# zkWallet

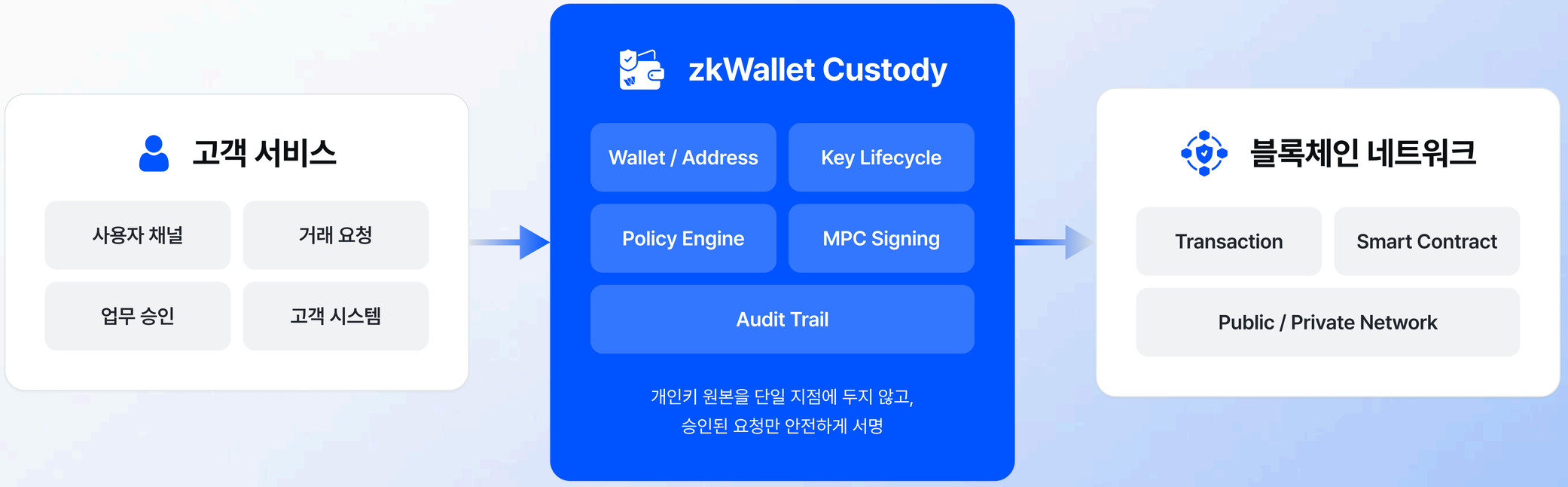
MPC 기반 키 관리/서명을 제공하는 고보안 Custodial Wallet Service

ZKRYPTO

01 INTRO

# zkWallet Custody란?

기관이 디지털자산 지갑, 수탁, 스테이블코인 발행 서비스를 운영할 때 자금 이동 권한을 MPC와 정책 기반 승인 체계로 통제하는 기관형 Wallet Service입니다.




**MPC Signing**
분산 키로 안전한 서명 수행

**Policy Control**
정책 기반 자금 이동 통제

**Audit Trail**
모든 활동의 기록 및 추적

**KMS · HSM Integration**
안전한 키 관리 인프라 연동

02 운영 리스크

# 기관형 디지털자산 서비스의 핵심 리스크

기관 고객에게 필요한 것은 단순한 지갑 생성이 아니라 자산 이동 권한에 대한 통제입니다.

### 키 유출

자산 탈취

운영 리스크

### 내부자 권한 오남용

무단 출금

권한 남용

### 승인 우회

통제 실패

프로세스 훼손

### 장애 · 거래 지연

고객 민원

업무 중단

### 감사 증적 부족

사고 조사 한계

외부감사 대응 부담

[통제 방향]

