

액세스 관리 핸드북



목차

서론

3

액세스 관리 용어집

4

ID 및 액세스 관리(IAM)

4

액세스 관리

5

IDaaS

6

ID 거버넌스 및 관리(IGA)

6

ID 페더레이션

7

통합 로그인

7

ID 제공자

8

SAML

9

WS-Fed

11

Open ID Connect

13

싱글 사인 온 (SSO)

15

패스워드 볼트

16

권한 부여

17

인증

17

컨텍스트 기반 인증

18

지속적 인증

19

서론

여러분은 오랫동안 액세스 관리에 대해 수많은 이야기를 들었을 것입니다. 사실상 우리는 ‘인증’과 ‘액세스 관리’라는 말을 같은 뜻으로 사용하는 경향이 있습니다. 그러나 사실 두 표현에는 차이가 있습니다. 인증을 통해 사용자의 ID가 검증되면, 액세스 관리는 사용자가 특정 리소스에 액세스할 수 있는 권한을 가지고 있다고 판단하여 해당 리소스에 설정된 액세스 정책을 적용하게 됩니다.

액세스 관리는 클라우드 리소스에 대한 액세스를 관리하는 데 있어 매우 중요한 요소입니다. 요즘 일반적으로 하루 종일 수많은 클라우드 애플리케이션에 액세스해야 합니다. 이것은 사용자와 IT 모두에게 번거로운 일입니다. 사용자는 수많은 패스워드를 외워야 합니다; 한편으로 IT 부문은 분실 패스워드를 수없이 재설정해야 합니다. 이 문제의 해결 방법이 바로 SSO입니다. 모든 클라우드 애플리케이션에 하나의 인증 정보를 부여함으로써 사용자는 한 번의 로그인으로 쉽게 여러 애플리케이션에 액세스할 수 있으므로 패스워드 재설정 소요되는 시간을 절약할 수 있습니다.

단일 ID는 이를 검증하기 위해 사용되는 인증 수준만큼 안전하기 때문에, 클라우드 액세스 보안을 유지하는 데 있어 사용자 ID의 검증 방식이 가장 중요합니다. 이 때문에 액세스 관리 솔루션과 싱글 사인 온 솔루션을 통해 애플리케이션 별로 정의된 액세스 정책을 세밀하게 제어할 수 있습니다. 위험도가 높은 상황에서 추가 인증 요소를 요구함으로써 마찰이 없는 사용자 경험이 유지됩니다.



액세스 관리 용어집

ID 및 액세스 관리(IAM)

ID 및 액세스 관리(IAM) 솔루션은 ID 거버넌스 및 관리(IGA) 기능과 액세스 관리(AM) 기능으로 구성되어 있습니다. IAM 솔루션은 애플리케이션에 대한 액세스를 허가(및 요청)하고(IGA), 액세스 제어를 실시하며(AM), 액세스 이벤트의 가시성을 확보(AM)하기 위한 체계적인 프레임 워크를 제공합니다. 대부분의 조직에서 IGA와 AM 컴포넌트를 각각 따로 배치하는 점을 감안했을 때 이 분야는 단일 IAM 스위트의 복합 기능이 아닌 개별적으로 독립된 솔루션군으로 점차 평가를 받고 있습니다.

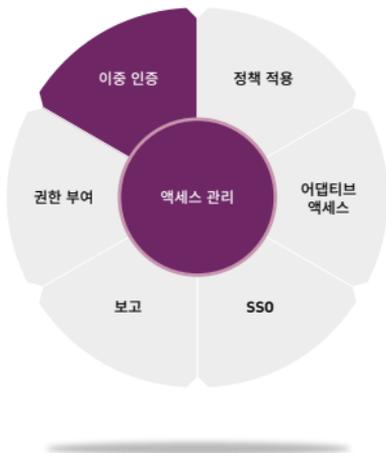
액세스 관리

액세스 관리는 사용자가 특정 리소스에 액세스하기 위한 권한을 가지고 있는지 판단하여 해당 리소스에 설정된 액세스 정책을 적용시킬 수 있는 기능입니다.

액세스 관리는 IT 관리자에 의해 정의된 액세스 정책에 기반하여 구현되며 어떤 그룹의 사용자(예: Sales, R&D, HR)가 어떤 클라우드 애플리케이션(예: Salesforce, Office 365, Jira, Taleo 등)에 액세스하는지 뿐만 아니라, 각 애플리케이션에 액세스하기 위해 필요한 사용자 속성 설정(예: 신뢰할 수 있는 네트워크, 비밀번호, OTP)에 대한 정보가 포함됩니다.

