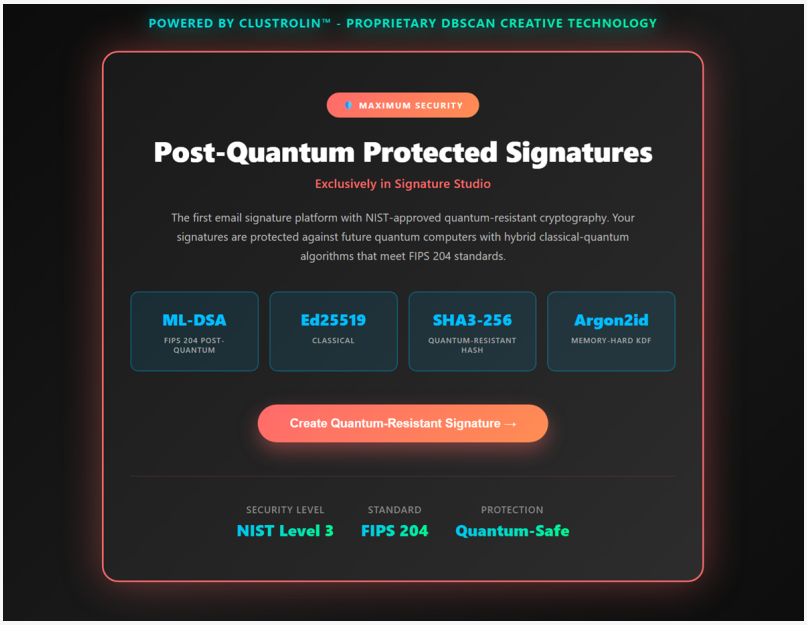
Smart Banner Hub Launches First Email Signature Platform with NIST-Approved Post-Quantum Cryptography

Portland startup introduces ML-DSA digital signatures, bringing quantum-resistant email authentication to professionals and small businesses.



Smart Banner Hub's Signature Studio introduces the world's first email signature platform with NIST-approved post-quantum cryptography, featuring ML-DSA, Ed25519, SHA3-256, and Argon2id algorithms meeting FIPS 204 standards.

BEAVERTON, OR, UNITED STATES, December 1, 2025 /EINPresswire.com/ -- BEAVERTON, OR — December 01, 2025 — Smart Banner Hub LLC today announced the deployment of NIST-approved post-quantum cryptography across its Maximum Security email signature platform, becoming the first company in the digital identity space to ship quantum-resistant signatures using ML-DSA (CRYSTALS-Dilithium) — the same cryptographic standard selected for U.S. federal systems.

The move positions Smart Banner Hub years ahead of the federal government's 2035 deadline for quantum-safe migration, offering businesses and professionals protection against a threat that most organizations haven't begun to address.

"Every RSA and elliptic curve signature in use today has an expiration date," said Ashwin Spencer, Founder and CEO of Smart Banner Hub. "When sufficiently powerful quantum computers arrive, Shor's algorithm will break them — regardless of key size. We're not waiting for that day. Our customers are protected now."

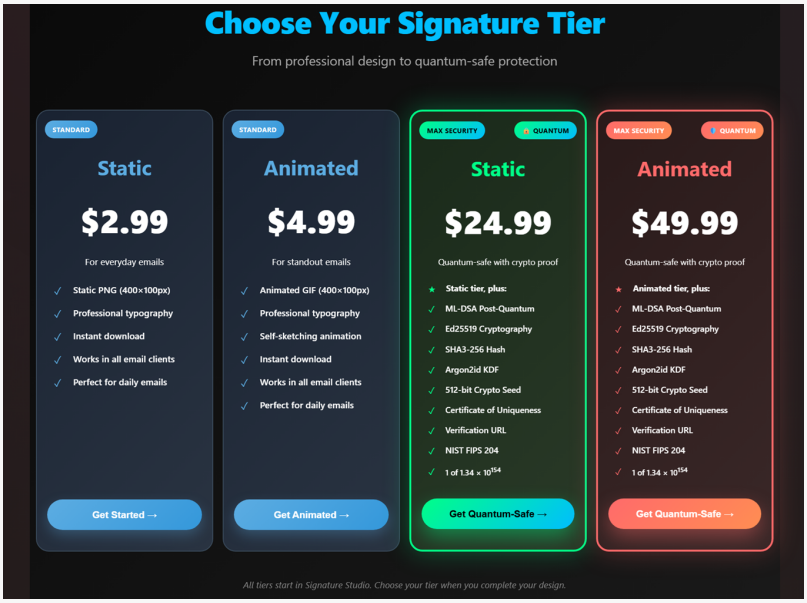
THE QUANTUM THREAT IS REAL

Cryptographic systems protecting everything from banking transactions to email authentication rely on mathematical problems that classical computers cannot solve efficiently. Quantum

computers running Shor's algorithm will render these protections obsolete.

