Solution Brief

탈레스 피싱 방지 FIDO2 및 Azure AD (Microsoft Entra의 일부)용 인증서 기반 인증

cpl.thalesgroup.com

THALES
Building a future we can all trust

사용자가 점점 더 많은 클라우드 기반 애플리케이션에 로그인하면서, 취약한 비밀번호가 신원 도용 및 보안 침해의 주요 원인으로 떠오르고 있습니다.

이 문제를 해결하고자 탈레스 FIDO2 보안키는 이제 Microsoft Entra 구성 기능의 일부인 Azure AD와의 원활한 통합을 지원합니다. 이는 조직에 매우 안전하며 비밀번호 없는 인증을 제공하고 Microsoft 환경이나 SaaS 애플리케이션, Windows 엔드포인트에 대한 무단 액세스 위험을 줄여줍니다.

비밀번호를 FIDO2 보안키로 대체하면 비밀번호 없는 최신 MFA 환경을 도입하게 되어 피싱 공격이나 계정 도용을 방지하고 최신 보안 지침과 규정을 충족할 수 있습니다.

탈레스 FIDO2 보안키는 동시에 다양한 애플리케이션을 지원합니다. FIDO2, WebAuthn, U2F, PKI 및 RFID를 한데 지원하는 하나의 키로 물리적 공간과 논리적 리소스에 모두 액세스할 수 있습니다.

비밀번호 없는 FIDO2 인증

비밀번호 없는 FIDO2 인증은 취약한 비밀번호를 강력한 피싱 방지 기능을 갖춘 WebAuthn 자격 증명으로 대체하여 보안 침해 위험을 줄입니다.

FIDO 인증은 사용자 로그인 경험을 더 편리하게 만들고 비밀번호 고유의 취약성을 극복하는 데 상당한 이점이 있기 때문에 최신 MFA 유형으로 큰 호응을 얻고 있습니다. 이점으로는 사용자 불편이 적다는 점과 피싱 공격에 대한 보안 수준이 높다는 점이 있습니다.

엄격한 규제 준수 의무 충족

탈레스 FIDO2 보안키, USB 토큰, 스마트 카드를 사용하면 모든 규제 조건을 충족할 수 있습니다. 이 제품들은 FIDO2 및 U2F 인증을 받았습니다. PKI-FIDO 결합 제품은 피싱 방지 MFA 및 NIST 규정에 대한 미 행정명령 법규를 준수하고 FIPS 140-2 또는 공통 기준(CC) 인증을 받았으며 Java 플랫폼 및 PKI 애플릿에 대한 ANSSI 인증도 받았습니다. 또한, eSignature 및 eSeal 애플리케이션의 eIDAS 규정을 준수합니다.

다수의 사용자 인증 여정지원

디지털 보안 부문에서 세계적인 선도 기업인 탈레스는 Azure AD와 통합하여 다양하고 강력한 FIDO2 보안키로 비밀번호 없는 인증 과정을 다수 지원합니다.

전한 SaaS 앱 액세스

대다수 사용자는 여러 앱에서 같은 비밀번호를 사용하기 때문에 사용자에게 FIDO 인증 기기를 제공하면 보안을 상당히 개선하고 헬프데스크 문의를 줄일 수 있습니다. 탈레스 FIDO 기기는 Azure AD와 완벽히 호환되며 Azure AD 관리 애플리케이션에 대한 액세스를 보호합니다.

일선 인력을 위한 네트워크 로그인

FIDO2 보안키는 비밀번호 없는 MFA를 제공하여 일선 인력과 같은 사용자가 Windows PC나 태블릿 같은 공유 기기에 안전하게 액세스할 수 있도록 지원합니다.

물리적 액세스와 논리적 액세스의 결합

탈레스 FIDO 스마트 카드는 편의성을 최적화할 수 있도록 물리적 액세스를 지원하기 때문에 사용자가 하나의 맞춤 주문 가능한 스마트 카드를 이용해 물리적 공간과 논리적 리소스에 모두 액세스할 수 있습니다.

PKI/CBA 환경의 현대화

Azure AD 클라우드 네이티브 CBA에 대한 새로운 지원 기능이 있기 때문에 PKI와 인증서 기반 인증(CBA)을 이용하는 조직은 이제 탈레스 PKI-FIDO 결합 스마트 카드나 USB 토큰을 사용하여 클라우드 및 디지털 혁신 이니셔티브를 도모할 수 있습니다. 사용자에게 단일 인증 장치를 제공하여 기존 앱, 네트워크 도메인, 클라우드 서비스에 대한 액세스를 보호함으로써 운영 비용을 줄이고 사용자 경험을 간소화합니다.

안전한 원격 액세스

사용자는 재택근무 중이든 출장 중이든 상관없이 다양한 위치에 있는 다수의 장치에서 웹 기반 애플리케이션에 로그인할 수 있습니다. 탈레스 FIDO 인증 기기는 엔드포인트 기기나 위치와 상관없이 MFA를 이용한 보안 원격 액세스를 제공하여 조직을 보호합니다.

