Rocket® software

Rocket® z/Assure®

Rocket® Quantum Safety Analyzer (RQSA)

Introduction

Quantum computing does not yet pose an immediate operational threat to mainframe systems, but it represents a critical strategic risk regarding data confidentiality. The primary concern is **"Harvest Now, Decrypt Later" (HNDL)** attacks against encrypted long lived, highly valued data commonly maintained on z/OS® platforms. Data stolen today will be broken into once functional quantum computers appear.

Subsequently, mainframes are now prime candidates for HNDL and are uniquely exposed due to:

01 **Data gravity**
Mainframes store decades of sensitive, regulated data.

02 **Longevity**
Mainframe data often has 20–40-year confidentiality requirements.

03 **Crypto inertia**
Some applications still rely on RSA key exchange, ECDSA signatures and Static Keys embedded in legacy code.

RQSA enhances an organization's security posture by providing total visibility into mainframe cryptographic risks. Through an agent-based approach, it automatically identifies quantum-vulnerable assets, quantifies exposure, and prioritizes what needs to be remediated first and helps you plan the migration.

By strategically prioritizing remediation efforts, RQSA enables more informed decision-making, minimizes future migration risks, and reinforces long-term confidence in both business operations and customer data integrity.

Rocket Quantum Safety Analyzer (RQSA) is uniquely positioned to help organizations address critical challenges, including:

- The complexity of crypto-migration.
- Exposure to "harvest now, decrypt later" (HNDL) threats.
- The impending obsolescence of traditional asymmetric encryption.

By leveraging RQSA, organizations gain enterprise-grade visibility into critical cryptographic and security components, including:

01

Integrated Cryptographic Service Facility (ICSF) activity for monitoring operational cryptographic processes.

02

Resource Access Control Facility (RACF) keyrings to assess key management and usage.

03

UNIX® System Services (USS) cipher configurations for evaluating encryption standards in distributed environments.

04

Cryptographic Coprocessor Data (COMPID) status information to track hardware security module health and readiness.

05

RACF® digital certificates for managing identity, trust chains, and secure communications.

06

General ICSF and cryptographic environment insights via COMPID, providing a consolidated view of system-wide cryptographic posture.

Key benefits

System-level crypto (ICSF, Coprocessors)

RQSA delivers a comprehensive, enterprise-level assessment of the cryptographic controls that underpin the confidentiality, integrity, and trust of modern digital environments. This evaluation spans industry-standard algorithms embedded across applications, operating systems, and communication protocols, encompassing symmetric encryption, asymmetric cryptography, hashing functions, and supporting randomness mechanisms.

Key algorithms evaluated include:

MD5 and **SHA-256**	• Cryptographic hashing algorithms used to ensure data integrity and detect tampering.
AES-128 and **AES-256**	• Symmetric encryption standards that safeguard sensitive data at rest and in transit.
ECC P-256 and **RSA-2048**	• Asymmetric cryptographic methods supporting secure key exchange, authentication, and digital signatures.
PRNG (Pseudo-Random Number Generation)	• Critical to generating secure cryptographic keys and ensuring the strength of encryption processes.

This analysis enables organizations to better understand their current cryptographic posture, identify potential vulnerabilities, and plan for future-ready, quantum-resilient security strategies.

Identity and certificates (RACF keyrings and certificates)

RQSA provides a comprehensive assessment of identity and certificate management practices by analyzing cryptographic libraries and communication protocols to evaluate usability, configuration integrity, and emerging quantum-related risks.

As part of this evaluation, RQSA examines:

OpenSSL - A widely adopted, enterprise-grade open-source cryptographic library used across diverse platforms.

- Delivers core cryptographic services, including encryption, hashing, key management, and secure communications via TLS/SSL.
- Assessment focuses on configuration practices, protocol implementation, dependency risks, and long-term viability in the context of evolving and quantum-resistant cryptographic standards.

Java™ Cryptography Architecture (JCA) and Java Cryptography Extension (JCE) - A standardized, provider-based framework supporting cryptographic operations within Java environments.