The National Institute of Standards and Technology (NIST) spent eight years evaluating quantum-resistant alternatives, finalizing three post-quantum cryptographic standards in August 2024. ML-DSA (formerly CRYSTALS-Dilithium), based on lattice cryptography, emerged as the primary standard for digital signatures.

Smart Banner Hub has implemented ML-DSA alongside its existing Ed25519 classical signatures, creating a hybrid approach that provides security against both current and future threats.



Smart Banner Hub's signature tier pricing, showing quantum-safe protection available starting at $24.99 — making NIST FIPS 204 post-quantum cryptography accessible to professionals and small businesses, not just enterprise customers.

WHAT SMART BANNER HUB DELIVERS

Smart Banner Hub's Maximum Security signatures now include:

> Every RSA and elliptic curve signature in use today has an expiration date. Shor's algorithm will break them — regardless of key size. We're not waiting. Our customers are protected now."
>
> *Ashwin Spencer*

 ML-DSA (CRYSTALS-Dilithium) — NIST FIPS 204 post-quantum digital signatures
 Ed25519 — Battle-tested classical cryptography for current protection
 SHA3-256 — Quantum-resistant hashing
 Argon2id — Memory-hard key derivation resistant to GPU and quantum attacks
 Clustrolin™ DBSCAN Creative Engine — Mathematically unique animated signatures

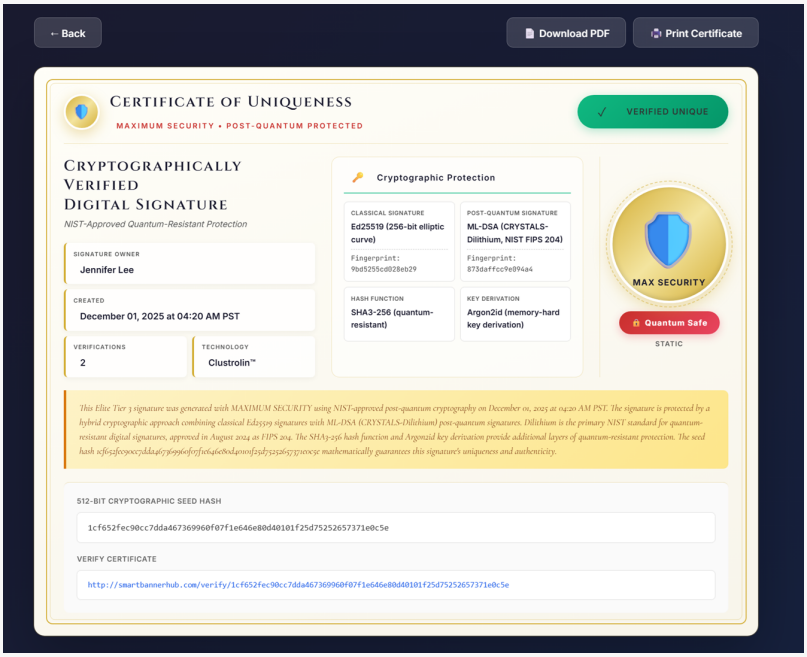
Each signature is backed by a 512-bit cryptographic seed with a uniqueness guarantee of approximately 10^154 possible combinations — more than the number of atoms in the observable universe.

BEYOND SECURITY THEATER

Spencer emphasized that the implementation uses real, production-ready post-quantum cryptography — not marketing claims.

"There's a lot of 'quantum-ready' language in the market that doesn't mean anything," Spencer said. "We're not using larger RSA keys and calling it quantum-resistant. We implemented actual lattice-based cryptography that mathematicians believe will withstand quantum attacks. Every claim on our certificates is technically accurate and defensible."

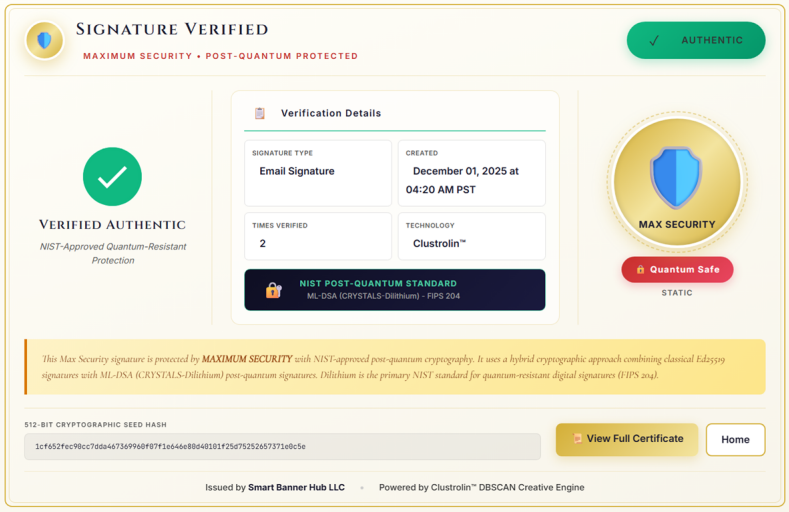
The platform provides cryptographic verification accessible via a simple link embedded in each email signature, allowing recipients to verify authenticity with one click.