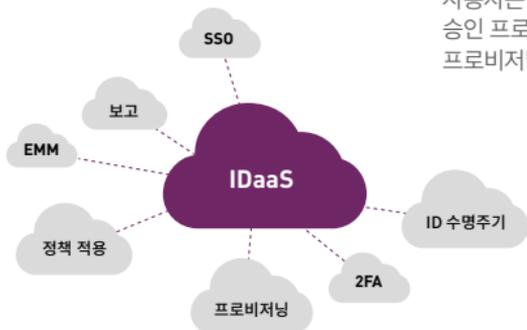
액세스 정책의 경우 클라우드 애플리케이션 기밀성에 맞추어 보다 많거나, 보다 적은 사용자 속성을 평가해야 합니다. 이러한 속성은 리스크 기반 또는 컨텍스트 기반 인증을 사용하여 평가되며, 이는 각 클라우드 애플리케이션에 대해 정의된 다른 액세스 정책을 실시하는 데 중심이 됩니다. [자세한 내용은 컨텍스트 기반 인증을 참조하십시오.]

또한 클라우드 액세스 관리의 핵심은 싱글 사인 온이며, 이를 통해 단일 사용자명-패스워드를 설정하거나 'ID'를 사용하여 모든 클라우드 애플리케이션에 로그인할 수 있습니다. [자세한 내용은 싱글 사인 온에 대한 설명을 참조하십시오.]



IDaaS

서비스로서의 아이덴티티라고도 불리는 IDaaS는 서비스로서의 IAM을 의미하며, ID 및 액세스 관리를 위하여 클라우드 기반 서비스 모델을 제공하는 ID 및 액세스 관리 (IAM)를 뜻합니다. IDaaS는 최근 몇 년간 별도의 시장으로 검토되었지만 최근 시장 동향을 고려하면, 향후에는 사내 설치, 소프트웨어 또는 클라우드 기반 플랫폼으로 제공되는 액세스 관리 및 IGA가 두 개의 다른 분야로 다루어질 것입니다.



ID 거버넌스 및 관리(IGA)

ID 거버넌스 및 관리(IGA) 솔루션은 “누구에게 접근 권한을 부여받아야 합니까 혹은 누가 ‘액세스 권한’을 부여받아야 합니까?” “실제로 누가 누구에 의해, 언제 어떤 애플리케이션에 액세스할 수 있습니까?”와 같은 질문의 답을 찾는 데 도움이 될 것입니다. 예를 들어, IGA 솔루션은 R&D 스태프가 GitHub, Jira 및 Confluence 등의 특정한 개발 애플리케이션에 액세스할 권리를 확립하는데 도움을 줍니다. IGA 솔루션은 R&D 그룹 멤버십을 기반으로 이러한 애플리케이션에 대한 접근을 자동으로 프로비저닝할 수 있습니다. 또한 R&D 사용자는 일부 IGA 솔루션에서 지원되는 관리 승인 프로세스를 거쳐 다른 애플리케이션에 프로비저닝된 접근을 요청할 수도 있습니다.

ID 페더레이션

ID 페더레이션은 신뢰할 수 있는 ID 제공자("IdP")라 불리는 단일 시스템이 사용자 인증을 관리하며, 클라우드 애플리케이션은 사용자가 액세스를 시도할 때마다 인증 프로세스를 ID 제공자에게 중계합니다. 연한된 ID는 사내외 관계없이 다수의 웹 애플리케이션의 자격 정보를 별도로 관리해야 하는 과제와 불만을 해결해줍니다. ID 페더레이션은 SAML 및 Open ID Connect 등과 같은 통합 프로토콜뿐만 아니라 Microsoft의 WS-Federation 등의 독점 프로토콜에도 의존합니다.

통합 로그인

통합 로그인은 SAML, Open ID Connect 등과 같은 통합 프로토콜의 기능으로, ID 제공자 모델을 사용하여 사용자를 인증하고, 인증 정보를 "인증 어서션(authentication assertion)"의 형태로 대상 시스템에 중계합니다. 어서션에는 '동의' 또는 '거부' 응답이 포함되어 있기 때문에 사용자는 액세스 거부 또는 허가를 받게 됩니다.

