nCIPHER

암호키 보호와 블록체인 보안사고 사례

nCipher 김동민

암호키 소개

Introduction of Encryption Key

암호화 기술의 사용

새로운 사용 사례에 대한 신뢰 제공

- IoT 신뢰 기반
- 블록체인

디지털 페이먼트 보안

- 지불결제 인증서 발급 및 관리
- 기기 및 클라우드를 통한 지급결제

멀티 클라우드 보안

- BYOK를 통한 키 보안 및 통제
- 클라우드 접근 보안 브로커 (CASBs)

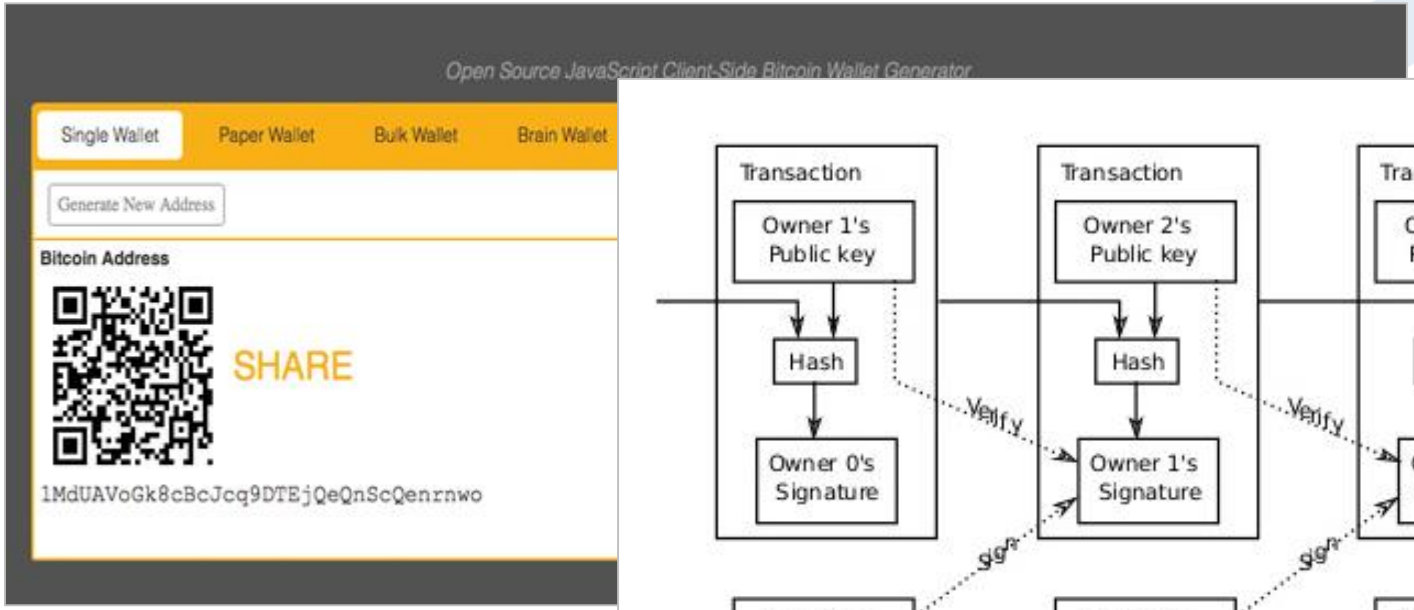
현재 비즈니스 애플리케이션에 기 적용되고 입증된 기초적 보안

- 데이터베이스 암호화
- 애플리케이션 암호화
- 코드 서명
- TLS/SSL 암호화
- PKI & 애플리케이션
- 기업 고객 인증

HSM 및 암호화 기술 활용

nCIPHER

블록체인 암호키


Open Source JavaScript Client-Side Bitcoin Wallet Generator
Single Wallet
Paper Wallet
Bulk Wallet
Brain Wallet
Generate New Address
Bitcoin Address
SHARE
1MdUAVoGk8cBcJcq9DTEjQeQnScQenrnwo

