

Metodické usmernenie pre poskytovateľov akreditovaných certifikačných služieb

V súvislosti so zákonom č. 214/2008 Z.z., ktorým sa mení a dopĺňa zákon č. 215/2002 Z.z. o elektronickej podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „novela zákona o elektronickej podpise“), ktorý nadobudol účinnosť 1.1.2009 upresňujeme niektoré skutočnosti pre akreditované certifikačné autority:

A: Uvedenie rodného čísla v kvalifikovanom certifikáte

V súlade s § 5 ods. 1 zákona o elektronickej podpise, ak sa v styku s orgánmi verejnej moci používa zaručený elektronický podpis, kvalifikovaný certifikát musí byť vydaný akreditovanou certifikačnou autoritou a musí obsahovať rodné číslo držiteľa certifikátu.

Rodné číslo v kvalifikovanom certifikáte musí byť uvedené v položke mena subjektu *Certificate-~~ts~~Certificate-subject-RelativeDistinguishedName-serialNumber* .

Formát odkazu na rodné číslo sa skladá z dvoch častí, ktoré sú oddelené jednou medzerou: znak(20). Znak medzera sa v položke *serialNumber* musí nachádzať iba raz.

Prvá časť z položky *serialNumber* pozostáva z troch úvodných znakov určujúcich typ odkazu na identitu, dvoch znakov krajiny a voliteľných upresňujúcich znakov.

V prípade kvalifikovaných certifikátov, obsahujúcich rodné číslo, tvoria prvú časť z položky *serialNumber* tri úvodné znaky označené „PNO“ pre identifikáciu na základe **rodného čísla prideleného osobe v súlade s §5 ods. 2 a 3 zákona č. 301/1995 Z. z. o rodnom čísle¹⁾**. Nasledujú dva znaky obsahujúce kód krajiny podľa ISO 3166 - "SK".

Druhá časť z položky *serialNumber* pozostáva z rodného čísla, ktoré tvoria číslice v desiatkovej sústave, bez uvedenia lomítka medzi prvou a druhou časťou rodného čísla, teda 10 miest alebo 9 miest (pri rodných číslach pridelených do 31.12.1953) podľa zákona o rodnom čísle 301/1995 z. z. (pr. *serialNumber* = "PNOSK 9959199999" ,*serialNumber* = "PNOSK 530919999").

¹ **Zákon č. 301/1995 Z. z. o rodnom čísle § 5 ods 2 :**

Príslušný matričný úrad pridáva rodné číslo pri zápise narodenia každej osobe, ktorá sa narodila na území Slovenskej republiky.

Zákon č. 301/1995 Z. z. o rodnom čísle § 5 ods 3 :

Ministerstvo pridáva rodné číslo

- a) občanovi Slovenskej republiky narodenému v cudzine, ktorého narodenie je na základe jeho žiadosti zapísané v osobitnej matrike,
- b) osobe narodenej na území Slovenskej republiky, ktorej doteraz nebolo pridelené a ktorá má na území Slovenskej republiky trvalý pobyt,
- c) cudzincovi, ktorému doteraz nebolo pridelené a ktorý má trvalý alebo dlhodobý pobyt na území Slovenskej republiky,
- d) utečencovi, ktorý má pobyt na území Slovenskej republiky, a doteraz ho nemá pridelené,
- e) osobe, ktorá nemá trvalý pobyt na území Slovenskej republiky, ak o jeho pridelenie požiada.

Kvalifikované certifikáty fyzickej osoby, používané v komunikácii s orgánmi verejnej moci v Slovenskej republike, musia v odkaze na identitu fyzickej osoby uvádzať údaj PNO obsahujúci rodné číslo osoby. Rodné číslo musí byť skontrolované a overené pri registračnom procese pri vydaní kvalifikovaného certifikátu².

Ak akreditovaná certifikačná autorita vydáva kvalifikovaný certifikát *cudzincovi, ktorý nemá pridelené rodné číslo* podľa zákona 301/1995 Z. z. o rodnom čísle, je nutné, aby v tejto položke namiesto rodného čísla bolo uvedené číslo pasu alebo číslo „občianskeho preukazu“ cudzinca, pre jednoznačné preukázanie totožnosti podpisovateľa (podrobnosti vid' nižšie).

B: Použitie kvalifikovaného certifikátu v elektronickej komunikácii so zaručeným elektronickým podpisom

V súlade s právnymi predpismi SR môžu akreditované certifikačné autority vydávať dva typy kvalifikovaných certifikátov, odlišené tým, že obsahujú alebo neobsahujú rodné číslo držiteľa certifikátu. Každý z nich však musí obsahovať odkaz na identitu fyzickej osoby držiteľa certifikátu.

Odkaz na identitu fyzickej osoby v kvalifikovanom certifikáte **musí** byť uvedený v položke mena subjektu *Certificate-tnsCertificate-subject-RelativeDistinguishedName-serialNumber* .

Kvalifikovaný certifikát musí obsahovať *minimálne* jednu položku *serialNumber* s odkazom na identitu fyzickej osoby. Položka *serialNumber* s odkazom na identitu fyzickej osoby musí obsahovať len údaj, ktorý bol overený pri registračnom procese pri vydaní kvalifikovaného certifikátu.

Formát odkazu na identitu fyzickej osoby sa skladá z **dvoch častí**, ktoré sú oddelené jednou medzerou: znak(20). Znak medzera sa v položke *serialNumber* musí nachádzať iba raz. V jednej položke *serialNumber* musí byť uvedený iba jeden odkaz na identitu fyzickej osoby.