통합 로그인을 사용하면 단 한 번의 로그인으로 모든 클라우드 응용프로그램에 동시에 액세스할 수 있습니다. 통합 로그인의 경우 다른 사용자명과 패스워드 설정 즉 'ID'를 사용하여 각각의 클라우드 애플리케이션에 로그인하는 것이 아니라 아침에 기업 네트워크에 로그인할 때나 밤에 VPN에 사용하는 동일한 ID로 office 365, Salesforce, AWS 등에 로그인할 수 있습니다.

ID 페더레이션은 신뢰할 수 있는 ID 제공자라 불리는 단일 시스템이 사용자 인증을 관리하며 클라우드 애플리케이션은 사용자가 액세스를 시도할 때마다 인증 프로세스를 ID 제공자에게 중계합니다.

ID 제공자

연계되지 않은 웹 사이트 간에 ID 데이터를 안전하게 교환할 수 있는 SAML 및 기타 ID 페더레이션 프로토콜은 ID 제공자 (IdP) 및 서비스 제공자 모델을 기반으로 합니다. 사용자가 서비스 제공자(클라우드 기반 서비스)에 액세스하면 인증 및/또는 인가 데이터에 대한 신뢰할 수 있는 ID 제공자에게 리디렉션됩니다. ID 제공자는 사용자 인증 데이터 (예 : 사용자 쿠키, 장치, 네트워크, OTP)를 검증하고 “동의” 또는 “거부” 응답을 생성하며, 해당 내용이 서비스 제공자에 송신됩니다. 인가 데이터에는 웹 메일 계정을 통한 전자 메일 주소 정보 또는 소셜네트워크 계정을 통한 친구 이름 등의 정보에 액세스하기 위한 권한이 포함될 수 있습니다.

예를 들어, 앞서 설명한 시나리오처럼 사용자가 클라우드 애플리케이션에 액세스하면 SafeNet 인증 서비스가 ID 제공자로서 기능합니다.

보안 토큰 서비스

ID 제공자 모델은 토큰 기반 인증 또는 보안 토큰 서비스라고도 불립니다. 보안 토큰 서비스(STS)는 ID 제공자에 해당하며, 인증 정보 의존군(Relying Party, RP)은 서비스 제공자에 해당합니다. SAML assertion을 바꾸는 대신 이를 보안 토큰이라고 합니다. 다른 이름, 동일한 개념.

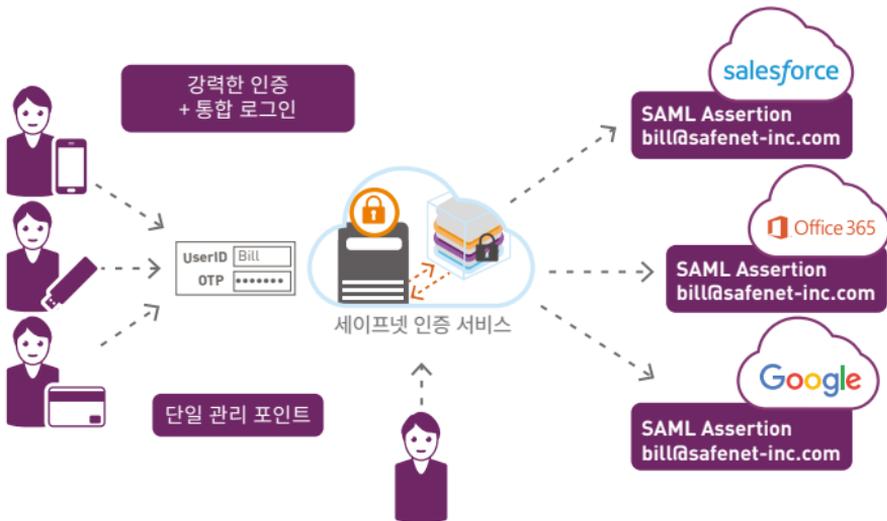


SAML

‘samme’이라고 발음하는 SAML은 연계되지 않은 웹사이트 간에 인가 데이터를 교환하기 위한 XML 기반의 개방형 표준 데이터 형식인 Security Assertion Markup Language의 약자로, ID 페더레이션 또는 통합 인증이라고도 불립니다. ID 페더레이션은 사용자의 현재 기업 ID를 클라우드로 확장하여, 현재 기업 ID로 클라우드 애플리케이션에 로그인할 수 있도록 하는 기능을 뜻합니다. SAML을 사용한 클라우드 애플리케이션에 대한 연계 인증은 사용자가 현재 기업 ID를 사용하며 모든 클라우드 애플리케이션에 로그인할 수 있으므로 5 또는 25의 사용자명과 패스워드 설정을 유지하는 것이 아니라 단 하나만 유지할 수 있습니다.

