Wallet Guru Platform Security Framework

1. Introduction

This document outlines the security framework implemented in the Wallet Guru platform, with a primary objective to ensure the confidentiality, integrity, and availability of user and transaction data. All security measures align with industry best practices and regulatory standards.

2. Data Encryption

- All user and transactional databases are encrypted using Advanced Encryption Standard (AES-256).
- This encryption is enforced both at rest and in transit.
- Data in Amazon DynamoDB is protected using AWS Key Management Service (KMS) for centralized key control.

3. Cloud Infrastructure Security

- The platform is deployed on AWS Elastic Kubernetes Service (EKS), with clusters operating within private subnets.
- This network design restricts direct public internet access to the compute resources.
- AWS Web Application Firewall (WAF) is configured to protect the Wallet Guru portal and its public APIs against common threats such as SQL injection and cross-site scripting (XSS).

4. Key Management

- AWS Key Management Service (KMS) is used for managing encryption keys used to secure data in DynamoDB.
- Integration with AWS KMS ensures that encryption keys are rotated and access-controlled according to best practices.

5. Optional Security Enhancements

- Amazon GuardDuty is enabled as an optional managed threat detection service.

- GuardDuty continuously monitors for malicious activity, unauthorized behavior, and potential threats across AWS accounts and workloads.

6. Summary

The Wallet Guru security framework provides strong protection for all user and transactional data through the use of industry-standard encryption, AWS-native security services, and a tightly secured cloud infrastructure. This layered approach ensures that security remains resilient against both external and internal threats.