MFA 설정 및 모범 사례

Passkey를 활용한 안전한 인증

MFA란?

Multi-Factor Authentication (다중 인증)

로그인 시 **2가지 이상의 인증 요소**를 요구하는 보안 방식

🧠 Something you KNOW	📱 Something you HAVE	👆 Something you ARE
비밀번호	Passkey	지문 (Touch ID)
PIN 코드	보안 키, 휴대폰	얼굴 (Face ID)

Passkey는 "가진 것" + "본인인 것"을 한 번에 해결!

AWS MFA 필수화 정책

2024년부터 AWS MFA 의무화

시기	대상
2024년 중반	Organizations 관리 계정 루트 사용자
2024년 7월	독립 계정 루트 사용자
향후	모든 계정 유형으로 확대 예정

AWS가 **Passkey**를 강력히 권장하는 이유가 있습니다

기존 TOTP의 한계

왜 Passkey를 권장할까요?

TOTP 피싱 공격 시나리오:

1. 👤 사용자가 피싱 사이트에 로그인 시도
2. 🎣 피싱 사이트가 진짜 AWS에 대신 로그인
3. 👤 사용자에게 "OTP 입력하세요" 요청
4. 👤 사용자가 OTP 코드 입력: `123456`
5. 😈 공격자가 OTP를 받아서 즉시 사용
6. ✅ 공격자 로그인 성공!

30초 안에 코드를 가로채면 악용 가능

Passkey는 피싱이 불가능

공개키 암호화 + 도메인 검증

Passkey 피싱 시도 시:

1. 👤 사용자가 피싱 사이트에 로그인 시도
2. 🎣 피싱 사이트가 Passkey 요청
3. 🛑 **도메인 불일치 감지!**
    - 등록된 도메인: `aws.amazon.com`
    - 현재 도메인: `fake-aws.com`
4. ❌ **인증 자동 거부**

Passkey는 등록된 도메인에서**만** 작동합니다

Passkey vs TOTP 비교

구분	🔐 Passkey	📱 TOTP (기존)
피싱 방지	✅ 완벽 차단	❌ 취약
사용 편의성	👆 터치/생체 인증	⌨️ 코드 수동 입력
코드 가로채기	✅ 불가능	❌ 가능
AWS 권장	⭐ 강력 권장	지원됨
복구	여러 기기 동기화	복구 코드 필요

iCloud Keychain이란?

Apple의 비밀번호 및 Passkey 동기화 서비스

특징:

- End-to-End 암호화 (Apple도 내용 확인 불가)
- Apple ID로 로그인된 모든 기기에 자동 동기화
- Mac, iPhone, iPad 간 Passkey 공유

즉, 한 번 등록하면 모든 Apple 기기에서 사용 가능!

iCloud Keychain + Passkey

Apple 생태계에서의 Passkey 동기화

☁️ **iCloud Keychain** (End-to-End 암호화)

⬇️ 자동 동기화 ⬇️

🖥️ Mac	📱 iPhone	📱 iPad
Touch ID 👆	Face ID 😍	Face ID 😍

하나의 Passkey가 **모든 Apple 기기**에서 사용 가능

Touch ID로 AWS 로그인

Mac에서의 실제 사용 흐름

1️⃣ AWS 콘솔 접속 → 비밀번호 입력

2️⃣ MFA 요청 화면 표시

> "🔐 Touch ID로 인증하세요"

3️⃣ MacBook 터치바의 Touch ID에 손가락 터치

4️⃣ 즉시 로그인 완료! ✅

⏱️ **코드 입력 없이 0.5초 만에 인증 완료**

Face ID로 AWS 로그인

iPhone에서의 실제 사용 흐름

1️⃣ AWS 콘솔 접속 → 비밀번호 입력

2️⃣ MFA 요청 화면 표시

> "🔐 Face ID로 인증하세요"

3️⃣ iPhone을 바라보기만 하면 됨 😊

4️⃣ 즉시 로그인 완료! ✅

⏱️ **손가락 하나 까딱 안 해도 인증 완료**

Cross-Device 인증

Windows PC에서 iPhone Face ID 사용하기

상황: Windows PC에 Passkey가 없는 경우

단계	🖥️ Windows PC	📱 iPhone
1	QR 코드 표시	-
2	-	QR 코드 스캔
3	-	Face ID 인증 😊
4	✅ 로그인 성공!	✅ 승인 완료

Windows에 Passkey가 없어도 iPhone으로 인증 가능!

