Adopting Post-Quantum Cryptography in a Zero Trust Architecture

Eric Jansen
Executive Vice President
Independent Software, Inc.

January 7, 2023

Contents

Introduction

Using guidance from the Cybersecurity and Infrastructure Security Agency's (CISA) "Shields Up" campaign, the U.S. government has recommended "all organizations --regardless of size-- adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets."[1] A key component to strengthening an enterprise cybersecurity posture is Zero Trust, a framework for verifying, assuring, and protecting data. This security model is not a new concept, but the landscape encompassing the security model has changed.

Today's enterprise environments consist of many interconnected segments: corporate networks, on-premises infrastructure and applications, cloud-based infrastructure and applications, remote and mobile workforce environments, and an increasing number of sensors and devices at the perimeter. This infrastructure evolution has created more opportunity for threats to access critical data, forcing organizations to reevaluate traditional data protection methodology. Traditional perimeter-based defenses are no longer adequate.

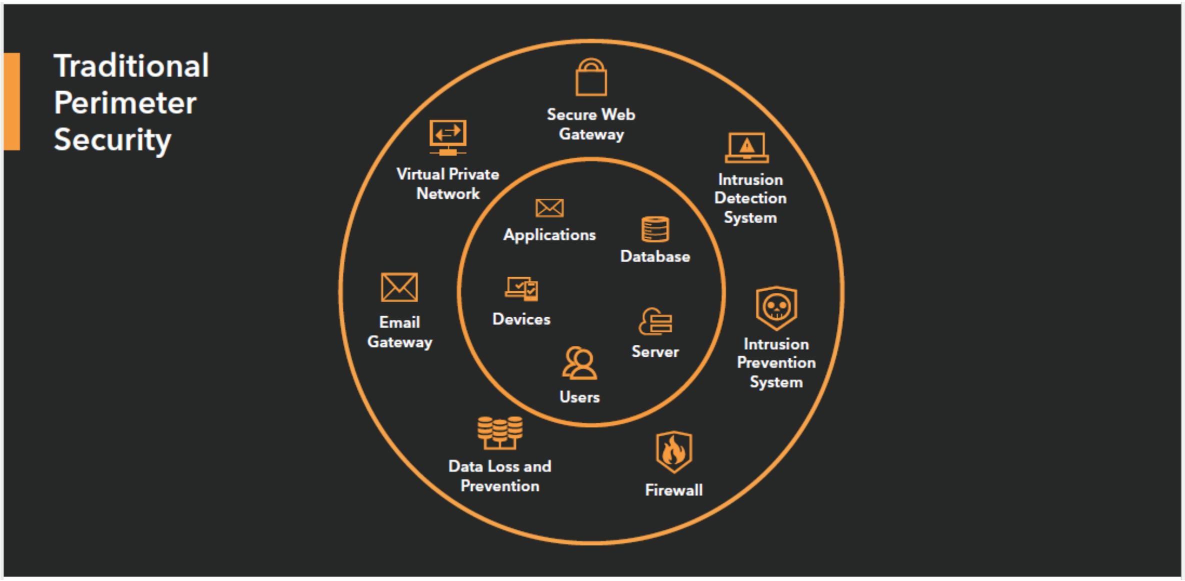


Figure 1: Traditional Perimeter-Based Security

A comprehensive approach to cyber risk mitigation that goes beyond mere threat detection is needed. Trust-based security on internal networks has enabled intruders to launch cyberattacks on strategic assets inside the data center perimeter. Insider attacks have also been rising annually, and now constitute a significant percentage of enterprise breaches. A newly remote workforce, precipitated by the global pandemic, has exacerbated security concerns by extending networks beyond traditional boundaries. The introduction of Bring Your Own Device (BYOD) policies and the extension of data centers to public clouds have also introduced increased risk.

