

## TANÚSÍTOTT HSM EGYSÉGEK – CERTIFIED CRYPTOGRAPHIC MODULES

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

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

<p><b>Eszköz neve – Device Name</b></p> <p><b>Thales nShield Connect QSCD HSM</b> <b>(nShield Connect 500+, 1500+, 6000+ (v11.72.03))</b></p> <p>Hardware Versions: nC2023E/nC3423E/nC4033E Firmware Versions: nCore firmware version 2.55.4, nShield Connect firmware image version 12.45.1.</p>
<p><b>Tanúsított termék – Certified product</b></p> <p><a href="https://www.ocsi.gov.it/documenti/accertamenti/ncipher/ac_rda_eidas_nshield_2019_v1.0.pdf">https://www.ocsi.gov.it/documenti/accertamenti/ncipher/ac_rda_eidas_nshield_2019_v1.0.pdf</a></p>
<p><b>Gyártó - Vendor</b></p> <p>Thales e-Security Limited (nCipher Security Limited)</p> <p><a href="https://cpl.thalesgroup.com/encryption/hardware-security-modules">https://cpl.thalesgroup.com/encryption/hardware-security-modules</a></p>
<p><b>Tanúsítási szint – Standard Level</b></p> <p>RQSCD - EAL4+</p>
<p><b>Tanúsítvány sorszám – Certificate number</b></p> <p>Attestato di Conformità n. 8/19.</p>
<p><b>Referencia hivatkozás – Reference link</b></p> <p><a href="https://www.acn.gov.it/portale/en/ocsi/elenco-qscd">https://www.acn.gov.it/portale/en/ocsi/elenco-qscd</a></p> <p><b>Security Policy:</b></p> <p><a href="https://www.acn.gov.it/portale/documents/20119/914698/st_ncipher_nshield_v1.1_public.pdf/421d1d1f-45b0-15f8-073a-cca51b39c9ec?t=1749546055060">https://www.acn.gov.it/portale/documents/20119/914698/st_ncipher_nshield_v1.1_public.pdf/421d1d1f-45b0-15f8-073a-cca51b39c9ec?t=1749546055060</a></p> <p><b>Certificate:</b></p> <p><a href="https://www.acn.gov.it/portale/documents/20119/914698/rc_ncipher_nshield_v1.0.pdf/0a43da48-e80f-771e-799e-fee6355657fc?t=1749546055059">https://www.acn.gov.it/portale/documents/20119/914698/rc_ncipher_nshield_v1.0.pdf/0a43da48-e80f-771e-799e-fee6355657fc?t=1749546055059</a></p>
<p><b>Tanúsítás dátuma – Validity date</b></p> <p>2019.11.28.</p>
<p><b>Státusz és Érvényessége – Status and Expiration</b></p> <p>Visszavonásig érvényes - Valid up to revocation</p>

<b>Eszköz neve – Device Name</b> <b>CryptoServer Se-Series Gen2</b> 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
<b>Tanúsított termék – Certified product</b> <a href="https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3925">https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3925</a>
<b>Gyártó - Vendor</b> Utimaco GmbH. <a href="https://utimaco.com/">https://utimaco.com/</a>
<b>Tanúsítási szint – Standard Level</b> FIPS 140-2 Level 3
<b>Sorszám – Reference number</b> 3925
<b>Referencia hivatkozás – Reference link</b> <b>Security Policy:</b> <a href="https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3925.pdf">https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3925.pdf</a> <b>Consolidated certificate:</b> <a href="https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/May%202021_010621_0658.pdf">https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/May%202021_010621_0658.pdf</a>
<b>Tanúsítás dátuma – Validity date</b> 2021.05.10.
<b>Státusz és Érvényessége – Status and Expiration</b> 2026.05.09.

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

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

<b>Eszköz neve – Device Name</b> <b>Entrust nShield 5s PCIe HSM</b> <b>Entrust nShield 5c (High) HSM</b> Firmware version: 13.5.1. Hardware version: NH2096-H-CC
<b>Tanúsított termék – Certified product</b> <a href="https://www.entrust.com/sites/default/files/documentation/licensingandagreements/entrust-security-product-certification-reference-document.pdf">https://www.entrust.com/sites/default/files/documentation/licensingandagreements/entrust-security-product-certification-reference-document.pdf</a> <a href="https://trustcb.com/download/?wpdmdl=4019">https://trustcb.com/download/?wpdmdl=4019</a>
<b>Gyártó – Vendor</b> <b>Thales</b> <a href="https://www.entrust.com/products/hsm/nshield-5c">https://www.entrust.com/products/hsm/nshield-5c</a>
<b>Tanúsítási szint – Standard Level</b> EAL4 augmented with ALC_FLR.2 and AVA_VAN.5
<b>Tanúsítvány sorszám – Certificate number</b> NSCIB-CC-2200057-01
<b>Referencia hivatkozás – Reference link</b> <b>Certificate:</b> <a href="https://trustcb.com/download/?wpdmdl=4019">https://trustcb.com/download/?wpdmdl=4019</a> <b>Certification Report:</b> <a href="https://trustcb.com/download/?wpdmdl=4207">https://trustcb.com/download/?wpdmdl=4207</a> <b>Security policy:</b> <a href="https://trustcb.com/download/?wpdmdl=4208">https://trustcb.com/download/?wpdmdl=4208</a>
<b>Tanúsítás dátuma – Validity date</b> 2024.04.11.
<b>Státusz és Érvényessége – Status and Expiration</b> 2029.04.11.