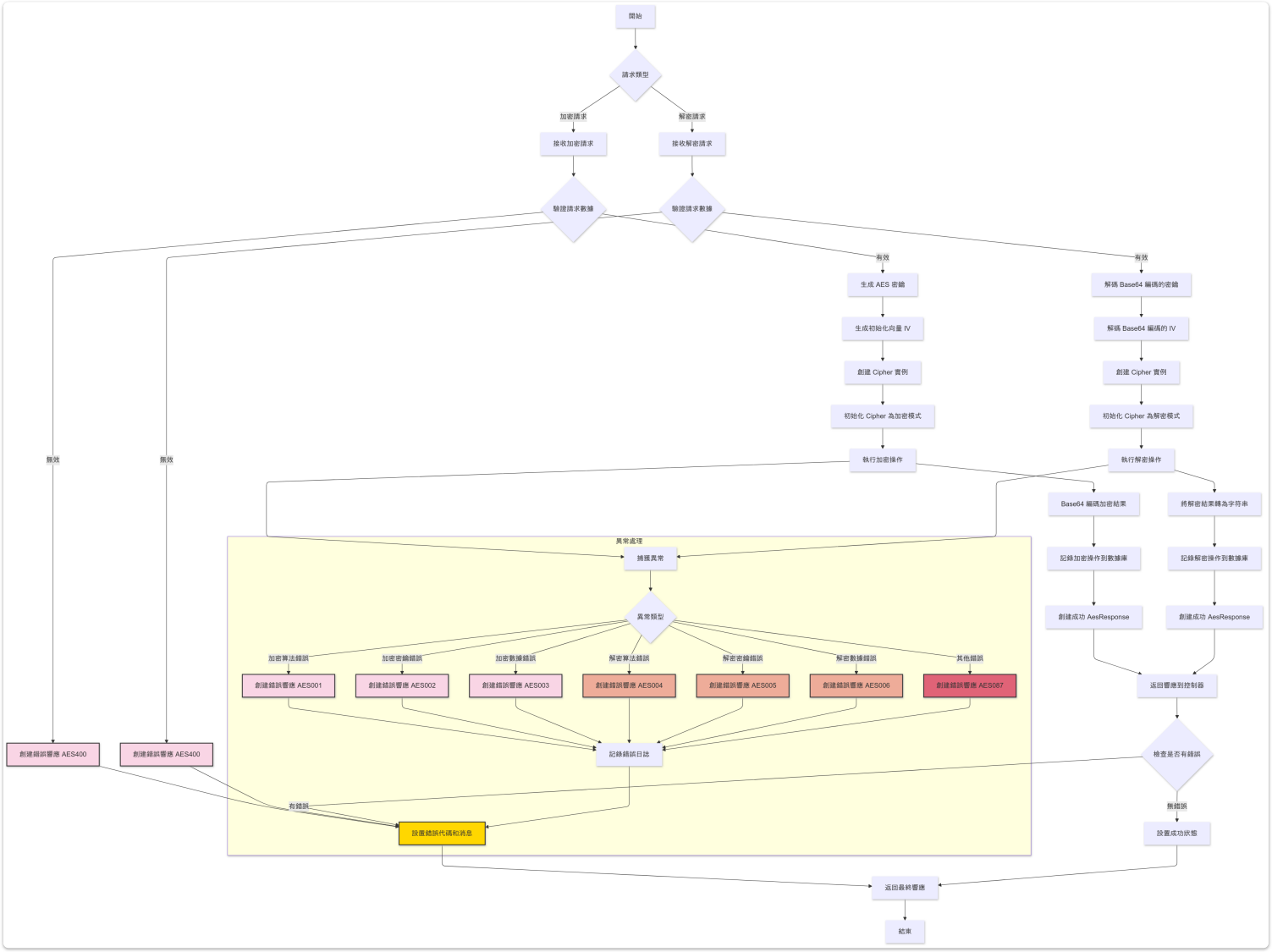
AES加密



AES API 文檔 1

1. 概述

- **功能簡介**：提供AES加密和解密服務，支援資料的加密和解密操作，並將操作記錄儲存到資料庫。
- **技術特點**：使用Java實現，支援RESTful API，整合資料庫記錄，提供安全的加密解密功能。

