DigiCert PKI Platform 서비스 기술서

서비스 개요

DigiCert PKI Platform 서비스("PKI Platform" 또는 "Platform")는 신규 인증서 발급, 기존 인증서 갱신, 신뢰할 수 없는 인증서 폐기에 이르는 전체 인증서 수명 주기를 관리하기 위한 유연한 PKI 플랫폼을 제공합니다. 또한 DigiCert PKI Platform는 이메일, 파일 시스템 또는 기타 데이터를 암호화하는 데 사용되는 인증서의 개인
키를 보증하고 복구하는 기능과 데이터 암호화, 문서 디지털 서명 또는 네트워크 인증과 같은 작업을 신뢰할 수 있는 인증서만 수행할 수 있도록 인증서의 현재 상태를 확인하는 여러 가지 검증 서비스를 제공합니다.

본 서비스 기술서는 참조 목적으로 포함되는 모든 첨부 문서와 함께 본 서비스 기술서에 기술되고 DigiCert가 제공하는 서비스에 대해 본 서비스 기술서를 참조 목적으로 통합하는 계약("계약"으로 총칭)의 일부를 구성합니다.

목차

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

기술/비즈니스 기능과 역량

서비스 특징

DigiCert PKI Platform는 관리 대상 서비스로서 내부 PKI와 관련된 비용을 크게 줄여줍니다. 한 예로 고객은 내부 PKI 배치에서 첫 번째 인증서를 발급하기 전에 암호 및 애플리케이션 서버 하드웨어를 획득하고 서버 및 클라이언트 라이센스를 구입해야 하며 직원 교육을 실시해야 합니다. 고객은 PKI 계층 구조를 관리하는 기본 정책과 인증 프로세스와 절차 및 신뢰할 수 있는 역할과 책임을 정의하는 인증 업무 규정으로써 자체 인증 정책(CP)을 수립해야 합니다. DigiCert PKI Platform는 업계 최고의 암호 및 애플리케이션 서버 하드웨어를 기반으로 하는 복수 사용자, 고가용성 환경으로 설계되었습니다. 이 환경은 강화된 보안 신원 조사를 통과한 전문 인력을 통해 연중무휴 24시간 모니터링되며 WebTrust 및 SOC-2 승인 자격 유지를 위해 정기적으로 감사를 받습니다.

- DigiCert PKI Platform는 **인증 기관(CA)** 계층 구조를 생성 및 관리합니다.
  - DigiCert PKI Platform를 사용할 수 있는 표준 CA 계층 구조는 다음과 같습니다.
    - DigiCert Trust Network – ***부록 A 참조***
    - 사설 인증 기관 – ***부록 B 참조***
    - Adobe® 문서 서명 서비스 – ***부록 C 참조***
    - LTE 인증 서비스 – ***부록 D 참조***
    - 제조업체 인증서 – ***부록 E 참조***
  - 각 서비스 계정에는 선택한 CA 계층 구조마다 하나 이상의 CA 인증서가 포함됩니다. 특정 볼륨에 대한 추가 CA 인증서는 추후에 구입할 수 있습니다. DigiCert 시스템과 서비스의 CA 인증서 및/또는 해당 키 쌍 추출은 당사자들 간의 합의를 따릅니다.
- DigiCert PKI Platform는 **인증서 수명 주기 관리를** 위한 2가지 배치 모델인 클라우드와 하이브리드 배치 모델을 제공합니다.
  - 클라우드 배치 모델은 DigiCert 데이터 센터에서 계정, 인증서 및 키 관리 도구를 호스트합니다.
  - 하이브리드 배치 모델 또한 모든 계정, 인증서 및 키 관리 도구를 DigiCert 데이터 센터에서 호스트하지만 이 모델은 등록 기관(RA) 및 디렉토리 통합 도구를 고객의 데이터 센터에 설치합니다.
  - 배치 모델은 비독점적이며 다양한 PKI 프로젝트의 요구에 따라 배치 모델을 조합하여 사용할 수 있습니다. 두 배치 모델 모두 인증서 수명 주기와 관련된 사용자 경험을 극적으로 향상시키도록 설계된 데스크탑 미들웨어인 PKI Client에 사용할 수 있습니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

- DigiCert PKI Platform는 다음과 같은 관리 도구를 제공합니다.
  - **PKI Manager** – PKI Manager는 DigiCert 데이터 센터에서 호스트하는 웹 포털로, PKI 관리자가 계정, 사용자, 인증서 및 키 관리와 관련된 작업을 수행할 수 있습니다.
    - **계정 관리:** PKI 관리자는 PKI Manager를 통해 인증 기관(CA), 시트 수, 계정과 연관된 보고서를 볼 수 있습니다. 또한 PKI 관리자는 PKI Manager를 통해 추가 PKI 관리자에게 책임을 생성하여 지정할 수 있습니다.
    - **사용자 관리:** PKI 관리자는 PKI Manager가 사용자를 추가 또는 해지하고 사용자마다 고유한 등록 코드를 생성하며 사용자에게 보내는 이메일 알림을 사용자 지정하도록 합니다. PKI Manager는 또한 사용자에게 타사 애플리케이션이 새로 발급된 인증서를 사용할 수 있도록 구성하는 문서 및 비디오 기반 지침을 사용자에게 제공할 수 있습니다.
    - **인증서 관리:** PKI 관리자는 PKI Manager를 통해 계정 내 CA마다 인증서 프로필을 구성할 수 있습니다. PKI 관리자는 이러한 인증서 프로필의 일부로 키 크기, 키 사용 및 서명 알고리즘과 같은 파라미터를 설정합니다. PKI 관리자는 또한 사용자 경험(OS/브라우저 또는 PKI Client를 통한 등록)과 보안 보호 수준을 선택합니다. PKI 관리자는 인증서의 개인 키 보증 여부를 결정합니다. PKI 관리자는 PKI Manager를 통해 인증서 프로필 구성뿐만 아니라 사용자가 더 이상 인증서를 필요로 하지 않거나(예를 들어 사용자가 퇴사하는 경우) 또는 개인 키가 손상되어(예를 들어 사용자가 랩탑을 분실한 경우) 신뢰할 수 없게 된 인증서를 폐기할 수 있습니다.
    - **키 관리:** PKI Manager는 PKI 관리자가 암호화 인증서의 개인 키를 복구할 수 있는 기능을 제공합니다.
  - **PKI Certificate Service** – PKI Certificate Service는 DigiCert 데이터 센터에서 사용자(즉 가입자)가 인증서를 요청할 수 있도록 인증서 등록 웹 페이지를 호스트합니다. 이 웹 페이지는 사용자에게 인증서를 요청하는 데 필요한 단계를 안내합니다. 또한 이 웹 페이지에는 PKI 관리자가 제공하는 타사 제품 구성 지침이 표시될 수 있습니다.
  - **Certificate Issuance Center** – Certificate Issuance Center는 DigiCert 데이터 센터에서 호스트하는 인증 엔진입니다. 이 인증 엔진은 PKI Certificate Service에서 제출되거나 PKI Enterprise Gateway에서 수신되거나 웹 서비스를 통해 전송된 인증서 서명 요청을 기반으로 인증서를 생성합니다. 이 인증서 엔진은 발급 인증 기관(CA)을 통해 해당 인증서에 서명합니다.
  - **PKI Enterprise Gateway** – PKI Enterprise Gateway는 필요한 경우 고객 데이터 센터에 설치되는 등록 기관(RA) 승인 애플리케이션입니다. 이 애플리케이션은 Lightweight Directory Access Protocol (LDAP) 소스(예: Microsoft® Active Directory®)와 완벽하게 통합되어 인증 요청을 자동으로 승인하고 인증 데이터를 LDAP 소스에 다시 게시합니다.
  - **PKI Client** – PKI Client는 인증서 수명 주기 관련 사용자 경험을 극적으로 향상시키도록 설계된 엔드포인트 미들웨어입니다. PKI Client는 Windows 및 MAC 운영 체제를 지원하는 데스크탑에서 사용할 수 있습니다. 브라우저 등록 작업 시 사용자는 Microsoft Internet Explorer®, Safari®, Chrome™ 또는 Mozilla® Firefox® 중 하나를 사용하여 인증서 등록 웹 페이지에서 인증서를 요청합니다. 이 기본 작업에 추가 소프트웨어가 필요하지는 않지만 그 유용성은 제한적인 것으로 알려져 있습니다. 예를 들어 Microsoft Internet Explorer가

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

생성하는 다수의 팝업 창에는 종종 사용자에게 혼란을 주는 경고 메시지가 포함됩니다. PKI Client를 사용하는 경우 일반 기능(즉 인증서 갱신)을 자동화하도록 인증서 수명 주기를 간소화하여 사용자 개입을 최소화합니다. PKI Client는 또한 인증서 보호를 위한 중앙 집중식 정책 관리 기능(예를 들어 PIN, 내보내기 등)을 제공합니다. 더불어 PKI Client는 타사 제품(예를 들어 무선, 가상 사설망 클라이언트 등)이 인증서를 사용하도록 자동 구성할 수 있습니다. DigiCert PKI Platform Certificate 수명 주기 관리 기능은 iOS와 같이 내장된 iOS OTA(Over-the-Air) 프로토콜 기능을 이용하는 모바일 기기에서도 사용할 수 있습니다. 이를 통해 iOS 장치 또는 애플리케이션이 Apple의 SCEP 프로토콜을 이용해 인증서 등록을 요청할 수 있습니다. Android OS처럼 iOS OTA에 상응하는 기능이 없는 모바일 운영 체제의 경우 DigiCert는 장치와 애플리케이션이 인증서를 사용할 수 있도록 구성하는 데 따른 복잡성을 유사한 수준으로 제거해주는 PKI Client를 제공합니다.

