

# 사용자 인증기술의 새로운 흐름과 그에 따른 암호키 관리 방법

nCipher Security 김동민



## HSM 이란?

와 를 보호하기 위한  
 받은 장비 입니다.

# 인증과 암호화 기술

인증의 요소 / 과거의 인증 방법 / PKI기술과 공인인증서

## ○ 정보보호의 목적

기밀성 (Confidentiality)

무결성 (Integrity)

가용성 (Availability)

부인방지 (Non-repudiation)

접근통제 (Access Control)

## ○ 인증의 요소

기밀성 (Confidentiality)

무결성 (Integrity)

가용성 (Availability)

부인방지 (Non-repudiation)

접근통제 (Access Control)

## ○ 오프라인



## ○ 오프라인



■ 인감증명서 시행령 [별지 제14호서식]

인감증명 발급사실 확인용 번호 42 - 2 -

신청인: 정 (생년월일: 19 ) 담당자: (전화: 043- )

\*이 용지는 위조식별표시가 되어 있음

### 인감증명서

주민등록 번호	본인	대리
성명 (한자)	정	
국적 (외국인)	(鄭)	
주소	전입	
주소	20 . . .	공동주택별경
용도	[V] 부동산 매수자 [ ] 자동차 매수자	
매수자의 주민등록번호	성명(법인명)	매수자의 이름
매수자의 주민등록상 주소	주소 (법인 소재지)	주민등록번호 (법인등록번호)
위의 기재사항을 확인합니다. (발급신청자) 발급신청자 이름, 서명		
비고		

1. 인감증명서 발급사실통보서비스를 신청하면 발급 사실을 휴대폰 문자로 즉시 통보받을 수 있습니다.
2. 인감증명서 발급 신청인이 본인인 경우에는 본인란에, 대리인이 신청하는 경우에는 대리인란에 O 표시됩니다.

## ○ 온라인

ID

Password

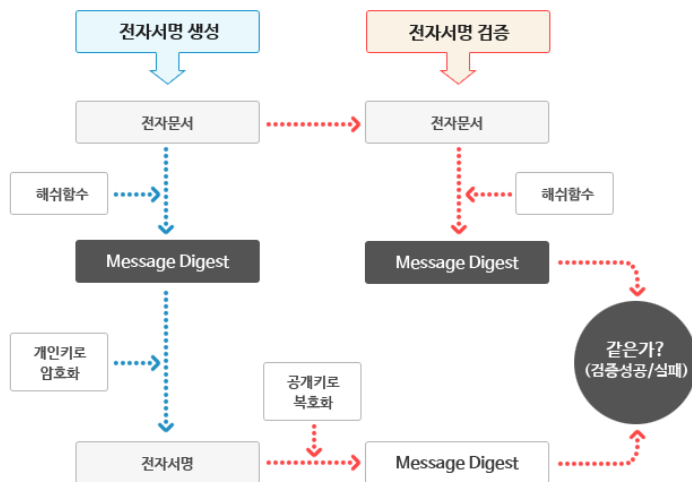
이름

주민등록번호

이메일



## ○ 공인인증서



주요 구성요소	설명
일련번호	공인인증서 일련번호
발행기관 식별명칭	공인인증기관 식별명칭
유효기간	공인인증서 유효기간 시작일과 만료일을 명시
소유자 식별명칭	공인인증서 소유자의 실명을 포함한 식별명칭
공개키	공인인증서 소유자의 공개키
공개키 사용목적	공개키의 사용목적을 명시(전자서명, 암호화 등)
인증서 정책	공인인증서 발행기관이 인증서를 발행하는데 적용한 인증서 정책과 인증업무 준칙을 명시
발행기관의 서명값	인증서 내용이 진실임을 증명하는 발행기관의 전자서명 값

출처 : 금융결제원

# 사용자 인증기술의 새로운 흐름

IoT 보고서 / 새로운 인증방법

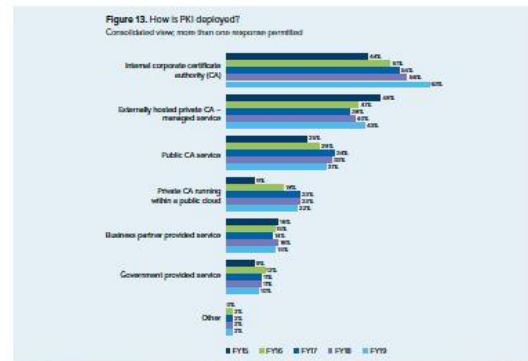
# Global PKI & IoT Trends Study



ncipher.com

What are the most popular methods for deploying enterprise PKI? The most cited method for deploying enterprise PKI, according to Figure 13, is through an internal corporate certificate authority (CA) or an externally hosted private CA – managed service, according to 63 percent and 43 percent of respondents, respectively.

The percentage of respondents who say their companies use externally hosted private CAs declined since 2015 (48 percent vs. 43 percent). Since 2015, more companies have deployed PKI using a private CA running within a public cloud, an increase from 9 percent to 22 percent of respondents.

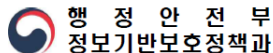


NCIPHER



## 공공웹사이트 인증 수단 소개서

2018. 9.



출처 : 행정안전부

### 제 2 절 인증수단 현황

< 인증수단 예시 >

인증수단	설명	비고
지 식 기 반	1-1.비밀번호 사용자와 서비스 제공자가 서로 공유한 비밀번호 또는 비밀정보로 인증하는 방법	디지털원케스 제공
	1-2.문답식인증 사용자가 사전에 등록한 질문에 대한 응답 값을 입력하여 인증하는 방법	-
	1-3.이미지인증 사용자가 사전에 등록된 이미지에 대한 응답 값을 입력하여 인증하는 방법	
	1-4. 아이핀 주민등록번호 대신 인터넷상에서 신분 (본인확인)을 확인하는 데 쓰이는 인증 수단	정보통신망법에 따른 본인확인수단
	1-5. 권·패턴인증 사전에 정해진 규칙에 맞추어 등록·저장한 권번호 또는 패턴을 입력하여 인증하는 방법	디지털원케스 도입 예정(2018년)
소 지 기 반	2-1. 휴대폰 본인확인 서비스 인터넷에서 생년월일, 성명, 휴대폰 번호 등 정보로 통신사(본인확인) 가맹점 통해 본인확인	정보통신망법에 따른 본인확인수단
	2-2. 휴대폰 SMS인증 사용자가 사전에 등록된 휴대폰에 문자(SMS)로 인증정보를 전송하면 사용자는 이를 입력하여 경당한 사용자임을 인증하는 방법	디지털원케스 제공
	2-3. 비대면본인확인 모바일앱인증 대면 본인확인이 필요한 서비스를 이용하고자 할 때 모바일 앱으로 본인을 인증하는 서비스	
	2-4. OTP 사용자와 발급자가 서로 공유한 OTP 생성키를 이용하여 1회만 사용가능한 비밀 번호(OTP)를 생성하고 이를 전달 또는 입력 하여 인증 * SW방식 HW방식 혼합형 방식이 있음	디지털원케스 제공

