5강 iOS MDM 동작 방식

개요 및 목표

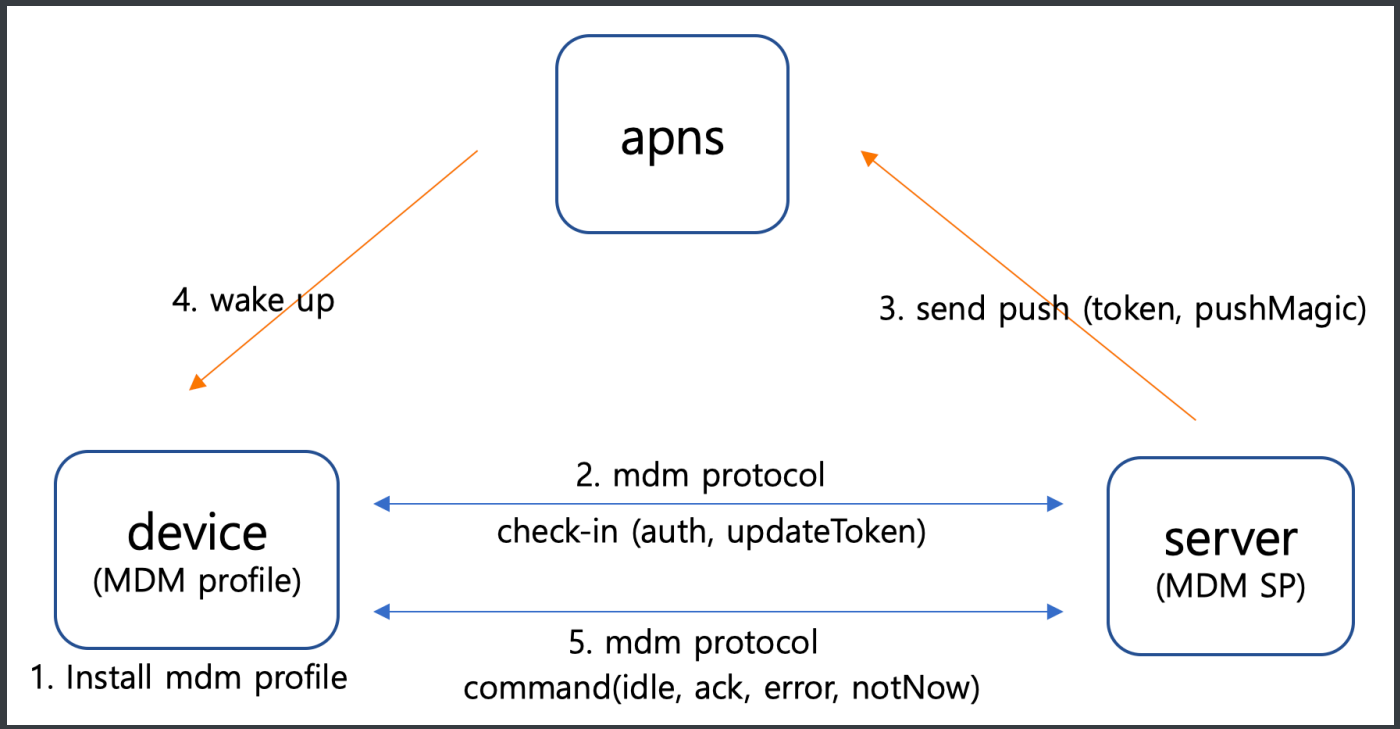
이번 강의에서는 MDM(Mobile Device Management) 동작방식을 이해하는것을 목표로 합니다.

MDM서버(SP)로부터 iOS 디바이스가 어떠한 원리로 관리를 받는지 알아보겠습니다.

이 기능의 핵심 또한 인증서와 프로파일 입니다.

MDM 푸시 인증서 및 MDM profile 생성과정을 살펴보고 원가드 제품을 MDM protocol 을 참고하여 설명드리겠습니다.

