Elixirr

클라우드 보안 관리자 (Azure Active Directory)

[1강] 인증과 권한 부여 (Authentication & Authorization)

학습 목표

학습 목표

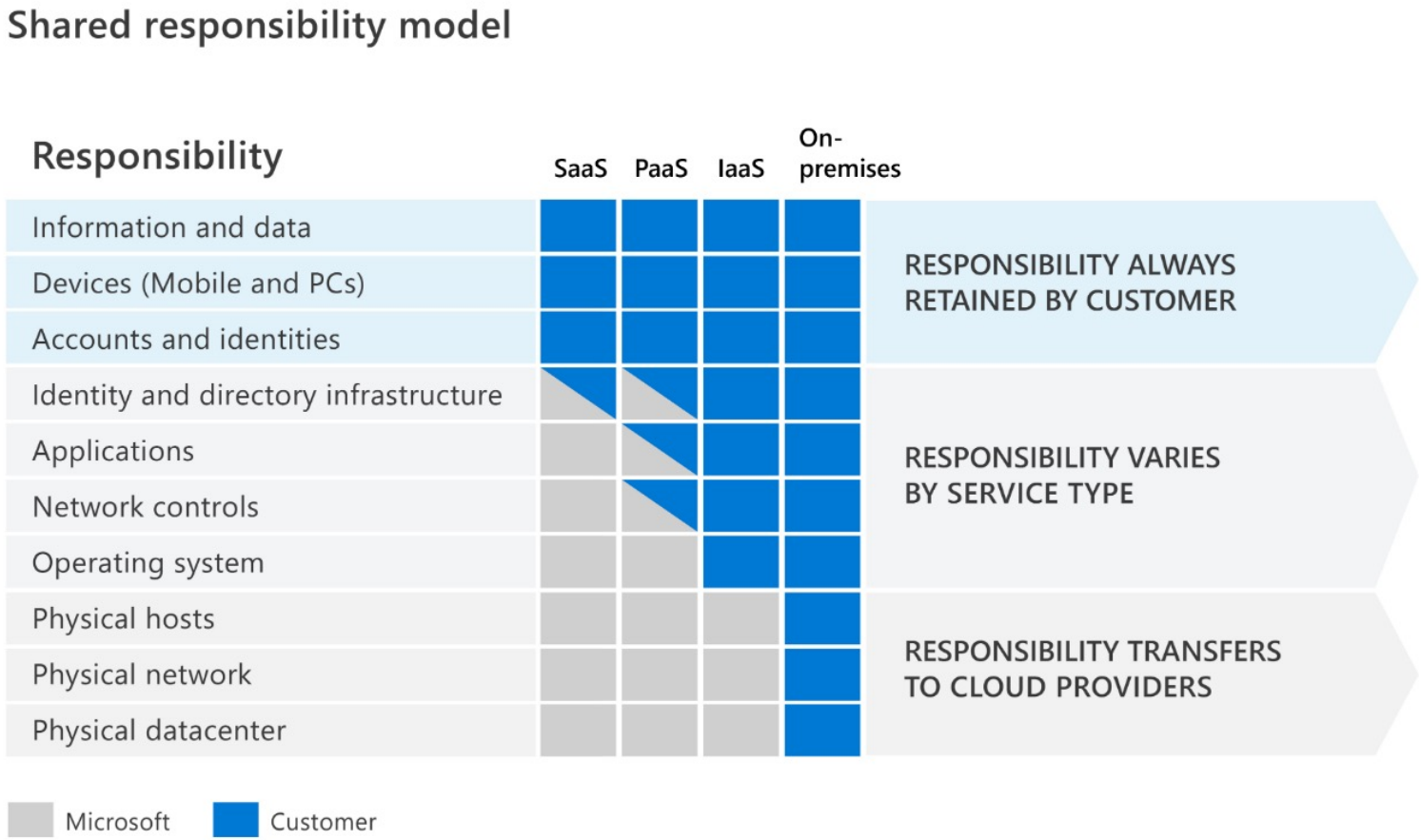
보안과 규정 준수에 대해 알아 봅니다.

인증과 권한 부여에 대해 알아 봅니다.

보안과 규정 준수

공유 책임 모델 (Shared Responsibility Model)

기업이 자체 서버에서 하드웨어 및 소프트웨어만 실행하는 경우에는 기업이 보안 및 규정 준수를 100% 책임진다.
클라우드 기반 서비스를 사용하면 고객과 클라우드 공급자 사이에서 책임이 분담된다.