- 8 -

# 클라우드 인증서 관리체계

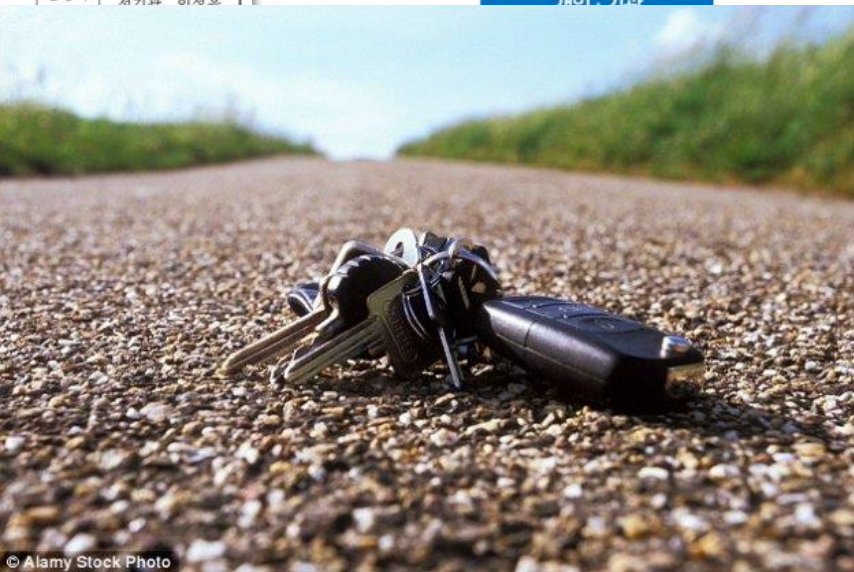
Certificate / Blockchain

# Blockchain Private Key

보도자료	작성과	행정정보공유과
2019년 1월 22일(화) 조간 (19. 1. 21. 12:00 이후)	담당자	과장 하승철 서기과 이서호
행정안전부	보도하여 주시기 바랍니다	

## 연말부터 등초본 등 각종 증명서 - 종이증명서를 전자증명서로 대체시

- 올 연말부터, 정부24에서 종이문서 등 등록등초본 등의 각종 증명서와 증명서 등본 형태로도 발급될 전망이다.
- 행정안전부(장관 김부겸)는 22일 정부24 등의 외부전문가와 함께, 종이증명서 발급을 줄이기 위한 '블록체인 기반의 전자증명서 발급 보고회'를 가졌다.
- 그 간 전자정부 추진의 대표적 과제인 민원인이 직접 관공서에 방문하여 증명서나 확인서를 발급받을 수 없게 되어 불편이 있어왔다.
  - 이로 인해, 국민은 종이문서를 발급받기 위해 관공서에 방문하고, 종이로 접수받은 증명서를 보관해야 하는 등 사회적 비용발생이 컸다.
  - 행정·공공기관 등 정부에서 발급하는 각종 증명서 2,700여종 연간 8억 7천만 건에 달한다. 만약 이 중에서 10%만 전자증명서로 대체해도 교통비 및 종이보관 비용 등 연간 5천억 원 규모의 사회적 비용을 절감할 수 있다.