  - **PKI Web Service** – DigiCert 데이터 센터에서 호스트되는 PKI Web Service는 DigiCert PKI Platform와 프로그래밍 방식으로 통합되는 기능을 제공합니다. 타사 애플리케이션이 인증 정책을 확보하고 PKI Web Service가 제공하는 API를 사용한 등록 및 갱신과 같은 인증서 수명 주기 기능을 수행할 수 있습니다.

- DigiCert PKI Platform가 제공하는 **인증 방법**은 다음과 같습니다.
  - **등록 코드를 사용한 인증** – 이 인증 유형을 선택하면 PKI 관리자가 사용자마다 고유한 등록 코드를 생성하여 인증 요청을 자동으로 승인할 수 있습니다. PKI 관리자는 인증서 등록 웹 페이지 링크가 포함된 인증서 초대장을 사용자에게 보낼 때 해당 사용자의 고유한 등록 코드를 포함시킵니다. 그러면 사용자는 인증서 등록 웹 페이지에 등록 코드와 추가 정보를 함께 포함시킵니다. Certificate Issuance Center는 이 등록 코드를 PKI Manager에서 생성된 정보와 비교합니다. 일치하는 항목이 있으면 Certificate Issuance Center에서 인증서를 발급합니다. 사용자가 입력한 등록 코드가 해당 사용자를 위해 생성된 등록 코드와 일치하지 않으면 Certificate Issuance Center에서 사용자에게 오류 메시지를 보냅니다.
  - **자동 인증** – 자동 인증은 LDAP 소스(즉 Microsoft Active Directory)의 데이터를 기반으로 인증 요청을 승인합니다. PKI Enterprise Gateway가 고객 데이터 센터에 설치되어 LDAP 소스와 통합되어야 합니다. 사용자가 PKI Certificate Service를 통해 인증 요청을 제출하면 PKI Enterprise Gateway가 인증 요청의 데이터와 LDAP 소스를 비교합니다. 데이터가 일치하면 PKI Enterprise Gateway가 인증 요청을 승인하고 등록 기관(RA) 인증서로 인증 요청을 서명하며 서명한 인증 요청을 Certificate Issuance Center로 보냅니다. 일치하지 않으면 PKI Enterprise Gateway가 인증 요청을 거부합니다.

- DigiCert PKI Platform가 제공하는 **인증서 검증 도구**는 다음과 같습니다.
  - **인증서 폐기 목록(CRL)** – 많은 타사 제품이 인증서 폐기 목록(CRL)을 통해 인증서의 현재 상태(예를 들어 사용 중, 폐기됨 등)를 확인하는 기능을 갖고 있습니다. CRL은 아직 만료되지 않았지만 폐기된 인증서의 블랙리스트입니다. 이 제품은 정기적으로 최신 CRL을 다운로드하거나 확인하도록 구성될 수 있습니다. CRL에 인증서가 나타나면 제품이 액세스를 거부합니다(예를 들어 네트워크 인증 거부, 디지털 문서 서명 거부 등). DigiCert는 최소한 24시간마다 CRL을 생성합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

- **온라인 인증서 상태 프로토콜(OCSP) –** 많은 타사 제품이 온라인 인증서 상태 프로토콜(OCSP)을 통해 인증서의 현재 상태(예를 들어 사용 중, 폐기됨 등)를 확인합니다. 폐기된 인증서는 모두 CRL에 나타나지만 표준 CRL의 경우 인증서 폐기에서 다음 CRL 실행까지 최대 24시간에 해당하는 시간 지연이 발생할 수 있습니다. DigiCert는 변경 시 인증서 상태(예를 들어 폐기됨, 보류됨 등)를 즉시 업데이트하므로 변경 내용이 DigiCert OCSP 도구인 Trusted Global Validation(TGV)에 거의 실시간으로 반영됩니다.

- DigiCert는 DigiCert PKI Platform 보완을 위해 다음과 같은 **하드웨어 옵션**을 제공합니다.
  - **SafeNet® PKI 토큰** - DigiCert는 SafeNet® 하드웨어 USB 토큰의 공인 리셀러입니다. 또한 이러한 토큰에는 리포지토리에서 확인 가능한 보증 정보 부록에 기술된 3년 보증이 적용됩니다. 이 토큰은 미연방 정보 처리 표준(FIPS) 140-2 및 공통 기준 표준을 충족합니다.
  - **SafeNet® 하드웨어 보안 모듈(HSM)** – DigiCert는 Luna® PCI 카드, Luna® SA 네트워크 어플라이언스, Luna® PCM 토큰으로 구성되는 SafeNet® Luna® 하드웨어 보안 모듈(HSM)의 공인 리셀러입니다. 이 HSM에는 또한 펌웨어 또는 관련 소프트웨어(예: SafeNet Authentication Client)가 포함될 수 있습니다. 이 HSM에는 1년 기본 보증이 적용되지만 추가 비용으로 DigiCert가 재판매하는 선택적 SafeNet 확장 보증 프로그램을 이용하실 수 있습니다. 이 HSM은 또한 FIPS 140-2 레벨 2 및 공통 기준 표준을 충족합니다.
    - 판매된 모든 HSM에 대한 소유권은 DigiCert에서 출고된 시점부터 고객 또는 고객이 지정한 당사자에게 이전됩니다. 모든 품목의 인도는 DigiCert 선적 지점 공장 인도(EXW) 기준입니다 – 2010 인코텀스. HSM 인도는 DigiCert 선적 지점에서 운송업체에 인도되는 시점에 완료됩니다. 운임 조건은 착불 또는 제3자입니다.
    - 고객이 DigiCert를 통해 HSM을 구입하고("고객 HSM") 해당 고객 HSM을 DigiCert 데이터 센터에 보관하기로 선택하는 경우 고객 HSM은 DigiCert 자체 HSM과 같은 방식으로 보관 및 보호됩니다. 고객에게 제공되는 DigiCert의 관련 서비스가 만료 또는 종료되는 시점에서 고객이 요청하는 경우 DigiCert는 고객 HSM을 업계 모범 사례에 따라 고객에게 인도합니다. 고객 HSM 인도 비용은 고객이 지불하지 않지만 고객이 고객 HSM 인도와 연계하여 기술 지원을 요청하는 경우 DigiCert는 별도 협의를 거쳐 양방이 상호 합의하는 작업 기술서에 따라 이전 지원을 제공합니다.

- DigiCert가 DigiCert PKI Platform를 통해 제공하는 **인증서** 또는 **시트** 유형은 다음과 같습니다.
  - **사용자 시트:** 가입자를 VPN/WiFi를 통해 개인 네트워크에 액세스하는 사용자로 인증하는 내용으로 가입자에게 발급된 인증서. 해당 *"사용자 시트"*로 발급된 인증서는 다양한 유형의 복수 사용자 인증서(사용자 시트 풀의 VPN, WiFi, SMIME 등)가 해당 사용자에게 발급될 수 있도록 허용합니다. 하나의 *사용자 시트*는 고유한 단일 사용자에게 발급된 여러 개의 인증서를 의미할 수 있습니다.
  - **장치 시트:** 장치(예를 들어 랩탑, 컴퓨터, LTE 장비 등)를 가입자로 여겨 발급하는 인증서로 해당 장치가 개인 네트워크에 액세스할 수 있도록 허용합니다. *사용자 시트*와 달리 *장치 시트*는 하나의 장치에 발급되고 1개의 물리적 장치에서만 사용할 수 있는 인증서를 의미합니다.
  - **서버 시트:** 조직의 내부 서버를 가입자로 여겨 발급하는 인증서로 서버에서 호스트하는 인트라넷 웹사이트에 대한 액세스를 요청하는 사용자 또는 장치에 해당 서버의 신원을 보증합니다. DigiCert PKI Platform는 이 솔루션의 일부로 사설 계층 조직 서버 인증서를 발급합니다. 물리적 또는 가상화 서버마다 서버 시트가 필요합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

- **조직 인증서:** 조직 또는 실체를 가입자로 여겨 발급하는 인증서로 신원 보증(예를 들어 개인 코드 서명 인증서의 경우) 및 디지털 서명(조직 수준의 Word 또는 PDF 서명의 경우)을 허용합니다. *조직 인증서*에는 다음과 같은 제약이 있습니다. 고객은 다음과 같은 방식으로 코드 서명 또는 기타 *조직 인증서*를 사용해서는 안 됩니다. (i) 고객 조직 이외의 다른 조직을 위해 또는 그러한 조직을 대신하여 (ii) 인증 신청서에 기재된 고객과 다른 도메인 및/또는 조직 이름과 관련하여 개인 또는 공용 키 작업을 수행하기 위해 (iii) 컨텐츠 수신자에게 불편을 줄 수 있는 컨텐츠를 포함하되 이에 한정되지 않는 악의적이거나 유해한 컨텐츠를 배포하기 위해 (iv) 고객이 허가한 직원 이외의 사람에게 인증서의 공용 키에 해당하는 개인 키에 대한 액세스를 허가하거나 제어 권한을 양도하는 방식으로(이러한 양도는 개인 키 보호를 위해 안전한 방식으로 수행되어야 함).