Transaction
Owner 1's Public key
Hash
Owner 0's Signature
Verify
Transaction
Owner 2's Public key
Hash
Owner 1's Signature
Verify
Transaction
Owner 3's Public key
Hash
Owner 2's Signature
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

블록체인 암호키의 특징

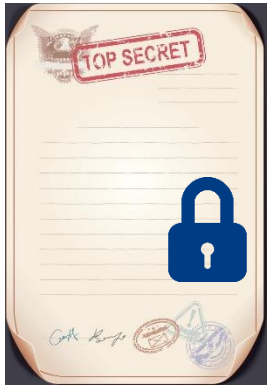
Features of Blockchain Key

블록체인 암호키의 가치

10,000,000 $

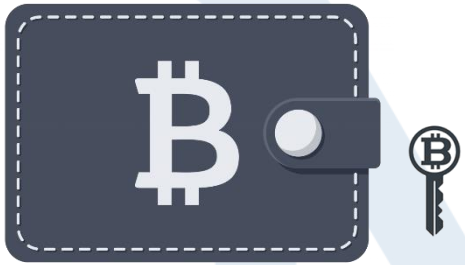
Bank Account Information

10,000,000 $



Document of New Tech

10,000,000 $



Blockchain Private Key

NCIPHER

블록체인 암호키의 해킹 매력도

	은행 인증서	기술 문서 암호키	블록체인 개인키
해커의 획득 투자비용	높음	높음	높음
환금성	낮음	매우 낮음	높음
사후 추적 위험성	높음	높음	낮음
파기 명령 시 피해	없음	낮음	높음

블록체인 보안사고 사례

Security issue case of Blockchain

블록체인 거래소 사고사례

Name	Reported Loss (Crypto)	Reported Loss (USD)	Occurred On	Source(s)
Bancor Exchange hack	24,984 ETH, 229M NPXS, 3.2M BNT	$23,500,000	July 2018	Bancor Official Twitter Cointelegraph
Coinrail Exchange hack	1,927 ETH, 2.6B NPXS, 93M ATX, 831M DENT	$40,000,000	June 2018	Coindesk
Misconfigured Ethereum Clients Incident	38,680 ETH	$20,000,000	2018 Ongoing	Bleeping Computer
MyEtherWallet DNS hack	215 ETH	$152,000	April 2018	Forbes
Coinsecure Theft	438 BTC	$3,300,000	April 2018	Coindesk
South Korean Bitcoin Pyramid Scheme	N/A	$20,000,000	April 2018	Coindesk
GainBitcoin India Ponzi Scheme	N/A	$300,000,000	April 2018	Cointelegraph
Dantang coin Ponzi	N/A	$13,000,000	April 2018	CryptocurrencyNews
iFan/Pincoin Token Scam	N/A	$650,000,000	April 2018	VNExpress
BTC Global Ponzi Scam	N/A	$50,000,000	Mar 2018	Coindesk
Coinhoarder Phishing Scams (ongoing)	N/A	$50,000,000	Feb 2018	Cisco Research

기타 사고사례

External factor

- Blockchain Code Attack
- Blockchain Node Attack
- Blockchain Wallet Attack

Internal factor

- Insider Crime
- Insider Careless

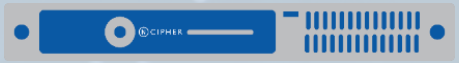
블록체인 보안의 51% 암호키 보호

Introduction of Encryption Key

암호키 보호 방안

Protecting the signing keys is critical!

Protecting the consensus logic is even better!



