|  |
| --- |
| 2025년 오픈소스 개발자대회 기능명세서 |
|  |



가. 기본정보(팀명 : SAGE)

□ 프로젝트명

ㅇ SAGE - Secure Agent Guarantee Engine

□ 프로젝트 개요

ㅇ SAGE는 AI 에이전트 간 통신의 무결성과 신뢰성을 보장하는 블록체인 기반 보안 라이브러리

ㅇ 주요 기능으로는

* RFC 9421 HTTP Message Signatures 완전 구현
* RFC 9180 및 Secp256k1/Ed25519 암호화 알고리즘 지원
* Ethereum 기반 블록체인 Contract로 Agent DID 관리
* 메시지 서명/검증 및 키 관리 기능 지원

**□ Test 환경 정보(최적의 테스트 환경 구현을 위해 상세하게 작성 바람)**

※ 테스트에 반드시 필요한 사항 등 함께 기재

ㅇ SW 정보

* SW명: SAGE Core Library
* SW 유형: Go 라이브러리 / 보안 미들웨어
* 개발 환경: Go 1.23+ (현재 1.23.0), Solidity 0.8.19
* Test 환경 상세:
  + Core Library/CLI: Go 1.23 이상
  + Smart Contract: Solidity 0.8.19
  + 블록체인 네트워크: Ethereum (Hardhat 로컬 노드)
  + Chain ID: 31337 (로컬)
  + Hardhat 버전: 2.26.3
  + Web3 라이브러리: ethers v6.4.0
  + 암호화 알고리즘: Secp256k1 (Ethereum 호환), Ed25519 (고성능 EdDSA), X25519 (HPKE 키 교환용)
* 필수 의존성:
  + Go 모듈: github.com/ethereum/go-ethereum v1.16.1, github.com/decred/dcrd/dcrec/secp256k1/v4 v4.4.0 외
  + Node.js 패키지: @nomicfoundation/hardhat-ethers v4.0.0, hardhat v2.26.3 외

나. 기능 리스트

| **대분류** | **중분류** | **소분류** |
| --- | --- | --- |
| RFC 9421 구현 | 메시지 서명 | HTTP 메시지 서명 생성, Signature-Input 헤더 생성, Signature 헤더 생성, 서명 필드 선택 및 정규화, Base64 인코딩 |
|  | 메시지 검증 | 서명 파싱 및 디코딩, 정규화된 메시지 재구성, 서명 검증 알고리즘 실행, 타임스탬프 유효성 검사, Nonce 중복 체크 |
|  | 메시지 빌더 | 메시지 구조 생성, 헤더 필드 추가, 메타데이터 설정, 서명 필드 지정 |
|  | 정규화 | Canonical Request 생성, 헤더 정규화, 경로 정규화, 쿼리 파라미터 정렬 |
| 암호화 키 관리 | 키 생성 | Secp256k1 키페어 생성, Ed25519 키페어 생성, X25519 키 생성 (HPKE용), RSA 키페어 생성 |
|  | 키 저장 | 파일 기반 저장 (PEM 형식), 메모리 기반 저장, 암호화된 저장소 (Vault), 키 회전 지원 |
|  | 키 형식 변환 | PEM 형식 인코딩/디코딩, JWK 형식 변환, 압축/비압축 공개키 변환, Ethereum 주소 생성 |
|  | 서명/검증 | ECDSA 서명 (Secp256k1), EdDSA 서명 (Ed25519), RSA-PSS 서명, 메시지 다이제스트 생성 |
| DID 관리 | DID 생성 | did:sage:ethereum 형식 생성, did:sage:solana 형식 생성, DID Document 생성, 메타데이터 설정 |
|  | DID 등록 | Ethereum 스마트 컨트랙트 등록, Solana 프로그램 등록, 공개키 온체인 저장, 메타데이터 저장 |
|  | DID 조회 | 블록체인에서 DID 조회, 공개키 검색, 메타데이터 조회, 활성 상태 확인 |
|  | DID 관리 | DID 업데이트, DID 비활성화, 키 회전, 소유권 이전 |
| 블록체인 연동 | Ethereum | Web3 연결 관리, 스마트 컨트랙트 호출, 트랜잭션 서명 및 전송, 이벤트 모니터링, 가스 예측 |
|  | 체인 레지스트리 | 멀티체인 지원, 체인별 프로바이더 관리, 네트워크 전환, 체인 상태 모니터링 |
| 메시지 처리 | Nonce 관리 | Nonce 생성, Nonce 저장 및 검증, 재전송 공격 방지, 만료 처리 |
|  | 메시지 순서 | 메시지 ID 생성, 순서 보장, 중복 감지, 타임스탬프 관리 |
|  | 검증 서비스 | 통합 검증 파이프라인, 체인별 검증 로직, 검증 옵션 설정, 검증 결과 캐싱 |
| CLI 도구 | sage-crypto | 키페어 생성 명령, 서명 생성 명령, 서명 검증 명령, 키 회전 명령, 주소 생성 명령 |
|  | sage-did | DID 등록 명령, DID 조회 명령, DID 업데이트 명령, DID 비활성화 명령, DID 검증 명령 |
|  | sage-verify | 메시지 검증 명령, 서명 검증 명령, 체인 상태 확인 |
| 세션 관리 | 세션 생성 | 세션 ID 생성, 세션 메타데이터 설정, 세션 암호화 키 생성, 세션 저장 |
|  | 세션 관리 | 세션 조회, 세션 갱신, 세션 만료 처리, 세션 삭제 |
|  | Nonce 관리 | 세션별 Nonce 관리, Nonce 풀 관리, Nonce 검증 |
| HPKE (Hybrid Public Key Encryption) | 암호화 | HPKE 컨텍스트 생성, 메시지 암호화, 인증된 암호화 (AEAD) |
|  | 복호화 | HPKE 컨텍스트 로드, 메시지 복호화, 인증 검증 |
|  | 키 교환 | DHKEM 키 교환, 공유 비밀 생성, 키 파생 |
| 헬스체크 | 상태 모니터링 | 시스템 상태 확인, 의존성 상태 확인, 블록체인 연결 상태 |
|  | 메트릭 수집 | 성능 메트릭, 에러 카운트, 처리량 측정 |