DIGICERT의 의무

- 필수 설치를 완료한 후 DigiCert는 고객에게 본 서비스 기술서에 명시된 서비스를 제공합니다.
- DigiCert는 고객과 해당 PKI Platform 관리자가 제공하는 지침에 따라 인증서를 발급, 관리, 폐기 및/또는 갱신합니다.
- 고객이 인증 신청서를 승인하면 DigiCert는 (1) 승인된 인증 신청서에 포함된 정보의 정확성을 신뢰할 수 있으며 (2) 해당 인증 신청서를 제출한 인증서 신청자를 위해 인증서를 발급합니다.
- 본 서비스 기술서에 따라 발급, 허가된 인증서에는 관리자 인증서를 포함하여 각 인증서가 발급된 날로부터 최대 12개월 간의 유효 기간이 적용됩니다.
- 단일 CA 키 생성 이벤트 기간에 DigiCert는 고객을 위해 DigiCert가 DigiCert Trust Network 고객 또는 고객이 선택한 다른 계층 구조를 대신하여 발급한 인증서 서명에 사용할 CA 키 쌍을 생성합니다.
- 각 키 쌍의 고객 CA 개인 키는 하나 이상의 하드웨어 보안 모듈에 저장됩니다.

고객의 책임

DigiCert는 고객이 필요한 정보를 제공하거나 필요한 조치를 수행하는 경우에만 서비스를 수행할 수 있습니다. 고객이 다음 책임에 수반되는 정보 제공/조치를 이행하지 않는 경우 아래 명시된 것처럼 DigiCert의 서비스 이행이 지연, 악화되거나 방해를 받을 수 있습니다.

- 개시 지원: 고객은 DigiCert가 서비스 제공을 시작하는 데 필요한 정보를 제공해야 합니다.
- 역량을 갖춘 고객 담당자: 고객은 DigiCert의 타당한 요청이 있는 경우 DigiCert의 서비스 제공을 도와줄 수 있는 적합한 담당자를 제공해야 합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

- 고객은 다음 사항을 보장해야 합니다.
  - 인증서 발급과 관련이 있고 고객이 직접 또는 고객을 대신하여 검증된 모든 정보 자료는 모든 측면에서 진실되고 정확합니다.
  - 고객의 인증 신청서 승인이 발급 오류를 야기하지 않습니다.
  - 고객이 인증서를 폐기하는 경우 DigiCert Trust Network CPS 또는 Adobe CPS(해당되는 경우)를 준수합니다.
  - 고객은 DigiCert Trust Network CPS 또는 Adobe CPS(해당되는 경우)를 실제로 준수합니다.
  - 고객은 RA 요구사항(해당되는 경우)을 실제로 준수합니다.
  - DigiCert에 제공되는 인증서 정보는 제3자의 지적 재산권을 침해하지 않습니다(예: 도메인 선점).
  - 인증 신청서의 정보(이메일 주소 포함)는 불법적인 목적으로 사용된 적이 없으며 앞으로도 사용되지 않습니다.
    - 고객의 PKI Platform 관리자는 (관리자 인증서 생성 시점 이후) 관리자 인증서의 개인 키, 본인 확인 문구, PIN, 소프트웨어 또는 개인 키를 보호하는 하드웨어 메커니즘을 소유하는 유일한 사람이며 앞으로도 그러합니다. 또한 권한이 없는 사람이 그러한 자료나 정보에 대해 액세스한 적이 없으며 앞으로도 그러합니다.
    - 고객은 관리자 인증서를 본 서비스 기술서 내용과 일치하는 허가받은 합법적인 용도로만 사용합니다.
    - 고객은 DigiCert 시스템 또는 소프트웨어의 기술 구현을 모니터링, 방해 또는 역설계하거나 DigiCert 시스템 또는 소프트웨어의 보안을 고의로 위태롭게 만들지 않습니다.

일반 및 기술 지원

DigiCert의 지원 및 유지 관리 약속은 고지사항에 나와 있는 해당 서비스 수준 합의서에 기술되어 있습니다.

서비스 관련 조건

자동 갱신 불가

합의서 내용에 반하는 어떤 사항에도 불구하고 NSL 서비스는 자동으로 갱신되지 않습니다. 고객은 NSL 서비스가 만료되기 전에 DigiCert 또는 그 채널 리셀러 파트너에게 갱신 요청을 해야 합니다.

서비스 조건

- **관리자 인증서:** 고객이 관리자 인증을 위한 인증 신청서를 제출하고 DigiCert가 관리자 인증에 필요한 인증 절차를 완료하면 DigiCert가 인증 신청서를 처리합니다. DigiCert는 고객의 관리자 인증을 위한 인증서 신청이 승인 또는 거부되었는지 여부를 고객에게 통지합니다. PKI Platform 관리자가 DigiCert가 제공하는 PIN을 사용하여 관리자 인증서를 수령하거나 다른 방법으로 관리자 인증서를 설치 또는 사용하는 경우 PKI Platform 관리자가 관리자 인증서를 수락한 것으로 간주됩니다. PKI

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

Platform 관리자가 관리자 인증서를 선택 또는 달리 설치한 후에는 PKI Platform 관리자가 인증서를 사용하기 전에 인증서에 포함된 정보를 검토해야 하며 오류가 있는 경우 DigiCert에 즉시 알려야 합니다. DigiCert는 그러한 통지를 받은 즉시 해당 관리자 인증서를 폐기하고 정정된 관리자 인증서를 발급합니다.

- **존속:** 합의서에 명시된 종료 조항 이외에 본 서비스 기술서와 관련 CPS에 명시된 폐기 및 보안 요구사항은 합의서 또는 관련 주문서가 종료된 후에도 본 기술서에 따라 발급된 모든 인증서의 유효 기간이 끝날 때까지 존속됩니다.
- **현지 법규 준수:** 고객은 본 서비스 기술서에 따라 DigiCert에서 생성된 공용 및 개인 키 쌍을 획득, 사용 또는 수락하는 데 있어 해당 키 쌍을 획득, 사용, 수락 또는 달리 수령하는 사법권의 관련 현지 법규, 규칙 및 규정(수출입 법규, 규칙 및 규정을 포함하되 이에 한정되지 않음)을 준수해야 합니다.
- **감사 권리:** DigiCert는 본 서비스 기술서 조항을 준수하기 위해 연간 최대 1회의 고객 절차 감사를 수행할 수 있습니다. 그러한 감사는 적합한 서면 고지에 따라 고객의 근무 시간 내에 수행되며 고객의 비즈니스 활동을 부당하게 방해해서는 안 됩니다. 고객은 해당 감사와 관련하여 DigiCert에 적극 협조해야 합니다. 감사 결과 고객이 서비스 기술서 약관을 위반한 것으로 밝혀지는 경우 (1) 고객은 DigiCert에 합리적인 수준의 감사 비용을 지불해야 하며 (2) 앞서 최대 1회로 명시된 연간 감사 횟수에도 불구하고 DigiCert가 본 서비스 기술서 준수를 위해 필요하다고 판단되는 경우 추가 감사를 실시할 수 있습니다. 연례 정기 감사는 지난 해 활동만을 대상으로 할 수 있습니다.
- **사용 제약:** 가입자에게 발급된 인증서는 해당 인증서 요청에 상응하지 않는 신뢰 당사자와 통합되거나 해당 당사자에 설치할 수 없습니다. 각각의 인증서는 해당 인증서 유형에 따라 정해진 용도로만 사용해야 합니다.
- CA 계층 구조별 추가 조건은 다음 내용을 참조하십시오.
  - DigiCert Trust Network – ***부록 A 참조***
  - 사설 인증 기관 – ***부록 B 참조***
  - Adobe® 문서 서명 서비스 – ***부록 C 참조***
  - LTE 인증 서비스 – ***부록 D 참조***
  - 제조업체 인증서 – ***부록 E 참조***

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

- 소프트웨어 형태의 서비스 구성요소 사용에는 소프트웨어와 함께 제공되는 라이센스 계약이 적용됩니다. 서비스 구성요소에 EULA가 함께 제공되지 않는 경우에는 고지사항에 나와 있는 b-hosted-service-component-eula-eng.pdf의 약관이 적용됩니다. 해당 서비스 구성요소 사용에 대한 추가 권리와 의무는 본 서비스 기술서에 규정됩니다.
- 서비스 기술서에 달리 명시된 경우를 제외하고, 서비스(함께 제공되는 호스트 서비스 소프트웨어 구성요소 포함)는 오픈 소스 및 별도 라이센스가 적용되는 기타 제3자 자료를 사용할 수 있습니다. 필요한 경우 해당 제3자 고지 (https://www.websecurity.symantec.com/legal/repository#managed-pki-service)를 참조하십시오.
- DigiCert는 서비스 유효성을 유지하기 위해 언제라도 서비스를 업데이트할 수 있습니다.
- 서비스는 전 세계에서 액세스 및 사용할 수 있으며 해당 시점의 최신 DigiCert 표준에 따라 관련 수출 규정 준수 제한 및 기술 제한이 적용됩니다.

