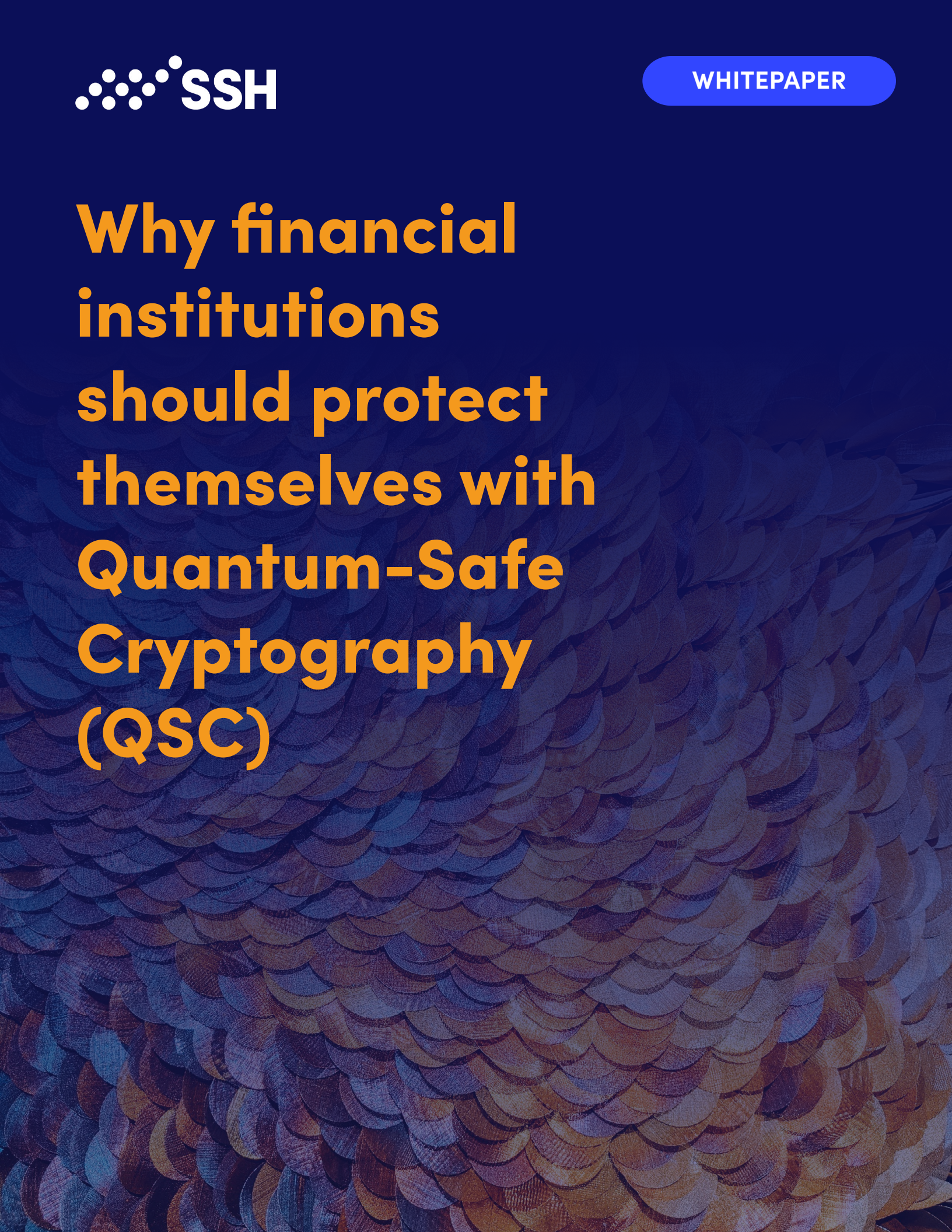
SSH

WHITEPAPER

Why financial institutions should protect themselves with Quantum-Safe Cryptography (QSC)



Introduction

The age of quantum computers has been looming on the horizon for some time now, and it can still can take years until their large-scale commercial use is viable. However, the move to quantum computers is likely to be gradual.

In the 1960s, personal computers did not exist yet but computers were already important in the military and business use. In a similar fashion, quantum computers will be first adopted by the military and by big businesses, like the financial industry. We can see this already happening: in 2021, the US 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."

In 2022, the US Quantum Cybersecurity Preparedness Act goes further. It emphasizes the need for government organizations to start taking necessary precautions against actors wielding the power of quantum computers. Commercial organizations will follow suit.

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

Financial data - a prime target for cybercriminals

Cybercrime is on the rise. Global losses during in 2020 exceeded $1 trillion. That is more than 1% of the global GDP. According to experts in Cyber Security Ventures, the annual global losses by 2025 might reach $10.5 trillion, making it the most profitable criminal segment - more than the illegal trade of all major drugs combined. In the future we will also see more and more of "hybrid warfare" – attacks by state-sponsored actors with practically unlimited resources.

In addition to directly targeting government organizations, they will also try to damage enterprises, like the financial sector, which are vital for societies and their economy, like the financial sector. The average cost of a breach in the financial sector is $5.71 million, or 35% more than the average for all industries.

