DIRAK Network HSM
Ağ Tipi Donanım Güvenlik Modülü

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 AKİS tabanlı yetki ve kimlik doğrulamasından sonra gerçekleştirilmektedir. Cihaz bünyesinde barındırdığı milli rastgele sayı üreteci ile de anahtar üretimine milli bir çözüm sunmaktadır.

TÜBİTAK BİLGEM UEKAE
T: 0262 648 1000 • F: 0262 648 1100 • E: bilgem@tubitak.gov.tr
W: www.bilgem.tubitak.gov.tr • A: PK.: 74, 41470, Gebze, Kocaeli

TÜBİTAK
BİLGEM

DIRAK Network HSM
DIRAK Ağ Tipi Donanım Güvenlik Modülü

TEKNİK ÖZELLİKLER

Kriptografik Özellikler

- RSA, ECDSA, DSA, ECDH
- AES, TripleDES, DE
- 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
- 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
- Milli rastgele sayı üreteci

Güvenlik

- CC EAL4+ sertifikası
- Tamper korumalı sert metal kapak

Uygulama Programlama Arayüzleri (APIs)

- PKCS#11 v2.20

Uygulama Destekleri

- Kod imzalama desteği
- OpenSSL uyumluluğu
- OpenVPN uyumluluğu

Yönetim

- Uzaktan cihaz yönetimi
- Uzaktan yönetim için GUI ve komut satırı yönetim programı
- Cihaz üzerinden yönetim için 3.9 inch dokunmatik ekran
- Kritik işlemlerde M-of-N yönetici doğrulaması
- İşlem kayıtlarını tutma
- 256 adede kadar PKCS#11 slotu
- PKCS#11 slotlarına kullanıcı atama sınırlandırması
- PKCS#11 slotlarına akıllı kartlı doğrulama ile erişim
- Yedek alma ve yedekten yükleme
- Parçalı anahtar yükleme
- Yazılım güncelleme

Performans

- RSA 2048-bit imzalama 3300 op/saniye
- RSA 4096-bit imzalama 675 op/saniye
- ECDSA 256-bit prime imzalama 5600 op/saniye

Yedeklilik

- Dual hot-swap güç kaynağı
- Aktif-Aktif yük dağıtımı
- 2 Adet Ethernet portu

Genel Özellikler

- Boyut 1U – 482mm x 416mm x 44mm
- 1 Gbit/s Ethernet
- 1 Adet USB girişi (Güncelleme ve yedek alma için)
- 1 Adet Akıllı Kart girişi
- Acil Silme butonu

Desteklenen İşletim Sistemleri

- Linux
- Windows

Müşteri Destek

hsmdestek@tubitak.gov.tr