**MPC**

분산 키 구조로 단일 키 유출 리스크 감소

**Policy Engine**

승인되지 않은 요청 차단

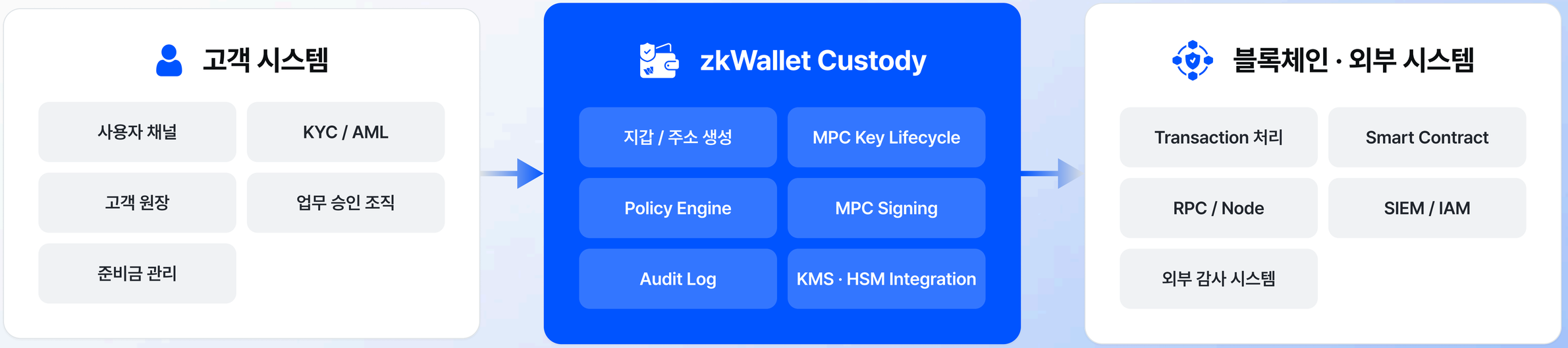
**Audit Trail**

감사 가능한 운영 체계 제공

03 제공 범위

# zkWallet Custody가 담당하는 영역

zkWallet Custody는 키, 지갑, 정책, 서명, 감사 영역을 담당하며 고객 업무 시스템과 연동됩니다.




KYC, AML, 준비금 관리는 고객 또는 연동 시스템 영역이며, 상세 연동 방식은 고객 환경에 따라 협의합니다.

04 ARCHITECTURE

# Reference Architecture

거래 요청은 정책 검증을 거쳐 MPC 서명으로 처리되고, 결과와 감사 로그가 고객 시스템으로 반환됩니다.

### 고객 채널 / API Gateway

- Web / Mobile / Partner
- REST / GraphQL API
- 인증 및 요청 검증

### Policy Engine

- 정책 검증 및 승인
- Key Lifecycle 검증
- 위험도 및 한도 체크
- 의사결정 / 송인 결과

### Wallet Service

- MWallet / Address 관리
- 거래 생성 및 큐잉
- 상태 관리 및 알림
- 결과 수신 및 응답

### MPC Signing Cluster

- MPC 키 분산 보관
- 거래 해시 서명
- 서명 합의 및 검증
- 서명 결과 반환

### Blockchain Network

- 트랜잭션 전송
- 블록체인 검증 및 확정
- 온체인 상태 반영
- 이벤트/영수증 수신

### KMS / HSM

- 키 생성 / 저장 / 관리
- 키 접근 제어 및 감사
- FIPS 140-2 Level 3+

### Confidential Computing

- 실행 환경 격리 (TEE)
- 메모리 · 코드 무결성
- 민감 정보 보호

### Audit Log

- 모든 활동 기록
- 위변조 방지 저장
- 검색 및 리포트

### Monitoring

- 시스템 상태 모니터링
- 알림 및 이상 탐지
- 성능 / SLA 추적

### Admin Console

- 정책 및 한도 관리
- 사용자 / 권한 관리
- 운영 및 설정 관리

배포 방식은 SaaS / Private Cloud / On-premise / Hybrid [TBD] 형태로 고객 환경에 따라 검토 가능합니다.

05 KEY LIFECYCLE

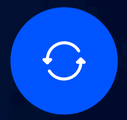
# MPC 기반 키 생애주기 관리

기관형 지갑은 키 생성 이후에도 갱신, 복구, 폐기, 감사가 지속 관리되어야 합니다.

## Generate

분산 키 생성

DKG



## Refresh

키 조각 갱신

Proactive Refresh

## Recover

승인 기반 복구

Share Recovery

## Retire

폐기

권한 회수

감사 기록

키 생애주기 이벤트는 정책과 감사 로그의 관리 대상입니다.

06 MPC SIGNING

# MPC 분산 서명 흐름

서명 요청은 정책 검증 후 여러 Party Node의 부분 서명으로 처리되며, 개인키 원본은 단일 지점에 모이지 않습니다.

