

Metodické usmernenie č. 3/2015

Národná agentúra pre sieťové a elektronické služby

vydáva toto metodické usmernenie ku konaniu o vydanie a inicializáciu kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať na Ústrednom portáli verejnej správy

Dátum zverejnenia: 10. 8. 2015

Verzia dokumentu: 18

Dátum aktualizácie: 26. 2. 2019

Článok I

Účel a rozsah použitia

Účelom tohto metodického usmernenia je poskytnúť orgánom verejnej moci (ďalej len „OVM“) a právnickým osobám (ďalej len „PO“) súhrnné informácie spojené s vydaním kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať a jeho inicializáciu v module centrálnej elektronickej podateľne (ďalej len „CEP“) na účely autorizácie¹ realizovanej prostredníctvom Ústredného portálu verejnej správy (ďalej len „ústredný portál“). Toto metodické usmernenie nie je určené pre tie subjekty, ktoré chcú autorizovať elektronické dokumenty kvalifikovanou elektronickou pečaťou vytváranou prostredníctvom vlastného externého certifikovaného zariadenia (čipová karta, USB kľúč a pod., t. j. nie v HSM module ÚPVS).

Kvalifikovanú elektronickú pečať je možné na ÚPVS vytvárať pomocou kľúčového páru v HSM module ÚPVS nasledovnými spôsobmi:

- integráciou na centrálnu elektronickú podateľňu (CEP),
- na portáli slovensko.sk v konštruktoře správy v elektronickej schránke pomocou tlačidla „Zapečatiť“. Návod na využívanie kvalifikovanej elektronickej pečate v konštruktoře správy je zverejnený na portáli slovensko.sk, v sekcii „[Návody pre inštitúcie](#)“,
- pôvodným spôsobom automatického vytvárania elektronickej pečate až po odoslaní elektronickej správy na základe nastavenia "Podpisovať v mene inštitúcie" v POSP.xml zaregistrovaného elektronickeho formulára. Túto možnosť neodporúčame používať nakoľko v takom prípade orgán verejnej moci nedisponuje zapečatenou verziou rozhodnutia, čo nie je v súlade so zákonom č. 395/2002 Z. z. o archívoch a registratúrach (najmä § 16 a § 16a), a preto ju plánujeme odstrániť v 2. alebo 3. kvartáli 2019.

¹ V zmysle § 23 ods. 3 zákona č. 305/2013 Z. z. o e-Governmente platí, ak osobitný právny predpis neustanovuje povinnosť OVM vykonať autorizáciu konkrétnou osobou v určitej funkcii (napr. starosta obce), a teda sa vyžaduje iba prejav vôle konať v mene OVM (v listinnej podobe je ekvivalentom pečiatka úradu), na autorizáciu sa môže použiť kvalifikovaná elektronická pečať OVM.

Článok II

Vymedzenie pojmov

Na účely tohto metodického usmernenia sa rozumie:

- a) **OVM** – orgán verejnej moci.
- b) **Ústredný portál verejnej správy** - informačný systém verejnej správy, prostredníctvom ktorého je možné centrálné vykonávať elektronickú komunikáciu s ktorýmkoľvek orgánom verejnej moci a pristupovať k spoločným modulom, a to najmä prostredníctvom siete internet podľa zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci (ďalej len „zákon o e-Governmente“).
- c) **Prevádzkovateľ ústredného portálu** – Národná agentúra pre sieťové a elektronické služby (ďalej len „NASES“), príspevková organizácia Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu so sídlom na Kollárovej 8, 917 002 Trnava, IČO: 42 156 424, detašované pracovisko BC OMNIPOLIS, Trnavská cesta 100, 821 01 Bratislava, konajúca prostredníctvom generálneho riaditeľa alebo inej poverenej osoby.
- d) **Kvalifikovaný certifikát pre kvalifikovanú elektronickú pečať** – je certifikát vydaný kvalifikovaným poskytovateľom dôveryhodných služieb orgánu verejnej moci alebo právnickej osobe a spĺňa všetky požiadavky ustanovené v Prílohe III Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES. Prostredníctvom kvalifikovaného certifikátu je možné vytvoriť kvalifikovanú elektronickú pečať určenú na autorizovanie elektronických dokumentov predovšetkým v rámci elektronickej komunikácie s OVM.
- e) **Kvalifikovaná elektronická pečať (KEPe)** – sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov, spĺňa požiadavky stanovené v Nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické

transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES a zároveň je vyhotovená pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronicкую pečať.

