NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Č: 00052/2018/TS/OCA-005

V Bratislave 11.04.2018

Národný bezpečnostný úrad ako vecne príslušný správny orgán podľa § 10 ods. 1 a 7 a § 11 ods. 1 písm. e) zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) vo veci certifikácie zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate Disig KeyPoint QSCD 1 na základe žiadosti žiadateľa ***Disig, a.s., Záhradnícka 151, 821 08 Bratislava, IČO 35 975 946*** (ďalej len „žiadateľ") posúdil zhodu **zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate Disig KeyPoint QSCD 1** podľa § 10 ods. 1 zákona o dôveryhodných službách a podľa článku 30 ods. 3 písm. b) nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 zo dňa 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie o eIDAS") a v súlade s § 46 a § 47 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov

v y d á v a

C E R T I F I K Á T

zariadenia na vyhotovenie
kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate
Disig KeyPoint QSCD 1

s platnosťou 5 rokov odo dňa nadobudnutia jeho právoplatnosti

pri dodržaní nasledovných obmedzení a podmienok použitia:

Disig KeyPoint QSCD 1 **môže prevádzkovať výlučne kvalifikovaný poskytovateľ dôveryhodných služieb v súlade s nariadením o eIDAS**. Musí byť prevádzkované v chránených priestoroch s príslušnými bezpečnostnými prevádzkovými a režimovými opatreniami (personálne, fyzické a objektové, bezpečnostné, organizačné, prístupové), ktoré sú potrebné k nasadeniu a prevádzke.

Kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý bude prevádzkovať Disig KeyPoint QSCD 1 v rámci svojej kvalifikovanej dôveryhodnej služby spravujúcej aj údaje na vyhotovenie elektronického podpisu alebo elektronickej pečate v mene podpisovateľa alebo vyhotoviteľa pečate musí:

- pred implementáciou zariadenia Disig KeyPoint QSCD 1 vykonať nezávislé posúdenie navrhovaného riešenia v zmysle v zmysle normy prEN 419241 – Bezpečnostné požiadavky pre dôveryhodné systémy podporujúce serverové podpisovanie,
- podpisovateľa alebo vyhotoviteľa pečate pred použitím kľúčového páru identifikovať a autentifikovať prostredníctvom prostriedkov elektronickej identifikácie podľa požiadaviek nariadenia (EÚ) č. 910/2014 a ďalších príslušných predpisov na úroveň zabezpečenia vysoká.

Zariadenie Disig KeyPoint QSCD 1 môže byť použité len s HSMs (Hardware Security Modules), ktoré sú certifikované v zmysle Common Criteria EAL 4+ a nachádzajú sa v zozname kvalifikovaných zariadení pre elektronický podpis resp. pečať v zmysle nariadenia (EÚ) č. 910/2014. Pri používaní zariadenia musia byť dodržané všetky požiadavky, ktoré boli definované pri certifikácii HSM.

Pri používaní Disig KeyPoint QSCD 1 musia byť dodržané požiadavky výrobcu, ktoré sa nachádzajú v dokumentoch:

- „KeyPointSEE 1.0 Bezpečnostné požiadavky na prevádzku verzia 1.1", súbor v elektronickej podobe SR_KeyPointSEE_v1_1.pdf s SHA256 digitálnym odtlačkom DF6FA374A9961B1CB20D204C1B84B0F7095BE34BDBE8B911B603765F9C984469,
- „Disig KeyPoint QSCD Požiadavky na bezpečnú prevádzku verzia 1.0", súbor v elektronickej podobe SR_Disig_KeyPoint_QSCD_1_0.pdf s SHA256 digitálnym odtlačkom A12FAE55B8409B498332FFE187352CCC9B0A20281405C939C1C9CD3B019EA333,
- „Disig KeyPoint Security Target", súbor v elektronickej podobe Disig_KeyPoint_Security_target.pdf s SHA256 digitálnym odtlačkom 5B2EA1DE72EAEF05825493E29EF5BAFB1F035FAB0594DBF6FCFAB85C7A09A0B6.

Súkromná časť kľúčového páru používateľa, ku ktorého verejnej časti je vydaný kvalifikovaný certifikát, musí byť chránená prístupovým PIN kódom známym iba používateľovi. Súkromný kľúč používateľa môže byť použitý na vytvorenie podpisu iba v prípade, ak už autentizovaný používateľ preukáže znalosť správneho používateľského PIN kódu.

Použité algoritmy a parametre musia byť v súlade s nariadením (EÚ) č. 910/2014 a zákona o dôveryhodných službách, najmä s podpisovou politikou podľa § 11 ods. 1 písm. m) zákona o dôveryhodných službách.

Odôvodnenie:

Národnému bezpečnostnému úradu bola dňa 22.09.2017 doručená žiadosť žiadateľa o certifikáciu zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate Disig KeyPoint QSCD 1.

Dňa 28.11.2017 bol žiadateľ vyzvaný na doplnenie dokumentácie v zmysle § 10 ods. 6 zákona o dôveryhodných službách.

Dňa 15.01.2018 bola žiadosť doplnená a vyhodnotená ako úplná a Národný bezpečnostný úrad začal konanie podľa § 10 ods. 7 zákona o dôveryhodných službách.

Na účely certifikácie predložil žiadateľ technickú dokumentáciu a dokument *„Audit Report Statement Disig KeyPoint QSCD verzia 1"*, ktorý vypracoval nezávislý audítor Ing. Marek Žáčik (CISA - Certified Information System Auditor, Certification Number - 13108217, SSCP - System Security Certified Practicioner). Podľa auditu je bezpečnostná úroveň certifikovaného zariadenia EAL 4+ AVA_VAN.5.

Pri certifikácii bol podľa čl. 30 ods. 3 písm. b) nariadenia (EÚ) č. 910/2014 využitý *„Alternatívny postup certifikácie zariadenia na vyhotovenie kvalifikovaného elektronického podpisu alebo zariadenia na vyhotovenie kvalifikovanej elektronickej pečate verzia 1.0"*.

Na základe vyššie uvedeného úrad rozhodol tak, ako je uvedené vo výrokovej časti tohto certifikátu.

Poučenie:

Proti tomuto certifikátu možno podať do 15 dní odo dňa jeho doručenia rozklad Národnému bezpečnostnému úradu, Budatínska 30, 851 06 Bratislava. Včas podaný rozklad má odkladný účinok. Tento certifikát nie je preskúmateľný súdom.

Ing. Jozef Magala
riaditeľ