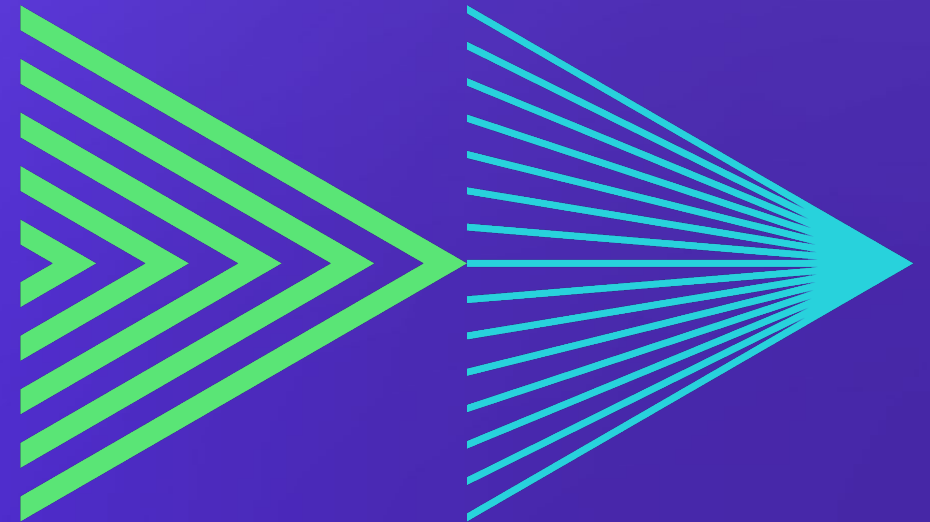


오픈소스 KeyCloak을 활용한 인증 서버 구축기

NHN Dooray 결재서비스개발팀

서태진, 한덕선



다룰 내용

1. 왜 Keycloak일까?
2. Keycloak 사용한 기능
3. 발생한 이슈 및 해결
4. 개선 방향

왜 Keycloak일까?

