be utilized by malicious actors to decrypt previously captured communications and secrets.

For that reason, authorities and national security experts urge public and federal institutions to adopt appropriate measures to protect their sensitive data already now.

Luckily, cybersecurity experts like SSH have collaborated for years with other businesses as well as governments (especially the Finnish government) to create and implement world-class post-quantum cryptography to mitigate the quantum threat.

With SSH's Tectia Quantum-Safe technology, you can ensure that your data in transit (the secrets of your organization) stays secure now and long into the age of quantum computers.

For more information on how to take Tectia Quantum-Safe technology into use in your organization, contact us.

Get to know our quantum-safe technology: Tectia SSH Client/Server & Tectia Server for IBM z/OS!

Find out more about how we use post-quantum technology to defend critical data of the leading organizations around the world.

CONTACT US

SSH

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION

+358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.

Tel: +1 212 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Hong Kong

SSH COMMUNICATIONS
SECURITY LTD.

+852 2593 1182
info.hk@ssh.com

SSH