The best solution for ensuring Smartphone security

Introduction to Mobile Device Management

NEXDIGM

WE ARE MAKING THE NEXT PARADIGM

Contents

1. 넥스다임 MDM 서비스 개요

1.1 스마트 기기 MDM 도입의 필요성

스마트 기기 MDM 도입의 필요성

- 스마트 기기 확산에 따른 단말 정보 유출 문제 이슈화 : 단말 분실 시에 저장된 정보 유출 방지 문제 부각
- 스마트 기기 보안성 이슈 : 악의적, 고의적 정보 유출, 악성코드를 통한 정보유출, 통신/저장매체를 통한 정보유출 문제 심각

MDM 솔루션 도입을 통한 스마트 기기 보안성 확보

스마트 기기 MDM 도입 필요

- 분실 단말 관리
- 스마트 기기 보안 정책 필요
- 단말 응용프로그램 관리

스마트 기기 보안성 강화

- 단말 저장 데이터 분실예방, 대응 (PIMS,E-Mail 등)
- 스마트 단말기를 통한 보안사고 제어 (네트워크 차단 등)
- 외장 매체를 통한 정보유출 방지

스마트 폰 응용프로그램 활성화

- 앱 스토어 활성화로 앱 서비스 확산
- 검증되지 않은 위해 앱 서비스 증가
- 악의적 앱 사용자 관리 체계 필요

보안서비스 제공 Needs 증대

- 스마트 기기 사용자 관리 필요
- 비 보안성 네트워크에 대한 관리자 단말 제어 필요성 증대
- 각 Application별 보안솔루션 적용에 따른 비용증가

정부 정책에 대응 필요

- 악의적.고의적 해킹 및 정부기관 정보 유출에 대한 이슈화
- 단말 제어 기능을 통한 보안성 강화

1.2 넥스다임 MDM 정의 및 특징

MDM 정의 및 특징

- 넥스다임 MDM 은 제조사/OS 제조사에 독립적인 표준 기술 규격을 적용한 단말 제어기술로 구현
- 국내 최초 MDM 론칭, 상용화 완료/ 타사와 달리 C2DM(안드로이드), APNS(애플) 방식이 아닌 E2E 보안 제공
- 공공기관용 스마트폰 가이드라인을 준수한 MDM 기술
- 아이폰/아이패드의 단말 특수성을 반영하는 2중 규격화 제공

MDM의 정의

MDM은 OTA(Over To Air)를 이용하여 언제 어디서나 모바일 기기가 네트워크에 연결된 상태인 경우,

모바일 기기를 관리할 수 있는 시스템으로서 원격에서 모바일 기기의 어플리케이션 배포,

데이터 및 환경 설정 변경, 분실 및 장치 관리를 통합적으로 수행하는 모바일 보안의 핵심 솔루션입니다.

MDM의 특징

I. 아이폰/아이패드 등 애플 단말 MDM 기술

- 폐쇄형 단말 OEM Protocol 기술 개발, 반영
  - IOS 기술 분석과 (Draft) RFC 표준 규격을 활용한 단말 관리기능 적용
  - 단말 Profile 기반 서비스 제공으로 편리하고 손쉽게 스마트 폰 관리 제공
  - 자체 규격화한 기술을 기반으로 국내 최초의 아이폰 제어 기술 확보