HSMs can protect the signing keys AND the process

암호키 보호 방안

Protect Signing Keys

- Generation and protection of signing keys within FIPS- and Common Criteria-certified HSM

Protect Signing Process

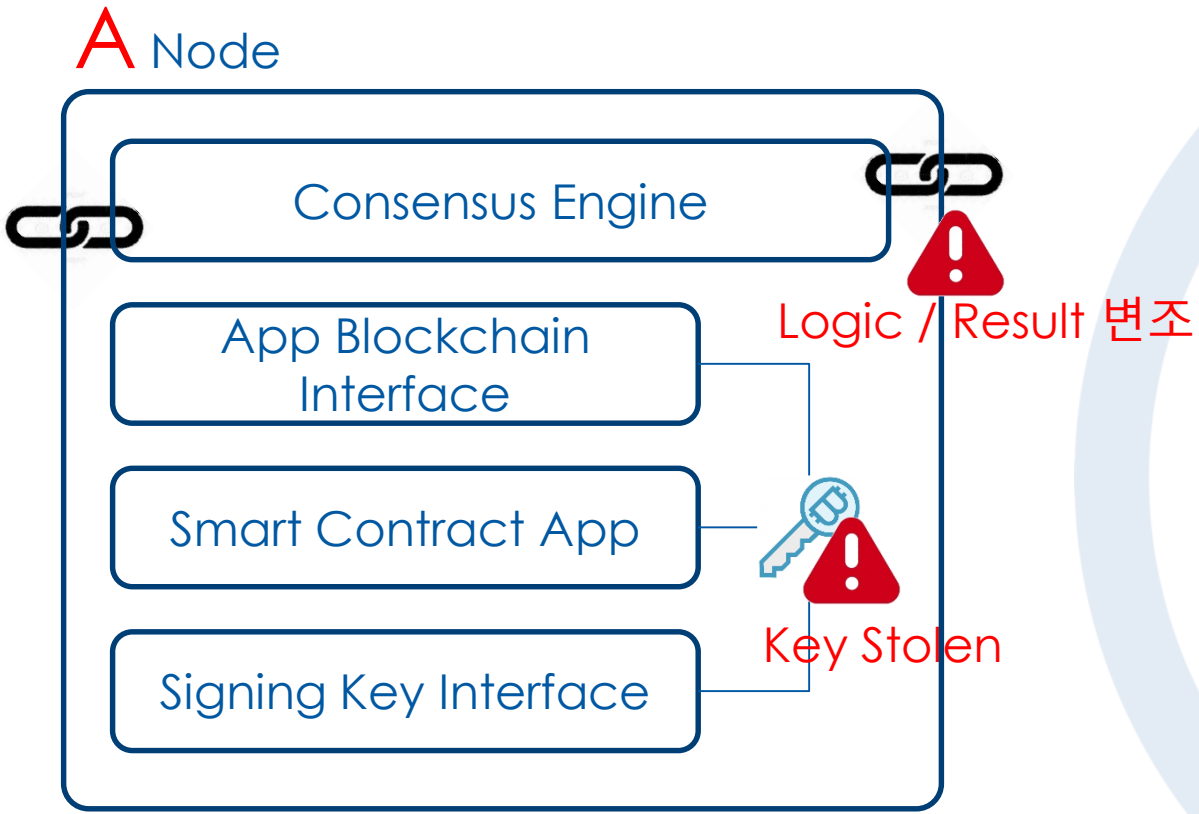
- Control over the signing process using the nShield CodeSafe execution environment

