Encryption Policy

Contents

Overview

This document outlines the use of encryption algorithms that have been proven to work effectively and that provide adequate protection for data at rest and in transit.

Scope

- RDS MySQL Database instances, S3 data file storage, EC2 instances
- All MENU Service endpoints

Policy

Encryption at rest

RDS MySQL Database instances, S3 data file storage, EC2 instances, Automated Backups, Read Replicas, and snapshots must be encrypted at rest by enabling the encryption option and the industry standard AES-256 encryption algorithm.
Cross-region Backup Read Replicas, data that is in transit between the source and the Read Replicas must be encrypted as well.

Encryption in transit

All MENU Service endpoints (server-side) must have configured the TLS 1.2 cryptographic protocol for encrypting all end-to-end communication from the clients to MENU Service endpoints.

Standards

AES-256 algorithm

Advanced Encryption Standard (AES) must be used as the basis for encryption technologies. This algorithm represents the actual cipher used for an approved application. ECDSA as defined in Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS) and X9.62-2005: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). The entities use the secure hash algorithm defined in Federal Information Processing Standards Publications, FIPS PUB 180-4, known as SHA384.

The use of proprietary encryption algorithms is not permitted for any purpose.

TLS 1.2 cryptographic protocol

TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions.

AWS Key Management Service (AWS KMS)

AWS Key Management Service (AWS KMS) is a managed service that makes it is used to create and control the encryption keys used to encrypt the data.
The master keys created in AWS KMS are protected by FIPS 140-2 validated cryptographic modules.

Definitions and Terms

AWS Official Glossary: https://docs.aws.amazon.com/general/latest/gr/glos-chap.html
NIST Glossary: https://csrc.nist.gov/glossary