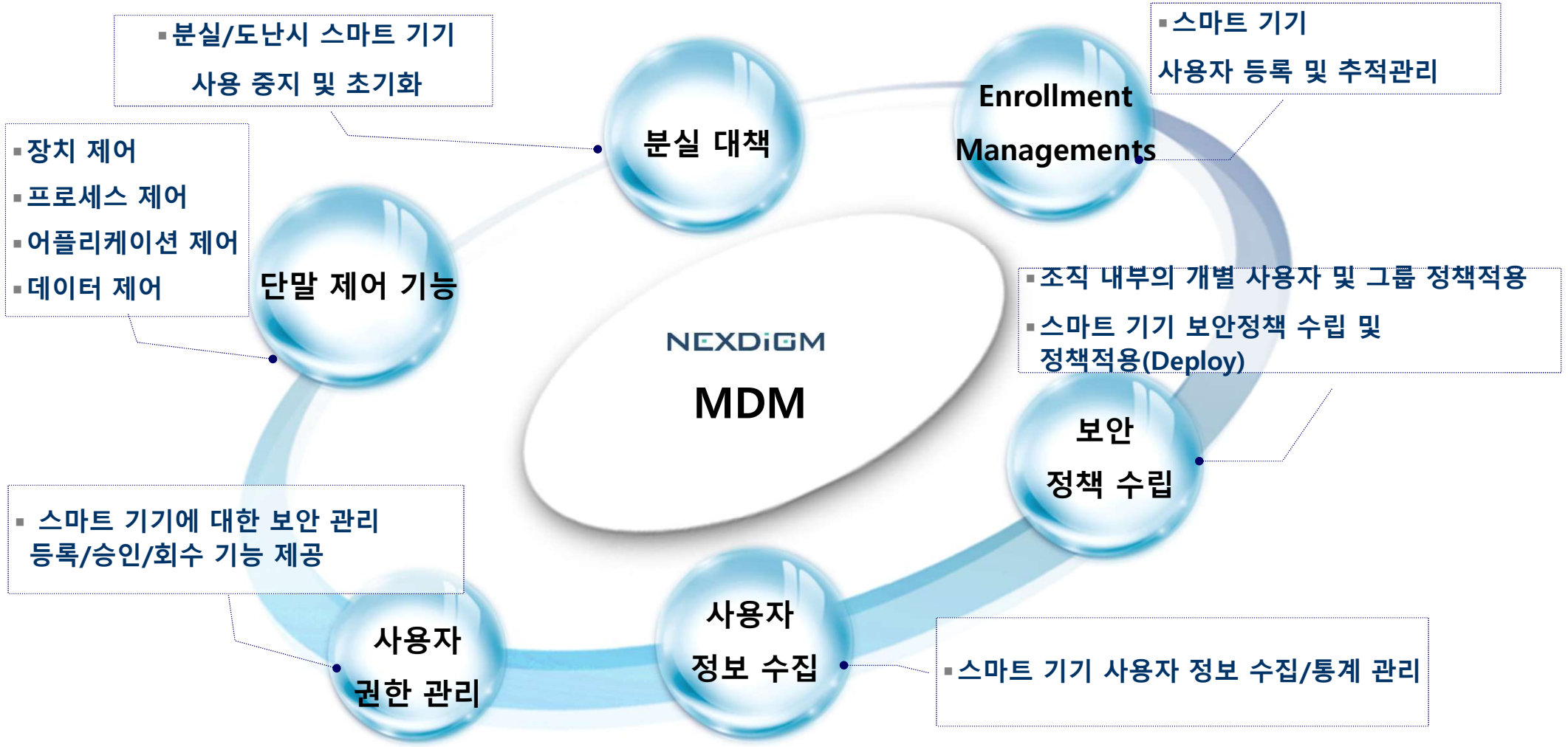
II. 안드로이드 단말 MDM 기술

- OMA DM 적용으로 OMTP 진영의 기술 개발 반영
  - 단말 OMA DM 표준 규격을 OS 레벨에서 적용, 제조사에 독립적인 기술확보
  - 단말 System API 레벨에서 모듈화를 지원, 3rd Party 어플리케이션 기술 지원
  - 제조사와의 모델별 공동 기술 개발을 통한 특수형 단말 MDM 기능 제공
- 단말 멀티 태스킹 지원을 통한 자체 규격 적용 가능
  - 규격화 된 MDM 모듈을 통해서 다양한 스마트폰 관리 서비스 지원
  - 규격화된 모듈(Library 형태)로 배포 정책 제공
  - 자체 통신 규격 적용 : 매체 및 App. 관리 등 다양한 보안 정책 지원

1.3 넥스다임 MDM 주요 제공 기능

MDM 제공 기능

- 넥스다임 MDM은 스마트 기기의 보안과 관리를 통합하여 제공하는 모바일 보안 솔루션입니다.
- 분실도난 대비, 원격 데이터 보호, 스마트 기기 기능 제어, 관리자 기능, Application 관리, 보안정책 수립 등의 기능을 제공합니다.



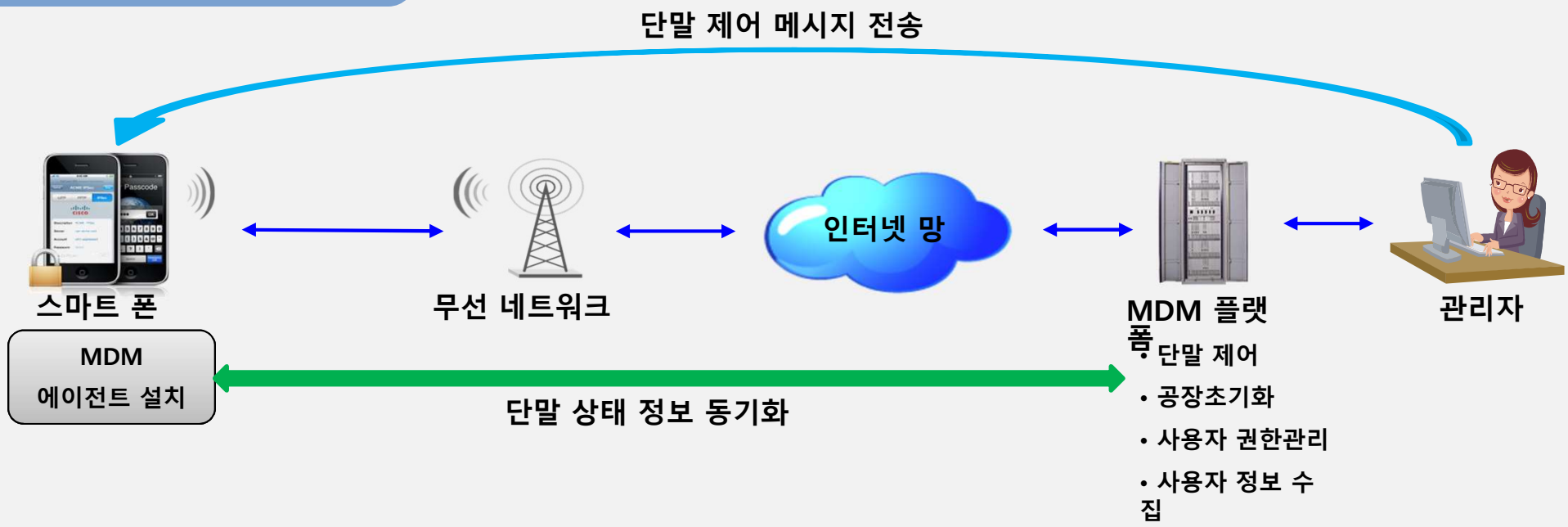
2. 넥스다임 MDM Architecture

2.1 넥스다임 MDM 서비스 구성도

넥스다임 MDM 서비스 구성도

- 네트워크를 통한 단말 저장 데이터 동기화 및 각종 보안 침입 및 분실 시에 개인 데이터를 보호하기 위한 단말관리 기능 서비스
- 스마트폰의 필수 서비스로 에이전트와 플랫폼으로 구성하여 단말제어를 수행