Passkey 유형: Synced Passkeys

☁️ 클라우드에 저장되어 여러 기기에서 사용

제공자	설명
iCloud Keychain	Apple 기기 간 동기화
Google Password Manager	Android/Chrome 동기화
1Password	크로스 플랫폼 (추천)
Bitwarden	크로스 플랫폼, 오픈소스

✅ 여러 기기에서 사용 가능

✅ 분실해도 복구 쉬움

⚠️ 클라우드 계정 보안이 중요

Passkey 유형: Device-bound

🔑 특정 하드웨어에만 저장

제품	특징
YubiKey	USB/NFC, 가장 널리 사용 ⭐
Google Titan	USB/Bluetooth
Feitian	다양한 폼팩터

✅ 최고 수준의 보안

✅ 물리적 소유 필요

⚠️ 분실 시 복구 어려움

👉 루트 계정에 권장

AWS에서 지원하는 인증기

🖥️ 플랫폼 인증기 (내장)

- Apple **Touch ID** (Mac)
- Apple **Face ID** (iPhone/iPad)
- **Android** 생체 인증
- Windows Hello (Cross-device만 지원)

🔑 로밍 인증기 (외장)

- **YubiKey** (USB/NFC) ⭐ 가장 인기
- Google Titan Key (USB/Bluetooth)
- 기타 FIDO2 호환 보안 키

📊 최대 8개 MFA 디바이스 등록 가능

Passkey 설정 방법

AWS 콘솔에서 설정하기

1. AWS 콘솔 로그인
2. 우측 상단 사용자명 클릭 → **"보안 자격 증명"**
3. **"MFA 디바이스 할당"** 클릭
4. **"Passkey 또는 보안 키"** 선택
5. 브라우저 프롬프트에서 인증 방법 선택:
   - 이 기기 (Touch ID/Face ID)
   - 보안 키 (YubiKey 등)
   - 다른 기기 (QR 코드로 휴대폰 사용)

권장 설정: 일반 사용자

👤 개발자, 비개발직군

우선순위	MFA 유형	용도
1순위	**Synced Passkey** (iCloud/1Password)	일상 로그인
2순위	하드웨어 키	백업용

💡 1Password 같은 크로스 플랫폼 도구 추천

권장 설정: 관리자/루트 계정

👑 높은 보안이 필요한 계정

우선순위	MFA 유형	용도
1순위	**YubiKey**	기본 인증
2순위	**두 번째 YubiKey**	금고에 보관
3순위	Synced Passkey	긴급 백업

⚠️ 루트 계정은 반드시 하드웨어 보안 키 사용!

기존 TOTP 사용자 전환 가이드

📱 Google Authenticator → 🔐 Passkey

1️⃣ 새 Passkey 등록 (기존 TOTP 유지)

- AWS는 최대 8개 MFA 동시 등록 가능

2️⃣ 1-2주간 Passkey로 로그인 연습

- 문제 발생 시 TOTP 백업으로 사용

3️⃣ 익숙해지면 TOTP 제거 (선택)

- 또는 백업용으로 유지해도 무방

💡 병행 사용 중에도 Passkey가 기본 옵션으로 표시됨

Passkey 분실 대비 전략

🔄 권장 설정 (3중 백업)

Primary	Backup 1	Backup 2
1Password Passkey	YubiKey (집)	YubiKey (회사 금고)

모두 같은 AWS 계정에 등록

⚠️ 모든 Passkey 분실 시:
관리자에게 연락 → MFA 초기화 → 새로 등록

요약

🔐 Session 5 핵심 정리

1. **Passkey** = 차세대 MFA (AWS 2024년부터 강력 권장)
2. **TOTP보다 안전 + 편리**
    - 피싱 불가능 (도메인 검증)
    - 코드 입력 불필요 (Touch ID/Face ID)
3. **iCloud Keychain**으로 Apple 기기 간 자동 동기화
4. **권장 조합**
    - 일반: Synced Passkey + 하드웨어 키 백업
    - 루트: 하드웨어 키 필수 (YubiKey 2개 권장)

전체 교육 요약

5개 세션에서 배운 내용

세션	주제	핵심
1	IAM 기본	사용자, 역할, 정책, 최소 권한
2	IAM Identity Center	중앙 관리, SSO
3	AWS CLI	단기 자격 증명
4	계정 vs IAM	계정 구조, Organizations
5	MFA	**Passkey로 안전한 인증**

핵심 보안 원칙

✅ 반드시 지켜야 할 것

- ☑️ 최소 권한 원칙 준수
- ☑️ **Passkey MFA 필수 설정**
- ☑️ 단기 자격 증명 사용 (IAM Identity Center + SSO)
- ☑️ 루트 계정 사용 최소화
- ☑️ 정기적인 권한 검토

감사합니다!

질문 있으신가요?