안전한 모바일 액세스

탈레스 FIDO 기기를 사용하면 휴대기기에서 모든 클라우드 리소스에 인증할 수 있습니다. NFC를 사용하여 비접촉식 스마트 카드를 기기에 대거나 SafeNet eToken Fusion USB-C를 휴대폰에 연결하면 됩니다.

관리자 액세스 컨트롤

높은 권한을 가진 관리자(관리자, VIP 등...)는 민감 데이터에 쉽게 액세스할 수 있는 상태입니다. 관리자 계정은 스피어 피싱이나 웨일링 공격의 주요 대상입니다.

관리자에게 FIDO2 보안키를 제공하여 취약한 비밀번호를 대체하면, 관리자만 관리자 리소스에 액세스하게 할 수 있습니다.

지원 플랫폼

탈레스 PKI/FIDO 보안키는 iOS, Android, Windows 11, 10, 8, Windows Server OS, macOS, Linux와 같이 다양한 운영체제를 지원합니다.

탈레스 FIDO2의 이점

Azure AD와의 완벽한 통합

- 모든 탈레스 FIDO2 보안 키는 Azure AD와 완벽하게 호환, 통합됩니다. Microsoft 기술팀의 검증을 거쳤습니다.

동급 최고 수준의 보안

- 탈레스는 전체 제조 주기를 관리하고 자체 FIDO 암호화 라이브러리를 개발하여 침해 위험을 줄입니다.

다양한 사용 사례 지원

- FIDO, PKI, 물리적 액세스를 하나의 기기로 결합
- 모바일 엔드포인트에서 강력한 인증 경험 가능

엄격한 보안 표준 준수

- U2F 및 FIDO2 인증 획득
- 피싱 방지 인증 관련 미국 및 유럽연합 규정 준수
- PKI 작업 대상 FIPS 및 CC 인증 획득

견고성 및 확장성으로 긴 수명 지원

- 경질 플라스틱, 변조 방지 USB FIDO 키
- 민감한 존재 감지기로 USB 포트 손상 방지
- 펌웨어 업데이트 지원으로 유지 관리 및 업그레이드 기능 향상

스마트 카드 - 폼 팩터

제품 특성	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
접촉식(ISO 7816)	FIDO 및 PKI	FIDO 및 PKI	해당 없음	PKI	PKI
비접촉식(ISO 14443)	FIDO 및 PKI	FIDO 및 PKI	FIDO 및 물리적 액세스	FIDO 및 물리적 액세스	FIDO 및 물리적 액세스
메모리					
메모리 칩	400 KB Java Flash	400 KB Java Flash	586 KB User ROM	접촉 칩: 400KB Java Flash 비접촉식 칩: 586KB User ROM	접촉 칩: 400KB Java Flash 비접촉식 칩: 586KB User ROM
무료 메모리 이용 가능 레지던트키(RK), 인증서 및 추가 애플릿과 데이터용	73 KB	55 KB	88.3~ 98.3 KB	접촉식:73 KB 비접촉식: 88.3 ~ 98.3KB	접촉식:73 KB 비접촉식: 88.3 ~ 98.3KB
키 용량					
FIDO 레지던트키(RK)	최대 8	최대 8	최대 8	최대 8	최대 8
PKI 키 컨테이너	20	20	해당 없음	20	20
지원되는 표준					
Java Card	3.0.4	3.0.5	3.0.4	3.0.4	접촉 칩: 3.0.5 비접촉 칩: 3.0.4
Global Platform	2.2.1	2.2.1	2.3	접촉 칩: 2.2.1 비접촉 칩: 2.3	접촉 칩: 2.2.1 비접촉 칩: 2.3
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔

Base CSP 미니드라이버 (SafeNet 미니드라이버)	✔	✔	해당 없음	✔	✔
암호화 알고리즘(PKI)					
해시: SHA-1, SHA-256, SHA-384, SHA-512	✔	✔	해당 없음	✔	✔
RSA(최대 RSA 4096비트)	✔	✔	해당 없음	✔	✔
RSA OAEP & RSA PSS	✔	✔	해당 없음	✔	✔
P-256비트 ECDSA, ECDH. P-384비트 및 P-521비트 ECDSA,	✔	✔	해당 없음	✔	✔
ECDH는	✔	✔	해당 없음	✔	✔
맞춤 구성으로 이용 가능	✔	✔	해당 없음	✔	✔
온카드 비대칭 키페어 생성 (RSA 최대 4096비트, 타원 곡선 최대 521비트)	✔	✔	해당 없음	✔	✔
대칭: AES - Microsoft Challenge/Response 전용 보안 메시징 및 3DES용	✔	✔	해당 없음	✔	✔

스마트 카드 - 폼 팩터(계속)