넥스다임 MDM 서비스 구성도

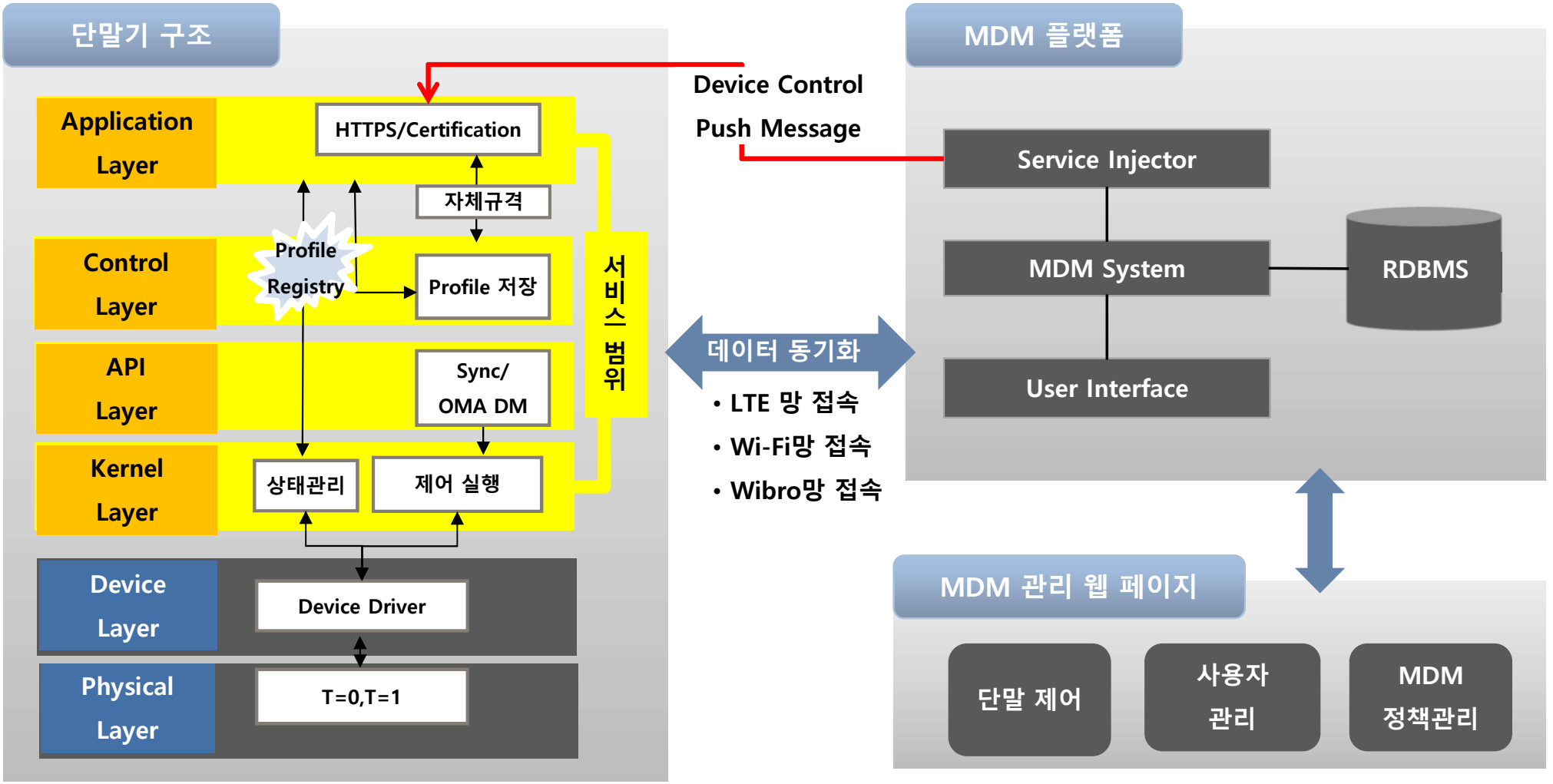


- MDM 에이전트 : 원격으로 단말기를 제어하기 위해서는 단말기에 클라이언트용 MDM 에이전트 설치
- MDM 플랫폼 : MDM 솔루션을 탑재한 플랫폼으로 SaaS, 또는 구축형으로 선택적 구축가능(SaaS 선택 시 별도의 구축 투자 불필요)
- 단말 제어 메시지 : 관리자가 MDM 전용 관리 웹 페이지에서 단말기를 제어하기 위한 신호를 원격으로 전송
- 단말 상태 정보 동기화 : 단말기에 설치된 MDM 에이전트와 MDM 플랫폼간에 단말기 상태 정보를 동기화하여 관리

2.2 넥스다임 MDM Architecture 구성도

넥스다임 MDM Architecture 구성도

- 단말 관리 기능을 수행하는 모듈을 라이브러리, Application, Profile 형태로 3rd Party 개발사에 지원
- 스마트 단말 관리 기술을 아래 구성도와 같이 정의



3. 넥스다임 MDM 세부 기능

3.1 넥스다임 MDM 세부 기능

넥스다임 MDM 세부 기능

- 고객사의 보안 정책에 따라서 넥스다임 MDM 버전을 관리하고 있으며, 고객사의 정책에 따라서 버전별로 지원 가능
- 최다 레퍼런스와 상용화 기술, 고객요구 반영의 결과로 최상의 관리 및 사용자 지원 제공

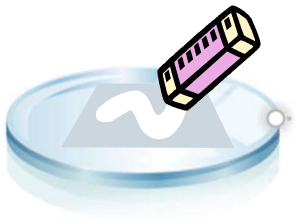
구분		Android(Above OS 6.0)
Application 종료 방지	Application 사용자 임의 종료 차단	●
S/W inventory 관리	Application 설치 및 삭제 기능	●
분실 관리 서비스	원격 초기화(Remote Wipe)	●
	원격 잠금(Remote Lock)	●
단말 제어 서비스	Message 전송	●
	카메라 제어	●
	스크린 캡처 제어	●
	블루투스 제어	●
	마이크 제어	●
	Wifi 제어	●
	USIM 관리	●
	SD card control	●
	Tethering Control	●
	USB 제어	●
	NFC 제어 지원	●
Application 관리 서비스	원격 S/W 관리	●
	브라우저 제어	●
	App store (Market) 제어	●
	You Tube 제어	●
사용자 관리 서비스	개인별/그룹별 정책관리	●
단말 모니터링 서비스	개인별/그룹별 단말 모니터링	●
	단말기 루팅 여부 모니터링	●
	단말의 MDM 동작여부 모니터링	●
	단말 위치 찾기(Map)	●
	GPS 제어	●
단말 프로세스 관리 서비스	Application 제어(White List)	●
사용자 DATA 관리 서비스	Directory 관리	●
	Backup 관리	●

●: 지원, X: 미지원, ◐: 부분지원, -: 해당사항 없음

3.2 분실 관리 서비스

분실 관리 서비스

- 단말기를 분실하거나 기타 이유로 단말기 내부의 중요 자료들을 보호할 수 없는 경우 해당 단말기를 제어할 수 있는 기능



원격 초기화

- 원격에서 지정한 단말기를 공장 초기화 상태로 만드는 기능
- Remote Factory reset

초기화 상태확인

- 초기화 시도 후 초기화 설정 확인 정보를 웹 서비스를 통해 확인하는 기
- 특정 조건 설정 및 앱을 재설정, 설치하는 기능

단말 잠금

- 원격에서 지정한 단말기를 관리자 비밀번호에 의해서 잠금 기능을 설정

단말 잠금 해지

- 잠금 상태의 단말기를 원격에서 해지시키는 기능
  * 관리자 지정 비밀번호 정보를 공유하여 잠금 해지 설정할 수 있도록 지원 가능

3.3 단말 제어 서비스

단말 제어 서비스

- 스마트 기기의 개별 기능을 선택적으로 사용제한, 해제할 수 있는 제어기능

카메라 제어

- 카메라 기능 차단
- 카메라 기능 차단 해제

블루투스 제어

- 블루투스 기능 차단
- 블루투스 기능 차단 해제

WIFI 제어

- Wifi 모뎀 기능 차단
- Wifi 모뎀 기능 차단 해제

외장 메모리 제어

- Micro SD 등 저장 매체 차단
- 외부 저장 매체 차단 해제

GPS 제어

- GPS 기능 차단
- GPS 기능 차단 해제

USB 제어

- USB 기능 차단
- USB 기능 차단 해제

테더링 제어

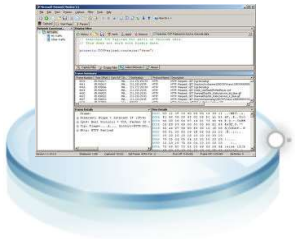
- 테더링 기능 차단
- 테더링 기능 차단 해제

* 제어 기능은 단말 모델 및 운영체제별로 제한될 수 있습니다.