Single-Sign On

한 번의 로그인으로 여러 가지 사이트를 이용

기존 인증

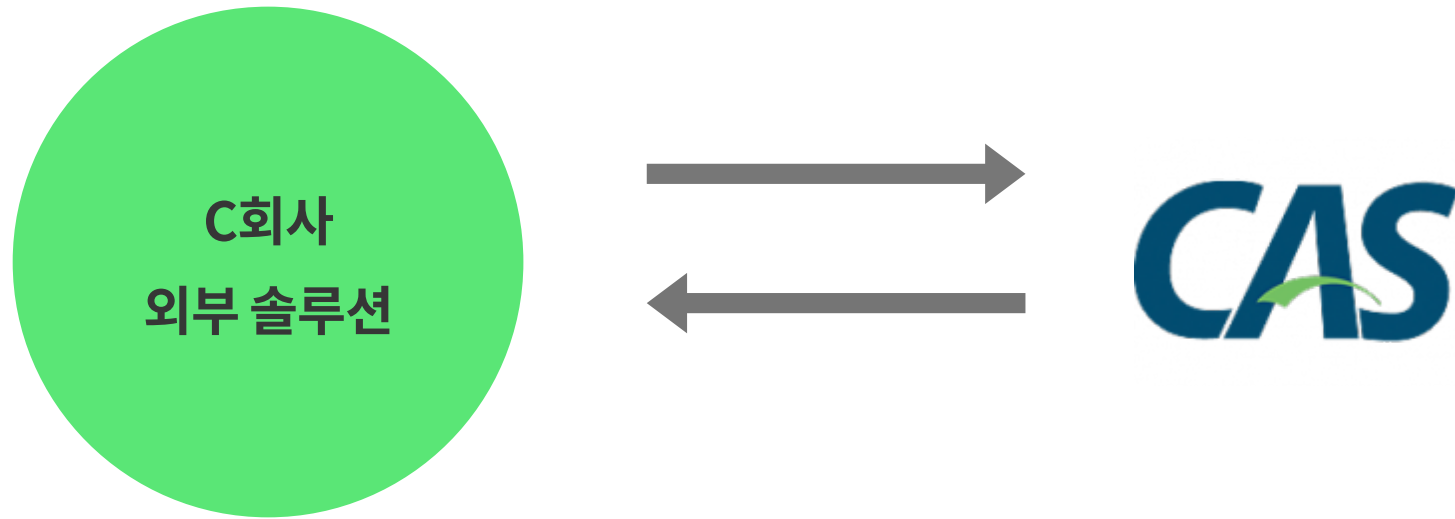


기존 인증

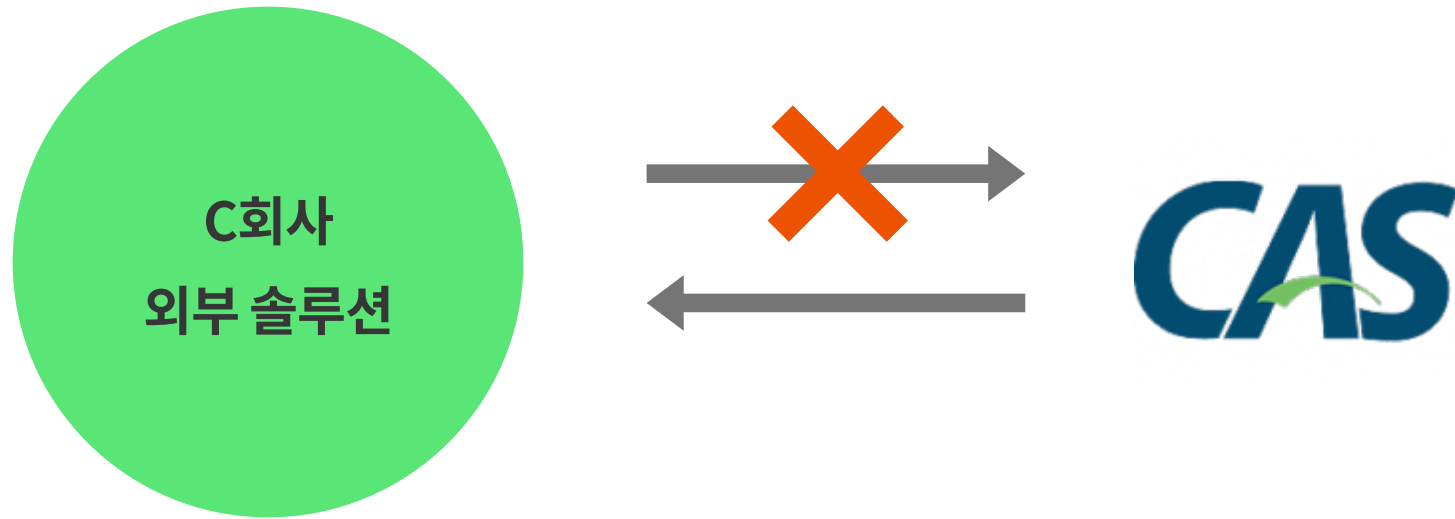
C회사
외부 솔루션



기존 인증



기존 인증



OpenSource SSO 비교



JAVA



JAVA



C#

OpenSource SSO 비교



Keycloak

JAVA
14.2k



CAS

JAVA
9.8k

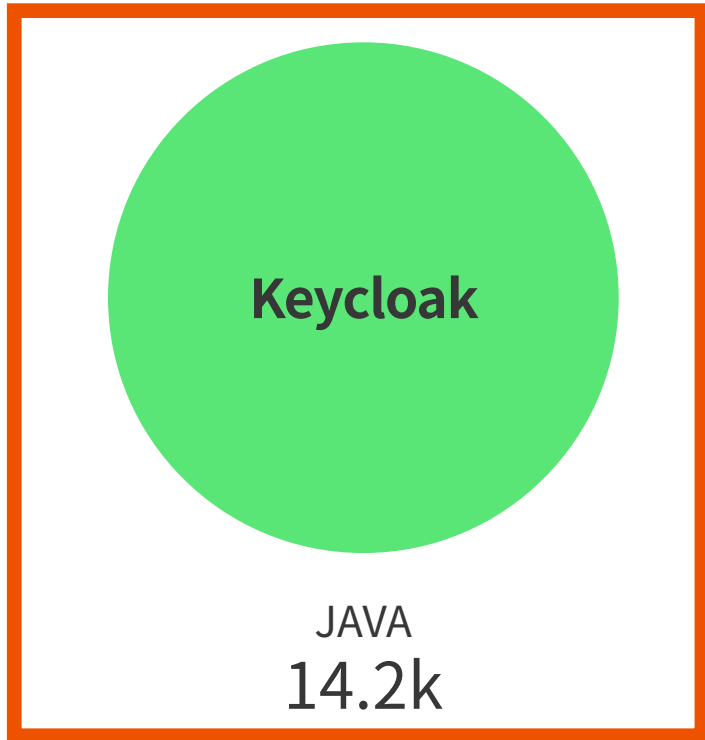


Identity Server

C#
8.9k

OpenSource SSO 비교

결정



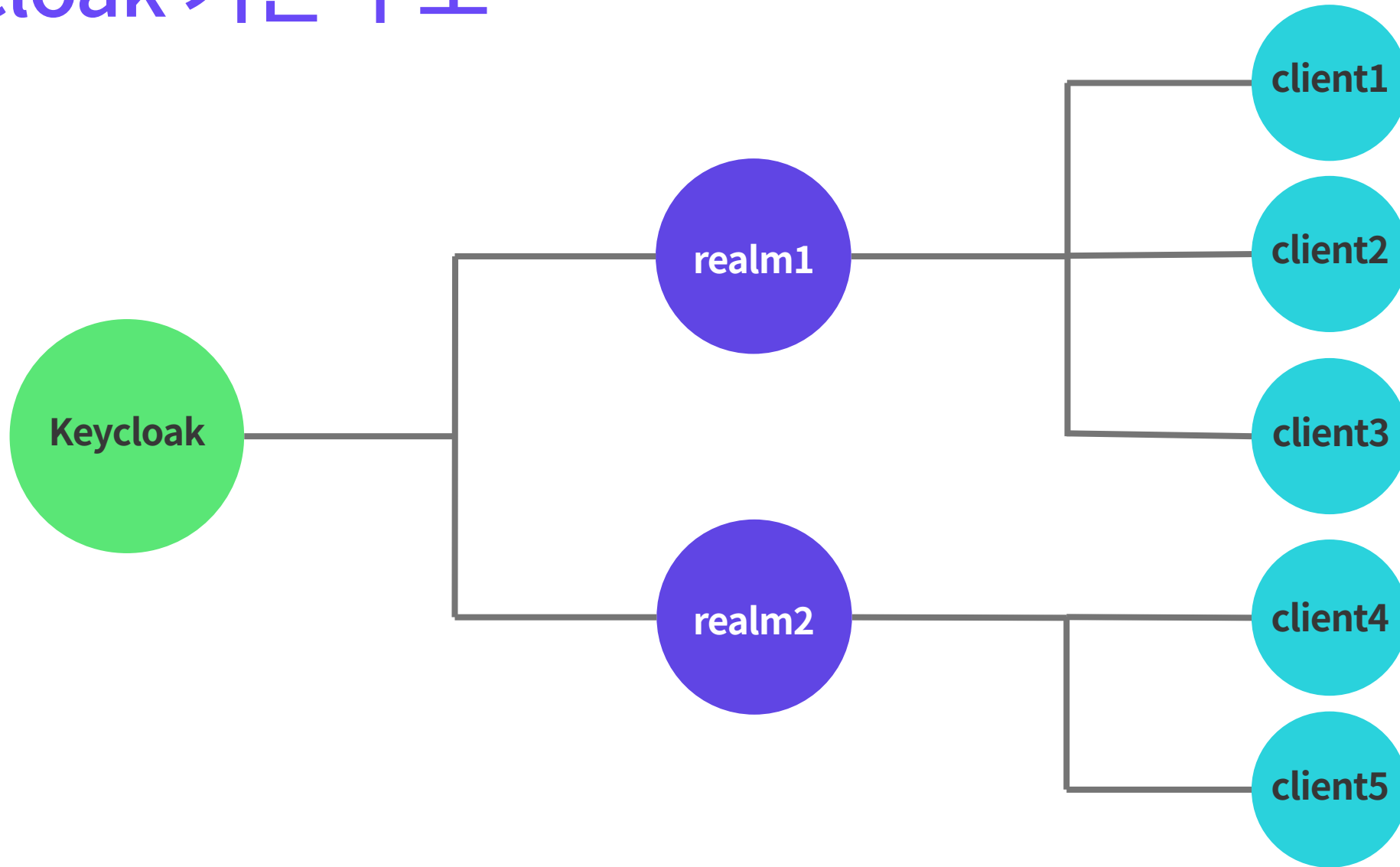
JAVA
9.8k



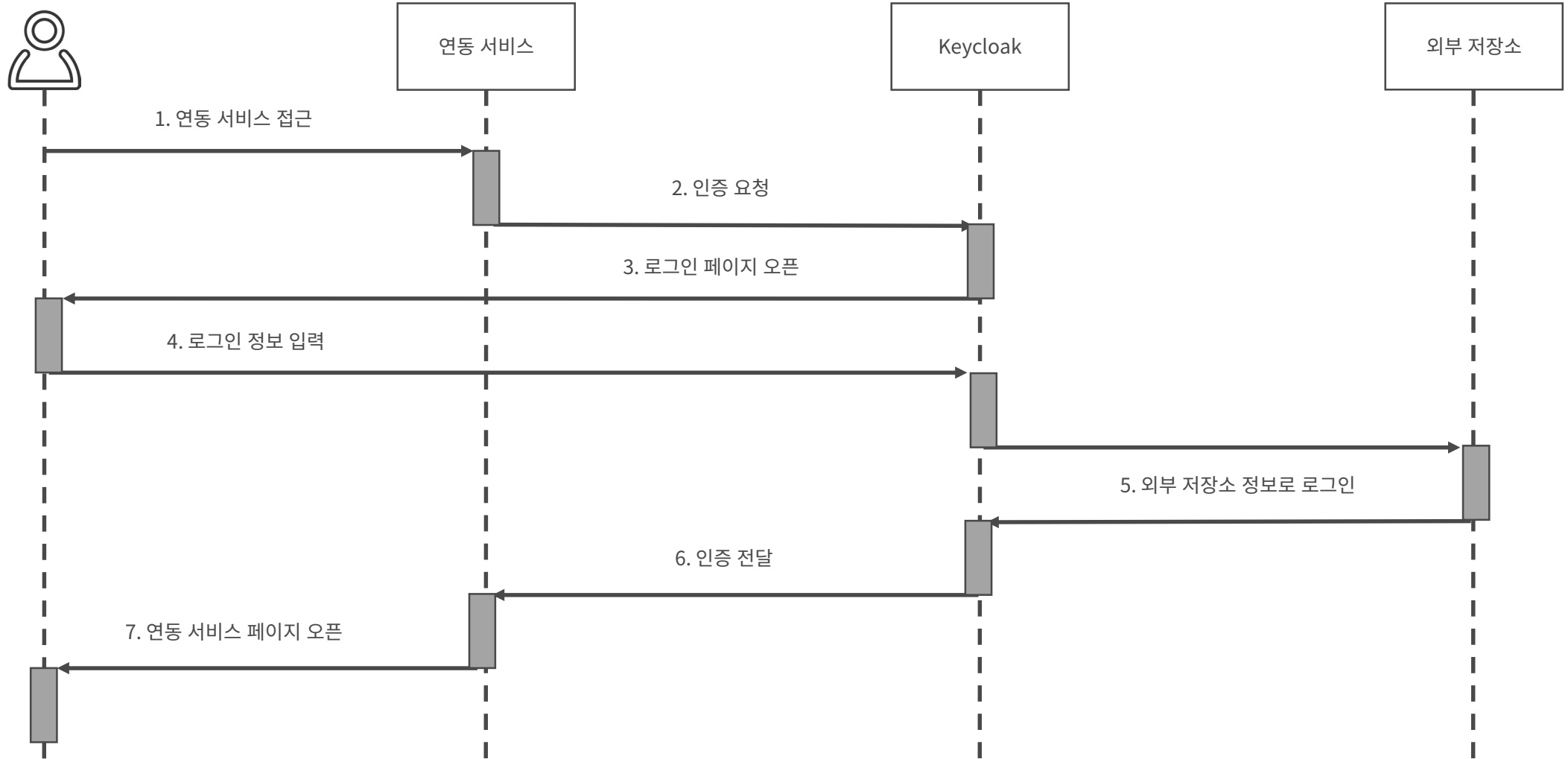
C#
8.9k

Keycloak 사용한 기능

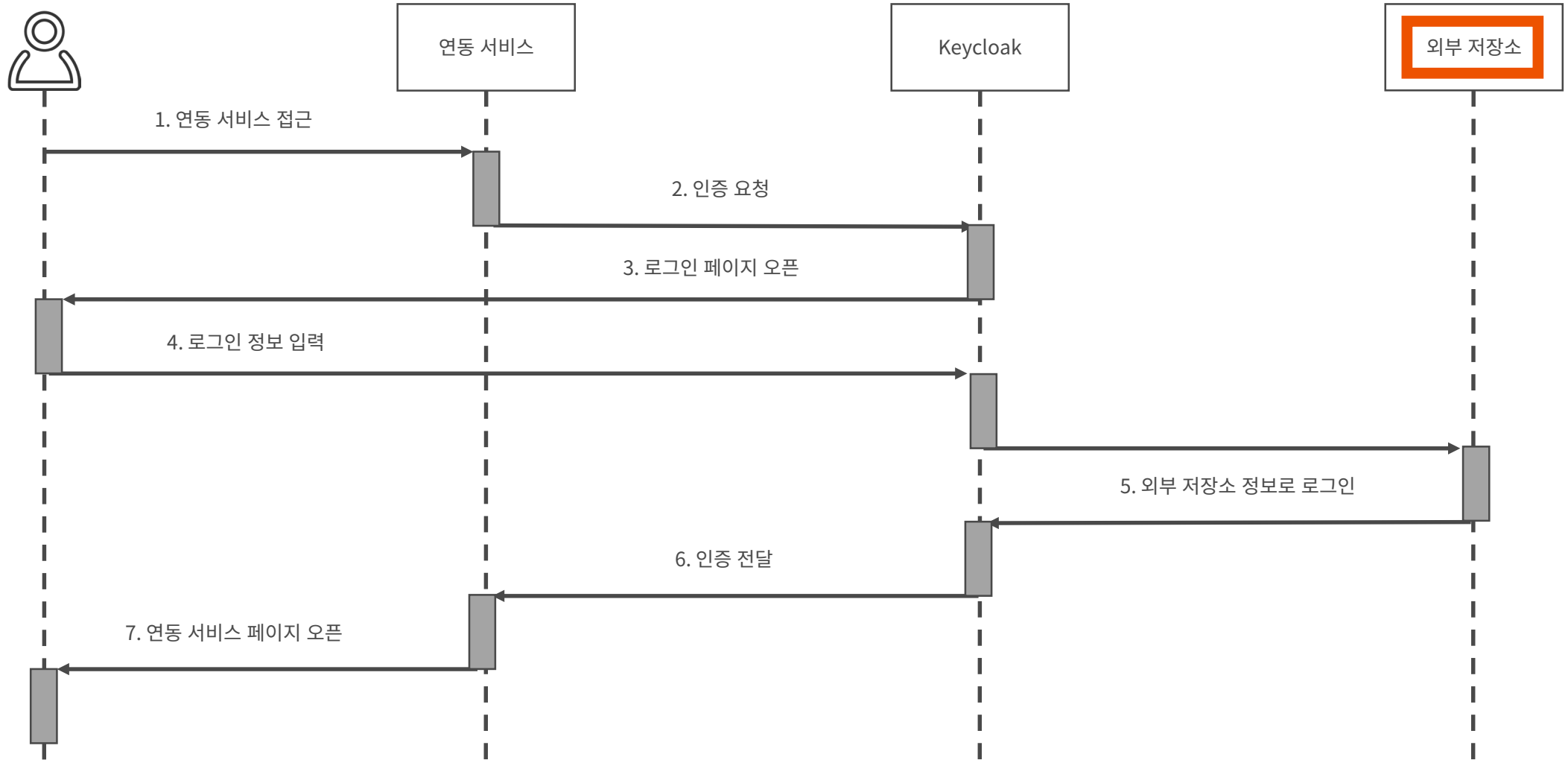
Keycloak 기본 구조



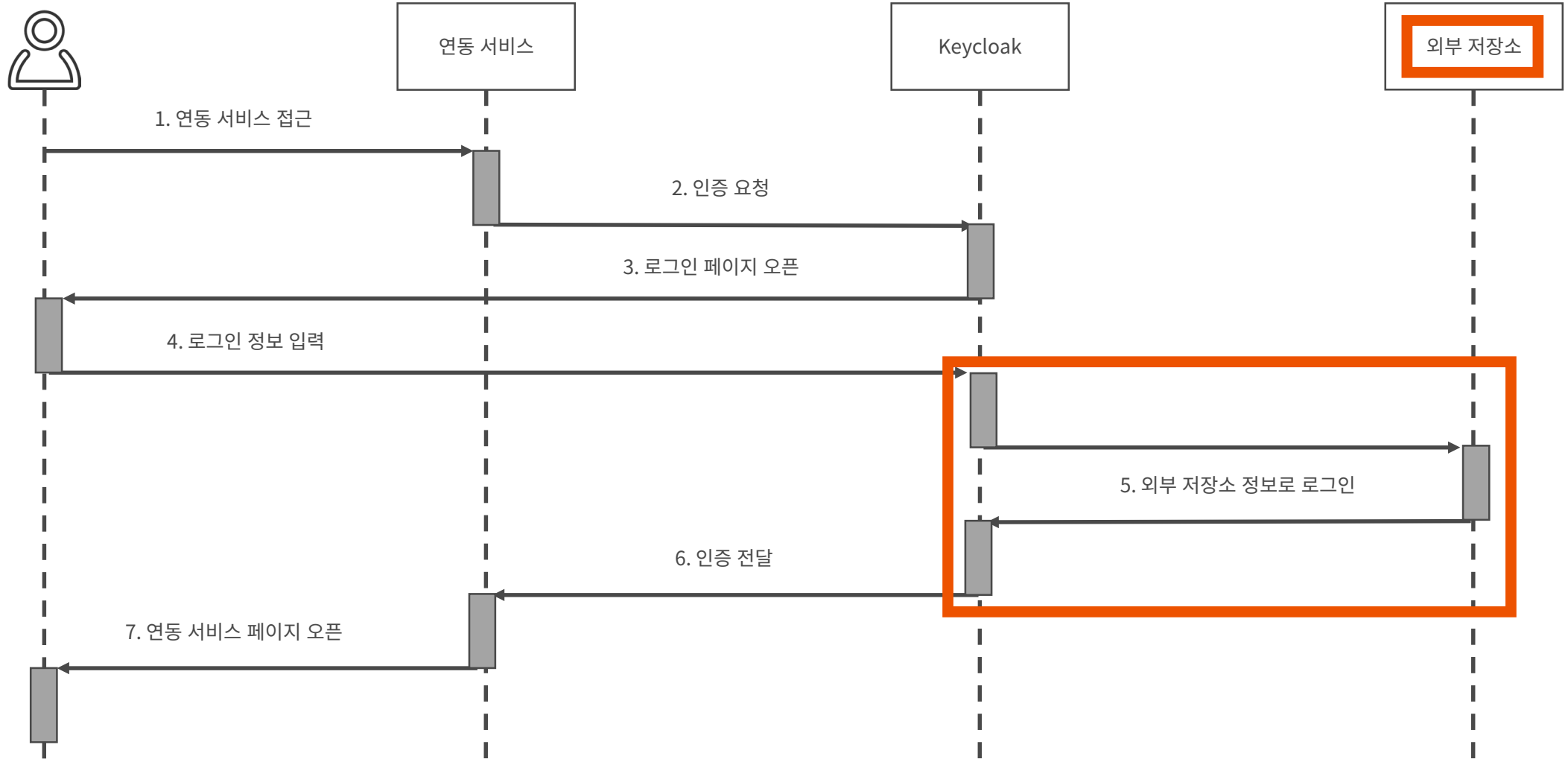
Keycloak 로그인 과정



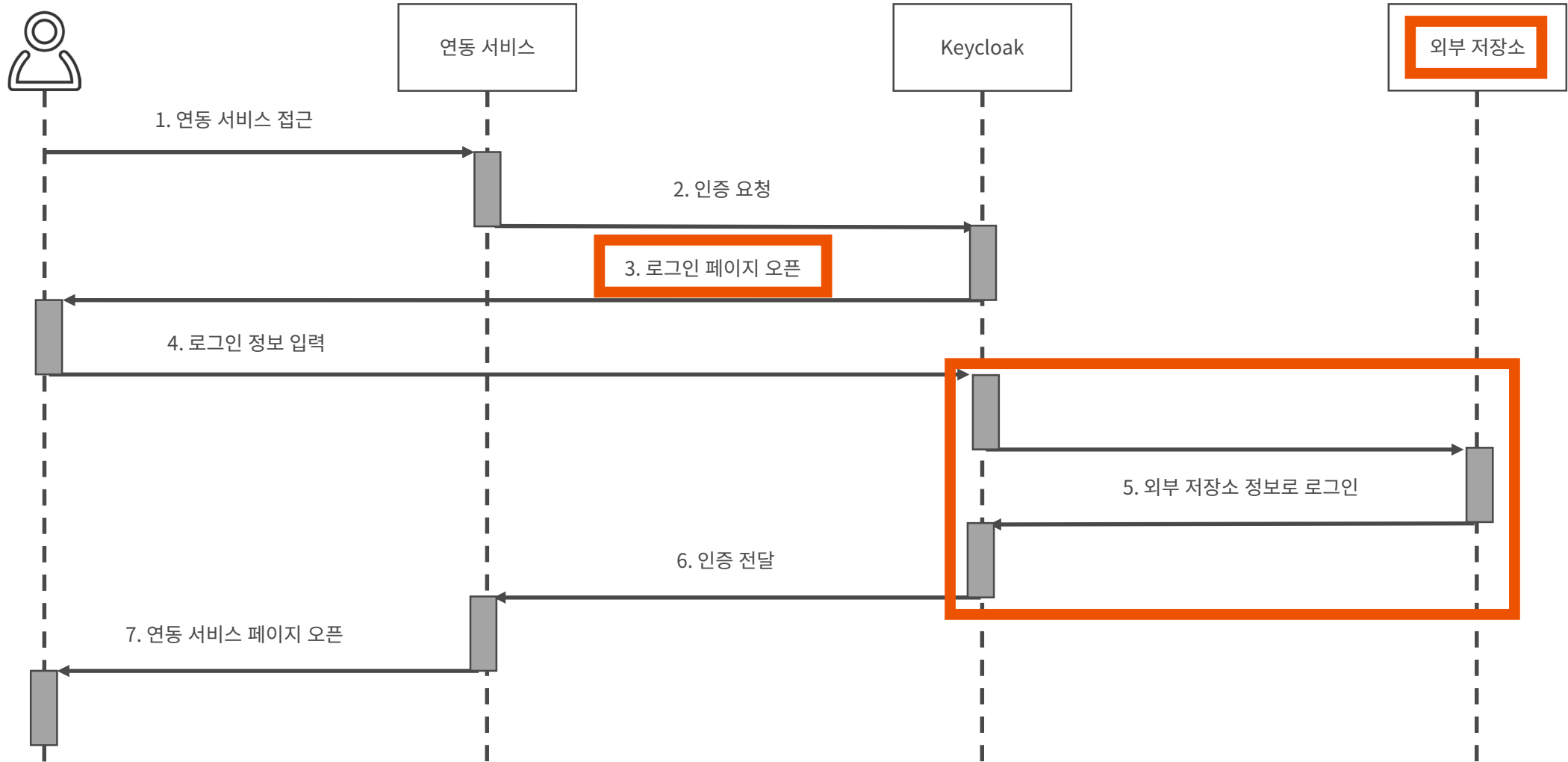
Keycloak 로그인 과정



Keycloak 로그인 과정

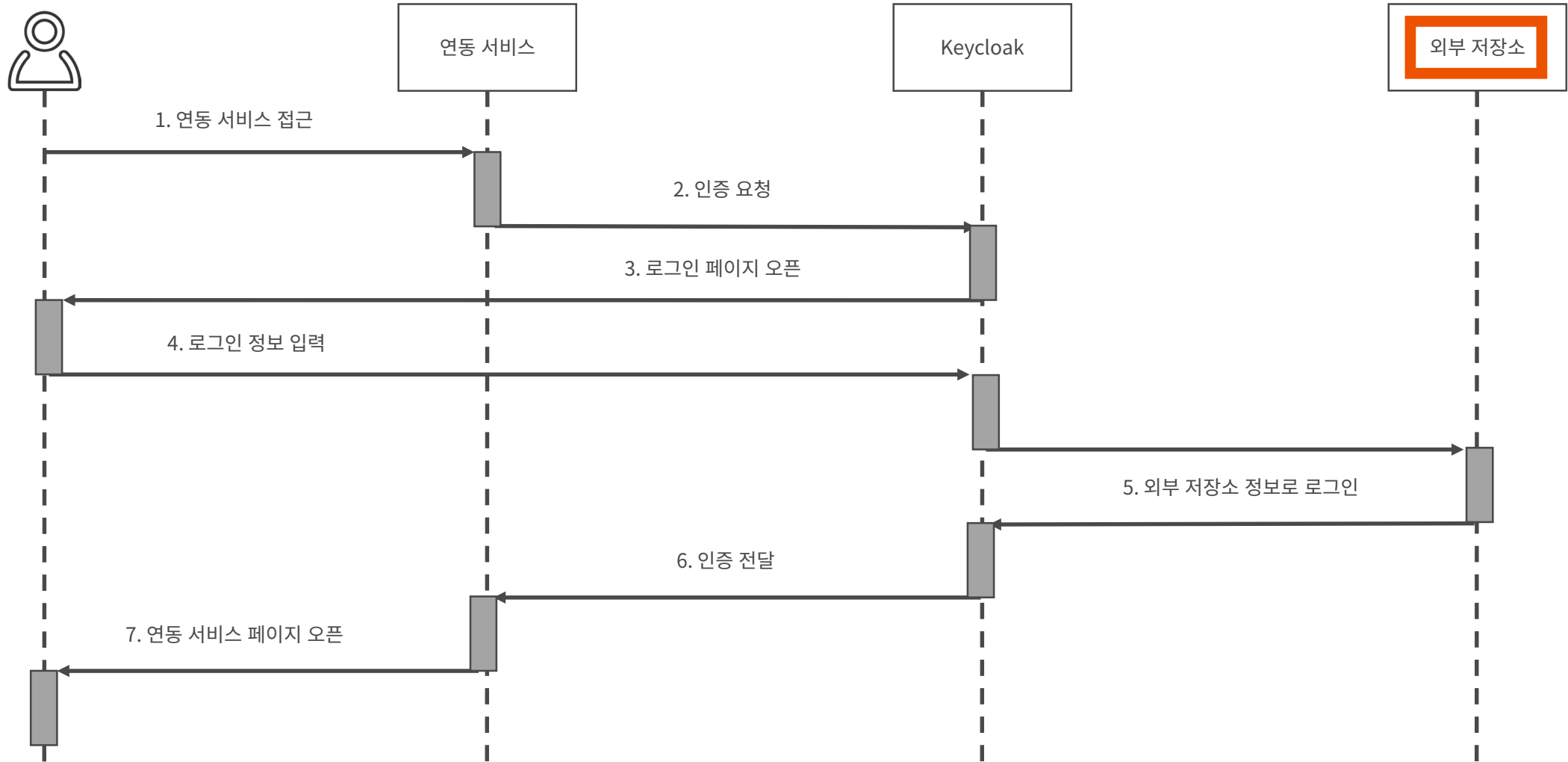


Keycloak 로그인 과정



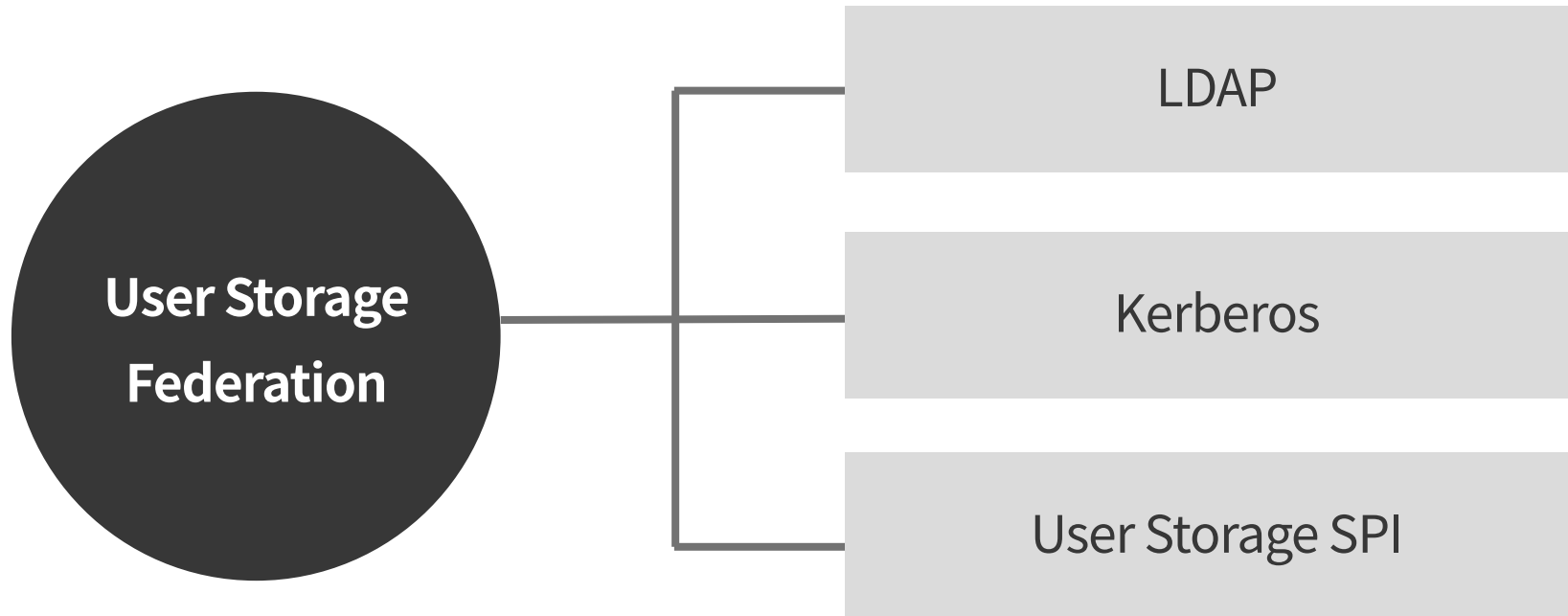
User Storage Federation

User Storage Federation



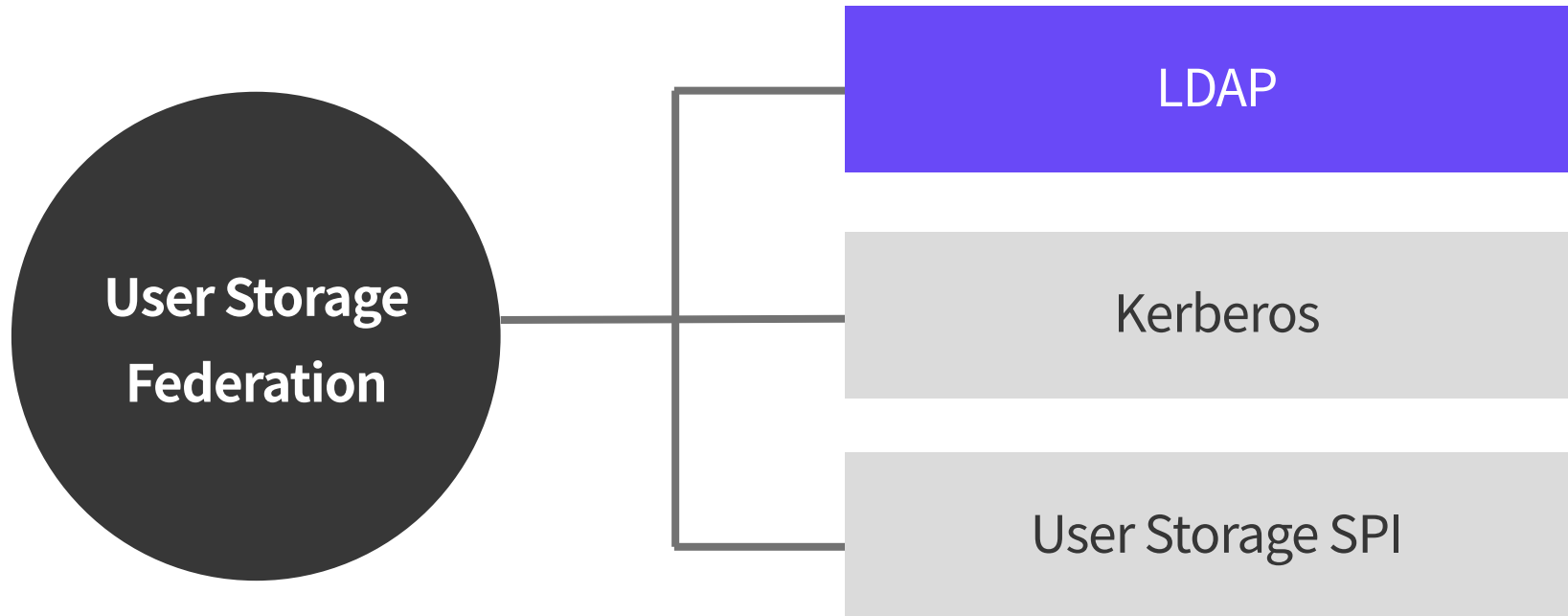
User Storage Federation

3가지 연동 방식



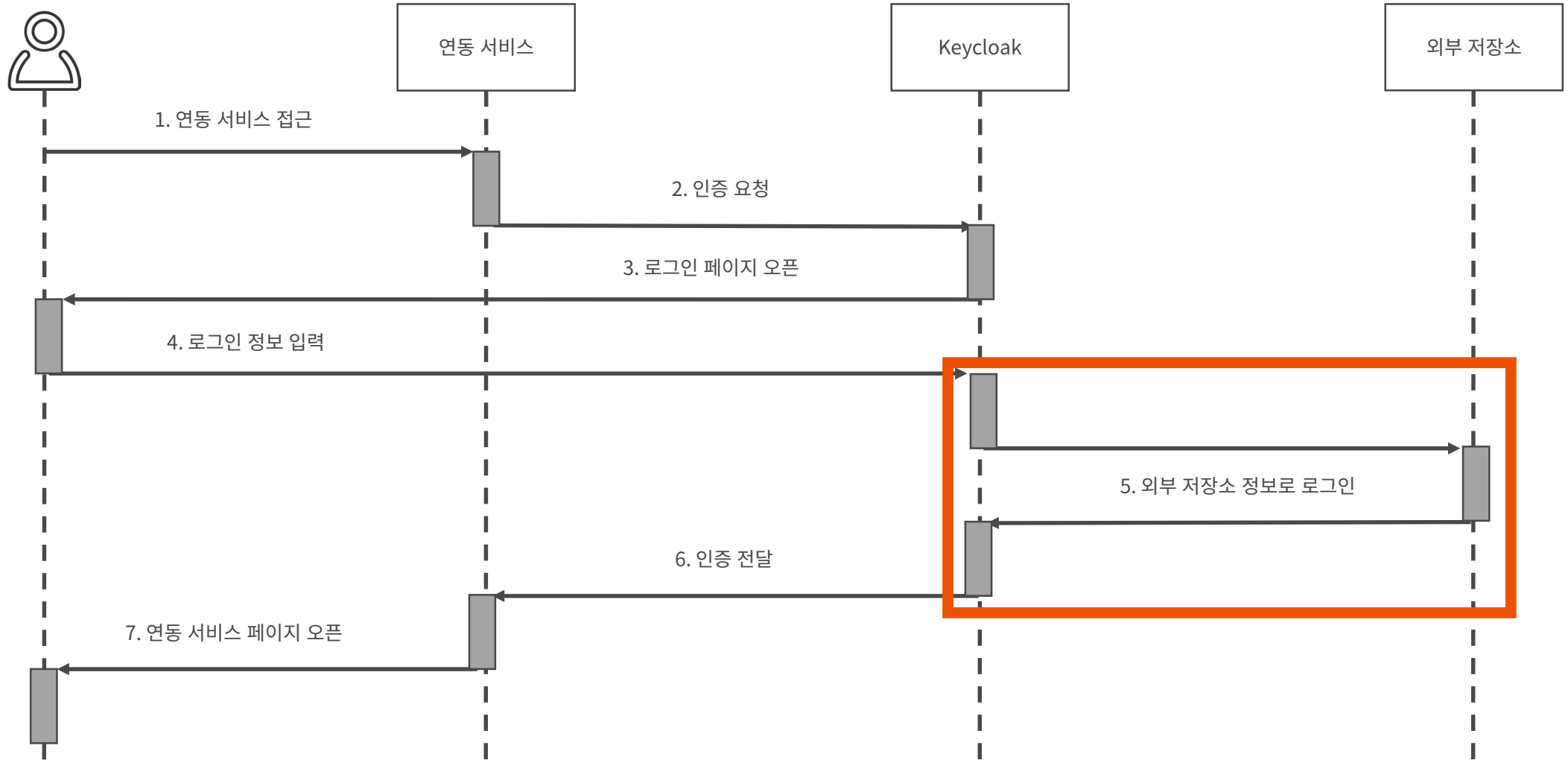
User Storage Federation

3가지 연동 방식

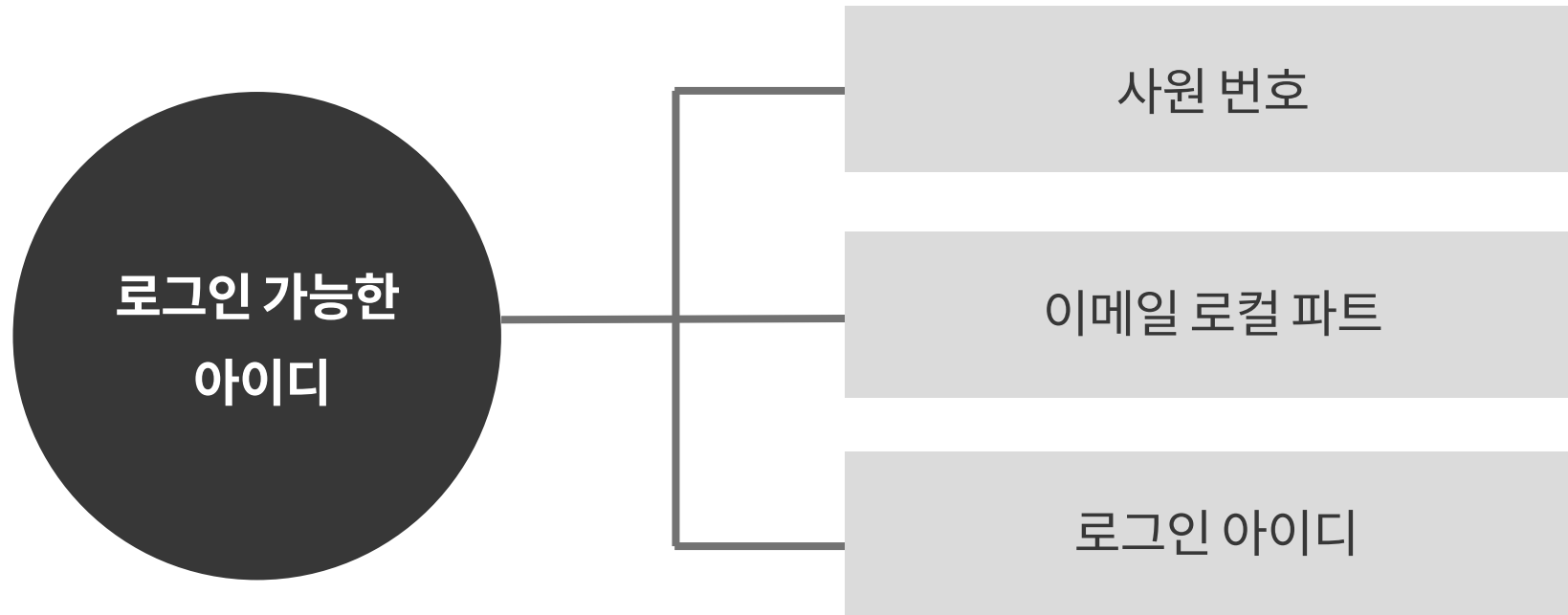


Authentication SPI

Authentication SPI



Authentication SPI



Authentication SPI



Authentication SPI



▶ 본인 인증 및 신규 비밀번호 발급



한덕선님은 5회 연속 잘못된 비밀번호 사용으로 인하여 입력이 차단되었습니다.
아래의 본인인증 후에 신규 비밀번호를 발급 받으셔야 합니다.

인증방법선택	<input checked="" type="radio"/> 휴대폰 <input type="radio"/> 외부메일
직원번호	<input type="text"/>
휴대폰	<input type="text"/>

▪ 직원번호와 회사에 등록된 휴대전화 번호/외부메일을 입력하시면 인증번호가 휴대전화 SMS/외부메일로 발송됩니다.

인증번호발송

잠금 계정
로그인 시도



▶ 계정잠김

사내시스템 사용이 다음과 같은 사유로 접근이 차단되었습니다.

1. 임시 계정이 만료된 경우
2. 기타 보안상의 사유로 연결이 일시적으로 차단된 경우

[관련 문의 : 사내정보시스템_운영([REDACTED]@nhn.com)]

Authentication SPI

Authentication > Flows > Browser

Browser			Requirement				New	Copy
Auth Type								
Cookie			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			
Kerberos			<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED			
Identity Provider Redirector			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		Actions ▾	
Forms			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL		
	Username Password Form		<input checked="" type="radio"/> REQUIRED					
