



Post Quantum Cryptography

An Overview of the Problem, USG Responses, and Oracle Initiatives

Introduction

Post-quantum computing technology is rapidly progressing. Post quantum computing poses a significant threat to the confidentiality of data-at-rest and data-in-motion as it is expected to render current encryption algorithms ineffective. Post Quantum Cryptography (PQC) is emerging as a fundamental technology for securing digital information against the threats posed by quantum computing.

This document discusses key aspects of the post-quantum era including:

- An overview of the problem
- U.S. Government initiatives and mandates
- Potential solutions to the problem
- Oracle PQC initiatives & GDI testing
- Commercial adoption & initiatives

PQC counters quantum computing threats to traditional encryption. Current state shows finalized NIST standards and early migrations, but adoption lags amid growing quantum risks. Future state anticipates cryptographically relevant quantum computers (CRQCs) by 2030-2035, demanding widespread PQC implementation. Oracle Government, Defense, & Intelligence (GDI) must prioritize crypto-agile systems to protect data and meet the requirements of our government customers.

The advent of CRQCs poses a significant threat to current encryption algorithms. Currently, the time taken to derive the private key for a given public key can take years. Using CRQCs, that time can be reduced to a matter of a few days or hours. This would mean the 10 to 20 years' timeframe of confidentiality requirement for sensitive information can no longer be met with existing cryptographic algorithms.

This is not just problem for the future; it's a problem now. Data harvested today can be stored for future decryption. Called "Harvest now, decrypt later" attacks, adversaries intercept and store data-in-transit for future quantum decryption, threatening long-term secrets in finance, healthcare, and government.

Quantum computers exploit Shor's algorithm to factor large numbers efficiently, breaking asymmetric encryption used in secure communications, digital signatures, and data protection. Grover's algorithm accelerates symmetric key searches, halving effective key

strength. Scalable quantum systems, expected by 2030, amplify these risks, and with the advent of AI, these timelines may accelerate significantly. Traditional methods like RSA and ECC are at risk from quantum algorithms, necessitating quantum-resistant alternatives.

PQC algorithms secure against both classical and quantum attacks, focusing on lattice-based, hash-based, code-based, and multivariate cryptography. NIST standardization finalizes PQC candidates like CRYSTALS-Kyber and Dilithium for deployment. Crypto agility enables seamless algorithm transitions in systems. Solutions include hybrid approaches combining classical and PQC methods for backward compatibility.

This document provides an overview of the PQC threat, identifies emerging government requirements, and details some of the work that GDI is doing to address the issues related to PQC.

U.S. Government Initiatives

In 2025, the U.S. National Institute of Standards and Technology (NIST) finalized several PQC standards, which are expected to be widely adopted. These new standards will affect everything from secure network communications to hardware infrastructure in government, financial, and private sectors. The urgency of this transition is further accelerated by the threat of “harvest now, decrypt later” attacks, where encrypted data is captured and stored and later decrypted once quantum technologies are available.

NIST finalized three PQC standards in August 2024: FIPS 203 (ML-KEM, lattice-based key encapsulation), FIPS 204 (ML-DSA, lattice-based signatures), and FIPS 205 (SLH-DSA, hash-based signatures). HQC (code-based) was added in March 2025. NIST held the sixth PQC Conference (Sept 24-26, 2025) in Gaithersburg, Maryland for in-depth discussions and collaborative engagement with academia, industry, and government.

USG and DoD Mandates

The Committee on National Security Systems (CNSS) Policy 15 (Mar 4, 2025): Mandates Commercial National Security Algorithm Suite (CNSA) 2.0 for NSS. Non-CNSA 1.0 systems: Comply or waiver by Sept 2025 (6 months post-release). No full CNSA 2.0 mandate before Dec 31, 2025. Quantum-safe in new NSS products by Jan 2030.

