

DigiCert® 기업용 PKI 플랫폼: 비즈니스용 Windows Hello 지원

암호가 필요없습니다!

암호가 필요없는 로그인 기능은 접속 지점에서 보안성을 증진시키는 한편 사용자의 로그인 체험을 단순화하는 방법으로 주목을 받고 있습니다. 암호가 강력해도 재전송 및 피싱 공격을 받기 쉽고, 서버가 뚫려서 노출될 수 있으며, 사용자가 암호를 기억하기 어려울 때도 있습니다. 그리고, 기업체에서 제로 트러스트 보안 모델을 도입하여 각 접속 지점에서 검증을 받아야 하기 때문에, 접속 보안은 사이버 공격으로부터 보호하고 기업체의 노동력을 구현하기 위한 IT 분야의 관심사로 그 중요성이 높아지고 있습니다. 암호가 필요없는 로그인 기능을 활용하면, 최종 사용자는 암호를 생성하거나 기억하지 않아도 되고 보다 안전한 방법으로 아이덴티티를 검증하게 됩니다.

“ 웹 애플리케이션 위반의
89%는
크리덴셜을 기만하는 것과
관련이 있습니다(도난당한
크리덴셜 또는 무차별
대입의 사용). ”

-Verizon 2021 데이터 위반
조사 보고서

비즈니스용 Windows Hello: 인증서 신뢰 모델

비즈니스용 Windows Hello(WHfB)는 Microsoft에서 로그인을 검증하기 위한 암호가 필요없는 인증 솔루션입니다. 이는 생체 또는 PIN 아이덴티티 크리덴셜을 사용하는 PC 및 모바일 기기에서 강력한 (멀티 팩터) 인증을 사용합니다.

WHfB용 인증서 신뢰 모델은 인증 기관(CA)에서 발행하는 인증서로 액티브 디렉토리(AD)를 인증하는 공개 키 기반구조(PKI)에 의해 지지되는 디지털 인증서를 사용합니다.

이 키 신뢰 모델은 공개 키로 AD를 인증하며 자체 서명된 인증서가 필요합니다.

WHfB, 키 신뢰 및 인증서 신뢰에서 도입한 2개의 주요 신뢰 모델 가운데, 다음에 관련된 기업체에서는 인증서 신뢰를 선호합니다.

- 용도 사례: 인증서 신뢰 모델을 사용하면, WHfB 인증서는 Windows 로그인용 스마트 카드 인증서와 동일한 방식으로 사용할 수 있습니다.
- 아이덴티티 및 접속 기술: 최종 사용자 인증서를 발행하고 관리하기 위해 이미 PKI를 사용하는 기업체에서도 PKI를 비즈니스용 Windows Hello와 결합해서 활용할 수 있습니다.

DigiCert® 기업용 PKI 플랫폼 및 비즈니스용 Windows Hello

DigiCert 기업용 PKI 플랫폼은 WHfB 인증서 신뢰 모델을 지원하여, 용도 사례 그리고 고객들이 암호가 필요없는 로그인 기능에 필요로 하는 편의성을 제공합니다. 다음과 같습니다.

- 사전 정의된 인증서 템플릿과 이에 상응하는 등록 방법으로 WHfB 인증서 관리가 **간편화됩니다**.
- Windows 도메인 결합 워크스테이션에 대해 WHfB에서 요구하는 클라이언트 인증 인증서의 제로-터치 프로비저닝과 자동화된 워크플로우로 온보딩이 **가속화됩니다**.
- 기타 기업용 용도 사례를 관리하는데 사용하는 것과 동일한 플랫폼으로 WHfB 디지털 인증서를 관리하기가 **용이합니다**.

WHfB 지원은 DigiCert 기업용 PKI 플랫폼에서 지원하는 여러 기능 중 하나입니다. 각 조직은 이 플랫폼을 사용하여 자동화된 워크플로우, 사전 구성된 템플릿, 복수의 등록 방법 및 제3자 업체 통합 기능에 기반하여 단순화된 디지털 인증서 프로비저닝과 관리 체험을 제공할 수 있습니다.

비즈니스용 Windows Hello 관리자인 경우, 이는 다음을 의미합니다.

PKI 플랫폼 기능	혜택
사전 정의된 WHfB용 인증서 템플릿	WHfB 도메인 컨트롤러, 등록 에이전트 및 사용자 인증을 위해 사전 정의된 인증서 템플릿으로 DigiCert 자동등록 서버(클라이언트 없음)를 통해 사용자 및 기기의 신속한 온보딩 지원
제로-터치 인증서 수명주기 관리	자동화된 인증서 갱신, 재발행, 만료 및 리-프로비저닝 기능으로 사용자 생산성과 보안성 증대
강력한 키 보호 및 정책 시행	신뢰 플랫폼 모듈(TPM)을 사용하는 키 생성 및 보호를 위한 옵션 제공, 그리고 TPM 사용에 대한 정책 시행
WHfB 제3자 업체의 시스템 및 애플리케이션과 중단없는 통합	연합 및 분산 시스템을 위한 SAML은 물론 REST API, SCEP 및 EST 지원을 활용한 통합 용이성
WHfB 및 기타 디지털 인증서에 대한 집중 관리와 집행	단 하나의 중앙 플랫폼에서 완전한 인증서 수명주기 관리, 추적, 감사 로그 및 보고서 작성 등 전자 차원에서 인증서의 가시성 및 제어 가능
신속한 플랫폼 배포	소프트웨어 및 HSM 기반 CA를 위해 신속한 배포와 온라인 CA 생성 가속화
유연성과 확장성이 매우 뛰어난 PKI 플랫폼	검증된 확장성과 함께 클라우드, 직접 설치식 및 하이브리드 모델을 비롯하여 복수의 PKI 플랫폼 배포 옵션 지원
다국어 지원	모든 웹 인터페이스, 관리 콘솔 및 최종 사용자 등록 웹 페이지에서 다국어를 지원합니다.

기술 요구사항

DigiCert® 기업용 PKI 플랫폼

- 도메인 결합 Windows 서버*에서 자동등록 서버를 활용한 PKI 플랫폼 8 또는
- 도메인 결합 Windows 서버에서 자동등록 서버를 활용한 기업용 PKI 매니저(2022년1분기 출시)

Windows 서버 운영체제(OS):

2019, 2016 또는 2012

디렉토리 서비스:

Windows 액티브 디렉토리(AD)*, Azure AD

싱글 사인온 솔루션:

Microsoft 액티브 디렉토리 연합 서비스(ADFS)

아이덴티티 데이터 동기화 솔루션:

Azure AD 커넥트

클라이언트 머신 OS:

Windows 10

*성분은 동일하게 지원되는 Windows 서버 OS에서 실행되어야 합니다.

자세한 정보 또는 무료 시험판 요청은 1.801.770.1736 또는 pki_info@digicert.com으로 문의하거나 digicert.com/pki/enterprise-pki-manager를 참조하십시오.