

CERTIFIED CRYPTOGRAPHIC MODULES - TANÚSÍTOTT HSM EGYSÉGEK

Eszköz neve és verziói Module name and versions	Tanúsított termék Certified product	Gyártó Vendor	Tanúsítási szint Standard overall level	Sorszám Reference	Referencia hivatkozás Related files URL	Tanúsítás dátuma Validation date	Státusz Status
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]	https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3268	SafeNet, Inc. https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/	FIPS Level3	3268	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/FIPSI40ConsolidatedCertAug2018.pdf	8/24/2018	Historical
ProtectServer Internal Express 2 (PSI-E2) Hardware Versions: VBD-05, Version Code 0200 Firmware Versions: 5.03.01 and 5.03.02	https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3564	SafeNet, Inc. https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/	FIPS Level3	3564	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/JulyConsolidatedCert.pdf	11/15/2019	Historical
Thales nShield Connect QSCD HSM (Thales nShield HSM Family v11.72.02 - nShield Connect 500, 500+, 1500, 1500+, 6000, 6000+) Hardware Versions: Hardserver version 2.92.1 Firmware Versions: nCore firmware version 2.55.1, nShield Connect firmware image version 0.9.9	https://www.commoncriteriaportal.org/files/efiles/rc_thales_nshield_v1.0.pdf	Thales e-Security Limited, https://www.thalesecurity.com/products/general-purpose-hsms/nshield-connect	RQSCD	1/16	Certification report: https://www.ocsi.gov.it/documenti/accertamenti/thales/ac_rda_nshield_v1.0.pdf Security target: https://www.ocsi.gov.it/documenti/certificazioni/thales/st_thales_nshield_v1.0_public.pdf	10/03/2016	Valid up to revocation
ATOS Bullsequana Edge védett környezetbe implementált AyaSAM v1.1 szoftver komponens és Thales nShield HSM Family v11.72.03 nShield Connect 6000+ nCore firmware version 2.55.4 kriptográfiai modul Firmware Version: nCore firmware version 2.55.4	https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD	MATRIX Kft. https://matrix-tanusito.hu/tanusitvanyok-2/	RQSCD	E-DSOL21T_TAN-QSCD_v2	Certification: https://matrix-tanusito.hu/wp-content/uploads/2022/06/E-DSOL21T_TAN-QSCD_v2_signed.pdf Certification annex: https://matrix-tanusito.hu/wp-content/uploads/2022/06/E-DSOL21T_TAN-QSCD_v2.ME-01_signed.pdf	11/05/2022	10/05/2025
CryptoServer Se-Series Gen2 Hardware 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 Firmware Versions: SecurityServer-Se2-Series-4.32.0.3-FIPS	https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3925	Utimaco GmbH. https://utimaco.com/products/categories/general-purpose-solutions/securityserver	FIPS Level3	3925	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	10/05/2021	05/09/2026