SAML 작동 방식

사용자가 클라우드 기반 애플리케이션에 로그인을 시도하면 인증을 위하여 신뢰할 수 있는 ID 제공자에 리디렉션됩니다. ID 제공자는 사용자명과 일회용 패스워드 등 사용자의 자격 증명 정보를 수집하고, 액세스 중인 클라우드 애플리케이션에 회신합니다. 이러한 응답을 SAML assertion이라 하며 SAML assertion에는 동의와 거부 응답이 포함됩니다. 이 응답을 기반으로 하여 Salesforce, Office 365 또는 DropBox 등과 같은 서비스 제공자는 애플리케이션에 대한 액세스를 차단하거나 허가합니다.



WS-Fed

WS-Federation 서비스(WS-Fed)는 마이크로소프트의 독점 ID 페더레이션 프로토콜입니다. WS-Fed는 Active Directory에 보관된 ID를 Office 365, Azure 등의 Microsoft 클라우드 애플리케이션으로 확장하기 위하여 Microsoft의 Active Directory Federation Services(ADFS)와 연계되어 작동합니다. SAML과 마찬가지로 WS-Fed 사용자는 ID 제공자 모델을 사용합니다. Microsoft 클라우드 애플리케이션에 액세스하면, 클라우드 애플리케이션이 사용자 접근에 대한 허가 또는 거부 응답을 기반으로 인증을 위해 해당 유저는 AD FS에 리디렉션됩니다.



OAuth

“oh-auth”라고 발음하는 OAuth는 공개 인증을 의미하며, 연계되지 않은 웹 사이트 간에 통합 또는 ‘토큰 기반’ 인증 및 권한 부여를 위한 오픈 표준형 인증 방식입니다. OAuth는 SAML, Open ID Connect, WS-Fed 등의 기타 ID 페더레이션 프로토콜과 마찬가지로, 신뢰할 수 있는 ID 제공자에 의하여 검증된 ID 를 갖고 있는 애플리케이션에 로그인할 수 있습니다. OAuth는 통합 인증보다 더 뛰어나기 때문에 사용자는 RP 웹 사이트가 연락처명 및 전자메일 주소 등의 특정 계정 정보에 액세스하도록 허용할 수 있습니다. 예를 들어, OAuth는 소셜 네트워크의 웹 사이트가 웹 메일의 연락처에 액세스하기 위해 사용하는 프로토콜로, 웹 메일의 연락처를 소셜네트워크에 초대할지 여부를 묻습니다.