3.4 어플리케이션 관리 서비스

어플리케이션 관리 서비스

- 사용자 단말기에 설치된 어플리케이션을 실시간으로 관리할 수 있는 기능



어플리케이션 모니터링

- 이용자별 어플리케이션 설치 리스트를 확인

어플리케이션 배포

- 원격에서 어플리케이션을 강제 또는 사용자 동의 후 설치할 수 있는 기능

어플리케이션 삭제

- 원격에서 어플리케이션을 강제 또는 사용자 동의 후 설치할 수 있는 기능

어플리케이션 패치

- 원격에서 어플리케이션을 강제 또는 사용자 동의 후 패치할 수 있는 기능

* 제어 기능은 단말 모델 및 운영체제별로 제한될 수 있습니다.

3.5 사용자 관리 서비스

사용자 관리 서비스

- 사용자를 그룹별로 생성하여 생성/이동/삭제할 수 있는 관리자 기능

그룹 관리

- 그룹 생성 기능 : 사용자 그룹을 생성할 수 있는 기능
- 그룹 삭제 기능 : 사용자 그룹을 삭제할 수 있는 기능

사용자 관리

- 사용자 생성 기능 : 정상적인 사용자 가입이 아닌 관리자에 의해 강제로 사용자를 생성할 수 있는 기능
- 사용자 삭제 기능 : 관리자에 의해서 사용자 강제 삭제기능
- 사용자 이동 기능 : 특정 그룹에 설정된 사용자를 다른 그룹으로 drag 이동 기능

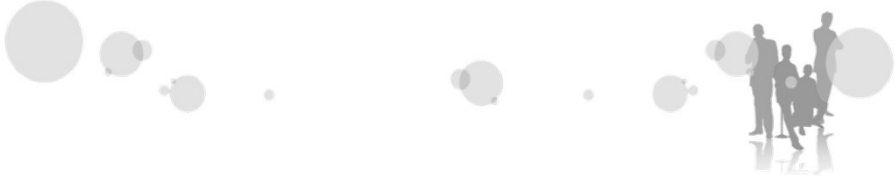
조직도 관리

- 이용자를 CSV 파일로 업로드 하여 강제 설정할 수 있는 기능

	A	B	C	D	E
1	관리팀				
2		관리1팀			
3		관리2팀			
4	영업부				
5		영업1팀			
6		영업2팀			
7	인사부				
8	행정부				
9		행정1팀			
10		행정2팀			
11		행정3팀			
12	개발팀				
13		서버개발			
14			오피스		
15			컨버전스		
16		클라이언트개발			
17			모바일		
18				아이폰	
19				안드로이드	
20			메신저		
21					
22					

관리자 기능

- Sub 관리자를 생성할 수 있고 그룹별로 관리자를 생성할 수 있는 기능



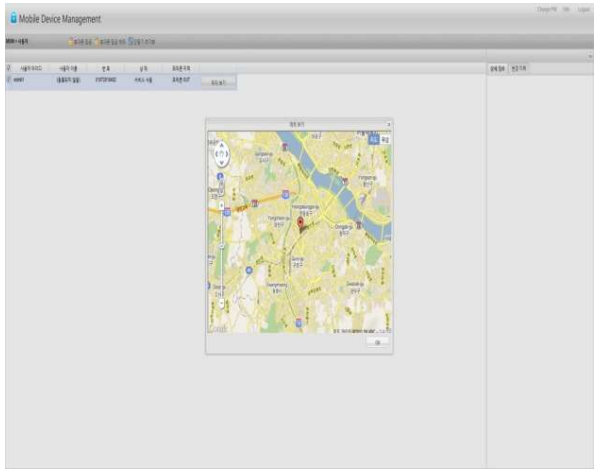
3.6 단말 모니터링 서비스

단말 모니터링 서비스

- 스마트 기기 사용자의 단말 현황 정보를 원격 모니터링할 수 있도록 웹 서비스를 제공하는 기능

사용자 위치 조회 기능

- 사용자를 조회하는 위치를 확인할 수 있는 기능



사용자 검색 기능

- 사용자를 검색하여 특정 사용자를 조회할 수 있는 기능

- 사용자의 어플리케이션 설치 현황을 모니터링 할 수 있는 기능

사용자 어플리케이션 조회 기능

- 사용자별 제어 이력을 모니터링 할 수 있는 기능

사용자 이력관리 기능

- 사용자의 제어 설정된 현황을 모니터링 할 수 있는 기능

제어 모니터링 기능

3.7 단말 프로세스 관리 서비스

단말 프로세스 관리 서비스

- 스마트 기기 관리 정책에 따라서 각종 세부 기능을 관리 제어하는 단말 프로세스 관리 서비스입니다.

White List 설정 기능

- 전체 사용자의 단말 프로세스 허용 정책에 따라 단말 프로세스를 설정할 수 있는 기능

단말 프로세스 권한 설정 기능

- 단말 프로세스 관리 정책에 따라 MDM 기능 모듈을 업무용 어플리케이션에 내장 기능

그룹별 프로세스 설정 기능

- 그룹별 단말 프로세스 허용 정책에 따라 그룹별 단말 프로세스 설정

단말 멀티 테스킹 방지 기능

- 업무용 프로그램이 구동 중에 타 프로세스가 구동되지 않도록 설정

Application Buffer Lock 기능

- 단말 프로세스 구동 중 사용된 임시 메모리 접근차단 기능

파일 암호화 기능

- 업무용 파일이 고의적 메모리 Tracing에 복사되어도 열리지 않도록 파일 암호화 적용 기능

특수사용자 단말 프로세스 설정기능

- 사용자의 어플리케이션 설치 현황을 모니터링 할 수 있는 기능

단말 프로세스 변경 기능

- 그룹/특수 사용자별 단말 프로세스를 변경할 수 있는 기능

White 리스트 변경 기능

- White List 설정을 변경하는 기능





3.8 사용자 Data 관리 서비스

사용자 Data 관리 서비스

- 사용자 스마트 기기를 백업/관리할 수 있는 기능으로 적용을 위해서는 별도의 스토리지 용량 산정 후 NAS 스토리지를 구성하여 제공

데이터 백업 기능
- 사용자 단말 데이터를 원격으로 백업하는 기능

데이터 관리 기능
- 사용자별 백업 데이터를 암호화하여 저장할 수 있는 기능

데이터 복구 기능
- 원격에서 사용자 스마트폰에 백업된 데이터로 복구시키는 기능

사용자 데이터 접근 권한 기능
- 사용자 데이터를 접근할 수 있는 권한을 설정하는 기능그룹 생성 기능 : 사용자 그룹을 생성할 수 있는 기능

스마트폰 이용 데이터 관리 기능
- 음성/SMS 통화내역, 로밍정보, 데이터 사용량 등 스마트 폰 이용통계 정보를 원격에서 관리하는 기능(넥스다임 고객센터 어플리케이션을 통해서 제공하는 기능임)