MDM 서비스 구성



MDM Push 인증서 생성 (이론 상 고객사와 벤더 양쪽에서 인증서 생성에 관여 함)

다른 문서로 단계 별로 설명

- Customer(고객사)
  1. 고객사의 개인정보로 csr 생성 (키쌍 생성)
  2. customer.csr -> customer.der로 변경 (mdm push plist 생성의 재료)
  3. vender(라온)로 der 전달 (고객사의 개인정보 및 서명 +공개키)

     -- vender 절차
  4. 고객사는 MDM Push 인증서를 생성하기 위해 apple enterprise 계정에 가입해야 한다.
  5. 고객사의 Enterprise계정 apple.com/iphone/business/integration/mdm/ 접속
  6. 최종적으로 받은 라온의 plist 파일을 업로드 하여 푸시 인증서를 다운로드 받고 키체인을 이용해 패스워드와 함께 sp 서버로 .p12파일을 전달한다.
  7. sp 서버에서는 .p12 와 패스워드로 MDM push를 보낸다. 누구에게??
     - Mdm 푸시 인증서에는 고객사의 id(apsp)가 있다.
     - 해당 id를 기준으로 고객사별 MDM profile을 생성하고 기기에 설치 한다.

- Vender(라온)
  4. 라온의 개인정보로 csr 생성 (키쌍 생성)
  5. 라온 엔터프라이즈 계정에서 csr 첨부하여 MDM.cer 파일 생성 및 다운로드 (키체인 저장)
  6. 키체인에서 내보내기 하여 .p12로 패스워드 설정
  7. apple ROOT_CA 인증서, apple 중간자 CA인증서를 다운로드
  8. 고객사에서 받은 customer.der와, 라온에서 생성한 mdm.p12를 이용하여 push 인증서를 생성하기 위한 encoded_plist를 생성한다.
     - 아래 참조 문서
     - 고객사의 der을 라온의 mdm 인증서 개인키로 서명문을 만든다
     - encoded_plist = sign(라온 개인키, customer원본) + customer원본 + ca 정보

MDM Profile 생성

다른 문서로 단계 별로 설명

- 고객사 마다 다른 MDM 푸시 인증서를 사용하고 있음
- MDM 푸시 인증서 및 apple ca 인증서를 재료로 MDM Profile을 생성한다.
- MDM 푸시인증서의 개인키로 MDM Profile을 서명 후 설치

MDM Protocol

원가드 제품을 예시로 단계 별로 설명

- check-in (프로파일 최초 설치시 프로토콜)
  - Authenticate message

MsgType	Topic	UDID
Authenticate	MDM 고객사 구분값 (A)	디바이스 구분값(B)

OS	BuildVer	ProdctNm	SerialNum	Imei	Meid
13.0	4.0.0.1	MDM	xxxx	xxx	Xxx

  - Token update message

MsgType	Topic	UDID	Token	PushMagic	UnlockToken
Authenticate	A	B	C	D	E

  - 배포된 앱 시작시 서버에서 설정한 고유값을 이용해서 앱 로그인 시 위 정보와 매핑한다. (https://developer.apple.com/library/archive/samplecode/sc2279/Introduction/Intro.html)

SerialNumber	UserId	UserPW
Xxxxx	djpark	1234

- check-out (프로파일 삭제 시 프로토콜)