Crypto Support

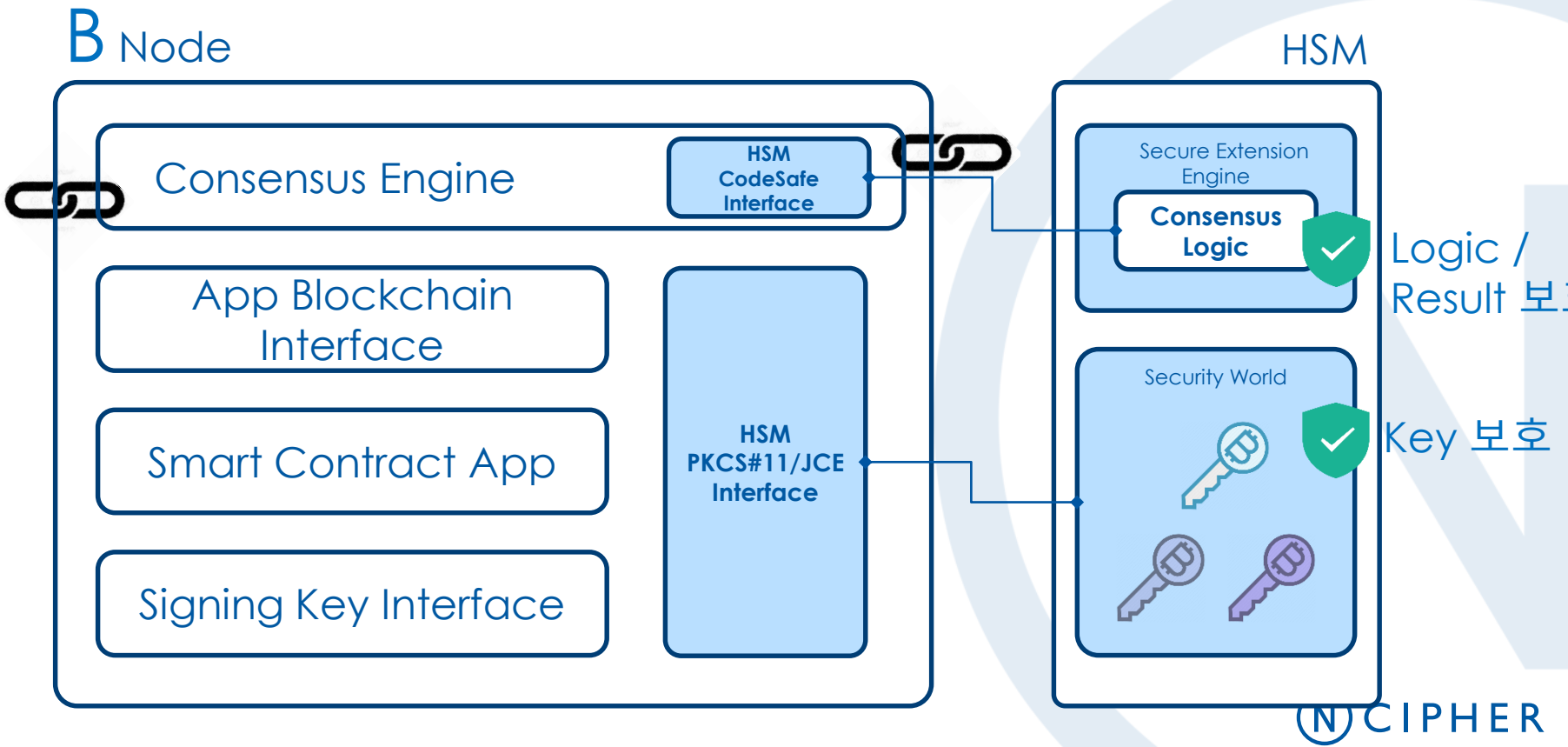
- Elliptic curves supported:
  - secp256k1, ECDSA
  - ED25519, EdDSA
- Hash:
  - SHA-2
  - RIPEMD-160
- Key derivation:
  - Hyperledger Client Key Derivation

nCIPHER

블록체인 항목 별 보안 적용



블록체인 항목 별 보안 적용



해외 적용 사례

- **LedgerX - Bitcoin exchange and clearinghouse**
  - Objective: Securely facilitate transfer of digital currency
  - Solution: nShield with CodeSafe
    - Software in HSM provides crypto and enforced quorum for transferring Bitcoin

LedgerX

- **Gem – Crytocurrency management platform**
  - Objective: Supply secure API to Bitcoin developers
  - Solution: nShield with CodeSafe
    - Software in HSM secures core components of Bitcoin, providing 'bank grade' security