This white paper discusses attack surfaces in current architectures, the risks associated with quantum computers on security and cryptography and demonstrates Independent Software's experience and currently available platform to guide the adoption of Post-Quantum Cryptography as part of the federal government's overall data protection strategy in a Zero Trust framework.

[1] https://www.cisa.gov/shields-up

What is Zero Trust?

Zero Trust principles are not new, but the concept is experiencing an influx of new renewed interest because it addresses many of the cybersecurity challenges that we face today. In 1994 Dr. Stephen Paul Marsh introduced the Zero Trust concept when he composed his doctoral thesis on “Formalising Trust as a Computational Concept.” He asserted that trust was a “social phenomenon” that could be understood by artificial intelligence. It wasn’t until 2010 that John Kindervag, an analyst at Forrester Research, challenged the conventional wisdom that creating a strong perimeter was enough to keep an organization secure. He also recommended not trusting anything inside the perimeter. The Zero Trust framework describes the process and technologies of implementing trust on a transactional basis and focuses on authentication and authorization of all users on a network while still maintaining the pace and availability of services.

As defined by National Institute of Standards and Technology (NIST) Special Publication 800-207, “Zero Trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services” under the assumption that the network is compromised. A Zero Trust architecture (ZTA) uses Zero Trust principles to develop and build an enterprise infrastructure and workflows. Zero Trust assumes there is no implicit trust granted to assets or user accounts based on their network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established.[2] Zero Trust requires all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location. The main concept behind Zero Trust security is “never trust, always verify.”

The CISA’s Zero Trust Maturity Model is one of many roadmaps, specific to the federal government, for agencies to reference as they transition towards a Zero Trust architecture. The goal of the maturity model is to assist agencies in developing trust strategies and implementation plans and present ways in which various CISA services can support Zero Trust solutions across agencies.

The maturity model, which includes five pillars and three cross-cutting capabilities, is based on the foundations of Zero Trust. Within each pillar, the maturity model provides agencies with specific examples of a traditional, advanced, and optimal Zero Trust architecture. CISA drafted the Zero Trust Maturity Model in June of 2021 to assist agencies in complying with Executive Order 14028, “Improving the Nation’s Cybersecurity.”[3]

[2] https://doi.org/10.6028/NIST.SP.800-207

[3] https://www.federalregister.gov/executive-order/14028

Tenets of Zero Trust

NIST Special Publication 800-207 Zero Trust Architecture states that a Zero Trust Architecture is designed and deployed with adherence to the following tenets:

- All Data Sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per session basis
- Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

In summary, Zero Trust is a set of guiding principles for workflow, operations, and systems design. The importance of strong encryption cannot be overstated: it is a key component, and without it all underlying security practices are at risk.

Securing the Global Network – The Need for Post-Quantum Cryptography

As quantum computing technology matures, the need for vastly more robust encryption keys becomes critical. Quantum computers, "a type of computer 158 million times faster than the most sophisticated supercomputer we have in the world today"[4], have sufficient computational power to crack the most sophisticated encryption algorithm known today. The shift toward quantum computers will necessitate a fundamental shift to a quantum-resistant cryptography system that is "secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks."[5]

Michele Mosca, Co-Founder and Deputy Director of the Institute for Quantum Computing at the University of Waterloo, developed a method for calculating the point in time when the impact of quantum computers on secure data transmissions will become a real threat. The method, known as Mosca's Inequality, is given as $\boldsymbol{D + T \geq Qc}$, where

- D = the amount of time we want to keep data secure,
- T = the time it will take for security systems to transition from classical to post-quantum,
- Qc = the time it will take for quantum processors to have reached a scale where they can breach existing encryption protocols

Simply put, the equation states that we need to begin transition to a post-quantum cryptography solution well in advance of the point in time when quantum computing is sufficiently advanced to breach existing encryption protocols. Using this equation, experts in government and commercial institutions have concluded that conditions that breached Mosca's Inequality were met in 2017.