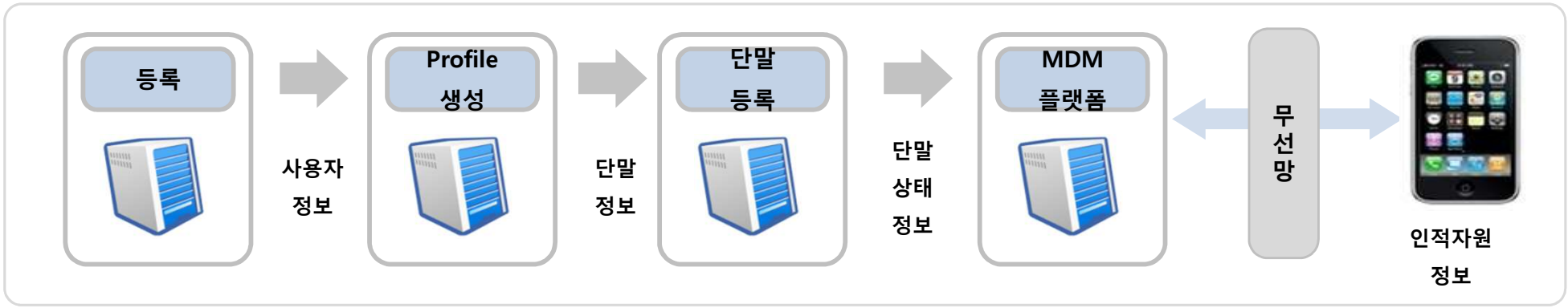
4. Use Case(적용) 시나리오

4.1 서비스 제공 방식

서비스 제공 방식

- MDM 서비스는 사용자 정보를 등록하여 Profile을 생성하고 단말기 정보를 MDM 플랫폼에 등록하여 서비스 제공

서비스 시나리오



동작 Logic

가입자 Profile Provisioning

- 단말기 부가서비스 가입자의 경우 Provisioning

✓애플 = 원격 Profile 배포

✓기타 = Application 배포, Module Preload 설치, 라이브러리 배포를 통한 CP Application 배포

- 단말 상태 등록/사용자 인증

✓단말 자동 설치 상태 = 단말 상태 등록 및 단말 관리 서비스 제공

✓단말 상태 등록 = 설치된 Profile를 통한 USIM 변경 및 Device Profile 변경 사항 서버 자동 등록

✓사용자 인증 체계 = 전화번호, USIM Serial 인증(월정액 서비스 인 경우 서비스 인증 추가)

MDM 동작

- 사용자 서비스 웹 인터페이스 접속
- 사용자 인증 후 서비스 기능 선택
- 단말 상태 현황 모니터링 후 선택된 기능 수행 = Control Push Message 발송
- 단말 Message 수신 후 해당 기능 수행 = 초기화, 백업 등

4.2 넥스다임 MDM 구동 화면

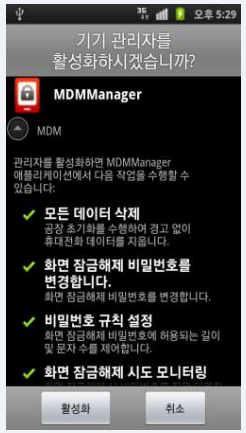
넥스다임 MDM 구동 화면

- 스마트 기기에서 구현되는 MDM 어플리케이션 예시 화면
- MDM 관리자가 사용하는 웹 터미널 상의 관리자 화면

화면 잠금상태

프로그램 실행차단

정상 사용 모드



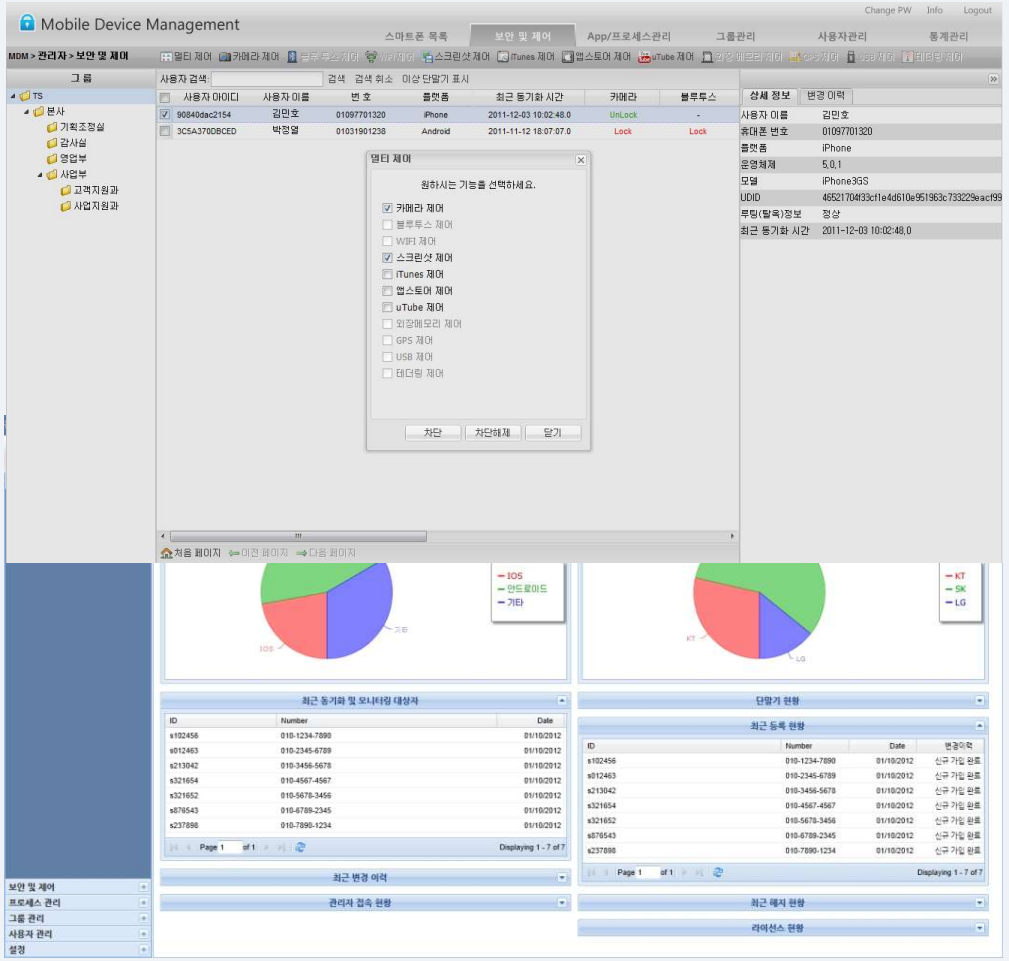
설치화면

모바일 AP 차단

카메라 차단

제어중 메인화면

GPS 차단



MDM Administrator(Web Terminal)