© Alamy Stock Photo

개요·기타

급정보전송

전자증명서 발급·유통센터

전자증명서보관  
진본성 확인  
발급·전송 등  
정보 저장  
전자문서지갑발급·관리

③ 전자증명서발급

요청

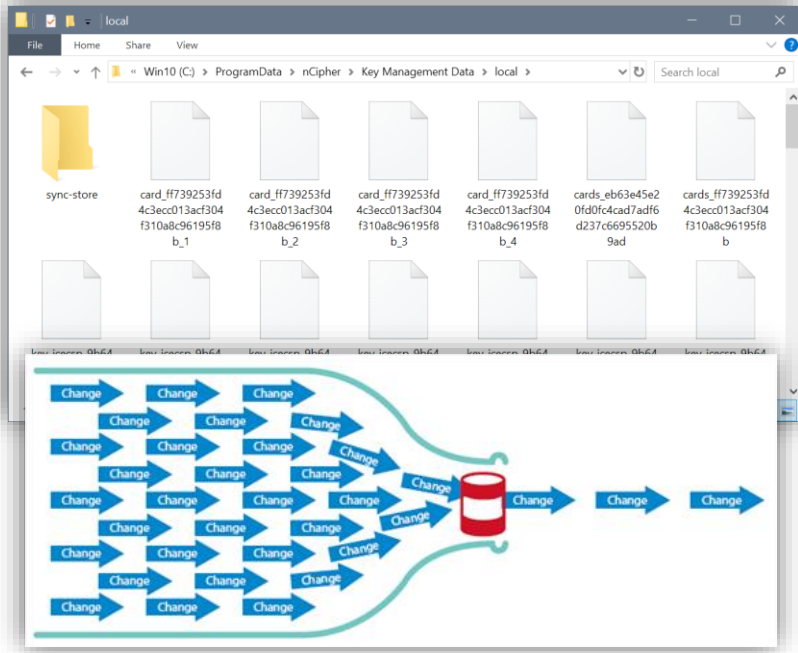
행정·공공기관



증명서 생성

출처 : 행정안전부

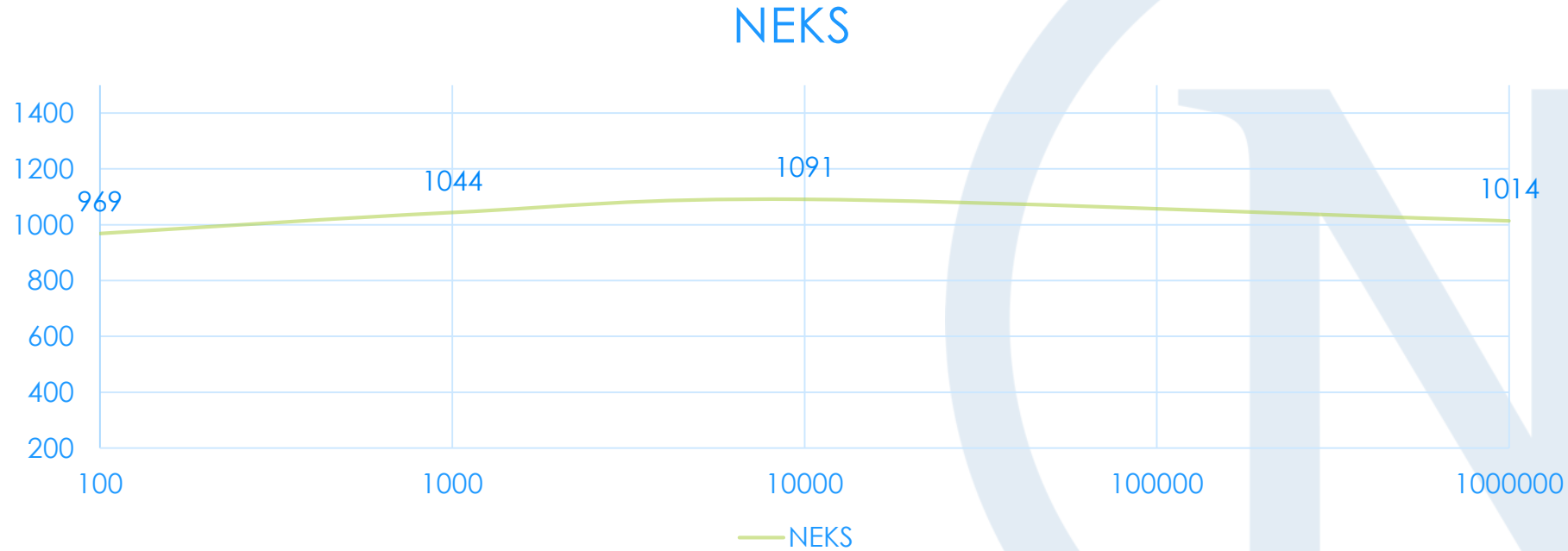
# Blockchain Private Key




ID	Key Blob
001	
002	
003	
004	
005	

# Blockchain Private Key

- NEKS is scalable with almost constant response time





 행정안전부	<b>보도자료</b> 2019년 3월 28일(목) 조간 (3. 27. 12:00 이후)부터 보도하여 주시기 바랍니다.	작성과 담당자	정보자원정책과 과장 이상민 사무관 장정욱
		연락처	044-205-2802 044-205-2810

## 올해까지 86% 공공 웹사이트, 플러그인 없이 서비스

- 문재인 정부의 플러그인 제거 국정과제 추진 가속화 -  
- 정부24, 건강보험, 국민연금 등 주요사이트는 7월까지 제거 완료 -

- 올 하반기부터 정부24(www.gov.kr)에서 인터넷으로 주민등록등본을 출력하거나 퇴직 근로자가 국민연금 홈페이지(www.nps.or.kr)에서 연금을 신청할 때 별도의 플러그인'을 설치하지 않고도 서비스를 이용할 수 있게 된다.

\* 인터넷 브라우저가 제공하지 않는 기능을 제공하기 위한 액티브X 및 EXE파일 등의 별도 설치 프로그램

- 행정안전부(장관 김부겸)는 국민들이 플러그인 설치없이 편리하게 전자정부서비스를 이용할 수 있도록 올해 말까지 각 기관 1,278개 대민 웹사이트에 포함된 2,014개의 플러그인을 제거할 계획이라고 밝혔다.

※ "불필요한 플러그인 제거 등 편리한 온라인 서비스 환경 구현"을 국정과제로 추진중

- 이에 따라, 행정-공공기관이 운영하는 전체 대민 웹사이트 8,059개 중 86%인 6,924개의 웹사이트가 플러그인 없는 서비스를 제공하게 된다.

- 작년에는 ▲홈택스 연말정산(국세청) ▲국가법령정보(법제처) ▲새얼 시스템(여가부) ▲기후정보포털(기상청) ▲다산콜센터(서울시) 등 776개 웹사이트에서 1,159개 플러그인을 제거하였으며,

## 3 전자서명

### 개요

전자서명은 서명자를 확인하고 서명자가 당해 전자문서에 서명했다는 사실을 나타내는 데 이용하기 위해 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보

전자서명은 전자문서의 서명자 식별, 신원확인, 문서내용의 위변조 방지, 거래(결제)사실에 대한 부인방지, 정보 노출 방지 등을 위해 사용

전자인증서는 사용자의 신원 등을 확인하기 위한 전자서명키를 담고 있는 파일로, 공인인증기관에서 보증한 공인인증서와 개별기관에서 보증한 사설인증서가 있음

전자서명에 사용되는 전자인증서는 일대일, 같은 관공공, 같은관공공, 같은관공공

전자서명은 전자문서의 서명자 식별, 신원확인, 문서내용의 위변조 방지, 거래(결제)사실에 대한 부인방지, 정보 노출 방지 등을 위해 사용

일련번호	인증서 일련번호
발행기관 식별명칭	인증기관 식별명칭
유효기간	인증서 유효기간 시작일과 만료일
소유자 식별명칭	인증서 소유자의 실명을 포함한 식별명칭
공개키	인증서 소유자의 공개키
공개키 사용목적	공개키의 사용목적을 명시(전자서명, 암호화 등)
인증서 정책	인증서 발행기관이 인증서를 발행하는데 적용한 인증서 정책과 인증업무 규칙을 명시
발행기관의 서명값	인증서 내용이 진실임을 증명하는 발행기관의 전자서명 값



