emudhra
Trust Delivered

CASE STUDY

Advancing Cryptographic Security with Post Quantum Cryptography (PQC) for the Defense Sector

Overview

eMudhra, a prominent product company in the Public Key Infrastructure (PKI) domain, is at the forefront of advancing cryptographic security with its innovative solutions. This case study highlights eMudhra's integration of Post Quantum Cryptography (PQC) algorithms into its flagship certificate manager, emCA, and its commitment to supporting the defense sector in establishing robust cryptographic security.

Challenge

The defense sector faces unprecedented challenges in securing sensitive information against the backdrop of rapidly evolving cyber threats. Traditional cryptographic methods are becoming increasingly vulnerable to potential quantum computing attacks, necessitating a transition to PQC algorithms. The defense sector requires a robust solution to generate and manage digital certificates based on PQC standards to ensure future-proof security.

Solution

As part of its ongoing research and development (R&D) efforts, eMudhra has successfully integrated PQC algorithms shortlisted by the National Institute of Standards and Technology (NIST) into emCA. This advancement enables the defense sector and certificate authorities (CAs) to issue PQC-based digital certificates, providing enhanced security against quantum threats.

Key Features of eMudhra's PQC Solution

PQC Algorithm Support:

- emCA supports a range of NIST-recommended PQC algorithms, including Dilithium2, Dilithium3, Dilithium5, Falcon-512, Falcon-1024, and Sphincs+.
- This comprehensive support ensures that the defense sector can adopt next-generation cryptographic standards.

Continuous Monitoring and Adaptation:

- eMudhra remains committed to staying abreast of developments in PQC algorithms as per NIST's recommendations.
- By closely monitoring NIST's progress, eMudhra ensures that its products remain at the forefront of technological innovation and continue to meet the evolving needs of the defense sector.

Transition Methodologies:

- eMudhra supports various transition methodologies recommended for PQC, including the generation of composite certificates, linked certificates, single PQC certificates and hybrid certificates.
- This flexibility allows the defense sector to transition seamlessly to PQC-based security.

Implementation

eMudhra's emCA can be deployed within the defense sector to establish both Private CAs and Public CAs. The deployment process involves:

Integration of PQC Algorithms:

- emCA is updated to support the latest PQC algorithms shortlisted by NIST.
- The integration process can be completed seamlessly to ensure no disruption to existing operations.

Training and Support:

- eMudhra can provide comprehensive training to the defense sector's IT personnel on the implementation and management of PQC-based certificates.
- Ongoing support to ensure that any issues are promptly addressed, and the defense sector remains equipped with the latest updates and enhancements.

Results

The integration of PQC algorithms into emCA has positioned eMudhra as a frontrunner in the adoption of next-generation cryptographic standards. Key results include:

Enhanced Security:

- The defense sector can now benefit from future-proof security against potential quantum computing attacks.
- PQC-based certificates provide a robust layer of security, ensuring the protection of sensitive information.

Leadership in PQC Adoption:

- eMudhra's proactive approach to integrating PQC algorithms has reinforced its reputation as a leader in cryptographic security.
- The defense sector's endorsement of eMudhra's solutions highlights the company's pivotal role in advancing PQC adoption.

Collaboration and Future Directions

Recognizing the collaborative nature of this transition, eMudhra is actively engaged with the defense sector and other stakeholders in a working group dedicated to advancing PQC adoption. By leveraging its expertise and resources, alongside contributions from HSM vendors, relying party application owners, and other industry players, eMudhra is confident in the collective ability to achieve desired outcomes and propel the PKI ecosystem into a new era of security and resilience.

eMudhra is grateful for the opportunity to contribute to the defense sector's PQC initiative and remains committed to providing full support to achieve its objectives. With the successful integration of PQC algorithms into emCA, eMudhra is poised to lead the charge in cryptographic security, ensuring that the defense sector remains secure against emerging threats.

emudhra
Trust Delivered

About eMudhra

eMudhra is a leading provider of digital trust solutions, specializing in Public Key Infrastructure (PKI), Post Quantum Cryptography (PQC), and Fully Homomorphic Encryption (FHE) technologies. With a robust portfolio that includes digital signature solutions, identity management, and secure transaction solutions, eMudhra empowers organizations across various sectors, including defense, finance, healthcare, and government, to enhance their digital security. Committed to innovation and excellence, eMudhra continuously invests in research and development to stay ahead of technological advancements, ensuring their solutions meet the highest standards of security and compliance. By integrating cutting-edge cryptographic technologies like PQC and FHE, eMudhra ensures that its clients are equipped to face future cyber threats with confidence. With a global presence and a strong customer base, eMudhra is dedicated to fostering a secure and digitally empowered world.