WHITE PAPER

Terniion™

CNSA 2.0 Compliance Documentation

Executive Summary

This document certifies that Xiid's Terniion™ solution not only meets but exceeds the requirements established in the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), as announced by the National Security Agency (NSA) in September 2022 and updated in May 2025. Xiid's Terniion architecture implements quantum-resistant cryptographic algorithms and maintains compliance with all CNSA 2.0 specifications for National Security Systems (NSS).

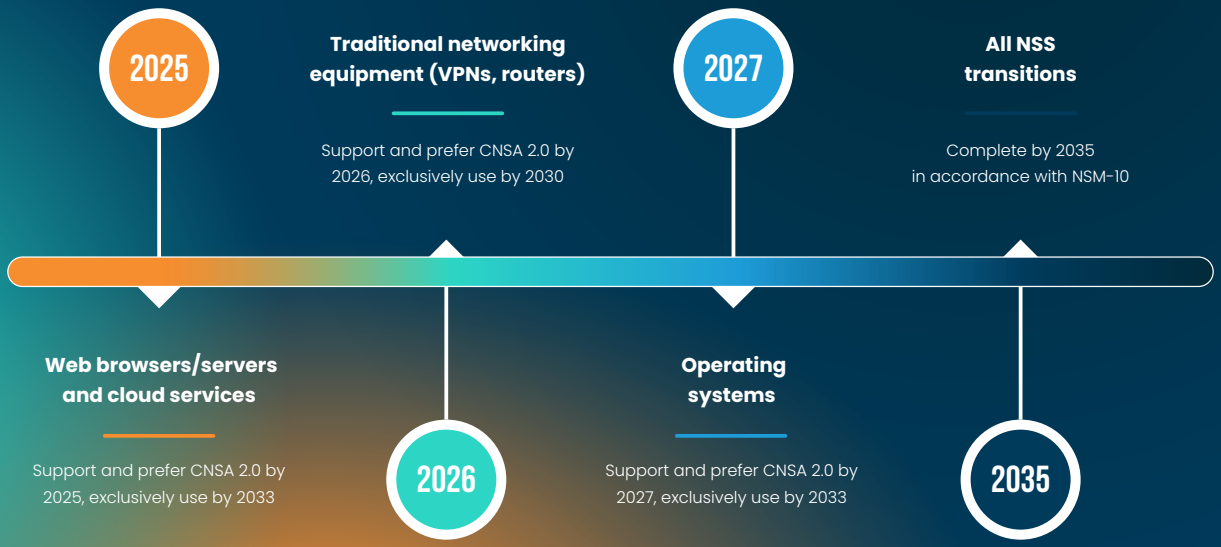
The Terniion platform implements a defense-in-depth encryption strategy utilizing three distinct layers of cryptographic protection, including NIST-approved post-quantum algorithms that surpass the minimum CNSA 2.0 requirements. Additionally, Xiid's outbound-only architecture provides enhanced security beyond CNSA 2.0 mandates by eliminating traditional attack vectors through closed inbound ports.

CNSA 2.0 Overview and Compliance Timeline

CNSA 2.0 represents the NSA's updated guidance for cryptographic protection against both classical and quantum computing threats. The suite addresses the urgent need to protect National Security Systems from cryptanalytically relevant quantum computers (CRQC) by mandating quantum-resistant algorithms.[1][2]

Key CNSA 2.0 Timeline Requirements

The NSA has established specific compliance deadlines for different technology categories. Xiid's Terniion solution currently implements CNSA 2.0-compliant algorithms, positioning organizations ahead of these mandatory compliance deadlines.



Terniion Architecture Overview

Xiid's Terniion technology establishes process-to-process communication channels that operate exclusively through outbound connections. This architecture fundamentally reimagines network security by eliminating traditional attack surfaces rather than defending against them. Using patented SealedTunnel™ technology creates triple-encrypted, quantum-secure tunnels that protect data in transit across any network environment, including hostile and degraded networks.

Terniion architecture ensures that all parties, including endpoints and intermediary systems, have no excessive knowledge of sensitive data or locations, implementing true zero-trust principles that exceed standard zero-trust implementations.