평가 라이센스

이 약관은 고객이 평가 목적으로 서비스에 액세스하는 경우에 적용됩니다.

- **사용 권리.** 고객에게 허가된 라이센스는 서비스의 내부, 비상업적, 비생산 평가 및 상호 운용성 테스트 목적으로만 제한적으로 사용됩니다. 고객은 이 밖에 다른 목적으로 서비스를 이용할 수 없습니다.
- **평가 기간.** 고객에게 허가되는 라이센스는 기간 제한적이며 고객이 평가판 라이센스를 등록할 때 지정된 평가 종료 날짜까지 유효합니다("평가 기간"). 고객이 서비스의 상용 라이센스를 구입하지 않는 한 고객에게 허가된 라이센스는 평가 기간 만료 시 종료됩니다.
- **종료 후.** 고객은 평가 기간 종료와 함께 서비스 이용을 중지해야 합니다. 기간 종료 후에도 종료일 이전에 발생한 양방의 의무는 계속 유효합니다. 본질적으로 종료, 취소 또는 만료 후에도 존속되는 조항은 계속 유지됩니다.
- **책임의 제한.** DIGICERT는 어떤 경우에도 매출 손실, 수익 손실 또는 간접 손해를 포함하되 이에 한정되지 않는 손해에 대해 책임을 지지 않으며 이는 그러한 가능성을 사전에 인지한 경우에도 해당됩니다.
- **면책.** 서비스에 DIGICERT가 일반적인 가용성을 공개적으로 발표하지 않은 기술이 포함되는 경우 해당 서비스가 일반적으로 사용 가능한 최종 제품 수준으로 작동하지 않을 수 있습니다. 서비스가 올바르게 운영되지 않고 최초 상업적 릴리스(해당되는 경우) 이전에 대폭 수정될 수도 있습니다. 양방은 평가 목적에 따라 또한 평가 목적으로 고객에게 제공되는 서비스 또는 소프트웨어가 어떤 보증도 없이 "있는 그대로" 제공된다는 사실을 인정합니다. DIGICERT는 상업성, 특정 목적에의 적합성 또는 제3자 권리 비침해에 대한 암묵적 보증을 포함하되 이에 한정되지 않는 모든 명시적, 내재적 또는 법적 보증을 부인합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

양방은 또한 서비스 기술서의 용도가 서비스를 기술하기 위한 것뿐이며 DIGICERT는 이로써 모든 진술, 보증, 서비스 수준 약속 또는 기타 DIGICERT의 약속, 의무 또는 책임을 부인한다는 사실을 인정합니다. 그 어떤 DIGICERT 대리인 또는 직원도 이 보증서의 내용을 수정, 확대하거나 추가할 수 없습니다.

- **우선 순위.** 이 섹션과 합의서의 다른 조항이 충돌하는 경우 이 섹션이 우선 적용되며 평가 목적으로 제공되는 동안 서비스에 대한 다른 해당 조항을 대체합니다.

MICROSOFT AUTO ENROLLMENT 사용

PKI Platform 서비스의 Microsoft Auto Enrollment 구성요소를 사용하는 경우 MICROSOFT가 요구하는 다음 추가 의무가 적용됩니다.

(a) **보증의 부인.** MICROSOFT와 그 계열사는 본 서비스 기술서에 따라 제공되는 서버 소프트웨어("서버 소프트웨어")에 대해 어떤 명시적, 암묵적 또는 법적 보증도 하지 않으며 그 성능 또는 성능 결함에 대해 책임을 지지 않습니다. MICROSOFT와 관련하여, 서버 소프트웨어는 모든 결함과 함께 있는 그대로 제공되며 MICROSOFT와 그 계열사는 본 문서에 따라 서버 소프트웨어와 관련된 모든(해당되는 경우) 암묵적 보증, 상업성 또는 특정 목적에의 적합성, 신뢰성 또는 가용성 조건을 포함하되 이에 한정되지 않는 명시적, 암묵적 또는 법적인 다른 모든 보증, 의무와 조건을 부인합니다. 또한 MICROSOFT와 그 계열사는 서버 소프트웨어와 관련된 소유권, 향유권, 기술서 관련성 또는 비침해성을 보장하거나 조건으로 제시하지 않습니다.

(b) **특정 손해 배제.** MICROSOFT는 관련 법에서 허용되는 최대 한도까지 서버 소프트웨어 사용 또는 사용 불능, 서버 소프트웨어를 통한 또는 서버 소프트웨어 사용으로 인해 달리 발생하거나 본 서비스 기술서의 약관에 따른 또는 그와 관련된 지원 또는 기타 서비스, 정보, 소프트웨어 및 관련 컨텐츠 제공 또는 제공 실패로 인한 또는 그와 관련된 어떤 특수, 부수적, 징벌적, 간접적 또는 결과적 손해(수익, 기밀 또는 기타 정보 손실, 사업 중단, 개인 상해, 개인 정보 손실, 선의 또는 합당한 주의를 포함한 의무 불이행, 방임 및 금전 또는 기타 손실에 대한 손해를 포함하되 이에 한정되지 않음)에 대해서도 책임을 지지 않으며 이는 MICROSOFT의 잘못, 불법 행위(방임 포함), 엄격한 책임, 계약 또는 보증 위반의 경우와 MICROSOFT가 그러한 손해의 가능성을 미리 알고 있었던 경우에도 해당됩니다.

(c) **서버 소프트웨어 요구사항.** 고객은 이 소프트웨어와 함께 제공되는 문서에 명시된 대로 본 서비스 기술서에 따라 제공되는 서버 소프트웨어의 사본 1부(관련 서비스 주문서 또는 작업 기술서에 달리 명시되지 않은 경우)만, 또한 기본 Microsoft Windows 2000 Professional, Windows XP Home/Professional 또는 Vista 클라이언트 운영 체제(또는 그 후속 버전)와의 상호 운용 및 통신을 위한 목적으로만 사용할 수 있습니다. 고객은 어떤 경우에도 개인 컴퓨터에서 서버 소프트웨어를 사용할 수 없습니다. 전술한 목적에서, **"개인 컴퓨터"**는 주 용도가 한 번에 한 명의 사용자가 사용하는 것이고 비디오 디스플레이와 키보드를 사용하도록 구성된 컴퓨터를 의미합니다.

(d) **제3자 수혜자.** 합의서의 모순되는 조항에도 불구하고, 고객은 본 문서에 따라 Microsoft Corporation이 서버 소프트웨어에 포함된 지적 재산권의 사용 허가자로서 소프트웨어에 포함된 Microsoft의 지적 재산권 또는 본 문서의 약관과 관련된 Microsoft의 기타 이익에 영향을 줄 수 있는 본 문서의 모든 조항을 이행할 수 있는 권리와 함께 본 서비스 기술서 약관의 제3자 수혜자가 된다는 데 동의합니다.