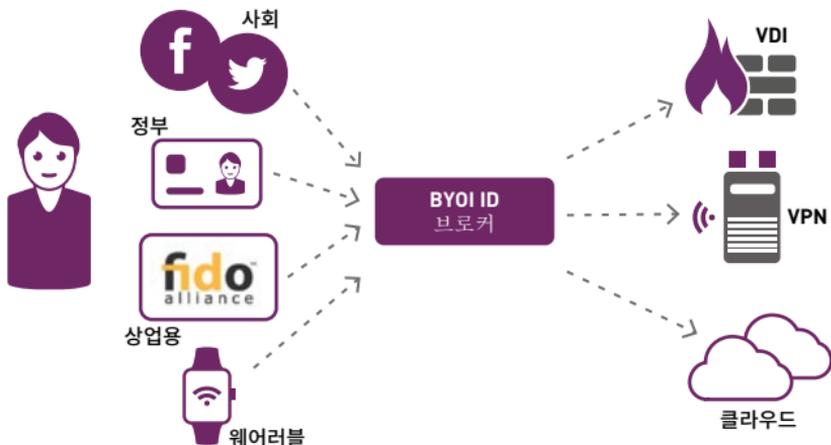


Open ID Connect

SAML과 마찬가지로, Open ID Connect는 ID 제공자 모델을 사용하는 개방형 표준 ID 페더레이션 프로토콜입니다. 그러나 쿠키를 사용하여 브라우저로 여는 애플리케이션에서만 동작하는 SAML과는 달리 Open ID Connect는 브라우저 기반 애플리케이션, 네이티브 모바일 애플리케이션 및 데스크톱 클라이언트 간에 싱글 사인 온 구현이 가능한 싱글 사인 온 프레임 워크를 제공합니다. 따라서 오늘날 싱글 사인 온 구현의 경우 클라우드와 브라우저 기반의 애플리케이션만 지원되지만, 많은 ID 제공자가 Open ID Connect를 채택하고 있기 때문에 데스크톱 클라이언트, 브라우저 기반 애플리케이션, 네이티브 모바일 애플리케이션 등 모든 리소스에 동시에 액세스할 수 있게 됩니다.

Bring Your Own Identity (BYOI)

ID 관리 분야의 경우, 공급 업체 및 조직에서 직원 또는 파트너가 기업 리소스에 액세스할 수 있도록 독자적인 ID의 사용을 허용하고 있습니다. 이러한 ID는 이론상 충분한 수준의 ID 보증을 제공하는 임의의 ID일 수 있습니다. 예를 들면 정부 발행의 신분증명서, 의료용 스마트카드 및 사회 ID, 전문 네트워크 ID 및 FIDO 등과 같이 상업적으로 이용 가능한 ID 등의 온라인 ID를 들 수 있습니다. 기업과 소비자의 세계는 더욱 긴밀하게 통합되고 있으며, 기업의 보안팀은 소비자 서비스에서 흔히 볼 수 있는 인증 방식과 동일한 방식으로 구현하라는 압박을 점점 거세게 받고 있습니다.



싱글 사인 온 (SSO)

SSO(Single Sign-On)은 단 한 번의 인증을 거친 후, 다양한 리소스에 액세스할 때 자동으로 인증되는 기능을 제공합니다. 이에 따라 각 응용프로그램 및 시스템에 개별적으로 로그인하여 인증을 받을 필요가 없어지며, 본질적으로 사용자와 대상 응용프로그램 간의 중개 역할을 담당하게 됩니다. 한편에서는 대상 애플리케이션과 시스템이 여전히 자체 인증 정보 저장소를 유지하고 있으며, 사용자의 시스템에 사인 온 프롬프트를 표시합니다.

SSO는 이러한 프롬프트에 응답하고 인증 정보를 단일 로그인/패스워드를 페어로 매핑합니다. [출처: 가트너] SSO는 독립형 솔루션은 물론 광범위한 액세스 관리 솔루션까지 다양한 ID 페더레이션 프로토콜로 구현할 수 있습니다. 여기에는 SAML 2.0 및 Open ID Connect 등 오픈 소스 프로토콜, Microsoft의 WS-Federation 등의 독자 프로토콜 및 패스워드 볼트, 리버스 프록시 등의 기술이 포함되어 있습니다.

패스워드 볼트

패스워드 매니저라고도 불리는 패스워드 볼트는 대상 애플리케이션이 레거시 애플리케이션 또는 커스텀 애플리케이션 등의 ID 페더레이션을 지원하지 않는 경우, 싱글 사인 온(SSO) 경험을 간단히 생성하는 방법입니다. 패스워드 볼트는 다른 웹 사이트의 패스워드를 보관하여 암호화함으로써 작동하는 시스템입니다. 전용 패스워드로 각 애플리케이션에 로그를 기록하는 대신에 사용자는 마스터 패스워드(패스워드 볼트를 암호화)로 간단히 인증할 수 있으므로 여러 패스워드를 유지할 필요가 없습니다.



권한 부여

권한 부여란 적절히 인증된 사용자가 해당 리소스 소유자 또는 관리자가 정의한 액세스 가능한 리소스에만 액세스할 수 있도록 하는 프로세스입니다. 소비자 세계에서 권한 부여란 클라우드 기반의 애플리케이션(소셜 네트워크 등)이 제휴하지 않는 웹 사이트(예를 들면 사용자의 웹 메일 계정)로부터 특정 정보에만 액세스하는 것을 사용자가 보증하는 프로세스를 가리키는 경우도 있습니다.