	Browser - Conditional OTP		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input checked="" type="radio"/> CONDITIONAL		
		Condition - User Configured	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED				
		OTP Form	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			

Authentication SPI

Authentication > Flows > Browser

Browser							New	Copy
Auth Type			Requirement					
Cookie			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			
Kerberos			<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED			
Identity Provider Redirector			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		Actions ▾	
Forms			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL		
	Username Password Form		<input checked="" type="radio"/> REQUIRED					
	Browser - Conditional OTP		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input checked="" type="radio"/> CONDITIONAL		
		Condition - User Configured	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED				
		OTP Form	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			

Authentication SPI

Authentication SPI 적용

Nhn Browser			New	Copy	Delete	Edit Flow	Add execution	Add flow
Auth Type			Requirement					
<input type="checkbox"/> ^ <input type="checkbox"/> v	Cookie		<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			Actions v
<input type="checkbox"/> ^ <input type="checkbox"/> v	Kerberos		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED			Actions v
<input type="checkbox"/> ^ <input type="checkbox"/> v	Identity Provider Redirector		<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			Actions v
<input type="checkbox"/> ^ <input type="checkbox"/> v	Nhn Browser Forms		<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL		Actions v
	<input type="checkbox"/> ^ <input type="checkbox"/> v	NHN Username Password Form	<input checked="" type="radio"/> REQUIRED					Actions v
	<input type="checkbox"/> ^ <input type="checkbox"/> v	Nhn Browser Browser - Conditional OTP	<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input checked="" type="radio"/> CONDITIONAL		Actions v