**X 10,000,000**

# HSM 도입의 ABC

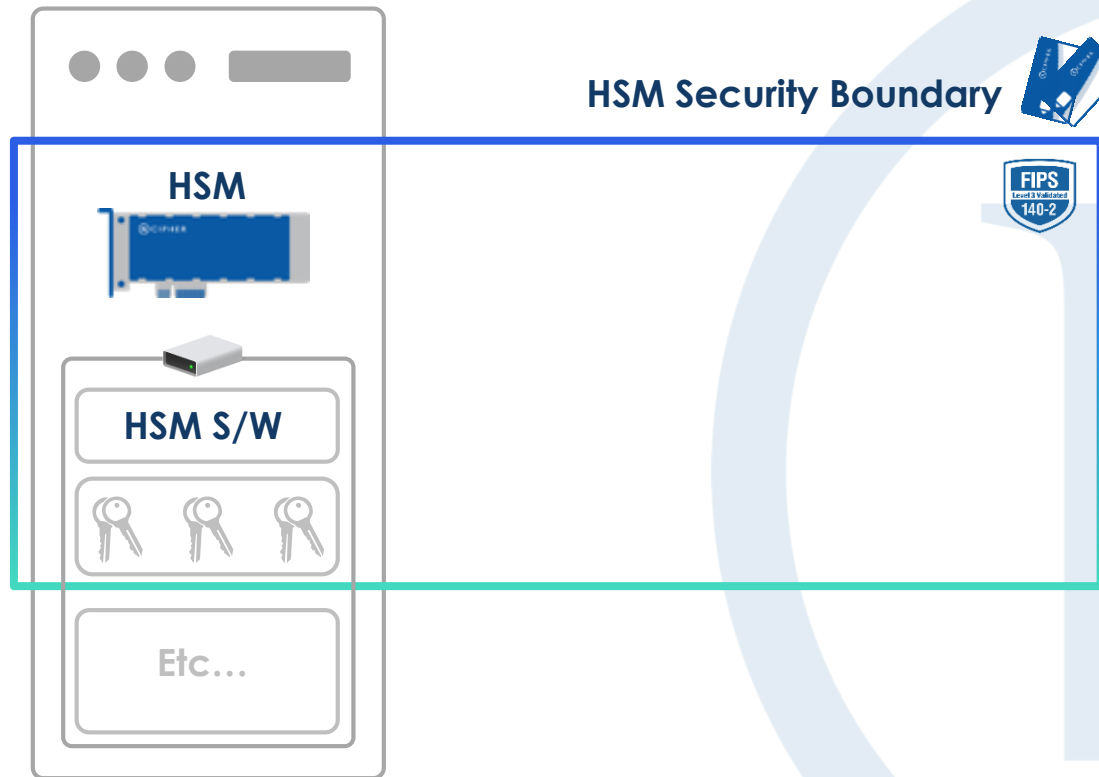
HSM 관련 지침 / HSM 도입 시나리오

# HSM 관련 지침

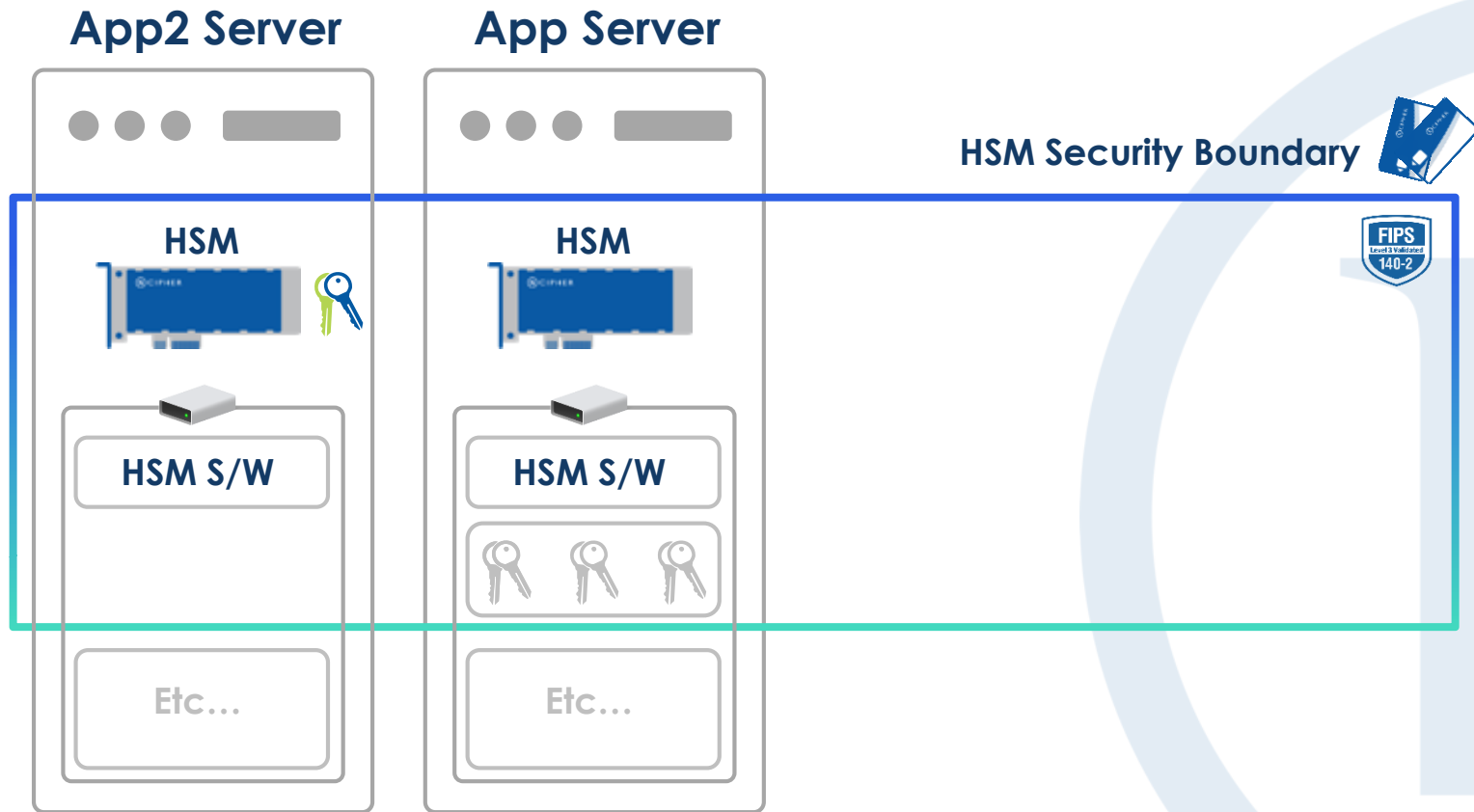