- f) **Žiadateľ** - právnická osoba alebo orgán verejnej moci, ktorý žiada o vydanie a inicializáciu kvalifikovaného certifikátu pre kvalifikovanú elektronicкую pečať a v ktorého mene sa v centrálnej elektronickej podateľni k dokumentom pridávajú kvalifikované elektronické pečate.
- g) **Kvalifikovaný poskytovateľ dôveryhodných služieb (poskytovateľ)** – poskytovateľ dôveryhodných služieb, ktorý poskytuje jednu alebo viacero kvalifikovaných dôveryhodných služieb a má udelený kvalifikovaný štatút. Vlastník certifikátu žiada poskytovateľa o vystavenie kvalifikovaného certifikátu pre kvalifikovanú elektronicкую pečať a poskytovateľ tento certifikát vystaví na základe elektronickej žiadosti o vydanie kvalifikovaného certifikátu (CSR, formát .req).
- h) **Integrácia** – prepájanie informačných systémov v správe žiadateľa na ústrednom portáli.
- i) **Dohoda o integračnom zámere** – dohoda uzatvorená medzi prevádzkovateľom ústredného portálu a žiadateľom o integráciu na ústrednom portáli, ktorá vymedzuje požiadavky na prepojenie, popis rol a zodpovedností, harmonogram, zásady komunikácie a jej riadenia a ďalšie nevyhnutné procesy v zmysle platného usmernenia SORO OPIS č. 14/2014 k integrácii informačných systémov verejnej správy.
- j) **HSM server** – certifikované bezpečné zariadenie určené na inicializáciu kvalifikovaného certifikátu pre kvalifikovanú elektronicкую pečať.
- k) **Poverený operátor HSM servera** – vykonáva inicializáciu kvalifikovaného certifikátu pre kvalifikovanú elektronicкую pečať.
- l) **Modul Centrálnej elektronickej podateľne (CEP)** – modul ústredného portálu, ktorý zabezpečuje funkcionality podateľne v zmysle platnej legislatívy: vedie evidenciu prijatých elektronických správ v úradnej komunikácii, overuje platnosť elektronických podpisov na elektronických dokumentoch a vystavuje doručenkú k prijatým podaniam. Okrem uvedeného sprostredkováva službu vyhotovenia kvalifikovanej elektronickej pečate na elektronických dokumentoch.

- m) **CSR (cert. signing request)** - žiadosť o vydanie kvalifikovaného certifikátu v elektronickej forme (formát .req).
- n) **Inicializácia kvalifikovaného certifikátu** - umožnenie pečatenia elektronických podaní alebo elektronických úradných dokumentov použitím kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať, ktorý bol vložený do centrálnej elektronickej podateľne a verejná časť kvalifikovaného certifikátu bola v centrálnej elektronickej podateľni priradená k existujúcej identite žiadateľa.
- o) **Register kvalifikovaných certifikátov** – informačný systém verejnej správy, v ktorom je vedený zoznam platných kvalifikovaných certifikátov pre modul úradnej komunikácie, ktoré boli vydané orgánom verejnej moci, ako aj údaje o tom, že takéto certifikáty boli zrušené. Správcom registra je Národný bezpečnostný úrad SR.