		<input type="checkbox"/> ^ <input type="checkbox"/> v	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED				Actions v
		<input type="checkbox"/> ^ <input type="checkbox"/> v	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			Actions v

Authentication SPI

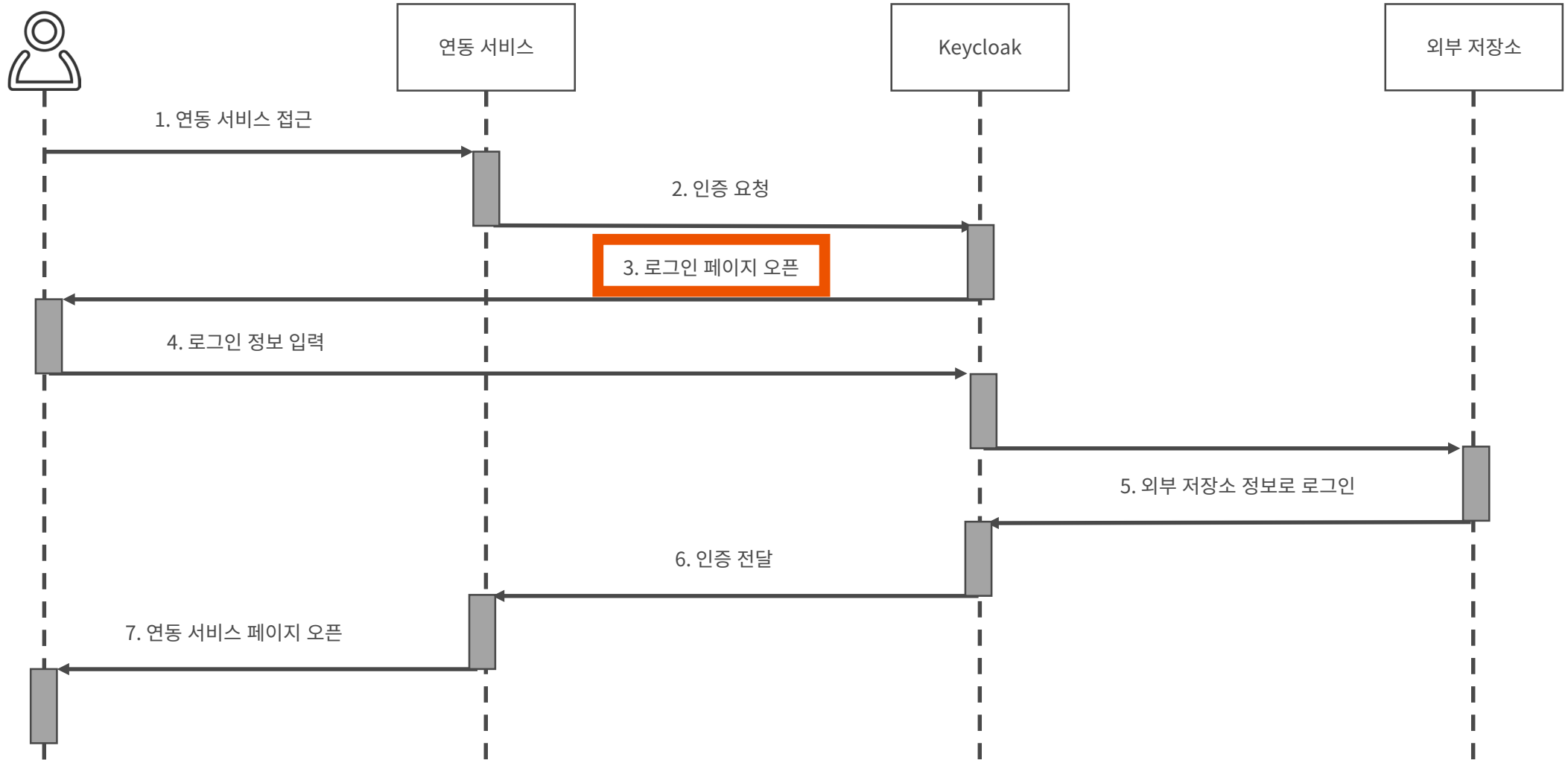
Authentication SPI 적용

Nhn Browser		Requirement					Actions
Cookie		<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		Actions	
Kerberos		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED		Actions	
Identity Provider Redirector		<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		Actions	
Nhn Browser Forms		<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL	Actions	
NHN Username Password Form		<input checked="" type="radio"/> REQUIRED				Actions	
Nhn Browser Browser - Conditional OTP		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input checked="" type="radio"/> CONDITIONAL	Actions	
	Condition - User Configured	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED			Actions	
	OTP Form	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		Actions	

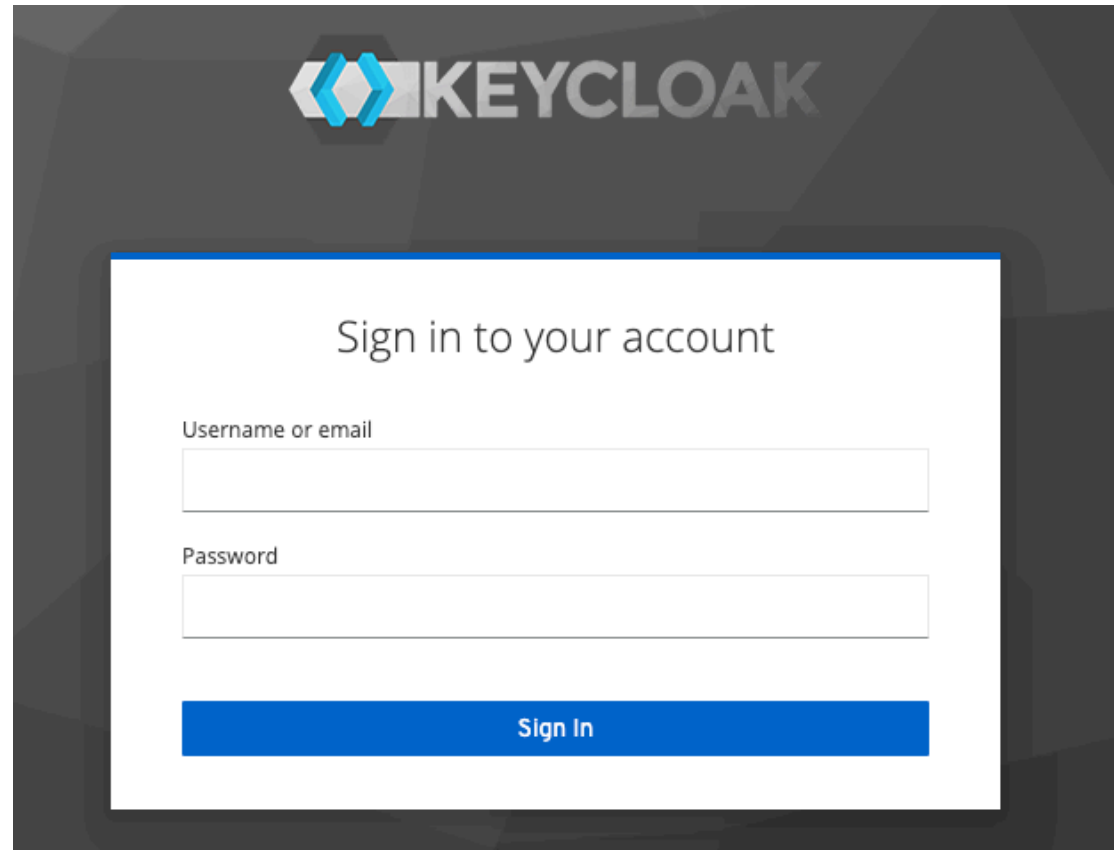
로그인 페이지

NHN FORWARD ▶▶▶

로그인 페이지



로그인 페이지



The image shows a Keycloak login page. At the top center, there is the Keycloak logo, which consists of a blue and white geometric icon followed by the word "KEYCLOAK" in a bold, sans-serif font. Below the logo, the text "Sign in to your account" is centered. Underneath this text, there are two input fields: the first is labeled "Username or email" and the second is labeled "Password". Both fields are empty. At the bottom of the form, there is a blue button with the text "Sign In" in white.

로그인 페이지



INTRANET SERVICE
LOGIN

ID

PASSWORD

 REMEMBER USER ID

FORGOT USER PASSWORD: | [HELP DESK](#)

LOGIN

LANGUAGE Korean GMT+09:00 (Seoul)

로그인 페이지



WHAT'S UP? INTRANET SERVICE LOGIN

ID

PASSWORD

REMEMBER USER ID

FORGOT USER PASSWORD: | [HELP DESK](#)

LOGIN

LANGUAGE Korean GMT+09:00 (Seoul)



keycloak

2022년 7월 1일 이후 비밀번호 변경을 안하셨다면 이 문구를 클릭하여 임시 비밀번호를 받아 로그인 시도해주세요.