CNSA 2.0 Compliance Summary Table

Algorithm Function	CNSA 2.0 Requirement	Xiid Implementation	Layer	Terniion Fully Compliant
Symmetric-Key Encryption	AES-256	AES-256 GCM AEAD	Innermost	☑
Key Establishment	ML-KEM-1024 (Kyber)	ML-KEM-1024	Middle	☑
Digital Signatures	ML-DSA Level V (Dilithium)	ML-DSA Level V	Middle	☑
Transport Security	TLS 1.3 compliant	TLS 1.3 quantum-supported	Outer	☑
Hashing Algorithms	SHA-384/SHA-512	SHA-512	All layers	☑

CNSA 2.0 Algorithm Compliance Details

Symmetric-Key Encryption: AES-256 GCM AEAD

CNSA 2.0 Requirement: Advanced Encryption Standard (AES) with 256-bit keys for symmetric block cipher information protection (FIPS PUB 197).[1]

Xiid Implementation: Terniion's innermost encryption layer utilizes AES-256 in Galois/Counter Mode (GCM) with Authenticated Encryption with Associated Data (AEAD). This configuration provides:

- 256-bit key length meeting the CNSA 2.0 requirement
- Authenticated encryption ensuring both confidentiality and integrity
- Quantum-secure symmetric encryption proven resistant to quantum computing attacks
- FIPS 197-compliant implementation

The use of AES-256 GCM AEAD represents best-in-class symmetric encryption, providing tamper-proof communications where any attempt to modify encrypted data is immediately detected. This innermost layer serves as the final protection barrier for all data traversing SealedTunnel connections.

Post-Quantum Key Establishment: ML-KEM (Kyber)

CNSA 2.0 Requirement: ML-KEM (Module Lattice-Based Key Encapsulation Mechanism, previously CRYSTALS-Kyber) using Level V parameters (ML-KEM-1024) for asymmetric key establishment (FIPS PUB 203, anticipated).[1][2]

Xiid Implementation: SealedTunnel's middle encryption layer implements ML-KEM-1024 (Kyber) for quantum-resistant key establishment. This lattice-based algorithm:

- Provides quantum-resistant key encapsulation meeting NIST FIPS 203 standards
- Uses Level V (ML-KEM-1024) parameters as specified by CNSA 2.0
- Protects against "Harvest Now, Decrypt Later" (HNDL) attacks where adversaries collect encrypted data for future quantum decryption
- Ensures forward secrecy and perfect forward secrecy (PFS) for all sessions

Xiid's lattice-based construction ensures that even quantum computers with Shor's algorithm capabilities cannot break the key establishment mechanism, future-proofing data protection for decades.

Post-Quantum Digital Signatures: ML-DSA (Dilithium)

CNSA 2.0 Requirement: ML-DSA (Module Lattice-Based Digital Signature Algorithm, previously CRYSTALS-Dilithium) using Level V parameters for asymmetric digital signatures (FIPS PUB 204, anticipated).[1][2]

Xiid Implementation: SealedTunnel's middle encryption layer incorporates ML-DSA (Dilithium) for quantum-resistant digital signatures. This implementation:

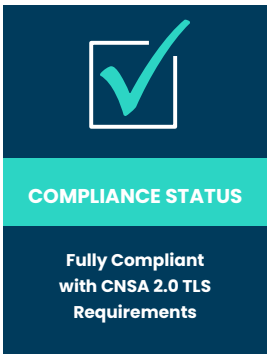
- Provides quantum-resistant authentication and non-repudiation
- Uses Level V parameters as mandated by CNSA 2.0
- Ensures integrity verification resistant to quantum computing attacks
- Complies with anticipated NIST FIPS 204 standards

The combination of ML-DSA signatures with ML-KEM key establishment in the middle layer creates a complete post-quantum cryptographic system that authenticates endpoints, establishes secure keys, and maintains quantum-resistant integrity throughout the connection lifecycle.

Outer Layer: TLS 1.3 with Quantum-Supported Cipher Suites

CNSA 2.0 Guidance: Web browsers, servers, and cloud services must support TLS configurations using CNSA 2.0 algorithms, with implementation following RFC 9151 for TLS and DTLS profiles.[1]

Xiid Implementation: SealedTunnel's outer encryption layer utilizes TLS 1.3 with quantum-supported cipher suites. This implementation:



- Provides transport-layer encryption using modern TLS 1.3 protocol
- Incorporates quantum-resistant cipher suite configurations
- Ensures compatibility with network infrastructure and inspection systems
- Disguises SealedTunnel traffic as standard HTTPS connections, providing operational security

The outer TLS 1.3 layer serves multiple purposes: it provides initial encryption, ensures compatibility with existing network infrastructure, and obfuscates the presence of the additional inner encryption layers from network observers.