인증

인증은 애플리케이션, 서비스, 컴퓨터 또는 디지털 환경에 로그인할 때 사용자가 제공하는 자격 정보에 기반하여 사용자 ID를 확인하거나 검증하는 프로세스입니다. 대부분의 인증 크리덴셜은 사용자명 등과 같은 사용자가 소유한 항목과 패스워드 등 사용자가 알고 있는 항목으로 구성됩니다. 사용자가 제공한 크리덴셜이 기본 애플리케이션 또는 ID 공급자에 의해 보관된 정보와 일치하는 경우, 사용자는 정상적으로 인증되어 액세스 권한이 부여됩니다.

컨텍스트 기반 인증

컨텍스트 기반 인증의 경우, 사용자가 애플리케이션에 로그인할 때 일련의 보충 정보를 평가하여 사용자의 ID를 확인합니다. 컨텍스트 정보의 가장 일반적인 타입은 사용자의 장소, 시각, IP 주소, 장치 타입, URL 및 애플리케이션 평판이 포함됩니다. 리스크 기반 또는 상황 반응적 인증이라고도 불리는 컨텍스트 기반 인증은 SSO와 가능한 한 투명하고 어려움 없이 인증 여행을 하고자 하는 액세스 관리 세계의 중심입니다.

사용자의 로그인 속성을 맥락(장치, 역할, 장소) 또는 행동(입력 속도, 페이지 뷰 시퀀스 등)에 기반하여 평가함으로써, 싱글 사인 온과 액세스 관리 솔루션은 사용자에게 요구되는 인증 레벨과 애플리케이션 별로 정의된 액세스 정책을 계속적으로 일치시킬 수 있습니다. 이처럼 인증은 모든 기업 리소스에 대한 포괄적이며 일률적인 규칙이 아니라 애플리케이션의 액세스 정책 별로 가능한 한 마찰이 없는 방식으로 세부적으로 적용됩니다.



지속적 인증

토큰, 비밀번호 또는 지문의 경우 - 인증은 기본적으로 예/아니오 식으로 결정됩니다. 이 시스템은 사용자의 ID를 확인하여 애플리케이션에 대한 액세스를 허가 또는 거부합니다.

그러나 컨텍스트 기반의 인증 및 행동 바이오 인증(타이핑 패턴 및 기타 물리적 특성 등) 등 새로운 기술로 인해 인증은 보다 지속적인 프로세스가 될 가능성이 있습니다. IP 주소, 모바일 파라미터, 알려진 장치, 운영체제 등 속성 범위를 평가함으로써 맥락 또는 리스크 기반 인증 방식으로 애플리케이션에 로그인할 때마다 개인 ID를 지속적으로 검증할 수 있습니다. 사실 사용자도 모르게 할 수도 있습니다.

문맥 인증은 사람의 ID를 검증하기 위하여 많은 비마찰 방법을 제공합니다. 이는 실제로 사용자 편의성과 다수의 클라우드 애플리케이션에 대해 세세하게 액세스를 제어할 수 있는 기능 간의 밸런스를 맞출 수 있습니다. 이것이 컨텍스트 기반 인증을 기반으로 한 지속적인 인증이 클라우드 액세스 관리의 기초인 이유입니다.



세이프넷 인수를 통해 Gemalto는 전 세계 기업 보안 솔루션의 가장 완벽한 포트폴리오 중 하나를 제공하며 디지털 ID, 거래, 지불 및 주변부터 중심에 이르기까지의 데이터에 대해 업계를 선도하는 보호 기능을 고객이 누릴 수 있도록 지원합니다. 세이프넷 아이덴티티 및 데이터 보호 솔루션을 포함하여 새롭게 확장된 Gemalto 포트폴리오는 혁신적인 암호화 방식, 최고 수준의 암호화 관리 기법 및 신원 관리 솔루션을 사용하여, 주요 금융 기관 및 정부 등 많은 수직 조직을 아우르는 기업이 데이터 중심의 보안 접근 방식을 취하여 문제가 되는 사안과 장소를 보호할 수 있게 해줍니다. Gemalto는 이러한 솔루션을 통해 각 조직이 민감한 기업 자산, 고객 정보에 대한 엄격한 데이터 프라이버시 규정을 준수하는 데 도움을 주고, 점점 디지털화 되어가는 세계에서 고객의 신뢰를 보호하기 위해 노력하므로 노출과 조작으로부터 디지털 거래가 안전해집니다.

문의: 전세계 지점 위치와 연락처 정보는 www.safenet-inc.kr 을 참조하십시오.

팔로우하기: blog.gemalto.com/security

③ GEMALTO.COM

gemalto
security to be free