04 LDIP 보고서 C — 거버넌스·배포·운영(정책·키·프로필·DevOps)

진행 상태	읽기 전

프로젝트: Project 4 · 기반: Flask(Python) · 작성: 2025-09-15

본 문서는 **거버넌스/정책/키관리/운영** 및 **배포/CI/OpenAPI** 등 플랫폼 운영 전반을 수록함. 코어 데이터 경로(Q/PAR/DET/CTX/ENC)는 **D1** 문서를 참조함.

---

6) KEY — 키 관리 모듈

역할: 키 링/버전/로테이션/감사. 초기엔 ENC 내 포함, 확장 시 분리.

기능

- 링/키 버전 관리, 로테이션 일정, `key_events` 기록
- KMS 키 상태·사용량 리포트

API(2단계)

- `GET /keys/rings` → `{items:[{ring_id, alias, state}]}`
- `POST /keys/rotate {ring_id}` → `{ok:true}`
- `GET /keys/usage?since&until` → `{calls:{GenerateDataKey:n,Decrypt:n}}`

DB(2단계)

- `key_rings(id,name,kms_key_arn,rotation_period_days,state,created_at)`
- `key_events(id,ring_id,event,detail,ts)`

---

7) PM — 정책관리 모듈

역할: 규칙/권한/보존/다운로드 정책 중앙 관리 및 집행. **마스킹 프로필** 지원.

기능

- 정책 세트 정의·버전, ABAC 스타일 바인딩

- 마스킹 프로필: 사용자/문서/태그 단위 프리셋
- 정책 평가 API로 허용/거부

API

- `GET /policies`, `POST /policies`
- `POST /bindings {subject,policy_id,condition}`
- `POST /evaluate {subject,action,resource}` → `{allow,reason}`
- `GET /mask-profiles?owner_id`, `POST /mask-profiles`, `POST /mask-profiles/bind`

DB

- `policies`, `policy_bindings`, `mask_profiles`, `mask_profile_bindings`

평가 우선순위

1. 조직 필수 정책 → 2) 마스킹 프로필 → 3) 요청시 지정 카테고리(덮어쓰기 규칙)

---

8) CLI — 명령행 도구 모듈

역할: 운영·배치·점검(일괄 암/복호화, 감사로그, 규칙 테스트)

예시

```
python -m tools.cli encrypt-batch --owner 1 --path ./samples
python -m tools.cli export-audit --since 2025-09-01 --until 2025-09-15 --o
ut audit.csv
python -m tools.cli test-rules --file ./samples/sample.txt --rules v1
```

부록 AC. /mask-profiles × scope/selectors E2E 시나리오

성공

- `DOCUMENT` 전체, `PAGE_RANGE(2~3)`, `PARAGRAPH_RANGE(5~8)`, `CELL_RANGE(Sheet1:B2:B10)`, `EXPLICIT` 좌표

  #### 경계

- 경계 겹침(any-overlap), 중복 프로필 충돌, 조직 필수 카테고리 우선 적용

오류

- 범위 초과/필수 선택자 누락/프로필-요청 충돌 → 표준 오류 코드(`X4001/V4001` 등)

부록 AD. convert/ocr 운영 정책

컨테이너 전략

- `convert`(LibreOffice headless): HWP/PPT/PPTX → DOCX/PDF 변환
- `ocr`(Tesseract ko+eng): 스캔 PDF/이미지 OCR

헬스체크(yaml)

```
convert:
  image: ghcr.io/linuxserver/libreoffice:latest
  healthcheck:
    test: ["CMD","bash","-lc","soffice --headless --version >/dev/null 2>&1"]
    interval: 30s
    timeout: 5s
    retries: 3
    start_period: 20s
ocr:
  image: tesseractshadow/tesseract4re:latest
  healthcheck:
    test: ["CMD","tesseract","--version"]
    interval: 30s
    timeout: 5s
    retries: 3
    start_period: 20s
```

타임아웃/재시도(Celery)

```
@celery.task(soft_time_limit=120, time_limit=150, autoretry_for=(Exceptio
n,), retry_backoff=True, retry_jitter=True, retry_kwargs={"max_retries": 2})
def convert_task(...): ...
@celery.task(soft_time_limit=60, time_limit=90, autoretry_for=(Exception,),
retry_backoff=True, retry_jitter=True, retry_kwargs={"max_retries": 2})
def ocr_task(...): ...
```

권장값

- convert: 120s/150s, 재시도 2회
- ocr: 페이지당 60s, 재시도 2회, 실패 페이지 부분성공 허용
- 페이지 상한: OCR 300p/작업, 변환 2000p/문서
- 크기 상한: 200MB 초과 승인 필요

부록 Y. Ubuntu/Docker 배포 가이드(요약)

- 설치·디렉터리·`docker-compose.yml` 예시·서비스 기동/정지·리버스 프록시·모니터링(상세는 D 문서 원본문)

부록 AE. OpenAPI 스펙 (YAML, v1)

> openapi.yaml로 저장하여 사용. (전 엔드포인트 포함)

```
# 길이 관계상 D 문서에 수록된 전문을 그대로 사용
# 본 문서에서도 동일 스펙을 유지
```

> 전문은 D 문서 원본문의 “부록 AE” 블록을 복사해 붙여넣기

부록 AF. CI 파이프라인 (GitHub Actions)

> 린트/정적분석/유닛·통합/도커빌드/스캔/스테이징 배포

```
# 길이 관계상 D 문서에 수록된 전문을 그대로 사용
# 본 문서에서도 동일 스펙을 유지
```

> 전문은 D 문서 원본문의 “부록 AF” 블록을 복사해 붙여넣기

부록 AA. 설계·생성 기준 체크리스트

- 코드 스타일(ruff/black), 타입힌트, 트랜잭션 범위, 로깅 레벨, 비밀 관리(.env/secret), 지표(p95 응답/큐 대기/KMS 실패율), 테스트 커버리지≥60%

문서 간 구분 요약

- **D1:** 코어 경로(Q/PAR/DET/CTX/ENC) + 샘플 데이터(AB) + 공통 API 요약(X)
- **D2**: 거버넌스·프로필·키·배포·운영(PM/KEY/CLI) + 변환/OCR(AD) + OpenAPI(AE) + CI(AF) + 체크리스트(AA)