CNSA 2.0 (May 30, 2025): Algorithms: ML-KEM 1024 (f/k/a Kyber)(Level V), ML-DSA-87(f/k/a Dilithium) (Level V); LMS/XMSS signing; AES-256; SHA2-384/512. No hybrid allowed except for extremely niche cases where pure PQC cannot function. NSS must use approved crypto; report progress via NSM-8/10. New software/firmware: CNSA 2.0 signing by 2025. Deployed non-1.0: Transition by 2025. All deployed: By 2030. Web/cloud: Prefer 2025,

exclusive 2033. Networking: Prefer 2026, exclusive 2030. OS: Prefer 2027, exclusive 2033. Full QR by 2035. “Prefer” means if it’s available on the market, it must be used.

Other EOs and Acts: Jan 2025 EO: PQC/hybrid in products; TLS 1.3 by 2030. May 2025: PQC in procurements. June 2025 EO: CISA PQC product list by Dec 1, 2025; NSA/OMB TLS requirements by Dec 1, 2025. July 2025 Act: National Quantum Cybersecurity Migration Strategy.

GSA/OMB: Buyers Guide (Jun 2025) for PQC transitions; supports EOs 14028, 13800, and the Quantum Act.

Mandate	Deadline	Scope
CNSS 15 Compliance	SEP-2025 (waiver)	NSS crypto
New Firmware Signing	2025	CNSA 2.0
PQC Product List	01-DEC-2025	CISA
TLS 1.3 Support	02-JAN-2030	Government Agencies

Timelines of GSA/OMB Mandates

DoW PQC Requirements (as of Sept 2025)

NSA's CNSA 2.0 (Sep 2022, updated 2024/2025) for National Security Systems (NSS), including DoW:

Category	Timeline	Details
Software/Firmware Signing	By 2025	Use ML-DSA/SLH-DSA; new products compliant
Networking Equipment	Prefer 2026; NLT 2030	Full (non-hybrid) PQC in TLS/VPNs/Routers/Firewalls
Browsers/Servers/Cloud	Prefer 2025; NLT 2033	PQC key exchange (ML-KEM)
Operating Systems	Prefer 2027; NLT 2033	Full quantum-resistant crypto
Full NSS Migration	By 2035	Inventory vulnerable systems; report via NSM-8/10

Timelines of NSA/CNSA Implementation Requirements

“Prefer” means if it’s available on the market, it must be used.

CNSS Policy 15 (Mar 2025) mandates compliance or waivers by Sept 2025. DoD PKI to integrate PQC for enduring protection.

Oracle’s Initiatives

Oracle is pursuing a transitional strategy that will help prepare for the post quantum era while maintaining existing technical capabilities and preventing compatibility issues with classical encryption mechanisms in our customers’ products and cloud services.

Oracle's cryptography teams are implementing the latest FIPS approved algorithms in our cryptography providers starting with the FIPS 203 ML-KEM key encapsulation algorithm. This is the first step in adding quantum safe capabilities to existing crypto protocols used by Oracle products and cloud services.

Oracle GDI has been working with our partner American Binary to develop and test PQC compliant Virtual Private Network (VPN) solutions. Oracle GDI has also performed testing on the Oracle Linux 10 operating system and has successfully provisioned resources on that platform using American Binary's CNSA 2.0 PQC conformant network protocol, including key exchange.

Adoption of PQC Technology

Early pilots in browsers such as Chrome and Firefox and operating systems such as Oracle Linux 10 support hybrid algorithms. Other operating systems that support hybrid compliance are Microsoft Windows, several Linux variants, macOS, iOS, Android and IBM z/OS. New federal mandates require PQC migration, and the USG has taken actions such as Executive Orders 14028 and 13800, and the National Quantum Act that was signed into law in 2018. Details about adoption of major Cloud Service Providers (CSPs) and some VPN vendors can be found in Appendix 1.

GDI PQC VPN Testing

Oracle Government, Defense, & Intelligence (GDI) has been working with our Partner American Binary (<https://www.ambit.inc>), an OPN Member, on potential solutions. American Binary's technology was reviewed by the Oracle Crypto Review Board and successfully passed their assessment.