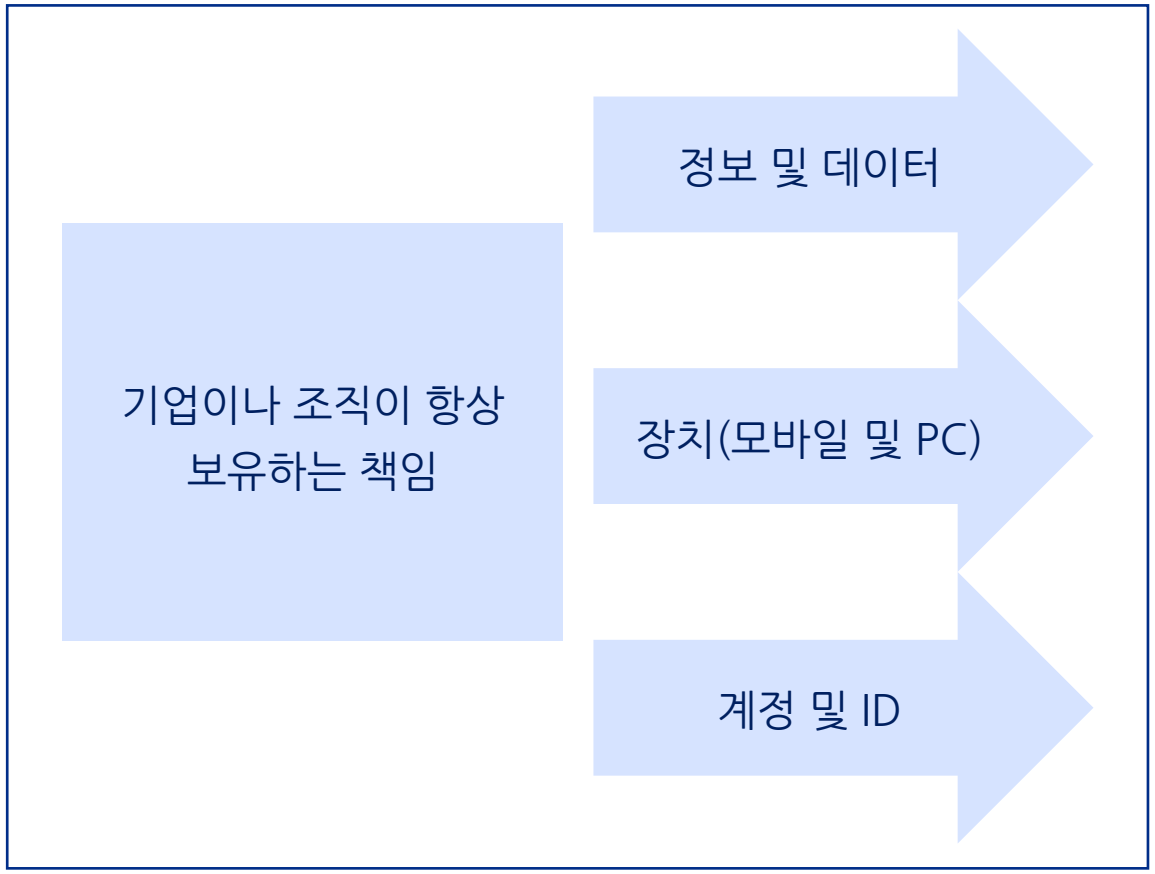
공유 책임 모델의 종류

- SaaS(Software as a Service)
- PaaS(Platform as a Service)
- IaaS(Infrastructure as a Service)
- On-premises datacenter

https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/2-describe-shared-responsibility-model

기업이나 조직의 보안 책임

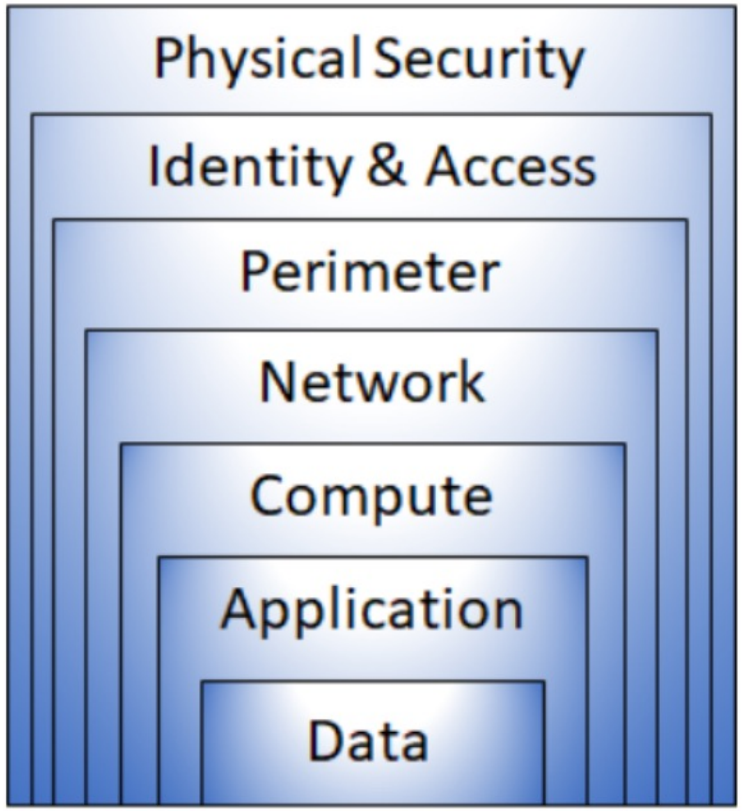
모든 클라우드 배포 유형에 대해 클라우드 고객은 데이터와 ID를 소유하므로 클라우드 고객은 공유 책임 모델의 어떤 것을 사용할지라도 모바일 장치, PC, 프린터 등을 포함한 리소스와 데이터 및 ID의 보안을 책임져야 한다.



공유 책임 모델의 이점은 기업이 자신의 책임과 클라우드 공급자의 책임에 대해서 명확하다는 것이구나!

심층 방어

심층 방어는 단일 경계에 의존하지 않고 계층화된 보안 접근 방식을 사용하여 공격의 진행을 늦춘다. 각 계층은 보호 기능을 제공하므로 한 계층이 위반되면 후속 계층에서 공격자의 데이터에 대한 무단 액세스를 방지한다.

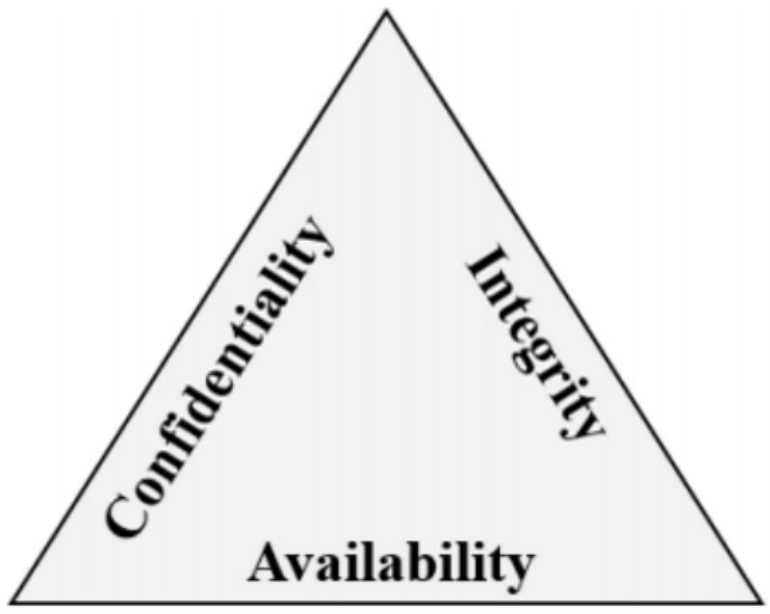


- 물리적 보안(Physical Security) : 데이터 센터에 대한 액세스를 승인된 직원으로 제한 등
- ID 및 액세스 보안 : 다단계 인증 또는 조건 기반 액세스 제어를 통해 인프라에 대한 액세스를 제어하고 변경
- 네트워크 경계 보안 : Ddos(분산 서비스 거부) 보호를 포함한 대규모 공격 필터링
- 네트워크 보안 : 리소스 간의 통신을 제한하기 위한 네트워크 세분화 및 네트워크 액세스 제어
- 컴퓨팅 계층 보안 : 특정 포트를 닫아 자체 서버 또는 클라우드에서 가상 머신에 대한 액세스를 보호
- 애플리케이션 보안 : 애플리케이션이 안전하고 보안 취약점이 없도록 보장
- 데이터 계층 보안 : 비즈니스 및 고객 데이터에 대한 액세스를 관리하는 제어와 데이터 보호를 위한 암호화

https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/3-describe-defense-depth

