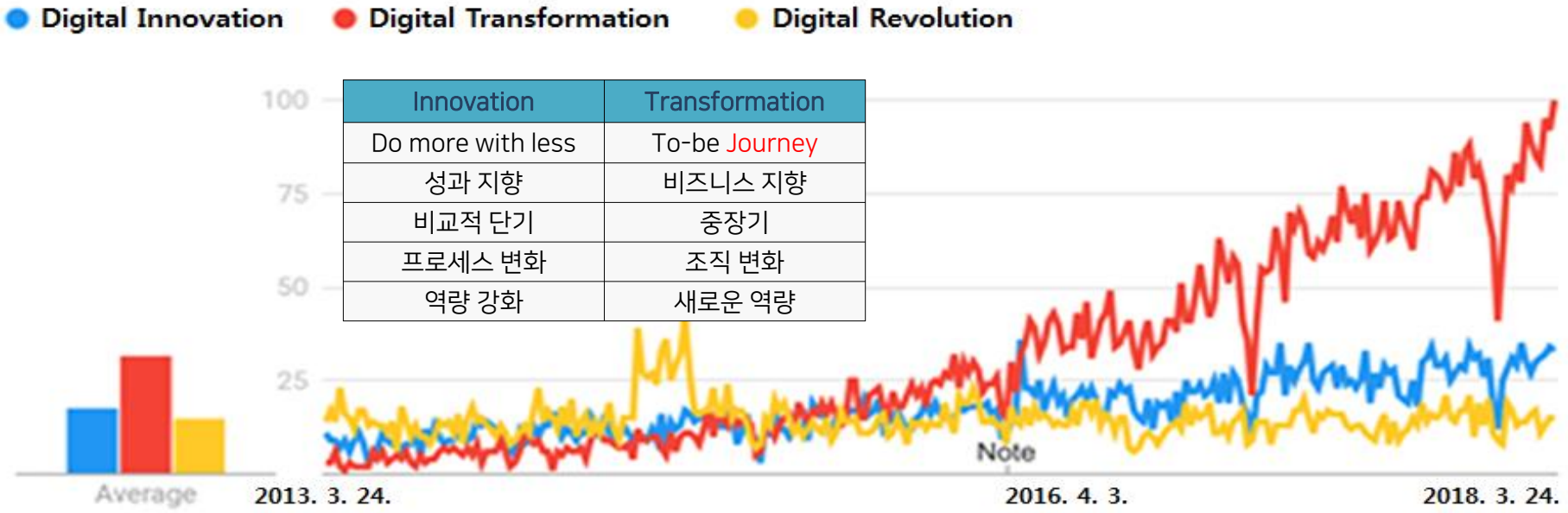
금융권 Open API 활용

Open API 소개

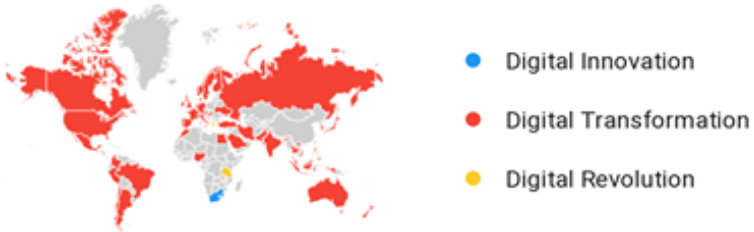
1.1 Google Trends : Digital Transformation

Digital Transformation(변환,탈바꿈)은 모바일과 사물인터넷 기반의 디지털 중심의 기업 혁신 '현상'을 의미. Digital Twin - '현실에 필요한 환경을, 디지털을 통해 현실로 이동/복제'하는 것을 의미.



Innovation	Transformation
Do more with less	To-be Journey
성과 지향	비즈니스 지향
비교적 단기	중장기
프로세스 변화	조직 변화
역량 강화	새로운 역량

지역별 관심도



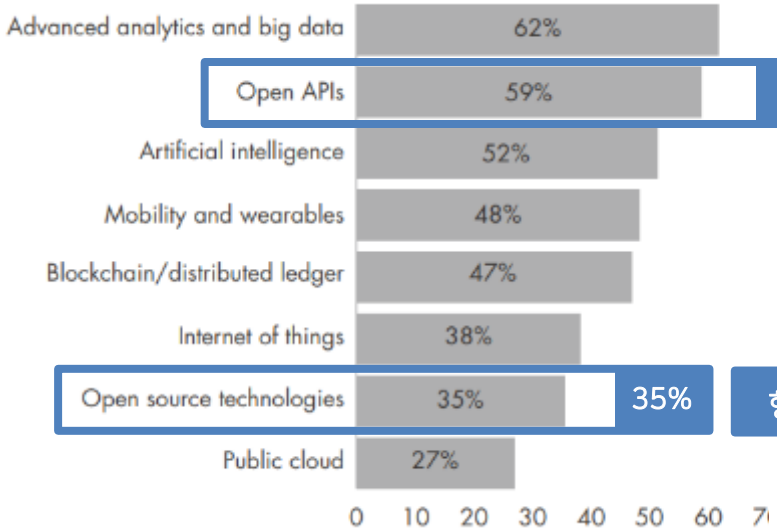
연관 검색어

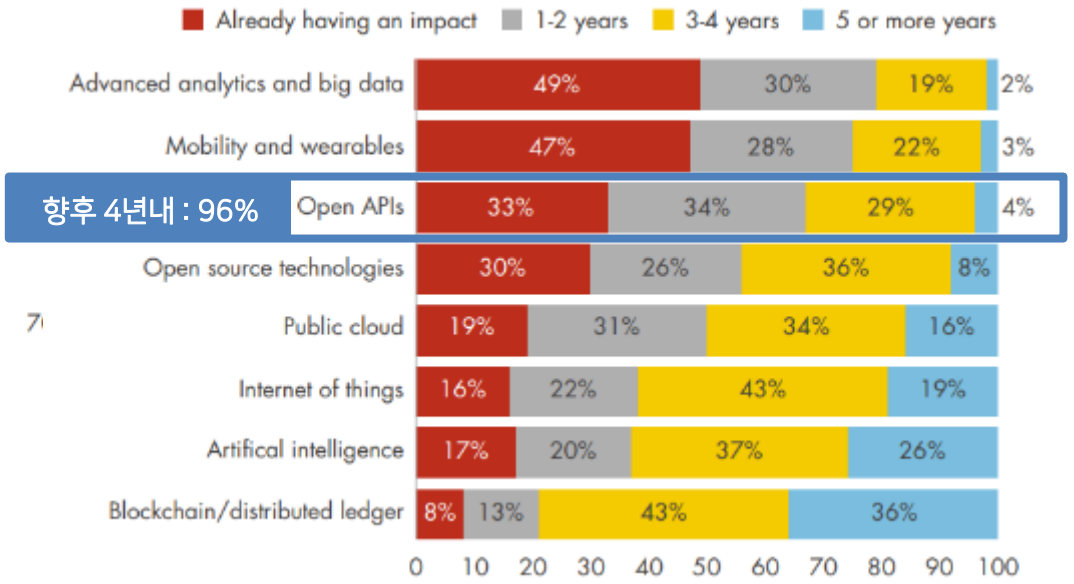
1	the digital transformation	100
2	digital business	69
3	business digital transformation	69
4	business transformation	68

1.2 금융권 비즈니스 모델의 DX 기술 및 투자

금융 서비스 사업 모델을 가진 기업들에게 비즈니스 모델에 영향을 줄 혁신 기술로서 Open API가 2번째 중요한 기술로 뽑혔고, 해당 혁신 기술들에 대한 투자도 실행하고 있는 것으로 조사됨.

그림 14 : 은행 비지니스모델에 대한 파괴적인 기술의 영향도
Figure 14 : Impact of disruptive technologies on banking business models





<출처: Efma-Infosys Finacle Innovation Survey, 2016.>

그림 15 : 파괴적인 기술의 영향을 미치는 기간
Figure 15: Time period for the impact of disruptive technologies

1.3 금융권의 Open API 를 도입하는 이유

선도적인 금융회사들이 Open API 를 도입하는 이유에 대해 살펴보면, 디지털 경험, 프로세스 최적화, 고객 기반 공유, 상품 확대, 규제 대응 등의 관점에서 나누어 살펴볼 수 있음.

- 운영 프로세스 개선 및 혁신
- 프로세스 자동화 및 최적화
- Regtech, AaaS 등

프로세스 최적화

- 디지털 고객 비중 확대 대응
- 디지털 기술 도입 및 적용
- 핀테크회사와 서비스 제휴

디지털 경험

- 고객 레버리지 확대
- 상품 기획 및 혁신 역량 강화
- 디지털 상품 및 서비스 회사

상품 확대

- 디지털 경제에 맞는 고객 유입
- 고객 분석 역량 강화
- 유통, 통신 등 회사 협업

고객 기반 공유

- 오픈 뱅킹 제도화 대응
- Personal Data 대응
- 데이터 사회적 책임 수행

규제 대응

<출처: 2e투이컨설팅 제97회 Y세미나 "금융회사, 오픈API로 연결하고, 혁신하라!">

1.4 금융권의 은행 10 대 트렌드

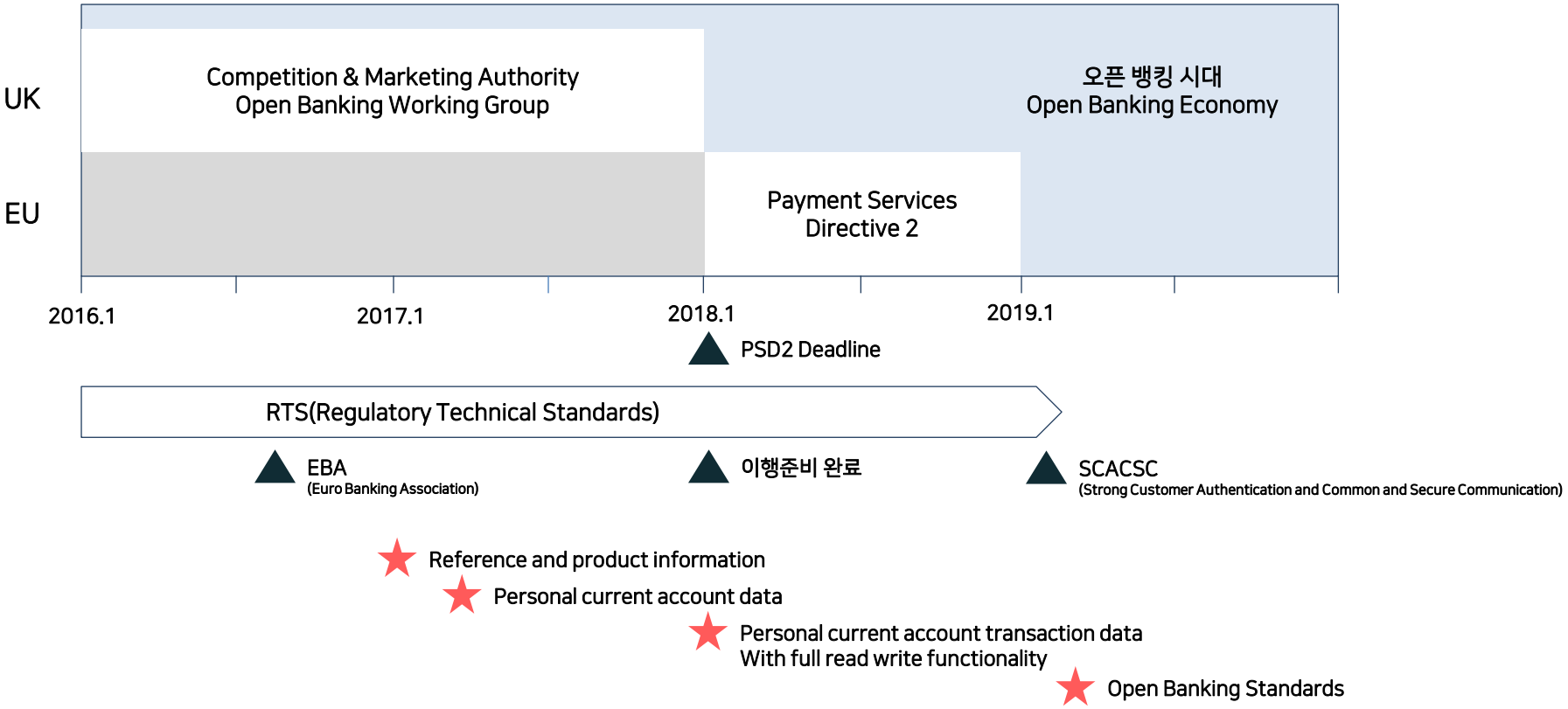
Capgemini에서 보고한 2017년 은행 10대 트랜드를 살펴보면, 1) 핀테크 기업은 파트너, 2) 디지털자산과 데이터를 Open API로 공개, 3) 핀테크 회사들을 위한 플랫폼 등이 있음.

1	핀테크 기업은 경쟁자가 아니라 파트너가 되고 있다.
2	은행은 디지털자산과 데이터로 수익을 창출하기 위하여 Open APIs를 사용하고 있다.
3	은행 비즈니스 모델은 많은 핀테크 회사들을 위한 플랫폼으로 변화하고 있다.
4	은행은 증가하는 사이버 위협에 대응하기 위해 사이버 보안시스템에 투자하고 있다.
5	유연성과 기민성을 제공하기 때문에, 은행들은 퍼블릭 클라우드 이용을 늘리고 있다.
6	은행은 고객 경험을 강화하기 위해 증강 현실을 테스트하고 있다.
7	은행은 분산 원장 기술의 Use Case를 찾아내고 이해하기 위해 공동작업을 하고 있다.
8	은행은 경쟁 수단으로 Cognitive Banking을 모색하고 있다.
9	은행은 Robotic Process Automation에 투자하여 효율성과 생산성을 향상시키고자 한다.
10	은행은 인증 위협과 부정 사용에 대응하기 위해 생체 인증을 사용하고 있다.

<출처: 2e투이컨설팅 제97회 Y세미나 "금융회사, 오픈API로 연결하고, 혁신하라!">

1.5 오픈 뱅킹 규제 변화

2018년 1월부터 유럽 전역에 도입된 PSD2는 고객이 인증하면 은행이 해당 고객 정보를 첨단기술업체에 제공하는 제도로서, 페이스북, 아마존, 알리바바까지 결제서비스 사업에 뛰어들고 있음.



*) PSD2 : the second Payment Services Directive

How banks can create value from the rise of the open API economy in financial service-CGI

<출처: 2e투이컨설팅 제97회 Y세미나 "금융회사, 오픈API로 연결하고, 혁신하라!">

1.6 오픈 뱅킹 모델

Open API를 활용한 오픈 뱅킹 모델은 ① 은행 자체 채널, ② 써드 파티 앱, ③ 외부 서비스와 융합, ④ 다수의 금융회사 데이터를 모아서 하나의 서비스로 제공, ⑤ 오픈 뱅킹 플랫폼 제공 등이 있음.

뱅크채널	앱 마켓	유통	융합	플랫폼
Open API를 은행의 자체 채널로 활용	은행 서비스를 Open API로 제공하여 써드파티가 새로운 앱 개발에 활용	Open API를 자신의 서비스를 외부에 제공하는 수단으로 활용 외부 서비스와 융합하여 제공	다수의 금융회사 데이터를 수집하여 하나의 Open API로 제공	오픈 뱅킹 플랫폼을 API 서비스로 제공
• 신속한 개발 • 개선된 사용자 경험	• 금융 생태계 구축 • 새로운 서비스 • 사용자 경험 혁신	• 파트너와 제휴로 최고 상품 제공	• 고객 중심 서비스 • 단일 인터페이스	• 비용 효율성 • 디지털 대응능력 • 상품 개발 능력
전통적 비즈니스	API 사용 수익	비즈니스 수익 공유	서비스 사용료	라이센스
대부분의 현재 금융회사	• BBVA • Credit Agricole • Capital One • NH농협은행 • 대신증권	• N26 • TrasferWise	• FIGO • Yodlee • XiGnite • PFM 회사	• FIDOR

<출처: 2e투이컨설팅 제97회 Y세미나 "금융회사, 오픈API로 연결하고, 혁신하라!">

Open API 플랫폼 소개

2.1 Open API를 통한 은행 Biz 확대

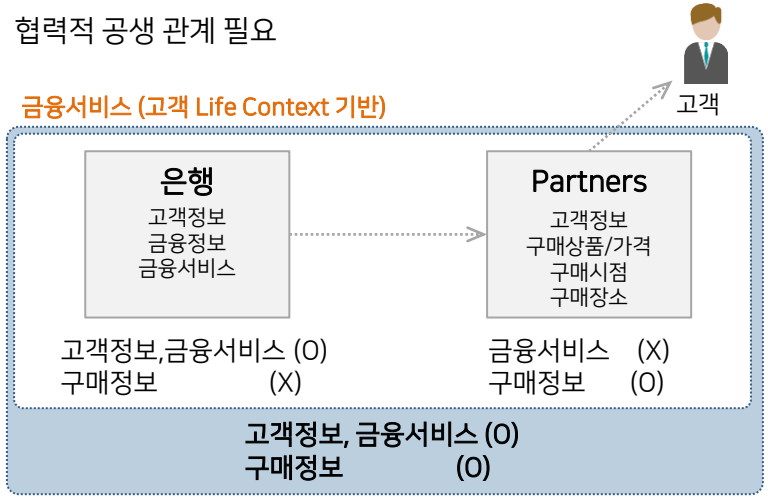
금융 회사의 수익성 악화로 신규 수익원 창출 필요성 증가. 금융 디지털 서비스 소비자들이 대거 등장함에 따라 3rd 파트너 업체와의 협력적 공생 관계가 필요. Open API기반의 오픈 뱅킹이 절실해짐.

금융산업 환경 악화에 따른 신규 수익원 창출 필요

- 금융회사의 수익성 악화(은행: 마진축소, 증권: 브로커리지 감소)로 신규 수익원 창출에 대한 필요성 증가
- 유망 IT기술이나 자원을 보유한 핀테크 기업에 대한 지분투자

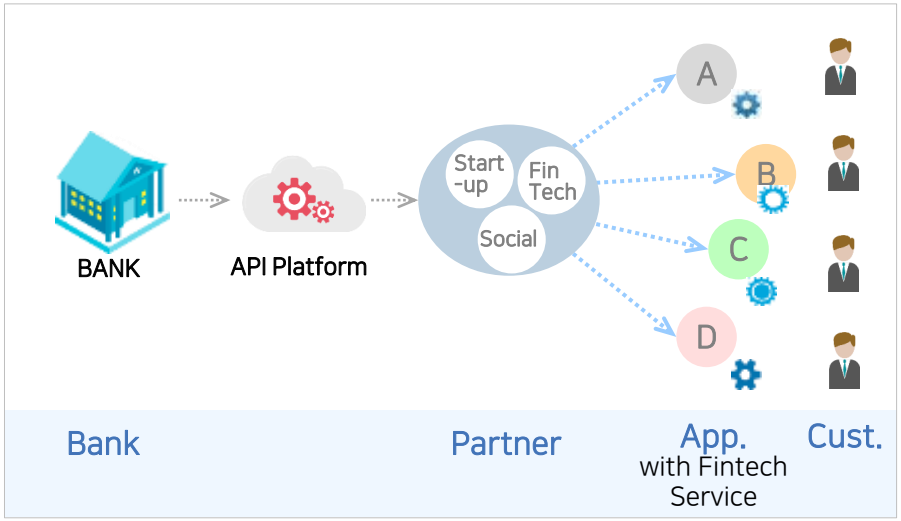
기술 진화에 따른 파트너사의 융합 시너지 필요

- 금융 디지털 서비스 소비자들의 대거 등장에 따른 파트너 업체와의 협력적 공생 관계 필요



정부의 정책적 지원

Open Banking Ecosystem



성공적인 Open Banking은,

은행-파트너를 긴밀히 연결하는 API Platform	API를 적용한 다양한 Application 서비스의 개발	고객 Context 기반의 편리하고 효율적인 금융서비스 제공

등을 보장하는 "Open Banking Ecosystem" 기반이어야 함.

2.2 국내 금융권 Open API 활용 Case

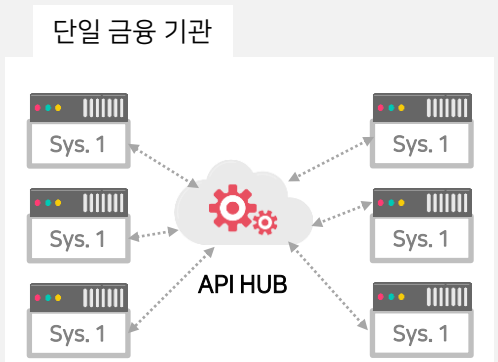
은행 내부 개발 프로세스 혁신 및 금융그룹 계열사간의 통합 시너지 확보 외 파트너를 통한 금융서비스의 무한 확대와 영업력 강화 목적으로 Open API 기반의 오픈 뱅킹 실현에 궁극적 목적이 있음.