Currently, American Binary's product, Ambit Client, is the only VPN solution on the market that is built to fully comply with CNSA 2.0, making it the only VPN solution that protects against today's "harvest now, decrypt later" attacks while providing future-proofing against other quantum attacks.

Ambit Client uses exclusively CNSA 2.0 algorithms (NIST Level 5) across all four key components (authentication, key exchange, bulk encryption, and hashing) and meets the highest bar for quantum-resistance.

American Binary is a U.S.-based cybersecurity firm located in Kirkland, Washington, founded in 2019. The company specializes in post-quantum encryption technologies and quantum-resistant cloud infrastructure, including VPNs, secure communication, and disk encryption designed to withstand quantum attacks. With a multidisciplinary team, American Binary has developed solutions that aim to meet or exceed U.S. government

standards for cryptographic security. Their products ensure data security against quantum computing threats, adhering to FIPS 140-3 and CNSA 2.0 standards.

GDI has tested several of American Binary's CNSA 2.0 PQC conformant VPN products. We have successfully tested PQC compliant VPN clients that connect to Oracle VPN endpoint servers in OCI that act as both an internet proxy and provide connectivity to resources in private subnets. Test environment and detailed results are available upon request.

Conclusion

Post quantum computing poses a significant threat to the confidentiality of data-at-rest and data-in-motion. The United States government and technology vendors are taking action to counter this threat, but implementation is difficult, time consuming, and costly.

Oracle is aware of the threats posed by the advent of cryptographically relevant quantum computers and is taking action to mitigate these threats. We know that our government customers are keenly aware of the situation, and they are publishing requirements and deadlines for implementation.

It is important that the GDI team is educated on PQC, so we are prepared to articulate to our customers what Oracle is doing to address the problems posed in the post-quantum era.

Appendix 1

Commercial Adoption - CSP Key Initiatives

All major cloud service providers are advancing PQC with hybrid integrations, NIST-standard tools, and migration plans to counter quantum threats. Below is an overview of some of the PQC initiatives of major CSPs.

AWS:

Multi-phase migration: ML-KEM/ML-DSA in AWS-LC (FIPS-140-3); hybrid TLS/QUIC/SSH; s2n-tls for PQC key exchange; transparent KMS/ACM/Secrets Manager; PQCP open-source. Phasing out Kyber by 2026.

Google Cloud:

Quantum-safe signatures (FIPS 204/205) in KMS preview; PQC in internal comms since 2022; hybrid TLS in Chrome; BoringCrypto library; Cryspen verification; HSM integration Q3 2025.

IBM Cloud:

ML-KEM/ML-DSA in cloud protocols (TLS); hybrid quantum-safe encryption. Quantum-Safe 360 transformation; crypto inventory/vulnerability scanning; CBOM for apps; aligns with CNSA 2.0.

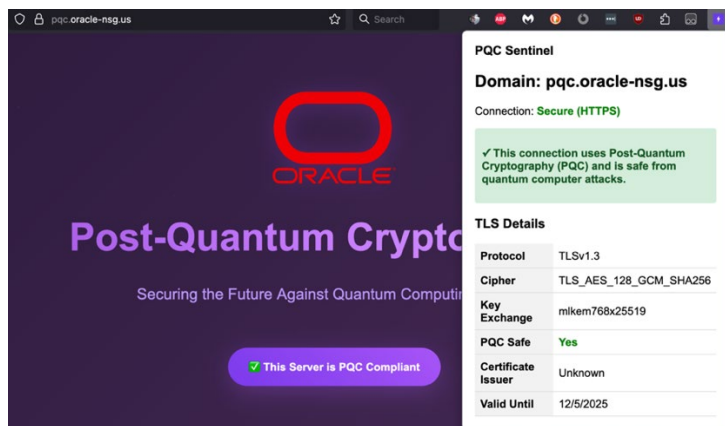
Microsoft Azure:

ML-KEM in TLS 1.3; Open Quantum Safe expansions; hybrid schemes in cloud/hardware; PQC in KMS/HSMs for key management.