# HSM 도입 시나리오

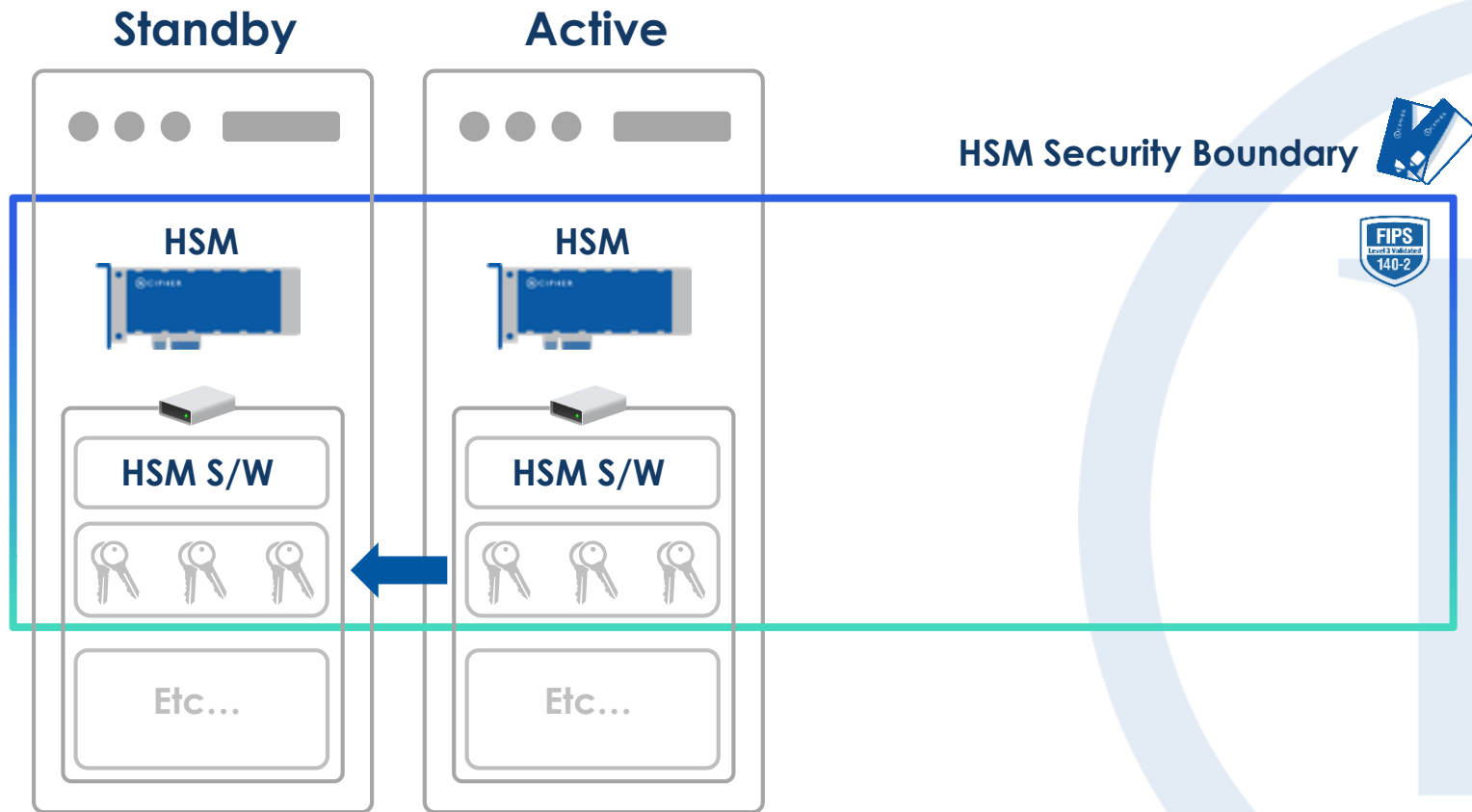
## App Server



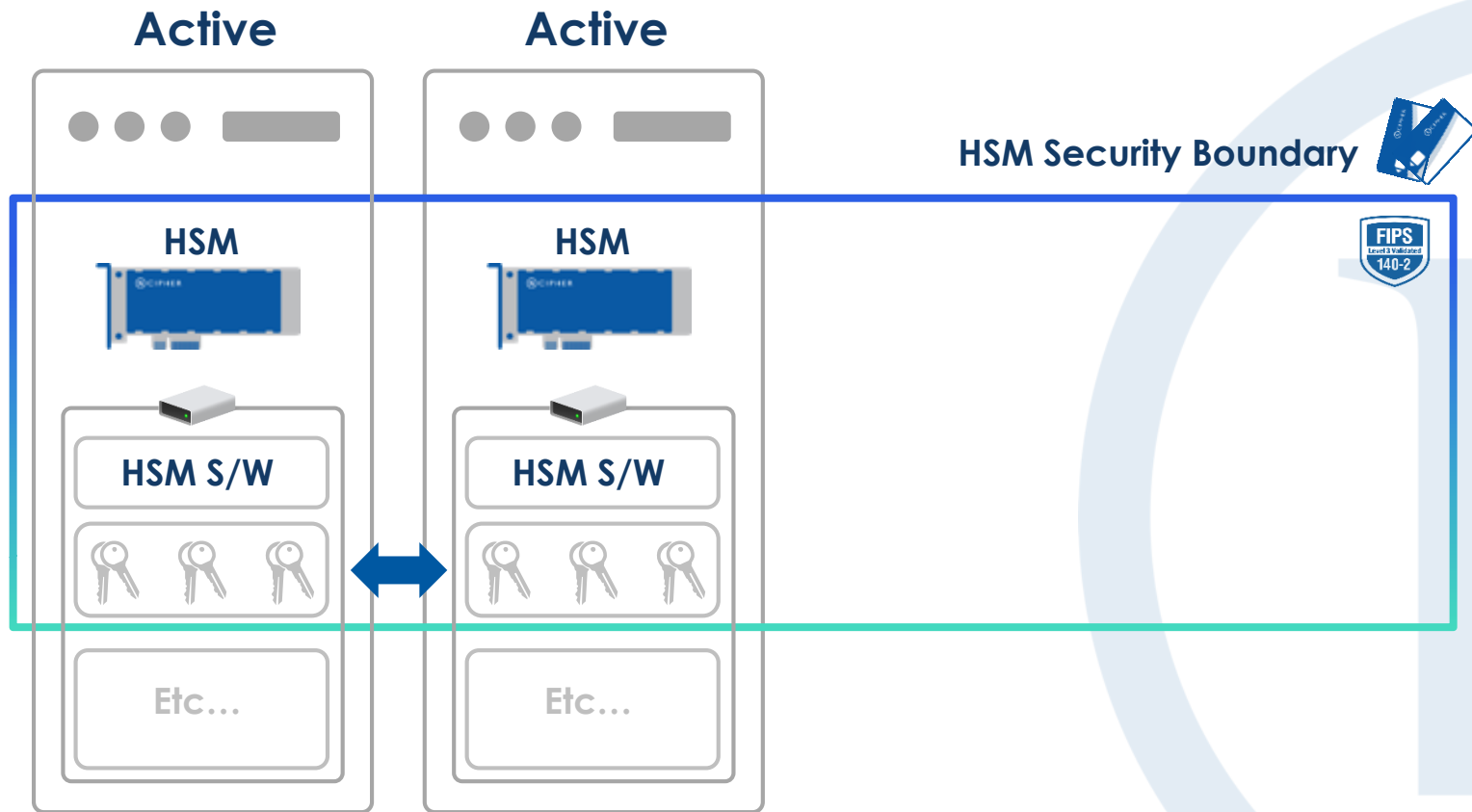