WHAT'S UP? INTRANET SERVICE LOGIN

ID

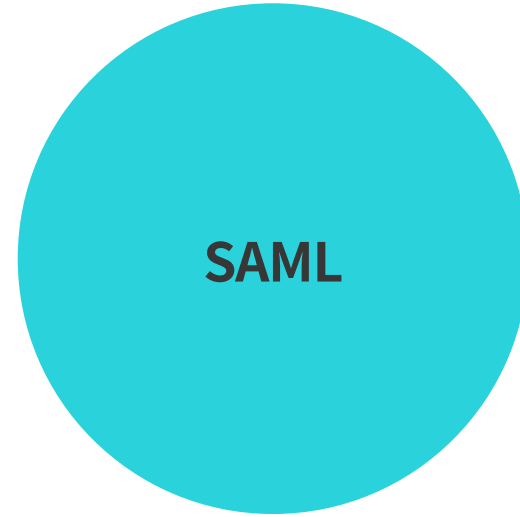
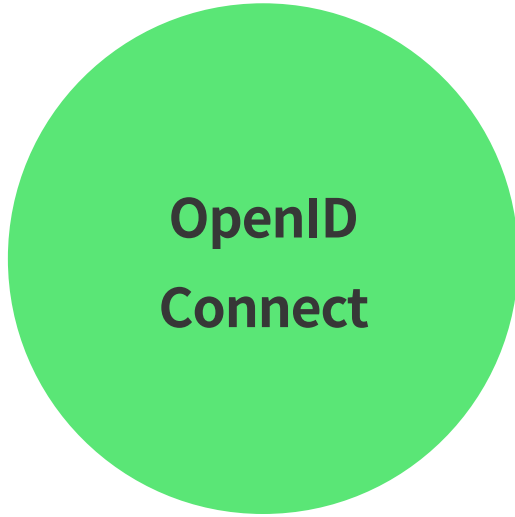
PASSWORD

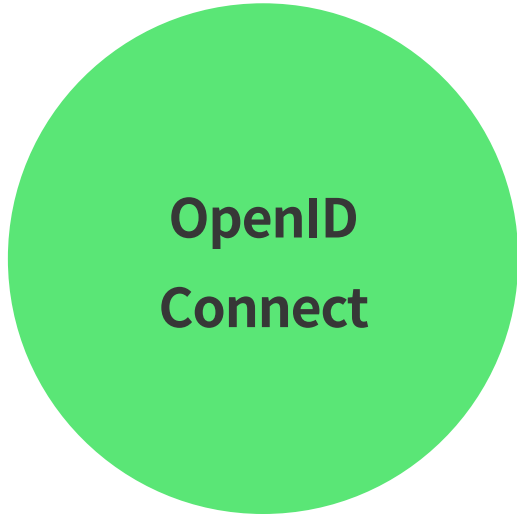
REMEMBER USER ID

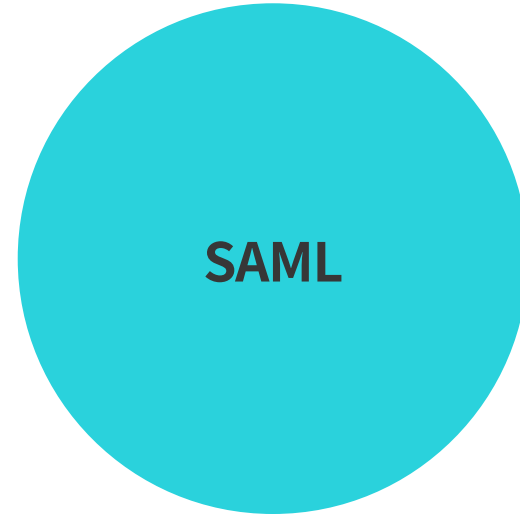
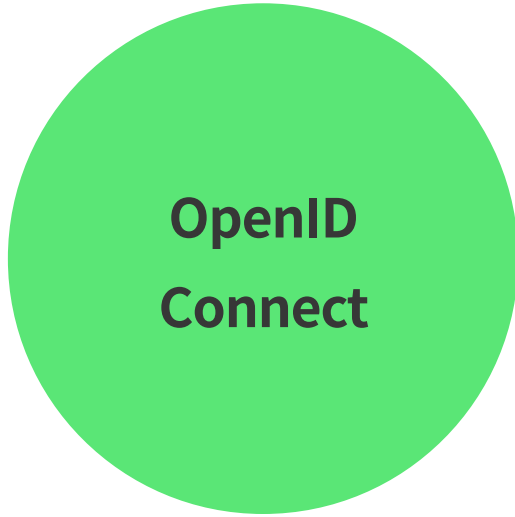
FORGOT USER PASSWORD: | [HELP DESK](#)

LOGIN

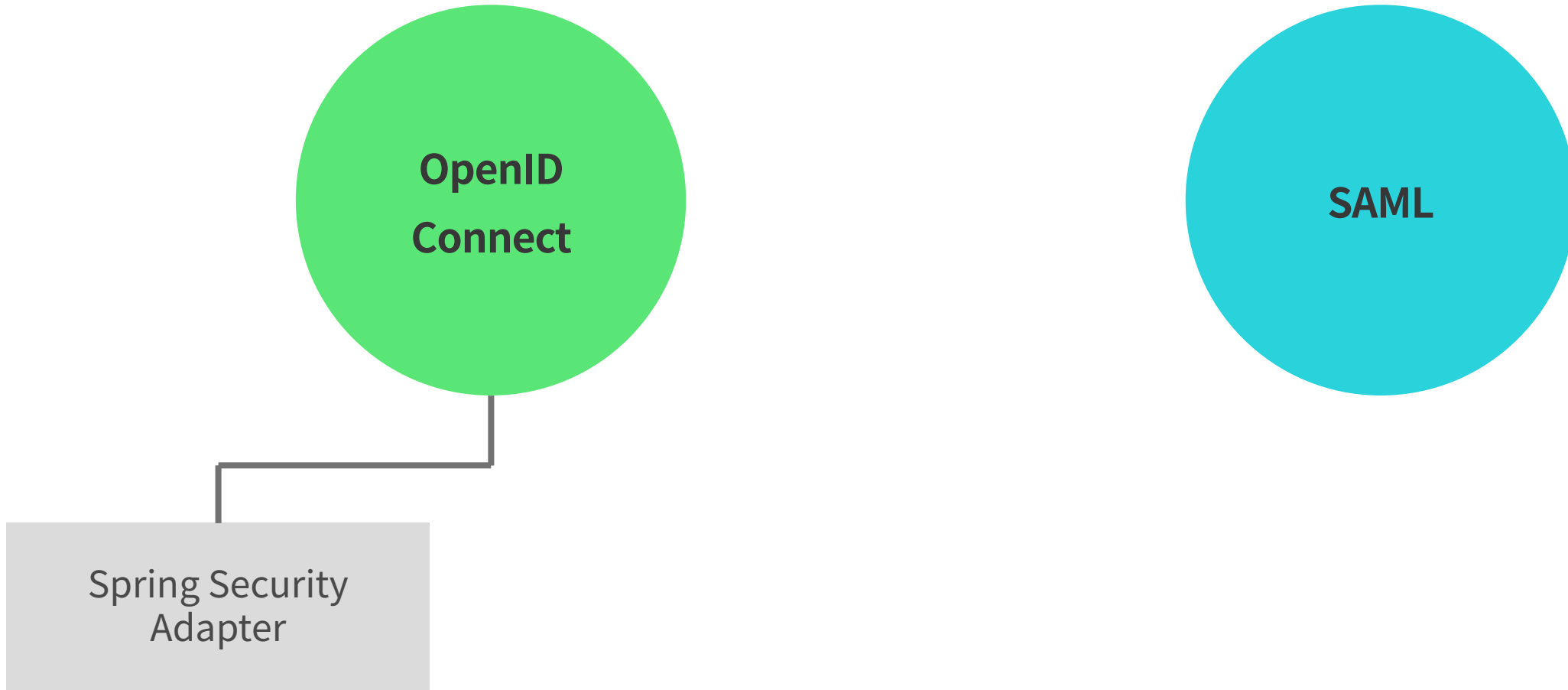
LANGUAGE Korean GMT+09:00 (Seoul)

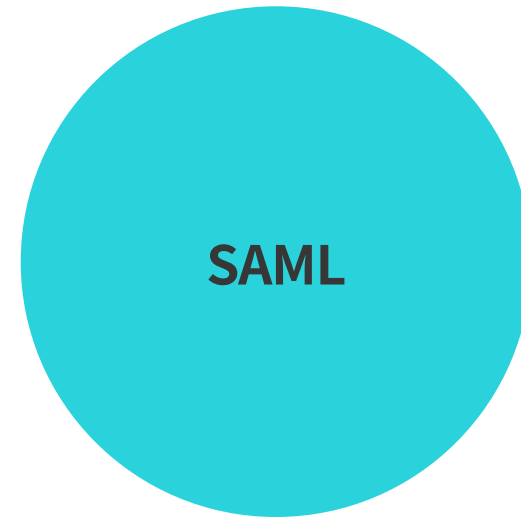
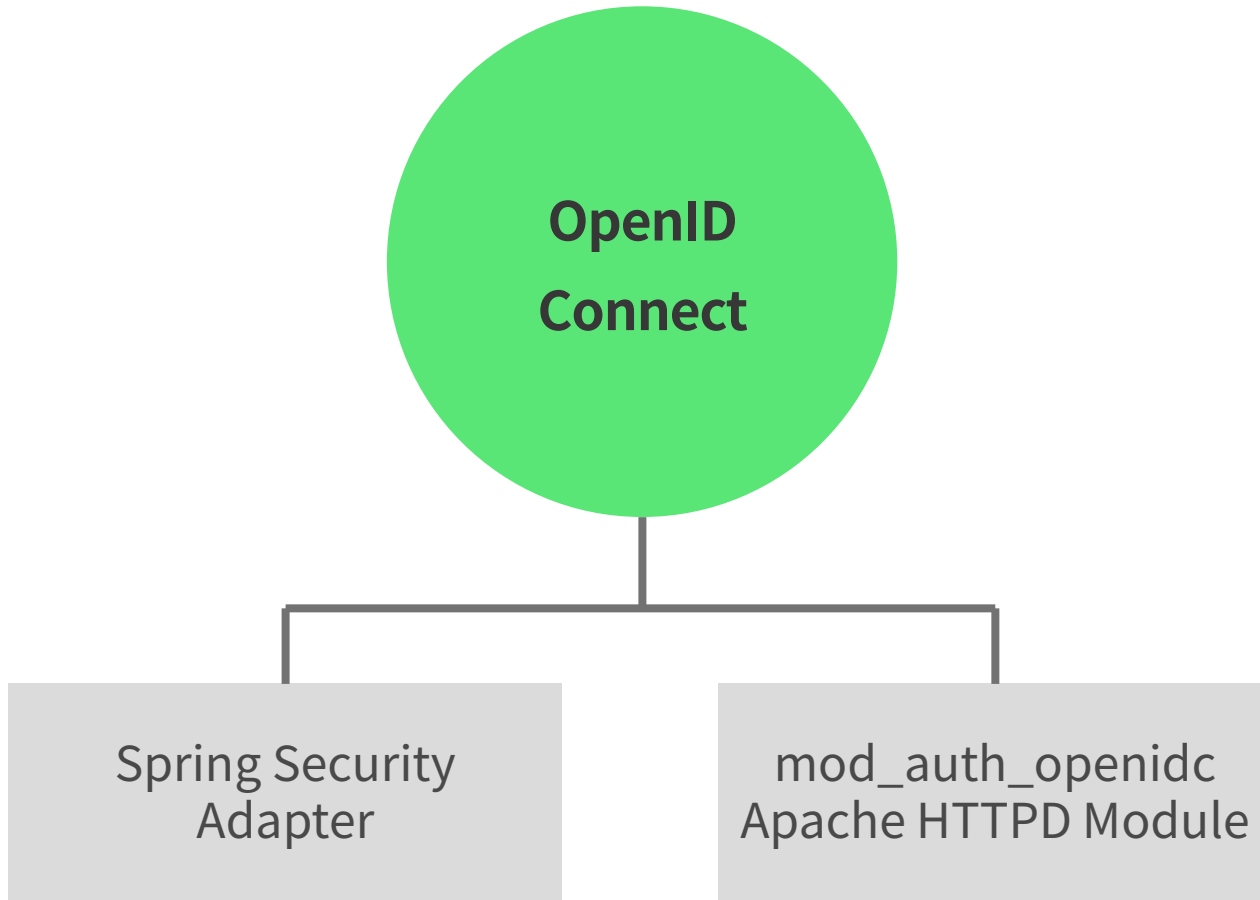