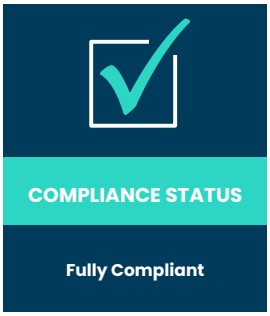
Secure Hashing Algorithms

CNSA 2.0 Requirement: SHA-384 or SHA-512 for computing condensed representations of information (FIPS PUB 180-4)[1].

Xiid Implementation: SealedTunnel utilizes SHA-512 hashing algorithms throughout its cryptographic operations:

- Certificate validation and integrity checking
- Key derivation functions
- Digital signature operations
- Data integrity verification
- Application process validation

These hash functions meet FIPS PUB 180-4 specifications and provide quantum-resistant hashing capabilities suitable for all classification levels.



Triple-Layer Encryption Architecture

Ternion's defense-in-depth encryption strategy implements three distinct layers of cryptographic protection, each serving specific security objectives:

Layer 1: Outer TLS 1.3 Encryption

Purpose: Transport security and network compatibility

Algorithm: TLS 1.3 with quantum-supported cipher suites

Function: Provides initial encryption, ensures compatibility with network infrastructure, obfuscates inner layers

Layer 2: Middle Post-Quantum Encryption

Purpose: Quantum-resistant key establishment and authentication

Algorithms: ML-KEM (Kyber) for key encapsulation, ML-DSA (Dilithium) for digital signatures

Function: Protects against quantum computing threats, prevents HNDL attacks, provides future-proof security

Layer 3: Inner AES-256 GCM AEAD

Purpose: Data confidentiality and integrity

Algorithm: AES-256 in GCM mode with AEAD

Function: Ensures data cannot be read or tampered with, provides quantum-secure symmetric encryption

This multi-layered approach ensures that even if one encryption layer were somehow compromised (theoretically), two additional independent layers continue protecting the data. The diversity of algorithms across layers—combining symmetric, asymmetric lattice-based, and transport-layer encryption—creates a cryptographic defense system that far exceeds single-layer protection.

Conclusion

Xiid's Terniion platform demonstrates comprehensive compliance with all CNSA 2.0 requirements while exceeding baseline mandates through its triple-layer encryption architecture and outbound-only communication model. The platform's implementation of AES-256 GCM AEAD for symmetric encryption, ML-KEM (Kyber) for post-quantum key establishment, ML-DSA (Dilithium) for post-quantum digital signatures, and TLS 1.3 with quantum-supported cipher suites ensures protection against both current and future quantum computing threats.

Organizations deploying Terniion today are positioned ahead of CNSA 2.0 compliance deadlines, with quantum-resistant protection already in place against Harvest Now, Decrypt Later threats and future quantum computing capabilities. The platform's proven performance in U.S. Department of Defense and federal agency deployments demonstrates real-world readiness for protecting the nation's most sensitive information.

References

[1] National Security Agency. (2022, September 7). Announcing the Commercial National Security Algorithm Suite 2.0. **NSA Cybersecurity Advisory**. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_ALGORITHMS.PDF

[2] National Security Agency. (2025, May 30). Announcing the Commercial National Security Algorithm Suite 2.0 (Updated). **NSA Cybersecurity Advisory**. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[3] Xiid Corporation. (2024). **More Secure, More Efficient, and More Value Than Zscaler**. Xiid White Paper.

[4] Xiid Corporation. (2024). **Xiid Delivers Post-Quantum Security**. https://www.xiid.com/other-resources/white-paper/xiid-delivers-post-quantum-security

[5] Xiid Corporation. (2025). **Securing CI/CD with SealedTunnel**. Xiid White Paper.

[6] Xiid Corporation. (2024). **Xiid Moving Target Defense: Revolutionizing Cybersecurity for the Modern Enterprise**. Xiid White Paper.

[7] PQShield. (2026, January 14). What is CNSA 2.0? The NSA's post-quantum roadmap. https://pqshield.com/what-is-cnsa-2-0-the-nsas-post-quantum-roadmap/

[8] Encryption Consulting. (2026, January 26). Quantum-Proof with CNSA 2.0. https://www.encryptionconsulting.com/quantum-proof-with-cnsa-2-0/