

Yubico får FIPS 140-3-validering för YubiHSM 2 FIPS

YubiHSM 2 FIPS ger ett starkt kryptografiskt skydd för nycklar, känslig information och identiteter för system och tjänster i moderna företagsmiljöer och industriella IT-miljöer.

[Yubico](#), ledande inom nätfiskeresistent autentisering och skaparen av YubiKey, meddelar idag att [YubiHSM 2 FIPS](#) har uppnått FIPS 140-3-validering med [certifikat nummer 5302](#), publicerat av National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP). Tillsammans med den tidigare FIPS 140-3-valideringen av [YubiKey 5 FIPS-serien](#) stärker detta Yubicos position som leverantör av modern, hårdvarubaserad säkerhet för organisationer som skyddar kritisk infrastruktur, tillverkningsystem, offentlig sektor och andra verksamheter med höga säkerhetskrav.

I takt med att cyberattacker i allt högre grad riktas mot kryptografiska nycklar, digitala identiteter och leverantörskedjor för mjukvara behöver organisationer starkare hårdvarubaserat skydd för känsliga system och verksamheter. YubiHSM 2 FIPS är särskilt utvecklad för att skydda kryptografiska nycklar och utföra säkra kryptografiska operationer i en fysisk, manipuleringssäker hårdvarumodul, en så kallad Hardware Security Module, HSM. Det hjälper organisationer att minska risken för att nycklar exponeras, att inloggningsuppgifter komprometteras och att obehöriga får åtkomst.

”AI-drivna cyberhot påskyndar attacker mot mjukvara, identiteter och kryptografisk infrastruktur”, säger Albert Biketi, produkt- och teknikchef på Yubico. ”YubiHSM 2 FIPS ger en hårdvarubaserad säkerhetsgrund för organisationer som behöver skydda känsliga system, tillverkningsmiljöer, industriell teknik och kritisk infrastruktur. FIPS 140-3-valideringen stärker Yubicos åtagande att leverera modernt kryptografiskt skydd för organisationer som möter en snabbt föränderlig hotbild.”

I takt med att amerikanska myndigheter och företag i reglerade branscher inför Zero Trust i snabbare takt stärker FIPS 140-3-valideringen av Yubicos kryptografiska YubiHSM 2-modul, enligt [NIST CMVP-certifikat nummer 5302](#), en viktig hårdvarubaserad grund för modern identitetssäkerhet, dataskydd och AI-säkerhet. NIST SP 800-207 beskriver Zero Trust som en säkerhetsmodell där åtkomst prövas löpande och med minsta möjliga behörighet, även i miljöer där nätverket inte kan betraktas som betrott. [CISA Zero Trust Maturity Model](#) och [NSA vägledningar för implementering av Zero Trust](#) omsätter dessa principer i praktisk vägledning för hur organisationer stegvis kan stärka säkerheten inom identitetshantering, enheter, applikationer och tjänster, data, automatisering och analys.

Anthropics senaste rapport om [Zero Trust för AI-agenter](#) utvidgar samma modell till AI-agenter, med fokus på kryptografiskt skyddade identiteter, tydligt avgränsade behörigheter för olika uppgifter och säkerhetsarkitekturer som är byggda för att stå emot och hantera intrång. YubiHSM hjälper organisationer att skydda kryptografiska nycklar, certifikat och inloggningsuppgifter, samtidigt som lösningen stödjer kontinuerlig verifiering, minsta möjliga åtkomst och kryptografiskt grundad tillit för verksamhetskritiska system och nya arbetsflöden med AI-agenter.

Den FIPS 140-3-validerade YubiHSM 2 FIPS-modulen uppfyller säkerhetskraven för Overall Level 3 och erbjuder avancerat fysiskt skydd för kryptografiska nycklar och andra känsliga säkerhetsfunktioner. Valideringen följer det senaste kryptografiska ramverket FIPS 140-3 och den internationella standarden ISO/IEC 19790, vilket hjälper organisationer att leva upp till globala krav på säkerhet och regelefterlevnad.

För mer information om YubiHSM 2 FIPS och FIPS 140-3-validering, besök:
<https://www.yubico.com/products/hardware-security-module/>

För mer information kontakta:

Karin Muskopf
Global Communications
press@yubico.com

Om Yubico

Yubico (Nasdaq Stockholm: YUBICO), som utvecklat YubiKey, erbjuder högsta möjliga skydd för att stoppa så kallade nätfiskeattacker, på engelska kallat phishing-resistant multi-factor authentication (MFA), vilket gör inloggning enkel, säker och tillgänglig för alla. Sedan företaget grundades 2007 har det varit ledande när det gäller att sätta globala standarder för säker åtkomst till datorer, mobila enheter, servrar, webbläsare och internetkonton. Yubico är grundare och huvudsaklig bidragare till de öppna autentiseringsstandarderna FIDO2, WebAuthn och FIDO Universal 2nd Factor (U2F) och är en pionjär när det gäller att leverera hårdvarubaserad nyckel-autentisering i stor skala till kunder i över 175 länder.

Yubicos teknologi möjliggör inloggning utan lösenord tack vare den mest säkra formen av nyckelteknologi. YubiKeys fungerar direkt i över tusen konsument- och företagsapplikationer och tjänster och levererar hög säkerhet med en snabb och enkel upplevelse.

Som en del av missionen att göra internet säkrare för alla donerar Yubico YubiKeys till organisationer som hjälper högriskpersoner genom det filantropiska initiativet Secure it Forward. Företaget har sitt huvudkontor i Stockholm, Santa Clara och Singapore. För mer information om Yubico, besök oss på www.yubico.com.

Bifogade filer

[Yubico får FIPS 140-3-validering för YubiHSM 2 FIPS](#)