2. 技術細節

- **協議**：HTTPS
- **請求方法**：POST
- **內容類型**：application/json
- **API URL**：
- 加密：`/aes/v2/encrypt`
- 解密：`/aes/v2/decrypt`
- **資料庫**：使用JDBC連接（DB2）

3. API端點

3.1 加密

- **路徑**：`/aes/v2/encrypt`

- 方法：POST
- 請求體格式：

```
{
"data": "要加密的數據"
}
```

```
{
     "data": "已BASE64的數據",

     "iv": "已BASE64的IV",

     "key": "已BASE64的KEY"
}
```

3.2 解密

- 路徑：`/aes/v2/decrypt`
- 方法：POST
- 請求體格式：

```
{
"data": "加密後的數據",
"key": "加密密鑰",
"iv": "初始化向量"
}
```

```
{

     "data": "解密後的數據",

     "iv": "已BASE64的IV",

     "key": "已BASE64的KEY"

}
```

4. 請求參數

4.1 加密請求

參數名	類型	必填	描述
data	String	是	要加密的原始數據

4.2 解密請求

參數名	類型	必填	描述
data	String	是	加密後的數據
key	String	是	用於解密的密鑰
iv	String	是	用於解密的初始化向量

5. 實現流程

5.1 加密流程

1. 接收加密請求
2. 驗證請求參數
3. 生成AES密鑰和初始化向量
4. 執行AES加密
5. 記錄加密操作到資料庫
6. 返回加密結果、密鑰和初始化向量

5.2 解密流程

1. 接收解密請求
2. 驗證請求參數
3. 使用提供的密鑰和初始化向量執行AES解密
4. 記錄解密操作到資料庫
5. 返回解密結果

6. 資料處理

- **輸入驗證**：
- 檢查加密/解密請求中的必要參數是否存在且不為空
- 對於解密請求，確保密鑰和初始化向量的格式正確

7. 依賴關係

- **外部庫**：
- JAX-RS (Jersey) 用於RESTful API
- Log4j2 用於日誌記錄
- JDBC Driver 用於資料庫操作
- **內部服務**：
- AesService 用於執行加密和解密操作
- AesDAO 用於資料庫操作
- **環境要求**：
- Java運行環境
- 配置正確的資料庫連接

8. 資料庫結構

AES_ENCRYPTION_DECRYPTION 表：

直欄名稱	資料類型綱目	資料類型名稱	直欄長度	比ull
DATA	SYSIBM	VARCHAR	255	是
DATARESULT	SYSIBM	VARCHAR	255	是
IV	SYSIBM	VARCHAR	255	是
KEY	SYSIBM	VARCHAR	255	是
TIMESTAMP	SYSIBM	TIMESTAMP	10	是

9. 錯誤處理

自定義錯誤處理

- AES400: 請求數據無效
- 錯誤類型：INVALID_REQUEST
- 錯誤訊息：請求數據不能為空
- AES001: 加密算法錯誤
- 錯誤類型：ENCRYPTION_ALGORITHM_ERROR
- 錯誤訊息：加密算法錯誤
- AES002: 無效的密鑰或IV
- 錯誤類型：INVALID_KEY_OR_IV
- 錯誤訊息：無效的密鑰或IV
- AES003: 數據加密錯誤
- 錯誤類型：ENCRYPTION_ERROR
- 錯誤訊息：數據加密錯誤
- AES004: 解密算法錯誤
- 錯誤類型：DECRYPTION_ALGORITHM_ERROR
- 錯誤訊息：解密算法錯誤
- AES005: 無效的密鑰或IV（解密時）
- 錯誤類型：INVALID_KEY_OR_IV_DECRYPTION
- 錯誤訊息：無效的密鑰或IV
- AES006: 數據解密錯誤
- 錯誤類型：DECRYPTION_ERROR
- 錯誤訊息：數據解密錯誤
- AES087: 未知錯誤
- 錯誤類型：UNKNOWN_ERROR
- 錯誤訊息：數據加密/解密錯誤

10. 回應格式

成功回應（加密）：

```
{
"data": "加密後的數據",
"key": "Base64編碼的密鑰",
"iv": "Base64編碼的初始化向量"
}
```

成功回應（解密）：

```
{
"data": "解密後的原始數據"
}
```

錯誤回應：

```
{
"errorCode": "錯誤代碼",
"errorMessage": "錯誤描述"
}
```