다. 기능 시험 항목

| **대분류** | **중분류** | **소분류** | 시험항목 | Result |
| --- | --- | --- | --- | --- |
| RFC 9421 구현 | 메시지 서명 | HTTP 서명 생성 | RFC 9421 준수 HTTP 메시지 서명 생성 확인 |  |
|  |  |  | Signature-Input 헤더 올바른 형식 생성 확인 |  |
|  |  |  | Signature 헤더 base64 인코딩 확인 |  |
|  |  |  | 필수 서명 필드 (created, expires, nonce) 포함 확인 |  |
|  |  | 정규화 | HTTP 요청 정규화 정확성 확인 |  |
|  |  |  | 헤더 필드 정렬 및 소문자 변환 확인 |  |
|  | 메시지 검증 | 서명 검증 | 유효한 서명 검증 성공 (true 반환) |  |
|  |  |  | 변조된 메시지 검증 실패 (false 반환) |  |
|  |  |  | 만료된 서명 거부 확인 |  |
|  |  |  | 타임스탬프 유효성 (5분 이내) 검사 |  |
|  |  | Nonce 관리 | Nonce 중복 감지 및 거부 |  |
|  |  |  | Nonce 만료 처리 확인 |  |
| 암호화 키 관리 | 키 생성 | Secp256k1 | 32바이트 개인키 생성 확인 |  |
|  |  |  | 65바이트 비압축 공개키 (0x04 prefix) 생성 확인 |  |
|  |  |  | 33바이트 압축 공개키 생성 확인 |  |
|  |  | Ed25519 | 32바이트 개인키 생성 확인 |  |
|  |  |  | 32바이트 공개키 생성 확인 |  |
|  | 키 저장 | 파일 저장 | PEM 형식 파일 저장 성공 |  |
|  |  |  | 파일 권한 설정 (0600) 확인 |  |
|  |  | 암호화 저장 | Vault 암호화 저장 성공 |  |
|  |  |  | 암호화된 키 복호화 성공 |  |
|  | 서명/검증 | ECDSA | Secp256k1 서명 생성 성공 |  |
|  |  |  | Ethereum 호환 서명 (v, r, s) 생성 확인 |  |
|  |  |  | 서명 검증 성공 |  |
|  |  | EdDSA | Ed25519 서명 생성 성공 |  |
|  |  |  | 64바이트 서명 생성 확인 |  |
|  |  |  | 서명 검증 성공 |  |
| DID 관리 | DID 생성 | 형식 검증 | did:sage:ethereum: 형식 준수 확인 |  |
|  |  |  | 유효한 체인 주소 포함 확인 |  |
|  | DID 등록 | 블록체인 등록 | Ethereum 스마트 컨트랙트 등록 성공 |  |
|  |  |  | 트랜잭션 해시 반환 확인 |  |
|  |  |  | 가스비 소모량 확인 (~653,000 gas) |  |
|  |  |  | 등록 후 온체인 조회 가능 확인 |  |
|  | DID 조회 | 블록체인 조회 | DID로 공개키 조회 성공 |  |
|  |  |  | 메타데이터 조회 성공 |  |
|  |  |  | 비활성화된 DID 조회 시 에러 반환 |  |
|  | DID 관리 | 업데이트 | 메타데이터 업데이트 성공 |  |
|  |  |  | 엔드포인트 변경 성공 |  |
|  |  | 비활성화 | DID 비활성화 트랜잭션 성공 |  |
|  |  |  | 비활성화 후 조회 시 inactive 상태 확인 |  |
| 블록체인 연동 | Ethereum | 연결 | Web3 Provider 연결 성공 |  |
