Meeting and Exceeding Cybersecurity Standards with the Randomized Data Handshake (RDH)

Chad Wanless, Dave Palachik

CEW Systems Canada Inc.
5 McAlpine Ave
Ajax, Ontario
L1T 4H9
chad.wanless@cew-s.com

1. Executive Summary

As cyber threats grow in sophistication and the emergence of quantum computing begins to undermine classical encryption schemes, the need for a new cryptographic framework has never been more urgent. Traditional methods relying on asymmetric key exchanges and transmitted credentials face vulnerabilities from both modern brute-force attacks and quantum-based decryption techniques such as Shor's and Grover's algorithms. The Randomized Data Handshake (RDH) system provides a robust and future-proof alternative.

RDH is a novel, zero-trust encryption and authentication framework that eliminates the need to transmit session keys or sensitive authentication data. Instead, RDH uses a pre-shared set of symmetric keys to generate randomized challenge instructions. These instructions allow both parties to independently derive matching session keys without ever transmitting them, effectively emulating the behavior of quantum entanglement in data exchange. The result is an encryption handshake that is immune to interception, resistant to quantum decryption, and suitable for even the most constrained environments like smart cards, IoT sensors, and unmanned systems.

This white paper provides a comprehensive analysis of RDH against the backdrop of major regulatory, cybersecurity, and payments standards. We show that RDH:

- Meets or exceeds the data security controls outlined in PCI-DSS
- Implements Zero Trust principles as defined in NIST SP 800-207
- Provides phishing-resistant authentication per NIST SP 800-63B and FIDO2
- Supports Strong Customer Authentication (SCA) as mandated by PSD2
- Aligns with the cryptographic goals of EMVCo and ISO 7816/14443 for contactless cards
- Surpasses the theoretical quantum safety levels of current NIST post-quantum candidates in constrained environments

RDH is already supported by a peer-reviewed white paper and third-party validation through Saskatchewan Polytechnic. With prototype-ready hardware configurations and practical deployment models for FinTech, POS terminals, and edge devices, RDH is ready to transition from R&D into operational use.

Supporting Publications:

- Peer-reviewed white paper: https://www.worldscientific.com/doi/10.1142/S2705109924710019

- Independent review by Saskatchewan Polytechnic: https://5d6f9aff-035d-4667-807c-4f3241f5df83.usrfiles.com/ugd/5d6f9a_89233d6ea24245c78687f7698d0e92a5.pdf

This document serves as both a compliance justification and an integration roadmap for industry partners, regulators, and technology integrators seeking a resilient and standards-aligned cryptographic upgrade path.

2. Overview of RDH

The Randomized Data Handshake (RDH) is a secure encryption and authentication protocol designed to work in high-risk, resource-constrained, and post-quantum environments. Unlike traditional encryption methods that rely on transmitting session keys, public keys, or identifiable credentials, RDH uses only randomized data to enable mutual authentication and session key generation.

At its core, RDH wraps around existing symmetric encryption algorithms like ASCON or AES, enhancing their security posture without replacing them. It employs two sets of pre-shared symmetric keys between communicating parties. When two RDH-enabled devices initiate a session, they exchange randomized, encrypted challenge instructions and test data—never the keys themselves. Each side independently uses these challenge instructions to derive matching temporary session keys from their pre-loaded key pool.

Because the session keys are never transmitted and the data exchanged is indistinguishable from noise, RDH renders intercepted communications useless to attackers. This makes RDH particularly valuable in zero-trust architectures, where devices cannot assume trust based on location, identity, or infrastructure.

Key features of RDH include:

- **No key transmission**: All keys are derived independently using randomized lookup instructions.
- **Quantum-resilient architecture**: By avoiding public key infrastructure (PKI) and using large symmetric key pools, RDH resists quantum attacks like Grover's algorithm.
- **Hardware-friendly**: RDH is optimized for embedded devices, smart cards, and IoT sensors where memory and compute resources are limited.
- **Man-in-the-middle immunity**: RDH verifies both parties through symmetric key authentication, eliminating spoofing risks.

- **Multipurpose deployment**: Originally developed for FinTech, RDH is also effective for POS terminals, secure drone communication, and edge computing in contested environments.

In practice, RDH emulates a form of quantum entanglement in communication. Just as entangled particles reflect changes in each other without observable transmission, RDH-enabled devices synchronize secure states using only indirect randomized instructions. This novel approach provides an elegant and resilient alternative to conventional encryption protocols.

3. Comparative Standards Analysis Table

The following table presents a side-by-side comparison of key cybersecurity and payment standards with the features and capabilities offered by the RDH protocol. This analysis demonstrates RDH's alignment with—and in many cases, its advancement beyond—the baseline requirements established by each standard.