4.3 시스템 지원 사양

시스템 지원 사양

- Application 지원 방식 : Application 또는 연동 규격서 배포, 내장형 라이브러리 지원
- 운용 서버 사양 : 아래 사양 참조

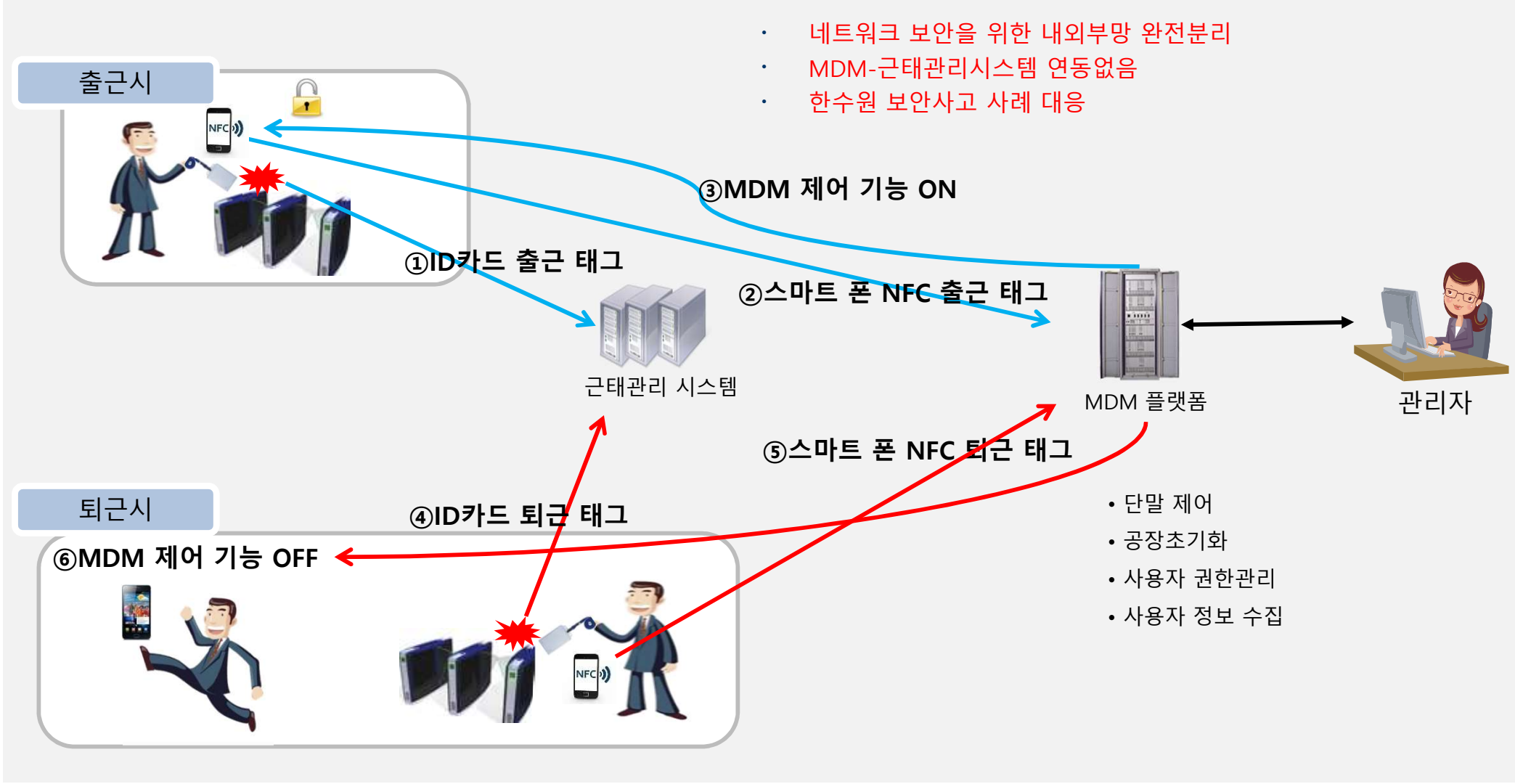
구분	지원 사양	
MDM Application Server	운영체제	Linux(Fedora)
	CPU	Xeon CPU x 2
	Memory	6G byte 이상
MDM Database Server	권장 RDBMS	My SQL(Oracle, MS-SQL 지원 가능)
	운영체제	Linux(지원 RDBMS 에 따른 운영체제)
	CPU	Xeon CPU x 2
	Memory	6G byte 이상

5. 출입통제 연계 적용방안

5.1 출입통제 MDM 솔루션 시나리오

MDM 서비스 시나리오

- 고객사 출입통제 시스템과 연계한 방식으로 운용
- ID 카드와 스마트 기기를 각각 출입 게이트에서 Tagging 방식으로 운영



5.2 출입통제 연계 MDM 공급 Reference(OO사이트)

서비스 제공 방식

- NFC 태그를 이용한 강제 보안 설정기능으로 보안존 제어(2014. 6)
- MDM 보안 존 운영 메커니즘 : NFC 태그를 이용하여 pkg, flag 값을 비교하여 운영체제가 앱을 호출하여 강제 보안 설정수행

MDM 작동 흐름

동작 Logic

NFC tag 처리동작

가) 보안존 밖에서 NFC태그를 이용하여 MDM 앱이 활성화되는 경우

→ 보안존 IN 상태로 전환한다.

(MDM 서버에서는 일반적인 보안존 진입 상태와 동일하게 판단한다.)

나) 보안존 밖에서 NFC 태그를 이용하여 보안존 IN 모드로 변경된 상태에서 다시 NFC 태그를 이용하여 앱이 활성화되는 경우

→ 보안존 OUT 모드로 변경한다.

(MDM 서버에서는 일반적인 보안존 이탈 상태와 동일하게 판단한다.)

MDM 동작

- NFC 에서 안드로이드 운영체제로 MDM 실행신호 수신
- 운영체제에서 MDM 앱 활성화
- Intent pkg, flag 값을 통한 상태변경 명령
- 상태변경 후 관리정책에 의한 MDM 운영

* NFC를 통한 제어는 안드로이드 운영체제에서만 가능합니다.

별첨

"Why NEXDIGM MDM?"