(e) **서버 클래스 2.** 고객이 서버 클래스 2를 선택하는 경우 고객은 (a) 최대 4개의 프로세서를 포함하고 각 해당 프로세서가 최대 32비트 및 4기가바이트의 RAM을 지원하며 (b) 메모리를 추가, 교체 또는 제거하려면 실행 중 재부팅이 필요한(**"핫 스와핑 기능"**) 서버에서 서버 소프트웨어를 사용할 수 있습니다. 고객은 핫 **스와핑 기능** 또는 클러스터링 기능을 지원하는 소프트웨어와 함께 서버 소프트웨어를 사용할 수 없습니다. 여기서 "클러스터링 기능"은 서버 그룹이 그룹 내 서버 노드 간에 애플리케이션 장애 복구를 사용하는 애플리케이션을 실행하기 위해 단일 고가용성 플랫폼 역할을 할 수 있는 기능을 의미합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

(f) **감사 권리.** DigiCert는 고객이 본 기술서의 모든 약관을 준수하는지 확인하기 위해 최소 14일 전에 고지하여 고객 사업장에서 정규 업무 시간에 고객을 감사하고 고객의 시설과 절차를 점검할 수 있습니다. 합의서의 모순되는 조항에도 불구하고(기밀성 조항까지 제한없이 포함), 고객이 이러한 감사 이행을 거부하고 고객이 서비스 기술서 약관을 준수하지 않는다고 믿을 만한 근거를 DigiCert가 갖고 있는 경우 고객은 DigiCert가 Microsoft 고객의 신원과 DigiCert가 생각하는 위반 증거를 공개할 수 있다는 데 동의합니다.

(g) **멀티플렉싱 장치.** 서버 소프트웨어가 제공하는 서비스에 직접 액세스하거나 이를 직접 사용하는 사용자 수를 줄여주는 하드웨어 또는 소프트웨어가 서버 소프트웨어가 제공하는 서비스에 액세스하거나 이를 사용하는 것으로 간주되는 사용자 수를 줄여주지는 않습니다. 서버 소프트웨어에 액세스하거나 이를 사용하는 사용자 수는 (a) 해당 서버 소프트웨어 또는 (b) 서버 소프트웨어가 해당 소프트웨어 또는 시스템을 인증 또는 허가하는 경우 다른 소프트웨어 또는 시스템(**"기타 인증 시스템"**)이 제공하는 서비스에 직접 또는 멀티플렉싱 장치를 통해 액세스하거나 사용하는 사용자 수와 같습니다. 여기서 사용되는 **"멀티플렉싱 장치"**는 서버 소프트웨어 또는 기타 인증 시스템이 적은 수의 연결을 통해 여러 다른 사용자에게 또는 이들 사용자를 대신하여 제공하는 서비스에 대한 액세스 권한을 직접 또는 간접적으로 제공하거나 보유하는 하드웨어 또는 소프트웨어를 의미합니다.

(h) **Windows CAL 요구사항.** 고객은 서버 소프트웨어 또는 기타 인증 시스템이 제공하는 서비스에 직접 또는 멀티플렉싱 장치를 통해 액세스 또는 사용하는 사용자마다 별도 Windows CAL을 확보, 지정해야 합니다. **"Windows CAL"**은 (a) Microsoft Windows Server 2003(Standard Edition, Enterprise Edition 또는 Datacenter Edition) 서버 운영 체제 제품(또는 그 후속 제품)(**"Windows Server"**)의 경우 Windows 장치 클라이언트 액세스 라이센스(**"CAL"**) 또는 Windows 사용자 CAL, 또는 (b) Windows Server에 액세스하고 이를 사용할 수 있는 권리를 개인 또는 전자 장치에 제공하는 Microsoft Core CAL을 의미합니다. (a), (b) 경우 모두 고객은 하나 이상의 해당 Microsoft Windows Server 운영 체제 제품 또는 전자 장치에 사용하기 위해 Windows Server를 구입했으며 사용자 또는 장치가 그 사용 기준이 됩니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

서비스 수준 합의서.

DigiCert의 서비스 가용성 약속은 고지사항에 나와 있는 해당 서비스 수준 합의서에 기술되어 있습니다.

정의

영문 서비스 기술서에서 대문자로 표시되고 합의서 또는 본 서비스 기술서에 달리 정의되지 않은 용어는 다음과 같은 의미를 갖습니다.

"관리자 인증서"는 DigiCert가 고객사 직원, 또는 관리자 역할을 수행하기 위해 PKI Manager에 액세스하는 단일 목적으로 PKI Platform 관리자로 지정된 다른 피신뢰자에게 발급한 인증서를 의미합니다.

[부록 D – LTE 인증 서비스만 해당] "관리자 인증서"는 DigiCert가 고객이 지명한 PKI Platform 관리자, 또는 최종 실체 LTE 인증서 또는 제조업체 인증서를 관리하기 위해 PKI Manager에 액세스할 목적으로 PKI Platform 관리자로 지정된 다른 피신뢰자에게 발급한 클라이언트 인증서를 의미합니다.

"관계자"는 다음 고객과 협력하는 개인을 의미합니다. (1) 임원, 이사, 직원, 파트너, 계약자, 인턴 또는 고객 조직 내 다른 사람, 또는 (2) 고객 조직과의 계약 관계를 유지 관리하는 개인으로 고객이 해당 개인의 신원을 강력하게 보증할 수 있는 비즈니스 기록을 갖고 있는 경우.

"CA 인증서"는 인증 기관(CA)에 발급된 디지털 인증서를 의미합니다.

"인증서" 또는 **"디지털 인증서"**는 최소한 발급 CA의 이름 또는 ID, 가입자, 가입자의 공용 키, 인증서의 유효 기간, 인증서 일련 번호, 발급 CA의 디지털 서명을 포함하는 디지털 기록을 의미합니다.

"인증 신청자"는 CA의 인증서 발급을 요청하는 개인 또는 조직을 의미합니다.

"인증서 신청"은 인증서 발급을 위해 인증 신청자(또는 허가받은 에이전트)가 CA에 제출하는 요청을 의미합니다.

"인증 기관" 또는 **"CA"**는 인증서를 발급, 보류 또는 폐기할 수 있는 개인 또는 실체를 의미합니다.

"인증서 관리 프로토콜" 또는 **"CMP"**는 LTE 또는 제조업체 인증서의 자동 등록 및 수명 주기 관리를 위한 프로토콜을 의미합니다. 장치는 CMP를 통해 DigiCert PKI Platform 시스템과 직접 연결됩니다. 장치는 PKI Platform 관리자의 사전 승인을 얻어야 DigiCert PKI Platform 시스템으로 CMP 요청을 보낼 수 있습니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

"인증 업무 규정" 또는 **"CPS"**는 CA 또는 RA가 인증서 발급에 이용하는 업무 규정을 나타내는 문서를 의미하며 때때로 수정됩니다. DigiCert Trust Network CPS 및 Adobe CPS의 인증 업무 규정은 DigiCert 웹사이트의 고지사항에 나와 있습니다.

"고객"은 서비스를 이용하는 실체를 의미합니다.

"발급 오류"는 (a) 인증서 발급 시 해당 CPS에서 요구하는 절차를 정확하게 따르지 않은 경우, (b) 인증서 주체로 명시되지 않은 개인, 실체 또는 대상에게 인증서를 발급하는 경우 또는 (c) 인증서 주체로 명시된 개인, 실체 또는 대상의 허가 없이 인증서를 발급하는 경우를 의미합니다.

"최종 사용자 라이센스 계약" 또는 **"EULA"**는 소프트웨어와 함께 제공되는 약관을 의미합니다.

"키 생성"은 신뢰할 수 있는 프로세스를 통해 개인 키 보관과 그 문서화를 위해 고객 CA 공용 키와 개인 키를 올바르게 생성하는 DigiCert 절차를 의미합니다.

"LTE 인증서"는 이름, 발급 CA 또는 운영자 네트워크의 네트워크 요소를 포함하여 장치에 저장되는 메시지를 의미합니다. 네트워크 요소는 운영자 기지국 또는 보안 게이트웨이 또는 다른 유사한 장치일 수 있습니다. LTE 인증서는 모든 경우 네트워크 요소의 공용 키, 인증서 유효 기간, 인증서 일련 번호 및 발급 CA의 디지털 서명을 포함합니다.

"PKI Platform 관리자"는 등록 기관의 직원 또는 RA 작업을 수행할 수 있는 다른 피신뢰자를 의미합니다.

[부록 D – LTE 인증 서비스만 해당] "PKI Platform 관리자"는 서비스 기술서에 기술된 특정 인증서 관련 관리 기능을 수행하도록 지정된 고객 또는 계열사의 신뢰할 수 있는 직원을 의미합니다.

"제조업체"는 배포 및 판매를 목적으로 장치를 제조하는 사업체를 의미합니다.

"제조업체 인증서"는 장치에 발급되어 제조 시점에 장치에 임베드되는 인증서를 의미합니다. 평균 수명은 35~40년이며 폐기 메커니즘이 필요하지 않습니다.

"유효 기간"은 인증서가 발급된 날짜 및 시간(또는 인증서에 명시된 경우 이후 특정 날짜 및 시간)부터 인증서가 만료되거나 조기에 폐기되는 날짜 및 시간까지의 기간을 의미합니다.

[부록 D – LTE 인증 서비스만 해당] "유효 기간"은 인증서가 발급된 날짜 및 시간부터 인증서가 만료되는 날짜 및 시간까지의 기간을 의미합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

"운영자"는 일반적으로 다른 국가 또는 지역에서 활동하는 고객의 자회사로 DigiCert가 고객의 하위 계정으로 간주하는 기업체를 의미합니다.

