HASSAS VERİLERİNİZ İÇİN ÜST DÜZEY KORUMA

HIGH LEVEL PROTECTION TO SECURE YOUR DATA

DIRAK Mini NHSM

AĞ TİPİ DONANIM GÜVENLİK MODÜLÜ

DIRAK MINI NHSM

DIRAK NETWORK HARDWARE SECURITY MODULE

TÜBİTAK

BİLGEM

DIRAK MİNİ NETWORK HSM

AĞ TİPİ DONANIM GÜVENLİK MODÜLÜ

BİLGEM DIRAK NHSM-M; şifreleme, imzalama, imza doğrulama, özet alma gibi kriptografik işlemleri, bir ağ üzerinden yüksek performansla ve güvenli olarak gerçekleştirmek üzere geliştirilmiş bir cihazdır.

BİLGEM DIRAK Network HSM; şifreleme, imzalama, imza doğrulama, özet alma gibi kriptografik işlemleri, bir ağ üzerinden yüksek performansla ve güvenli olarak gerçekleştirmek üzere geliştirilmiş bir cihazdır. Cihaz ile istemci arasındaki haberleşme, karşılıklı doğrulama ile kurulan güvenli kanallar üzerinden yürütülmektedir.

İşlemlerde kullanılan anahtarların fiziksel saldırı korumalı kriptografik sınır içerisinde saklanması neticesinde, bu hassas varlıklar için yüksek güvenlik sağlanır. İlklendirme, yedekleme, yazılım güncelleme, kullanıcı doğrulaması gibi kritik güvenlik işlemleri milli akıllı kart işletim sistemi AKİS tabanlı yetki ve kimlik doğrulamasından sonra gerçekleştirilmektedir. Cihaz bünyesinde barındırdığı milli rastgele sayı üreteci ile de anahtar üretimine milli bir çözüm sunmaktadır.

TEKNİK ÖZELLİKLER

Uygulama Programlama Arayüzleri (APIs)	• PKCS#11 v2.20 • MA3 API
Yönetim	• Uzaktan cihaz yönetimi • Uzaktan yönetim için kullanımı kolay bir GUI ve komut satırı yönetim programı • Cihaz üzerinden yönetim için 3.9 inch dokunmatik ekran • Kritik işlemlerde M-of-N yönetici doğrulaması • Güvenli yazılım güncelleme • Güvenli yedek alma ve yedek yükleme • Parçalı anahtar yükleme • İşlem kayıtlarını tutma • 256 adete kadar PKCS#11 slotu • PKCS#11 slotlarına kullanıcı atama sınırlandırması • PKCS#11 slotlarına akıllı kartlı doğrulama ile erişim • SNMP üzerinden cihaz izlenebilirliği sağlama • Yaygın kullanılan cihaz izleme araçları ile kolay entegrasyon • TLS üzerinden güvenli bağlantı • Aktif-Aktif ve Aktif-Pasif olarak yedekli ve ölçeklenebilir çalışma
Kriptografik Özellikler	• RSA, ECDSA, DSA, edDSA ECDH • AES, TripleDES, DES • SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD160 • SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC • AES CMAC • RSA, ECDSA, DSA, ECDH asimetrik anahtar üretimi, AES, DES, TripleDES simetrik anahtar üretimi • Secp tanımlı eğriler, özel prime eğriler ve gizli eğriler ile işlem yapabilme • Milenage (5G) • BIP32 ve SLIP-10 (Blokzincir) • XMSS (Kuantum-güvenli algoritma) • Milli rastgele sayı üreteci