Článok III

Všeobecné ustanovenia

1. Podmienkou na inicializáciu kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať na ústrednom portáli je zriadená elektronická schránka žiadateľa. V prípade právnickej osoby je podmienkou aj integrácia právnickej osoby na ústredný portál.²
2. Žiadateľ je v konaní o vydanie a inicializáciu kvalifikovaného certifikátu zastúpený štatutárnym zástupcom žiadateľa. Štatutár žiadateľa môže na účely konania o vydanie a inicializáciu kvalifikovaného certifikátu a všetkých úkonov s tým spojených splnomocniť alebo poveriť inú osobu. Splnomocnenie musí byť úradne overené. Poverenie nie je potrebné úradne overiť za podmienky, že je vytlačené na hlavičkovom papieri žiadateľa, podpísané štatutárnym zástupcom a opatrené pečiatkou.

² Žiadateľ – právnická osoba, ktorá má záujem o pečatenie elektronických podaní KEPe prostredníctvom ústredného portálu, uvedie túto skutočnosť do požiadaviek vymedzených v Dohode o integračnom zámere. Pre podporu integrácie môže využiť databázu znalostí ústredného portálu (ďalej len „Partner framework portal“, „PFP“). Bližšie informácie o registrácii na PFP sú zverejnené na adrese <https://www.nases.gov.sk/sluzby/usmernenie-k-integracii/index.html> v sekcii určenej integráciám.

3. Žiadateľ si na účely vydania kvalifikovaného certifikátu vyberie kvalifikovaného poskytovateľa dôveryhodných služieb.
4. Podmienky vydávania kvalifikovaného certifikátu sa u jednotlivých kvalifikovaných poskytovateľov dôveryhodných služieb môžu líšiť.

Článok IV

Žiadosť o vydanie a inicializáciu kvalifikovaného certifikátu na ústrednom portáli

1. Žiadateľ môže požiadať o vydanie a inicializáciu kvalifikovaného certifikátu na ústrednom portáli elektronicky prostredníctvom elektronickej služby Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu – ÚPVS s názvom **Vydanie a inicializácia kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať** (ďalej len „služba“) sprístupnenej na ústrednom portáli na adrese <https://schranka1.slovensko.sk/FormConstructor/Default.aspx?IdService=29542>. Služba je dostupná po prihlásení sa na ústredný portál. Elektronický formulár je potrebné pred odoslaním podpísať kvalifikovaným elektronickým podpisom iba vtedy, ak žiadosť podáva splnomocnená osoba. V takomto prípade je potrebné k žiadosti priložiť aj splnomocnenie, resp. poverenie za splnenia podmienok podľa Článku III ods. 2.
2. Prevádzkovateľ ústredného portálu na základe prijatej žiadosti a údajov v nej uvedených, prostredníctvom povereného operátora HSM servera vygeneruje elektronickú žiadosť o vydanie kvalifikovaného certifikátu vo formáte .req (ďalej len „CSR“). Súčasne s CSR je vygenerovaná privátna časť budúceho kvalifikovaného certifikátu, ktorá zostáva uložená v certifikovanom bezpečnom zariadení Úradu podpredsedu vlády SR pre investície a informatizáciu.
3. Vygenerovaná elektronická žiadosť CSR vo formáte .req v súbore .zip je zaslaná žiadateľovi prostredníctvom ústredného portálu do jeho elektronickej schránky.
4. Žiadateľ môže požiadať o doručenie „Záznamu z generovania asymetrického kľúčového páru a elektronickej žiadosti vo formáte PKCS#10 pre kvalifikovaný

certifikát pre kvalifikovanú elektronickú pečať“. Vzor tvorí prílohu č. 1 tohto metodického usmernenia.