넥스다임은 지난 10여 년간 kt 및 공공부문의 모바일, 단말 제어형 서비스를 직접 구축, 운영하는 경험을 통해

스마트 기기 기반 모바일 서비스에 대한 문제들을 이해하고 해결하는 노하우가 있습니다.

1. 국가정보원 MDM 보안기준 충족

- 모바일 전자정부 보안 가이드라인 충족(행정안전부)
- 국가보안기술 연구소 보안 가이드라인 기준 충족
- 경찰청 등 고급 정보 보안 요구사항 충족(EL 4)
- 국내 다수 공공기관 상용적용 레퍼런스

2. End to End security

- WAP push(SMS) 서비스 방식이 아닌 E2E 서비스
- Android Push Notification(C2DM) 서비스 방식이 아닌 E2E 서비스
- 제 3자 경유 방식이 아닌 보안 무결성 보장

3. 기본적 단말제어 기능 완벽 구현, 구동

- 완벽하고 실효성 있는 하드웨어 제어기능
- 독자 알고리즘에 의한 Rooting 및 Jail-breaking 탐지
- USB, SD card, GPS 제어 완벽 구현
- Wifi, 카메라, Bluetooth 제어
- 백신 결합 서비스 (Background 연동)

4. 특화 및 맞춤 서비스 기능

- MDM 사용자에 의한 임의 종료 제어 기능으로 완벽한 기기통제
- 소프트웨어 Inventory 관리 (Application 설치/삭제)
- 출입연동 제어(접촉식 RF tag, 위치기반 제어)

Why NEXDIGM MDM?

Project Experience – Mobile Device Management

Unique & best ! 국내 최초 상용화, 최다 공공부문 사이트, 검증된 MDM solution provider!

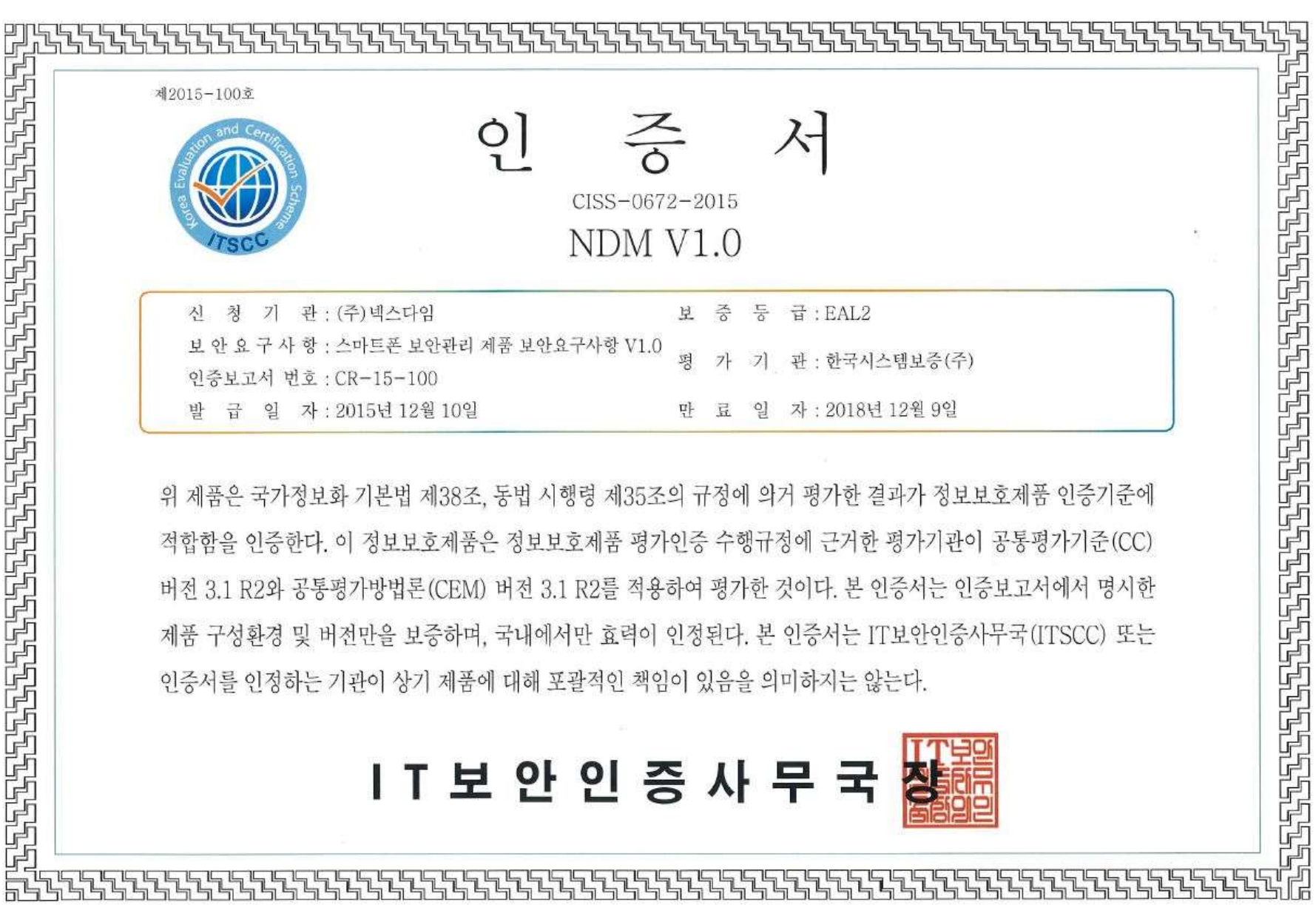
국내 최대(2만대 이상)의 스마트 기기가 핵심 보안 요구 공공기관 및 기업에서 넥스다임 MDM을 사용하고 있습니다.

발주처	운영체제	구축완료	비고
Bizmeka Mobile office	iOS, Android	2010. 6	중소기업형 ASP, MS Exchange 변경
케이티	iOS, Android	2010. 8	MS Exchange 서비스 변경
행정안전부	iOS, Android	2010. 11	시범사업 종료
방송통신위원회	iOS, Android	2010. 11	
포스코건설, 신한금융지주, 한화그룹, GS건설, 대림산업, 보라매병원	iOS, Android	2010	MS Exchange 서비스 변경
경찰청	Android	2011 ~ 2018	보안적합성 인증완료
대한지적공사	iOS, Android	2011. 6	
인천국제공항공사(IIAC)	iOS, Android	2011. 8	
한국 농어촌 공사	iOS, Android	2011. 10	
성모병원, 하이닉스, 부산교육대학	iOS, Android	2011	서비스 종료
청와대	iOS, Android	2012. 6	
충청남도 소방안전본부	Android	2012 ~ 2018	보안적합성 인증완료
OO 사이트	Android	2014 ~ 2015	Cell ID 기반

