NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Alternatívny postup certifikácie
zariadenia na vyhotovenie kvalifikovaného elektronického podpisu alebo zariadenia na vyhotovenie kvalifikovanej elektronickej pečate

Verzia 1.0

Národný bezpečnostný úrad | Budatínska 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | fax: +421 2 6869 1700 | podatelna@nbu.gov.sk | www.nbu.gov.sk

Obsah:

1. Revízie

Verzia	Popis	Vytvoril	Platnosť od
1.0	Základná verzia	Kolektív autorov	26.03.2018

2. Predmet dokumentu

Tento dokument upravuje postup pri posudzovaní zhody zariadenia na vyhotovenie kvalifikovaného elektronického podpisu alebo zariadenia na vyhotovenie kvalifikovanej elektronickej pečate (ďalej len „QSCD“) v zmysle § 10 ods. 1 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) v súlade s Nariadením 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 (EÚ) č. 910/2014“) a príslušnými vykonávacími rozhodnutiami pri certifikácii podľa alternatívneho postupu v súlade s článkom 30 ods. 3 písm. b) nariadenia (EÚ) č. 910/2014.

3. Certifikačný orgán

Národný bezpečnostný úrad ako certifikačný orgán v zmysle § 10 ods. 1 zákona o dôveryhodných službách posudzuje zhodu QSCD v súlade s požiadavkami uvedenými v prílohe II k nariadeniu (EÚ) č. 910/2014.

Kým Komisia (EÚ) nevytvorí zoznam noriem na bezpečnostné posúdenie produktov informačných technológií, ktoré sa vzťahujú na certifikáciu QSCD v prípadoch, keď kvalifikovaný poskytovateľ dôveryhodných služieb spravuje údaje na vyhotovenie kvalifikovaného elektronického podpisu alebo údaje na vyhotovenie kvalifikovanej elektronickej pečate v mene podpisovateľa alebo zhotoviteľa pečate, certifikácia takýchto produktov sa musí zakladať na postupe, ktorý podľa článku 30 ods. 3 písm. b) využíva úrovne bezpečnosti porovnateľné s úrovňami, aké sa požadujú v článku 30 ods. 3 písm. a) nariadenia (EÚ) č. 910/2014 a ktorý sa oznamuje Komisii.

Ak Komisia (EÚ) vydá zoznam noriem na bezpečnostné posúdenie produktov informačných technológií, ktoré sa vzťahujú na certifikáciu QSCD v prípadoch, kedy kvalifikovaný poskytovateľ dôveryhodných služieb spravuje údaje na vyhotovenie kvalifikovaného elektronického podpisu alebo údaje na vyhotovenie kvalifikovanej elektronickej pečate v mene podpisovateľa alebo zhotoviteľa pečate, certifikačný orgán bude postupovať v procese posudzovania zhody podľa týchto noriem.

4. Legislatíva, použité normy a štandardy

Zoznam noriem, štandardov a ďalších legislatívnych požiadaviek, ktoré sú zohľadnené pri alternatívnom posudzovaní zhody QSCD:

1 Nariadenie (EÚ) č. 910/2014

2 Vykonávacie rozhodnutie Komisie (EÚ) 2016/650 z 25. apríla 2016, ktorým sa stanovujú normy posudzovania bezpečnosti zariadení na vyhotovenie kvalifikovaného podpisu a pečate podľa článku 30 ods. 3 a článku 39 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (ďalej len „vykonávacieho rozhodnutie Komisie (EÚ) 2016/650“)

3 ISO/IEC 15408 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT (Common Criteria)

4 ISO/IEC 18045 Informačné technológie. Bezpečnostné techniky. Metodika hodnotenia bezpečnosti IT

5 Zákon 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)

6 prEN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

7 prEN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

8 prEN 419221-5 Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services

9 Vykonávacie nariadenie Komisie č. 2015/1502, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

5. Predmet posudzovania zhody

Podľa článku 3 ods. 23 nariadenia (EÚ) č. 910/2014 je zariadenie na vyhotovenie kvalifikovaného elektronického podpisu zariadenie na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II nariadenia (EÚ) č. 910/2014.

