LANCOM
SYSTEMS

White Paper

Is VPN still secure enough as an encryption technology for the post-quantum age?

The ongoing development of quantum computers presents fundamental challenges to traditional encryption technologies such as VPN. Virtual Private Networks (VPNs), often based on the Internet Key Exchange (IKE) protocol, are the backbone of many modern IT security solutions. But how secure is this technology given the growing threat posed by quantum computers?

A first step to protect against the threats presented by quantum computers is the introduction of Post-Quantum Pre-shared Keys (PQ-PSKs or PPK) in the IKEv2 protocol. This technology offers a promising basis for making VPNs future-proof and countering potential attacks by quantum computers at an early stage.

LANCOM Systems' strategy for the post-quantum era

LANCOM Systems is at an early stage pursuing a future-oriented strategy to prepare its products and solutions for the threats of the post-quantum age. The aim is to enable companies, authorities, and operators of critical infrastructures to make a secure transition into an era when quantum computers could soon endanger asymmetric encryption methods.

Proactive preparation and compliance with standards

LANCOM Systems is following the recommendations of the German Federal Office for Information Security (BSI) for the introduction of post-quantum cryptography, as described in the statement from the BSI in November 2024[1].

The company is committed to a gradual and practical integration of post-quantum security mechanisms into its product range to help its customers make a sustainable and secure transition.

Introducing Post-Quantum Pre-shared Keys

A central element of this strategy is the introduction of post-quantum pre-shared keys (PQ-PSKs) in the IKEv2 protocol. This technology will be available from 2025 with LCOS 10.90 and offers an initial protective measure against potential attacks by quantum computers.

Expanding post-quantum functionalities

Throughout 2025, LANCOM Systems will further expand its post-quantum functionalities. LCOS FX 11.3 and the implementation of ML-KEM marks the arrival of an even more robust security architecture featuring the latest findings in post-quantum cryptography.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html?nn=129156#Download=1

Quantum computing and the threat to classic encryption

Why quantum computing threatens conventional cryptography

Quantum computers use the laws of quantum mechanics to perform complex calculations in extremely short times. They are able to break two fundamental pillars of cryptography:

1. **Asymmetric encryption**: Algorithms such as RSA and Elliptic Curve Cryptography (ECC) are based on mathematical problems that can be effectively solved by quantum algorithms such as Shor's algorithm.
2. **Symmetrical encryption**: Even symmetric algorithms like AES are affected by quantum computers, although the damage here is less severe (e.g. by Grover's algorithm).

Impact on VPNs

VPNs that use IKEv2 as their key-exchange protocol use asymmetric cryptography to securely exchange session keys. These keys could in the future be compromised by quantum computers, which could expose all encrypted data—even retroactively.

Post-quantum pre-shared keys (PQ-PSKs): The solution

How PQ-PSKs work

Post-quantum pre-shared keys (PQ-PSKs) supplement traditional cryptographic mechanisms by integrating an additional, quantum-resistant security component into the key-exchange process. This uses a key shared in advance between the communication partners (pre-shared key), which is independent of asymmetric algorithms. This principle is based on hybrid cryptography, which combines traditional and quantum-safe methods and leverages the security strengths of both approaches.

1. **Additional protective layer**
   The PQ-PSK is introduced as an additional authentication and encryption factor during key negotiation with the IKEv2 protocol. This creates a security mechanism that remains intact even if classical asymmetric cryptography is cracked by a quantum attack. The PQ-PSK is integrated into the process by using it in combination with established methods (e.g. RSA or ECC), which strengthens the entire key exchange.
2. **Quantum resistance through robust algorithms**
   PQ-PSKs rely on algorithms that are resistant to quantum computers. These algorithms are based on mathematical problems that are difficult to solve even for quantum computers, such as:
   - **Lattice-based cryptography**: Security is based on the difficulty of finding the shortest vectors in lattice structures.
   - **Code-based cryptography**: Use of error-correcting codes as the basis for encryption.

- **Multi-variable polynomial systems**: Problems with multiple variables that are difficult to calculate.

3. **Pre-shared key**
The key is securely provisioned outside of the regular key-exchange process. This can be done through physical handover, a separate secure connection, or other best practices. This physical or separate distribution ensures that the PQ-PSK cannot be intercepted by attackers, even if the traffic itself is monitored.
4. **Integrated security check**
During the handshake phase in the IKEv2 protocol, each party checks the validity of the PQ-PSK. This protects not only against future quantum attacks, but also against current attacks including man-in-the-middle attacks, where an attacker tries to manipulate the key negotiation.
5. **Retroactive protection**
A particularly important aspect of PQ-PSKs is the protection against Store-Now-Decrypt-Later (SNDL) attacks. In these attacks, attackers store encrypted data in order to decrypt it once powerful quantum computers become available. By using PQ-PSKs, the stored data remains secure because it cannot be decrypted without access to the pre-shared key.
6. **Compatibility and transition phases**
PQ-PSKs can be integrated into existing IKEv2-based VPN infrastructures without having to completely replace the asymmetric methods. This hybrid approach facilitates implementation and allows organizations to invest in the new technology step by step. Classical systems can still be used while adding a quantum-safe layer.

Advantages of PQ-PSKs

→ Resistance to quantum attacks: PQ-PSKs use quantum-resistant algorithms that cannot be efficiently cracked even with powerful quantum computers.
→ Seamless integration: The technology can be integrated into existing IKEv2-based VPN infrastructures without requiring fundamental changes.
→ Long-term protection: Companies can today secure their encryption against future threats.

Practical application and implementation

Introduction into existing network infrastructures

The introduction of post-quantum pre-shared keys is particularly relevant for industries and scenarios where long-term confidentiality and data integrity are critical. Here are some examples and the associated need for action.

1) Corporate networks

Companies that transfer sensitive data between sites, such as financial data, internal strategy documents, or personal data, face the challenge of protecting this information against future threats.

2) Critical infrastructures

Operators of energy, water, and transport networks must protect themselves against potential attacks because their networks are particularly lucrative for attackers.

3) Healthcare

Electronic patient records, medical research results, and other confidential information must be protected to comply with data-protection regulations such as GDPR, and to ensure patient trust.

4) Financial sector

Banks and financial service providers process large volumes of transactions and sensitive customer data that must be protected in the long term.

5) Authorities and public administration

Authorities store and transmit data with long-term confidentiality, such as classified information, citizen data, and strategic planning.

The need for action may differ between sectors, but in every case the practical implementation takes place in two simple steps:

1) Firmware update

Existing VPN endpoints must be updated with firmware versions that support PQ-PSKs.

2) Configuration

Updating an existing VPN connection to use the PQ-PSK.

The concrete implementation of step 2 in a LANCOM infrastructure is described in this Knowledge Base article:
https://knowledgebase.lancom-systems.de/pages/viewpage.action?pageId=210894931

Future security through PQ-PSKs

The introduction of post-quantum pre-shared keys represents an important first step in preparing VPNs for the post-quantum era. Although quantum computers are not currently capable of cracking traditional encryption such as RSA or ECC, their development is being actively pursued. Once powerful quantum computers become available, they could quite quickly compromise asymmetric encryption algorithms. It is therefore vital not to wait for the technological breakthrough of quantum computers, but to start securing IT infrastructures now.

Conclusion

VPNs remain a viable security solution when supplemented with cutting-edge technologies such as PQ-PSKs. Companies that embrace this development early on will gain a decisive advantage in an increasingly uncertain digital world. Investing in post-quantum technologies is not only a precautionary measure, but also an expression of innovation and foresight.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.eu | lancom-systems.com