Článok V

Vydanie kvalifikovaného certifikátu kvalifikovaným poskytovateľom dôveryhodných služieb

1. Žiadateľ odovzdanú elektronickú žiadosť CSR vo formáte .req následne zasiela vybranému kvalifikovanému poskytovateľovi dôveryhodných služieb, ktorý žiadateľovi kvalifikovaný certifikát vydá. Podmienky na vydanie kvalifikovaných certifikátov sa môžu pri jednotlivých kvalifikovaných poskytovateľoch dôveryhodných služieb navzájom líšiť.
2. Kvalifikovaný poskytovateľ dôveryhodných služieb na základe overenia CSR a zaslaných parametrov vydá kvalifikovaný certifikát pre kvalifikovanú elektronickú pečať vo formáte .cert, ktorého súčasťou je verejná časť. **Odporúčame vám si skontrolovať, či certifikát obsahuje príznak pre kvalifikovanú elektronickú pečať „QcSSCD“/„QcQSCD“.** Viac informácií o uvedení príznaku a spôsoboch jeho kontroly nájdete v „Návode na vydanie a inicializáciu kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať na autorizovanie vlastných rozhodnutí OVM automatizovaným spôsobom na ústrednom portáli“, str. 10 a nasledujúce, ktorý je zverejnený na portáli slovensko.sk, v sekcii „Návody“, v časti „Návody pre inštitúcie“, na adrese https://www.slovensko.sk/img/CMS4/Navody/Nove_ES/navod_KSC.pdf.
3. Žiadateľ zašle prevádzkovateľovi ústredného portálu takto vygenerovaný kvalifikovaný certifikát elektronicky prostredníctvom elektronickej schránky v súbore .zip.

Článok VI

Inicializácia kvalifikovaného certifikátu v module centrálnej elektronickej podateľne (CEP)

1. Prijatý kvalifikovaný certifikát vo formáte .cert je následne prevádzkovateľom ústredného portálu inicializovaný v module CEP tak, že verejná časť kvalifikovaného certifikátu je priradená k existujúcej identite žiadateľa.

2. O úspešnej inicializácii kvalifikovaného certifikátu je vyhotovený „Protokol o inicializácii kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať“, ktorý je doručený žiadateľovi.
3. Vzor protokolu o inicializácii kvalifikovaného certifikátu tvorí prílohu č. 2 tohto metodického usmernenia.

Článok VII

Testovanie a potvrdenie funkcionality pečatenia prostredníctvom KEPe na ústrednom portáli

1. Žiadateľ je povinný vykonať testovanie pečatenia prostredníctvom KEPe a potvrdiť funkčnosť inicializovaného kvalifikovaného certifikátu do štrnástich pracovných dní od jeho inicializácie.
2. Ak žiadateľ v lehote štrnástich pracovných dní nepotvrdí funkčnosť pečatenia prostredníctvom KEPe, považuje sa inicializácia kvalifikovaného certifikátu na tvorbu kvalifikovanej elektronickej pečate za úspešnú.

Článok VIII

Hlásenie nedostatkov a chýb funkčnosti

Zistené nedostatky alebo chyby funkčnosti pečatenia prostredníctvom KEPe hlási žiadateľ prostredníctvom kontaktného formulára Ústrednému kontaktnému centru. Kontaktný formulár je dostupný na adrese <https://www.slovensko.sk/sk/pomoc>.

Článok IX

Záverečné ustanovenia

1. Metodické usmernenie vychádza z informácií a podkladov uvedených v zákone 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 zákone č. 305/2013 Z. z. o e-Governmente a zo zverejnených metodických pokynov na portáli Národného bezpečnostného úradu Slovenskej republiky.