Podľa článku 3 ods. 32 nariadenia (EÚ) č. 910/2014 je zariadenie na vyhotovenie kvalifikovanej elektronickej pečate zariadenie na vyhotovenie elektronickej pečate, ktoré primerane spĺňa požiadavky stanovené v prílohe II nariadenia (EÚ) č. 910/2014.

Zariadenie na vzdialené vyhotovenie kvalifikovaného elektronického podpisu alebo vzdialené vyhotovenie kvalifikovanej elektronickej pečate je zariadenie na vyhotovenie kvalifikovaného elektronického podpisu alebo kvalifikovanej pečate podľa nariadenia (EÚ) č. 910/2014, ktoré spravuje výhradne kvalifikovaný poskytovateľ dôveryhodných služieb a je zabezpečená identifikácia a autentifikácia podpisovateľa alebo zhotoviteľa pečate podľa nariadenia (EÚ) č. 910/2014.

6. Požiadavky na QSCD

QSCD je možné začať používať len po posúdení v rámci správy o posúdení zhody kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý bude poskytovať toto QSCD v rámci svojej kvalifikovanej dôveryhodnej služby spravujúcej aj údaje na vyhotovenie elektronického podpisu alebo pečate v mene podpisovateľa alebo vyhotoviteľa pečate, ktorú vydal orgán posudzovania zhody.

6.1. Požiadavky na zariadenia na vyhotovenie kvalifikovaných elektronických podpisov

6.1.1. Požiadavky podľa prílohy II nariadenia (EÚ) č. 910/2014

Podľa článku 29 ods. 1 nariadenia (EÚ) č. 910/2014 musia zariadenia na vyhotovenie kvalifikovaných elektronických podpisov spĺňať požiadavky stanovené v prílohe II nariadenia (EÚ) č. 910/2014:

1. Zariadenia na vyhotovenie kvalifikovaných elektronických podpisov musia vhodnými technickými a procedurálnymi prostriedkami zabezpečovať prinajmenšom, aby:
    a) v primeranej miere bola zaručená dôvernosť údajov na vyhotovenie elektronického podpisu použitých na vyhotovenie elektronického podpisu,
    b) sa údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu mohli v praxi objaviť iba raz,
    c) údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu nebolo možné s primeranou úrovňou zabezpečenia odvodiť a elektronický podpis bol spoľahlivo chránený proti falšovaniu pomocou aktuálne dostupných technológií,
    d) oprávnený podpisovateľ mohol údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu spoľahlivo chrániť pred použitím inými osobami.
2. Zariadenia na vyhotovenie kvalifikovaných elektronických podpisov nesmú meniť údaje, ktoré sa majú podpísať, ani brániť, aby sa takéto údaje podpisovateľovi pred podpísaním zobrazili.
3. Generovať alebo spravovať údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môže výhradne kvalifikovaný poskytovateľ dôveryhodných služieb.
4. Bez toho, aby bol dotknutý bod 1 písm. d), kvalifikovaní poskytovatelia dôveryhodných služieb spravujúci údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môžu údaje na vyhotovenie elektronického podpisu duplikovať len na účely zálohovania za predpokladu, že sú splnené tieto požiadavky:
    a) bezpečnosť duplikovaných súborov údajov musí byť na rovnakej úrovni ako v prípade pôvodných súborov údajov,
    b) počet duplikovaných súborov údajov nesmie prekročiť minimálne množstvo nevyhnutné na zabezpečenie kontinuity služby.

Pre zariadenia na vzdialené vyhotovenie elektronického podpisu sú body 3. a 4. obzvlášť dôležité.

6.1.2. Ďalšie požiadavky

Kvalifikovaný poskytovateľ dôveryhodných služieb spravujúci kľúčový pár osobe musí osobu 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 v zmysle vykonávacie nariadenia Komisie č. 2015/1502.