**서명 요청 수신**

사용자 또는 서비스로부터
서명 요청 접수

**정책 검증 · 송인 확인**

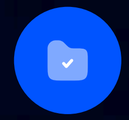
Policy Engine을 통해
정책 검증 및 송인 확인

**Party Node 공동 서명**

여러 Party Node가
부분 서명 생성 및 전송

**서명값 생성**

부분 서명을 결합하여
최종 서명값 생성



**결과 반환 · 로그 기록**

서명 결과를 반환하고
감사 로그를 안전하게 기록

**Threshold 구성 [TBD]**

서명에 필요한 임계값(T)과 총 Party Node 수(N) 설정

**Party Node 배치 [기술 미팅에서 설계]**

지리적 분산 및 기용성을 고려한 Party Node 배치 전략 수립

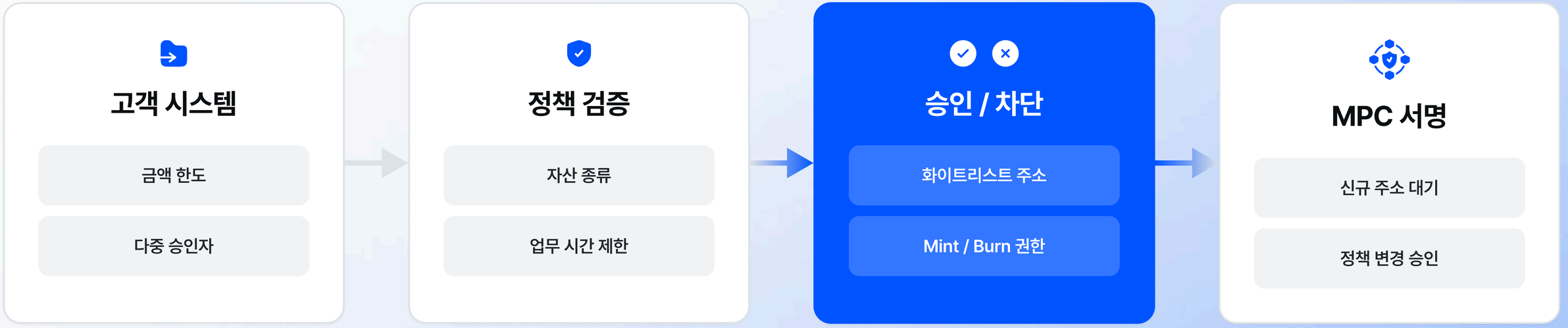
**Coordinator는 세션을 관리하고 부분 서명을 결합**

세션 생성, 상태 관리, 부분 서명 수집 및 결합을 통해
최종 서명값을 생성

07 POLICY ENGINE

# 승인된 요청만 서명하는 Policy Engine

zkWallet Custody의 핵심 가치는 서명 기능이 아니라 어떤 요청을 서명할 것인가를 통제하는 것입니다.




정책 조건은 고객 업무 프로세스와 내부통제 기준에 맞춰 설계합니다.

04 AUDIT

# Audit & Traceability

모든 서명 요청과 승인 과정은 사후 검토 가능한 감사 이벤트로 남아야 합니다.

| Request ID | User / Role | Policy ID | Asset | Amount | Destination | Approval Result | Signing Session | Tx Hash | Timestamp |
|---|---|---|---|---|---|---|---|---|---|
| REQ-2025-0001 | Ops / Admin | POL-001 | USDC | 10,000 | 0xAbc...1234 | Approved | SES-0001 | 0×9f3a...c1b7 | 2025-05-24 10:15:23 UTC |
| REQ-2025-0002 | Treasury / Ops | POL-002 | ETH | 2.50 | 0xDef...5678 | Approved | SES-0002 | 0×2b7e...9d4a | 2025-05-24 10:28:41 UTC |
| REQ-2025-0003 | Finance / Viewer | POL-003 | USDT | 25,000 | 0×987...abcd | Rejected | SES-0003 | - | 2025-05-24 10:36:59 UTC |

[감사 로그 예시]

실제 로그 필드와 보관정책은 고객 규제 및 운영 기준에 따라 협의합니다.

**내부감사**
정책 준수 및 통제 운영의 적정성 검증

**사고 조사**
이상 거래 및 보안 사고의 원인 분석

**책임소재 확인**
요청자, 승인자, 서명자 활동 추적

**외부감사 대응**
감사 요청 시 근거 자료 신속 제공

**운영 리포트**
운영 현황 및 KPI 기반 리포트 생성

09 SECURE EXECUTION

# Secure Execution Environment

분산 키 조각과 민감 연산은 고객 보안 요구사항에 따라 KMS/HSM 및 보호 실행 환경과 연동할 수 있습니다.

## Confidential Computing

민감 연산 격리

메모리 보호

보호 실행 영역

## KMS / HSM Integration

Key Share Access Control

고객 보안 정책 반영

외부 보안 인프라 연동

**Secret / Share 보호**

**민감 연산 격리**

**기존 보안 인프라 연계**

구체적 적용 방식은 고객 인프라, 클라우드, 보안 정책에 따라 결정됩니다.

10 CUSTOMER SCENARIOS

# 고객군별 적용 시나리오

금융사, 수탁사, 스테이블코인 발행사는 각기 다른 업무 흐름에서 정책 기반 자금 이동 통제를 적용할 수 있습니다.

## 금융사

고객 지갑 개설

디지털자산 전송

결제 · 송금 서비스 연계

후속 검토 질문

**어떤 고객 채널과 자산을 우선 연동할 것인가?**

## 수탁사

고객 자산 출금 송인

수탁 지갑 운영

고객별 감사 추적

후속 검토 질문

**출금 송인 정책과 고객별 원장 구조는 어떻게 운영되는가?**

## 스테이블코인 발행사

Mint / Burn 송인

발행 권한 통제

발행 · 상환 이력 관리

후속 검토 질문

**Mint / Burn 권한과 준비금 확인 절차는 어떻게 연결되는가?**

후속 기술 미팅에서는 고객별 우선 시나리오와 PoC 후보 범위를 함께 정리합니다.