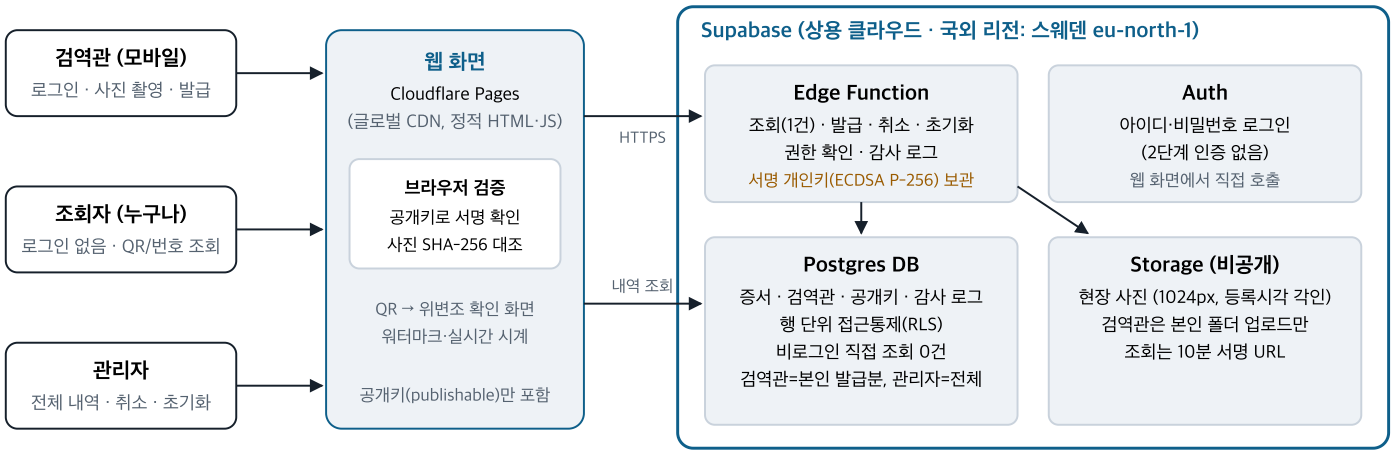
선박 전자증서 확인 데모 — 시스템 구성 및 보안 검토 질의서

검역관이 현장 사진과 함께 전자증서를 발급하고, 누구나 QR·증서번호로 진위를 확인하는 체계의 시범 구성에 대해 보안 검토 의견을 요청합니다.

시연용 프로토타입
작성 2026-11-02
https://ev-ship-ecert.pages.dev

1. 시스템 구성도



2. 현재 구성 요약

- **데이터**: 선박명·국적·IMO·항구, 검역관 아이디·성명, 현장 사진. 데모는 전부 가상 데이터
- **위변조 탐지**: 내용·사진 해시를 서명. 한 글자라도 바뀌면 "위변조 의심"
- **계정**: 검역관·관리자 아이디·비밀번호. 2단계 인증·기관 SSO 없음
- **비밀값**: 화면에는 공개키만, 서버 키·서명키는 서버 비밀 저장소에만
- **서명**: 자체 발급 ECDSA P-256 키. 개인키는 서버 비밀값, 공개키는 공개해 누구나 검증
- **공개 조회**: 로그인 없이 1건씩만 조회. 목록 조회 불가, 속도 제한은 없음
- **호스팅**: Cloudflare(글로벌 CDN), Supabase(스웨덴 리전). 국내 리전·CSAP 인증 아님
- **감사**: 발급·취소·초기화를 감사 로그 테이블에 기록 (관리자만 열람)

3. 질의 사항

#	분야	질의	데모 현황 (참고)
1	**클라우드 이용**	검역 업무 데이터를 국외 리전 상용 클라우드에 두어도 되는지, 실서비스 시 CSAP 인증·국내 리전·기관 전용 클라우드가 필수인지	Supabase 스웨덴 리전, Cloudflare 글로벌 CDN
2	**전자서명 효력**	자체 발급 서명이 행정 증서 진위확인 용도로 인정 가능한지, 전자서명법상 인증 전자서명·GPKI 적용이 필요한지	ECDSA P-256 자체 키, 브라우저에서 공개키 검증
3	**서명키 관리**	개인키를 HSM·KMS에 보관해야 하는지, 키 교체 주기와 유출 시 폐기·재발급 절차 기준	함수 비밀값 보관, 키 ID로 버전 구분
4	**개인정보**	검역관 성명·아이디, 현장 사진(인물 포함 가능)의 처리 근거와 보관 기간, 사진 속 제3자 얼굴 처리 기준	사진 1024px 축소·각인 후 비공개 저장
5	**공개 조회 범위**	선박명·국적·IMO만으로 증서를 보여 주는 것이 허용되는지, 무차별 조회 방지(속도 제한·캡차) 요구 수준	로그인 없음, 1건씩 응답, 속도 제한 없음
6	**계정·인증**	검역관·관리자 로그인에 공무원 인증서·기관 SSO·2단계 인증 연계가 필요한지, 관리자 접근 IP 제한 필요 여부	아이디·비밀번호만 사용
7	**내부망 연계**	기존 검역정보시스템과 연계할 때 망분리·연계 방식(API, 중계서버) 요건	연계 없음 (독립 시연)
8	**검토 절차**	정보화사업 보안성 검토, 웹 취약점 점검, 개인정보 영향평가 대상 여부와 제출해야 할 산출물	미실시
9	**로그·감사**	발급·취소 기록의 보관 기간, 위변조 방지(무결성) 요건, 접속 기록 보관 기준	감사 로그 테이블, 별도 무결성 보호 없음