6.2. Požiadavky na zariadenia na vyhotovenie kvalifikovaných elektronických pečatí

Podľa článku 39 ods. 1 nariadenia (EÚ) č. 910/2014 musia kvalifikované zariadenia na vyhotovenie elektronických pečatí primerane spĺňať požiadavky stanovené v prílohe II.

Zariadenia na vzdialené vyhotovenie elektronického podpisu alebo vzdialené vyhotovenie elektronickej pečate musí spravovať kvalifikovaný poskytovateľ dôveryhodných služieb. Kvalifikovaný poskytovateľ dôveryhodných služieb spravujúci kľúčový pár osobe, musí osobu 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 v zmysle vykonávacie nariadenia Komisie č. 2015/1502.

6.3. Ďalšie požiadavky na QSCD

Technické zariadenia, komponenty a postupy musia byť vyhodnotené v porovnaní s bezpečnostným cieľom a musia spĺňať požiadavky profilu ochrany a bezpečnostného zámeru s minimálnou bezpečnostnou úrovňou EAL 4+ (AVA_VAN.5) v závislosti od implementácie QSCD v rámci služieb poskytovaných kvalifikovaným poskytovateľom dôveryhodných služieb, ktorý spravuje údaje na vyhotovenie elektronického podpisu alebo pečate v mene podpisovateľa alebo zhotoviteľa pečate v súlade s prEN 419221-5 alebo s prEN 419241-2 podľa prEN 419241-1.

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.

Posúdenie musí byť vykonané na základe auditnej správy od nezávislého audítora alebo akreditovaného skúšobného laboratória. Minimálne požiadavky na audítorov a laboratóriá úrad zverejní na svojom webovom sídle.

V prípade vzdialeného vyhotovenia kvalifikovaného elektronického podpisu alebo kvalifikovanej elektronickej pečate môže byť technická implementácia niektorých požiadaviek nahradená technicko-organizačnými opatreniami, ktoré poskytovateľ dôveryhodných služieb musí mať zadefinované v svojej dokumentácii. QSCD môže prevádzkovať výlučne kvalifikovaný poskytovateľ dôveryhodných služieb v súlade s nariadením (EÚ) č. 910/2014. Musí byť prevádzkované v chránených priestoroch s príslušnými bezpečnostnými prevádzkovými a režimovými opatreniami (personálne, fyzické a objektové, bezpečnostné, organizačné, prístupové) a musí spĺňať požiadavky prEN 419241-1 Bezpečnostné požiadavky pre dôveryhodné systémy podporujúce serverové podpisovanie.

7. Podklady k procesu certifikácie

7.1. Predmet certifikácie

Predmet certifikácie je samotný produkt s podporným softvérom, o ktorého certifikáciu žiadateľ žiada.

7.2. Technická dokumentácia

a) Identifikácia produktu
b) Identifikácia výrobcu
c) Popis produktu

d) Popis funkcionality produktu

e) Popis životného cyklu

f) Príručky a manuály (užívateľská, inštalačná príručka, administrátorská príručka, ...)

g) Podmienky prevádzky

h) Bezpečnostný zámer (Security Target) a profil ochrany (Protection Profile)

Profil ochrany a bezpečnostný zámer produktu alebo systému musia byť štruktúrované dokumenty, ktorých štruktúra je určená medzinárodnou normou *ISO/IEC 15408 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT, časti 1 až 3 (Common Criteria).*

Profil ochrany musí byť v súlade s vykonávacím rozhodnutím Komisie (EÚ) 2016/650 alebo v alternatívnom prípade s profilom ochrany uvedeným v kapitole 4 ods. 7 tohto dokumentu.

i) Podporované štandardy, normy a protokoly

j) Zoznam, parametre a vlastnosti kryptografických funkcií

k) Testovacie scenáre a vyhodnotenie testovania nezávislým audítorom

l) Bezpečnostné certifikáty, certifikáty kompatibility (ak existujú)

m) Auditná správa o splnení požiadaviek

Pre potreby certifikácie je potrebné predložiť aj **auditnú správu o splnení požiadaviek profilu ochrany a bezpečnostného zámeru s minimálnou bezpečnostnou úrovňou EAL 4+ (AVA_VAN.5)** od audítora alebo akreditovaného skúšobného laboratória. Náklady spojené s preskúmaním zhody produktu (bezpečnostný audit) hradí žiadateľ.

