Spring Boot Microservices

Beginner to Guru

Configuration Property Encrypt / Decrypt

At Rest Encryption with Spring Cloud Config

- Spring Cloud Configuration supports property encryption and decryption

- Should be used for sensitive data such as passwords

- Java Cryptography Extension (JCE)

  - Prior to Java 8 u162 required additional setup

  - Older examples will refer to download and install of JCE

  - Included by default in Java 11+

Configuration

- Spring Cloud Configuration will store encrypted properties as:

  - {cipher}<your encrypted value here>

- When a Spring Cloud Config client requests an encrypted property the value is decrypted and presented to the client in the request

- Must set a symmetric key in property 'encrypt.key' - should prefer setting this as environment variable

- asymmetric (public / private) keys also supported - see documentation for details

Encryption / Decryption

- Spring Cloud Configuration provides endpoints for property encryption / decryption

  - POST /encrypt - will encrypt body of post

  - POST /decrypt - will decrypt body of post

SPRING FRAMEWORK GURU