# HSM 도입 시나리오



# HSM 도입 시나리오



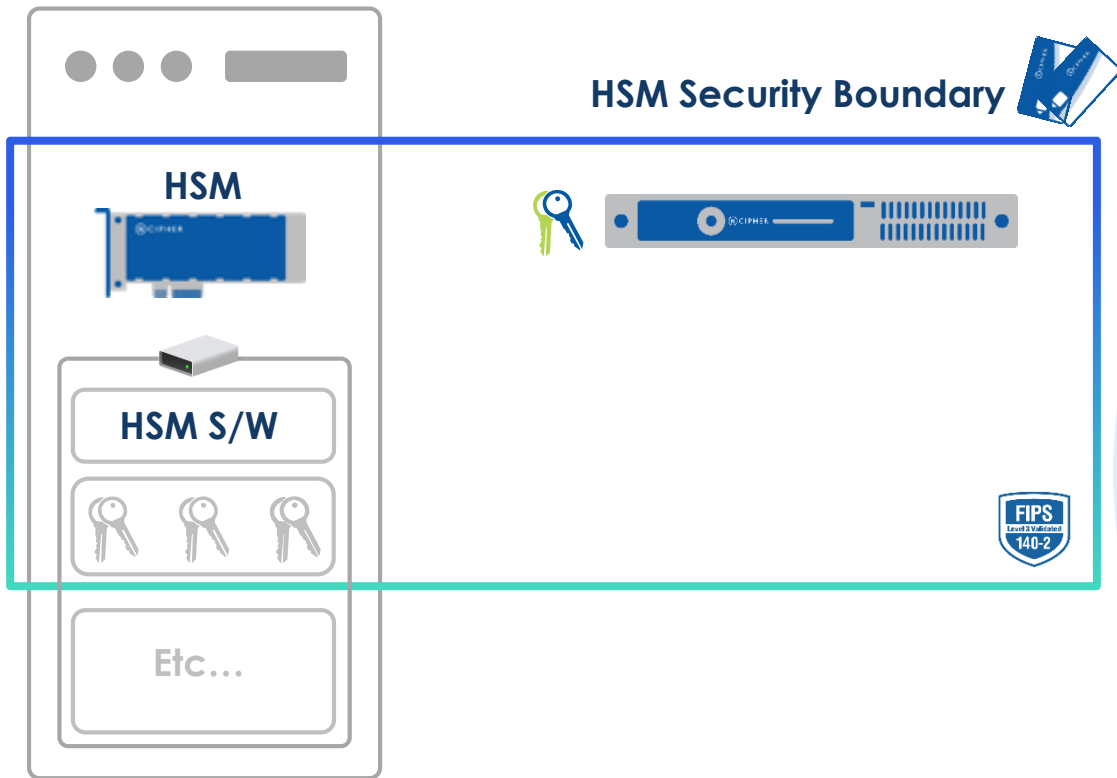
# HSM 도입 시나리오



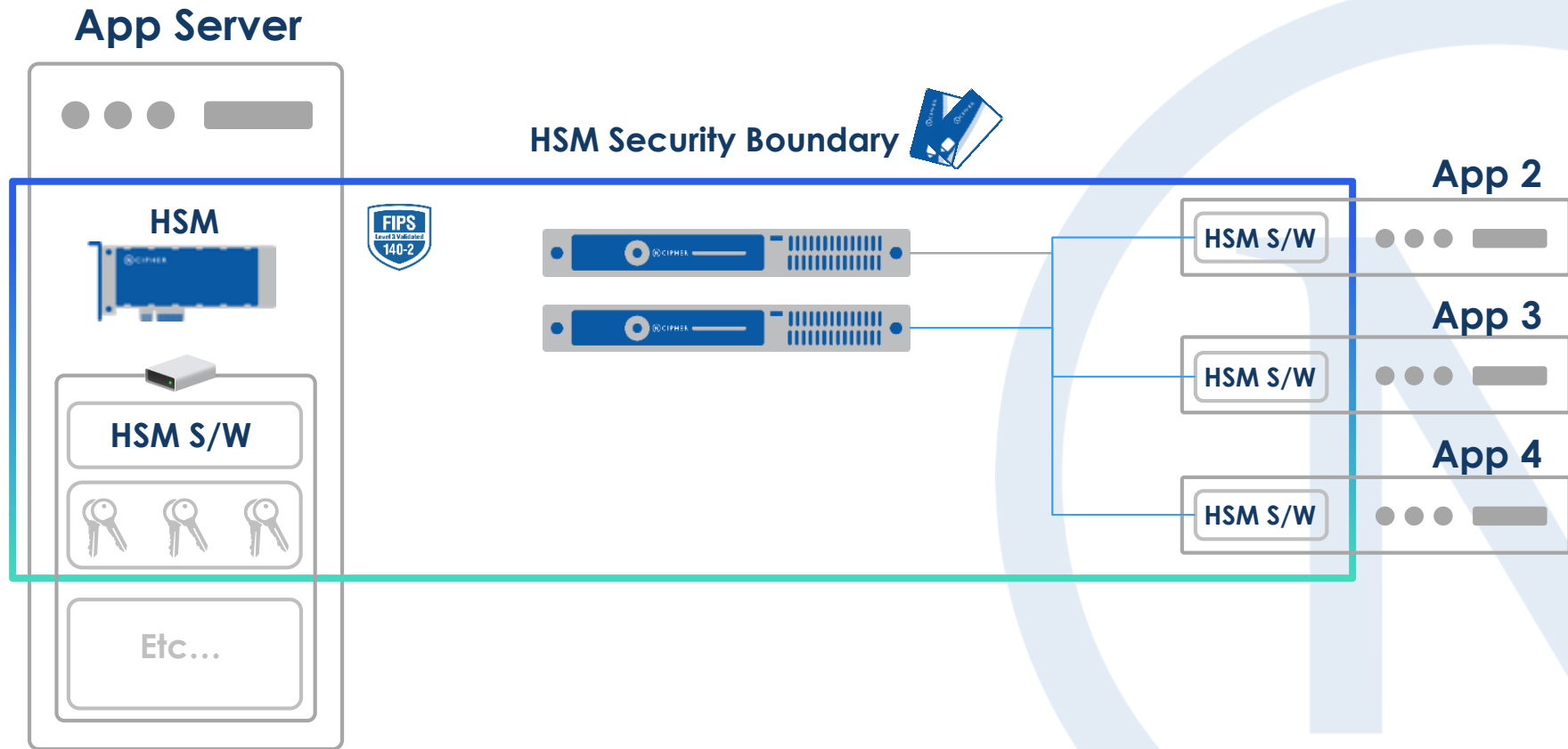


# HSM 도입 시나리오