8. Proces posúdenia zhody

1. Žiadateľom o certifikáciu môže byť právnická alebo fyzická osoba. Žiadosť sa predkladá Národnému bezpečnostnému úradu elektronicky alebo v listinnej podobe na tlačive, ktorého vzor zverejnil Národný bezpečnostný úrad na svojom webovom sídle.

2. Ak žiadosť neobsahuje všetky zákonom požadované náležitosti, Národný bezpečnostný úrad vyzve žiadateľa, aby ju v stanovenom termíne doplnil.

3. Ak žiadosť obsahuje všetky zákonom požadované náležitosti, Národný bezpečnostný úrad vyzve žiadateľa na zaplatenie správneho poplatku.

4. Žiadosť sa považuje za úplnú, ak obsahuje všetky požadované náležitosti a bol zaplatený správny poplatok. Od tejto doby sa začína počítať zákonom stanovená lehota na posúdenie zhody.

5. Ak existujú normy na bezpečnostné posúdenie produktov informačných technológií, ktoré sa vzťahujú na certifikáciu QSCD, Národný bezpečnostný úrad postupuje podľa noriem, ktoré zverejnila Komisia, v zmysle nariadenia (EÚ) č. 910/2014, príslušných vykonávacích rozhodnutí a zákona o dôveryhodných službách.

6. Ak neexistujú normy na bezpečnostné posúdenie produktov informačných technológií, ktoré sa vzťahujú na certifikáciu QSCD, Národný bezpečnostný úrad postupuje podľa tohto alternatívneho postupu, pričom musí byť zabezpečená úroveň bezpečnosti porovnateľná s úrovňami, aké sa požadujú v článku 30 ods. 3 písm. a) nariadenia (EÚ) č. 910/2014, a ktorý sa oznamuje Komisii prostredníctvom verejného alebo súkromného subjektu uvedeného v článku 30 ods. 1 nariadenia (EÚ) č. 910/2014.

7. Ak Národný bezpečnostný úrad uzná zhodu QSCD v súlade s požiadavkami uvedenými v prílohe II k nariadeniu (EÚ) č. 910/2014, vydá certifikát; v opačnom prípade vydá rozhodnutie o nesplnení požiadaviek.
8. Názov certifikovaného produktu (spolu s certifikátom) Národný bezpečnostný úrad uverejní na svojom webovom sídle a oznámi Komisii (EÚ) nové certifikované QSCD.

9. Obsah certifikátu

Certifikát QSCD vydaný Národným bezpečnostným úradom podľa § 10 ods. 1 zákona o dôveryhodných službách v súlade s článkom 30 ods. 3 písm. b) nariadenia (EÚ) č. 910/2014 obsahuje:

a. Identifikácia produktu
b. Identifikácia výrobcu
c. Vyjadrenie o zhode, bezpečnostná úroveň certifikovaného produktu
d. Použitie produktu
e. Podmienky a obmedzenia použitia
f. Identifikácia audítora, laboratória
g. Platnosť certifikátu

10. Záver

Tento alternatívny postup certifikácie QSCD je platný kým Komisia (EÚ) nevydá zoznam noriem na bezpečnostné posúdenie produktov informačných technológií, ktoré sa vzťahujú na certifikáciu QSCD v prípadoch, keď kvalifikovaný poskytovateľ dôveryhodných služieb spravuje údaje na vyhotovenie kvalifikovaného elektronického podpisu alebo údaje na vyhotovenie kvalifikovanej elektronickej pečate v mene podpisovateľa alebo zhotoviteľa pečate.

V Bratislave 26.3.2018

mjr. Ing. Bibiána Magáthová, PhD.

zástupkyňa riaditeľa technickej sekcie