Smart Banner Hub's Certificate of Uniqueness displays cryptographically verified digital signature details including Ed25519, ML-DSA (CRYSTALS-Dilithium), SHA3-256, and Argon2id protection with the 512-bit seed hash and one-click verification link.

DEMOCRATIZING ADVANCED CRYPTOGRAPHY

Smart Banner Hub's mission is to make enterprise-grade cryptographic protection accessible to professionals and small businesses — not just Fortune 500 companies with dedicated security teams.



Smart Banner Hub's public verification page confirms signature authenticity with one click, displaying NIST post-quantum standard compliance, Clustrolin™ technology, and the 512-bit cryptographic seed hash.

"NIST-level cryptography shouldn't require a NIST-level budget," Spencer said. "A freelancer protecting their personal brand deserves the same cryptographic guarantees as a multinational corporation. We built this for everyone."

The company's Clustrolin™ DBSCAN Creative Engine transforms standard email signatures into animated, mathematically unique visual identities — combining aesthetic differentiation with cryptographic proof of authenticity.

AVAILABILITY

Smart Banner Hub's Maximum Security signatures with post-quantum cryptography are available now at smartbannerhub.com. The Maximum Security package includes full ML-DSA (Dilithium) post-quantum protection, static (PNG) and animated (GIF) DBSCAN signatures, and certificates of uniqueness with complete cryptographic verification.

==========

ABOUT SMART BANNER HUB

Smart Banner Hub LLC, based in Beaverton, Oregon, is pioneering the intersection of mathematical creativity and digital identity. The company's proprietary Clustrolin™ DBSCAN Creative Engine transforms everyday content into algorithmically unique animated signatures, serving innovation and human emotion.

Founded by Ashwin Spencer — a former cybersecurity teaching assistant at the University of Missouri - St. Louis with five degrees (including MS Computer Science, MS Analytics from Georgia Tech, and MS Electrical & Computer Engineering) and 20+ years of experience in aerospace, defense, and technology at companies including NAVAIR, Raytheon, Pratt & Whitney, Boeing, Charter, and Intel — Smart Banner Hub has been featured on AP News and hundreds of media outlets as a category creator in mathematical creativity applications.

==========

MEDIA CONTACT

Ashwin Spencer
Founder & CEO, Smart Banner Hub LLC
ashwin@smartbannerhub.com
+1 971-217-6983

Digital Resources:
Website: https://smartbannerhub.com
LinkedIn: https://linkedin.com/in/ashwinspencer
Press Kit: https://smartbannerhub.com/presskit.html

==========

TECHNICAL BACKGROUND

WHAT IS POST-QUANTUM CRYPTOGRAPHY?

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to resist attacks from quantum computers. Current widely-used algorithms like RSA and elliptic curve cryptography (ECC) will be broken by quantum computers running Shor's algorithm. NIST finalized three post-quantum standards in August 2024 after an eight-year evaluation process.

WHAT IS ML-DSA (CRYSTALS-DILITHIUM)?

ML-DSA (Module-Lattice-Based Digital Signature Algorithm), previously known as CRYSTALS-Dilithium, is NIST's primary standard for post-quantum digital signatures (FIPS 204). It is based on the hardness of the Module Learning With Errors (MLWE) problem — a mathematical challenge believed to be resistant to both classical and quantum attacks.

WHAT IS THE HYBRID APPROACH?

Smart Banner Hub uses both classical (Ed25519) and post-quantum (ML-DSA) signatures simultaneously. This provides defense in depth: if one algorithm is compromised, the other still provides protection. This is the approach recommended by NIST during the transition period to post-quantum cryptography.

FEDERAL TIMELINE

The U.S. federal government has mandated full migration to quantum-safe cryptography by 2035, with legacy algorithms (RSA, ECC) to be phased out by 2030. Smart Banner Hub's implementation puts its customers ahead of this timeline.

Ashwin Spencer
Smart Banner Hub LLC
+1 971-217-6983
email us here
Visit us on social media:
LinkedIn