Case 1

은행 내부 프로세스 혁신

시스템 연계 API HUB

- Private API
- 내부 시스템을 단일 API로 정의
- API 표준 전문 및 전문 관리
- API 기반 개발/테스트 환경 구축

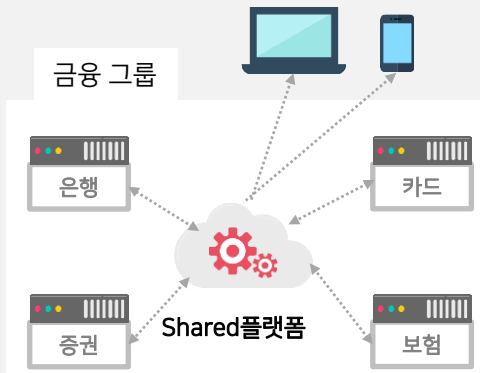


Case 2

MSA기반 통합 플랫폼

시스템 연계 API HUB

- Private / Public API
- API 중심 마이크로 서비스 개발
- 마이크로 서비스 플랫폼 개발

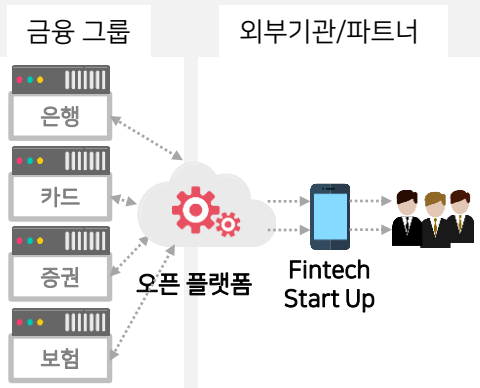


Case 3

오픈 뱅킹 플랫폼 구축

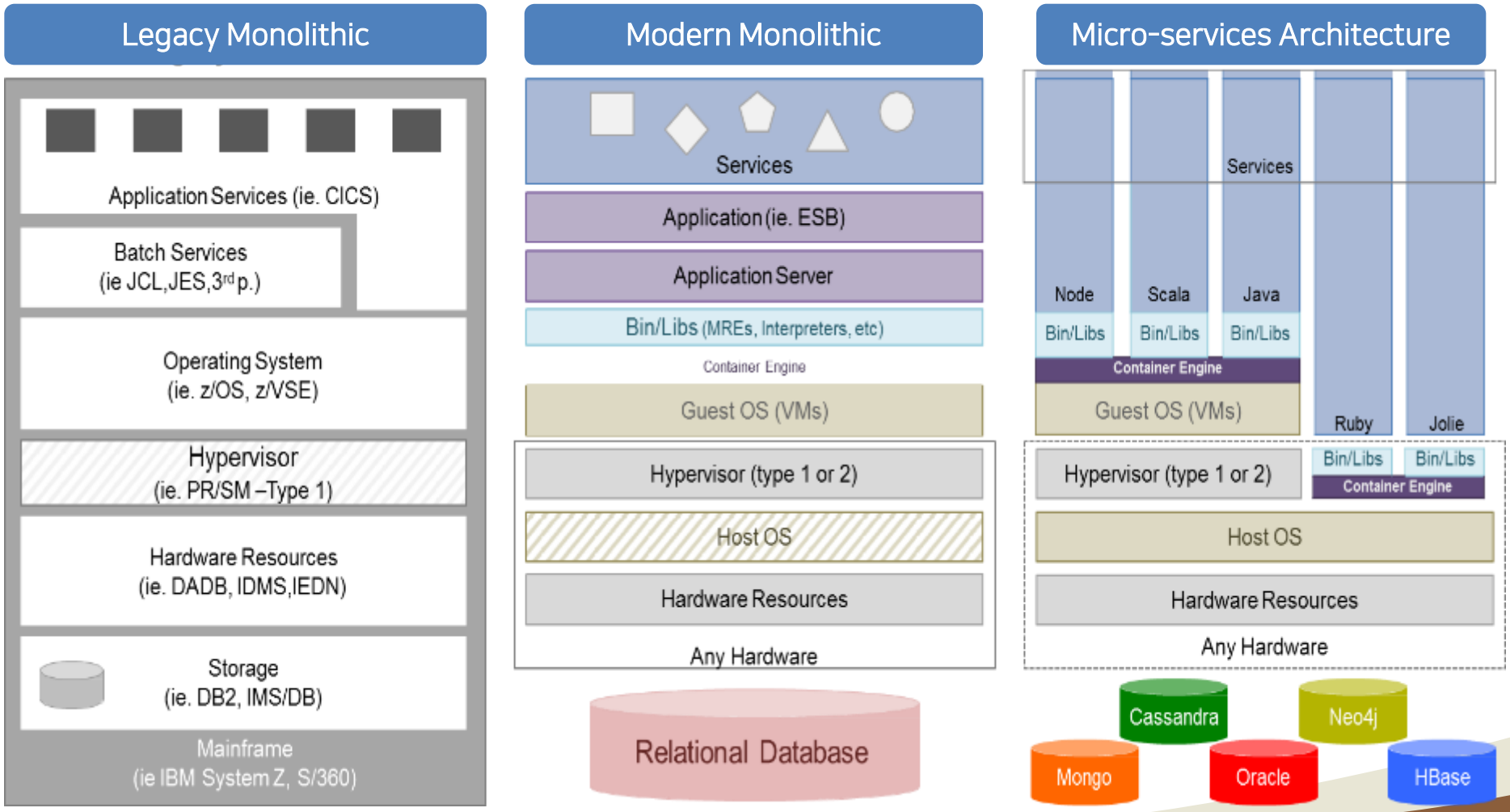
시스템 연계 API HUB

- Open API, Partner API
- 다양한 디지털 채널로의 확장
- 다양한 파트너 및 서비스 발굴
- 디지털 오픈 플랫폼 구축



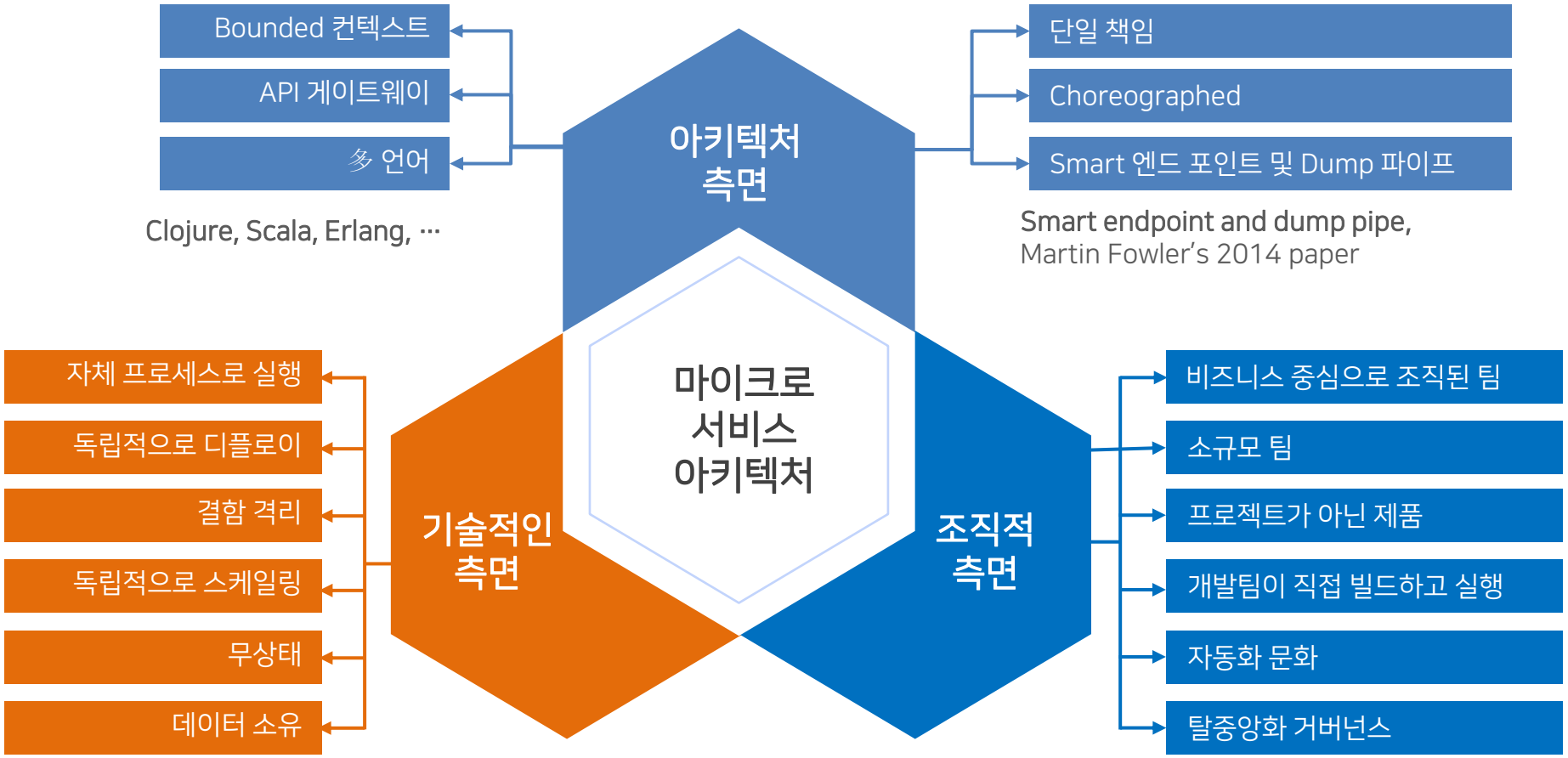
2.3 클라우드 네이티브 애플리케이션의 등장

Mainframe/TP-Monitor 등 레거시 모놀리식, J2EE/.NET 등 모던 모놀리식에서 Netflix와 같은 인터넷 기업의 Cloud Native Application을 구현하기 위한 마이크로 서비스 아키텍처가 등장함.



2.4 마이크로 서비스 아키텍처의 세 가지 측면

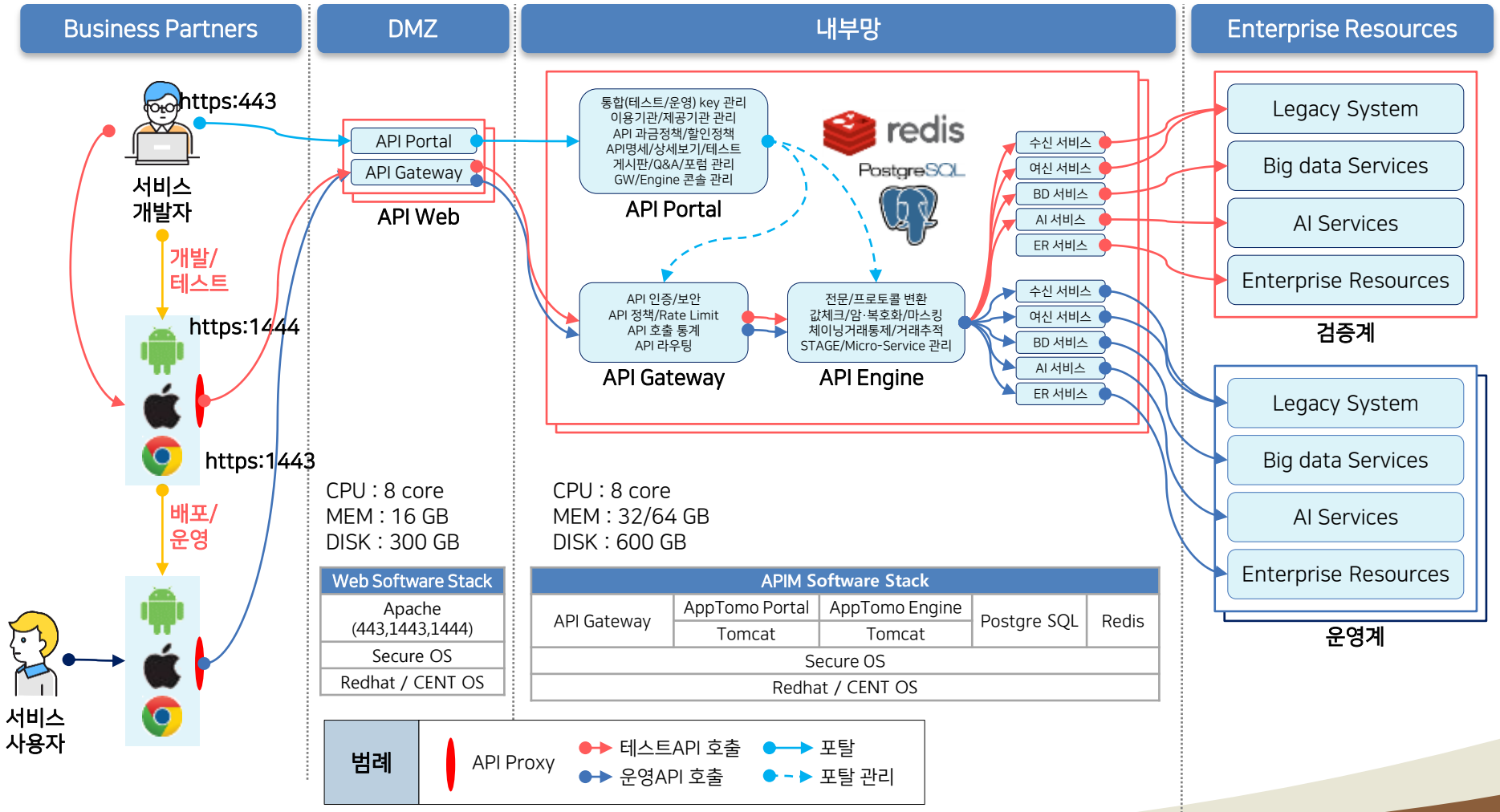
클라우드 네이티브 애플리케이션을 구현하기 위한 마이크로 서비스 아키텍처에 대해 아키텍처 측면, 기술적인 측면, 조직적 측면 등 3 가지 측면에서 살펴볼 수 있음.



<Source : Microservices and SOA | Oracle OpenWorld | San Francisco | September 18-22, 2016>

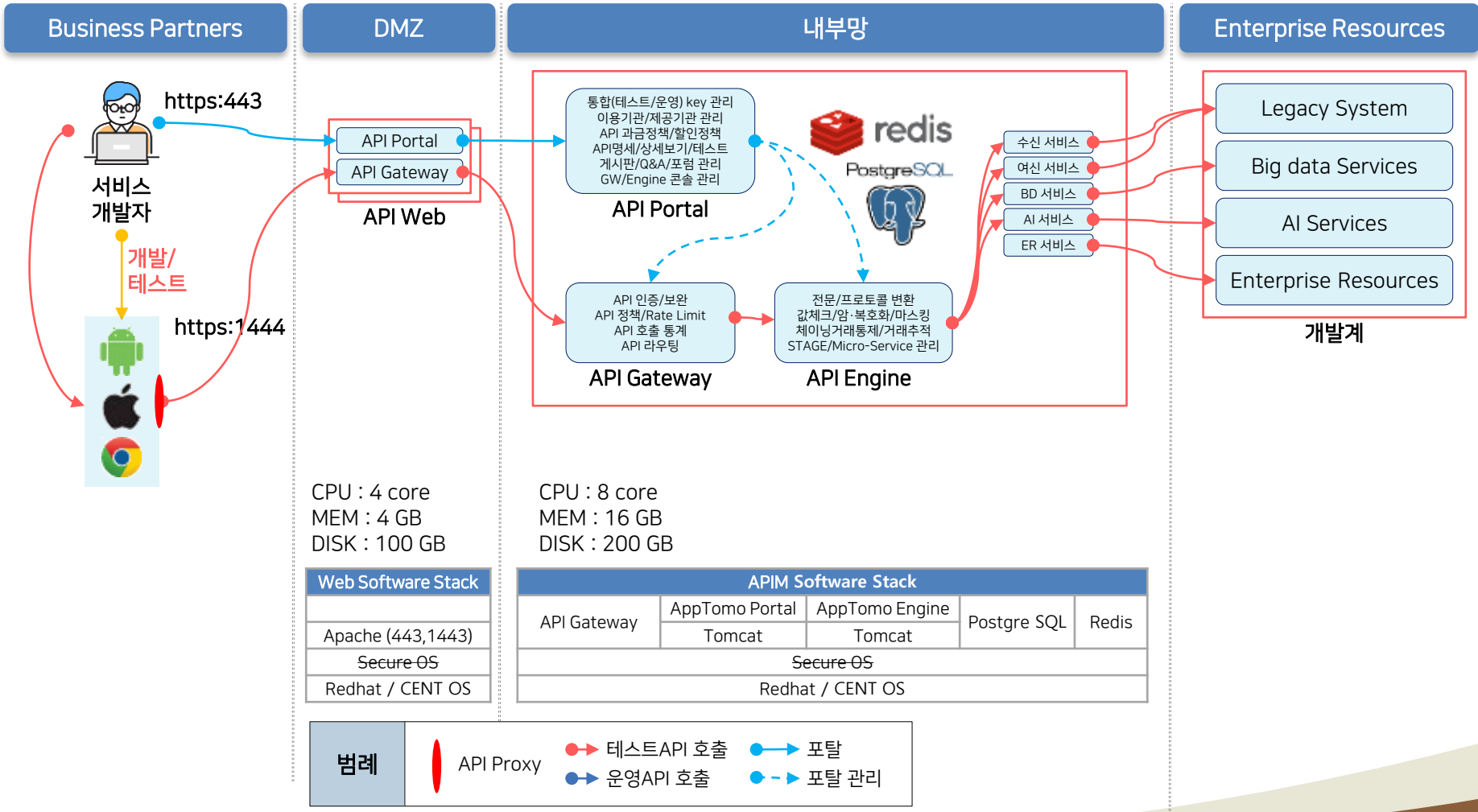
2.5 Open API 플랫폼 구성안 (운영·검증계)

유니버셜리얼타임에서 제안하는 Open API 플랫폼은 Web Server, APIM(Gateway, Portal, Engine, Postgre SQL, Redis) Server 등으로 구성되며, 각각의 서버는 운영계 이중화 2대, 검증계 1대임.



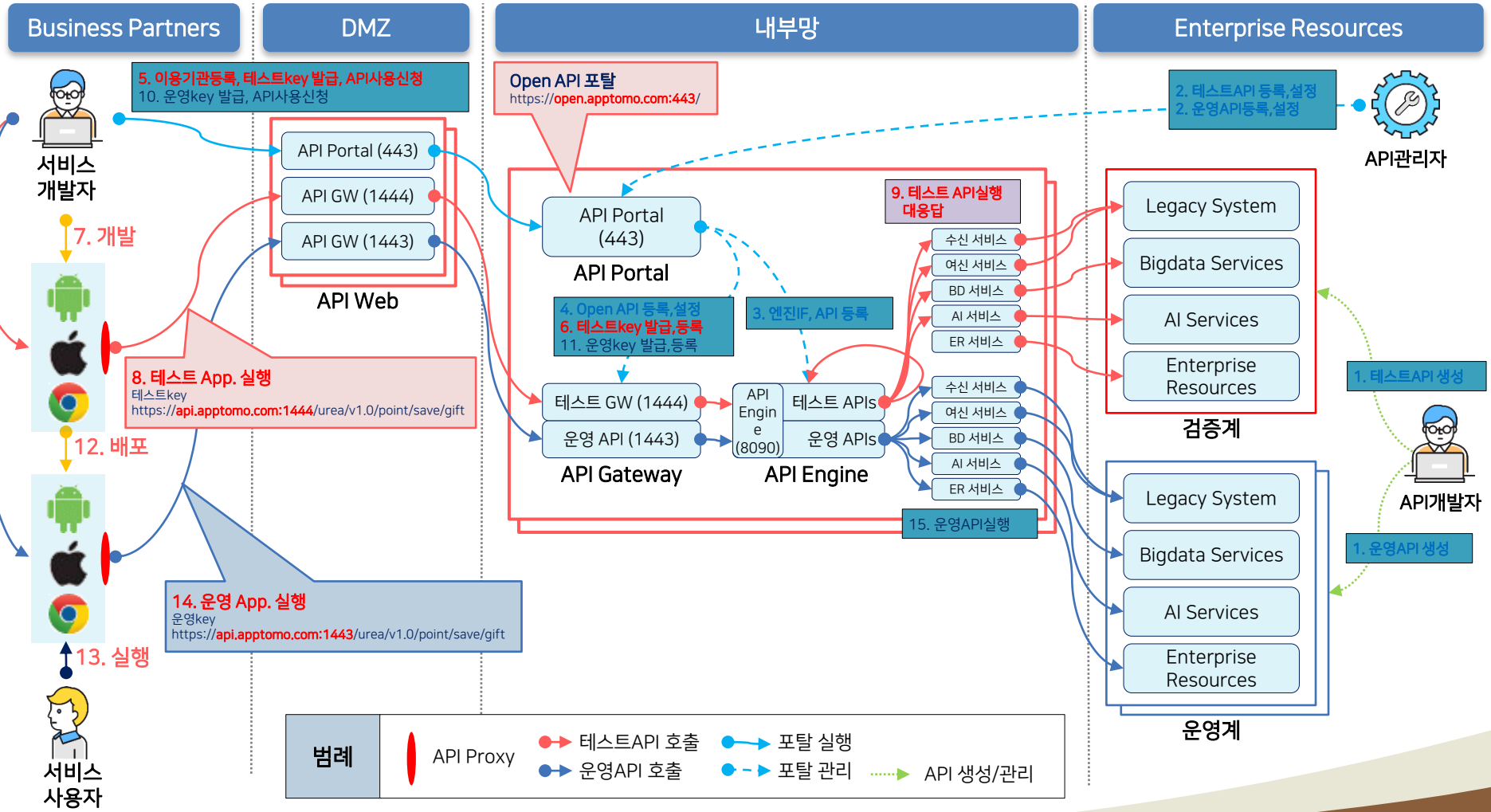
2.5 Open API 플랫폼 구성안 (개발계)

유니버셜리얼타임에서 제안하는 Open API 플랫폼은 Web Server, APIM(Gateway, Portal, Engine, Postgre SQL, Redis) Server 등으로 구성되며, 각각의 서버는 운영계 이중화 2대, 개발계 1대임.



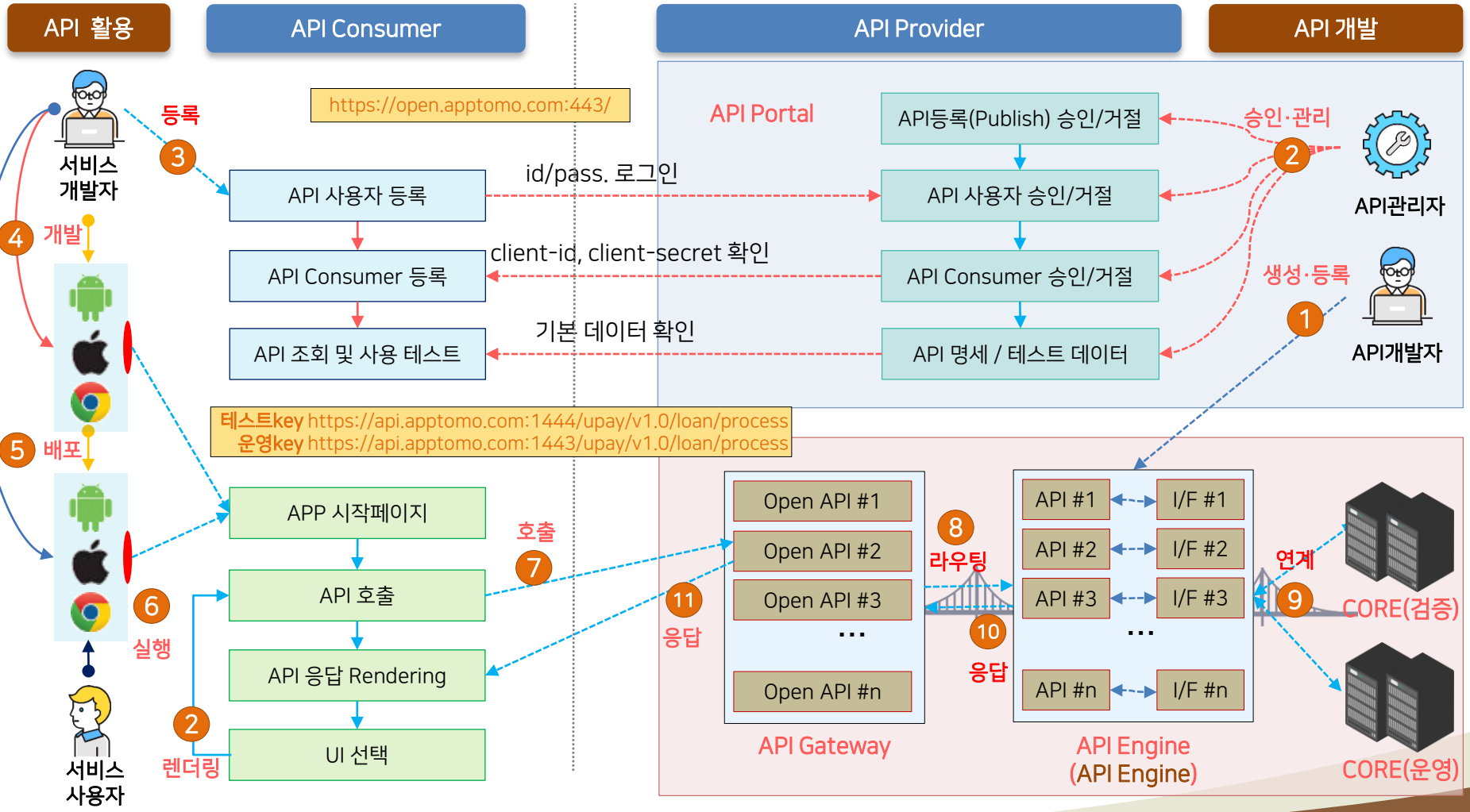
2.6 Open API 플랫폼 서비스 흐름도

Open API 라이프사이클을 살펴보면, ①②③④API 생성·등록·승인, ⑤⑥⑦⑧⑨테스트APP 등록·개발·테스트, ⑩⑪⑫운영APP 등록·배포, ⑬⑭⑮운영APP실행 및 Open API 실행 등의 서비스 흐름을 갖음.



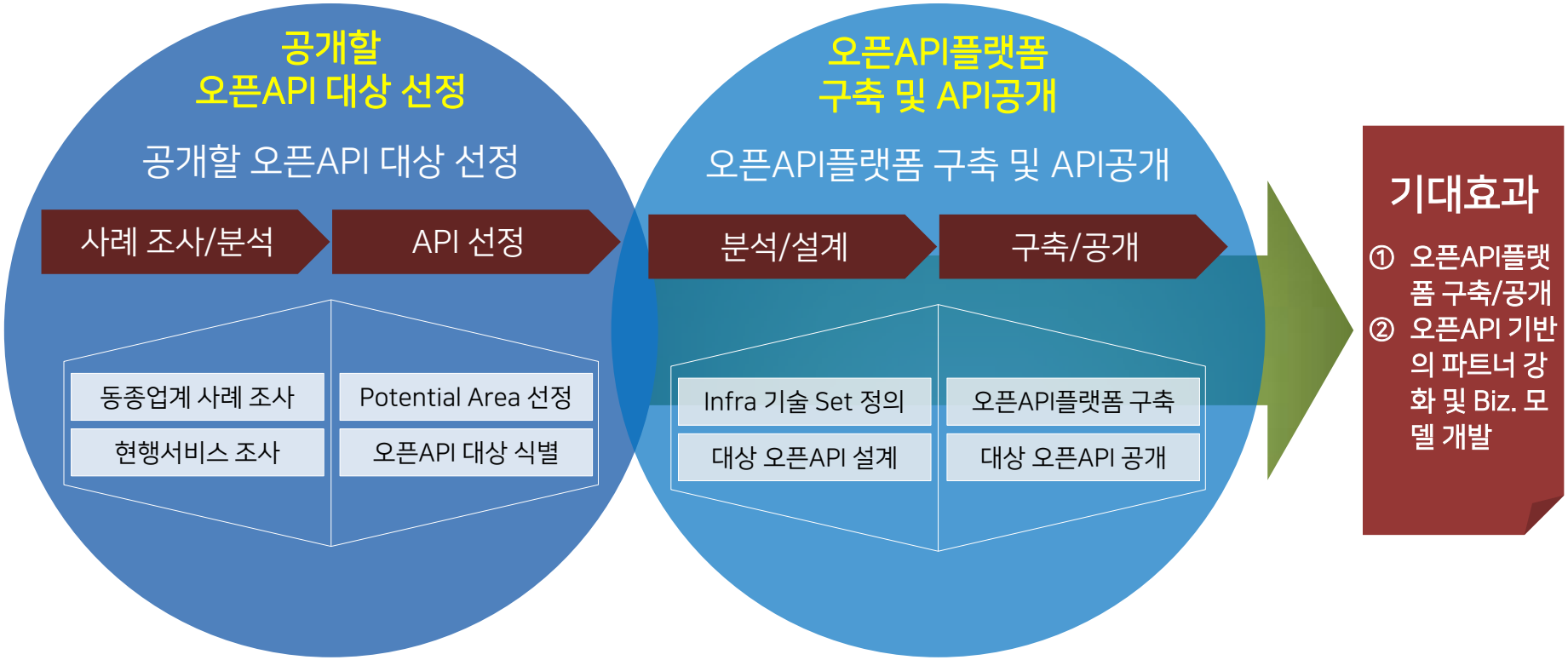
2.7 Open API 플랫폼 서비스 프로세스

Open API 플랫폼 서비스 프로세스를 살펴보면, ①②API 생성·등록·승인, ③④⑤API활용 APP 개발·배포, ⑥⑦APP실행·Open API 호출, ⑧⑨⑩⑪Open API 인증·라우팅·레거시 실행·전문 변환 리턴, ⑫Open API 응답 렌더링 등 구성.



2.8 Open API 플랫폼 구축 전략

주요 전략은 ① 공개할 Open API 도출, ② 대상 Open API 분석/설계, ③ Legacy 연동을 위한 아답터 개발, ④ API 포탈 커스터마이징 및 API 활용 서비스 등을 동시에 Parallel하게 개발·구축해야 함.

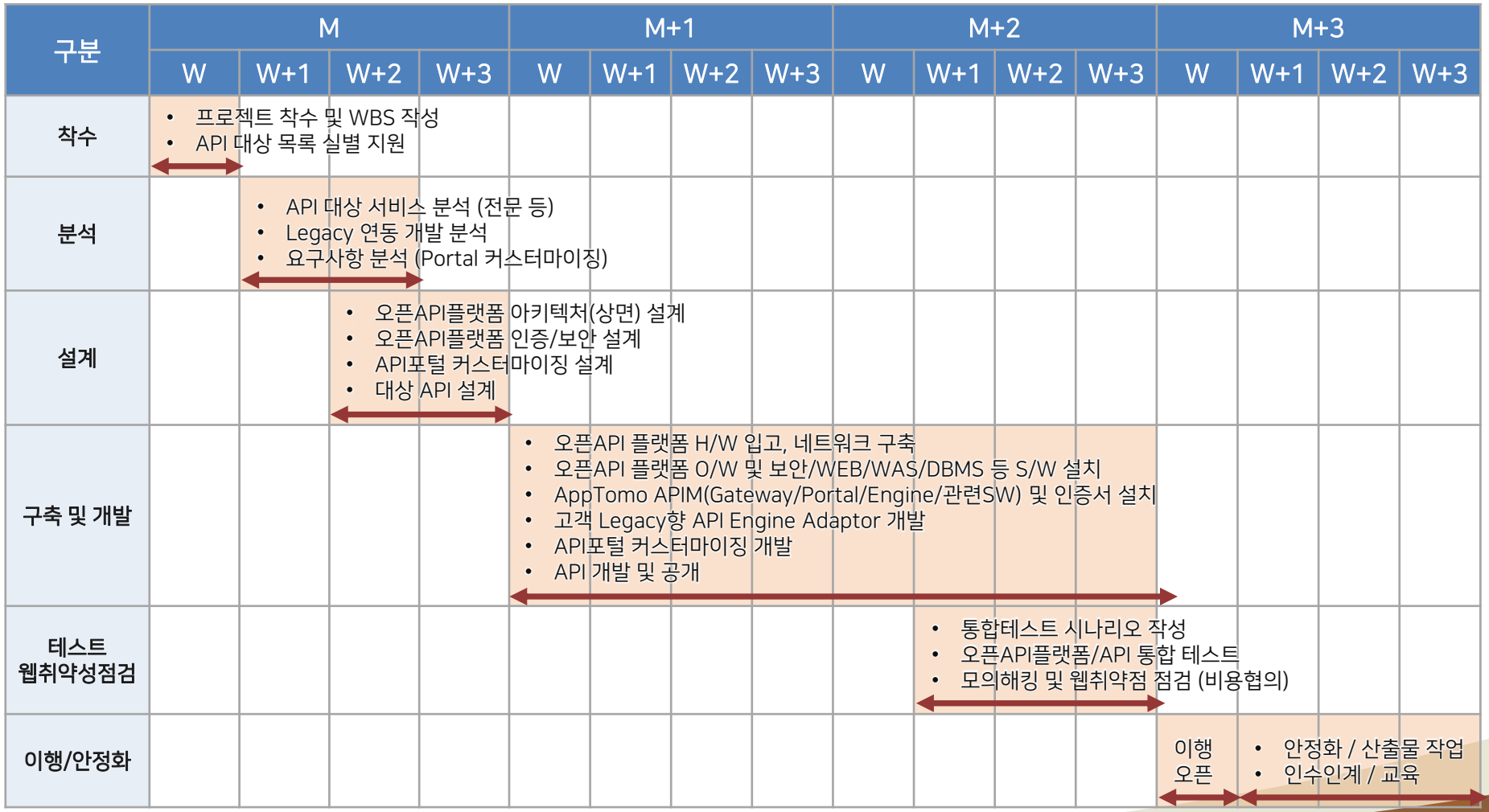


- 오픈API 개념 및 사례 공유 수행
- 프로세스 혁신팀과 협업 및 대상API선정

- API 플랫폼 H/W, N/W, O/S, S/W 등 구축
- API Developer Portal 커스터마이징
- API 테스트 및 API 공개
- API활용 서비스 or 데모 개발 (별도 협의)

2.9 Open API 플랫폼 구축 일정

① 프로젝트 착수, ② API 대상 서비스 분석 및 Open API 도출과 설계, ③ Open API 플랫폼 구축 및 API 활용서비스 개발, ④ 통합 테스트 및 웹취약성 점검, ⑤ 이행·안정화 등의 일정으로 진행됨.



오픈 API 플랫폼 구축 프로젝트

3.1 Open API 플랫폼 구축 배경 및 목적

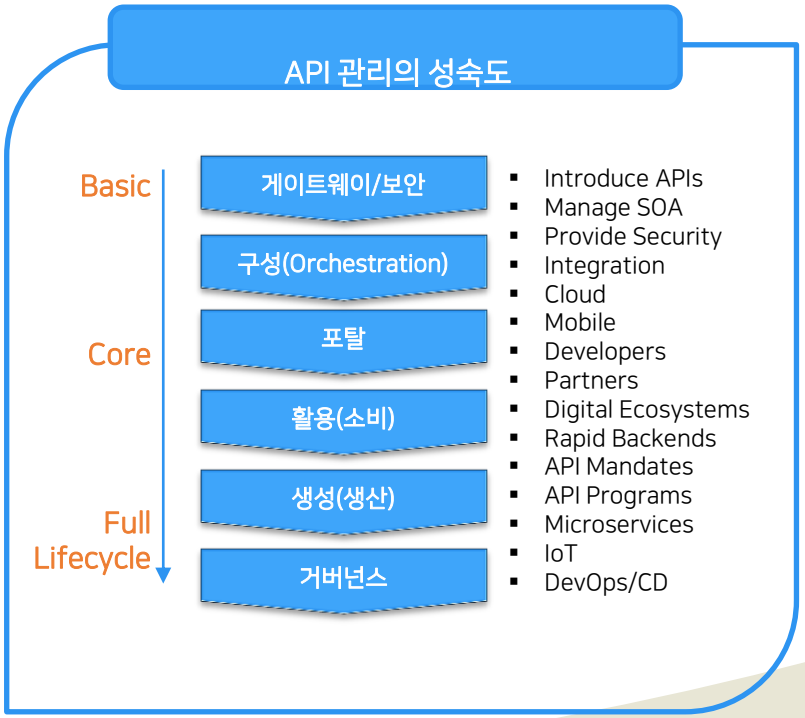
급변하는 금융산업 환경에서 금융회사와 핀테크 등 외부기업 간의 파트너십이 중요해지면서 여러 비 금융 기업과 금융 회사간에 정보를 교환하고 협력 비즈니스 모델을 구축/지원할 수 있는 표준 인프라 기반 확보는 이제는 필수 과제가 됨.

내/외부에서 API을 쉽고 빠르게 확장할 수 있는 API 플랫폼

"API Business에 대한 요구"

"신속하고 유연한 비즈니스 가치 창출을 위한 핵심입니다."

내/외부에서 API을 쉽게 활용	• 정보연계 효율향상 및 공용화 기반 마련 • 내/외부 정보 및 서비스 개방 요구 증대 • 비즈니스 로직 개발보다 보안/관리 등 비기능 구현에 따른 지연
제휴사와 손쉬운 비즈니스 확장	• API를 Product로 인식하고 관리하기 위한 인프라의 부재 • 분산 서비스 별 각기 다른 Legacy 연동 기술의 한계 • 비즈니스 도메인 간의 손쉬운 서비스 공유 방법 필요 • 통일된 보안 및 식별 정책 부재
API 비즈니스 모델 지원	• 지속적인 서비스 증가와 유료화 등을 포용할 수 있는 플랫폼 필요 • API를 Product로 인식하고 관리하기 위한 인프라의 부재 • 마이데이터 관련 금융권 데이터 표준 API 대응



3.2 Open API 플랫폼 구축 범위

Open API 플랫폼의 구축 프로젝트의 범위는 API Gateway, API Engine, API Portal, API Monitoring 솔루션을 구축하는 것임. 이와 함께, Open API 플랫폼에 맞게 고객사 API 개발에 대한 교육 및 가이드를 포함.

Open API 플랫폼 구축과 고객사 API 개발에 대한 가이드

API Gateway

보안 통신	메시지 검증	라우팅/부하분산	데이터 변환
프로토콜 변환	API 접근 제한	로그 및 이력 관리	사용자 인증
암호화/마스킹	OAuth	제휴사 및 앱 인증	API Rate Limit
Caching	API 위협 보호	토큰 발급 및 관리	Access Control

API Engine (API Engine)

API 등록 및 승인	API 명세 생성	API 테스트 지원
API 생성/버전 관리	API Chaining	전문 관리
관리자 기능	Adapter 추가 지원	키 관리 (UI)
다양한 보고서	공통 코드 관리	거래 추적 지원

API Monitoring

API 상태 체크	API 사용 통계	Gateway 상태 체크	이벤트 알람

API Portal

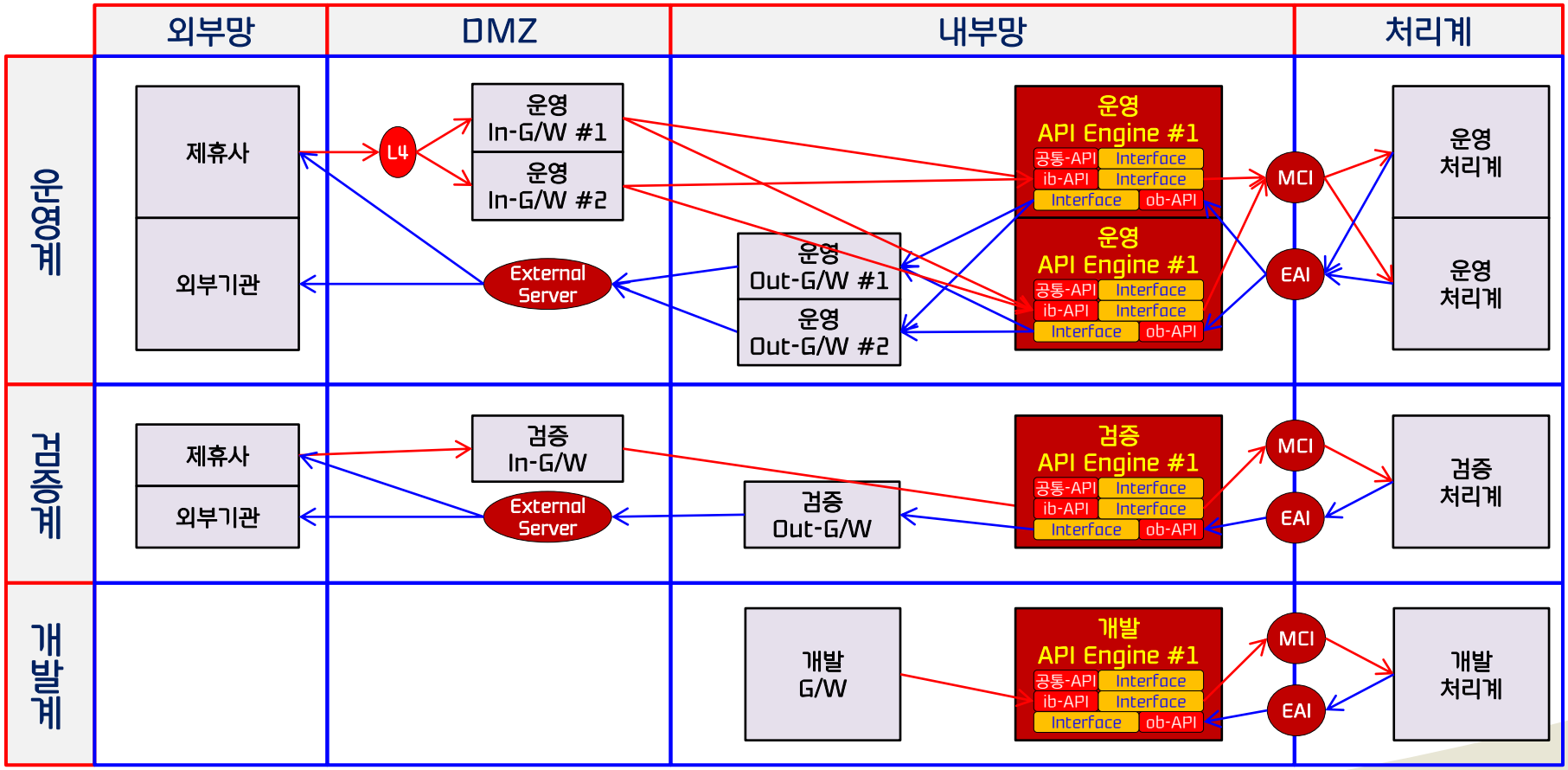
이용/제공기관관리	Open API 관리	APP/키 관리	API 커뮤니티

솔루션	내용(기능요약)
API Gateway	API Transaction 통제 및 거버넌스를 위한 핵심 코어 어플리케이션으로 내부 정책 및 설정 역할을 수행
API Portal	이용/제공기관 관리, Open API 관리, APP/키 관리, API 개발자 커뮤니티 등을 제공하는 어플리케이션
API Engine (API Engine)	API 서비스의 메시지 변환 및 검증, 서비스 라우팅 지원 프레임워크 + API 관리 포탈
API Monitoring	API GW 및 API Transaction 에 대한 세밀한 상태를 모니터링 하고 이슈에 대한 Troubleshooting 지원

3.3 Open API 플랫폼 구축 방안

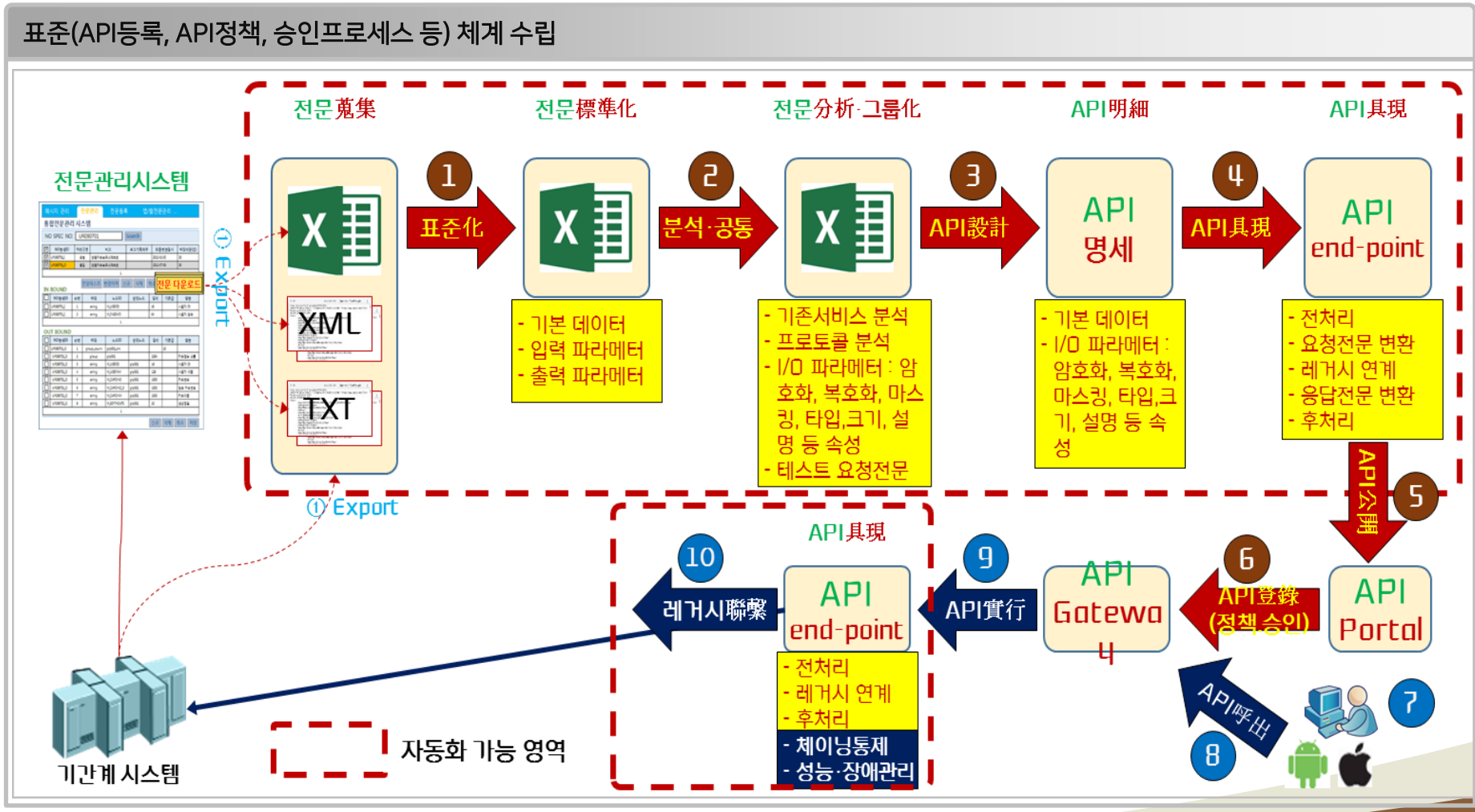
제휴사에 (In-Bound) Open API를 제공하기 위해 "API Gateway → API Engine → MCI 서버 → 처리계"를 연계하여 레거시 트랜잭션을 수행하고, 처리계에서 (Out-Bound) Open API를 실행하기 위해 반대의 호출 흐름을 제공함.

API Engine 구축 방안



3.4 레거시 서비스의 Open API 공개 방안

①인터페이스 선정, ②전문 분석, ③전문 대응 API 설계, ④API 구현체(end-point)를 구현, ⑤API 포털에 공개, ⑥G/W에 API 등록, ⑦API 테스트, ⑧서비스에서 API 호출, ⑨API G/W가 API 실행, ⑩API Engine이 해당 레거시 서비스 실행.



오픈 API 플랫폼 주요 기술

4.1 인증 방안 (1/8)

APIM 솔루션은 API 를 호출한 사용자와 클라이언트가 맞다는 것을 확인 하기 위한 인증 수단으로 디바이스, 앱, 사용자의 각 레벨에서 단일 혹은 결합된 인증 방법을 위한 모듈을 내장하여 제공함.

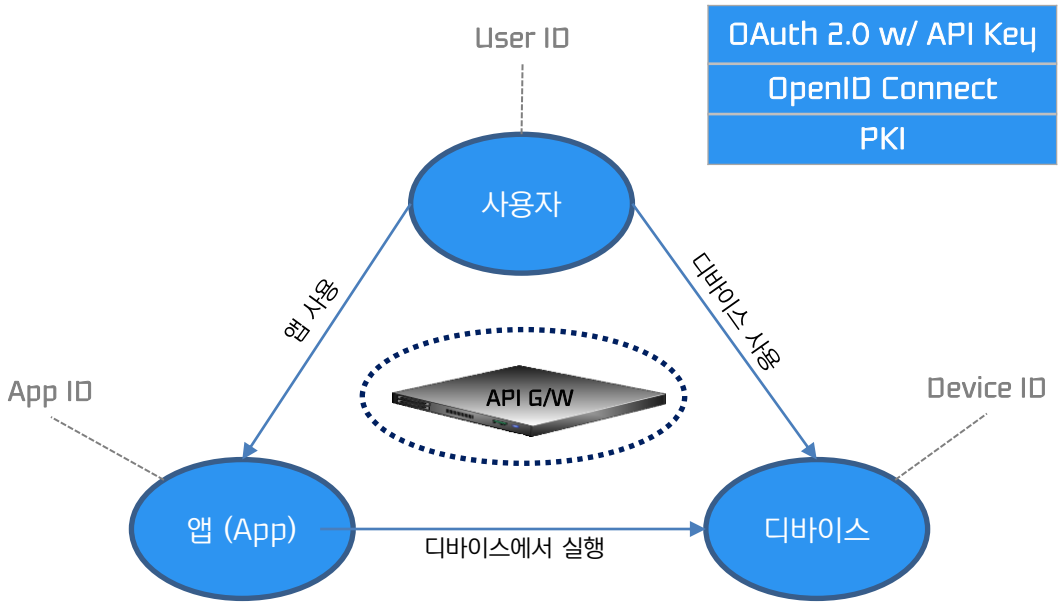
주요 인증 방식

API G/W에서는 하기와 같은 주요 인증 방식을 제공합니다.

- **디바이스 레벨**
  - Mutual SSL 인증
  - IP 기반 인증
- **어플리케이션 레벨**
  - API Key 인증
  - 클라이언트 방식 (OAuth 인증)
- **사용자 레벨**
  - Basic 인증
  - 제 3자 인증 (ID Federation, SSO 솔루션)
  - API Token 방식 (OAuth 인증)
- **어플리케이션 + 사용자 레벨**
  - API Token + 클라이언트 방식 (OAuth 인증)

주요 프로토콜 전략

- 3 legged 방식의 계층적 인증 보안으로 API 보안을 제공
- API G/W는 사용자, 앱, 디바이스의 관계를 관리



4.1 인증 방안 (2/8)

APIM 솔루션은 API 를 호출한 사용자와 클라이언트가 맞다는 것을 확인 하기 위한 인증 수단으로 디바이스, 앱, 사용자의 각 레벨에서 단일 혹은 결합된 인증 방법을 위한 모듈을 내장하여 제공함.

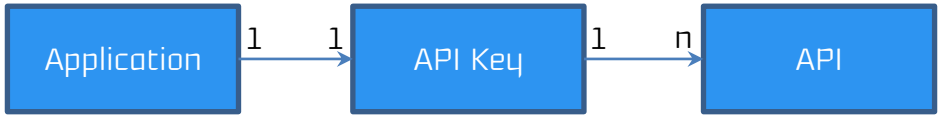
API Key 인증

API 게이트웨이는 어플리케이션을 식별하고 인증하기 위한 API Key 인증 방법을 제공합니다.

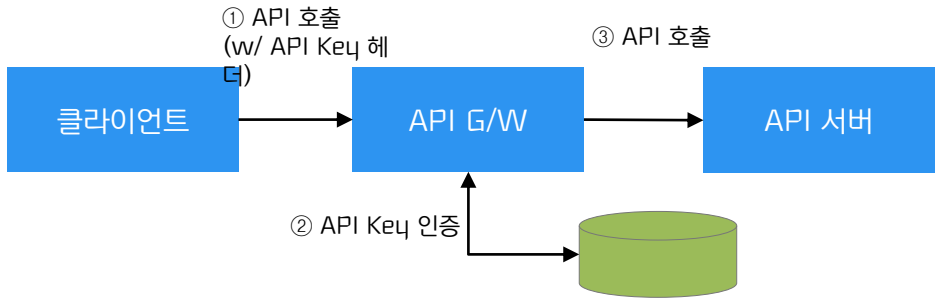
- **엔티티 관계**
  - 하나의 클라이언트 어플리케이션은 하나의 API Key를 가짐 (1:1)
  - 하나의 API Key 는 하나 혹은 여러 개의 API 와 매핑 관계를 가짐 (1:n)
  - 클라이언트 어플리케이션 별로 각기 다른 고유한 API Key 를 할당함으로써, API 의 부적절한 접근 위험을 방지

- **API Key 인증 프로세스**
  1) 클라이언트는 API Key를 헤더에 첨부하여 API 호출
  2) 게이트웨이는 API Key를 추출하고 API Key를 인증
  3) 인증 결과가 정상이면 API 서버로 요청 라우팅

API Key 엔티티 관계



API Key 인증 프로세스



4.1 인증 방안 (3/8)

APIM 솔루션은 API 를 호출한 사용자와 클라이언트가 맞다는 것을 확인 하기 위한 인증 수단으로 디바이스, 앱, 사용자의 각 레벨에서 단일 혹은 결합된 인증 방법을 위한 모듈을 내장하여 제공함.

API Token 및 클라이언트 인증

API 게이트웨이는 API Token 인증 및 클라이언트 인증 방식을 지원하기 위한 방법으로 OAuth 2.0 Tool Kit을 제공합니다.

OAuth 2.0 Tool Kit 은 OAuth 2.0의 다음 네 가지 Grant Type을 모두 지원하며, 추가적으로 OAuth 2.0 Extension Grant Type을 이용하여 API G/W는 SAML Bearer OAuth 인증 타입을 지원합니다.

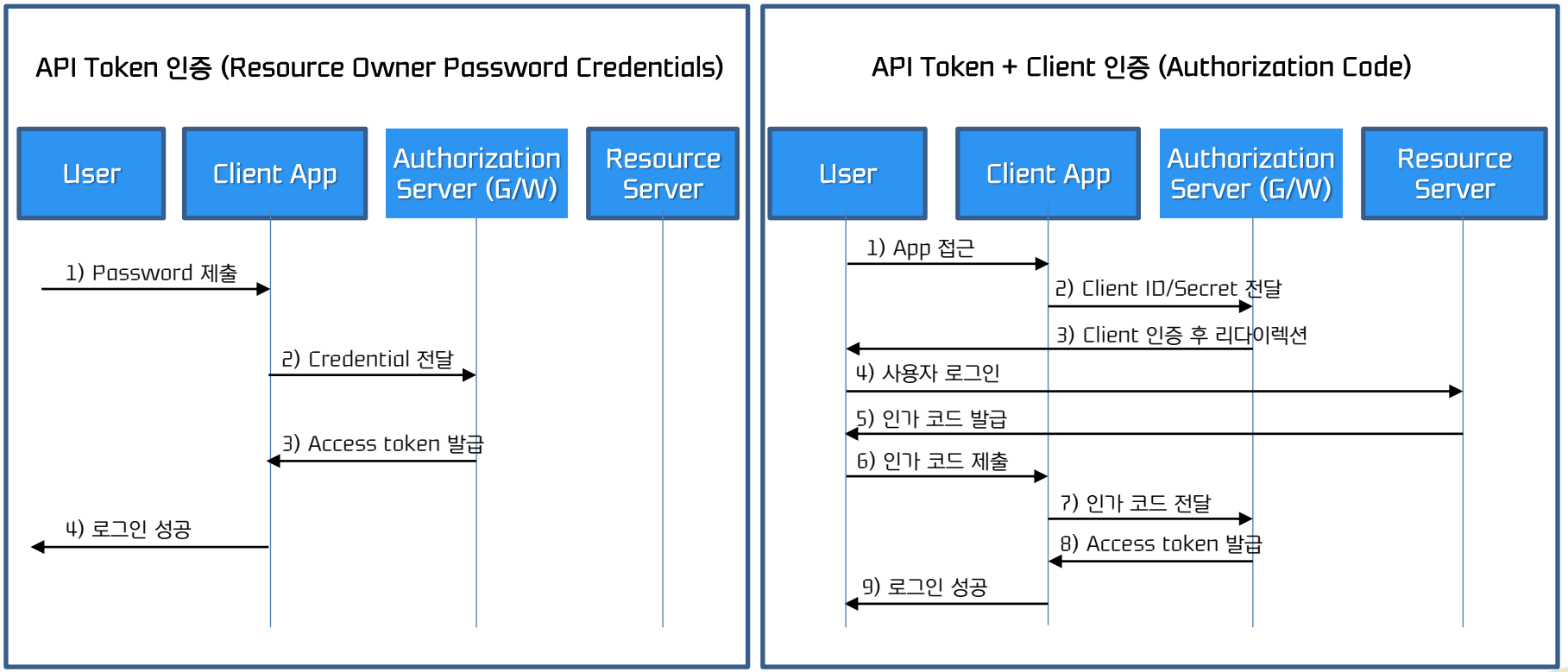
- **Authorization Code**
  - 사용자 아이디와 비밀번호, 그리고 클라이언트 ID와 Secret으로 API 토큰 발급
- **Implicit**
  - 사용자 아이디와 비밀번호로 API 토큰 발급 (Browser용)
- **Client Credentials**
  - 클라이언트 ID와 Secret으로 API 토큰 발급
- **Resource Owner Password Credentials**
  - 사용자 아이디와 비밀번호로 API 토큰 발급
- **SAML Bearer OAuth**
  - SAML Assertion을 기반으로 API 토큰 발급

구분	인증 방식	OAuth 2.0 Grant Type
매핑 #1	API Token + 클라이언트 인증 방식	Authorization Code
매핑 #2	API Token 방식	Implicit
매핑 #3	클라이언트 인증 방식	Client Credentials
매핑 #4	API Token 방식	Resource owner password credentials
매핑 #5	API Token + SAML 인증 방식	Extension (SAML Bearer OAuth)

4.1 인증 방안 (4/8)

APIM 솔루션은 API 를 호출한 사용자와 클라이언트가 맞다는 것을 확인 하기 위한 인증 수단으로 디바이스, 앱, 사용자의 각 레벨에서 단일 혹은 결합된 인증 방법을 위한 모듈을 내장하여 제공함.

API Token 및 클라이언트 인증 프로세스



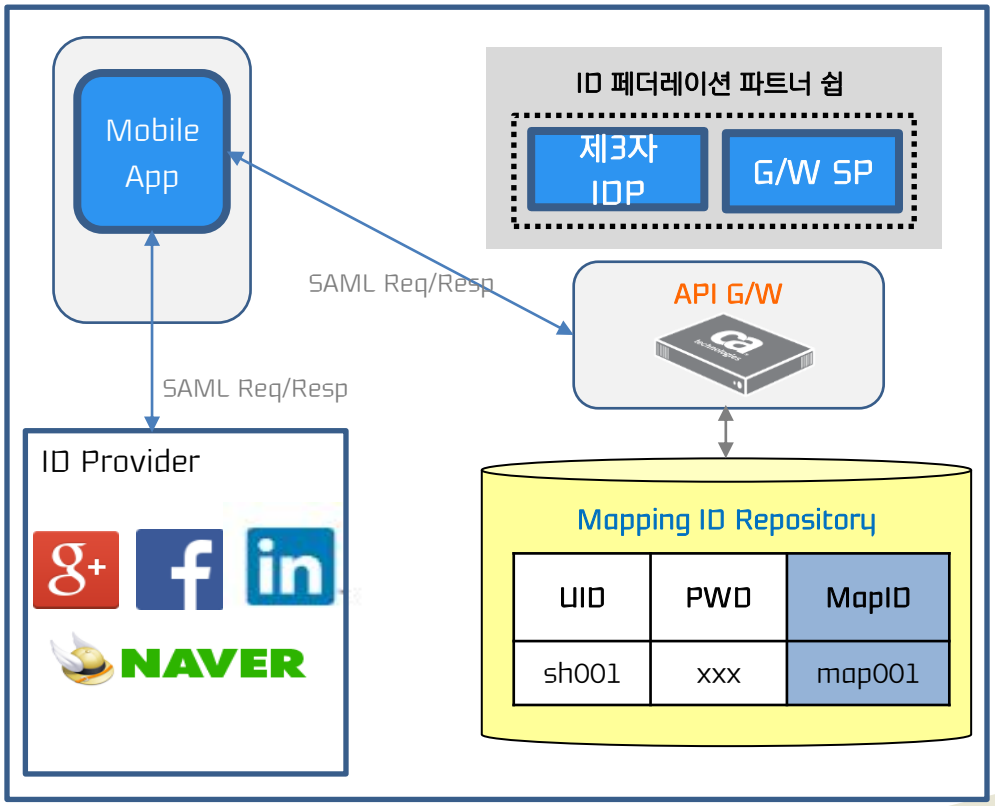
4.1 인증 방안 (5/8)

APIM 솔루션은 API 를 호출한 사용자와 클라이언트가 맞다는 것을 확인 하기 위한 인증 수단으로 디바이스, 앱, 사용자의 각 레벨에서 단일 혹은 결합된 인증 방법을 위한 모듈을 내장하여 제공함.

제3자 인증

API 게이트웨이는 Social Login 또는 ID Federation 기술을 통해 제 3 자의 사용자 Credential을 사용한 인증을 제공합니다.

- **Social Login**
  - Google, Facebook, LinkedIn, Twitter, Salesforce 등의 사용자 Credential을 사용하여 게이트웨이가 인증
- **ID Federation**
  - 네이버, 야후, 핀테크 기업 또는 타 계열사의 ID 를 사용한 인증연계에 SAML 프로토콜을 지원
  - 제 3자 이용기관은 ID 공급자의 IDP (Identity Provider) 로 동작
  - API G/W는 SP (Service Provider) 로서 동작하도록 제3자 IDP와 SAML 파트너 쉽 구성
  - 사용자 매핑을 위한 Key를 가지는 ID Repository 를 통한 연계 지원



4.1 인증 방안 (6/8)

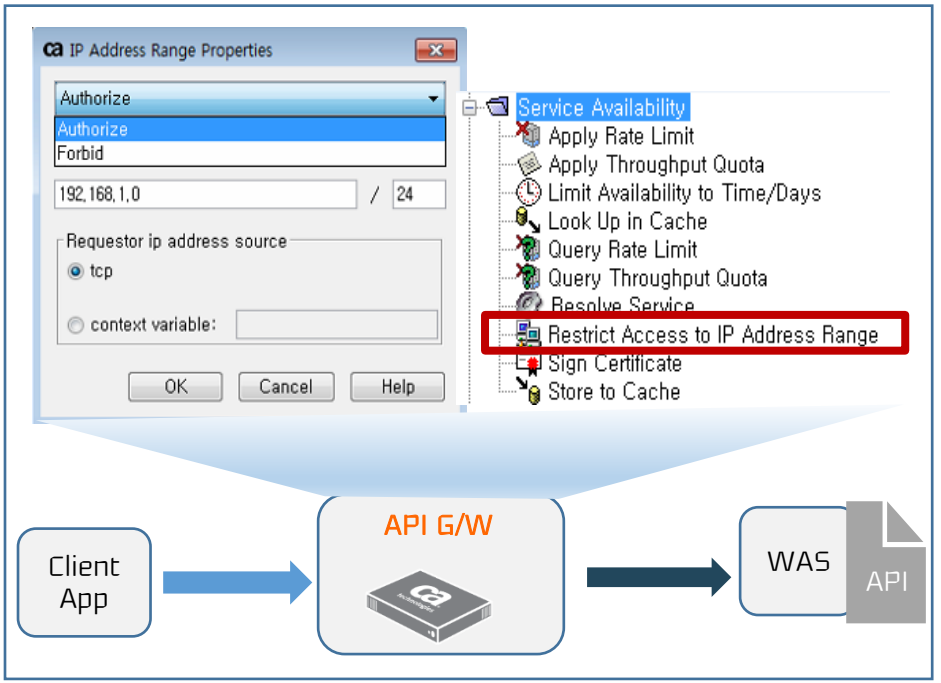
APIM 솔루션은 API 를 호출한 사용자와 클라이언트가 맞다는 것을 확인 하기 위한 인증 수단으로 디바이스, 앱, 사용자의 각 레벨에서 단일 혹은 결합된 인증 방법을 위한 모듈을 내장하여 제공함.

IP 기반 인증

API 게이트웨이는 간단한 정책 설정을 통해 클라이언트의 IP 에 기반한 인증을 제공하며 두가지 인증 타입을 지원합니다.

- White List IP 인증
  - 설정한 IP 또는 IP 대역에 한해 API 접근을 허용
- Black List IP 인증
  - 설정한 IP 또는 IP 대역에 한해 API 접근을 차단

IP 기반 접근 통제 정책
- White List, Black List 여부
- 특정 IP, 특정 IP 대역 설정 (CIDR 표기)
- IP 주소를 가져오는 방법 (TCP 또는 Custom 변수)



4.1 인증 방안 (7/8)

APIM 솔루션은 API 를 호출한 사용자와 클라이언트가 맞다는 것을 확인 하기 위한 인증 수단으로 디바이스, 앱, 사용자의 각 레벨에서 단일 혹은 결합된 인증 방법을 위한 모듈을 내장하여 제공함.

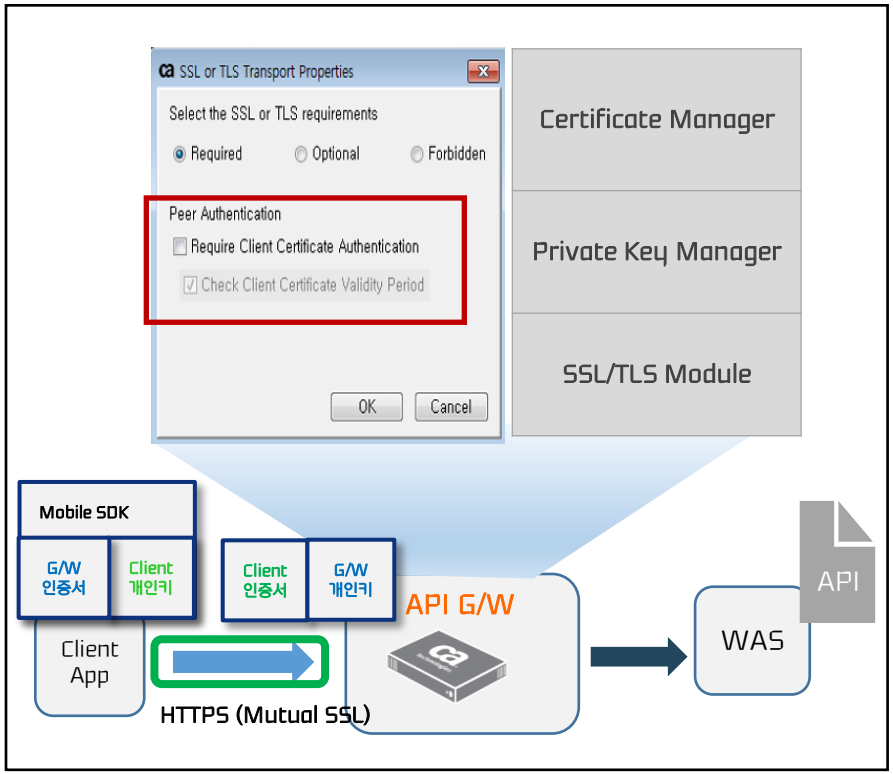
Mutual SSL 인증

API 게이트웨이는 다음과 같은 클라이언트와 G/W 사이드의 모듈을 통해 클라이언트의 인증서를 인증함으로써 API 게이트웨이 간의 양방향 SSL 을 제공합니다.

- 게이트웨이 CA/RA
  - 개인키와 인증서를 관리하고 CSR에 서명하는 인증 기관
- SSL/TLS 인증 Assertion
  - Client의 SSL 연결을 인증하는 모듈
- Mobile SDK
  - 모바일에서 Client 개인키의 생성을 지원

*** SSL/TLS 인증 정책**
지원되는 SSL/TLS 모드
- Required, Optional, Forbidden

양방향 SSL 설정
- 클라이언트 인증서 인증
- 클라이언트 인증서 만료 여부 체크



4.1 인증 방안 (8/8)

API Gateway는 보안 관련 다양한 인증 프로토콜을 지원함.

다양한 사용자 인증/인가 표준 프로토콜 지원

X.509 Certificate	SSL Client Certificate (Mutual SSL), PKI CA/RA
User Name /Password	HTTP Basic Auth, HTTP Digest Auth, Encrypted User Name Token, XPath Credential
Microsoft	Windows Integrated Authentication, NTLM, Kerberos
Security token	WS-Security, WS-Trust, WS Federation, WS-SecureExchange, SAML
OAuth	OAuth 1.0, OAuth 2.0 (Bearer/HMAC), OpenIDConnect 1.0, JWT(JSON Web Token)
기타	SSH Credential, FTP Credential, XACML Request creation/validation

4.2 인가 방안 (1/3)

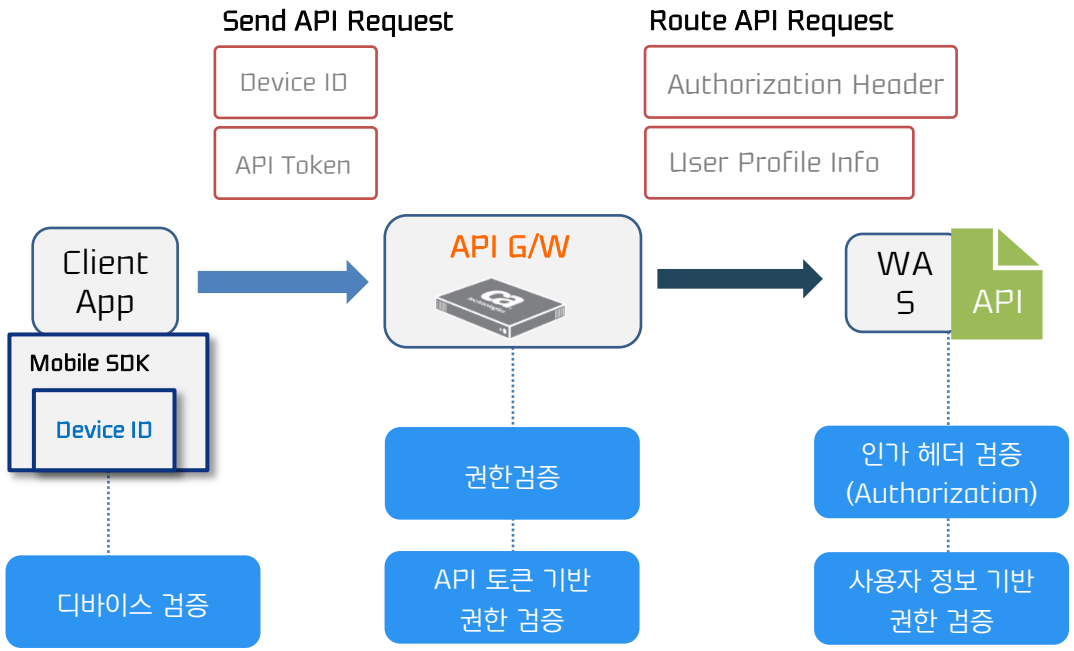
APIM 솔루션은 인증을 받은 사용자가 해당 권한을 가진 API 에만 접근 할 수 있도록 하는 권한 검증 메카니즘을 클라이언트와 API G/W, API 서버 단에 걸쳐 제공함.

주요 인가 방식

API G/W에서는 하기와 같은 주요 인가 방식을 클라이언트, API G/W, API 서버 단에 제공합니다.

- **클라이언트**
  - 디바이스 검증 (Device ID)
- **API G/W**
  - 권한 검증
  - API 토큰 기반 권한 검증 (ACL)
- **API 서버**
  - 인가 헤더 검증 (Authorization Header)
  - 사용자 정보 권한 검증

API 권한 인가 위치



4.2 인가 방안 (2/3)

APIM 솔루션은 인증을 받은 사용자가 해당 권한을 가진 API 에만 접근 할 수 있도록 하는 권한 검증 메카니즘을 클라이언트와 API G/W, API 서버 단에 걸쳐 제공함.

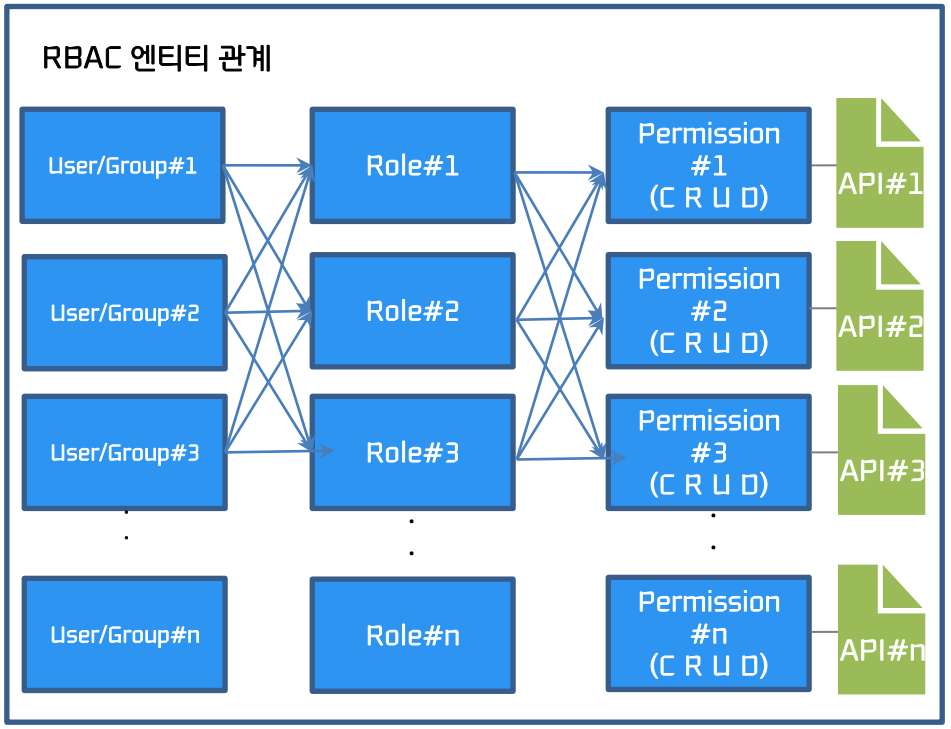
역할 기반 권한 검증 (RBAC)

API G/W의 RBAC 접근 통제는 하기의 Identity Provider 의 사용자/그룹에 대응하여 제공합니다.

Internal Identity Provider
: 게이트웨이 내부 데이터베이스에서 사용자를 인증

LDAP Identity Provider
: 외부 LDAP 서버에서 사용자를 인증

- RBAC 엔티티
  - User/Group
    : 인증된 사용자 또는 그 그룹을 Role 에 할당
  - Role
    : 단일 혹은 다중 퍼미션 세트를 포함
  - Permission
    : 각 API 에 대한 CRUD 메트릭스를 할당



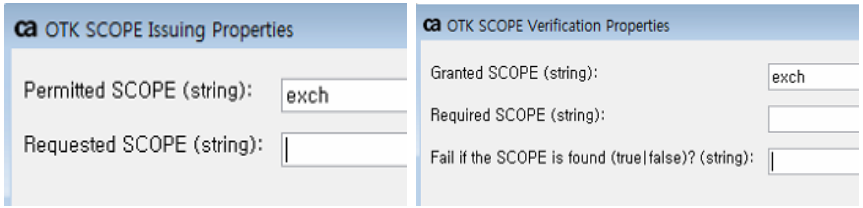
4.2 인가 방안 (3/3)

APIM 솔루션은 인증을 받은 사용자가 해당 권한을 가진 API 에만 접근 할 수 있도록 하는 권한 검증 메카니즘을 클라이언트와 API G/W, API 서버 단에 걸쳐 제공함.

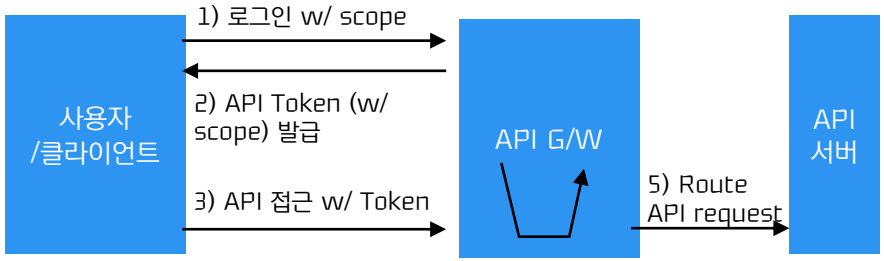
API토큰 기반 권한 검증(ACL)

API G/W는 OAuth 토큰의 Scope 을 발급 및 검증하는 기능을 제공하여 API를 호출하는 사용자의 권한을 검증 합니다.

- **OAuth Scope 발급/검증 기능**



- **OAuth Scope 검증 프로세스**
  1) 사용자는 Scope 명시하여 OAuth 로그인
  2) G/W는 Scope 을 포함하여 OAuth 토큰 발급
  3) 사용자가 클라이언트 앱을 통해 API 접근
  4) G/W는 요청된 API에 대한 허용되는 Scope 검증
  5) 허용 Scope과 전달된 Scope이 일치시 API 서버로 요청을 라우팅



4) Scope Verification

	OAuth Scope	API
1	exch	/Exchange
2	exch_rate	/ExchangeRate
3	usr_info	/User

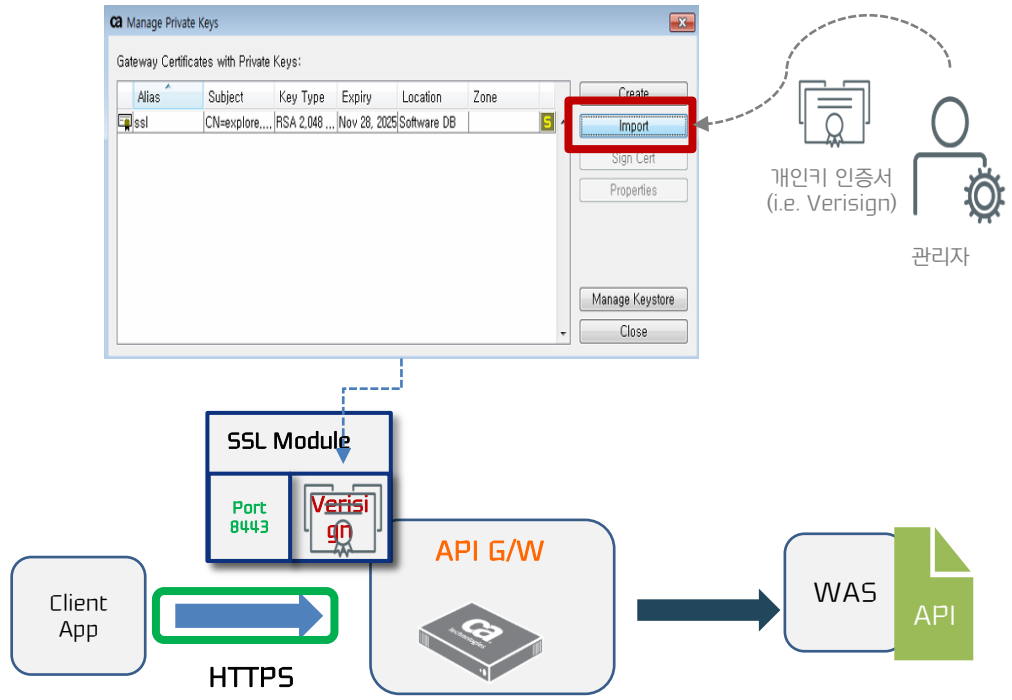
4.3 네트워크 레벨 암호화

APIM 솔루션은 클라이언트와 G/W간 공개 네트워크 상의 안전한 통신을 위해 SSL (HTTPS) 통신 기능을 기본으로 지원하며, 사설 인증서 뿐만이 아니라 공인 인증서 기반의 SSL 또한 제공함.

주요 SSL 기능

- G/W의 Listen Port 별 인증서 할당
  - Default SSL 인증서 사용 또는, Listen Port를 분리하여 해당 포트에 특정 SSL 인증서 할당 지원
- 와일드카드 호스트이름 인증서 지원
  - RFC 2818에 정의된 HTTPS 호스트이름의 WildCard 매칭을 지원 (i.e. *.sub.domain.com)
- 암호화 알고리즘 선택 제공
  - SSL에 사용할 수 있는 알고리즘 리스트를 제공하여 취약한 알고리즘 사용을 방지
- SSL/TLS 버전 선택 제공
  - TLS1.0, TLS 1.1, TLS1.2 등 프로토콜 선택을 제공하여 취약한 프로토콜 사용을 방지
- 클라이언트 인증서 인증 제공
  - 클라이언트 인증서 기반의 Mutual SLI 인증

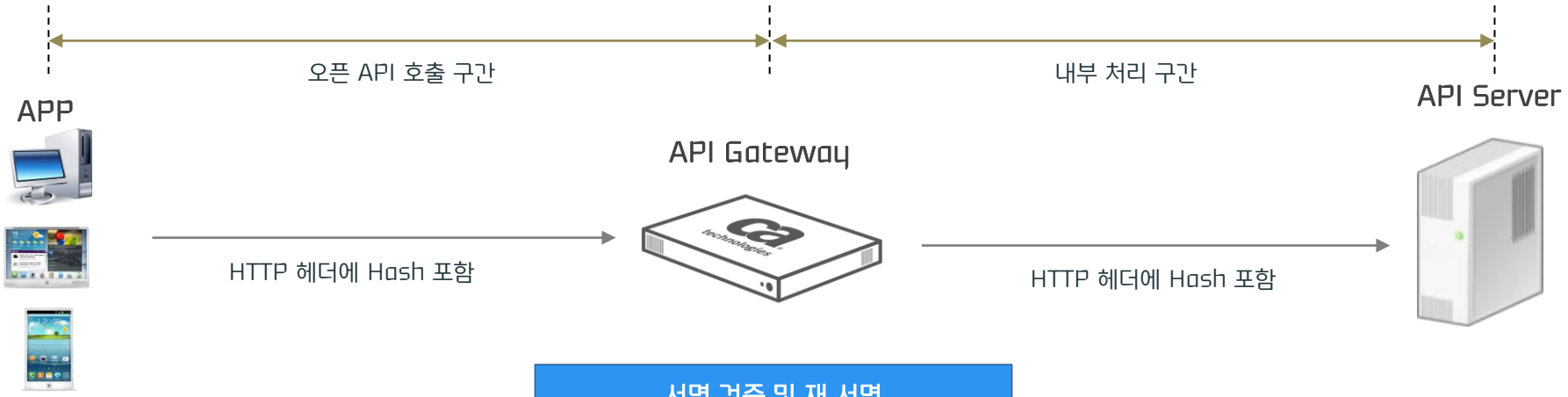
공인 인증서 기반 SSL 구성



4.4 메시지 무결성 보장

데이터 무결성과 안정성을 보장하기 위하여 이미 타 은행에 적용한 오픈 API 호출 및 내부 처리구간에서 데이터에 대한 서명값을 이용한 검증방식을 사용함.

데이터 무결성과 안정성



데이터 서명

- Access Token 또는 Client id 값을 key로 Payload에 대한 HMAC SHA 256 Hash 생성

서명 검증 및 재 서명

- Access Token 또는 Client id 값을 key로 Payload에 대한 HMAC SHA 256 Hash 생성하여 헤더의 Hash와 비교
- Gateway에서 인증 및 변환 작업 후의 데이터에 대해 다시 HMAC SHA 256 Hash 생성

서명 검증

- 전달된 데이터에 대한 HMAC SHA 256 Hash 생성하여 헤더의 Hash와 비교

4.5 메시지 본문 암호화 (1/2)

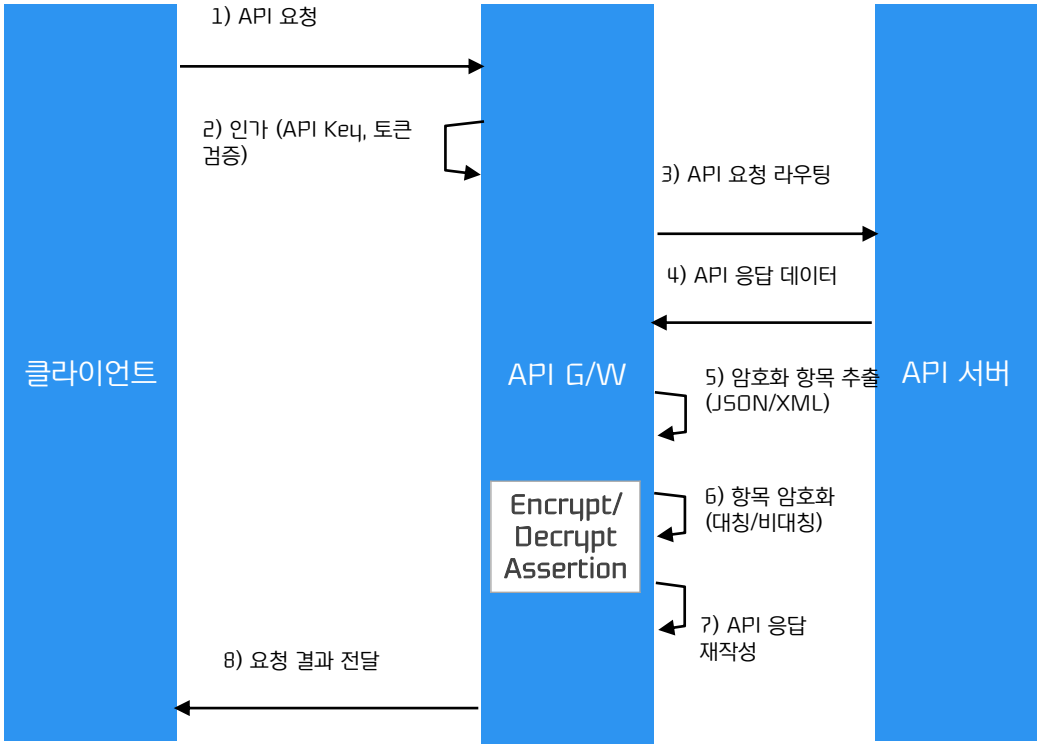
APIM 솔루션은 전체 메시지 혹은 민감한 특정 항목에 대한 비대칭키 방식과 대칭키 방식의 암호화를 제공함.

메시지 암호화 기능

API G/W의 API 정책에 하기의 암복호화 기능을 적용하여 민감한 데이터 노출을 방지 합니다.

- 비대칭키 암호화
  - Encrypt/Decrypt 여부
  - 암복호화에 사용할 인증서/개인키
  - Mode/Padding (ECB/No padding, ECB/PKCS1 padding, ECB/OAEP with SHA-1 and MGF-1 padding
- 대칭키 암호화
  - Encrypt/Decrypt 여부
  - Key/IV
  - 알고리즘 (AES/CBC/PKCS5Padding, DES/CBC/PKCS5Padding,DESede/CBC/PKCS5Padding, PGP)

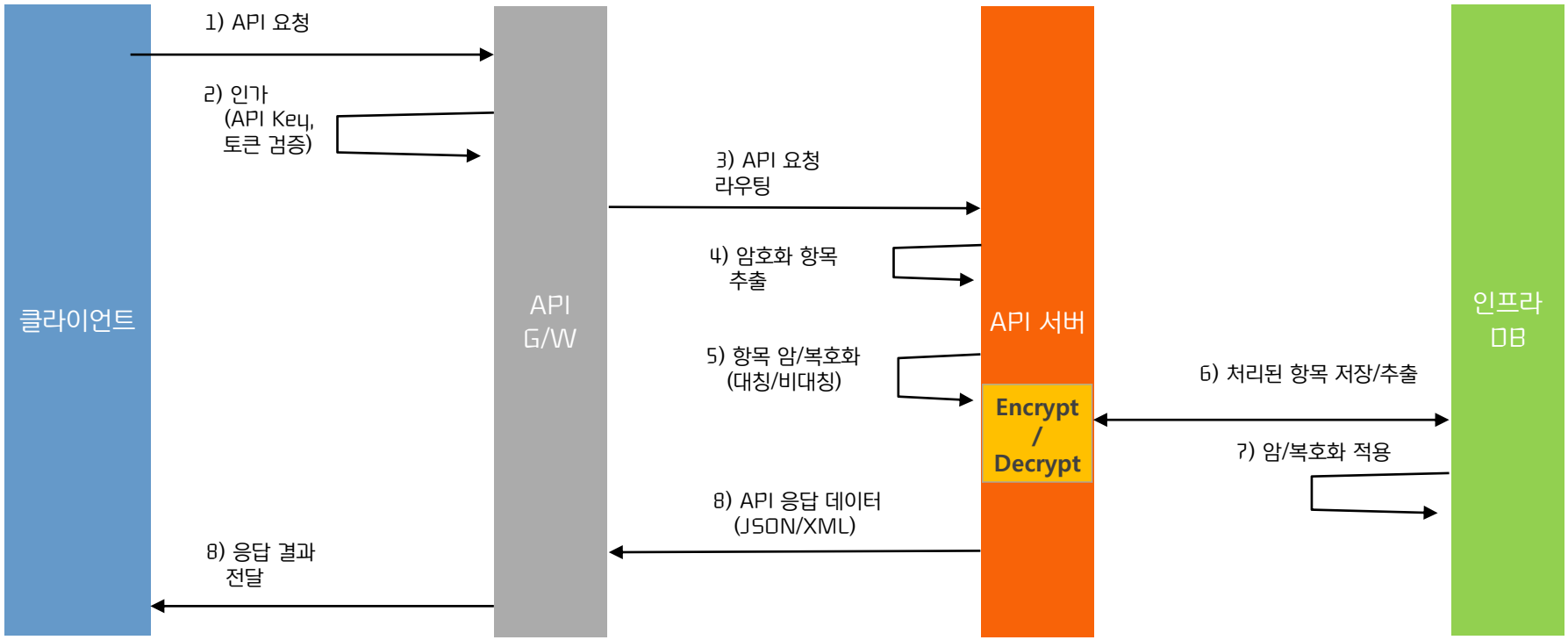
특정 항목 암호화 프로세스



4.5 메시지 본문 암호화 (2/2)

API 업무 처리 시 DB에 데이터 반영이나 비즈니스 처리 시 민감한 특정 데이터에 대해서는 대칭키/비대칭키 방식의 암/복호화 기능을 제공함.

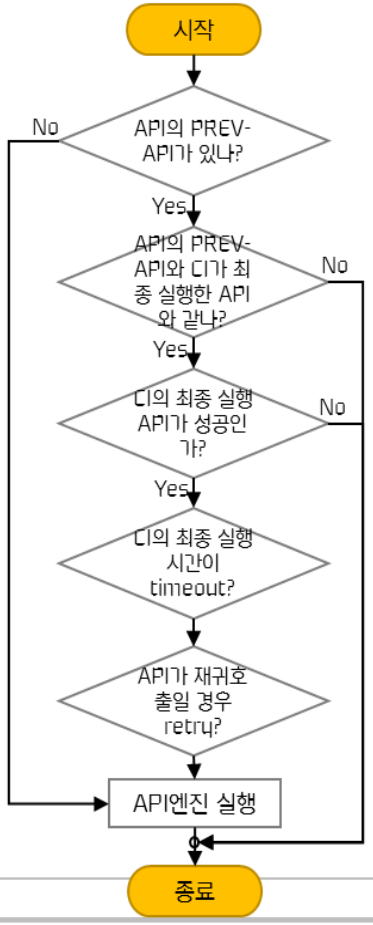
DB 및 데이터 암·복호화 기능



4.6 API 체이닝 거래 (1/3)

"API 체이닝거래"는 ① API_ITF90001, ② API_ITF90002, ③ API_ITF90003, ④ API_ITF90004, ⑤ API_ITF90005, ⑥ API_ITF90006, ⑦ API_ITF90005 등의 API가 순서데로 실행되어야 하는 순차적인 거래임.

API 체이닝 거래 지원 (1/4)



H카드 → 단기카드대출 → 단기카드대출 신청 / 신청하기

- ✓ 반드시 순서대로 API가 호출되어야 한다.
- ✓ ②API는 ①API가 실행된 후여야 한다.
- ✓ ②API의 PREV-API는 ①API이다.
- ✓ ①API의 PREV-API는 없다.
- ✓ PREV-API : API = n : 1

HTTPMethod	POST
authorization	Bearer 7dhf7466-n424-4n8e-9672-2d5eddddc1945
hskey	ijkGkw4qd InRijiQfxV3FMA0If6RKuMjrtvA/RrfK3TrF=
apikey	l7xx99c70455a9084e2a9c6af04ff99027e3
tmin	P0Enrnrc51-nn5n-45nn-8849-nn0n4454n12c2
apiUrl	/v1.0/CRM/crmhservices/limit
ciNo	F4PIs45uiscs8qu ... jnQWpFWWnhKnmShR+05
jumin_no	7304251234567
clnt_n	P00811934?
clnt_nm	홍길동
ifId	ITF90002
svcId	SVW_ITF90002

<고객이 실행한 API정보>

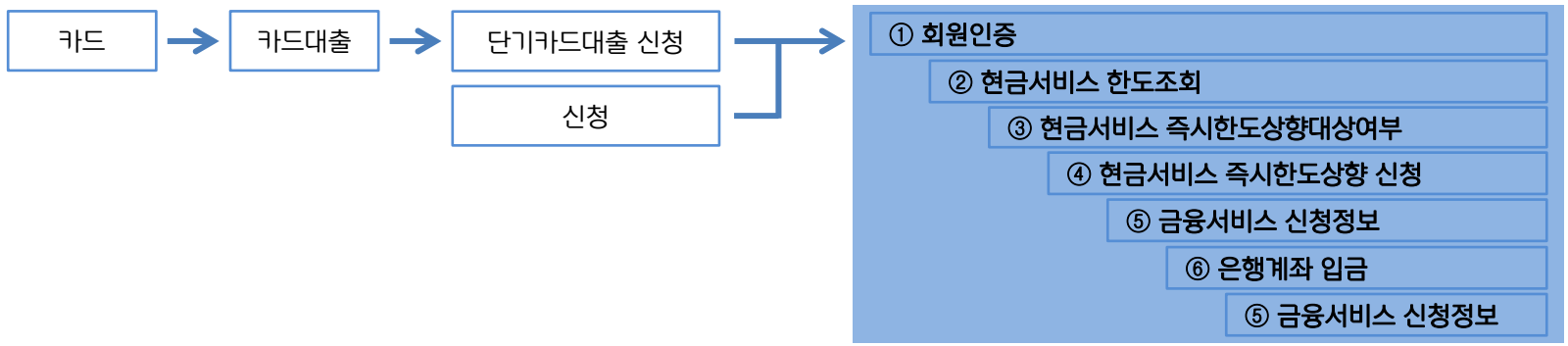
- ① API_ITF90001 회원인증(비밀번호체크)
- ② API_ITF90002 현금서비스한도조회
- ③ API_ITF90003 현금서비스 즉시한도상향대상여부 조회
- ④ API_ITF90004 현금서비스 즉시한도상향 신청
- ⑤ API_ITF90005 금융서비스 신청정보
- ⑥ API_ITF90006 은행계좌입금
- ⑦ API_ITF90005 금융서비스 신청정보

Authorization, hsKey, apiKey, 암복호화 적용

4.6 API 체이닝 거래 (2/3)

① 회원인증, ② 현금서비스 한도조회, ③ 현금서비스 즉시한도상향대상여부, ④ 현금서비스 즉시한도상향 신청, ⑤ 금융서비스 신청정보, ⑥ 은행계좌 입금, ⑤ 금융서비스 신청정보 등의 API들은 체이닝 거래로 설정되어 순차적으로 실행됨.

API 체이닝 거래 지원 (2/4)

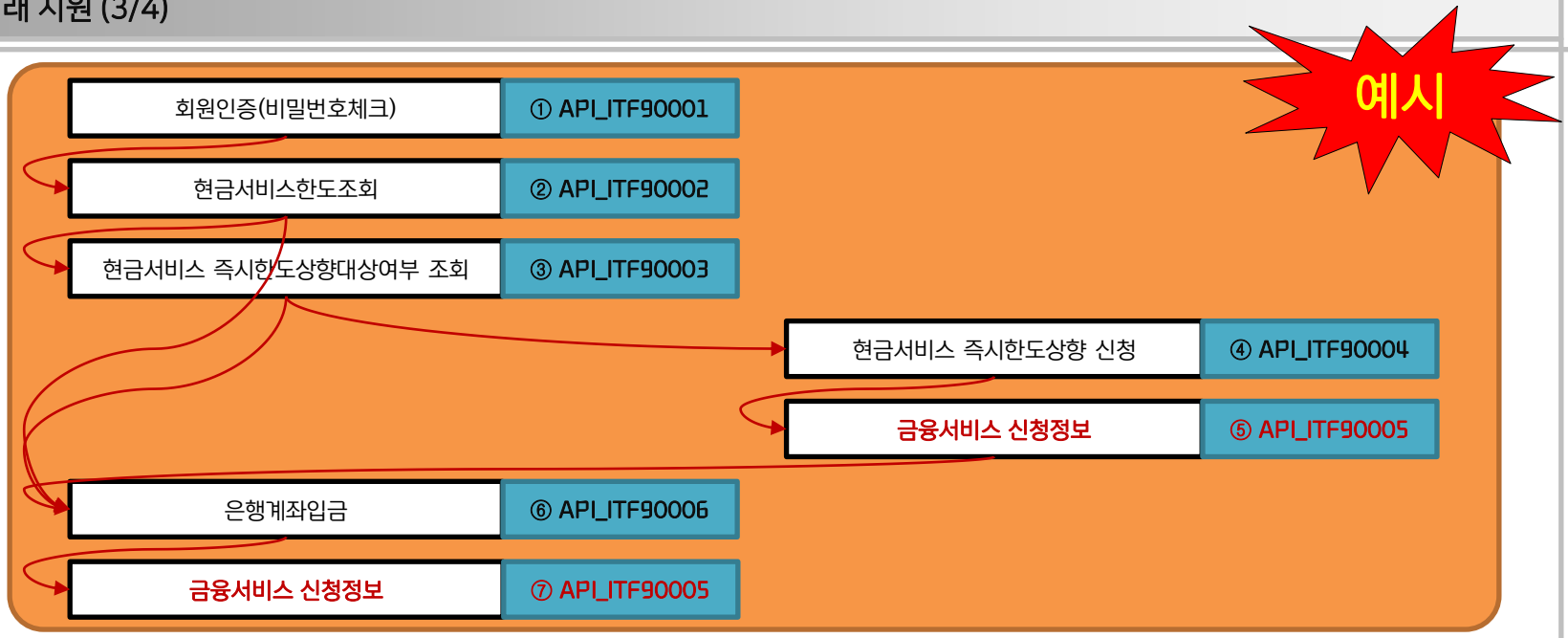


순서	거래명	API		인터페이스	
		ID	URI	ID	API Process
①	회원인증	API_ITF90001	/v1.0/CRD/auth/membercheck	ITF90001	com.apptomo.apis.proc.biz.card.ITF90001_ApiProcess
②	현금서비스 한도조회	API_ITF90002	/v1.0/CRD/cash/limit	ITF90002	com.apptomo.apis.proc.biz.card.ITF90002_ApiProcess
③	현금서비스 즉시한도상향대상여부	API_ITF90003	/v1.0/CRD/limits/uptarget	ITF90003	com.apptomo.apis.proc.biz.card.ITF90003_ApiProcess
④	현금서비스 즉시한도상향 신청	API_ITF90004	/v1.0/CRD/limits/cashUpApply	ITF90004	com.apptomo.apis.proc.biz.card.ITF90004_ApiProcess
⑤	금융서비스 신청정보	API_ITF90005	/v1.0/CRD/financial/applyinfo	ITF90005	com.apptomo.apis.proc.biz.card.ITF90005_ApiProcess
⑥	은행계좌입금	API_ITF90006	/v1.0/CRD/accounts/receipt	ITF90006	com.apptomo.apis.proc.biz.card.ITF90006_ApiProcess
⑤	금융서비스 신청정보	API_ITF90005	/v1.0/CRD/financial/applyinfo	ITF90005	com.apptomo.apis.proc.biz.card.ITF90007_ApiProcess

4.6 API 체이닝 거래 (3/3)

① 회원인증, ② 현금서비스 한도조회, ③ 현금서비스 즉시한도상향대상여부, ④ 현금서비스 즉시한도상향 신청, ⑤ 금융서비스 신청정보, ⑥ 은행계좌 입금, ⑤ 금융서비스 신청정보 등의 API들은 체이닝 거래로 설정되어 순차적으로 실행됨.

API 체이닝 거래 지원 (3/4)

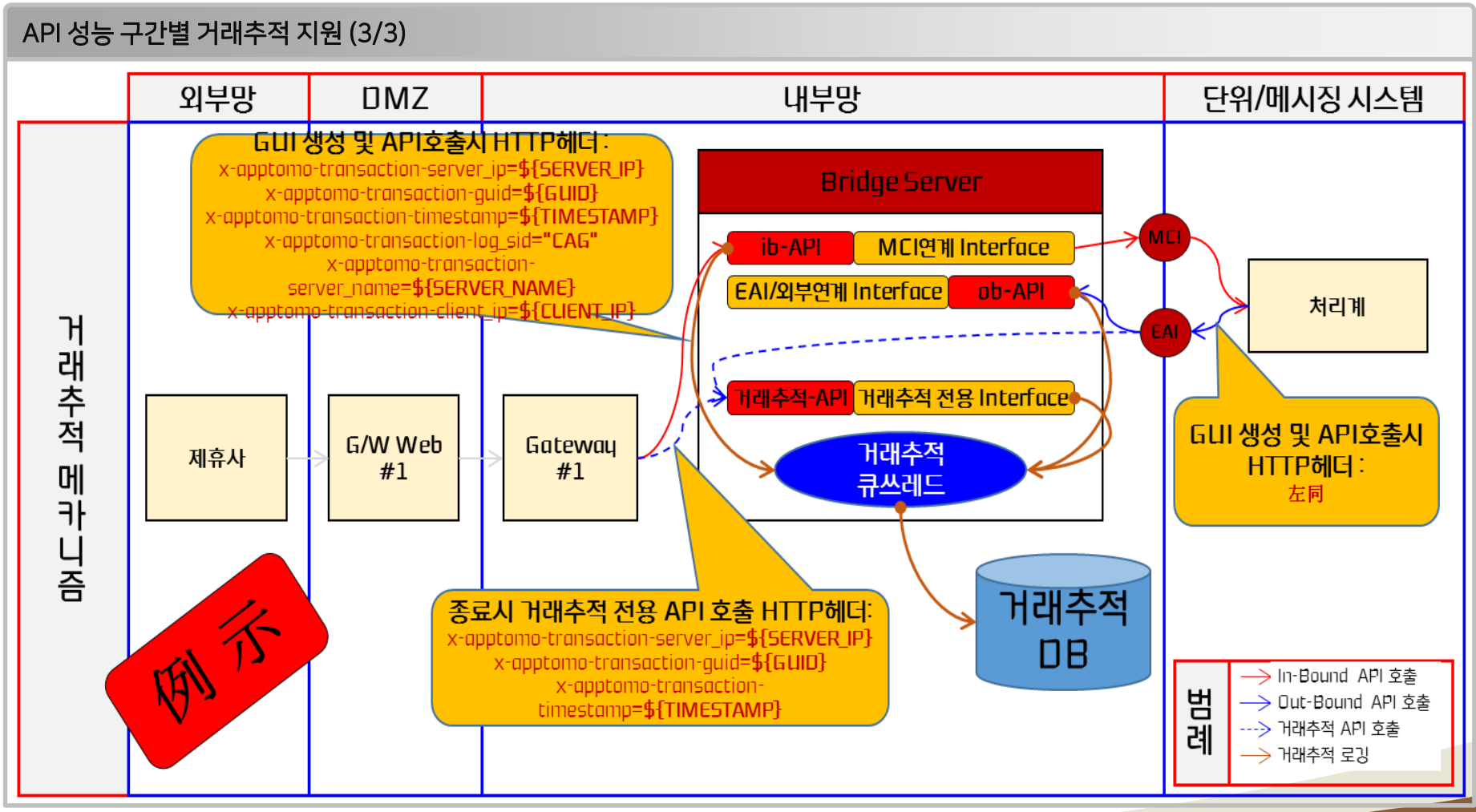


구분	API_ITF90001	API_ITF90002	API_ITF90003	API_ITF90004	API_ITF90005	API_ITF90006
설명	회원인증(비밀번호체크)	현금서비스한도조회	현금서비스 즉시한도상향 대상여부 조회	현금서비스 즉시한도상향 신청	금융서비스 신청정보	은행계좌입금
PREV-API SET	없음	API_ITF90001	API_ITF90002	API_ITF90003	API_ITF90004 API_ITF90006	API_ITF90002 API_ITF90003 API_ITF90005

4.7 API 성능 구간별 거래추적

각 API 호출 건에 대해 Gateway 구간에 대한 거래추적을 하기 위해, 다음과 같이 Gateway에서 API Engine로 API호출 할 때, HTTP 헤더에 추가 정보를 제공함. 또한, API Engine의 거래추적 전용 API를 호출하여 종료 관련 정보를 전달함.

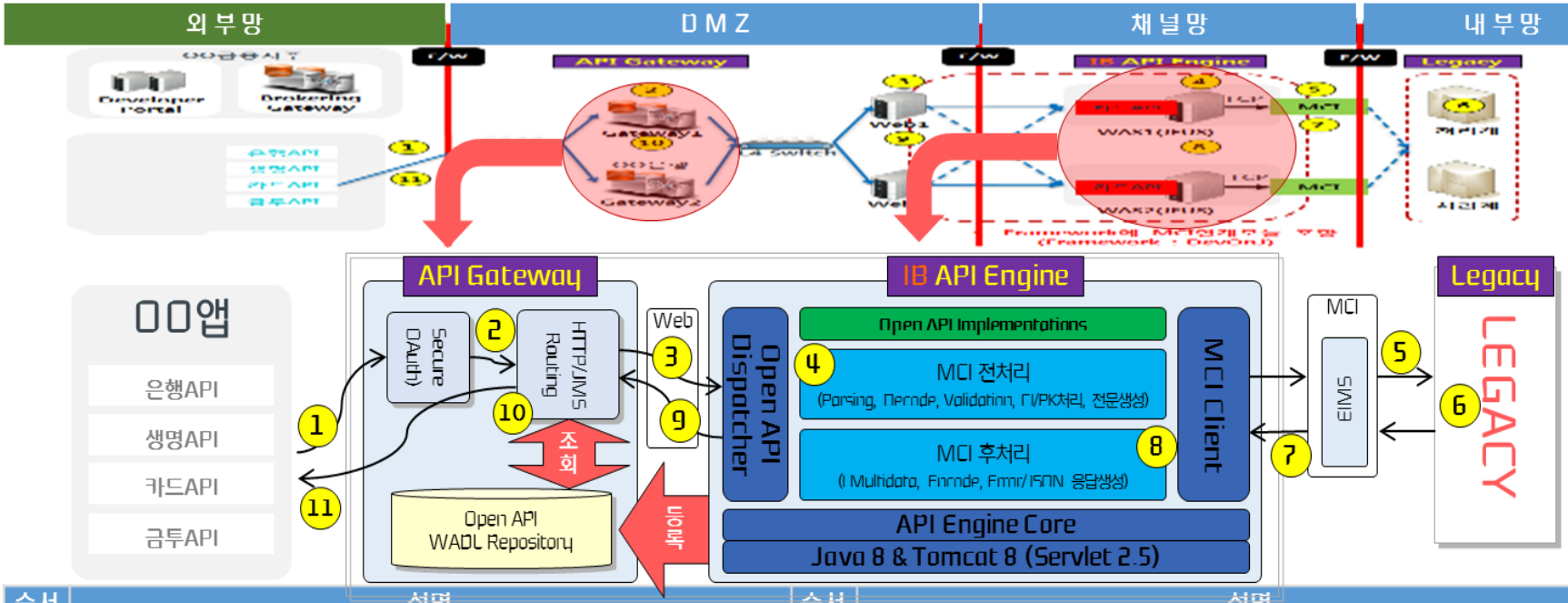
API 성능 구간별 거래추적 지원 (3/3)



4.8 In-bound/Out-bound API 관리 방안 (1/3)

API Engine은 고객사의 모든 API에 대한 end-point를 제공하며, Gateway로부터 전달받은 API에 대해 1) 전처리 작업 및 MCI 전문 생성, 2) MCI를 호출, 3) MCI 응답 후처리 및 응답 리턴 등의 작업을 수행함.

효율적인 Inbound/Outbound 관리 방안 제시 (1/3)

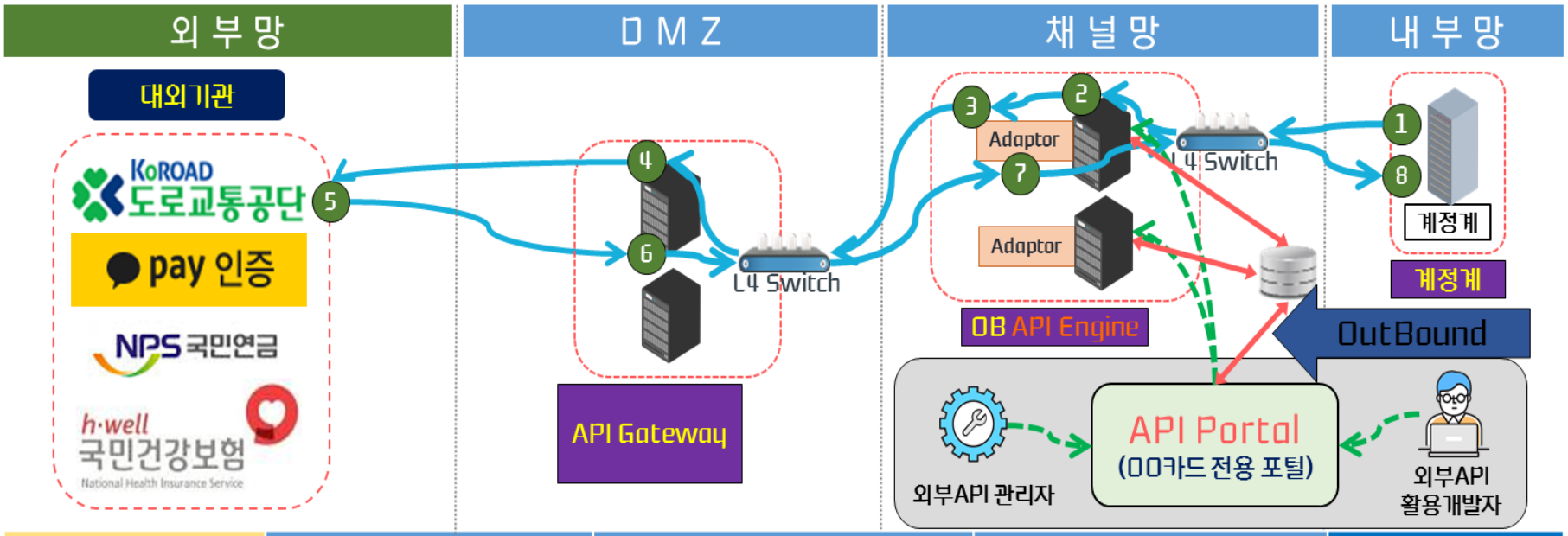


순서	설명	순서	설명
①	HTTPS를 통해 OO카드 Open API를 호출한다.	⑥	해당 서비스는 자체 로직을 실행하고, MCI에게 결과값을 리턴한다.
②	G/W는 Open API 요청을 인증하고, 유효한 요청을 WEB에 전달한다.	⑦	MCI는 리턴받은 응답 전문을, 호출한 API Engine에게 전달한다.
③	Web은 전달받은 요청을 InBound API Engine에게 전달한다.	⑧	**MCI에게 전달받은 응답 전문을 JSON데이터로 변환한 후, Web에게 응답한다.**
④	**InBound API Engine은 HTTPS 요청과 함께 전달된 Parameter를 파싱/복호화하고, 공통 CI 값을 OO카드 내부 primary key로 변환한 후, MCI를 통해 레거시를 호출합니다.**	⑨	IB API Engine으로부터 응답받은 JSON 데이터를 Gateway에게 전달한다.
⑤	InBound API Engine에게 전달받은 전문에 따라 Legacy 서비스를 실행한다.	⑩	Web으로부터 전달받은 JSON데이터를 Client에게 응답한다.
		⑪	응답받은 HTTPS 응답상태 값에 따라 JSON 데이터를 처리한다.

4.8 In-bound/Out-bound API 관리 방안 (2/3)

Out-Bound Open API Platform을 구축하면, 1) 외부 API를 연계하기 위한 OB API Engine 구축하고, 2) 외부 API를 등록 관리하기 위한 카드 전용 API Portal을 구축하며, 3) DMZ구간에 Dummy WEB(or API G/W)을 둠.

효율적인 Inbound/Outbound 관리 방안 제시 (2/3)

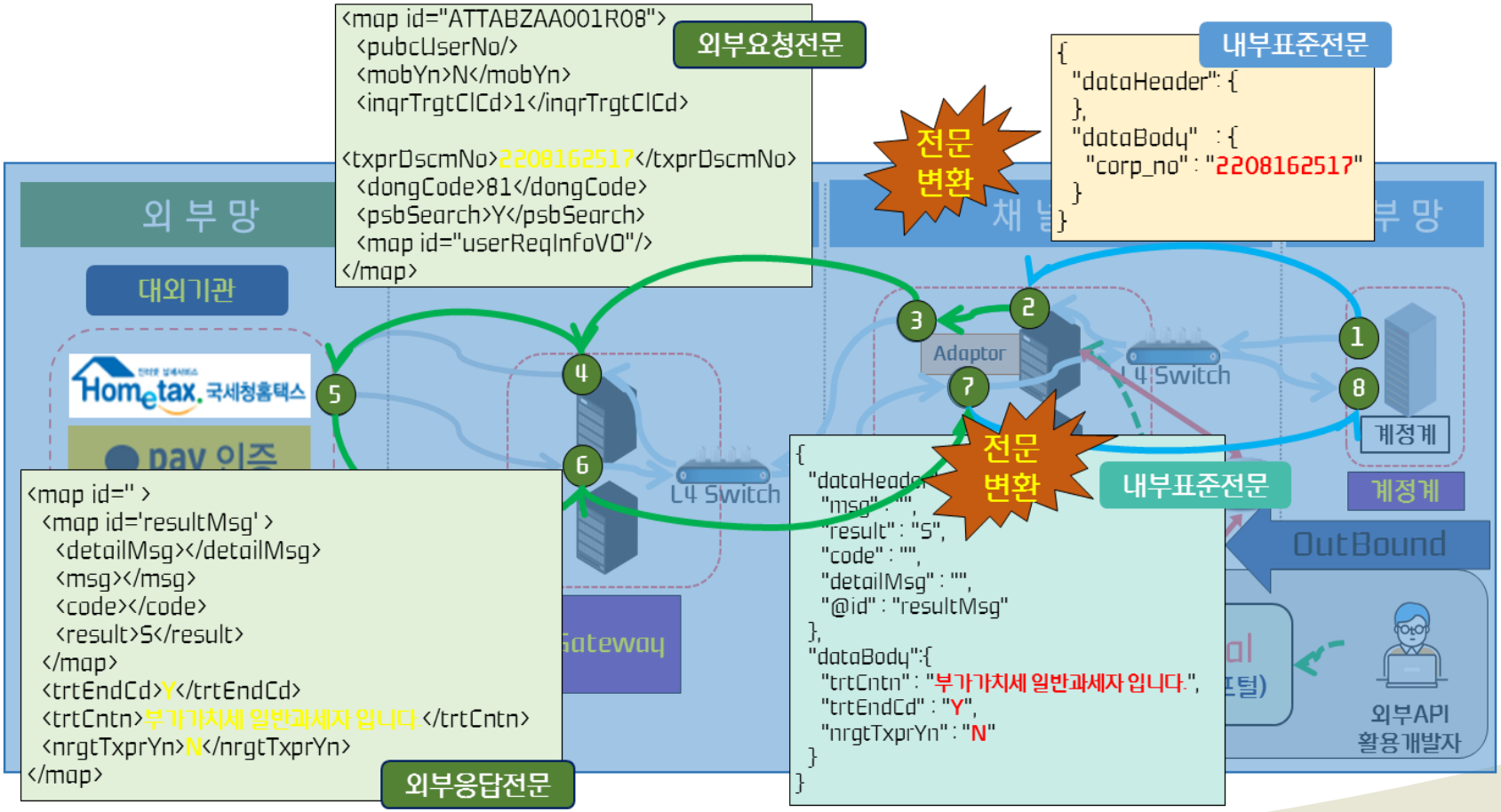


대외기관	API Gateway	API Portal	OutBound API Engine	API관리자/개발자, API활용시스템
• JSON/XML데이터 REST API 제공 • HTTP/HTTPS 통신 • KEY, OAuth2.0 인증 • 인증/보안 프로세스	• 외부 API 호출 연계 • API G/W 활용 가능 ➔ API G/W : 인증, 라우팅	• 사용자 권한 관리 (SSO연동) • 사용자/Consumer 승인/거절 • API 등록/사용 승인/거절 • API현황 대시보드/통계 • API 탐색/명세/테스트 • API 개발지원 (게시판/Q&A/포럼)	• 대응답(MockUp) API • 체이닝거래 제어/거래추적 • IN/OUT 파라메터 관리 • 전문(JSON/XML/RAW) 변환 • 대내/대외 연동 프로토콜 지원 • 대내/대외 연동 Adaptor 지원	• 외부API 관리자 • 외부API활용 개발자 • 외부API활용 시스템

4.8 In-bound/Out-bound API 관리 방안 (3/3)

"국세청 법인 휴·폐업 여부 조회" 서비스를 사용하기 위해, 1) 내부 JSON전문을 국세청 서비스 전용 요청 전문으로 변환 해 주고, 2) 국세청 서비스 응답 전문을 내부 JSON전문으로 변환해 줌.

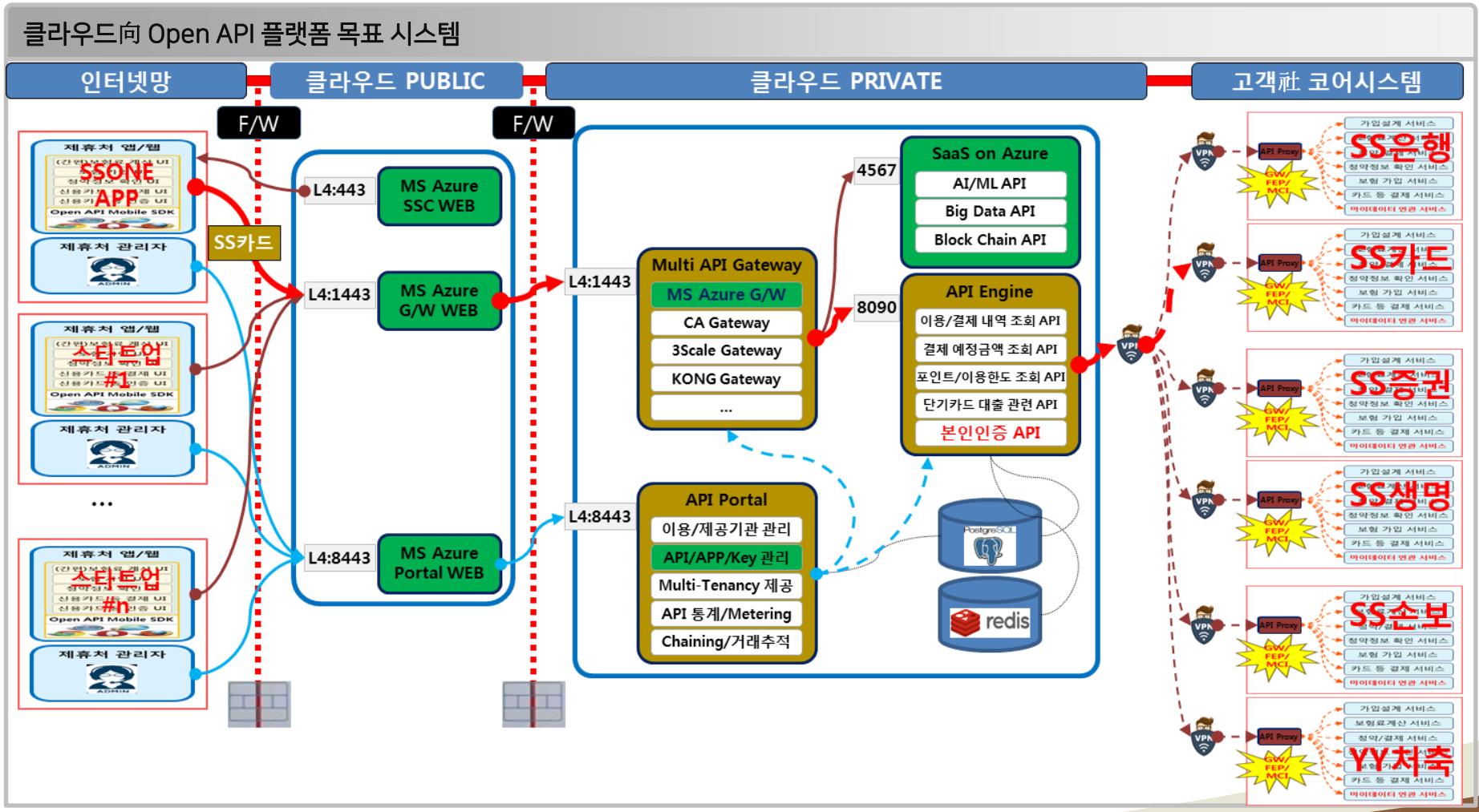
효율적인 Inbound/Outbound 관리 방안 제시 (3/3)



오픈 API관리 시장 전망

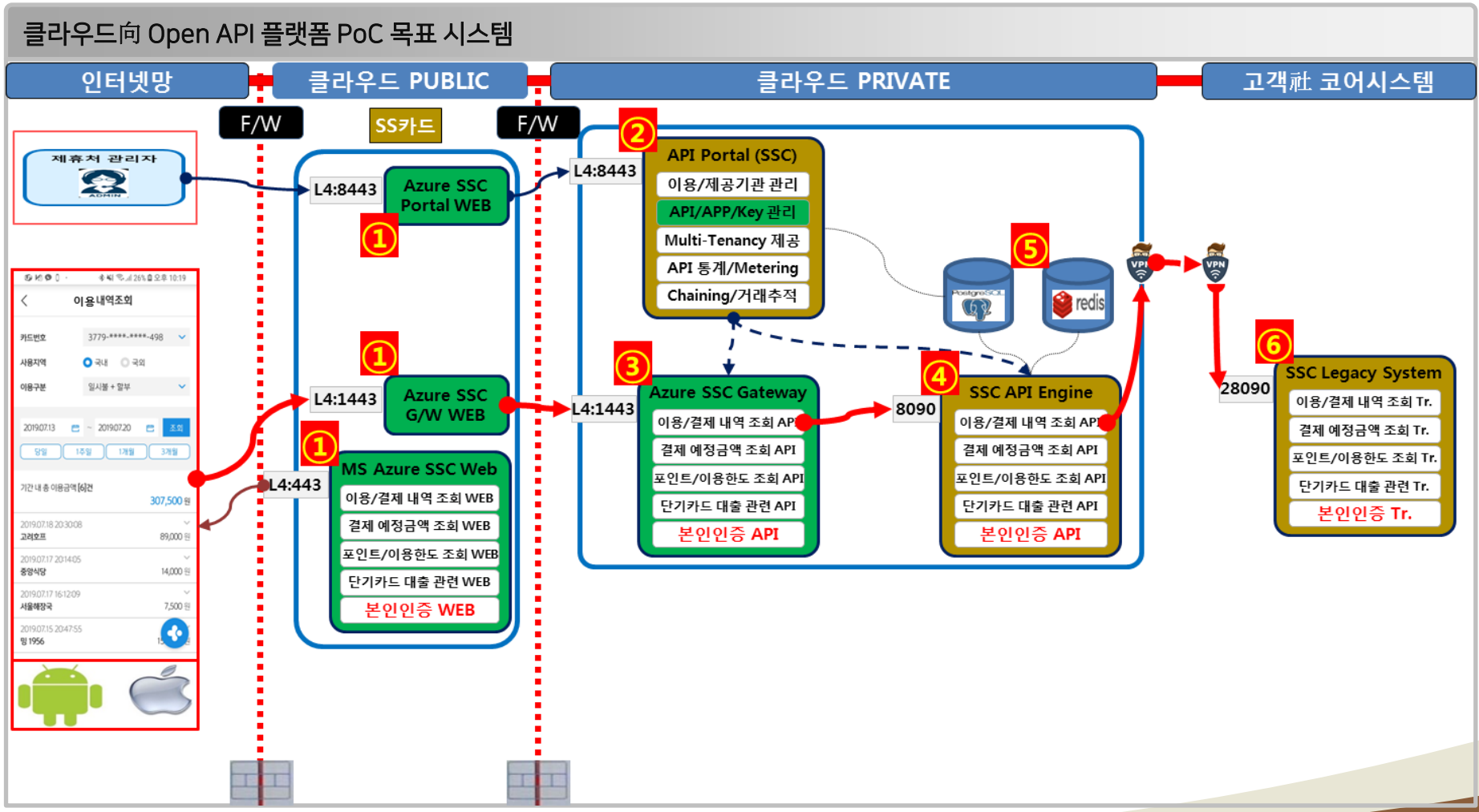
5.1 Open API Platform as a Service

대한민국 금융, 물류, 제조 등 기업의 데이터 및 서비스를 Open API로 제공하기 위해, 상용 클라우드 내에 API Gateway, API Portal, API Engine 등을 구성하고, API Engine은 VPN으로 FEP를 통해서 기업의 레거시 및 원장을 연계함.