|  |  |  | 체인 ID 확인 (로컬: 31337) |  |
|  |  | 트랜잭션 | 트랜잭션 서명 성공 |  |
|  |  |  | 트랜잭션 전송 및 확인 |  |
|  |  |  | 가스 예측 정확도 (±10%) |  |
|  | 컨트랙트 | 배포 | AgentRegistry 컨트랙트 배포 성공 |  |
|  |  |  | 컨트랙트 주소 반환 확인 |  |
|  |  | 호출 | registerAgent 함수 호출 성공 |  |
|  |  |  | getAgent 함수 호출 성공 |  |
|  |  |  | 이벤트 로그 확인 |  |
| 메시지 처리 | Nonce 관리 | 생성/검증 | 유니크한 Nonce 생성 확인 |  |
|  |  |  | 사용된 Nonce 재사용 방지 |  |
|  |  |  | Nonce TTL(5분) 만료 처리 |  |
|  | 메시지 순서 | 순서 보장 | 메시지 ID 유니크성 확인 |  |
|  |  |  | 타임스탬프 순서 정렬 확인 |  |
|  |  |  | 중복 메시지 감지 및 거부 |  |
|  | 검증 서비스 | 통합 검증 | DID 활성 상태 확인 |  |
|  |  |  | 공개키로 서명 검증 |  |
|  |  |  | 타임스탬프 & Nonce 검증 |  |
|  |  |  | 검증 결과 캐싱 동작 확인 |  |
| CLI 도구 | sage-crypto | 키 생성 | generate 명령으로 키페어 생성 성공 |  |
|  |  |  | --type secp256k1 옵션 동작 확인 |  |
|  |  |  | --type ed25519 옵션 동작 확인 |  |
|  |  | 서명 | sign 명령으로 메시지 서명 성공 |  |
|  |  |  | verify 명령으로 서명 검증 성공 |  |
|  |  | 주소 생성 | address 명령으로 Ethereum 주소 생성 |  |
|  | sage-did | DID 등록 | register 명령으로 DID 등록 성공 |  |
|  |  |  | --chain ethereum 옵션 동작 확인 |  |
|  |  | DID 조회 | resolve 명령으로 DID 조회 성공 |  |
|  |  |  | list 명령으로 전체 DID 목록 조회 |  |
|  |  | DID 관리 | update 명령으로 메타데이터 수정 |  |
|  |  |  | deactivate 명령으로 DID 비활성화 |  |
|  |  |  | verify 명령으로 DID 검증 |  |
| 세션 관리 | 세션 생성 | 초기화 | 유니크한 세션 ID 생성 확인 |  |
|  |  |  | 세션 암호화 키 생성 확인 |  |
|  |  |  | 세션 메타데이터 설정 확인 |  |
|  | 세션 관리 | 조회/갱신 | 세션 ID로 조회 성공 |  |
|  |  |  | 세션 갱신 및 TTL 연장 확인 |  |
|  |  |  | 만료된 세션 자동 삭제 확인 |  |
| HPKE | 암호화/복호화 | DHKEM | X25519 키 교환 성공 |  |
|  |  |  | 공유 비밀 생성 확인 |  |
|  |  | AEAD | ChaCha20Poly1305 암호화 성공 |  |
|  |  |  | 인증 태그 검증 성공 |  |
|  |  |  | 복호화 및 무결성 확인 |  |
| 헬스체크 | 상태 모니터링 | 시스템 | /health 엔드포인트 응답 확인 |  |
|  |  |  | 블록체인 연결 상태 확인 |  |
|  |  |  | 메모리/CPU 사용률 확인 |  |

\* Pass/Fail : 심사위원이 평가하는 사항으로 공란으로 비워두세요