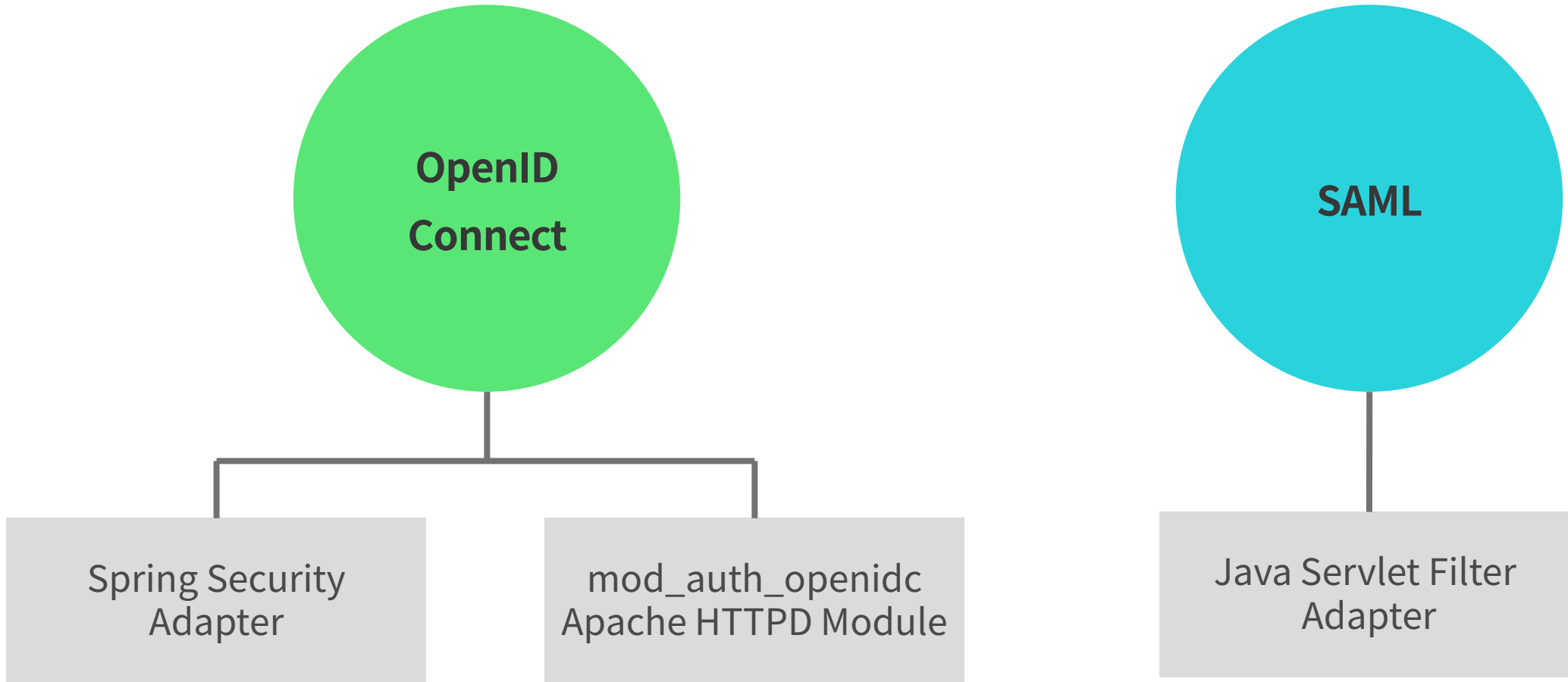




연동 방식





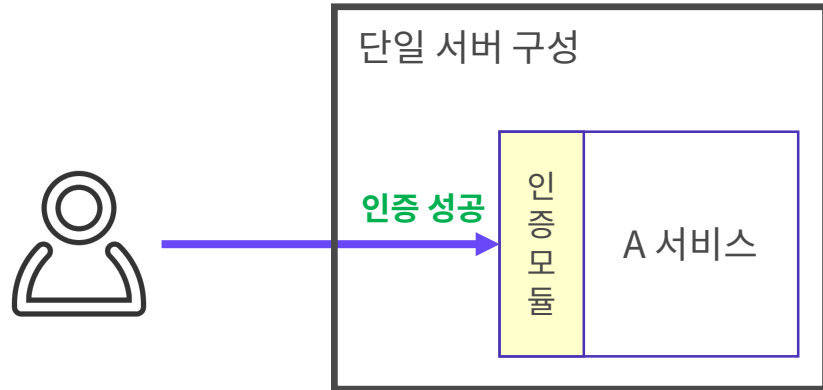


발생한 이슈 및 해결

이슈1: 서버 환경 구성

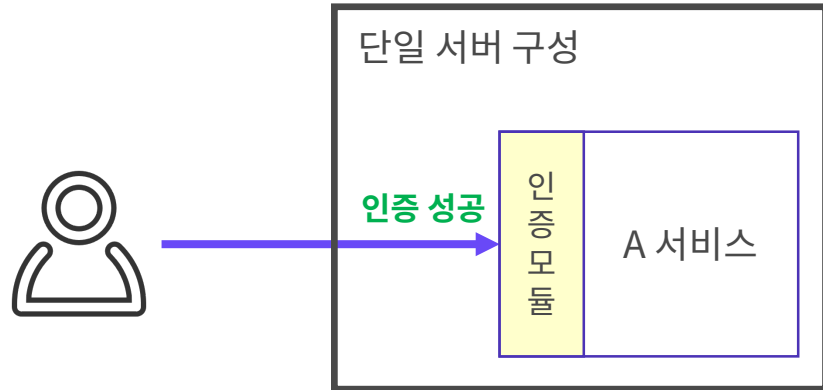
이슈1: 서버 환경 구성

DEV

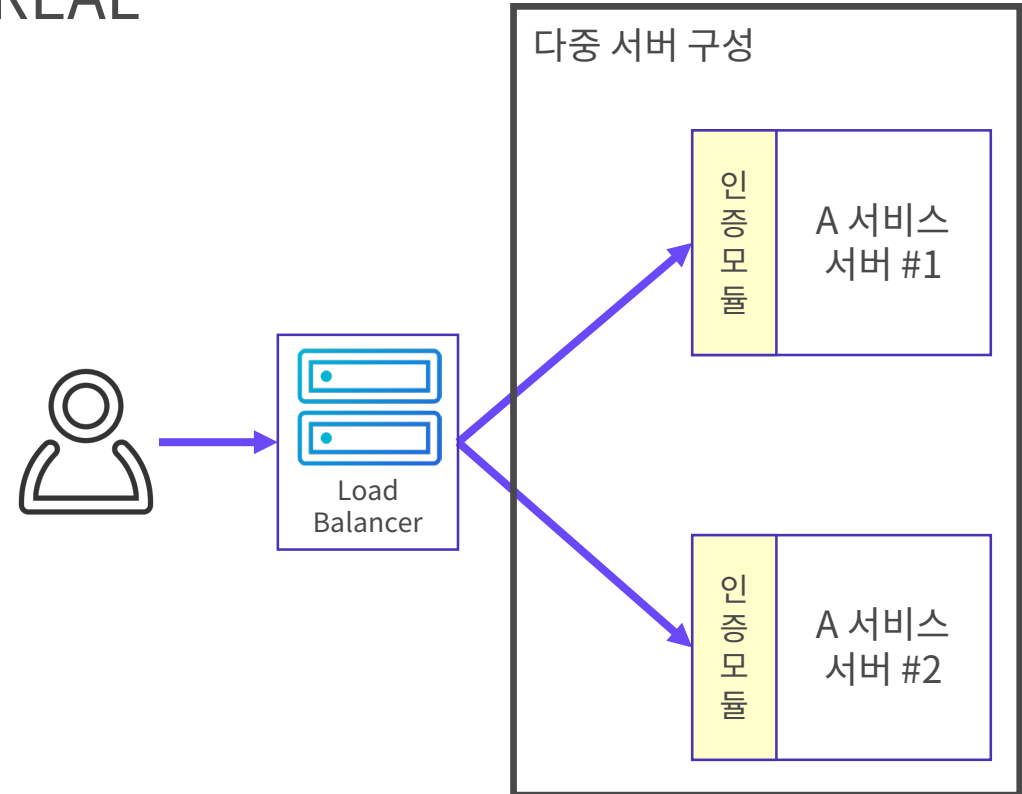


이슈1: 서버 환경 구성

DEV

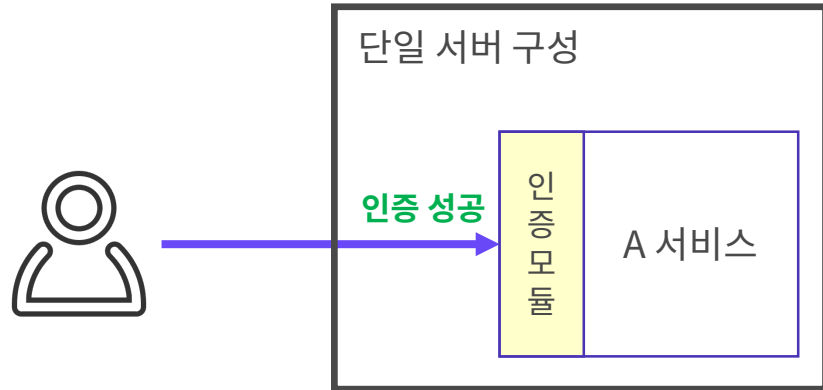


REAL

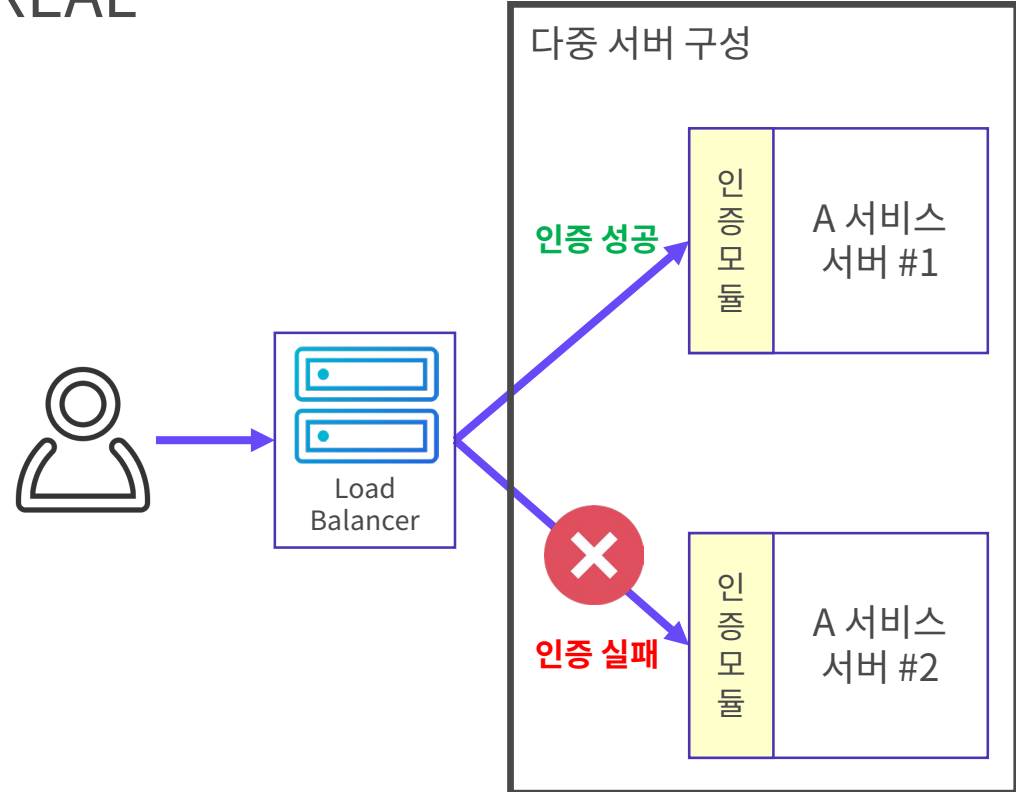


이슈1: 서버 환경 구성

DEV

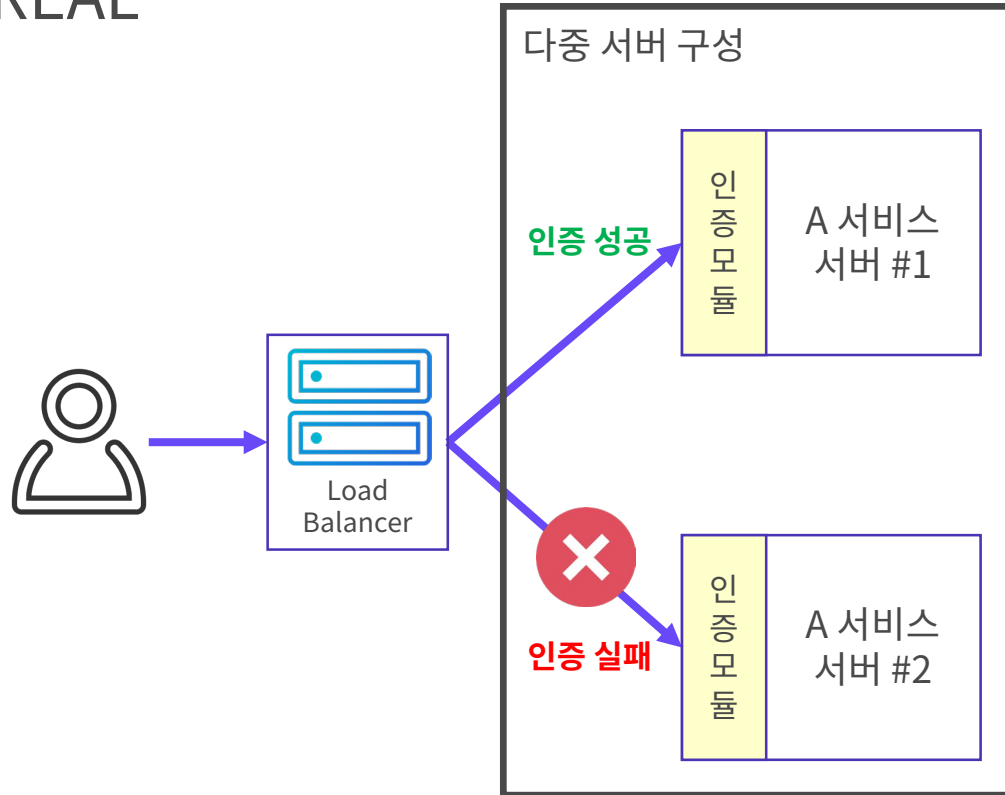


REAL



이슈1: 서버 환경 구성

REAL



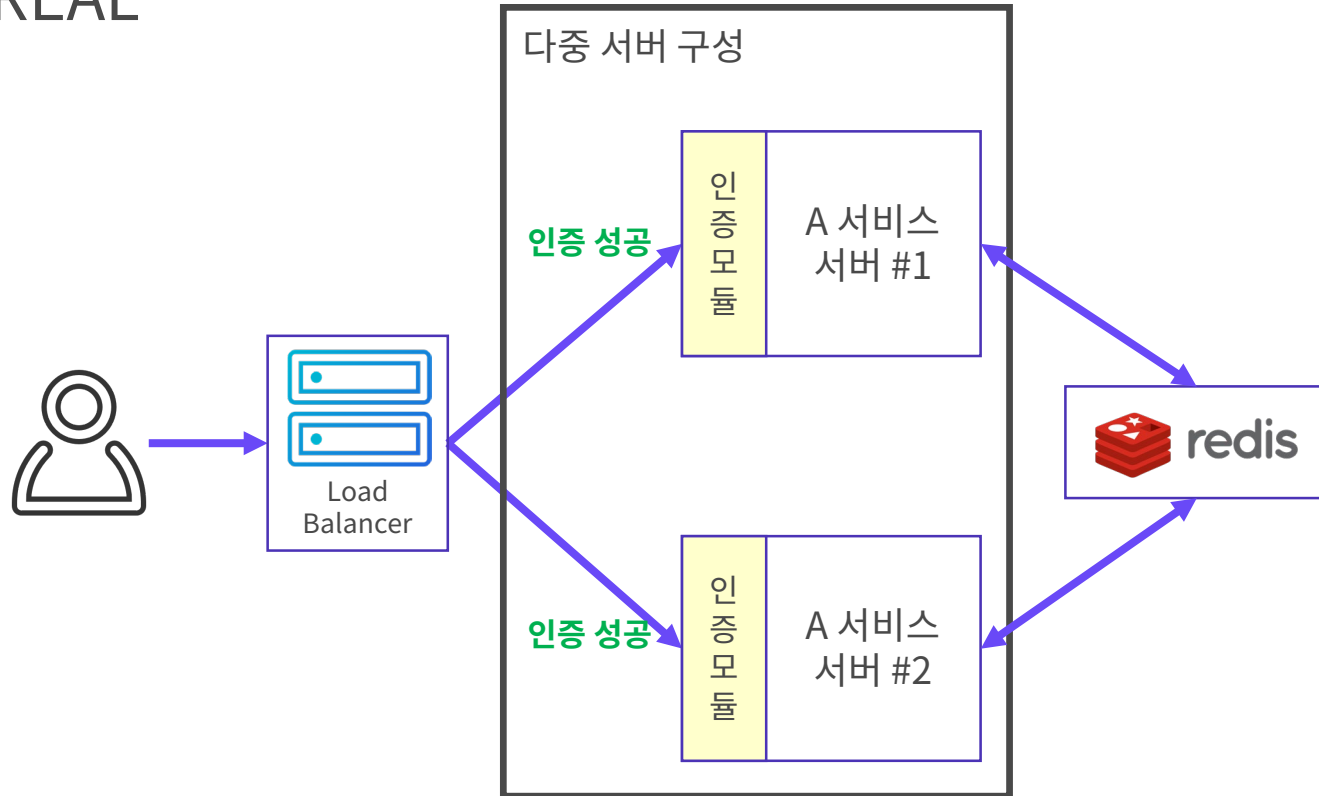
이슈1: 서버 환경 구성

해결완료

이슈1: 서버 환경 구성

해결 완료

REAL

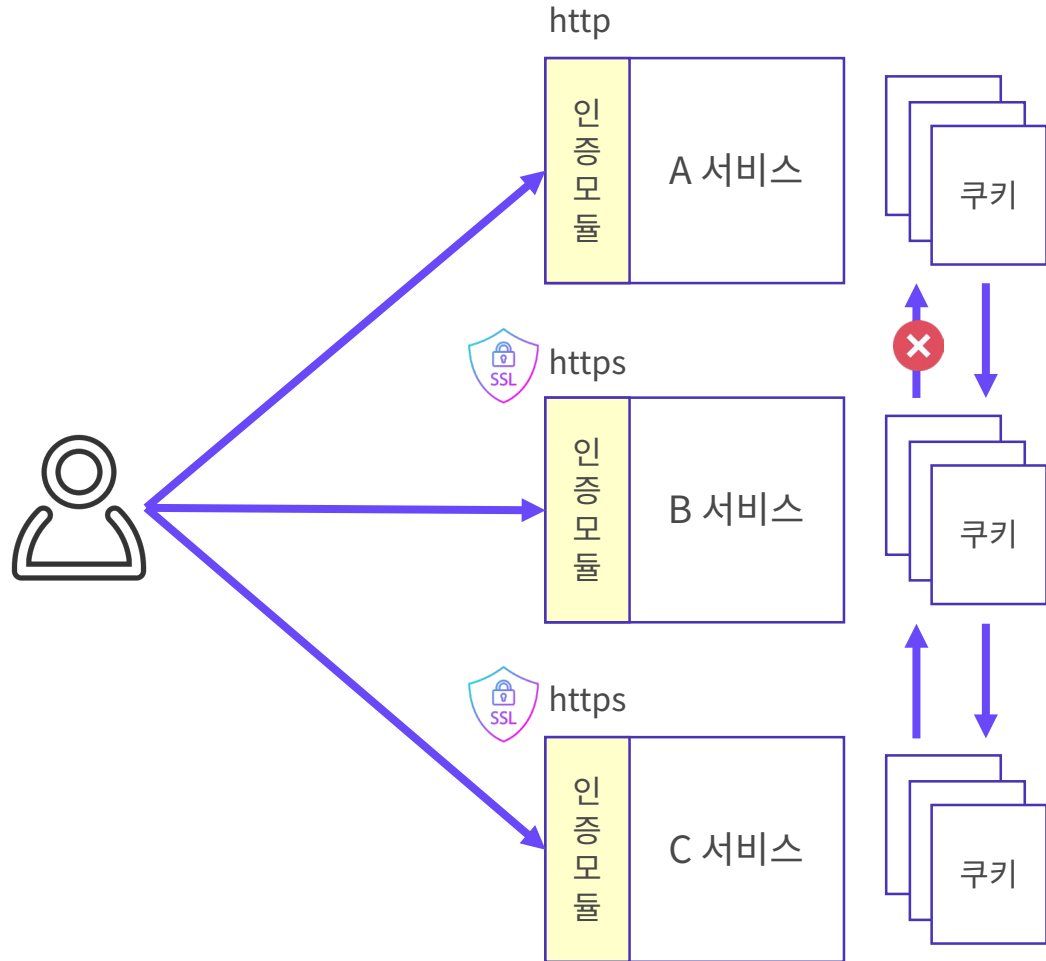


redis 적용

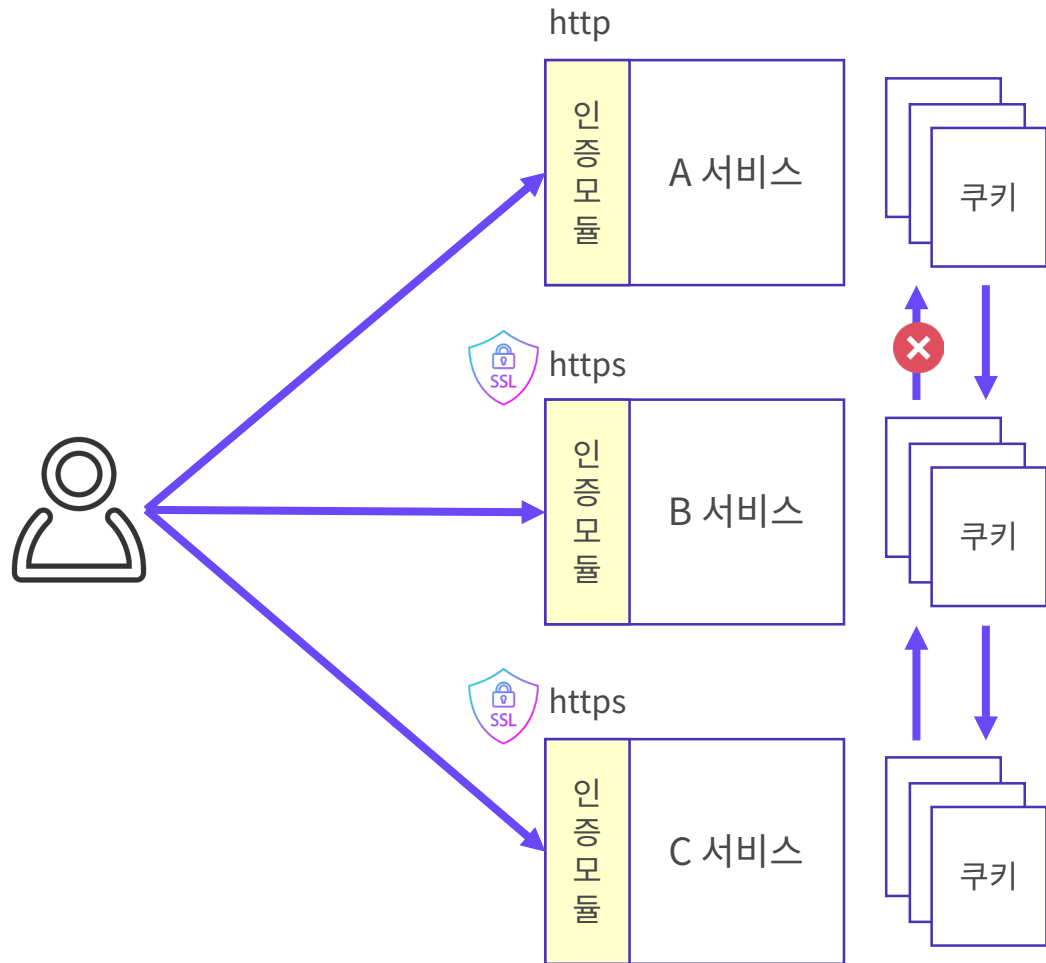
세션 공유를 통한 인증 정보 공유

이슈2: 쿠키 공유

이슈2: 쿠키 공유



이슈2: 쿠키 공유



http → https 인지 실패

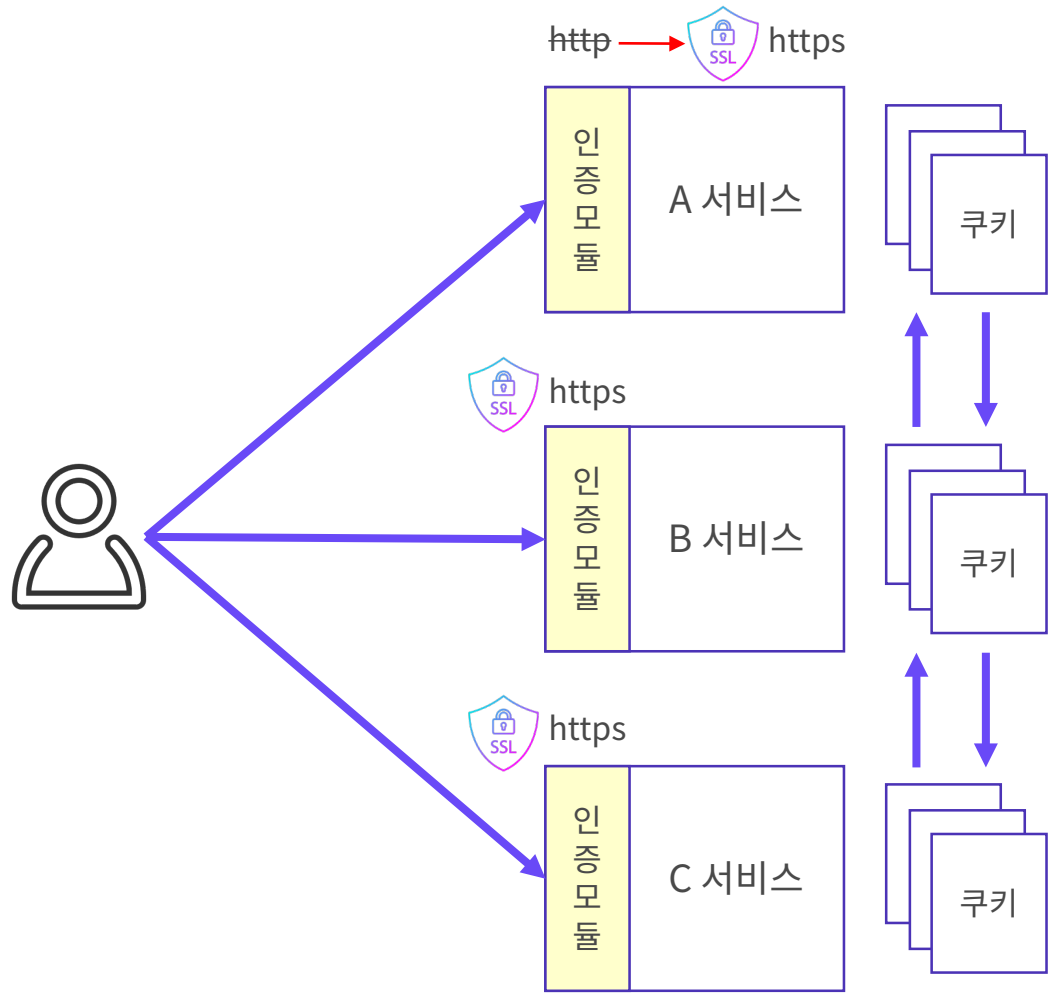