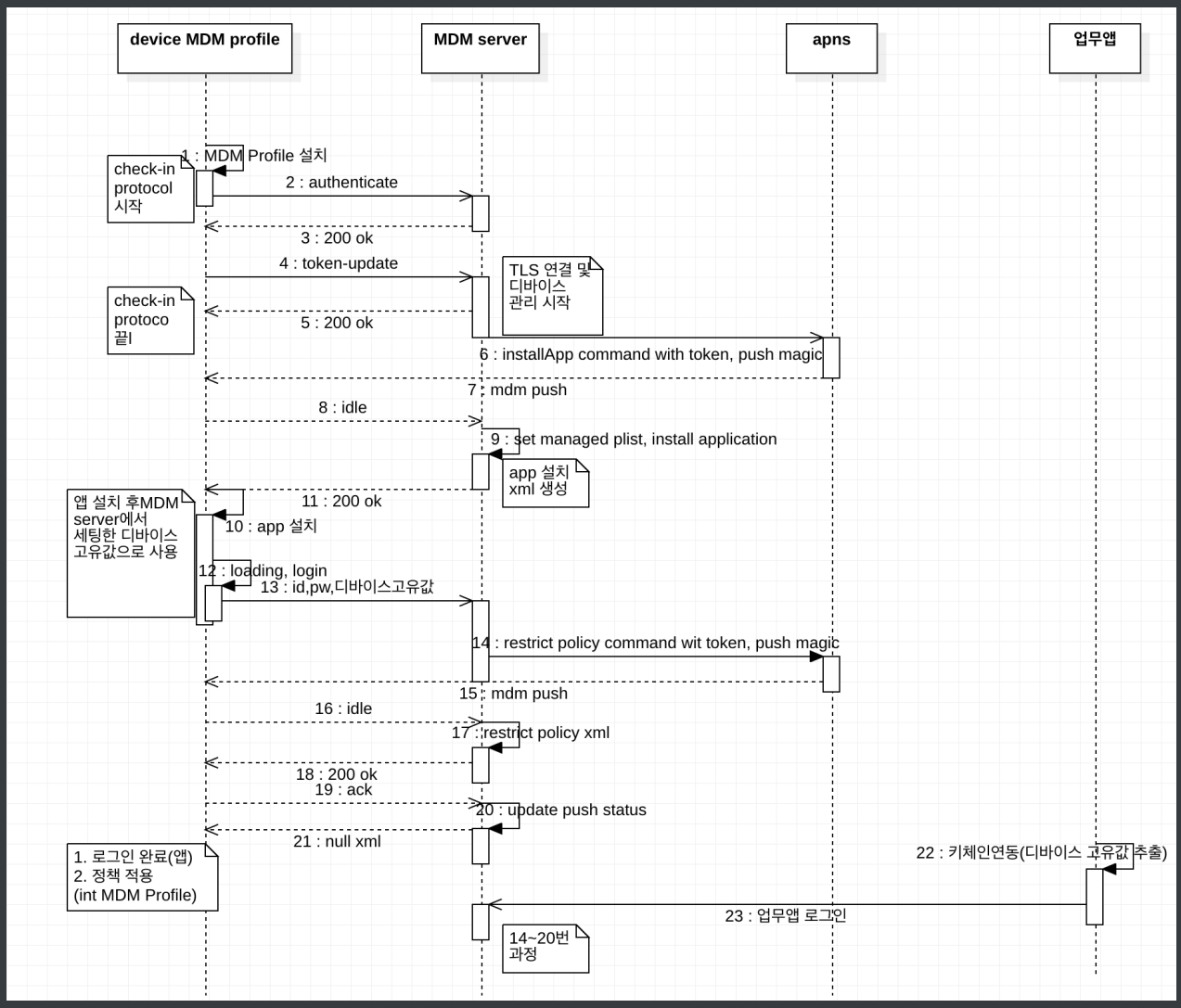
MsgType	Topic	UDID
	A	B

    - 프로파일 삭제 시 배포한 앱 모두 삭제 옵션
- command (모바일 디비이스 관리 프로토콜) / request type별

  아래 명령을 수행시 아래 table과 같이 명령에 대한 이력을 관리 해야 함 (idle/ ack/ error/ notnow 상태 존재)

commandUUID	command	status	result	date
Xxxx-xxxx-xxxx-xxxx	Apps	1	1	20211031..

    - DeviceInfomation (디바이스 정보조회)
    - InstalledApplicationList (설치된 앱 리스트 조회) - 원가드 -> 업무앱 관리
    - InstallApplication (앱 설치) 원가드, 업무앱
    - RemoveApplication (앱 삭제)
    - InstallProfile (제한정책) 카메라 화면 캡쳐, ...
    - RemoveProfile (정책해제)
    - DeviceLock (화면잠금)
    - EraseDevice (공장초기화)
    - ClearPasscode (사용자 패스코드 초기화)



참조

- 애플 기기 MDM 개요
  - https://support.apple.com/ko-kr/guide/mdm/mdmbf9e668/web
- MDM Server java 기반
  - https://github.com/zuoyy/IOS-MDM-Server/tree/master/src/com/zuoyy
- encoded_plist 생성 java 기반
  - https://developer.apple.com/documentation/devicemanagement/implementing_device_management/setting_up_push_notifications_for_your_mdm_customers
- encoded_plist 생성 python 기반
  - https://github.com/grinich/mdmvendorsign/blob/f3565f5191e2a2d3a19b41589986bb5fba9fb555/mdm_vendor_sign.py
- apple mdm protocol 문서
  - https://developer.apple.com/business/documentation/MDM-Protocol-Reference.pd

f

- apple mdm configuration profile 문서(제한정책 payload 포함)
  - https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf