cpl.thalesgroup.com

THALES

액세스 매니지먼트 핸드북

목차

소개

여러분은 액세스 관리에 대한 수많은 정보를 들었을 것입니다. "인증"과 "액세스 관리"라는 두 용어는 거의 동일한 의미로 사용되고 있습니다. 하지만 이 둘 사이에는 차이가 존재합니다. 인증은 사용자의 ID를 평가하는 반면, 액세스 관리는 사용자가 특정 리소스에 접근할 수 있는 권한을 갖고 있는지 결정하며 그 리소스에 대해 설정된 액세스 정책을 실행합니다.

액세스 관리는 클라우드 리소스에 대한 접근 관리할 때 매우 중요합니다. 요즘은 하루에도 수많은 클라우드 앱에 액세스해야 합니다. 이것은 사용자와 IT 팀 모두에게 귀찮은 일입니다. 사용자는 수많은 비밀번호를 기억해야 하고, IT 팀은 잊어버린 비밀번호를 끝없이 초기화해야 합니다. 이 문제에 대한 해결책이 바로 SSO입니다. 사용자는 모든 클라우드 앱에 대해 하나의 인증서만 소유함으로써 여러 앱에 한 번에 손쉽게 로그인할 수 있고, IT 팀은 비밀번호 초기화에 소모되는 귀중한 시간을 절감할 수 있습니다.

단일 ID는 오직 그것을 평가하기 위해 사용되는 인증만큼만 안전하기 때문에, 클라우드 액세스 보안의 유지를 위해 사용자 ID를 확인하는 방법이 매우 중요해지고 있습니다. 이를 위해, 액세스 관리 솔루션과 싱글사인온 솔루션은 애플리케이션별로 정의된 액세스 정책에 대해 세부 제어기능을 제공합니다. 고위험 상황에서 추가 인증 요소를 요청함으로써 원활한 사용자 경험을 유지할 수 있습니다.

액세스 관리 용어집

인증 및 액세스 관리

인증과 액세스 관리 솔루션은 ID 관할 및 관리(IGA) 기능과 액세스 관리(AM) 기능으로 구성됩니다. IAM 솔루션은 애플리케이션에 대한 액세스 권한을 부여(및 요청)하고(IGA), 액세스 컨트롤을 시행하며(AM), 액세스 이벤트에 대한 가시성을 확보하기 위한(AM) 체계적인 프레임워크를 제공합니다. 대부분의 조직에서 IGA와 AM 구성요소를 각기 별도로 배포한다는 점을 고려할 때, 이들 분야는 단일한 인증 및 액세스 관리의 복합적인 기능이 아니라 서로 독립적인 솔루션 제품군으로 평가되는 경향이 높아지고 있습니다.

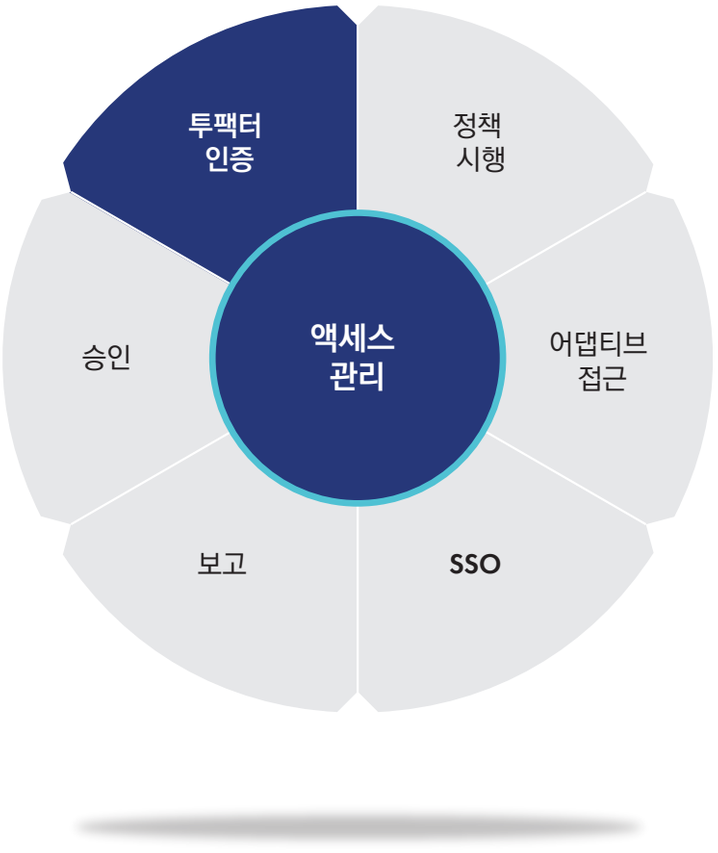
액세스 관리

액세스 관리란 사용자가 특정 리소스에 대한 액세스 권한을 갖고 있는지 여부를 결정하고 그 리소스에 대해 설정된 액세스 정책을 시행하는 기능입니다.

액세스 관리는 IT 관리자가 정의한 액세스 정책을 기반으로 구현되며, 어떤 사용자 그룹(예: 판매, 연구개발, 인사)이 어떤 클라우드 애플리케이션(예: Salesforce, Office 365, Jira, Taleo)에 액세스할 수 있는지와 같은 정보를 포함합니다. 여기에는 각 애플리케이션에 액세스하는 데 필요한 다양한 사용자 속성(예: 신뢰할 수 있는 네트워크, 비밀번호, OTP) 역시 포함됩니다.

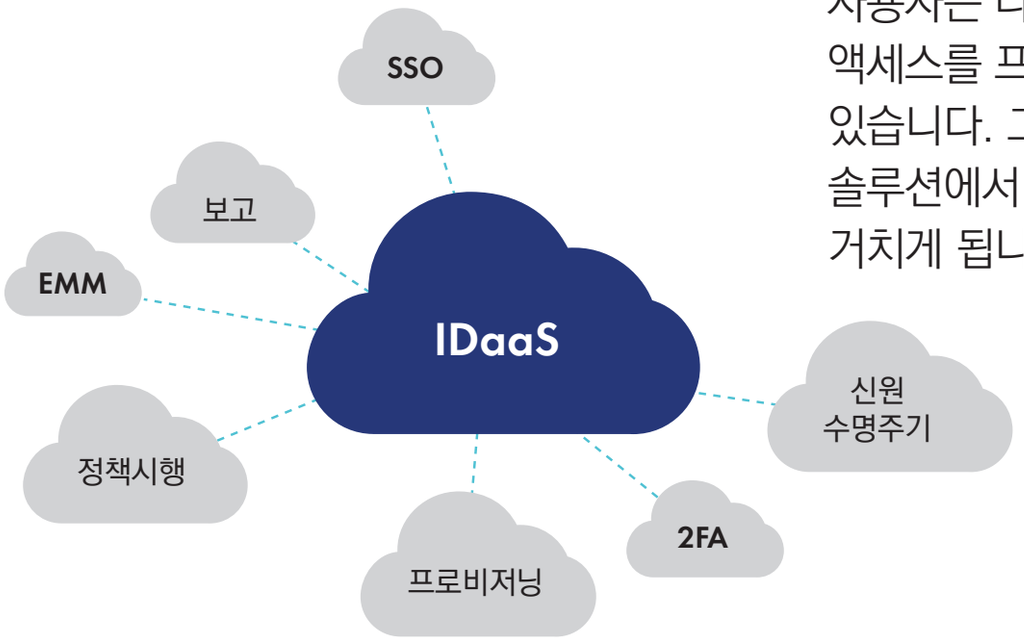
액세스 정책에 따라 평가해야 하는 사용자 속성은 클라우드 애플리케이션의 민감도에 따라 더 많거나 적을 수 있습니다. 이러한 속성은 위험 기반 또는 컨텍스트 기반 인증을 사용하여 평가되며, 이는 각 클라우드 애플리케이션에 대해 정의된 다양한 액세스 정책을 시행하는 데 있어 핵심이 됩니다. (자세한 내용은 컨텍스트 기반 인증 섹션을 참고하십시오.)

또한 클라우드 액세스 관리의 중심에는 싱글사인온(SSO)이 있습니다. SSO는 단일 사용자 이름 및 비밀번호 세트(즉 'ID')를 사용하여 모든 클라우드 애플리케이션에 로그인할 수 있도록 하는 기능입니다. (자세한 내용은 싱글사인온 섹션을 참고하십시오.)



IDaaS

IDaaS란 IAM-as-a-Service(ID 서비스라고도 함)의 약어로, 액세스 관리 및 인증을 위한 클라우드기반 서비스를 제공하는 ID 및 액세스 관리(IAM) 솔루션을 설명하는 용어입니다. 지난 수년 간 IDaaS는 최근의 시장 동향을 고려하여 하나의 독립된 시장으로 평가되어 왔습니다. 그러나 앞으로는 액세스 관리와 IGA라는 두 개의 독립된 분야로 나뉘어 취급될 으로, 전달 방식은 온프레미스 설치, 소프트웨어, 클라우드 기반 플랫폼 등이 될 것으로 예상됩니다.



ID 관할 및 관리(IGA)

ID 관할 및 관리(IGA) 솔루션은 "누가 액세스를 받아야 하는가, 또는 누가 어떤 애플리케이션에 대한 '액세스 자격을 받았나'?" 및 "실제로 누가 어떤 애플리케이션에, 누구에 의해 언제 액세스를 부여받았나?"에 대한 답을 찾을 수 있도록 지원합니다. 예를 들어, IGA 솔루션은 연구개발 직원이 GitHub, Jira, Confluence 와 같은 특정 개발 애플리케이션에 액세스 자격을 받을 수 있도록 설정할 수 있게 도와줍니다. IGA 솔루션은 직원의 연구개발 그룹 멤버십을 기반으로 이러한 애플리케이션에 대한 액세스를 자동으로 프로비저닝할 수 있습니다. 또 연구개발 사용자는 다른 애플리케이션에 대한 액세스를 프로비저닝할 것을 요청할 수도 있습니다. 그러면 이 요청은 일부 IGA 솔루션에서 지원하는 관리 승인 프로세스를 거치게 됩니다.

ID 연계

신뢰할 수 있는 ID 제공자("IdP")라고 불리는 단일 시스템은 ID 연계를 통해 사용자의 인증을 관할합니다. 사용자가 클라우드 앱에 액세스하려고 할 때마다 항상 그 앱이 인증 프로세스를 이 ID 제공자에게 중계하는 방식입니다. 연계형 ID는 조직의 내부든 외부든 관계없이 수많은 웹 앱에 대한 자격 증명을 별도 관리함으로써 발생하는 어려움과 불편을 해결합니다. ID 연계는 SAML 및 OpenID Connect 같은 연계 프로토콜뿐만 아니라 Microsoft의 WS-Federation 같은 독점 프로토콜도 사용합니다.

연계형 로그인

연계형 로그인은 SAML, OpenID Connect 등과 같은 연계 프로토콜의 한 기능으로서, ID 제공자의 모델을 사용하여 사용자를 인증하고 해당 인증 정보를 "인증 주장(authentication assertion)"의 형식으로 대상 시스템에 중계합니다. 이 주장에는 '수락' 또는 '거부' 응답이 포함되어 있고, 이로써 사용자의 액세스가 거부 또는 허용됩니다.

사용자는 연계형 로그인으로 한 번만 로그인하고 자신의 모든 클라우드 애플리케이션에 액세스할 수 있습니다. 연계형 로그인을 사용하면 클라우드 애플리케이션마다 각기 다른 사용자 이름과 비밀번호 세트(즉 "ID")를 사용하여 로그인할 필요 없이, 오전에 기업 네트워크에 로그인할 때 또는 야간에 VPN으로 로그인할 때 사용하는 것과 동일한 ID로 Office 365, Salesforce, AWS 등에 로그인할 수 있습니다.

신뢰할 수 있는 ID 제공자라고 불리는 단일 시스템은 ID 연계를 통해 사용자의 인증을 관할합니다. 사용자가 클라우드 앱에 액세스하려고 할 때마다 항상 그 앱이 인증 프로세스를 이 ID 제공자에게 중계하는 방식입니다.

ID 제공자

SAML, 그리고 비가맹 웹사이트 간에 ID 데이터를 안전하게 교환할 수 있는 다른 ID 연계 프로토콜은 ID 제공자(IdP) 및 서비스 제공자 모델을 기반으로 합니다. 사용자가 서비스 제공자(클라우드 기반 서비스)에 액세스하면, 인증 및/또는 승인 데이터를 위해 신뢰할 수 있는 ID 제공자에게 리디렉션됩니다. ID 제공자는 사용자 인증 데이터(예: 사용자 쿠키, 장치, 네트워크, OTP)를 확인하고 "수락" 또는 "거부" 응답을 생성한 다음 서비스 제공자에게 전송합니다. 승인 데이터에는 웹메일 계정의 이메일 주소나 소셜 네트워크 계정의 친구 이름과 같은 정보에 액세스할 수 있는 권한이 포함될 수 있습니다.

예를 들어, SafeNet Trusted Access는 사용자가 위의 상황에서와 같이 클라우드 애플리케이션에 액세스할 때 ID 제공자로서 작동합니다.

보안 토큰 서비스

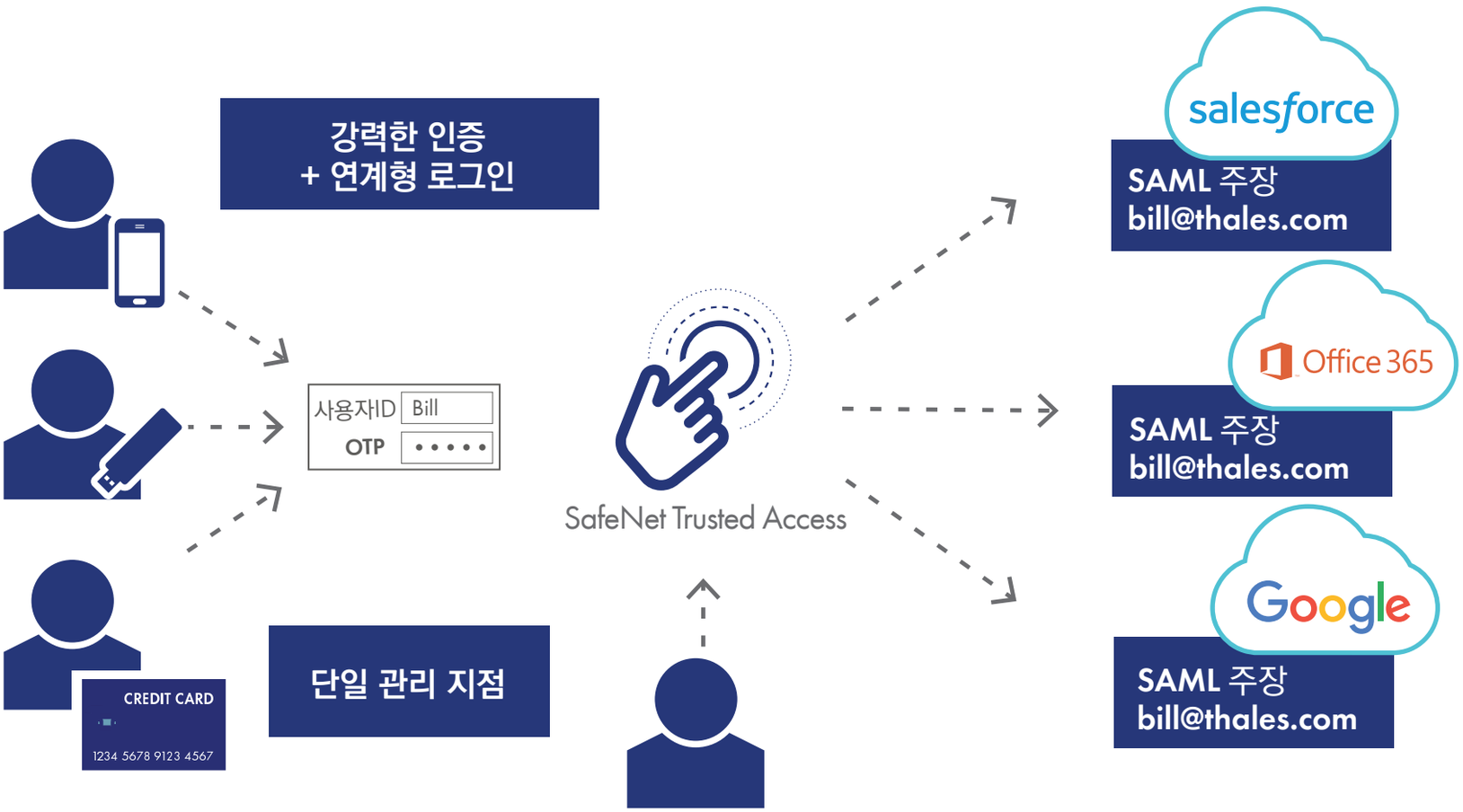
ID 제공자 모델은 토큰 기반 인증 또는 보안 토큰 서비스라고도 불립니다. 보안 토큰 서비스(STS)는 ID 제공자에 해당하며, 위탁 당사자(RP)는 서비스 제공자에 해당합니다. 또 SAML 인증 주장의 교환 대신에, 보안 토큰이라고 부릅니다. 다른 이름이지만 개념은 동일합니다.

SAML

SAML(Security Assertion Markup Language)은 '샘엘'이라고 발음하며, 인증정보 제공자와 서비스 제공자 간의 인증 및 인가 데이터를 교환하기 위한 개방형 표준 데이터 포맷입니다. 샘엘은 ID연계 또는 연계형 인증으로 불리우기도 합니다. ID 연계란 사용자의 현재 기업 ID를 클라우드로 확장하여 자신의 현재 기업 ID로 클라우드 애플리케이션에 로그인할 수 있는 기능을 의미합니다. SAML을 사용한 클라우드 앱에 대한 연계형 인증을 통해 사용자는 자신의 기업용 ID로 모든 클라우드 애플리케이션에 로그인할 수 있습니다. 즉 사용자 이름 및 비밀번호 세트를 수십개가 아닌 단 1개만 유지 관리하면 되는 것입니다.

SAML이 작동하는 방법

사용자가 클라우드 기반 애플리케이션에 로그인하려고 하면 인증을 위해 신뢰할 수 있는 ID 제공자에게 리디렉션됩니다. ID 제공자는 사용자의 자격 증명(예: 사용자 이름 및 일회용 비밀번호)을 수집하여 응답을 액세스 시도 중인 클라우드 애플리케이션에 반환합니다. 이 응답을 SAML 주장이라고 하며 SAML 주장에는 수락 또는 거부 응답이 포함되어 있습니다. 이 응답에 따라 서비스 제공자(예: Salesforce, Office 365, DropBox)는 애플리케이션에 대한 액세스를 차단하거나 허용합니다.



WS-Fed

WS-Federation Services(WS-Fed)는 Microsoft의 독점 ID 연계 프로토콜입니다. WS-Fed는 Microsoft의 Active Directory Federation Services(AD FS)와 함께 작동하여 Active Directory에 저장된 ID를 Office 365나 Azure 같은 Microsoft의 클라우드 애플리케이션으로 확장합니다. SAML처럼, WS-Fed는 ID 제공자 모델을 사용합니다. Microsoft 클라우드 애플리케이션에 액세스할 때 사용자는 인증을 위해 AD FS로 리디렉션되고, 그 응답에 따라 해당 클라우드 애플리케이션은 사용자에게 액세스 권한을 부여 또는 거부하게 됩니다.

OAuth

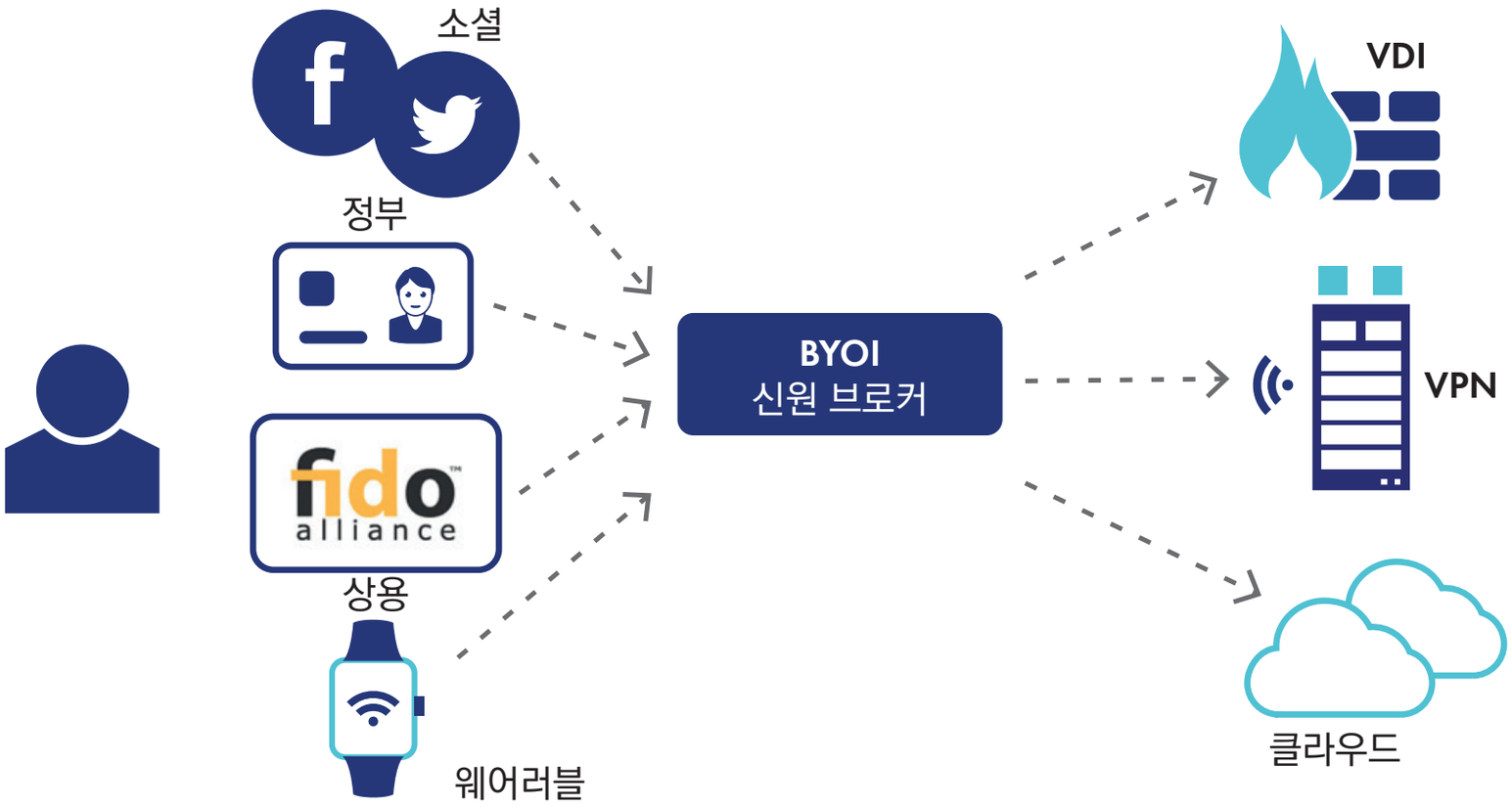
공개 승인(Open Authorization)의 줄임말인 OAuth는 "오-오스"라고 발음하며, 비가맹 웹사이트 간의 연계형 또는 "토큰 기반" 인증 및 승인을 위한 공개 표준입니다. SAML, OpenID Connect, WS-Fed 같은 다른 ID 연계 프로토콜과 마찬가지로, OAuth 도 신뢰할 수 있는 ID 제공자에게 확인된 ID로 애플리케이션에 로그인할 수 있게 해줍니다. OAuth는 연계형 인증을 뛰어넘어 사용자가 위탁 당사자(RP) 웹사이트에 연락처 이름 및 이메일 주소와 같은 특정 계정 정보에 액세스할 수 있는 권한을 부여할 수 있게 해줍니다. 예를 들어 소셜 네트워크 웹사이트에서 사용자의 웹메일 연락처에 액세스하여 웹메일 연락처에 있는 사람을 사용자의 소셜 네트워크에 초대할 것인지 물을 때 사용하는 프로토콜이 OAuth입니다.

OpenID Connect

SAML과 마찬가지로 OpenID Connect는 ID 제공자 모델을 사용하는 공개 표준 ID 연계 프로토콜입니다. 그러나 쿠키를 사용하여 작동하기 때문에 브라우저에서 열리는 애플리케이션('브라우저 기반 애플리케이션')에 대해서만 작동하는 SAML과 달리, OpenID Connect는 브라우저 기반 애플리케이션, 네이티브 모바일 앱, 데스크톱 클라이언트 (예: 리치 클라이언트 및 일부 VPN) 모두에서 싱글사인온을 구현할 수 있는 싱글사인온 프레임워크를 제공합니다. 따라서 오늘날 대부분의 싱글사인온 구현은 클라우드 및 브라우저 기반 앱만 지원하지만, OpenID Connect를 채택하는 ID 제공자가 증가하고 있기 때문에, 데스크톱 클라이언트, 브라우저 기반 애플리케이션, 네이티브 모바일 애플리케이션 등 어떠한 리소스에도 단 한 번의 인증으로 동시에 접근할 수 있게 될 것입니다.

ID 각자 준비(BYOI)

벤더와 조직은 직원과 파트너로 하여금 자신의 ID를 사용하여 기업 리소스에 액세스할 수 있는 방법을 찾고 있습니다. 충분한 수준의 ID 보장을 제공하기만 한다면 이론적으로는 어떤 ID든 가능합니다. 예를 들어 정부 발급 신분증, 의료용 스마트 카드뿐 아니라 사회복지 관련 ID, 업계 인력 교류 모임 관련 ID, FIDO 같은 상용 ID도 가능합니다. 소비자 서비스에서 통상 볼 수 있는 것과 동일한 유형의 인증 방법을 구현해야 한다는 요구를 그 어느때 보다 많이 받고있는 기업 보안 팀과 함께, 기업의 세계와 소비자의 세계가 서로 융합되고 있습니다.



싱글사인온(SSO)

싱글사인온(SSO)은 다양한 리소스에 액세스할 때 한 번 인증하고 나면 차후 자동으로 인증되는 기능을 제공합니다. 개별 애플리케이션과 시스템에 따로 로그인하고 인증할 필요가 없으며, 본질적으로 사용자와 대상 애플리케이션 사이의 중개자 역할을 합니다. 대상 애플리케이션과 시스템은 이면에서는 여전히 자체 자격 증명 스토어를 유지하고 사용자 시스템에 사인온 프롬프트를 표시합니다. SSO는 이러한 프롬프트에 응답하고 자격 증명을 단일 로그인/비밀번호 쌍에 매핑합니다. (출처: Gartner)

독립된 개별 솔루션이든 더 넓은 범위의 액세스 관리 솔루션이든, SSO는 다양한 ID 연계 프로토콜을 통해 달성할 수 있습니다. 여기에는 SAML 2.0 및 OpenID Connect와 같은 오픈 소스 프로토콜, Microsoft의 WS-Federation과 같은 독점 프로토콜, 그리고 비밀번호 저장 및 리버스 프록시와 같은 그 밖의 기술이 포함됩니다.

비밀번호 저장소

비밀번호 관리자라고도 부르는 비밀번호 저장소는 대상 애플리케이션이 ID 연계 프로토콜을 지원하지 않는 경우(예: 레거시 또는 사용자 정의된 애플리케이션) 싱글사인온(SSO) 환경을 간단하게 만들 수 있는 방법입니다. 비밀번호 저장소는 다른 웹사이트의 비밀번호를 저장하고 암호화하여 작동하는 시스템입니다. 사용자는 애플리케이션마다 따로 전용 비밀번호를 사용하여 로그인하는 대신 (암호 저장소를 해독하는) 마스터 비밀번호로 간단하게 인증할 수 있으므로 별도의 암호를 유지할 필요가 없습니다.

승인

승인은 인증된 사용자가 액세스가 허용된 리소스에만 접근할 수 있도록, 해당 리소스의 소유자나 관리자가 정의하는 프로세스입니다. 소비자 세계에서 승인은 사용자가 클라우드 기반 애플리케이션(예: 소셜 네트워크)이 비가맹 웹사이트(예: 사용자의 웹메일 계정)의 특정 정보에만 접근할 수 있도록 정의하는 프로세스를 이르는 용어일 때도 있습니다.

인증

인증은 애플리케이션, 서비스, 컴퓨터 또는 디지털 환경에 로그인할 때 사용자가 제공한 자격 증명을 기반으로 사용자의 ID를 검증하거나 확인하는 프로세스입니다. 대부분의 인증 자격 증명은 사용자가 가지고 있는 어떤 것(예: 사용자 이름)과 사용자가 알고 있는 어떤 것(예: 비밀번호)으로 구성됩니다. 사용자가 제공한 자격 증명이 기본 애플리케이션이나 ID 제공자가 저장되어 있는 자격 증명과 일치하면 성공적으로 사용자 인증이 완료되어 액세스 권한을 받게 됩니다.

컨텍스트 기반 인증

컨텍스트 기반 인증은 개인이 애플리케이션에 로그인할 때 다양한 보충 정보를 평가하여 사용자의 ID를 확인합니다. 가장 일반적인 컨텍스트 정보 유형으로는 사용자의 위치, 시간, IP 주소, 장치 유형, URL, 애플리케이션 평가 등이 있습니다. 위험 기반 인증 또는 적응형 인증이라고도 부르는 컨텍스트 기반 인증의 인증과정은 SSO 및 액세스 관리 세계의 핵심이며, 이 과정을 가급적 투명하고 고통이 없도록 하는 것이 목표입니다.

싱글사인온 및 액세스 관리 솔루션은 컨텍스트 기반(장치, 역할, 위치) 또는 행동 기반(입력 속도, 페이지 보기 순서)에 따라 사용자의 로그인 속성을 평가함으로써, 각 애플리케이션에 대해 정의된 액세스 정책에 맞추어 사용자에게 요구되는 인증 수준을 지속적으로 일치시킬 수 있습니다. 이러한 방식으로 인증이 모든 기업 리소스에 대한 포괄적이고 동일한 규칙이 아니라 애플리케이션의 액세스 정책에 따라 가능한 한 가장 마찰이 없는 방식으로 세분화되어 적용됩니다.

지속적 인증

인증은 기본적으로 토큰이나 비밀번호나 지문을 활용하여 예와 아니요 중 하나를 결정하는 것입니다. 즉 시스템은 사용자 ID를 확인하고 그에 따라 액세스를 허용 또는 거부합니다.

그러나 컨텍스트 기반 인증이나 행동기반 생체인식(예: 입력 패턴 및 기타 물리적 특성)과 같은 최신 기술 덕분에 인증이 보다 지속적인 프로세스가 되고 있습니다. IP 주소, 모바일 매개변수, 알려진 장치, 운영체제 등의 다양한 속성을 평가함으로써, 컨텍스트 또는 위험 기반 인증은 한 개인이 애플리케이션에 로그인할 때마다 ID를 지속적으로 확인할 수 있습니다. 사실 사용자가 알지 못하는 상태에서도 이것이 가능합니다.

컨텍스트 기반 인증 덕분에 개인의 ID를 매끄럽게 확인할 수 있는 방법이 많아졌습니다. 또한 바로 이 덕분에 수많은 클라우드 애플리케이션에 세부적인 액세스 컨트롤을 적용하는 능력과 사용자 편의 사이에서 균형을 맞출 수 있게 되었습니다. 컨텍스트 기반 인증을 기반으로 하는 지속적 인증의 개념이 클라우드 액세스 관리의 근간이 되는 이유가 바로 여기에 있습니다.

대한민국 – 서울특별시 용산구 한남동 독서당로 98 여선교회관 6층
| 전화: 82.2.3278.8202 팩스: 82.2.3278.8290 |
이메일: krsales.cpl@thalesgroup.com

> cpl.thalesgroup.com <