사이버 보안 전략의 목표

기술, 프로세스 및 교육은 사이버 보안 전략의 요소이며, 그 목표에는 기밀성(Confidentiality), 무결성(Integrity) 및 가용성(Availability)이 보장되어야 한다. 이 세가지 원칙을 CIA라고 한다.



https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/3-describe-defense-depth

- 기밀성 (Confidentiality) - 고객 정보, 암호 또는 재무 데이터와 같은 민감 데이터를 기밀로 유지하기 위해 데이터 암호화 및 암호화 키도 기밀로 유지
- 무결성 (Integrity) - 데이터가 조작되거나 변경되지 않았다는 확신을 갖기 위해 데이터 또는 메시지를 올바르게 유지하는 것을 말한다. 데이터를 암호화하면 기밀이 유지되지만 암호화되기 전과 같도록 해독할 수 있어야 한다.
- 가용성 (Availability) - 필요한 사람이 필요할 때 데이터를 사용할 수 있어야 한다는 원칙. 암호화된 형식으로 데이터를 저장하는 것이 안전하지만 직원은 해독된 데이터에 액세스되어야 한다.

사이버 보안 전략의 목표는 시스템, 네트워크, 애플리케이션 및 데이터의 기밀성, 무결성 및 가용성을 유지하는 것

제로 트러스트 모델의 구현 원칙

제로 트러스트 모델은 기업 네트워크의 방화벽 뒤에 있는 리소스를 포함한 모든 것이 신뢰할 수 없는 개방형 네트워크에 있다고 가정한다. '아무도 믿지 말고 모든 것을 검증한다'는 원칙에 따라 운영된다.

명시적 확인

항상 사용자 ID, 위치, 장치, 서비스 및 데이터 분류, 이상을 포함하여 사용 가능한 데이터 포인트를 기반으로 인증하고 권한 부여

최소 권한 액세스

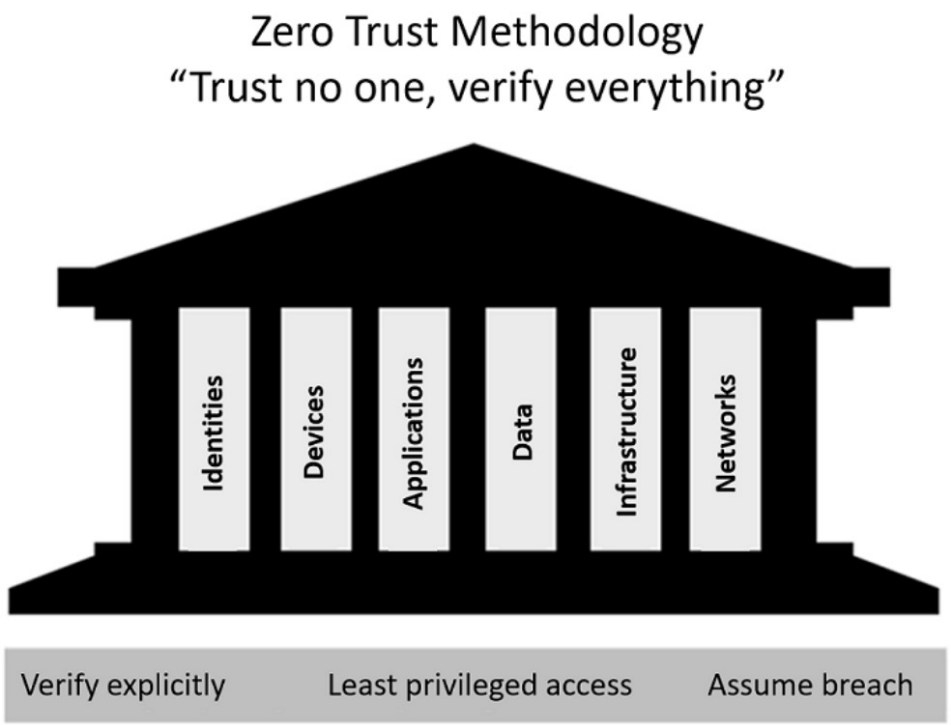
Just-In-Time(JIT)과 Just-Enough-Access(JEA), 위험에 따른 맞춤형 정책 및 데이터 보호를 통해 사용자 액세스를 제한하여 데이터와 생산성을 모두 보호

위반 가정

네트워크, 사용자, 장치 및 애플리케이션별로 액세스를 분류. 암호화를 사용하여 데이터를 보호하고 분석을 사용하여 가시성을 확보하고 위협을 감지하고 보안을 강화.

제로 트러스트 모델 (Zero Trust Model)의 기본 요소

제로 트러스트 모델에서는 모든 요소가 함께 작동하여 종단 간 보안을 제공한다. 아래 6가지 요소는 제로 트러스트 모델의 기본 요소이다.

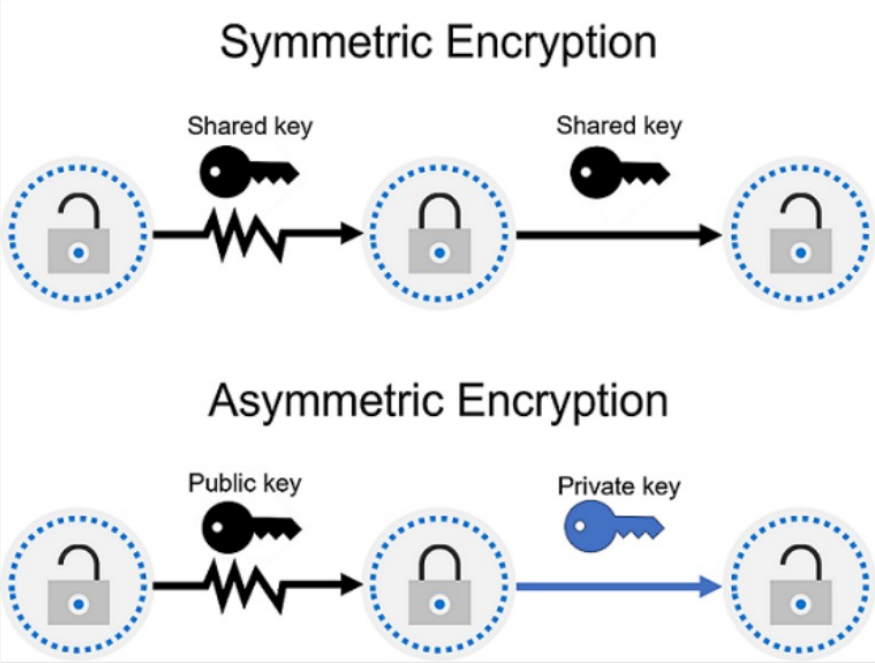


https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/4-describe-zero-trust-model

- ID - 사용자, 서비스, 장치 가능. ID가 리소스에 액세스하려고 하면 최소 권한 액세스 원칙 준수
- Device - 데이터가 장치에서 클라우드로 흐를 때 장치는 대규모 공격 대상이 될 수 있다. 상태 및 규정 준수를 위해 장치 모니터링 중요
- 애플리케이션 - 중앙에서 관리되지 않은 Shadow IT가 있는지 모니터링하고 이러한 애플리케이션에는 권한 및 액세스 관리 필요
- 데이터 - 속성에 따라 분류, 레이블 지정 및 암호화되어야 한다.
- 인프라 - 기업 자체 서버 또는 클라우드 기반이든 인프라는 위협 요소. 보안을 개선하기 위해 버전, JIT 액세스 평가, 원격 분석 사용하여 공격 및 이상 징후 감시. 위험 행동을 자동으로 차단하거나 표시하고 보호 조치.
- 네트워크 - 네트워크를 세분화하여 실시간 위협 보호, 종단 간 암호화, 모니터링 및 분석 사용

암호화 (Encryption)

암호화는 승인되지 않은 사람이 데이터를 읽을 수 없고 사용할 수 없도록 만드는 프로세스로서, 사용하거나 읽으려면 암호를 해독해야 하고 이를 위해서 비밀 키를 사용한다.



- 암호화에는 대칭 암호화(Symmetric Encryption)와 비대칭 암호화(Asymmetric Encryption)이 있다.
- 대칭 암호화 (Symmetric Encryption) - 동일한 키를 사용하여 데이터를 암호화하고 해독.
- 비대칭 암호화 (Asymmetric Encryption) - 공개 키(Public Key)와 개인 캐(Private Key)를 사용. 두개의 키 모두 데이터 암호화 가능하나 단일 키를 사용하여 해독 불가능. 해독을 위해서는 페어링 된 키가 필요.
- 비대칭 암호화는 HTTPS 프로토콜 및 전자 데이터 서명 솔루션을 사용하여 인터텟 사이트에 액세스하는 작업에 사용.

https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/5-describe-encryption-hashing

암호화 대상

암호화는 사용 중인 데이터를 암호화하는 것 이외에도 미사용 데이터 및 전송 중인 데이터를 보호할 수 있다.

미사용 데이터

서버와 같은 물리적 장치에 저장된 데이터로서 데이터베이스 또는 스토리지 계정에 저장된 데이터이다. 저장된 위치에 관계없이 데이터를 해독하는 데 필요한 키와 비밀 번호 없이 데이터를 읽을 수 없도록 한다.

전송 중인 데이터

인터넷이나 개인 네트워크를 통해 이동하는 데이터로서 보안 전송은 여러 계층에서 처리할 수 있고 네트워크를 통해 데이터를 보내기 전에 응용 프로그램 계층에서 데이터를 암호화 가능. 예) HTTPS

사용 중인 데이터

RAM 또는 CPU 캐시와 같은 비영구적 저장소의 데이터 보안과 관련. CPU가 데이터를 처리하는 동안 데이터를 보호하고 암호화된 상태로 유지하는 보안 잠금 생성 기술(Enclave)을 통해 구현

해시 (Hash)

해시 함수란 임의의 길이를 가지고 있는 메시지를 받아들여 고정된 길이의 출력값으로 변환시켜 주는 함수를 말한다. 해시 함수에 의해 출력되어 나온 값을 '해시값(Hash Value)'이라고 한다.

임의의 메시지

해시값

https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/5-describe-encryption-hashing

사이버 보안에서의 해시 함수

- 기밀성과 무결성을 위한 용도로 사용
- 비밀번호와 같은 임의의 정보를 해시 함수에 통과시키면, 고정길이의 해시값으로 출력
  - 복호화 어려움
  - 문서 축약
  - 위변조 여부 검증
- 이러한 특징은 비밀번호 암호화, 전자서명, 블록체인 등에서 기반 기술로 사용되는데 중요한 역할을 한다.

해시에서 알아야 할 것

모두 암호화 기법이지만 해시는 단방향 암호화 기법이고 암호화(Encryption)는 양방향 암호화 기법이다. 해시는 비밀번호 “abcdefhgi23456”을 해시함수를 이용하여 고정된 길이의 암호화된 문자열로 변환하는 것이다.

해시 알고리즘은 모두에게 알려져 있다.

→ 해시 알고리즘은 해커들에게도 공개되어 있기 때문에 해시 알고리즘을 만들 때 엄청나게 많은 검증을 거치게 되고 많은 개발자들이 검증된 것들을 사용한다.

해시 알고리즘은 특정 입력에 대해 항상 같은 해시 값을 리턴한다.

→ 어떤 입력인지 몰라도 해시함수를 이용해서 해시된 값이 일치하면 입력이 같다는 점을 이용해서 ‘인증’이 가능하다.

해시 함수를 이용해서 변환한다고 보안이 완벽하다고 할 수 없다.

→ 해커가 무차별적으로 임의의 값을 입력하면서 비밀번호를 알아낼 수 있다. 이것을 보안하기 위해 비밀번호에 솔트(salt)값을 넣는 방법과 해시 함수를 여러 번 돌리는 방법이 있다. 솔트값을 사용하면 대량의 개인정보 유출을 막을 수 있다.

규정 준수에서 알아야 할 개념

현재 매일 엄청난 데이터가 생성되고 활용되고 있기 때문에 데이터에 대한 의존도가 갈수록 높아지고 있다. 이러한 데이터를 수집, 보존하는데 필요한 규정에 대해서 알아본다.

데이터 보존

데이터를 저장할 수 있는 실제 위치, 그리고 다른 국가에서 데이터를 전송, 처리, 액세스할 수 있는 방법에 대한 정보를 제공한다.

데이터 주권

데이터 특히 개인 데이터가 실제로 수집, 보관, 처리되는 국가/지역의 법률과 규정이 데이터에 적용된다.

데이터 프라이버시

프라이버시에 관한 법률과 규정의 기본 원칙은 개인 데이터 수집, 처리, 사용, 공유 방식을 명확하게 설명하고 관련 공지를 제공해야 한다.

보안에서 ID의 개념

ID (Identification)

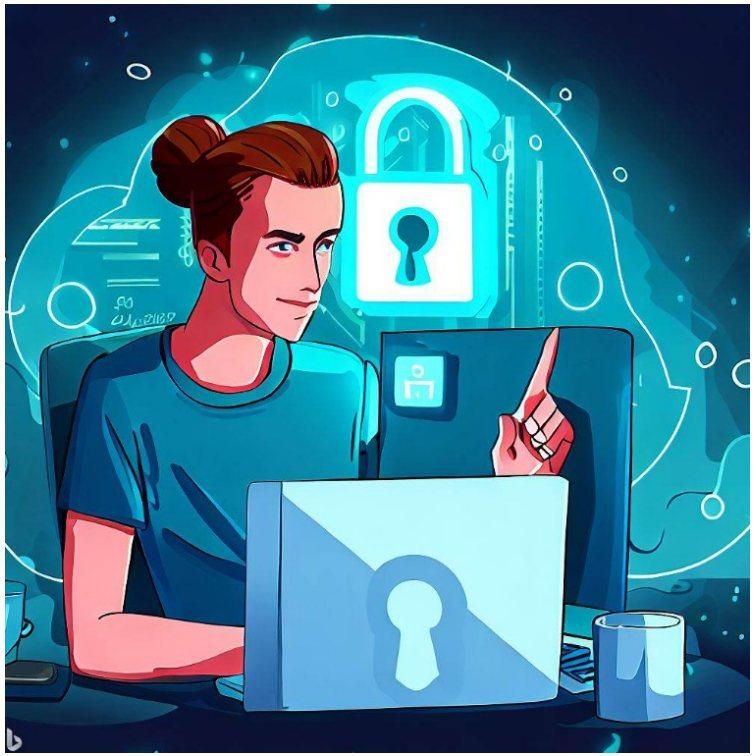
모든 사람과 장치에는 서비스에 액세스하는 데 사용할 수 있는 ID가 있다. ID는 네트워크와 클라우드에서 사람과 사물을 식별하는 방식으로 누가 또는 무엇이 조직의 데이터 및 기타 서비스에 액세스하는지 확인하는 기본이다.

Cloud ID

- 중앙에서 사용자와 그룹을 관리하는 IDaaS(Identity as a Service)
- Cloud ID를 사용하면 조직에서 사용되는 계정을 보다 세부적으로 제어할 수 있다.
- 클라우드 리소스에 대한 액세스 권한을 관리하는 데 사용되며, Cloud ID를 사용하면 사용자 및 그룹을 중앙에서 관리할 수 있다.

인증 (Authentication, AuthN)

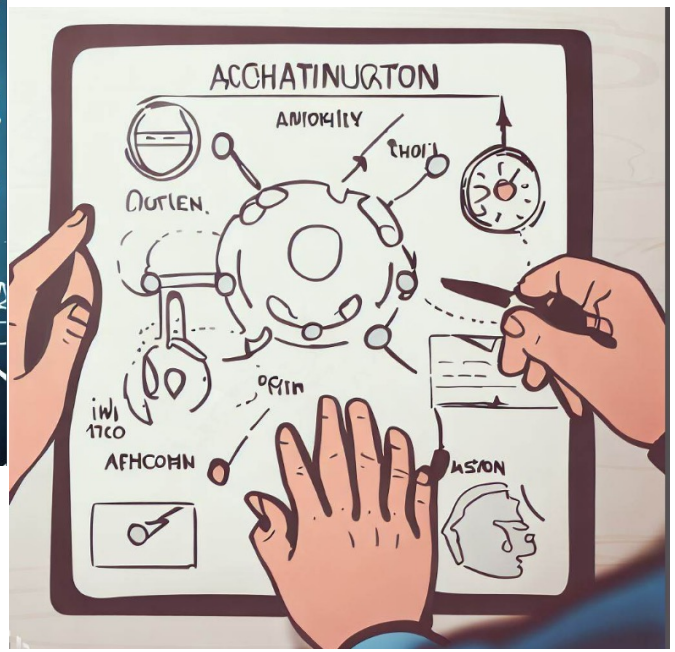
클라우드 내의 리소스에 접근하려는 개인, 서비스 또는 디바이스의 ID를 검증하는 과정이다. 공항에서 여권으로 신원을 확인하는 과정과 유사하다.



- 인증은 사람이 말하는 사람이 맞는지 증명하는 과정이다.
- 신용 카드로 물품을 구매하는 경우 추가 신분증을 제시해야 한다. 이것은 그들이 카드에 이름이 표시된 사람임을 증명하는 것으로 사용자는 자신의 ID를 증명하는 일종의 인증 역할을 하는 운전면허증을 보여 줄 수 있다.