"사설 계층 조직"은 DigiCert Trust Network 이외의 계층에서 인증서를 발급하는 인증 기관 또는 고객의 규정에 따라 고객의 루트 CA에서 하나 이상의 CA를 거쳐 가입자까지 이어지는 범위 내에서 인증서를 발급하는 CA 시스템으로 구성되는 도메인을 의미합니다. 사설 계층 조직에서 발급된 인증서는 발급을 허가하는 조직의 요구는 충족하지만 공개 채널을 통한 조직 및/또는 개인 간의 상호 작용을 위한 용도는 아닙니다.

"개인 키"는 디지털 서명을 생성하고 알고리즘에 따라 (기밀 유지를 위해) 해당 공용 키로 암호화된 메시지 또는 파일을 해독하는 데 사용되는 수학 키(소유자가 비밀유지)를 의미합니다.

"공용 키"는 공개 가능하며 해당 개인 키로 생성된 서명을 확인하는 데 사용되는 수학 키를 의미합니다. 알고리즘에 따라 공용 키는 또한 해당 개인 키로 해독할 수 있는 메시지 또는 파일을 암호화하는 데 사용됩니다.

"등록 기관" 또는 **"RA"**는 인증서의 인증 신청자 식별 및 승인을 수행하거나 인증서 폐기 요청을 시작 또는 처리하거나 인증서 갱신 또는 재발급을 위해 애플리케이션을 승인하는 실체를 의미합니다. RA는 인증 신청자의 대리인이 아닙니다. RA는 RA의 허가받은 PKI Platform 관리자에게만 인증서 신청 승인 권한을 위임할 수 있습니다.

"신뢰 당사자"는 인증서 및/또는 디지털 서명 신뢰와 관련된 역할을 수행하는 개인, 실체 또는 대상을 의미합니다. 신뢰 당사자는 또한 가입자가 될 수도, 그렇지 않을 수도 있습니다.

"고지사항"은 관련 CPS 준수를 위해 유지 관리되는 일련의 문서(https://www.websecurity.symantec.com/legal/repository)를 의미합니다.

"루트 CA"는 신뢰할 수 있는 계층 조직의 도메인에서 대표 실체를 의미하며 "루트 인증서"로 식별됩니다.

"시트"는 가입자에게 실제로 발급된 인증서 수에 관계없이 허가받은 서비스 최종 사용자에 해당하는 단일 가입자를 의미합니다.

"서비스 구성요소"는 서비스에 필요한 경우, 서비스를 받기 위해 고객 컴퓨터 각각에 설치되어야 하는 소프트웨어를 의미합니다. 서비스 구성요소에는 DigiCert가 서비스의 일부로 별도 제공할 수 있는 소프트웨어 및 관련 문서가 포함됩니다.

"소프트웨어"는 DigiCert가 고객에게 허가하고 해당 EULA 또는 경우에 따라 본 서비스 기술서의 약관으로 관리되는 개체 코드 형식의 각 DigiCert 또는 사용권 허가자 소프트웨어 프로그램을 의미하며 본 기술서에 따라 제공되는 새로운 릴리스 또는 업데이트를 포함하되 이에 한정되지 않습니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

"가입자"는 인증서의 주체이자 인증서가 발급된 개인, 실체 또는 대상을 의미하며 발급 시 인증서에 나열되는 공용 키에 상응하는 개인 키를 사용할 수 있고 사용 권한이 있습니다.

"가입자 합의"는 인증서와 관련된 가입자의 권리와 의무에 적용되는 지정된 인증서 관련 서비스의 프로비저닝과 관련하여 가입자와 CA 또는 DigiCert 간에 이행되는 합의입니다. DigiCert Trust Network 가입자 합의는 DigiCert 웹사이트의 고지사항에 게시됩니다.

"가입 문서"는 서비스와 관련된 고객의 권리와 의무를 상세하게 정의하는 다음 관련 문서 중 하나 이상을 의미합니다: DigiCert 인증서 또는 DigiCert가 발급하는 유사 문서 또는 서비스와 함께 또는 사전, 사후에 작성되는 고객과 DigiCert 간의 서면 합의.

"DigiCert Trust Network" 은 DigiCert Trust Network CPS가 관리하는 인증서 기반 공용 키 인프라를 의미하며 DigiCert와 그 계열사 및 해당 고객, 가입자, 신뢰 당사자의 전 세계 인증서 배치와 사용을 지원합니다.

"피신뢰자"는 고객과 해당 제품, 서비스, 시설 및/또는 규정의 인프라 신뢰성을 관리해야 하는 고객의 직원, 계약자 또는 컨설턴트를 의미합니다.

부록.

부록 A: DigiCert Trust Network

DigiCert PKI Platform 서비스는 DigiCert Trust Network에서 인증서를 발급할 수 있는 기능을 고객에게 제공합니다. DigiCert는 가장 널리 사용되는 웹 브라우저, 이메일 애플리케이션, 운영 체제, 네트워크 어플라이언스에 DigiCert Trust Network 기본 인증 기관(PCA)을 임베드하기 위해 하드웨어 및 소프트웨어 공급업체와 협력해왔습니다. 그 결과, 이 PCA 중 하나에 연결되는 인증서는 자동으로 이들 애플리케이션의 신뢰를 받을 수 있습니다. 이러한 인증서는 관리자 또는 사용자의 특별한 준비 없이 조직 전체에서 일반적으로 사용될 수 있습니다. 한 예로 많은 고객이 이메일을 디지털 서명 및/또는 암호화하는 보안 이메일에 DigiCert Trust Network 인증서를 사용하고 있습니다.

DigiCert Trust Network을 인증 기관(CA)으로 선택하는 고객에게는 계정 설정 과정에서 클래스 2 CPA에 연결되는 발급 CA가 자동으로 프로비저닝됩니다. 고객이 다른 상표 이름을 원하거나 CA의 기본값을 변경하려는 경우 추가 CA 생성 옵션을 구입할 수 있습니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

참고: 고객과 사용자는 이러한 인증서 발급, 관리 및 사용을 위해 DigiCert Trust Network 인증 업무 규정(CPS)을 준수해야 합니다.

추가 서비스 조건 – DigiCert Trust Network에만 적용

지명. DigiCert는 본 기술서에서 DigiCert Trust Network CPS에 따라 DigiCert Trust Network 내에서 고객을 비 DigiCert CA로 지명하며 고객은 그러한 지명을 수락합니다.

DigiCert Trust Network CPS. 고객은 본 서비스 기술서에 따라 DigiCert에 아웃소싱된 기능을 제외한 모든 요구사항을 충족해야 하며 주기적으로 수정되는 DigiCert Trust Network CPS를 포함하되 이에 한정되지 않는 DigiCert Trust Network 내 CA 및/또는 RA에 부과되는 모든 의무를 수행해야 합니다. DigiCert는
PKI Manager에 정보를 게시하여 고객이 지명한 PKI Platform 관리자에게 수정사항을 고지합니다.

지명. 고객은 한 명 이상의 허가받은 고객 직원 또는 피신뢰자를 PKI Platform 관리자로 지명해야 합니다. 해당 PKI Platform 관리자는 고객을 대신하여 추가 PKI Platform 관리자를 지명할 수 있어야 합니다. 고객은 본 서비스 기술서에 따라 인증서를 받는 PKI Platform 관리자가 해당 가입자 합의의 약관을 준수할 수 있도록 해야 합니다.

관리자 역할. 고객은 DigiCert가 지정하는 하드웨어와 소프트웨어를 사용하여 인증 신청서의 정보 검증, 해당 인증서 신청 승인 또는 거절, 인증서 폐기 요구사항을 포함하되 이에 한정되지 않으며 주기적으로 수정되는 DigiCert Trust Network CPS에 명시된 요구사항을 준수해야 합니다. 고객은 그러한 역할을 만족할 만한 수준으로 전문적이고 능숙하게 수행해야 합니다. 고객은 인증서 신청자가 고객의 관계자인
경우에만 인증서 신청을 승인해야 합니다. 고객이 인증서를 발급한 가입자가 더 이상 관계자로서 고객과 관계를 유지하지 않는 경우 고객은 즉시 PKI Manager를 통해 해당 가입자의 인증서 폐기를 요청해야 합니다. PKI Platform 관리자에게 고객을 대신하여 PKI Platform 관리자 역할을 이행할 수 있는 권한이 더 이상 없는 경우 고객은 즉시 해당 PKI Platform 관리자의 관리자 인증서 폐기를 요청해야 합니다.

