TÜBİTAK BİLGEM
BİLİŞİM VE BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ

DIRAK

Mini Network HSM

(DIRAK NHSM-M)

AĞ TİPİ DONANIM GÜVENLİK 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.

DIRAK Mini Network HSM (DIRAK NHSM-M)

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
Kriptografik Özellikler
RSA, ECDSA, DSA, 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
RSA, ECDSA, DSA, ECDH asimetirk 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
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 adete kadar PKCS#11 slotu
PKCS#11 slotlarına kullanıcı atama sınırlandırması
Performans
RSA 2048-bit imzalama 300 op/saniye
RSA 4096-bit imzalama 60 op/saniye
ECDSA 256-bit prime imzalama 500 op/saniye
Aktif Yedeklilik
Aktif Yedeklilik
RSA 4096-bit imzalama 60 op/saniye
Genel Özellikler
Gigabit ethernet
1 Adet USB girişi (Güncelleme ve yedek alma için)
1 Adet Kart okuyucu girişi
Acil Silme butonu
Desteklenen İşletim Sistemleri
Linux
Windows