https 서비스에서의 Secure한 쿠키

이슈2: 쿠키 공유

해결방안-1

이슈2: 쿠키 공유

해결방안-1



전체 서비스 SSL 적용

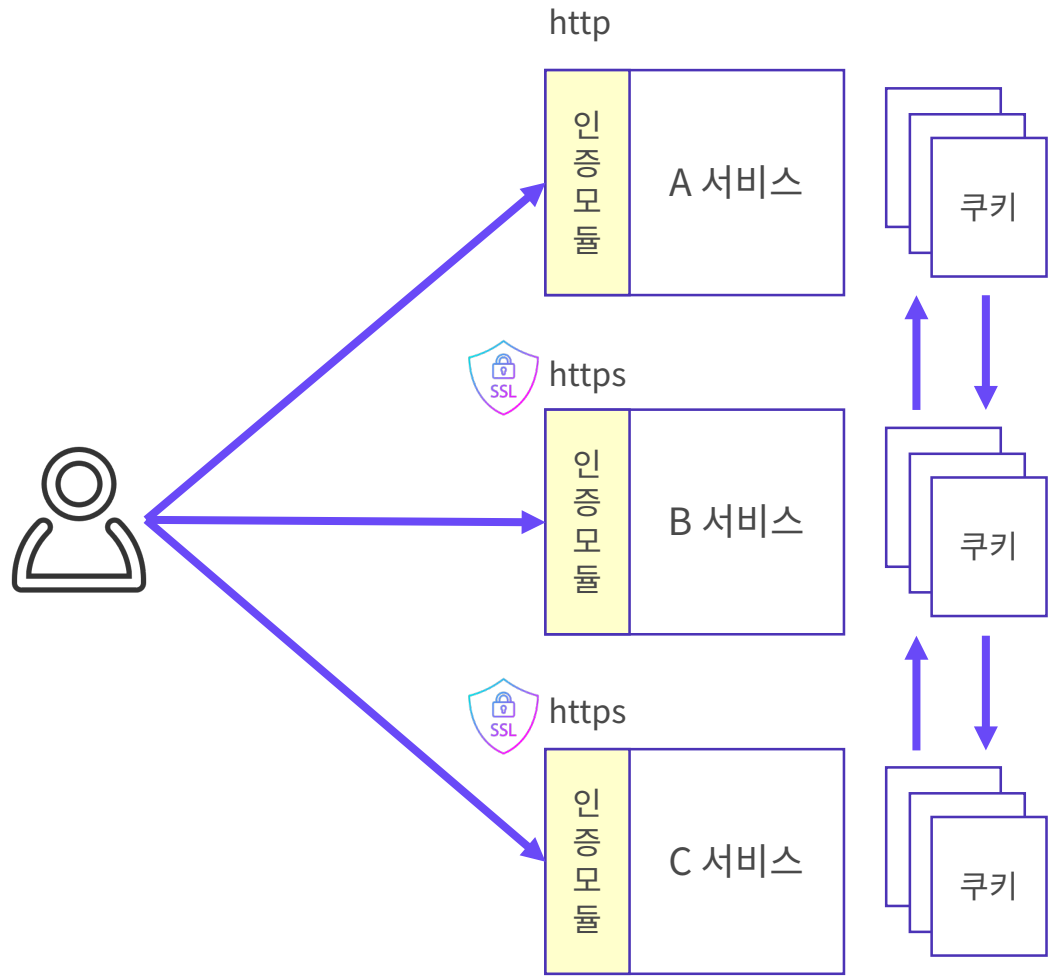
“기술적” 접근보다는 “정책적” 접근 필요

이슈2: 쿠키 공유

해결방안-2

이슈2: 쿠키 공유

해결방안-2



쿠키 생성 시 http에서의 생성

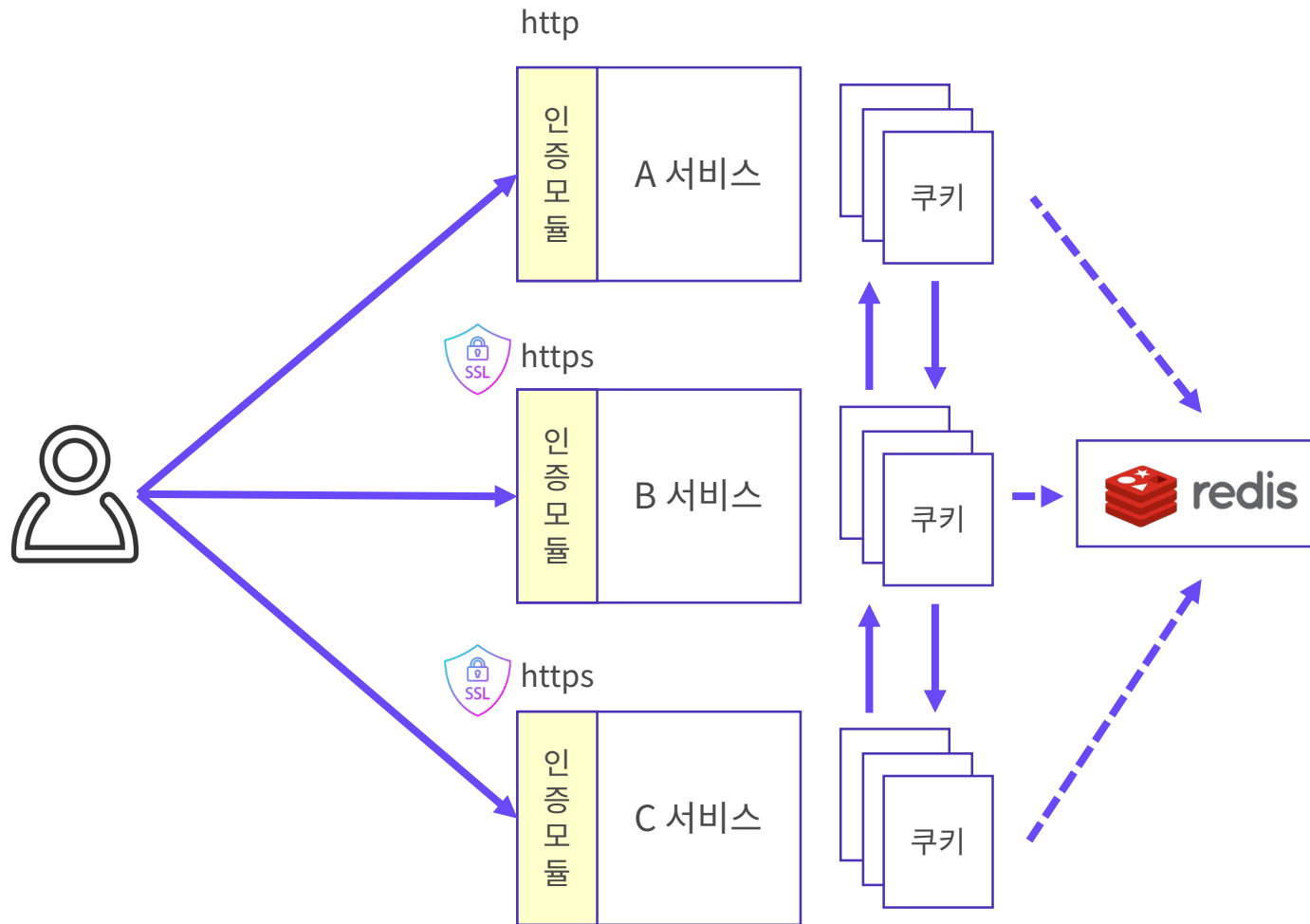
Secure하지 않기 때문에 **보안에 취약**

이슈2: 쿠키 공유

해결방안-3

이슈2: 쿠키 공유

해결방안-3



쿠키의 대체 세션

인증 공유를 위한 redis를 적극 활용

이슈3: Legacy System의 한계

이슈3: Legacy System의 한계

전환 대상 100+

이슈3: Legacy System의 한계

전환 대상 100+



이슈3: Legacy System의 한계

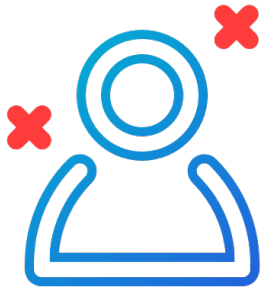
전환 대상 100+

그 중 약 30%가 Legacy System

이슈3: Legacy System의 한계

전환 대상 100+

그 중 약 30%가 Legacy System



이슈3: Legacy System의 한계

전환 대상 100+

그 중 약 30%가 Legacy System

이슈3: Legacy System의 한계

해결완료