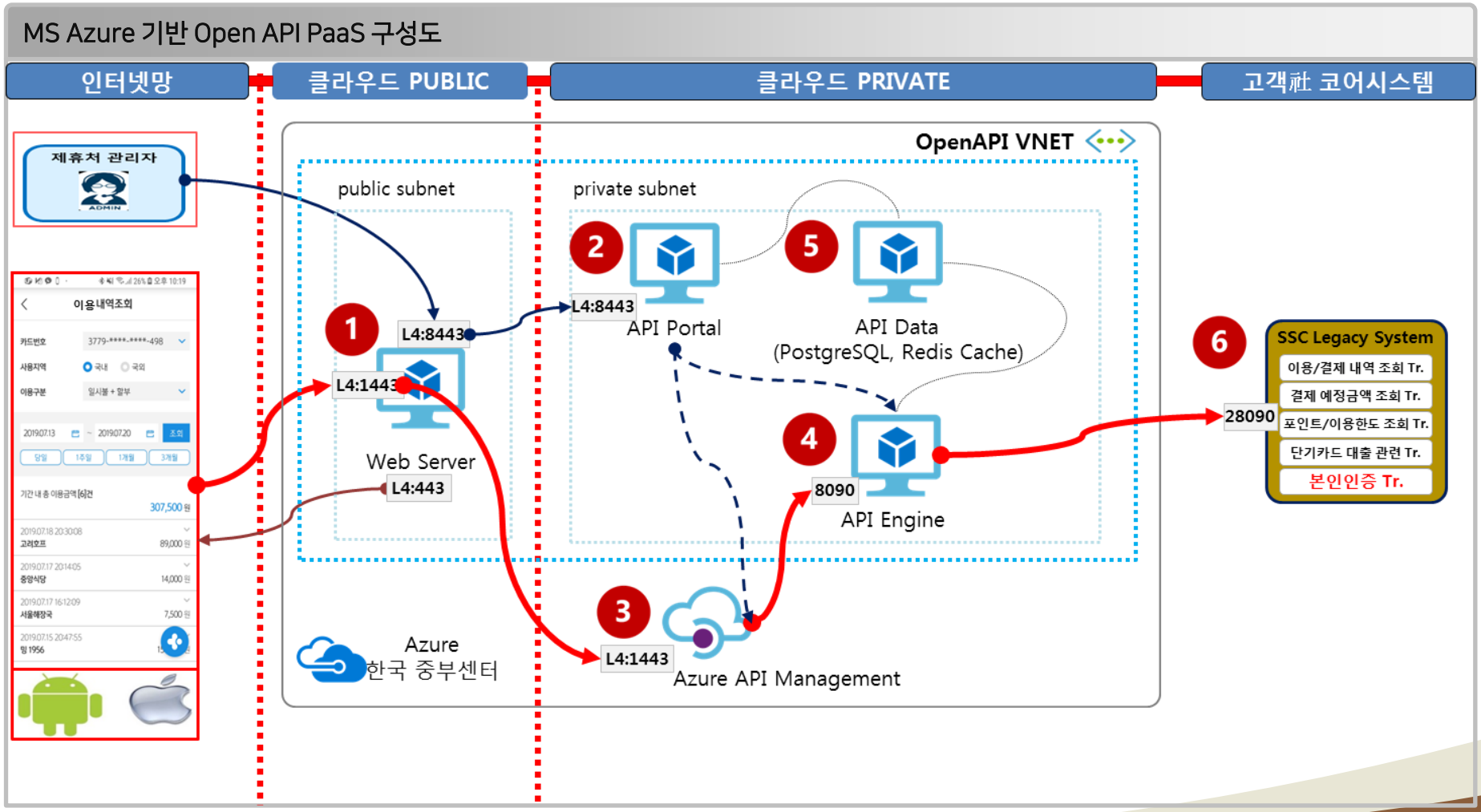
5.2 Open API PaaS 구성도 (1/3)

"Open API PaaS" 시스템은 상용 클라우드 내에, ① G/W Web 및 Portal Web 등을 위한 VM, ② API Portal VM, ③ G/W VM, ④ API Engine VM, ⑤ APIM Data VM 등을 구성. 클라우드의 VPN(보안망)을 통한 ⑥ 레거시 시스템 연계함.



5.2 Open API PaaS 구성도 - MS Azure 기반 (2/3)

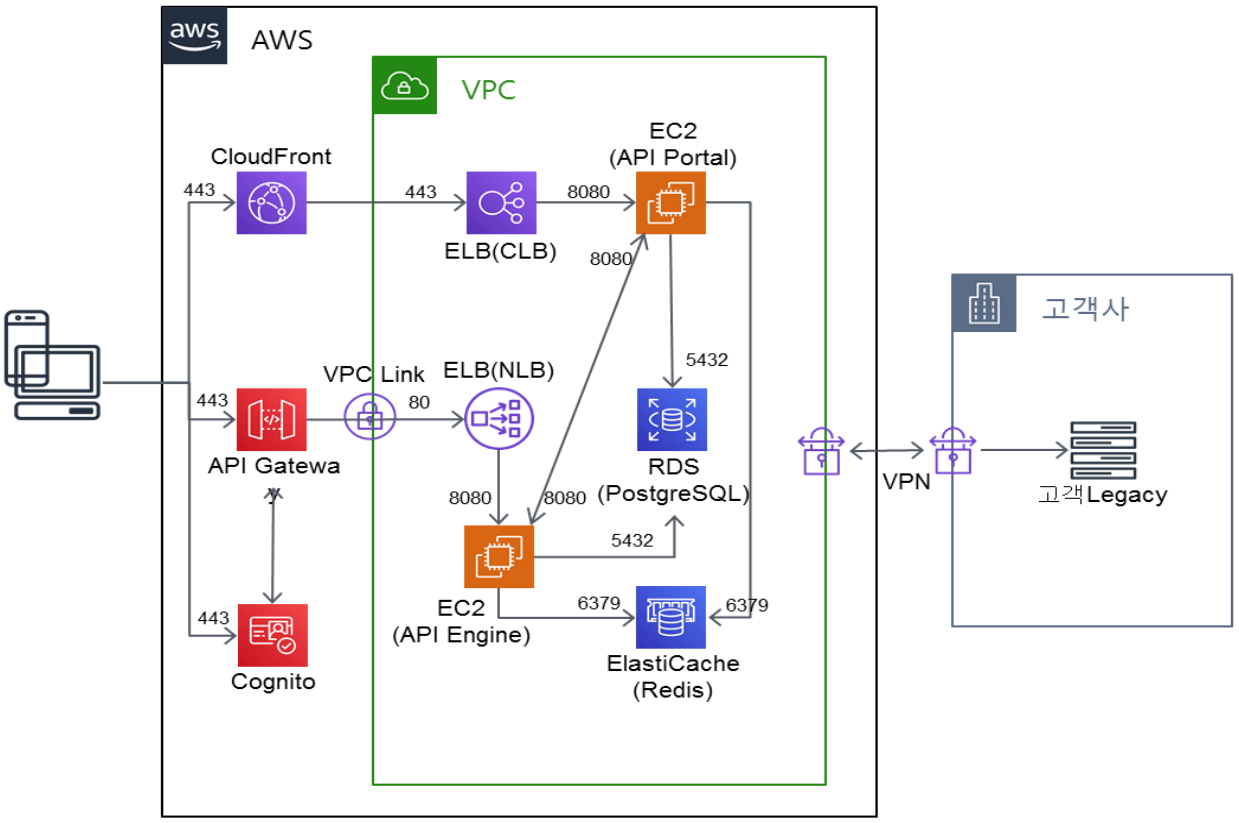
"Open API PaaS" 시스템은 상용 클라우드 내에, ① G/W Web 및 Portal Web 등을 위한 VM, ② API Portal VM, ③ G/W VM, ④ API Engine VM, ⑤ APIM Data VM 등을 구성. 클라우드의 VPN(보안망)을 통한 ⑥ 레거시 시스템 연계함.



5.2 Open API PaaS 구성도 - AWS 기반 (3/3)

"Open API PaaS" 시스템은 상용 클라우드 내에, ① G/W Web 및 Portal Web 등을 위한 VM, ② API Portal VM, ③ G/W VM, ④ API Engine VM, ⑤ APIM Data VM 등을 구성. 클라우드의 VPN(보안망)을 통한 ⑥ 레거시 시스템 연계함.

AWS 기반 Open API PaaS 구성도



+ AWS 구성 내역

- **CloudFront**
  AWS CDN 솔루션 이며 WAF, Shield 기능을 제공
  (본 PoC에서 제외될 수 있음)
- **API Gateway**
  애플리케이션이 백엔드 서비스의 데이터, 비즈니스 로직 또는 기능에 액세스 할 수 있도록 '관문' 역할을 하는 REST API 를 제공
- **Cognito**
  웹 및 모바일 앱에 대한 인증, 권한 부여 및 사용자 관리를 제공
- **VPC Link**
  API Gateway 프라이빗 통합으로 VPC 외부 클라이언트의 액세스를 위해 Amazon VPC 뒤의 리소스 연결 제공
- **Elastic Load Balancing (CLB, NLB)**
  애플리케이션 트래픽을 인스턴스와 같은 여러 대상에 자동으로 분산하는 기능을 제공
- **EC2 (API Portal, API Engine)**
  - Type : t3.large
  - OS : CentOS 7.3
  - EBS : 20G
- **RDS**
  - Type : db.t3.large
  - Engine : PostgreSQL 9.6.9
  - EBS : 20G
- **ElastiCache**
  - Type : cache.t2.medium
  - Engine : Redis 5.0

5.3 Open API PaaS 시스템 사양

"Open API PaaS" 시스템은 상용 클라우드 내에, ① G/W Web 및 Portal Web 등을 위한 VM, ② API Portal VM, ③ G/W VM, ④ API Engine VM, ⑤ APIM Data VM 등을 구성. 클라우드의 VPN(보안망)을 통한 ⑥ 레거시 시스템 연계함.

클라우드向 Open API 플랫폼 목표 시스템 사양

VM구분	S/W 구분	솔루션 구분	파일 형태	용량 (MB)	디렉토리
VM #1 (SSC Web)	OS	CentOS 7.3	-	-	
	Web Serverr	Apache Web Server			
		CPU:8core, MEM:16GB, DISK:20GB			
VM #2 (API Portal)	OS	CentOS 7.3	-	-	
	Java	Java 1.8	rpm파일	345	
	WAS	apache-tomcat-8.5.4	rpm파일	10	/sw/tomcat/portal
	API Portal	apptomo.APIP.v4.0	war파일	200	/sw/apptomo/portal
	기타 로그 디렉토리			100	/logs/portal
		CPU:8core, MEM:16GB, DISK:20GB		655	
VM #3 (API Gateway)	OS	-	-	-	
	API Gateway	MS Azure Open API Gateway	rpm파일	15	/sw/gateway
		CPU:8core, MEM:16GB, DISK:20GB			
VM #4 (API Engine)	OS	CentOS 7.3	-	-	
	Java	Java 1.8	rpm파일	345	
	WAS	apache-tomcat-8.5.4	rpm파일	10	/sw/tomcat/engine
	API Portal	apptomo.APIE.v4.0	war파일	200	/sw/apptomo/engine
	기타 로그 디렉토리			100	/logs/engine
		CPU:8core, MEM:16GB, DISK:20GB		655	
VM #5 (API Data)	OS	CentOS 7.3	-	-	
	Java	Java 1.8	rpm파일	345	
	DBMS	postgresql96-server-9.6.9	rpm파일	1,024	
			DB데이터	10,240	
	Cache	Redis	tar파일	66	
		CPU:8core, MEM:32GB, DISK:40GB		11,675	
VM #6 (SSC Legacy System)	OS	Windows 7	-	-	
	Java	Java 1.8	rpm파일	345	/sw/apptomo/legacy
	Java Application	TCP/IP Server Application	zip 파일	50	
		CPU:8core, MEM:16GB, DISK:20GB		395	

On-Prem. 오픈 API 구축 사례

6.1 Open API 금융권 구축 사례

국내 금융권 오픈API플랫폼 구축 사례를 살펴보면 다음과 같습니다. 오픈API 플랫폼을 구축하기 위해 API Gateway, API Portal, API Engine 등을 도입합니다.

Open API 금융권 구축 사례

고객사	사업명	시기	기간	구축 제품			수행사	특징	비고
				API Gateway	API Portal	API Engine			
손해보험	AWS 기반의 오픈API 플랫폼 구축	2019.09	1개월	AWS	AppTomo	AppTomo	유니버셜리얼타임	AWS 기반 Open API 플랫폼 구축, VPN을 통한 레거시 연계	구축중
은행	오픈API 플랫폼 구축	2019.09		CA	UNO		유앤아워스	우리은행 레퍼런스를 그대로 벤치마킹	우선협상중
캐피탈	API플랫폼 구축	2019.10	3개월	CA	AppTomo	AppTomo	유앤아워스		우선협상중
공제조합	오픈API 플랫폼 구축	2019.07	4개월	D-Bridge			싸이버이매지네이션	Open API를 통한 조합 연계	구축중
증권	오픈API 플랫폼 구축	2019.07		IBM			모코엠시스		구축중
생명	클라우드 기반의 오픈이노베이션 시스템 구축	2019.07	4개월	CA	AppTomo	AppTomo	베스핀글로벌	핀테크 업체에게 클라우드 DevOps 개발 환경 제공	구축중
화재	B2B2C 표준 플랫폼 구축 2단계	2019.06	8개월	CA	UNO		유앤아워스	B2B2C 고도화	2단계
생명	OPEN API 시스템 구축	2019.05	4개월	D-Bridge			사이버이메지네이션	TOSS 연계를 위해 Open API로 제공	구축완료
은행	오픈API 플랫폼 구축	2019.02	6개월	CA	UNO		유앤아워스	GitHub 기반의 개발리소스 및 핀테크블로그 제공	구축완료
손보	일반보험 오픈 API 시스템 개발	2019.02	4개월	D-Bridge			사이버이메지네이션	파일럿	구축완료
뱅크	제휴사 연계를 위한 API플랫폼 구축	2018.11	6개월	ZUUL	UNO		알앤비소프트	Netflex의 게이트웨이 ZUUL을 커스터마이징	구축완료
멤버스	오픈 API 플랫폼 구축	2018.10	4개월	CA	UNO		일루텍코리아	대외 제휴사와의 인터페이스 표준화	구축완료
은행	IBK BOX 플랫폼 구축	2018.08	6개월	CA, IBM	UNO		프리커스	중소기업 경영지원 디지털 플랫폼 구축의 일환	구축완료
은행	오픈 API 플랫폼 구축	2018.07	6개월	CA	UNO		유앤아워스	독자 오픈 API 플랫폼을 중심으로 서비스를 내재화	구축완료
화재	B2B2C 표준 플랫폼 구축	2018.06	8개월	CA	UNO		유클릭	정부의 규제완화에 따른 B2B2C 신규 판매채널 확대	구축완료
생명	오픈 API 플랫폼 구축	2018.06	4개월	CA	UNO		프리커스		구축완료
카드	API Engine 도입 사업	2018.06	3개월			AppTomo	유니버셜리얼타임	Open API 대응 내부 시스템 채널과 연계 기반 마련	구축완료
카드	오픈 API 플랫폼 구축	2018.04	3개월	CA	UNO		유앤아워스		구축완료
은행	Open API 기반의 위비톡3.0 구축	2017.12	3개월	CA	UNO		유앤아워스		구축완료
생명	해커톤 수행을 위한 Open API 시스템 구축	2017.09	3개월	KONG	AppTomo	AppTomo	LG CNS	해커톤용 오픈API플랫폼 구축	구축완료
은행	오픈 API 플랫폼 구축	2017.09	4개월	CA	UNO		유앤아워스	혁신적인 비즈니스 모델 개발을 위한 개방형 금융플랫폼	구축완료
카드	Open API 플랫폼 구축	2017.06	6개월	CA	UNO		제네시스	데이터 허브로써의 API 플랫폼 구축	구축완료
Bank	Open Bank Platform 구축	2017.03	4개월	CA	UNO		유앤아워스	Open Bank Service 및 플랫폼 연동	구축완료
금융그룹	그룹 Open API 플랫폼 구축	2016.12	3개월	CA	UNO		유앤아워스	8개 그룹사별 API 구축 및 외부 API 연동	구축완료
금융그룹	오픈API 표준 플랫폼 구축	2016.08	6개월	CA	UNO	AppTomo	유앤아워스	5개 계열사, Shared Platform 구축	구축완료
코스콤	자본시장 공동 핀테크 오픈플랫폼 구축	2016.03	4개월	CA	UNO		유앤아워스	국내 14개 금융투자회사가 공동 구축	구축완료
금융결제원	은행권 공동 핀테크 금융플랫폼 구축	2016.01	4개월	CA	UNO		일루텍코리아	시중 16개 은행이 참여	구축완료
은행	NH핀테크 오픈플랫폼 구축	2015.05	7개월	In-house			웹캐시	은행권 최초로 'NH핀테크 오픈플랫폼'을 구축	구축완료

6.2 주요 Open API 개발자 포탈

국내 금융권 오픈API플랫폼 구축 사례를 살펴보면 다음과 같습니다. API Gateway를 도입하고, API를 개발하고, API 개발자포탈을 오픈하고 있습니다.

금융권 주요 Open API 개발자 포탈

- 오픈플랫폼 : https://www.open-platform.or.kr/main
- 신한은행 : https://openapi.shinhan.com
- https://bankapi.shinhan.com/#/
- 우리은행 : https://developer.wooribank.com/intro
- KEB하나은행 : https://openapi.kebhana.com/
- KOSCOM : https://koscom.gitbook.io/open-api/
- SK : https://openapi.sk.com/
- 네이버 : https://developers.naver.com/main/