Gem

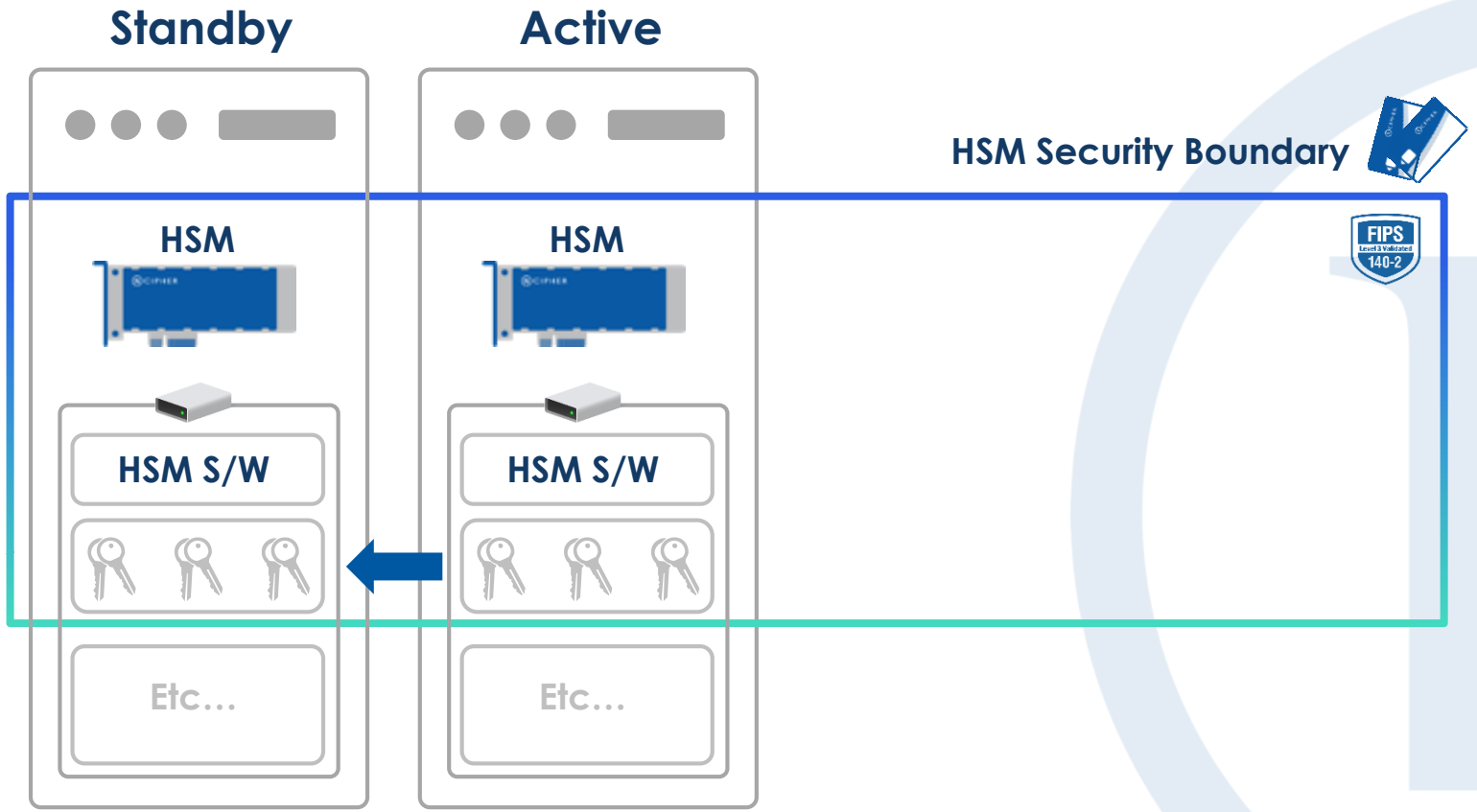
- **Chain - Provides permissioned blockchain infrastructure**
  - Integration: nShield with CodeSafe
    - Implement blockchain cryptography and protect root keys in HSM
  - Visa introduced B2B Connect service based on Chain

Chain

- **Accenture – Simplifies security integration for blockchain**
  - Used Fabric, a Hyperledger technology
  - Integration: nShield with CodeSafe