권한 부여 (Authorization, AuthZ)

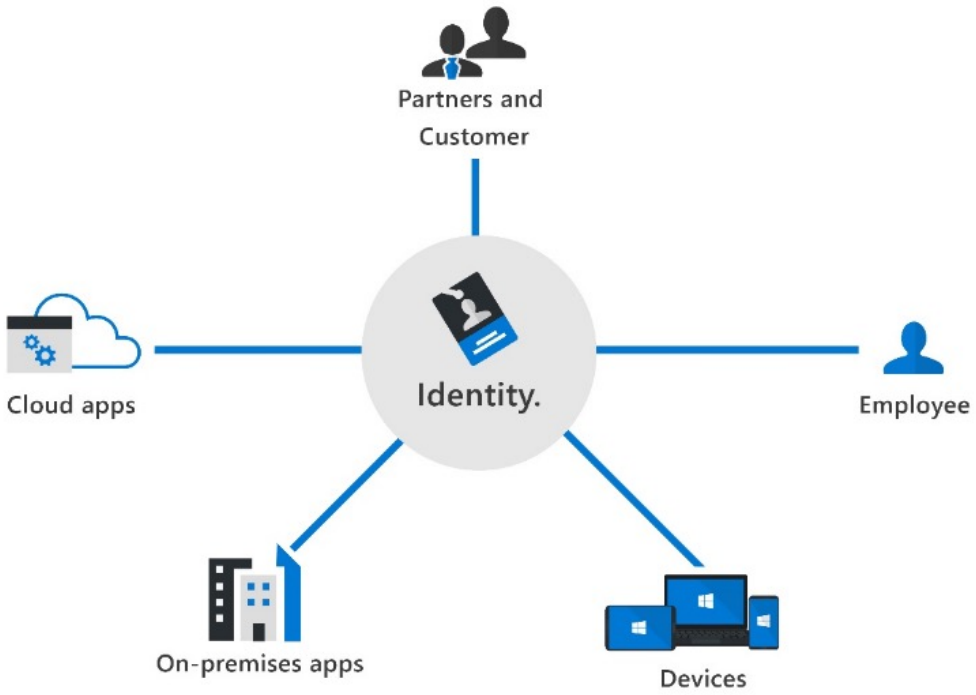
권한 부여는 인증된 사용자에게 제공되는 데이터와 리소스에 대한 액세스 또는 권한 수준을 결정하는 과정이다.



- 호텔에서 숙박할 때 가장 먼저 할 일은 리셉션으로 이동하여 '인증 프로세스'를 시작하는 것이다. 접수원이 당신이 누구인지 확인하면 키 카드를 받고 방으로 한다. 키 카드를 인증 프로세스이다.
- 키 카드를 사용하여 호텔 객실과 같이 액세스가 허용된 문과 엘리베이터를 열 수 있게 되는데 이것을 권한 부여이다.

보안의 기본은 ID

디지털 협업이 달라지고 있고 회사는 재택 근무를 일반화하고 있기 때문에 직원은 언제 어디서나 모든 장치에서 협업하고 회사의 리소스에 액세스해야 한다.



https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/3-define-identity-primary-security-perimeter

- 기업의 보안은 더 이상 기업 자체 내의 네트워크에 한정할 수 없다.
- 회사는 기존의 경계 기반 보안 모델로는 충분하지 않고 다음으로 확장되어야 한다.
  - 회사 네트워크 외부에서 구동되는 SaaS 애프리케이션
  - 직원이 재택 근무 중에 회사 리소스에 액세스하는데 사용하는 개인 장치
  - 회사 데이터와 상호 작용하거나 공동 작업할 때 파트너 또는 고객이 사용하는 관리되지 않는 장치
  - 회사 네트워크 전체와 고객 위치 내부에 설치되는 IoT 장치를 포함하는 사물 인터넷

ID 적용의 4가지 원칙

개인의 신원에는 사용자 이름, 암호, 권한 부여 수준과 같은 자신을 인증하는 데 사용하는 정보가 포함되고 이를 ID라고 할 수 있으며 사용자, 애플리케이션, 장치 또는 기타 항목과 연결된다.

관 리	사용자, 장치 및 서비스에 대한 ID의 생성 및 관리에 관한 것으로 관리자는 ID의 특성이 변경(생성, 엡데이트, 삭제)될 수 있는 방법과 상황을 관리
인 증	인증 원칙은 IT 시스템이 신원에 대한 충분한 증거를 확보하는데 필요한 정보를 알려주기 때문에 정당한 자격 증명을 위해 당사자에게 물어보는 행위
권한 부여(승인)	인증된 사람 또는 서비스가 액세스하려는 애플리케이션 또는 서비스 내에서 갖는 액세스 수준을 결정하기 위해 수신 ID 데이터를 처리
감 사	누가 무엇을 어디서 어떻게 수행하는지 추적하는 것으로 심층 보고, 경고 및 ID 관리가 포함

최신 인증

최신 인증은 클라이언트와 서버 간에 사용되는 인증 및 권한 부여 방법을 총칭하는 용어이다.

최신 인증에는 IdP(ID 공급자)의 역할이 중요합니다.

IdP는 인증, 권한 부여 및 감사 서비스를 제공합니다.

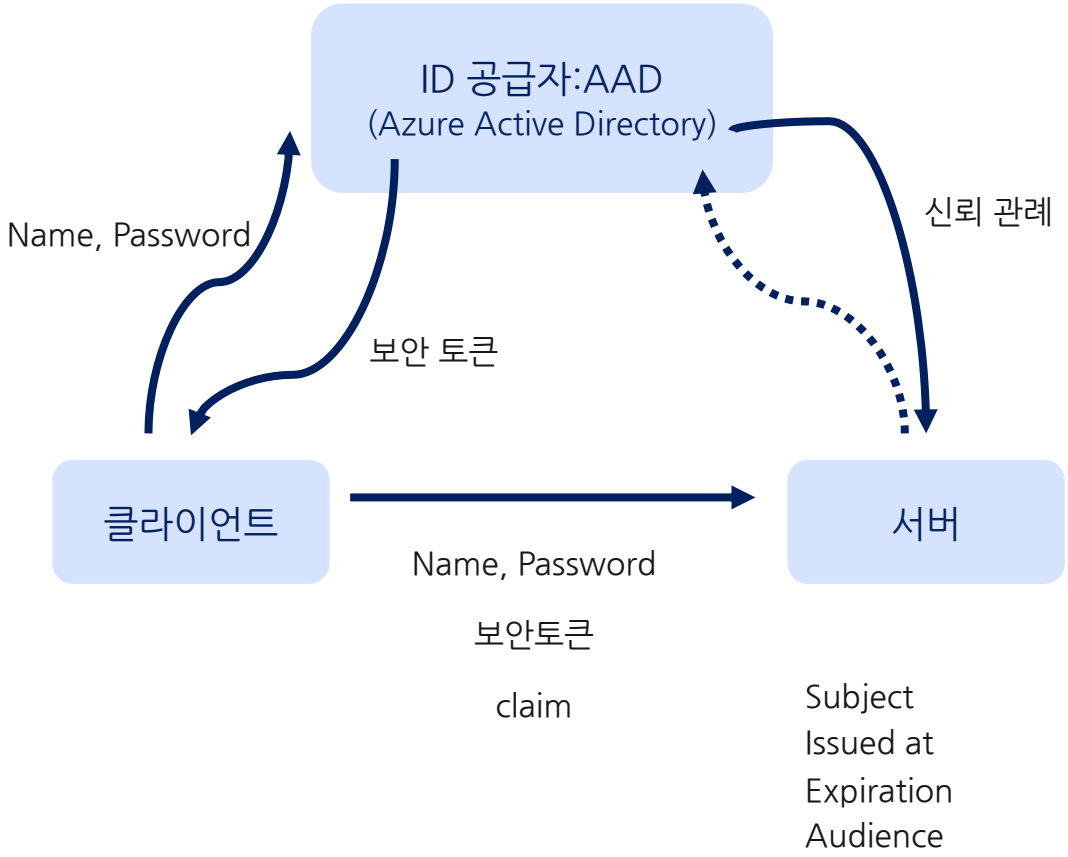
IdP를 사용하는 조직은 인증 및 권한 부여 원칙을 제정하고 사용자 행동을 모니터링하는 등의 다양한 작업을 수행합니다.

