TANÚSÍTOTT HSM EGYSÉGEK – CERTIFIED CRYPTOGRAPHIC MODULES

Eszköz neve – Device Name **SafeNet PCIe Hardware Security Module and SafeNet PCIe Hardware Security Module for SafeNet Network HSM** Hardware Versions: VBD-05-0100 [1, 2], VBD-05-0101 [1, 2], VBD-05-0102 [1, 2] and VBD-05-0103 [1, 2] Firmware Versions: 6.24.6 [1] and 6.24.7 [2]
Tanúsított termék – Certified product https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3268
Gyártó - Vendor Thales e-Security Limited (SafeNet Inc.) https://cpl.thalesgroup.com/encryption/hardware-security-modules
Tanúsítási szint – Standard Level FIPS 140-2 Level 3
Tanúsítvány sorszám – Certificate number 3268
Referencia hivatkozás – Reference link **Security Policy:** https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3268.pdf **Consolidated Certificate:** https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/FIPS140ConsolidatedCertAug2018.pdf
Tanúsítás dátuma – Validity date 2018.08.24.
Státusz és Érvényessége – Status and Expiration Historical

Eszköz neve – Device Name **ProtectServer Internal Express 2 (PSI-E2)** Hardware Versions: VBD-05, Version Code 0200 Firmware Versions: 5.03.01 and 5.03.02
Tanúsított termék – Certified product https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3564
Gyártó - Vendor Thales e-Security Limited (SafeNet Inc.) https://cpl.thalesgroup.com/encryption/hardware-security-modules
Tanúsítási szint – Standard Level FIPS 140-2 Level 3
Tanúsítvány sorszám – Certificate Number 3564
Referencia hivatkozás – Reference link **Security Policy:** https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3564.pdf **Consolidated Certificate:** https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/FIPS140ConsolidatedCertNov2019.pdf
Tanúsítás dátuma – Validity date 2019.11.15.
Státusz és Érvényessége – Status and Expiration Historical

Eszköz neve – Device Name **Thales nShield Connect QSCD HSM** **(nShield Connect 500+, 1500+, 6000+ (v11.72.03))** Hardware Versions: nC2023E/nC3423E/nC4033E Firmware Versions: nCore firmware version 2.55.4, nShield Connect firmware image version 12.45.1.
Tanúsított termék – Certified product https://www.ocsi.gov.it/documenti/accertamenti/ncipher/ac_rda_eidas_nshield_2019_v1.0.pdf
Gyártó - Vendor Thales e-Security Limited (nCipher Security Limited) https://cpl.thalesgroup.com/encryption/hardware-security-modules
Tanúsítási szint – Standard Level RQSCD - EAL4+
Tanúsítvány sorszám – Certificate number Attestato di Conformità n. 4/19
Referencia hivatkozás – Reference link **Security Policy:** https://www.ocsi.gov.it/documenti/certificazioni/ncipher/st_ncipher_nshield_v1.1_public.pdf **Certificate:** https://www.ocsi.gov.it/documenti/accertamenti/ncipher/ac_rda_eidas_nshield_2019_v1.0.pdf
Tanúsítás dátuma – Validity date 2019.11.28.
Státusz és Érvényessége – Status and Expiration Visszavonásig érvényes - Valid up to revocation

Eszköz neve – Device Name **CryptoServer Se-Series Gen2** Hadware Versions: CryptoServer Se-Series Gen2 5.01.2.0, CryptoServer Se-Series Gen2 5.01.4.0, and CryptoServer Se-Series Gen2 5.01.4.2 and optional component: crypto accelerator Exar DX8204 Frimware Versions: SecurityServer-Se2-Series-4.32.0.3-FIPS
Tanúsított termék – Certified product https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3925
Gyártó - Vendor Utimaco GmbH. https://utimaco.com/
Tanúsítási szint – Standard Level FIPS 140-2 Level 3
Sorszám – Reference number 3925
Referencia hivatkozás – Reference link **Security Policy:** **https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3925.pdf** **Consolidated certificate:** **https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/May%202021_010621_0658.pdf**
Tanúsítás dátuma – Validity date 2021.05.10.
Státusz és Érvényessége – Status and Expiration 2026.05.09.

Eszköz neve – Device Name **Entrust nShield Connect XC / Solo XC HSM** Firmware version: 12.60.15
Tanúsított termék – Certified product https://www.tuv-nederland.nl/assets/files/cerfiticaten/2021/06/eidas-certificate-21-0368256.pdf
Gyártó – Vendor **Entrust Corp.** https://www.entrust.com/
Tanúsítási szint – Standard Level EAL4 with AVA_VAN.5 and ALC_FLR.2
Tanúsítvány sorszám – Certificate number CC-21-0368256-eIDAS
Referencia hivatkozás – Reference link **Entrust Security certification reference document:** https://www.entrust.com/sites/default/files/documentation/licensingandagreements/entrust-security-product-certification-reference-document.pdf **Certificate:** https://www.tuv-nederland.nl/assets/files/cerfiticaten/2021/06/eidas-certificate-21-0368256.pdf **Certification report:** https://www.tuv-nederland.nl/assets/files/cerfiticaten/2021/06/nscib-cc-0368256-cr-1.0.pdf **Security target:** https://www.tuv-nederland.nl/assets/files/cerfiticaten/2021/07/nscib-cc-0368256_1m1-st.pdf **Assurance continuity maintenance report:** https://www.tuv-nederland.nl/assets/files/cerfiticaten/2021/07/nscib-cc-0368256_1m1-ma-1.0.pdf
Tanúsítás dátuma – Validity date 2021.06.10.
Státusz és Érvényessége – Status and Expiration 2026.06.10.

Eszköz neve – Device Name **Thales ProtectServer 3 – PL25** Firmware version: 7.01.01 Hardware version: 8085-000048-00
Tanúsított termék – Certified product https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4110
Gyártó – Vendor **Thales** https://cpl.thalesgroup.com/resources/encryption/protectserver-3-pcie-hsm-product-brief
Tanúsítási szint – Standard Level FIPS 140-2 Level 3
Tanúsítvány sorszám – Certificate number 4110
Referencia hivatkozás – Reference link **Certificate:** https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/December%202021_020122_0905_signed.pdf **Security policy:** https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp4110.pdf
Tanúsítás dátuma – Validity date 2021.12.02.
Státusz és Érvényessége – Status and Expiration 2026.09.21.