제품 특성	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
인증					
칩: CC EAL6+	✔	✔	✔	✔	✔
NIST 인증 - FIPS 140-2 L2	해당 없음	✔	해당 없음	해당 없음	✔
Java 플랫폼: CC EAL5+/ PP 자바 카드 인증 획득	✔	해당 없음	해당 없음	✔	해당 없음
Java 플랫폼 + PKI 애플릿: CC EAL5+/PP QSCD	✔	해당 없음	해당 없음	✔	해당 없음
eSignature 및 eSeal에 대한 eIDAS 인증 획득	✔	해당 없음	해당 없음	✔	해당 없음
프랑스 ANSSI	✔	해당 없음	해당 없음	✔	해당 없음
물리적 액세스 - Mifare Classic 및 DesFire 구성	해당 없음	해당 없음	✔	✔	✔
기타 PKI 기능					
PIN 정책 자체 포함	✔	✔	해당 없음	✔	✔
다중 PIN 지원	✔	✔	해당 없음	✔	✔
맞춤 디자인 및 브랜딩	✔	✔	해당 없음	✔	✔
인증					
Windows 10 및 기타 FIDO 호환 운영체제에서 FIDO 지원	✔	✔	✔	✔	✔
Windows, macOS X 및 Linux에서 PKI 지원	✔	✔	해당 없음	✔	✔

토큰 - 폼 팩터

제품 특성	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion 공통 기준(CC)
폼 팩터	USB-A	USB-A 또는 USB-C	USB-A 또는 USB-C
메모리			
메모리 칩	400KB Java Flash	400KB Java Flash	400KB Java Flash
무료 메모리 이용 가능(레지던트키(RK), 인증서 및 추가 애플릿과 데이터용)	90KB	55KB	73KB
키 용량			
FIDO 레지던트키(RK)	최대 8	최대 8	최대 8
PKI 키 컨테이너	해당 없음	20	20
지원되는 표준			
Java Card	3.0.4	3.0.4	3.0.4
Global Platform	2.2.1	2.2.1	2.2.1
FIDO 2.0	✔	✔	✔
U2F	✔	✔	✔
Base CSP 미니드라이버 (SafeNet 미니드라이버)	해당 없음	✔	✔
암호화 알고리즘(PKI)			
해시: SHA-1, SHA-256, SHA-384, SHA-512.	해당 없음	✔	✔
RSA(최대 RSA 4096비트)	해당 없음	✔	✔
RSA OAEP & RSA PSS	해당 없음	✔	✔
P-256비트 ECDSA, ECDH. P-384비트 및 P-521비트 ECDSA,	해당 없음	✔	✔
ECDH는	해당 없음	✔	✔
맞춤 구성으로 이용 가능	해당 없음	✔	✔
온카드 비대칭 키페어 생성 (RSA 최대 4096비트, 타원 곡선 최대 521비트)	해당 없음	✔	✔
대칭: AES - Microsoft Challenge/Response 전용 보안 메시징 및 3DES용	해당 없음	✔	✔

제품 특성	 SafeNet eToken FIDO	 SafeNet eToken Fusion USB-A 또는 USB-C	 SafeNet eToken Fusion 공통 기준(CC)
인증			
칩: CC EAL6+	✔	해당 없음	✔
NIST 인증 - FIPS 140-2 L2	해당 없음	해당 없음	해당 없음
Java 플랫폼: CC EAL5+/ PP 자바 카드 인증 획득	✔	해당 없음	✔
Java 플랫폼 + PKI 애플릿: CC EAL5+/PP QSCD	해당 없음	해당 없음	✔
eSignature 및 eSeal에 대한 eIDAS 인증 획득	해당 없음	해당 없음	✔
프랑스 ANSSI	해당 없음	해당 없음	✔
물리적 액세스 - Mifare Classic 및 DesFire 구성	해당 없음	해당 없음	해당 없음
기타 PKI 기능			
PIN 정책 자체 포함	해당 없음	✔	✔
다중 PIN 지원	해당 없음	✔	✔
맞춤 디자인 및	해당 없음	✔	✔
운영체제			
Windows 10 및 기타 FIDO 호환 운영체제에서 FIDO 지원	✔	✔	✔
Windows, macOS X 및 Linux에서 PKI 지원	해당 없음	✔	✔

탈레스 OneWelcome ID 및 액세스 관리 솔루션 소개

업계를 선도하는 탈레스의 인력 및 고객 ID·액세스 관리(Customer Identity & Access Management, CIAM) 솔루션은 기업이 IT 리소스, 웹 및 클라우드 기반 애플리케이션에 대한 액세스를 중앙에서 관리하고 보호할 수 있도록 지원합니다. 기업은 정책 기반 SSO 및 범용 인증 방식을 사용하여 유출을 효과적으로 방지하고 클라우드로 안전하게 마이그레이션하며 규제 준수를 간소화할 수 있습니다.

탈레스 소개

귀하의 데이터를 보호하는 기업들은 탈레스를 통해 자신들의 데이터를 보호합니다. 데이터 보안에 대해 중요한 결정을 내려야 하는 순간이 증가하고 있습니다. 암호화 전략을 수립하거나, 클라우드로 데이터를 이전하거나, 규제 준수 요구사항을 충족시켜야 하는 모든 순간에 탈레스를 믿고 찾아주십시오. 탈레스는 귀하의 안전한 디지털 트랜스포메이션을 지원합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.

연락처 - 모든 사무실 위치 및 연락처 정보는 cpl.thalesgroup.com/contact-us를 참조하시기 바랍니다.