2. Za správnosť dodaných údajov zo strany žiadateľa a poskytovateľa dôveryhodných služieb zodpovedá žiadateľ o vydanie a inicializáciu kvalifikovaného certifikátu.
3. Postup uvedený v článku IV a V je všeobecný. Niektoré procesné, prípadne formálne detaily môžu byť odlišné v závislosti od konkrétneho kvalifikovaného poskytovateľa dôveryhodných služieb.
4. Metodické usmernenie definuje postupnosť krokov pri vydaní a inicializácii jedného kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať – pričom proces uvedený v článkoch III až VI trvá spravidla 3 až 5 pracovných dní.
5. V prípade nečinnosti žiadateľa a nedodaní kvalifikovaného certifikátu vo formáte .cert do troch mesiacov od vygenerovania CSR prevádzkovateľ ústredného portálu konanie o vydanie a inicializáciu kvalifikovaného certifikátu zastaví.
6. Metodické usmernenie nie je aplikovateľné pre testovacie prostredie ústredného portálu.
7. Administrácia a životný cyklus inicializovaného kvalifikovaného certifikátu je v kompetencii žiadateľa.
8. Prevádzkovateľ ústredného portálu nezodpovedá za údaje a iné súčasti procesu vydania kvalifikovaného certifikátu, ako aj za aktivity spojené s prípadnou expiráciou certifikátu.

Článok X **Účinnosť**

Toto metodické usmernenie je účinné odo dňa zverejnenia na ústrednom portáli.

V Bratislave, 25. 2. 2019

Záznam z generovania asymetrického kľúčového páru a elektronickej žiadosti vo formáte PKCS#10 pre kvalifikovaný certifikát pre elektronicnú pečať

Identifikácia prevádzkovateľa informačného systému určeného na vyhotovovanie kvalifikovanej elektronickej pečate:

Dátum a miesto generovania:

Dátum:

Miesto:

Identifikácia zariadenia, v ktorom bol generovaný asymetrický kľúčový pár:

Zariadenie na vyhotovenie kvalifikovanej elektronickej pečate:

ID produktu:

SN:

Popis:

Výrobca:

Údaje o verejnom kľúči:

Použitý asymetrický algoritmus, modulus:

Hash verejného kľúča (SHA1):

Údaje o elektronickej žiadosti vo formáte PKCS#10:

Názov súboru:

Kompletné DN:

Hash PKCS#10 žiadosti (SHA-256):

Výpis PKCS#10 žiadosti v Base64 kódovaní:

Zoznam osôb prítomných pri generovaní asymetrického kľúčového páru (titul, meno, priezvisko, organizácia, funkcia):

Žiadateľ o kvalifikovaný certifikát pre elektronicnú pečať deklaruje, že kryptografické kľúče (verejný a súkromný kľúč), z ktorých verejný sa nachádza v predloženej PKCS#10 žiadosti boli generované v zariadení na vyhotovovanie kvalifikovanej elektronickej pečate, ktoré spĺňa požiadavky zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronicke transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov.

titul, meno, priezvisko, funkcia, podpis
zodpovednej osoby s podpisovou právomocou



ÚRAD PODPRESEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU



Protokol o inicializácii kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať (KSC)

Inštitúcia, pre ktorú bol KSC inicializovaný:

KSC bol úspešne inicializovaný pre používanie na ÚPVS.

Inicializáciu overil

miesto, dátum

meno, priezvisko a podpis

Zoznam zmien:

Dátum zmeny	Verzia	Popis zmien
14.12.2017	13	str. 9: úprava Záznamu z generovania asymetrického kľúčového páru v zmysle zákona o dôveryhodných službách
5.2.2018	14	str. 7: vypustenie Článku IX z dôvodu, že § 60c zákona o e-Governmente stratil účinnosť
21.5.2018	15	str. 1: doplnenie článku I. účel a rozsah použitia
24.9.2018	16	str. 6: Článok V ods. 2 – doplnenie informácie o príznaku QcSSCD“/„QcQSCD
31.12.2018	17	„Úrad vlády SR“ sa v celom texte nahrádza slovami „Úrad podpredsedu vlády SR pre investície a informatizáciu“ str. 11: nový vzhľad protokolu
26.2.2019	18	Str. 2: Článok I – úprava účelu a rozsahu použitia v súvislosti s integráciou na CEP a doplnenie poznámky 1 pod čiarou – kedy je možné v zmysle zákona o e-Governmente vykonať autorizáciu kvalifikovanou elektronickou pečaťou. Str. 7: Článok V ods. 2 – výmena odkazu na nový návod KSC