SSH

The Financial sector routinely handles and stores the personal data of its customers. In a widely published case in 2019, Capital One, a large bank in the US, leaked the data of 100 million customers. The data in question was related to credit applications and did not contain actual payment data. The bank in question considered the total cost of managing the breach as $100-$150 million. Add to that, the company incurred $80M in fines from the US regulators. The cost of an individual customer record compromised was thus between $1.80 and $2.30.

In an earlier settlement in 2017, the credit-reporting company Equifax was fined $4.75 per a compromised customer record. For companies operating in Europe, GDPR allows for huge punitive damages.

In the case of Capital One, we can say that the bank was lucky that no payment data, card number or login information was compromised. If primary account numbers (PAN) fall into the wrong hands, the cardholder might expect fraudulent charges on his or her credit card bill. For the issuer, this means processing chargebacks, issuing replacement cards and losing reputation. A set of Payment Card Industry Data Security Standard (PCI-DSS) regulations exist to protect the PANs from exposure, and the fines for noncompliance can be up to $100k per month.

How quantum computing will 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 strenght 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. As an example, the formerly widely used 512-bit RSA is no longer used and replaced by its 2048-bit counterpart, which should be, according to NIST, good until 2030. And after that, we can just add more bits, right?

Unfortunately, this is where quantum computing breaks the tried and true methods. All currently widely used encryption algorithms are vulnerable to an attack called prime factoring, which a quantum computer does very well. While current quantum computers cannot perform this attack very 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 (2021). That still gives you five or ten years to upgrade your systems, right?

SSH

Financial data is at risk

1 Recording sessions for later abuse

Every financial institution 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, for example, a Permanent account number (PAN). The lifetime of a payment card is usually more thant five years, since new cards are routinely issued with the same PAN, just by moving changing the expiration date farther into the future.

By recording and storing encrypted communication in 2021, 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 2021, break the encryption and have access to plaintext PANs. For the cardholder this means potentially fraudulent charges and for the bank the massive task of changing a huge number of PANs - while dealing with angry customers and authorities.

Normally, this process is too slow for bad actors but if the potential prize is big enough, it is an attractive enough proposition for black hat groups with enough resources. Needless to say, financial information is always a valuable target.

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

Do you have any data in your organization that is still relevant after 5 to 10 years?

2 Preparation needs to start sooner than companies 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 already 26 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 – that it still is today.

However, historically speaking it has taken almost 20 years to deploy the modern public key cryptography infrastructure as we know it. Even if it takes 15-20 years for quantum computing to be a serious threat, the preparation for its arrival needs to start now. Waiting until the technology is close to implementation or reacting after it's available is already too late.

SSH

3 Quantum-Safe Cryptography can exist side by side with classic cryptography

Technologies to mitigate quantum risks exist already. Quantum-safe cryptography (QSC) - also called Post-Quantum Cryptography (PQC) - can replace existing and quantum-vulnerable algorithms used in current cryptography with an upgraded version that can resists the threat posed by both classical and quantum computers to cryptography. Both key agreement and digital signatures can be made quantum-safe, and QSC can be implemented in both software and hardware. For example, the National Cybersecurity Center (NCSC) is a firm believer that adoption of QSC will provide the most effective mitigation for the quantum computing threat.

4 Preparation for migration

Large organizations should factor the Quantum Threat into their long-term roadmaps and identify which of their systems will be a high priority for transition. The priority systems and data should include those that contain and process sensitive personal data, business-critical data and in general are hardest to replace. The standardization of QSC/PQC protocols is progressing fast, and an early set of NIST recommended set of algorithms is practically already available, so it is time for serious businesses to start the migration process.

Future-proof encryption with Tectia Quantum-Safe

Fortunately, quantum computers are not able to render obsolete all kinds of encryption algorithms. PQC, or Post-Quantum Cryptography, algorithms have been under development for years and are ongoing standardization in 2021. Quantum computers do not provide a significant advantage against PQC algorithms.

For maximum security, hybrid algorithms are recommended, containing a traditional component and a post-quantum component. Together they are able to withstand both types of attacks.

To make your connections future-proof, well past the eventual advent of the Quantum computers, SSH has launched Tectia Quantum-Safe Edition, a new Quantum-Safe SSH Client/Server application. Able to secure remote access (with the SSH protocol), file transfers (with the SFTP protocol), or or any type of tunneled TCP connection.

[Learn more about Tectia SSH Client/Server Quantum-Safe Edition >>>]

SSH

Conclusion

There is no need to delay the quantum adoption. Big businesses and nation-states are racing to develop quantum computers, making their serious adoption more and more realistic every day.

At the same time, seasoned cybersecurity experts, like SSH, have collaborated for years with other businesses and the Finnish government to create world-class post-quantum cryptography to mitigate the quantum threat.

SSH's 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 backwards compatible with earlier Tectia and third-party SSH clients and servers. By selecting Tectia Quantum-Safe Edition, you make sure that your data in transit – the secrets of your organization – will stay secure long into the age of quantum computers.

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

Get to know Tectia SSH Client/Server Quantum-Safe Edition!

Want to find out more about how we use post-quantum technology to defend critical data of the leading organizations around the world? Contact us to learn more.

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
Karvaamokuja 2b, Suite 600
FI-00380 Helsinki
Finland
+358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001
USA
Tel: +1 212 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Hong Kong

SSH COMMUNICATIONS
SECURITY LTD.
35/F Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
+852 2593 1182
info.hk@ssh.com

SSH