NHN FORWARD ▶▶

전환 대상 100+

그중 약 30%가 Legacy System

이슈3: Legacy System의 한계

해결완료

NHN FORWARD ▶▶

전환 대상 100+

그중 약 30%가 Legacy System

구축 단계에서의 전략 수립

Legacy System 지원을 위한 추가 개발(SPI 활용)


개선 방향

인증 보안 강화

인증 보안 강화

새로운 환경
로그인 모니터링

인증 보안 강화



새로운 환경
로그인 모니터링



2단계 인증

인증 보안 강화

새로운 환경
로그인 모니터링

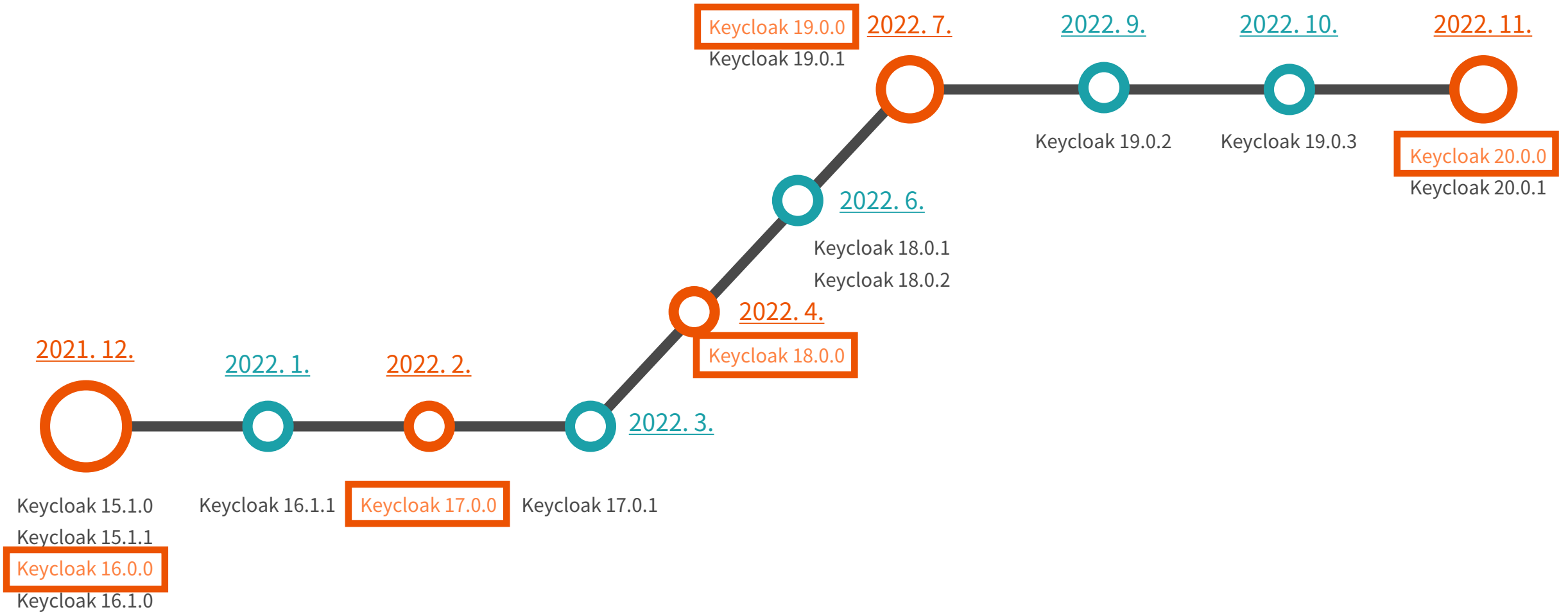
2단계 인증

인증 강제 종료

버전 업그레이드

NHN FORWARD ▶▶▶

버전 업그레이드



버전 업그레이드

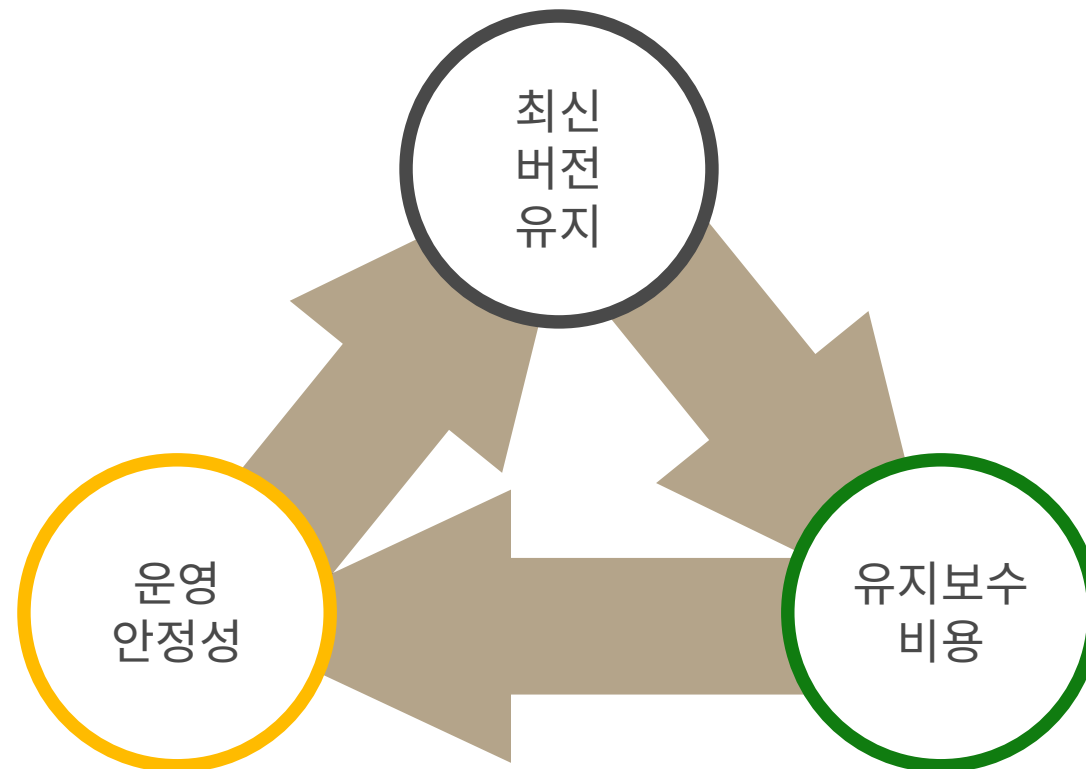
버전 업그레이드는?

버전 업그레이드는 **신중하게!**

하지만, Release Note는 항상 예의주시하자.

버전 업그레이드는 **신중하게!**

하지만, Release Note는 항상 예의주시하자.



그 외 여러 가지

그 외 여러 가지

- IDC 이중화
 - 대규모 장애에 대비
 - 높은 구축 비용

그 외 여러 가지

- IDC 이중화
 - 대규모 장애에 대비
 - 높은 구축 비용
- 인증 중복 체크
 - 보안 신뢰 상승
 - 외부 심사 대응(ITGC 등)

Q & A

고맙습니다.