In 2016, NIST warned that all organizations should start preparing for the coming quantum

[4] https://www.livescience.com/quantum-computing

[5] https://csrc.nist.gov/Projects/post-quantum-cryptography

cryptographic break. This sentiment was reinforced in the group's April 2021 report, **Getting Ready for Post-Quantum Cryptography** (PQC), a thorough review of the challenges associated with adopting and using PQC algorithms after the standardization process is complete.[6] We know that cryptographic transitions can take years, even decades to fully complete. In 2005 and again in 2007, NIST recommended through special report SP 800-57 that users move from 1024-bit to 2048-bit RSA by 2010. In 2011, NIST upgraded their policy and issued special publication SP 800-131A to allow for a three-year transition period from 1024 to 2048 bits ending Dec. 31, 2013. It took more than 20 years for the Advanced Encryption Standard (AES) to completely replace Data Encryption Standard (DES) and 3DES.

While the PQC selection process is on pace to be finalized by 2023, NIST cautions organizations that another 5-15 more years will be needed after the publication of the cryptographic standard before full transition is completed.

This timing is problematic on three fronts:

- A quantum computer may be available before then
- There is no guarantee that the cryptographic standards selected will not be broken by adversaries or vulnerable to implementation errors if they have not already been broken
- "Harvest today, decrypt tomorrow" attacks are happening now

Cryptographic transitions are disruptive and resource intensive. The replacement of algorithms can require changing or replacing libraries, validations tools, hardware, operating systems, application code, device protocols, and user/administrative procedures. Most enterprises would prefer to avoid expensive "rip and replace" security projects in favor of an incremental transition toward quantum-safety.

Independent Software works with its customers to prioritize workloads and develop budget allocations that consider quantum-safe technologies to help plan for unknowns, address evolving security threats, maintain data privacy and governance, and ensure a flawless digital user experience in a Zero Trust Architecture. We have solid experience developing roadmaps that deliver future-proof solutions to protect data and communication networks across any medium (e.g., fiber, copper, wireless, satellite, undersea cable) and without distance concerns, and our solution integrates with the existing cryptographic infrastructure to bring the encryption environment into the quantum era with minimal lift or outlay.

[6] https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final

Getting Started on the Journey

With key-generation collisions in the cloud caused by low entropy or growing man-in-the-middle attacks taking over critical control systems, how can the government properly plan for continued high-risk disruptions such as these while addressing known and unknown vulnerabilities in the environment? In evaluating the risk for quantum attack, what steps can, and should, be taken today?

With the release of NSM-8[7] and NSM-10[8] in 2022, the government is looking to begin the quantum readiness journey by embracing post-quantum cryptography as part of the Zero Trust security model. However, different data types require different protection levels — or defense-in-depth countermeasures. The government must have a firm understanding of the various risk-tolerance levels of their data and corresponding risk-related consequences. Recognizing factors that influence data privacy and security regulations, both locally and globally, are performed as part of Independent Software's development of a risk management strategy in the soon-to-be quantum era. We then work with the government customer to evaluate and deploy practical and highly scalable quantum-safe technologies that are available today.

Safeguarding Data with Quantum-Safe Key Delivery

Industry is currently debating as to when a true quantum computer will be commercially available, but none argue that current encryption methods will not withstand a quantum computer attack. Q-day aside, other driving factors point to the urgent need for ultra-secure encryption to protect transmitted data by both government agencies and commercial organizations.

Public Key Encryption (PKE) systems that protect our digital universe were devised back in the 1980s when the computing landscape was very different and the hyperconnected world of today unimaginable. Classic encryption (e.g., TLS/SSL) sends the encryption key and the data it protects down the same transmission tunnel. An attacker needs only to compromise one connection to obtain the protected information. This outdated architecture and fundamental design flaw has given rise to popular attack vectors including man-in-the-middle, brute force, and even ransomware attacks.