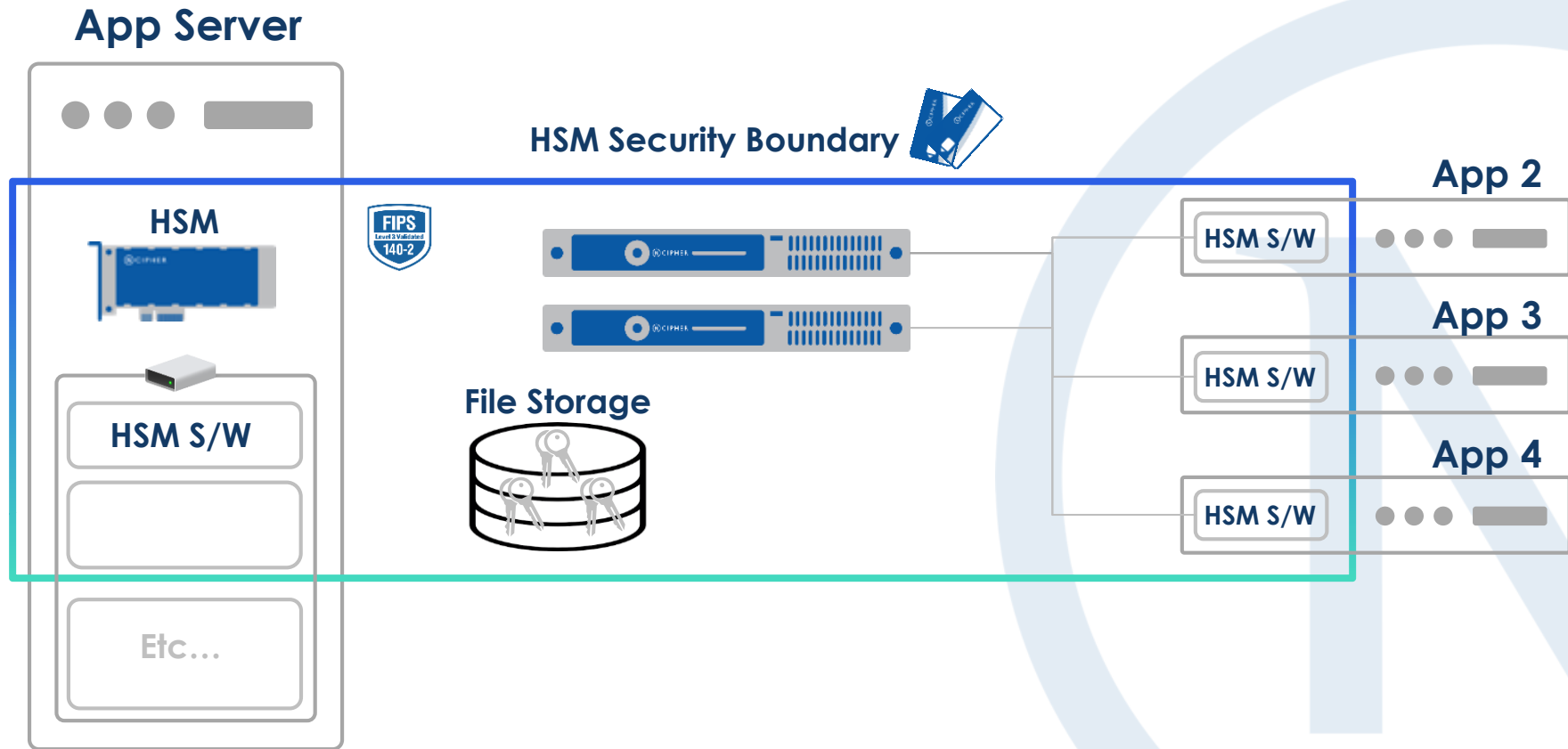
## App Server



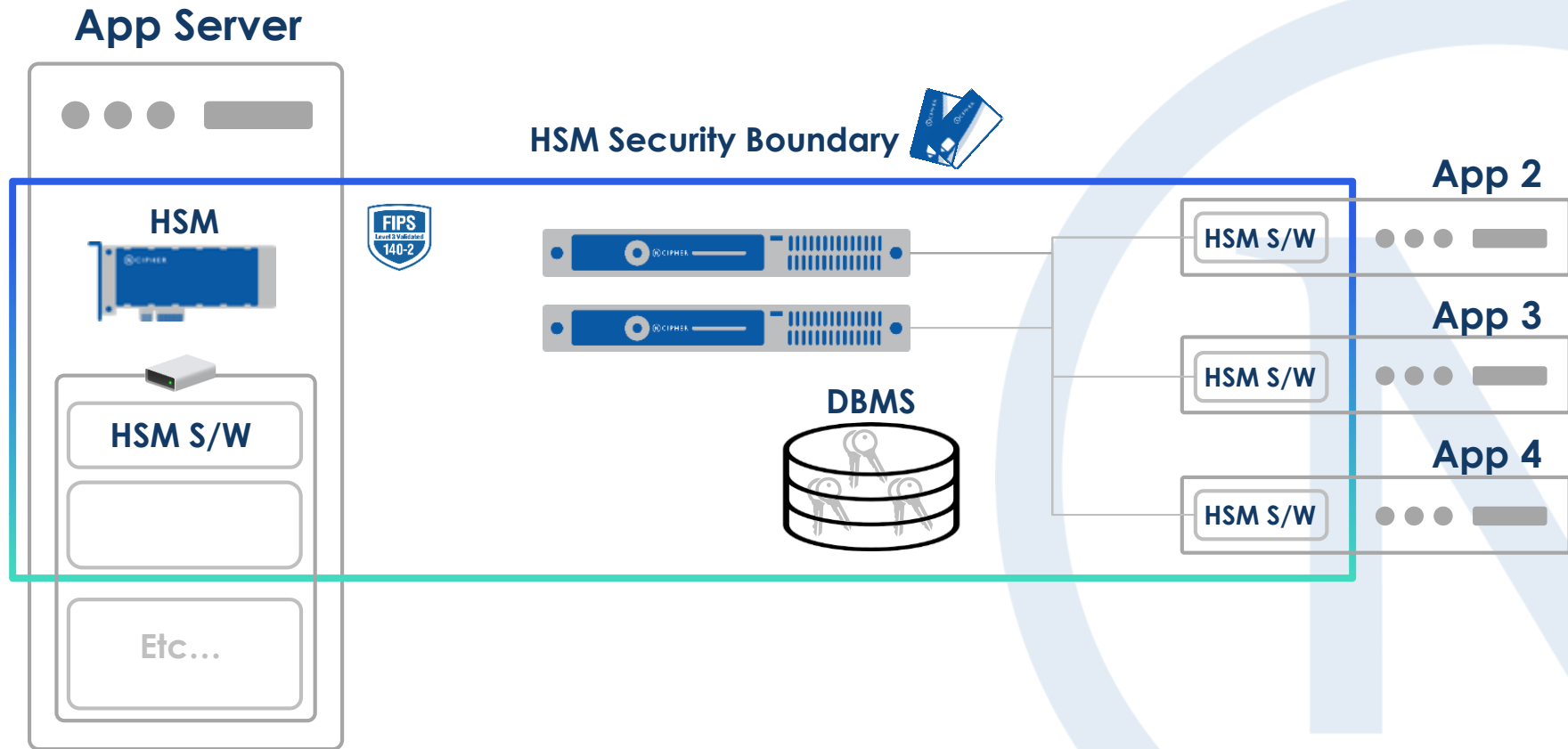
# HSM 도입 시나리오



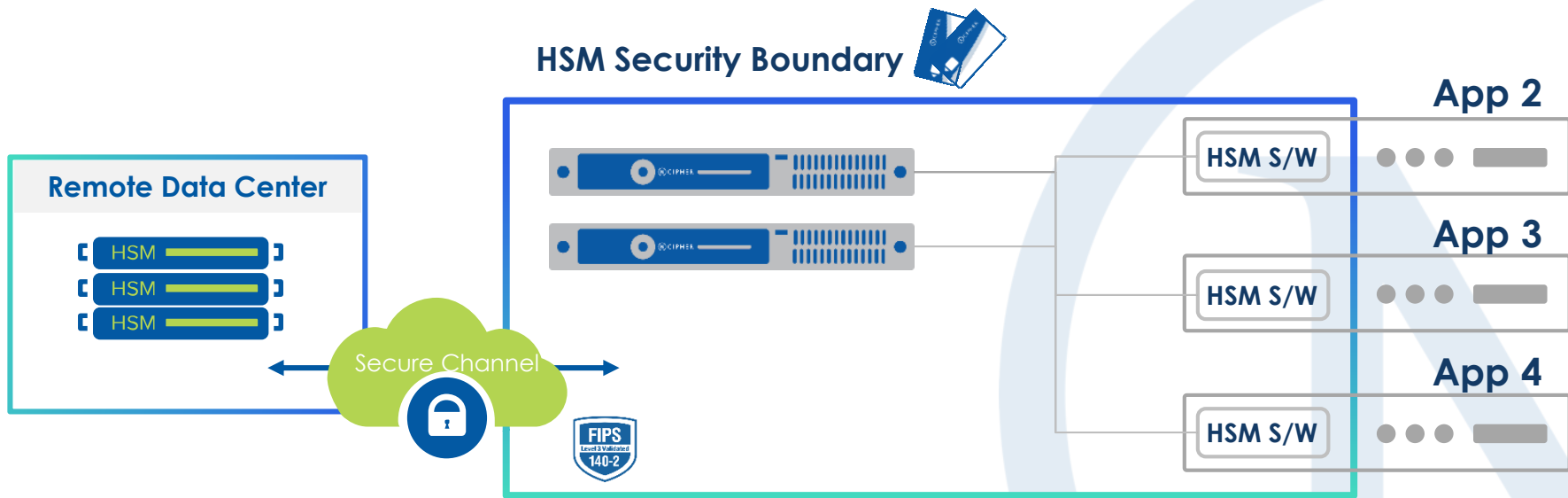