Standard / Framework	**Key Requirement or Objective**	**RDH Alignment and Enhancement**
PCI-DSS	Protect cardholder data, avoid plaintext transmission	RDH never transmits card data or session keys; encrypted handshake only
NIST SP 800-63B	Phishing-resistant, multi-factor authentication	RDH supports 2FA via smart card/NFC and password or PIN
NIST SP 800-207 (Zero Trust)	No implicit trust; context-based access	RDH ensures mutual authentication with no shared credential exposure
EMVCo / ISO 7816 / 14443	Secure contactless smart card authentication	RDH complements smart card standards with quantum-resilient session handling
FIDO2 / WebAuthn	Local device-based key generation; no shared secrets	RDH uses device-resident key pools and randomized derivation

PSD2 (EU)	Strong Customer Authentication (SCA) for payments	RDH enables card + device-based SCA for e-commerce and POS
NIST Post-Quantum Cryptography	Resistance to Grover's and Shor's algorithms	RDH uses 2,048-bit key pools and randomized instructions, not math-based PKI
FIPS 140-3 (Cryptographic Modules)	Use of validated cryptographic components	RDH wraps around validated symmetric ciphers like AES and ASCON

This table illustrates that RDH is not only compliant with major security frameworks but also introduces novel cryptographic mechanics that mitigate real-world threats such as POS terminal swaps, keyboard logging malware, NFC walk-by skimming, and replay attacks. These capabilities make RDH a highly versatile and standards-compatible upgrade path.

4. Deep Dive by Standard

PCI-DSS: RDH surpasses PCI-DSS requirements by eliminating cardholder data (CHD) from the transaction stream. Because RDH never transmits PAN, CVV, expiration dates, or session keys, it prevents CHD exposure at rest and in transit. By converting all credential handling into randomized challenge instructions, RDH exceeds current expectations for point-of-sale and online payment security.

NIST SP 800-63B: This guideline prioritizes phishing-resistant authentication mechanisms. RDH supports physical tokens (e.g., NFC-enabled smart cards) and a second factor (password or PIN) without ever revealing or storing authentication secrets in an accessible format. The randomized session generation model makes RDH inherently resilient to phishing, replay, and spoofing.

NIST SP 800-207 (Zero Trust Architecture): RDH implements mutual authentication without assuming device, network, or identity trust. By using randomized challenge instructions, devices verify each other dynamically at each transaction, ensuring compliance with Zero Trust principles. Every session is independently authenticated using local keys, and no central authority is assumed.

EMVCo / ISO 7816 / ISO 14443: While EMV smart cards rely on legacy cryptographic protocols and sometimes share identifiers in cleartext, RDH adds a randomized encryption wrapper that makes communication sessions quantum-resilient and opaque to observers. When

embedded in a card chip or secure element, RDH enables enhanced contactless and NFC operations without breaking backward compatibility.

FIDO2 / WebAuthn: RDH aligns with FIDO2 objectives by enabling hardware-resident identity verification without shared secrets or centralized storage. RDH provides the added benefit of post-quantum resilience and offline authentication (e.g., smart card to POS) even where networked identity services are unavailable.

PSD2 (EU Directive): RDH enables Strong Customer Authentication by combining something the user has (the smart card) and something the user knows (PIN/password), while securing the exchange with randomized encrypted sessions. The system can also be extended to biometric PIN entry for higher-assurance SCA compliance in digital banking and e-commerce.

NIST Post-Quantum Cryptography Guidelines: Where most post-quantum algorithms depend on large key exchanges and polynomial math (susceptible to side-channel or storage risks), RDH bypasses these methods entirely. Using 2,048-bit key pools and randomized index instructions, RDH creates ephemeral session keys without transmission, and is resistant to Grover-based search due to its lack of deterministic structure.

FIPS 140-3: RDH enhances compliance by wrapping around validated symmetric encryption modules like AES or ASCON. It does not require changes to core cryptographic engines, enabling easier integration within certified hardware and software environments that meet FIPS 140-3 requirements.

7. Conclusion and Next Steps

The Randomized Data Handshake (RDH) is a timely and practical response to the rising urgency of data protection in an age of escalating cyber threats and quantum computing. It combines quantum-safe cryptography with zero-trust principles, providing strong security without increasing complexity or requiring transmission of sensitive credentials.

This white paper has shown that RDH meets or exceeds the requirements of today's dominant security standards, including PCI-DSS, NIST guidelines, PSD2, FIPS 140-3, and EMVCo protocols. Moreover, RDH's unique architecture not only addresses modern cybersecurity challenges but anticipates future threats, particularly those introduced by quantum computing and edge-based communications.

To realize its potential impact, RDH is ready for:

- **Pilot deployment** in FinTech, healthcare, and smart infrastructure environments
- **Integration** into commercial products, including POS terminals, NFC readers, and mobile banking apps

- **Evaluation** by regulatory and certification bodies for inclusion in cybersecurity and digital identity standards
- **Collaboration** with institutions like NIST, PCI SSC, and EMVCo to test, validate, and standardize the protocol

With third-party validation, peer-reviewed research, and implementation-ready components, RDH offers governments, financial institutions, and cybersecurity vendors a compelling path forward. We welcome engagement from industry stakeholders to further pilot, test, and standardize RDH as a foundational element of tomorrow's secure communications infrastructure.

