

nCipher netHSM termékismertető

Bárhonnan elérhető és mégis biztonságos security modul

A vállalaton belül található érzékeny információ mennyisége folyamatosan nő (ügyféladatok, pénzügyi eredmények, kimutatások, kutatások, stb.). Ma már ugyan sok ügyfél használ külön védelmet, esetleg titkosítást ezen információk védelmére, azonban maga a titkosító kulcs is ugyanolyan (sőt sokkal jobban) védendő adat, mint a fent felsoroltak. Ezért is kiemelten fontos ezen kulcsok megfelelő kezelése, tárolása, megújítása.



Az elérhető előnyök

- Hardveres kulcsmenedzsment megoldás
- Teljeskörűen ellenőrizhető a kritikus információkhoz történő hozzáférés
- Központosított menedzsment, hálózati elérés
- Üzleti folyamatok védelme (akár titkosítás, akár digitális aláírás esetén használható megoldás)
- Megbízható, tanúsítványokkal elismert (FIPS validated security) megoldás
- Skálázható, titkosított termékek, melyek a hálózaton keresztül – megfelelő jogosultsággal elérhetőek
- Egyszerű integráció
- Külső gyártók termékeinek támogatása
- Saját fejlesztőkészlet (nCipher CodeSafe)
- Nagy teljesítménye miatt másodpercenként több száz kulcslekérdezésre is lehetőség van
- Failover modul segítségével transzparens és hibaűrítővé tehető a kulcskezelés
- SOA támogatás

A szoftveres megoldások nem nyújtanak megfelelő védelmet

A mai modern adatvédelmi megoldásoknak már nem csak a hálózaton kívüli támadások ellen kell védelmet nyújtania, de a vállalaton belüli támadások ellen is. A belső támadások ellen azonban a pusztán szoftveres megoldások már kevésbé védettek, míg a hardveres megoldások (ahol a védendő kulcs nem is hagyhatja el az eszközt) elegendő biztonságot nyújtanak.

Biztonság a hardveren belül

Az appliance biztonságos, tamper-resistant környezetet biztosít a védendő kulcsok számára.

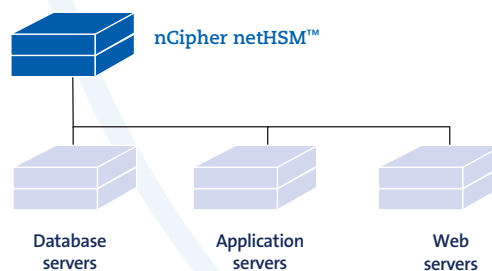
Az nCipher netHSM eszköze támogatja a secure code execution-t (ez esetben a kívánt kód is az eszközön belül fut) és a kulcs tárolást is az eszközön belül, így növelve a biztonságot. A kritikus információk nem hallgathatóak le, nem módosíthatók (ez a titkosítás miatt rögtön kiderülne). Az nCipher netHSM eszköze tehát mind a logikai, mind a fizikai támadások ellen védelmet nyújt.

Szerepkör alapú hozzáférés

A szerepkörök segítségével (melyek tetszőlegesen tesztre is szabhatóak) a kulcsok generálása, letiltása, kezelése, adminisztrálása, lekérdezése is szabályozható.

A védelem tovább növelhető a smart card-ok használatával, melyek kétfaktoros azonosítást követelnek meg az operátoroktól, adminisztrátoroktól.

nCipher CodeSafe



The shared nCipher netHSM module provides scalable, cost-effective encryption services to enterprise servers.

Biztonságos alkalmazások aláírása – az alkalmazások megjelölésével kivédhető a nem támogatott alkalmazások futtatása

End-to-end security – a végpontok között az adatok titkosítva továbbítódnak, a kulcs pedig semmilyen körülmények között nem hagyja el az eszközt

Megfelelőség – a megszerzett minősítések és a törvényi előírásoknak való megfelelés miatt akár bankok, állami hivatalok, védelmi erők számára is elegendő védelmet nyújt

Skálázható megoldás

Standard API-k használatával pillanatok alatt integrálható az nCipher megoldása bármilyen vállalati infrastruktúrába, hiszen támogatott (többek között) többfajta web, alkalmazás szerver, különböző adatbázisok, és PKI rendszerek.

Technikai specifikáció

Két – jelenleg elérhető – verzió:

- o nCipher netHSM 500
- o nCipher netHSM 2000

Mindkettő FIPS 140-2 Level 3 szintű tanúsítvánnyal rendelkezik. Képesek együttműködni Microsoft Windows, Sun Solaris, HP-UX, IBM AIX, és Linux alapú rendszerekkel is.

Bővebb információ: <http://ncipher.com/Products/Hardware%20Security%20Modules/netHSM.aspx>

Portok	2 x 10/100 Ethernet (RJ45)
User interface	Matrix LCD
Támogatott operációs rendszerek (nToken támogatás is)	AIX HP-UX Linux Solaris Windows (Windows Server 2008 támogatás is)
Támogatott szimmetrikus kulcsú algoritmusok	AES ARC4 (kompatibilis RC4-el) DES TripleDES
Támogatott publikus kulcsú algoritmusok	DSA ElGamal RSA ECC (opcionális)
Támogatott kulcscsere algoritmusok	Diffie-Hellman DES/TripleDES XOR
Támogatott hash algoritmusok	MD2 MD5 RIPEMD 160 SHA-2 SHA-1

North America

nCipher, Inc.
1655 McCarthy Blvd
Milpitas, CA 95035 USA
92 Montvale Avenue #4500
Stoneham, MA 02180 USA
Tel: +1 800 nCIPHER

Elérhetőségek

nCipher EMEA régió
Jupiter House
Station Road
Cambridge CB1 2JD
UK
Tel: +44 (0) 1223-723600

Disztributor

DNS Hungária Kft.
HU-1117
Budapest, Gábor Dénes utca 2, II. emelet
Tel: +36 1 371-2-370
www.dns-hungary.hu
ncipher@dns-hungary.hu

www.ncipher.com
info@ncipher.com