고객의 가입자. 고객은 본 서비스 기술서에 따라 인증서를 받는 가입자가 해당 가입자 합의의 약관을 준수하도록 해야 하며, 가입자는 인증서 등록 조건으로 이에 동의해야 합니다. 고객은 해당 가입자 합의 약관이 DigiCert Trust Network CPS의 합의 약관과 동일한 수준으로 CA를 보호하도록 해야 합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

DigiCert의 보증. DigiCert는 다음 사항을 보증합니다. (i) DigiCert는 인증서 생성 과정에서 합당한 주의를 기울이지 않아 인증서 정보에 오류를 야기하지 않습니다. (ii) DigiCert는 인증서 발급 시 모든 중요 측면에서 DigiCert Trust Network CPS를 준수합니다. (iii) 폐기 서비스와 고지사항 이용에 있어 모든 중요 측면에서 DigiCert Trust Network CPS를 준수합니다.

부록 B: 사설 인증 기관

DigiCert PKI Platform 서비스는 사설 인증 기관(CA)에서 인증서를 발급할 수 있는 기능을 고객에게 제공합니다. DigiCert는 이 CA를 대신하여 개인/공용 키 쌍을 생성하는 키 세레모니라는 안전하고 공식적인 절차를 수행합니다. 이러한 인증서는 일반적으로 조직 자원에 대한 액세스를 제어하는 데 사용됩니다. 예를 들어 많은 고객이 VPN 또는 WiFi를 통한 개인 네트워크 액세스에 있어 사설 CA만을 신뢰함으로써 네트워크에 대한 무단 액세스를 방지합니다.

모든 고객을 대상으로 계정 설정 과정에서 사설 인증 기관(CA)이 자동으로 프로비저닝됩니다. 이 CA는 계정 설정을 위해 심사를 거쳐 DigiCert에 제공되는 고객의 법적 실체 이름을 기반으로 합니다. 고객이 해당 조직에 다른 상표 이름을 사용하거나(예를 들어 법적 실체 이름 대신 브랜드 이름) CA의 기본 이름을 변경하려는 경우 고객은 추가 CA 생성 옵션을 구입할 수 있습니다.

참고: 고객은 해당 사설 CA에서의 인증서 발급, 관리, 사용에 대한 자체 인증 업무 규정(CPS)을 정의 및 이행해야 합니다.

추가 서비스 조건 – 사설 인증 기관에만 적용

지명. 고객은 한 명 이상의 허가받은 고객 직원 또는 피신뢰자를 PKI Platform 관리자로 지명해야 합니다. 해당 PKI Platform 관리자는 고객을 대신하여 추가 PKI Platform 관리자를 지명할 수 있어야 합니다. 고객은 본 서비스 기술서에 따라 인증서를 받는 PKI Platform 관리자가 해당 가입자 합의의 약관을 준수할 수 있도록 해야 합니다.

관리자 역할. 고객은 DigiCert가 지정한 하드웨어와 소프트웨어를 사용하는 PKI Platform 관리자를 통해 인증서 신청의 정보를 검증하고 해당 인증서 신청을 승인 또는 거부해야 하며 DigiCert가 인증서를 발급, 갱신 및 폐기하도록 알려주어야 합니다. PKI Platform 관리자에게 고객을 대신하여 PKI Platform 관리자 역할을 이행할 수 있는 권한이 더 이상 없는 경우 고객은 즉시 해당 PKI Platform 관리자의 관리자 인증서 폐기를 요청해야 합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

DigiCert의 보증. DigiCert는 DigiCert가 인증서 생성 과정에서 합당한 주의를 기울이지 않아 인증서 정보에 오류를 야기하지 않음을 보증합니다.

부록 C: Adobe® 문서 서명 서비스

DigiCert PKI Platform 서비스는 Adobe® Document Signing Services에서 인증서를 발급할 수 있는 기능을 고객에게 제공합니다. DigiCert는 Adobe Acrobat®, Reader® 및 LiveCycle® 제품이 자동으로 신뢰하는 인증서 발급을 위해 Adobe와 협력해왔습니다. 이러한 인증서는 해당 제품에서 PDF(Portable Document File)를 디지털 서명하는 데 사용됩니다.

Adobe를 인증 기관(CA)으로 선택하는 고객에게는 계정 설정 과정에서 Adobe Document Signing Services에 대해 Symantec의 중간 CA에 연결되는 발급 CA가 자동으로 프로비저닝됩니다. 이 CA는 계정 설정을 위해 심사를 거쳐 DigiCert에 제공되는 고객의 법적 실체 이름을 기반으로 합니다. 고객이 해당 조직의 다른 상표 이름을 사용하려 하거나(예를 들어 법적 실체 이름 대신 브랜드 이름) CA의 기본값을 변경하려는 경우 추가 CA 생성 옵션을 구입할 수 있습니다.

참고: 고객과 사용자는 이러한 인증서 발급, 관리 및 사용을 위해 Adobe CDS 인증 업무 규정(CPS) 또는 Adobe ATL CPS(해당하는 경우)를 준수해야 합니다.

AATL의 경우 고객은 SHA256 또는 ECC 중 하나를 선택할 수 있습니다.

추가 서비스 조건 – Adobe® Document Signing Services에만 적용

지명. 고객은 한 명 이상의 허가받은 고객 직원 또는 피신뢰자를 PKI Platform 관리자로 지명해야 합니다. 해당 PKI Platform 관리자는 고객을 대신하여 추가 PKI Platform 관리자를 지명할 수 있어야 합니다. 고객은 본 서비스 기술서에 따라 인증서를 받는 PKI Platform 관리자가 해당 가입자 합의 약관 및 CPS를 준수할 수 있도록 해야 합니다.

관리자 역할. 고객은 DigiCert가 지정한 하드웨어와 소프트웨어를 사용하는 PKI Platform 관리자를 통해 인증서 신청의 정보를 검증하고 해당 인증서 신청을 승인 또는 거부해야 하며, DigiCert가 PKI Manager에서 게시하고 비정기적으로 수정되는 CPS에 따라 인증서를 발급, 갱신 및 폐기하도록 알려주어야 합니다. PKI Platform 관리자에게 고객을 대신하여 PKI Platform 관리자 역할을 이행할 수 있는 권한이 더 이상 없는 경우 고객은 즉시 해당 PKI Platform 관리자의 관리자 인증서 폐기를 요청해야 합니다.

고객의 가입자. 고객은 본 서비스 기술서에 따라 인증서를 받는 가입자가 해당 가입자 합의의 약관을 준수하도록 해야 하며, 가입자는 인증서 등록 조건으로 이에 동의해야 합니다. 고객은 해당 가입자 합의 약관이 CPS의 합의 약관과 동일한 수준으로 CA를 보호하도록 해야 합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

DigiCert의 보증. DigiCert는 DigiCert가 인증서 생성 과정에서 합당한 주의를 기울이지 않아 인증서 정보에 오류를 야기하지 않음을 보증합니다.

부록 D: LTE 인증 서비스

Symantec™ LTE 서비스("LTES" 또는 "서비스")는 운영자 LTE 장비에 통합될 장치 인증서를 사설 계층 조직에서 얻을 수 있는 기능을 고객에게 제공합니다. 고객 또는 운영자는 인증서 관리 프로토콜(CMP)과 같은 프로그래밍 인터페이스를 통해 LTES에 대한 요청을 DigiCert에 제출합니다.

추가 서비스 조건 – LTE 인증 서비스에만 적용

지명. 고객은 한 명 이상의 허가받은 고객 및/또는 운영자 직원을 해당 직원을 채용하는 실체를 위한 PKI Platform 관리자로 지명해야 합니다. 고객은 본 서비스 기술서에 따라 관리자 인증서를 받는 PKI Platform 관리자가 해당 인증서와 관련된 해당 가입자 합의의 약관을 준수하고 PKI Platform 관리자 인증서를 본 서비스 기술서에 부합되는 허가받은 합법적인 목적으로만 사용하도록 해야 합니다. 고객은 가입자의 허가받은 PKI Platform 관리자 자격이 소멸되는 경우 즉시 해당 관리자 인증서 폐기를 요청해야 합니다.

관리자 역할. 고객 및/또는 운영자는 필요한 경우 지명된 PKI Platform 관리자를 통해 다음 사항을 책임져야 합니다.

1. 운영자 하위 계정 생성
2. 인증서 프로필 생성
3. 제조업체 CA 인증서 제공
4. 검증용 IP 주소 블록 제공
5. 새 장치 등록 및 향후 요청을 위한 사전 승인 설정
6. 네트워크상 요소의 CMP 응답자 URL 구성.

계정 승인 및 인증서 발급. 고객은 해당 운영자의 연락처 정보, 해당 운영자의 PKI Platform 관리자로 지정된 개인의 신원 정보(즉 등록 정보 포함), 각 운영자에게 허가된 LTE 인증서와 사이트의 수를 포함하여 본 서비스 기술서에 따라 발급된 LET 인증서를 받을 수 있는 운영자의 사전 서면 승인을 DigiCert에 제공해야 합니다. 고객은 각 PKI Platform 관리자가 (해당 PKI Platform 관리자 인증서 생성 시점 이후) 해당 인증서의 개인 키, PIN, 소프트웨어 또는 개인 키를 보호하는 하드웨어 메커니즘을 소유하는 유일한 사람이며 앞으로도 그러하다는 사실과 권한없는 사람이 전술한 자료 또는 정보에 액세스한 적이 없으며 앞으로도 그러할 것이라는 사실을 확인하고 해당 운영자가 그러한 사실을 확인하도록 해야 합니다.