MDM	ISP, 구축, 보안 컨설팅

IT 보안인증사무국 스마트폰 보안관리 제품 보안요구사항 준수

NDM V.1.0 – 공통평가기준(Common Criteria) 인증서



제2015-100호

인 증 서

CISS-0672-2015

NDM V1.0

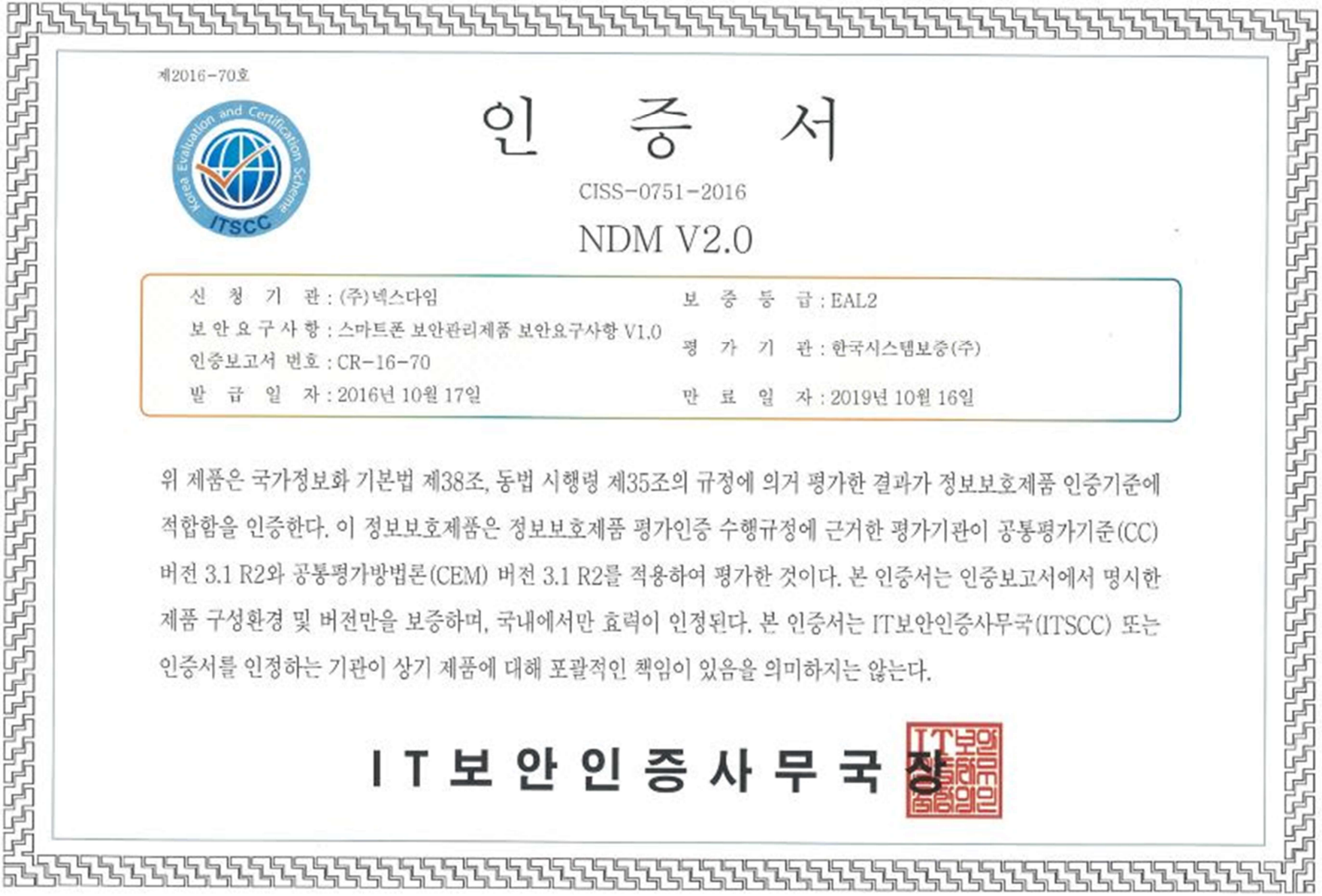
신 청 기 관 : (주)넥스다임	보 증 등 급 : EAL2
보 안 요 구 사 항 : 스마트폰 보안관리 제품 보안요구사항 V1.0	평 가 기 관 : 한국시스템보증(주)
인증보고서 번호 : CR-15-100	
발 급 일 자 : 2015년 12월 10일	만 료 일 자 : 2018년 12월 9일

위 제품은 국가정보화 기본법 제38조, 동법 시행령 제35조의 규정에 의거 평가한 결과가 정보보호제품 인증기준에 적합함을 인증한다. 이 정보보호제품은 정보보호제품 평가인증 수행규정에 근거한 평가기관이 공통평가기준(CC) 버전 3.1 R2와 공통평가방법론(CEM) 버전 3.1 R2를 적용하여 평가한 것이다. 본 인증서는 인증보고서에서 명시한 제품 구성환경 및 버전만을 보증하며, 국내에서만 효력이 인정된다. 본 인증서는 IT보안인증사무국(ITSCC) 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

IT보안인증사무국장

IT 보안인증사무국 스마트폰 보안관리 제품 보안요구사항 준수

NDM V.2.0 – 공통평가기준(Common Criteria) 인증서



제2016-70호

인 증 서

CISS-0751-2016

NDM V2.0

신 청 기 관 : (주)넥스다임	보 증 등 급 : EAL2
보 안 요 구 사 항 : 스마트폰 보안관리제품 보안요구사항 V1.0	평 가 기 관 : 한국시스템보증(주)
인증보고서 번호 : CR-16-70	
발 급 일 자 : 2016년 10월 17일	만 료 일 자 : 2019년 10월 16일

위 제품은 국가정보화 기본법 제38조, 동법 시행령 제35조의 규정에 의거 평가한 결과가 정보보호제품 인증기준에 적합함을 인증한다. 이 정보보호제품은 정보보호제품 평가인증 수행규정에 근거한 평가기관이 공통평가기준(CC) 버전 3.1 R2와 공통평가방법론(CEM) 버전 3.1 R2를 적용하여 평가한 것이다. 본 인증서는 인증보고서에서 명시한 제품 구성환경 및 버전만을 보증하며, 국내에서만 효력이 인정된다. 본 인증서는 IT보안인증사무국(ITSCC) 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

IT보안인증사무국장

Thank you for attention

주식회사 넥스다임

경기도 안양시 동안구 학의로 268, 메가밸리 310

TEL 031-420-4766/ FAX 031-420-4765

E-MAIL. stararoa@nexdigm.co.kr

URL. www.nexdigm.co.kr