Oracle:

Java 24 (Mar 2025) adds ML-KEM (FIPS 203), ML-DSA (FIPS 204); backports to LTS; AI-optimized Vector API; OCI implements FIPS 203; hybrid via QMware; OpenSSL 3.5 PQC; Arqit Quantum defense partnership, Oracle Linux 10 with PQC support.

Oracle Linux 10 web server
running PQC compliant
Key Exchange



Oracle Government, Defense, & Intelligence

VPN Vendor Initiatives

VPN vendors are already implementing PQC compliant solutions. Many networking companies are ahead of CSPs in releasing PQC-enabled VPN products, which can be deployed in a CSP environment. Below are some details on their efforts:

American Binary:

Offers CNSA 2.0 conformant quantum-safe VPN solutions on a variety of platforms including MacOS, Windows, Android, and IOS.

Cisco:

Developed NIST PQC contributions; founding member of Linux Foundation's Post-Quantum Cryptography Alliance; IETF quantum-safe PKI with ML-DSA. Phased hybrids (classical + PQC like ML-KEM); white papers/guides for HNDL risks; crypto-agile protocols

Fortinet:

Integrates quantum-resistant encryption into its Next-Generation Firewalls (NGFWs) and VPN solutions to future-proof enterprise networks against quantum threats.

Juniper Networks:

Offers a quantum-safe VPN solution in partnership with Evolution Q, demonstrating crypto-agility.

Palo Alto Networks:

Supports PQC in its IKE VPN for next-generation firewalls, indicating a commitment to incorporating quantum-safe standards.

NordVPN:

Provides a post-quantum encryption feature for its NordLynx protocol on multiple platforms. It is activated by the user and works in a hybrid mode.

Appendix 2

References

Post-Quantum Cryptography (NIST)

<https://csrc.nist.gov/projects/post-quantum-cryptography>

Executive Order 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

<https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure>

Executive Order 14028 - Improving the Nation's Cybersecurity

<https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>

H.R.6227 - National Quantum Initiative Act

<https://www.congress.gov/bill/115th-congress/house-bill/6227/all-actions>

The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ

https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

American Binary (Oracle OPN Partner)

<https://www.ambit.inc/>

Appendix 3

Oracle GDI's Work with American Binary

Oracle Government, Defense, and Intelligence and American Binary have been working together for several months testing and evaluating PQC VPN technology. This document provides an overview of the testing, the test infrastructure, and test results.

Mission and Industry Positioning: American Binary positions itself as a driver of next-generation cybersecurity, with a focus on resilient quantum-safe networks for both businesses and government clients.

Testing and Evaluation

Oracle and American Binary have been working together for the past year to test and evaluate PQC VPN solutions. This has included testing on a variety of platforms including:

- Oracle Linux 10 (x86_64, AMD, ARM)
- macOS Sequoia build 15.6.1 (Apple M1 Silicon)
- Microsoft Windows 11 x64
- Microsoft Windows 10 x64 VM running on VMware ESXi
- Ubuntu Linux 24.04.3 LTS (GNU/Linux 6.14.0-1011-oracle x86_64)
- Android version 15, kernel version 6.1.99-android14-11 on Galaxy S24+ smartphone

Note that testing is ongoing and additional testing will include:

- iOS (iPhone)
- Windows Server

Currently, the infrastructure includes several Oracle resources including Mac, Windows, and Android clients and an Ubuntu server hosted in Oracle Cloud Infrastructure (OCI). These systems have been used to evaluate the use of American Binary's PQC technology in an operational environment.