Güvenlik	• CC EAL4+ sertifikası • ISO 19790 Level-3 (FIPS 140-2 muadili) • Tamper korumalı sert metal kapak • Çevresel koşullara göre tamper koruması
Uygulama Destekleri	• Kod imzalama desteği • OpenSSL uyumluluğu • OpenVPN uyumluluğu • 5G Güvenlik • Blokzincir Uygulamaları • E-İmza • E-Fatura • E-Mühür • SSL/TLS • PKI uygulamaları (Sertifika imzalama-doğrulama, Anahtar oluşturma-saklama)
Performans	• RSA 2048-bit imzalama 400 op/saniye • RSA 4096-bit imzalama 85 op/saniye • ECDSA 256-bit prime imzalama 1000 op/saniye • AES 256-bit işlem 1400 op/saniye
Aktif Yedeklilik	• Dual hot-swap güç kaynağı • 2 adet ethernet portu
Genel Özellikler	• Boyut: 1U • Gigabit ethernet • 1 Adet USB girişi (Güncelleme ve yedek alma için) • 1 Adet Kart okuyucu girişi • Acil Silme butonu
Desteklenen İşletim Sistemleri	• Linux • Windows
Müşteri Destek	• hsmdestek@tubitak.gov.tr

DIRAK MINI NETWORK HSM

NETWORK HARDWARE SECURITY MODULE

BİLGEM DIRAK NHSM-M is primarily developed to perform critical cryptographic operations such as signing, verification, encryption etc. over a network in a secure and fast way.

The communication between the device and the client takes place on a secure channel which is established after mutual authentication. Network HSM protects the keys that are involved in the cryptographic operations from physical and cyber attacks and provides high security for the critical assets. The national smartcard operating system AKIS is used for operator and role authentication during critical processes such as initialization, backup, firmware update, user authentication etc. The module also provides a national solution to key generation problem, with a national random number generator.

TECHNICAL SPECIFICATIONS

Application Programming Interfaces (APIs)	• PKCS#11 v2.20 • MA3 API
Management	• Remote device management • GUI and command prompt management applications • 3.9-inch LCD touch panel for local management • M-of-N administrator authentication in critical functions • Audit logging • Up to 256 PKCS#11 slots • User assignment restriction to PKCS#11 slots • Smartcard authentication to access PKCS#11 slots • Backup and restore functionality • Firmware update • Providing device monitoring via SNMP • Easy integration with common device monitoring tools • Secure connection over TLS • Redundant and scalable operation as Active-Active and Active-Passive
Cryptographic Specifications	• RSA, ECDSA, DSA, EdDSA, ECDH • AES, TripleDES, DES • Milenage • SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD160 • SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC • AES CMAC • RSA, ECDSA, DSA, ECDH asymmetric key generation, AES, DES, TripleDES symmetric key generation • Operation capability with secp prime, custom curves and secret curves • Milenage (5G) • BIP32 and SLIP-10 (Blockchain) • XMSS (Quantum-secure algorithm) • National random number generator

Security	• CC EAL4+ certificate • ISO 19790 Level-3 (equivalent of FIPS 140-2) • Tamper resistant hard metal cover • Tamper protection according to environmental conditions
Supported Applications	• Code Signing • OpenSSL support • OpenVPN support • 5G Security • Blockchain Applications • E-Signature • E- Invoice • E- Seal • SSL/TLS • PKI Applications (Certificate sign-verify, Key generation-storage)
Performance	• RSA 2048-bit sign 400 ops/sec • RSA 4096-bit sign 85 ops/sec • ECDSA 256-bit prime sign 1000 ops/sec • AES 256-bit operation 1400 op/sec
Active Backup	• Dual hot-swap power supplies • 2 Ethernet ports
Physical Interface	• Size: 1U • 1 Gbit/s Ethernet • 1 USB Port (for Update and Backup Process) • 1 Smart Card Port • Emergency Erase Button
Supported Operating Systems	• Linux • Windows
Customer Support	• hsmdestek@tubitak.gov.tr

BİLGEM
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

T: +90 262 648 1000 • F: +90 262 648 1100 • E: bilgem@tubitak.gov.tr
W: bilgem.tubitak.gov.tr • A: PK.: 74, 41470, Gebze, Kocaeli TÜRKİYE