IdP와 최신 인증에서 제공되는 기본적인 기능은 SSO(Single Sign-On) 지원입니다.

클라우드 기반 ID 공급자의 예로는 Microsoft Azure Active Directory가 있습니다.

ID 공급자

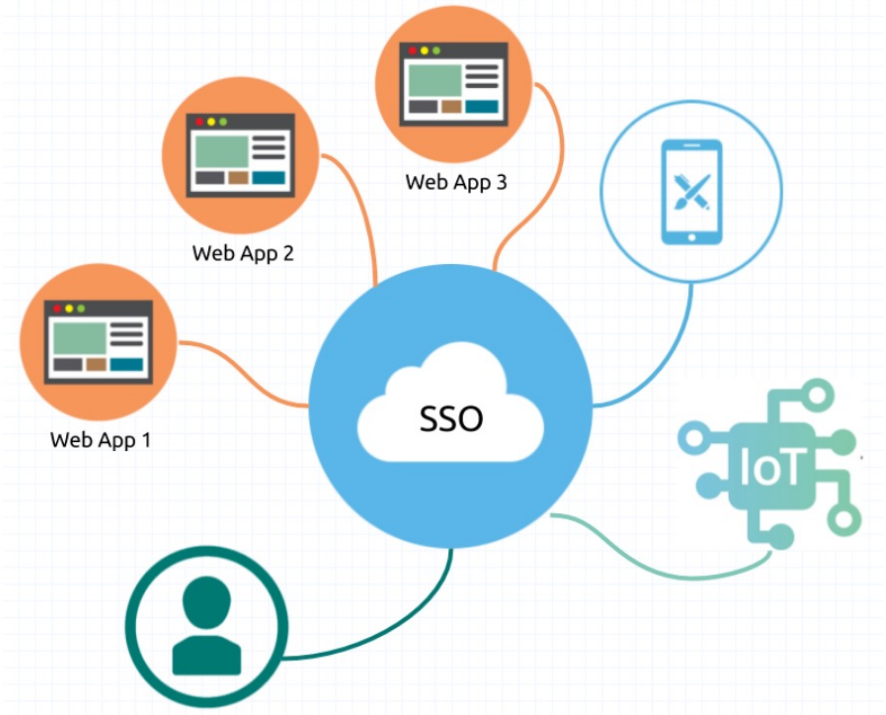
최신 인증의 중심에는 ID 공급자의 역할이 있는데 인증, 권한 부여 및 감사 서비스를 제공하면서 ID 정보를 생성, 유지 및 관리한다. 최신 인증을 사용하면 인증 서비스를 포함한 모든 서비스가 중앙 ID 공급자에 의해 제공된다.



- 서버에서 사용자를 인증하는 데 사용되는 정보는 ID 공급자가 중앙에서 자장하고 관리
- 중앙 ID 공급자를 통해 조직은 인증 및 권한 부여 정책을 설정하고, 사용자 행동을 모니터링하고 의심스러운 활동을 식별
- 마이크로소프트의 Azure Active Directory(AAD)는 클라우드 기반 ID 공급자의 예이다.

싱글 사인 온(Single Sign-On, SSO)

ID 공급자 기본 기능은 SSO(Single Sign-On) 지원이다. SSO를 사용하면 사용자가 한 번 로그인하고 해당 자격 증명을 사용하여 여러 애플리케이션 또는 리소스에 액세스할 수 있다.



https://toma0912.tistory.com/75

- 한번의 로그인으로 여러 다른 사이트에서 자동적으로 접속하여 이용하는 방법
- 일반적으로 서로 다른 시스템에서 각각의 사용자 정보를 관리하고 필요에 따라 사용자 정보를 연동해서 사용
- 하나의 사용자 정보를 기반으로 여러 시스템을 하나의 통합 인증을 사용하게 하는 것
- 하나의 시스템에서 인증할 경우, 타 시스템에서는 인증 정보가 있는지 확인하고, 있으면 로그인 처리하고 없으면 다시 통합 인증을 하도록 만드는 것

디렉토리(Directory)의 개념

컴퓨터 네트워크 분야에서 디렉토리는 네트워크를 구성하는 개체에 대한 정보를 저장하는 계층 구조이다. 디렉토리 서비스는 디렉토리를 저장하고 네트워크 사용자, 관리자, 서비스 및 응용 프로그램에서 사용할 수 있게 한다.