5. Use Case Alignment

RDH was originally designed for secure financial transactions and has since evolved into a flexible encryption layer applicable to a wide range of civilian applications. Below are example use cases that illustrate RDH's versatility.

Civilian Sector Applications:

- **Point-of-Sale Terminals (POS):** RDH-enabled smart cards prevent terminal tampering, eliminate card skimming risks, and provide mutual authentication without requiring data to be transmitted or stored. Each transaction is verified through session keys derived from random instructions, neutralizing intercept attacks.
- **E-Commerce Transactions:** RDH supports 2FA via card tap or secure NFC reader, protecting customers from malware, keystroke logging, and phishing attacks. Cardholder information is never entered manually or transmitted, significantly reducing fraud.
- **Banking & FinTech:** RDH allows secure login, transaction approval, and multi-factor authentication using dedicated cards or NFC-enabled phones with embedded secure elements. It prevents walk-by skimming and offers real-time protection with minimal latency.
- **Healthcare & Telemedicine:** Secure transmission of patient data over Wi-Fi or mobile links using RDH-enhanced devices ensures privacy compliance (e.g., HIPAA/GDPR) while reducing the impact of man-in-the-middle attacks in critical care environments.

These use cases demonstrate how RDH addresses long-standing weaknesses in current systems—such as transmission of authentication data, reliance on asymmetric encryption for session key exchange, and vulnerability to interception. Whether embedded in e-commerce platforms, financial apps, healthcare devices, or IoT endpoints, RDH adapts to the security landscape while maintaining regulatory alignment and real-world performance.

6. Regulatory and Compliance Readiness

RDH is designed with regulatory alignment at its core. Its compatibility with existing and emerging cybersecurity frameworks makes it a strong candidate for real-world deployment across regulated industries. Several aspects of RDH's architecture support immediate engagement with relevant bodies:

- **PCI-DSS**: RDH eliminates the transmission of cardholder data, significantly reducing compliance burden and risk of breach. It enhances transaction integrity at both the device and network level.
- **EMVCo and ISO 14443**: RDH enhances contactless smart card protocols by introducing randomized challenge-response mechanisms that are quantum-resilient and backward-compatible.
- **NIST SP 800 series**: RDH directly aligns with SP 800-63B for digital identity assurance and SP 800-207 for Zero Trust Architecture. The mutual authentication and key-independent session creation methods also support secure access practices defined in SP 800-53.
- **PSD2 (EU Directive)**: RDH enables Strong Customer Authentication (SCA) for both physical and digital payment environments, fulfilling regulatory mandates without relying on biometric storage or cloud-managed tokens.
- **FIPS 140-3**: RDH complements FIPS-compliant symmetric algorithms such as AES and ASCON and can be deployed within validated cryptographic modules without modification.

To accelerate adoption, RDH is supported by a peer-reviewed technical paper and third-party validation through Saskatchewan Polytechnic's Digital Innovation Center of Excellence. These foundations provide confidence to regulators, banking institutions, and cybersecurity authorities.

RDH is also well-positioned for formal engagement with bodies such as:

- **NIST NCCoE**: Potential for contribution to post-quantum cryptography and zero trust pilot programs.
- **EMVCo**: Through technical working groups or as a candidate for secure payment protocol enhancements.
- **PCI SSC**: As a quantum-safe enhancement to PCI-validated device architectures.

RDH's readiness includes not only technical capability but alignment with key industry certifications, compliance controls, and implementation pathways, making it a near-term candidate for pilot integration, sandbox testing, or standards contribution.

7. Conclusion and Next Steps

The Randomized Data Handshake (RDH) is a timely and practical response to the rising urgency of data protection in an age of escalating cyber threats and quantum computing. It combines quantum-safe cryptography with zero-trust principles, providing strong security without increasing complexity or requiring transmission of sensitive credentials.

This white paper has shown that RDH meets or exceeds the requirements of today's dominant security standards, including PCI-DSS, NIST guidelines, PSD2, FIPS 140-3, and EMVCo protocols. Moreover, RDH's unique architecture not only addresses modern cybersecurity challenges but anticipates future threats, particularly those introduced by quantum computing and edge-based communications.

To realize its potential impact, RDH is ready for:

- **Pilot deployment** in FinTech, healthcare, and smart infrastructure environments
- **Integration** into commercial products, including POS terminals, NFC readers, and mobile banking apps
- **Evaluation** by regulatory and certification bodies for inclusion in cybersecurity and digital identity standards
- **Collaboration** with institutions like NIST, PCI SSC, and EMVCo to test, validate, and standardize the protocol

With third-party validation, peer-reviewed research, and implementation-ready components, RDH offers governments, financial institutions, and cybersecurity vendors a compelling path forward. We welcome engagement from industry stakeholders to further

pilot, test, and standardize RDH as a foundational element of tomorrow's secure communications infrastructure.

Contact: To learn more, collaborate, or request implementation materials: Chad Wanless, CEW Systems Canada Inc.
Email: contact@cew-s.com
Website: https://www.cew-s.com