# HSM 도입 시나리오



# HSM 도입 시나리오

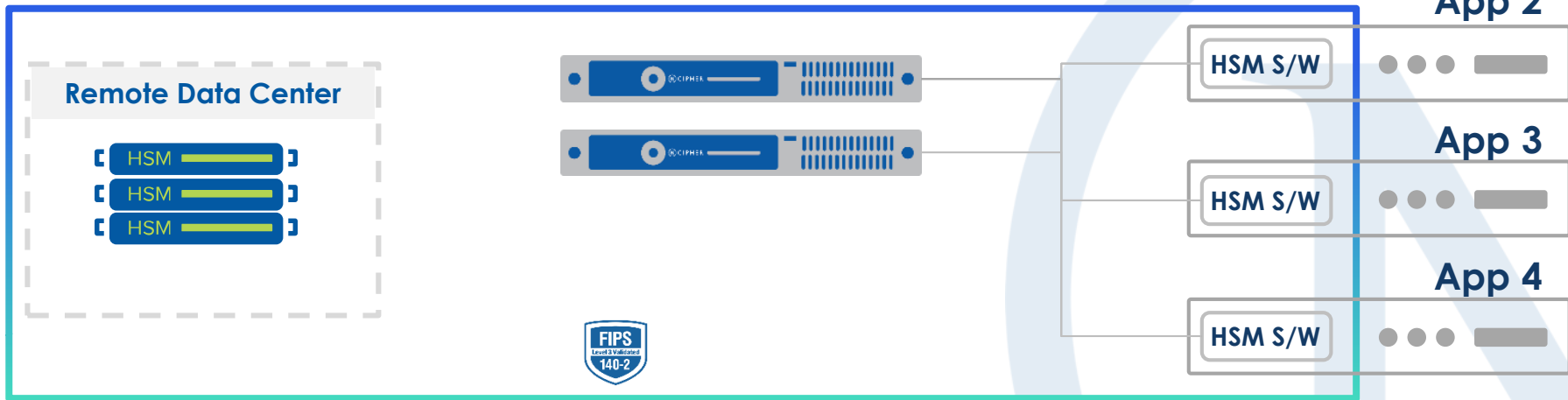


# HSM 도입 시나리오



# HSM 도입 시나리오

## HSM Security Boundary





감사합니다