Each year new studies are published that highlight how key management practices are rife with vulnerabilities and enterprises' failure to institute security hygiene best practices. In a recent Data Threat Report, Thales found that 69% of government entities use an array of firewalls or IPsec for encrypting network data. Relying on outdated technologies such as IPsec, a twenty-five-year-old protocol not designed for high bandwidth networks, introduces risk due to IPsec's lack of automated key rotation or active tamper response causing far-reaching consequences in the event of a breach.

A critical ingredient to strong encryption is unpredictability and randomness. Random numbers are used to make cryptographic keys, but true randomness is debatable due to the increase in computing power and techniques like machine learning and quantum computing

[7] National Security Memorandum/NSM-8
[8] National Security Memorandum/NSM-10

that make latent patterns in the key easier to detect and traditional sources of randomness easier to break. However, quantum randomness in the subatomic realm is plentiful, and entropy from Quantum Random Number Generated (QRNG) keys could soon become common practice.

The Process

Independent Software performs the following steps as part of our process to develop a realistic quantum-safe cybersecurity roadmap that secures existing network communication links, builds a scalable foundation for protecting data in motion, and keeps pace with the evolving threat landscape as new risks emerge from the continued advancement of computing:

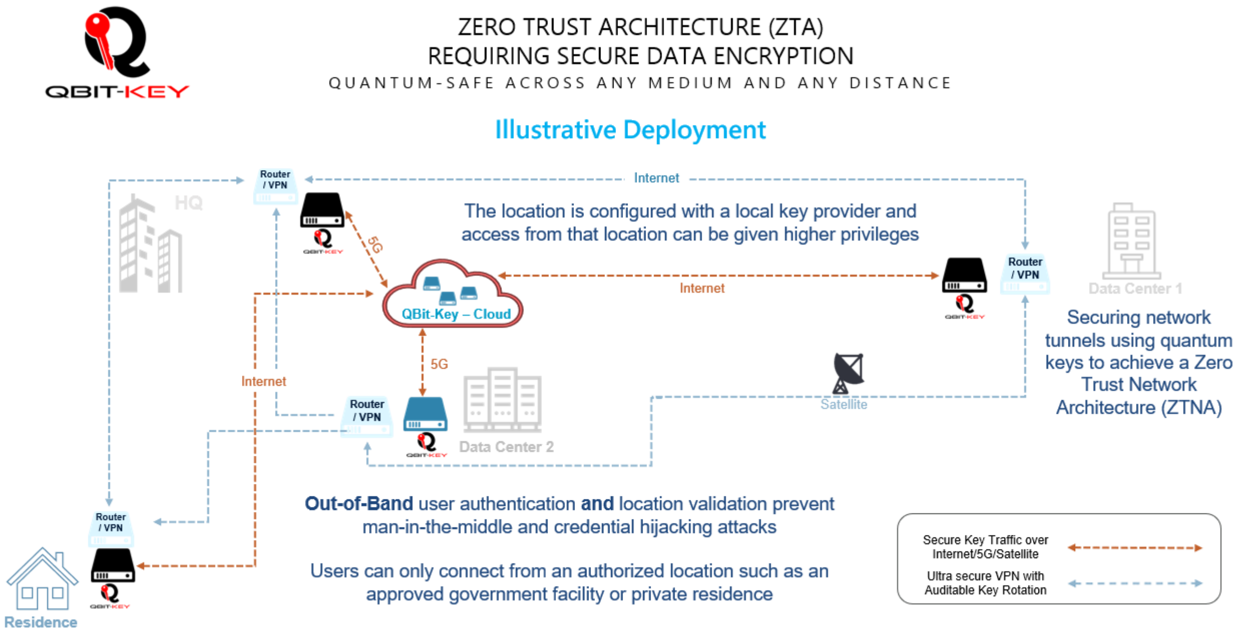
- Use the cyber-risk quantification and management platform of the government choosing to calculate the risk profile including risk-tolerance level for sensitive data.
- Determine the data privacy and security regulatory landscape by identifying all applicable laws, foreign and domestic, to be imposed on the enterprise.
- Use a top-down approach based on high-risk applications, classifying sensitive and persistent data including data processed by applications hosted through third-party vendors and cloud providers.
- For all sensitive or persistent data, develop network diagrams that embrace Zero Trust security and defense-in-depth or multi-layered security safeguards for the entire communications infrastructure – including critical third-party service providers.
- Identify required controls at all layers of the stack from the network layer to the application layer and develop the “to-be” architecture to address identified and prioritized risks and vulnerabilities from the results of any prior cybersecurity risk assessments or audits including entries in the risk register.
- Map the results of the regulatory and compliance requirements and applicable privacy principles including data subject rights, data sharing, data protection to the proposed solutions architecture.
- Initiate a pilot program to apply quantum-proof security controls across a select data network and communications infrastructure.
- Based on the results of the pilot and lessons learned, develop a quantum-safe network infrastructure refresh roadmap.