- RQSA evaluates implementation consistency, configuration security, and alignment with enterprise cryptographic policies and standards.
- Analysis helps identify gaps in governance, potential vulnerabilities, and opportunities to strengthen the overall cryptographic posture.

This holistic approach enables organizations to ensure robust identity management, strengthen trust frameworks, and align certificate and cryptographic practices with future-ready security requirements.

Application/Runtime (USS, OpenSSL, SSH)

RQSA provides in-depth analysis of application and runtime-level cryptographic controls across UNIX System Services (USS), OpenSSL implementations, and Secure Shell (SSH) configurations. This assessment focuses on identifying security posture, configuration effectiveness, and exposure to emerging risks, including those introduced by quantum computing.

Secure shell (SSH) assessment

RQSA evaluates SSH implementations, which are widely used to enable secure remote access and encrypted data transfer across enterprise environments. Key areas of analysis include:

- **Authentication and key exchange mechanisms** - Reviewing the use of RSA or ECC algorithms.
- **Session encryption** - Assessing symmetric encryption standards, such as AES, used to ensure confidentiality of active sessions.
- **Configuration and lifecycle management** - Evaluating algorithm selection, key management practices, and overall configuration hygiene.

Quantum risk consideration

Traditional SSH implementations rely on cryptographic algorithms that are not resistant to quantum-enabled attacks. Without adopting post-quantum cryptographic methods or enabling cryptographic agility, organizations may face long-term confidentiality risks, particularly from “harvest now, decrypt later” threat scenarios.

SSH establishes secure communications through a combination of **asymmetric cryptography** (for authentication and key exchange) and **symmetric encryption** (to protect session data). RQSA’s analysis helps organizations identify vulnerabilities in this model and prioritize remediation strategies aligned with future-ready, quantum-resilient security frameworks.

Post-quantum risk mitigation strategy

RQSA enables organizations to proactively address emerging post-quantum cryptographic risks by delivering actionable insights and a structured approach to mitigation. As quantum computing advances, traditional cryptographic algorithms - particularly those used in asymmetric encryption - face the potential for rapid obsolescence, introducing significant long-term security challenges.

01

Cryptographic inventory and visibility

Establish a comprehensive inventory of cryptographic assets, algorithms, key usage, and dependencies across applications, infrastructure, and data flows. RQSA provides the foundational visibility required to identify vulnerable components and prioritize remediation efforts.

02

Cryptographic agility

Implement frameworks and architectures that support rapid replacement or updating of cryptographic algorithms without significant disruption. This ensures the ability to transition seamlessly to post-quantum cryptographic standards as they mature.

03

Adoption of post-quantum cryptography (PQC)

Begin evaluating and integrating quantum-resistant algorithms based on emerging standards (e.g., NIST PQC candidates). Early adoption reduces exposure to future decryption risks and positions organizations for compliance with evolving regulatory expectations.

04

Prioritization of high-risk data and systems

Focus mitigation efforts on sensitive data with long confidentiality lifecycles, particularly where “harvest now, decrypt later” (HNDL) threats are most relevant. This includes intellectual property, regulated data, and long-lived credentials.

05

Strengthening key management practices

Enhance lifecycle management for cryptographic keys, including generation, storage, rotation, and revocation. Strong key governance reduces exposure during the transition to quantum-resilient methods.

06

Protocol and configuration modernization

Update or replace legacy protocols and configurations that rely on quantum-vulnerable algorithms. This includes modernizing TLS/SSL, SSH, and VPN implementations to support stronger or hybrid cryptographic models.

07

Hybrid cryptographic approaches

Deploy hybrid solutions that combine classical and post-quantum algorithms to maintain interoperability while gradually introducing quantum-resistant protections.

08

Ongoing monitoring and compliance alignment

Continuously monitor cryptographic posture and align with evolving industry standards, regulatory guidance, and best practices related to post-quantum readiness.

By leveraging the power of RQSA, organizations will be able to utilize these strategies, reduce long-term exposure, maintain trust in their digital ecosystems, and ensure a controlled, risk-based transition to quantum-resilient security architectures.

About Rocket Software

Rocket Software is a global technology leader in modernization and a partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,200 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-18724_Broch_Rocket_Quantum_Safety_Analyzer_v2