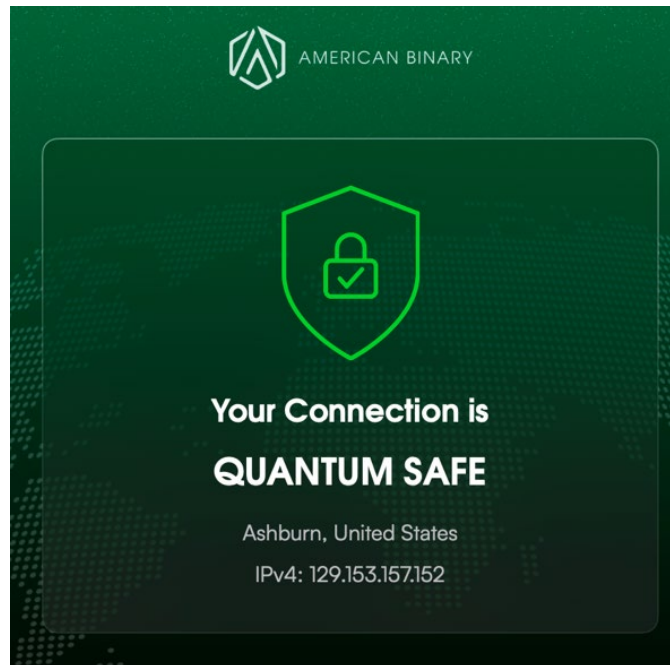
During the testing, Oracle made some recommendations to American Binary for minor changes and enhancements to the client software, all of which were quickly addressed or put in the pipeline for future builds.

The PQC VPN server that was used is an Ubuntu Linux machine running in Oracle Cloud in the Ashburn (IAD) region. It is configured on a VM.Standard.E4.Flex instance with 1 OCPU and 16GB of memory. Its network bandwidth is 1Gbps.

The MacOS, Windows 11, and Android clients are operating in the Oracle lab in Georgia that has both wired and wireless networks that were used in the testing. The lab network is

routed through a network firewall running pfSense version 2.8.1 (amd64). Note that due to the rural location of the lab, the broadband connection is asymmetric and is satellite based using SpaceX Starlink.

The Windows 10 client is running in the Oracle lab in Reston, VA. That network has a 1GB symmetric fiber connection to the internet and also runs through a pfSense firewall. The system runs on a VMware ESXi host and has a 1GB wired Ethernet connection to the network.

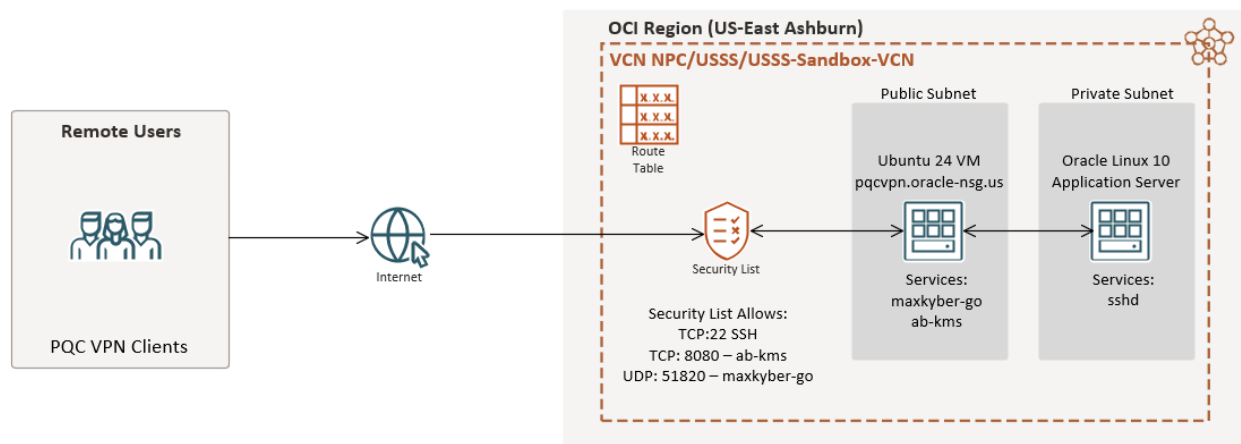


Ambit Client Running on macOS



Government Defense & Intelligence

OCI-PQC POC Infrastructure



ORACLE	OCI-PQC VPN Network Diagram					
	Oracle Government Defense & Intelligence					
Proof-of-Concept Design	Size: Cust	Date: 03SEP25	Drawing # 0925-01	Revision: 1.1	GCM ID: 0-0000000	
Oracle Government Defense & Intelligence	scale: Not to scale		by: Phil M.Dolbow			sheet: 1

Network Diagram

Performance tests were conducted using the Google Chrome browser and the fast.com speed test website. The performance testing was done with clients connected and disconnected from the American Binary PQC VPN client. The speed tests were run several times on each client, and the test results were averaged.