PKI Platform 관리자가 PKI Manager를 통해 요청된 인증서 수를 앞에 명시된 대로 고객이 허가한 인증서 요청을 제출하는 경우 DigiCert는 (i) 해당 인증서 요청 각각에서 정보의 정확성을 신뢰하고 (ii) 요청한 PKI Platform 관리자에게 해당 인증서를 발급, 제공할 수 있습니다. 본 서비스 기술서에 따라 발급 또는 허가된 장치 인증서의 유효 기간은 인증서 발급일로부터 1, 2 또는 3년입니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

DigiCert는 수령한 주문서에서 전술한 요구사항을 충족하는 모든 주문을 이행합니다. 본 서비스 기술서에서 모순되는 조항에도 불구하고, 인증서를 요청할 수 있는 운영자의 수와 인증서를 요청할 수 있는 프로덕션 사이트 및 PKI Platform 관리자의 수는 해당 주문서에 명시된 수로 엄격하게 제한됩니다.

제조업체 의무 이행. 고객은 DigiCert 시스템 또는 소프트웨어의 기술 구현을 모니터링, 방해 또는 역설계하거나 DigiCert 시스템 또는 소프트웨어의 보안을 고의로 위태롭게 만들어서는 안 되며 지명된 제조업체에도 같은 제약을 가해야 합니다.

CA 인증서. 본 서비스 기술서 내용에 반하는 어떤 사항에도 불구하고, DigiCert는 DigiCert의 표준 PKI 규정 및 정책에 따라 2개의 고객 루트 인증서와 선택적으로 각 루트 인증서에 따라 발급된 최대 2개의 CA 인증서를 생성, 호스트하며 CA 인증서는 본 기술서에 따라 고객에게 서비스를 제공하기 위한 목적으로만 사용됩니다. 추가 CA 인증서는 별도 구매할 수 있습니다. DigiCert는 표준 PKI 규정과 정책에 따라 고객의 요청을 기반으로 운영자를 선택하고 이들을 위한 하위 계정을 생성합니다.

IP 주소 구성. 새 운영자를 참여시키는 과정에서 DigiCert에 일련의 유효한 IP 주소를 제공해야 합니다. DigiCert 시스템은 유효한 IP 주소로부터 수신되는 CMP 요청에만 대응하며 구성된 IP 주소에서 전송되지 않는 다른 모든 요청은 거부됩니다. 이 구성은 운영자가 수행해야 합니다.

계정 활성화. 사전 구매 시, DigiCert는 다음 요건이 충족되었다는 전제하에 미국 내 하위 계정의 경우 10일(평일 기준) 이내, 미국 외 계정의 경우 상업적으로 합당한 기간 내에 활성화하기 위해 통상적으로 합당한 노력을 기울입니다: (i) 필요한 등록 프로세스 완료 (ii) 운영자 및 해당 PKI Platform 관리자 인증. DigiCert가 적시에 인증을 수행하려면 이 기간 동안 이 PKI Platform 관리자에 액세스할 수 있어야 합니다.

DigiCert의 보증. DigiCert는 DigiCert가 인증서 생성 과정에서 합당한 주의를 기울이지 않아 본 기술서에 따라 발급된 인증서에 오류를 야기하지 않음을 보증합니다.

부록 E: 제조업체 인증서

DigiCert PKI Platform 서비스는 제조업체 에코시스템 장치로의 통합을 위해 사설 계층 조직에서 제조업체 인증서를 발급할 수 있는 기능을 고객에게 제공합니다. 제조업체 인증서는 장치 인증 또는 장치에서 전송한 메시지를 암호화하는 데 사용됩니다. 고객은 배치 인터페이스를 사용하여 DigiCert PKI Platform 서비스로부터 제조업체 인증서를 요청합니다.

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

추가 서비스 조건 - 제조업체 인증서에만 적용

지명. 고객은 한 명 이상의 허가받은 고객 직원을 해당 직원을 채용하는 실체를 위한 PKI Platform 관리자로 지명해야 합니다. 고객은 본 서비스 기술서에 따라 관리자 인증서를 받는 PKI Platform 관리자가 해당 인증서와 관련된 해당 가입자 합의의 약관을 준수하고 관리자 인증서를 본 서비스 기술서에 부합되는 허가받은 합법적인 목적으로만 사용하도록 해야 합니다. 고객은 가입자의 허가받은 서비스 관리자 자격이 소멸되는 경우 즉시 해당 관리자 인증서 폐기를 요청해야 합니다.

관리자 역할. 고객 및/또는 운영자는 필요한 경우 지명된 PKI Platform 관리자를 통해 다음 사항을 책임져야 합니다.

1. 하위 계정 생성
2. 인증서 프로필 생성
3. 제조업체 CA 인증서 제공
4. 인증서 발급을 위한 배치 요청 제출.

제조업체 의무 이행. 고객은 DigiCert 시스템 또는 소프트웨어의 기술 구현을 모니터링, 방해 또는 역설계하거나 DigiCert 시스템 또는 소프트웨어의 보안을 고의로 위태롭게 만들어서는 안 되며 지명된 제조업체에도 같은 제약을 가해야 합니다.

인증서 발급. 서비스 관리자가 PKI Manager를 통해 배치 인증서 요청을 제출하면 DigiCert는 (i) 해당 인증서 요청 각각에서 정보의 정확성을 신뢰하고 (ii) 요청한 PKI Platform 관리자에게 해당 인증서를 발급, 제공할 수 있습니다. . DigiCert는 수령한 주문서에서 전술한 요구사항을 충족하는 모든 주문을 이행합니다. 본 서비스 기술서에서 모순되는 조항에도 불구하고, 요청할 수 있는 인증서 수는 해당 주문서에 지정된 수로 엄격히 제한됩니다.

계정 활성화. 사전 구매 시, DigiCert는 다음 요건이 충족되었다는 전제하에 미국 내 계정의 경우 10일(평일 기준) 이내, 미국 외 계정의 경우 상업적으로 합당한 기간 내에 활성화하기 위해 통상적으로 합당한 노력을 기울입니다: (i) 필요한 등록 프로세스 완료 (ii) 고객 및 해당 PKI Platform 관리자 인증. DigiCert가 적시에 인증을 수행하려면 이 기간 동안 이 PKI Platform 관리자에 액세스할 수 있어야 합니다.

DigiCert의 보증. DigiCert는 DigiCert가 인증서 생성 과정에서 합당한 주의를 기울이지 않아 본 기술서에 따라 발급된 인증서에 오류를 야기하지 않음을 보증합니다.

개인 루트 CA의 필수 조건. 제조업체 인증서는 루트 CA의 사설 계층 조직 내에서 유효하므로 DigiCert의 제조업체 인증서 프로비저닝은 고객의 루트 CA가 요구하는 모든 조건 충족을 전제로 할 수 있습니다. 이는 루트 CA가 산업 컨소시엄 또는 표준 제정 단체와 같은 고객 이외의 제3자이고 해당 제조업체 인증서를 해당 루트 CA가 관리하는 에코시스템에서만 사용하려 하는 경우

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.

DigiCert가 호스트하는 루트 인증서에 따라 발급된 제조업체 인증서를 받기 위한 전제조건에 해당합니다. 그러한 전제조건에는 루트 CA가 지정하는 추가 문서의 이행이 제한없이 포함될 수 있습니다. **루트 CA는 해당 에코시스템을 대상으로 한 제조업체 인증서 발급에 절대적인 권한을 가지며 고객에게 인증서를 발급하지 말라고 DigiCert에게 지시할 수 있습니다. DigiCert는 루트 CA가 수행하는 조치와 관련된 모든 책임을 부인합니다. 루트 CA는 에코시스템의 각 제조업체 인증서에서 소유하는 모든 독점 및 지적 재산권을 보유합니다. 루트 CA가 소유하는 그러한 권리는 루트 CA가 지정하는 문서에 따라 고객에게 허가됩니다. 고객은 루트 CA가 요청하는 경우 DigiCert가 고객의 신원과 모든 인증서 판매를 보고해야 함을 인정하고 이에 동의합니다.**

자세한 정보

DIGICERT, INC.
2801 Thanksgiving Way, Suite 500
Lehi, Utah 84043
United States
https://www.digicert.com/

© 2018 DigiCert, Inc. All rights reserved. DigiCert는 미국 및 기타 국가에서 DigiCert, Inc.의 등록 상표입니다. 다른 모든 상표 및 등록 상표는 해당 소유자의 재산입니다.