Delivering the Future of Encryption

Independent Software offers the only Department of Defense (DoD) accredited and Federal Information Processing Standard (FIPS) 140-3 validated dynamic and crypto-agile quantum-safe key delivery system that can scale to meet the government’s mission and budgetary requirements. This platform is best characterized as a simple architecture overlay, leveraging an out-of-band symmetric key delivery technology to supplement native encryption with an additional key-encrypting-key (KEK) transmitted independent of the data path and through a quantum-protected tunnel. Administrators can increase quantum protection levels at any time with no interruptions to the network or enterprise business. Moreover, the crypto-agile technology supports quantum keys from any source (e.g., PQC, Quantum Key Distribution, QRNG, etc.) and works across any network medium.

In addition to addressing the quantum threat head-on, this unique solution can be deployed today to overcome the inherent vulnerabilities of PKE — primarily the key and data traveling together and the low entropy of public keys. The use of its patent-pending out-of-band symmetric key delivery technology essentially removes man-in-the-middle attacks because there is no middle anymore.

Independent Software's QBit-Key platform improves and automates basic security hygiene practices. For example, most VPNs rely on the IPsec protocol using static keys that are not frequently (or ever) rotated, which is a poor security practice that weakens the overall security posture of the network. In the QBit-Key hive, keys are generated and rotated on demand and even on every transfer, providing key delivery to every VPN node automatically. With QBit-Key, secure continuous key rotation is the norm rather than the exception.


QBIT-KEY
ZERO TRUST ARCHITECTURE (ZTA)
REQUIRING SECURE DATA ENCRYPTION
QUANTUM-SAFE ACROSS ANY MEDIUM AND ANY DISTANCE
Illustrative Deployment
HQ
Router / VPN
Internet
5G
QBit-Key – Cloud
Internet
Router / VPN
Data Center 1
Internet
5G
Router / VPN
Data Center 2
Satellite
Router / VPN
Residence
Secure Key Traffic over Internet/5G/Satellite
Ultra secure VPN with Auditable Key Rotation

The location is configured with a local key provider and access from that location can be given higher privileges

Securing network tunnels using quantum keys to achieve a Zero Trust Network Architecture (ZTNA)

Out-of-Band user authentication **and** location validation prevent man-in-the-middle and credential hijacking attacks

Users can only connect from an authorized location such as an approved government facility or private residence

Figure 2: Illustrative Quantum-Safe Network as Part of a Zero Trust Architecture

Conclusion

Zero Trust is not a single technology solution, but a larger cybersecurity strategy and operational practice. A successful Zero Trust Architecture uses Zero Trust principles to develop and build an enterprise infrastructure and workflows, and all communication is secured regardless of network location. Encryption is vital to communication security, and Independent Software's QBit-Key platform is the only FIPS 140-3 crypto-agile technology supporting source-agnostic quantum keys that is available today.