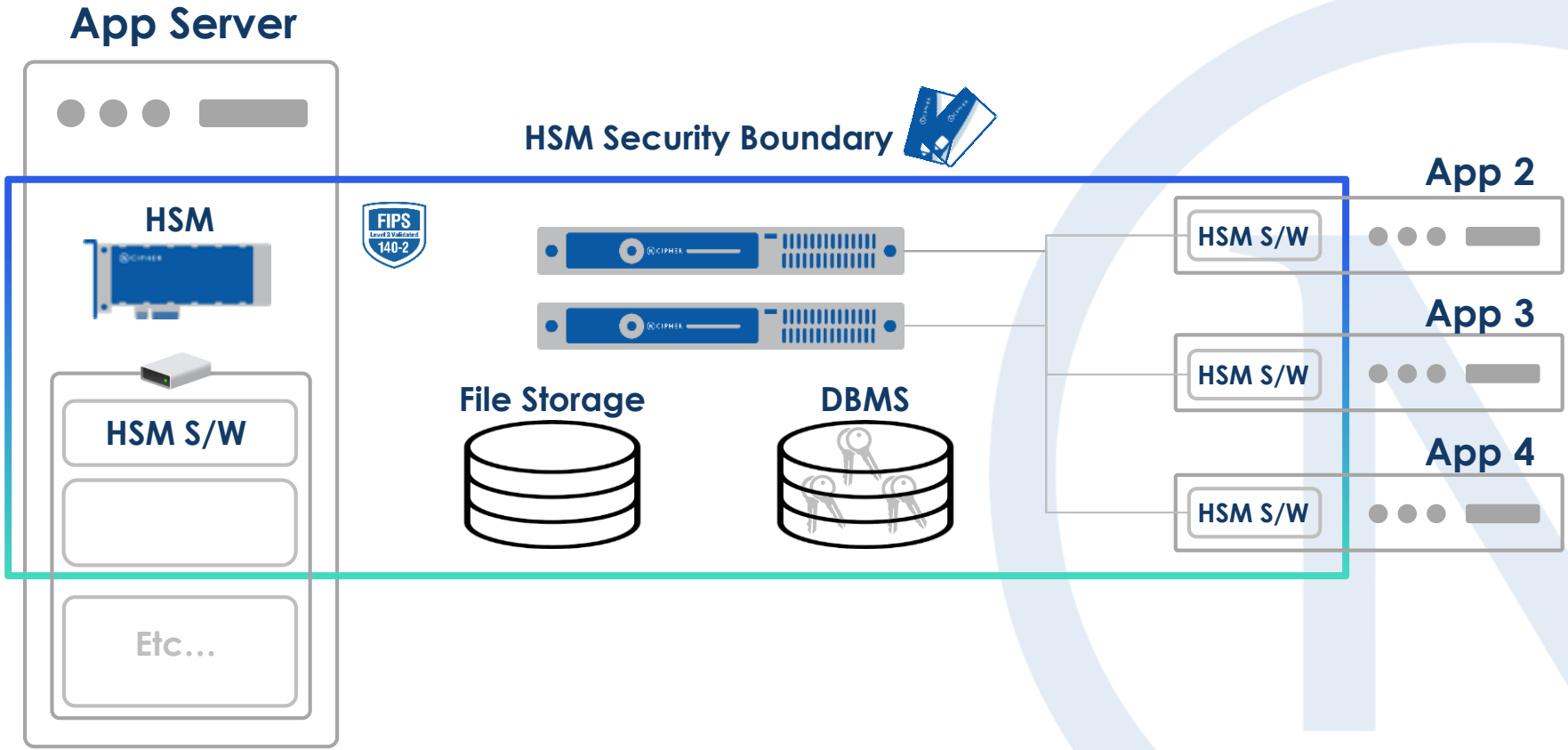
accenture

암호키 유실 대응



nCIPHER

대량의 암호키 보호


App Server
HSM Security Boundary
HSM
FIPS 140-2
HSM S/W
Etc…
File Storage
DBMS
App 2
HSM S/W
App 3
HSM S/W
App 4
HSM S/W

감사합니다