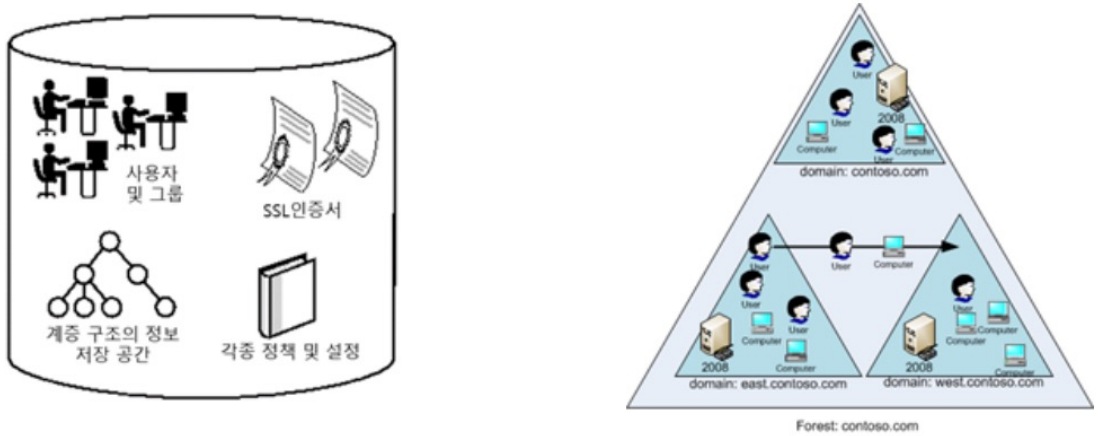


그림) 디렉토리 서비스의 계층적 관리 체계

- 디렉토리 서비스는 디렉터리 데이터를 저장하며 네트워크 사용자, 관리자, 서비스 및 애플리케이션에 이 데이터를 제공
- 이러한 유형의 서비스 중 가장 널리 알려진 것이 온 프레미스 IT 인프라를 사용하는 Active Directory Domain Service(AD DS)이다.
- 더욱 개선된 ID 및 액세스 관리 솔루션인 Azure Active Directory는 조직이 클라우드 및 온 프레미스에서 모든 앱을 관리하는 데 사용할 수 있는 IDaaS(Identity as a Service)를 제공

https://cloud.gowit.co.kr/it%EB%A6%AC%EB%8D%94%EC%89%BD%EA%B3%BC-%EC%A0%84%EB%9E%B5-%EC%99%9C-%EB%94%94%EB%A0%89%ED%86%A0%EB%A6%AC-%EC%84%9C%EB%B9%84%EC%8A%A4%EA%B0%80-it-%EC%97%85%EB%AC%B4%EC%97%90-%EC%A4%91%EC%9A%94/

디렉토리 서비스 (Directory Service)

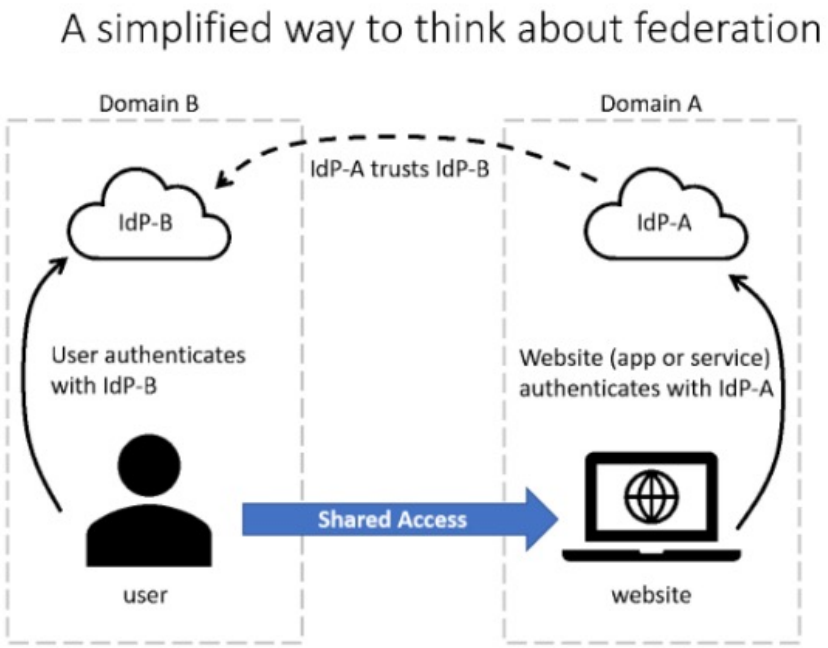
디렉토리는 데이터 집합 또는 목록을 의미하며 IT의 디렉토리 서비스는 기업이 보유한 네트워크 및 컴퓨팅 자원과 사용자 정보를 저장하고 관리해주는 SW 및 응용 프로그램이다.

https://cloud.gowit.co.kr/it%EB%A6%AC%EB%8D%94%EC%89%BD%EA%B3%BC-%EC%A0%84%EB%9E%B5-%EC%99%9C-%EB%94%94%EB%A0%89%ED%86%A0%EB%A6%AC-%EC%84%9C%EB%B9%84%EC%8A%A4%EA%B0%80-it-%EC%97%85%EB%AC%B4%EC%97%90-%EC%A4%91%EC%9A%94/

- 네트워크 자원 - 네트워크에 연결된 컴퓨터(PC, 서버 등), 프린터, 스토리지 등
- 컴퓨팅 자원 - 파일, 보안 인증서, 컴퓨터 설정 정보 등
- 기업은 디렉토리 서비스라는 솔루션을 통해 정확한 IT자원 현황 파악, IT자원 운영 관리 강화, IT예산 운영 효율화 및 보안을 극대화한다.
- 사용자의 로그인 정보, 권한 관리 및 컴퓨터 설정 정보 등의 보안 관리를 중앙에서 통합 운영하고 모든 정보를 이중화하여 암호 분실, 컴퓨터 교체, 보안 위협에 빠르게 대응할 수 있다.
- 싱글 사인 온(SSO)체계 구현으로 사용자의 IT 자원 접근 및 이용 효율을 높여준다.

페더레이션(Federation)

페더레이션을 사용하면 각 도메인의 ID 공급자 사이에 신뢰 관계를 설정하여 조직 또는 도메인 경계를 넘어 서비스에 액세스할 수 있다. 하나의 사용자 이름과 비밀번호를 사용하여 도메인 경계를 넘어 리소스에 액세스할 수 있다.



- 도메인 A의 웹 사이트는 ID 공급자 A(IdP-A)의 인증 서비스를 사용하고 도메인 B의 사용자는 ID 공급자 B(IdP-B)로 인증
- IdP-A와 IdP-B와 신뢰 관계 형성
- 웹 사이트에 접속하려는 사용자가 웹 사이트에 자격 증명을 제공하면 웹 사이트는 사용자를 신뢰하고 액세스를 허용.
- 이는 두 ID 공급자 사이에 이미 설정된 신뢰 때문에 허용되는 것이다.

https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/6-describe-concept-federation