Performance Test results:

Mac Client (connected to 5g wireless access point):

Disconnected: 87 Mbps down, 30 Mbps up, Latency: 30ms

Connected: 87 Mbps down, 12 Mbps up, Latency: 38ms

Windows 11 Client (connected to 1Gb wired network):

Disconnected: 160 Mbps down, 19 Mbps up, Latency: 22ms

Connected: 130 Mbps down, 20 Mbps up, Latency: 34ms

Windows 10 Client (connected to 1Gb wired network):

Disconnected: 810 Mbps down, 370 Mbps up, Latency: 2ms

Connected: 280 Mbps down, 200 Mbps up, Latency: 4ms

Android Client (connected to 5g wireless access point):

Disconnected: 100 Mbps down, 45 Mbps up, Latency: 30ms

Connected: 66 Mbps down, 48 Mbps up, Latency: 40ms

Ubuntu Server CPU load and memory usage:

```
top - 18:21:24 up 6 days, 4:08, 1 user, load average: 1.82, 0.79, 0.30
Tasks: 122 total, 1 running, 121 sleeping, 0 stopped, 0 zombie
%Cpu(s): 9.5 us, 39.5 sy, 0.0 ni, 13.0 id, 0.0 wa, 0.0 hi, 13.0 si, 25.0 st
MiB Mem : 15989.7 total, 14164.2 free, 533.4 used, 1580.2 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 15456.3 avail Mem
```

Notes:

Side-by-side testing was done with the Cisco Anyconnect VPN client connected to OCNA US Midwest V2. Performance degradation was typically much higher than the American Binary client. The Oracle Cisco VPN testing was done only on the MacOS client, and the results were as follows: Connected: 51 Mbps down, 13 Mbps up, Latency: 49ms.

As seen above, the load on the VPN server was minimal with a load average of less than 2% and less than 4 GB of memory in use. This screenshot was taken when bandwidth testing

was being performed. When there was no load on the VPN server, the CPU load average was stable at 0.00%.

The client software is simple to use, has a nice UI, and connects very fast and is stable on all platforms we tested.

It is unknown where the bottleneck is in the tests on the Windows 10 system in the Oracle lab in Reston. Note that the latency on the system increases from 2ms to around 150ms when the load test is running.

When connected to the public facing server, systems in a private subnet in the same VCN are reachable via the PQC VPN when the security lists are configured to allow that traffic.

Recommended Enhancements:

- Implement a site-to-site solution for interconnecting on-prem and cloud devices as well as cloud-cloud systems. Ultimately, enhance the OCI site-to-site IPSEC VPN solution to have the option to use PQC technology.
- Add the capability to turn split tunnelling on/off in the American Binary administration console.
- Add the solution to the Oracle Marketplace, preferably a preconfigured appliance running on the Oracle Linux 10 platform.
- Adding the ability for the server to route between connected clients would be very beneficial.

Conclusion

Working together, Oracle and American Binary successfully tested the PQC VPN client-server architecture using resources in Oracle Cloud. The tests demonstrated that the client works on multiple platforms and although throughput and latency degrade somewhat, this is typical of all VPN products.

The advent of quantum computing marks a paradigm shift in cybersecurity risk, requiring immediate action in transitioning to quantum-safe technologies. Oracle and American Binary exemplify the industry's push toward PQC by innovating field-tested, standards-compliant solutions aimed at protecting the world's most critical digital assets from emerging quantum threats. Organizations looking to protect their information infrastructure must proactively adopt PQC technologies and companies like Oracle and American Binary are paving the way.