Prvá časť z položky *serialNumber* pozostáva z troch úvodných znakov určujúcich typ odkazu na identitu, dvoch znakov krajiny a voliteľných upresňujúcich znakov.

Tri úvodné znaky určujú tri typy odkazu na identitu:

1. „PAS“ pre identifikáciu na základe čísla pasu
2. „IDC“ pre identifikáciu na základe čísla identifikačnej karty (pr. občiansky preukaz)
3. „PNO“ pre identifikáciu na základe rodného čísla u občanov SR alebo cudzincov, ktorí majú pridelené rodné číslo podľa zákona o rodnom čísle 301/1995 z. z.

Nasledujú dva znaky obsahujúce kód krajiny podľa ISO 3166 (pre Slovensko "SK"), ktorá údaje uvedené v druhej časti vydala.

² **Zákon č. 301/1995 Z. z. o rodnom čísle § 6 :**

(1) Rodné číslo sa preukazuje niektorým z týchto dokladov:

- a) občianskym preukazom,
- b) cestovným dokladom,
- c) rodným listom,
- d) preukazom povolením na pobyt pre cudzinca, ak je v ňom vyznačené,
- e) osvedčením o rodnom čísle (ďalej len "osvedčenie"), ktorého vzor je v prílohe tohto zákona.

Druhá časť z položky *serialNumber* pozostáva z údajov, ktorých typ určujú prvé tri úvodné znaky.

Pri „PAS“ a „IDC“ sa uvedie séria a číslo identifikačného dokladu

(pr. *serialNumber* = "PASSK P3000180", *serialNumber* = "IDCSK SP989783").

Pri „PNO“ sa použije rodné číslo, bez uvedenia lomítka medzi prvou a druhou časťou rodného čísla, teda 10 miestne alebo 9 miestne.

(pr. *serialNumber* = "PNOSK 9959199999" ,*serialNumber* = "PNOSK 535919999").

Odporúčame akreditovaným poskytovateľom certifikačných služieb pri vydávaní kvalifikovaných certifikátov v súlade s legislatívou SR uvádzať minimálne jeden z vyššie uvedených odkazov na identitu fyzickej osoby aj v prípade, že nebudú použité v komunikácii s orgánmi verejnej moci.

Zaručený elektronický podpis vytvorený a overovaný s použitím kvalifikovaného certifikátu (či obsahuje rodné číslo alebo neobsahuje rodné číslo držiteľa) je zaručený elektronický podpis v súlade s legislatívou SR.

C: Certifikáty na správu kvalifikovaného certifikátu

V súlade so znením § 6 a § 7 novely zákona č. 215/2002 Z.z. o elektronickom podpise **kvalifikovaný certifikát je iba certifikát vydaný fyzickej osobe** (pri splnení ďalších podmienok).

Certifikát úradu (KCA) a certifikát akreditovanej certifikačnej autority (ACA) vydaný úradom nie sú kvalifikované certifikáty, rovnako ako ďalšie certifikáty používané pri poskytovaní akreditovaných certifikačných služieb podľa §2 písm. 1 číslo 1 "správa kvalifikovaných certifikátov" nie sú kvalifikované certifikáty.

Formát a obsah týchto certifikátov je naďalej stanovený štandardom NBÚ „Schválené formáty kvalifikovaných certifikátov“, v prílohe B ktorého sú uvedené príklady, a nazývame ich „certifikáty na správu“.

Podľa RFC 3739 a podľa ETSI TS 101 862 je jednoznačná identifikácia typu kvalifikovaného certifikátu koncového užívateľa pre vytváranie ZEP (Qualified Electronic Signatures) pomocou OID v QCStatements. Kvalifikovaný certifikát musí obsahovať OID identifikátor ***id-etsi-qcs-QcCompliance*** a ak kvalifikovaný certifikát neobsahuje certifikačnú politiku OID QCP SK (1 3 158 36061701 0 0 0 1 2 2), tak musí obsahovať aj *id-etsi-qcs-QcSSCD*.

Uvedené certifikáty na správu teda **nesmú** obsahovať OID identifikátor:

- *esi4-qcStatement-1(id-etsi-qcs-QcCompliance)* označujúci, že certifikát je kvalifikovaný
- *esi4-qcStatement-4(id-etsi-qcs-QcSSCD)* označujúci, že súkromný kľúč, patriaci k verejnemu kľúču uvedenému v kvalifikovanom certifikáte, je uložený v bezpečnom zariadení SSCD (CWA 14169).

Zároveň však tieto certifikáty **musia** obsahovať v rozšírení CertificatePolicies OID certifikačnej politiky QCP SK (1 3 158 36061701 0 0 0 1 2 2), ktorá jednoznačne určuje pri zostavení certifikačnej cesty, že ide o certifikát určený pre správu kvalifikovaných certifikátov – teda o akreditovanú certifikačnú službu.

D: Prechodné obdobie pre používanie produktov pre ZEP

Certifikované produkty pre zaručený elektronický podpis, využívajúce podpisové schémy s asymetrickým šifrovým algoritmom RSA s parametrom MinModLen 1024 bitov alebo nižším a certifikované produkty, využívajúce hašovaciu funkciu SHA1, je možné používať do uplynutia doby platnosti certifikátu produktu, najdlhšie však do 31. decembra 2009.

Certifikáty pre poskytovanie akreditovaných certifikačných služieb, využívajúce hašovaciu funkciu SHA1 a algoritmus RSA s parametrom MinModLen nižším ako 2048 bitov, je možné používať na overovanie do 31. decembra 2010.

Pri poskytovaní akreditovaných certifikačných služieb je možné pre vydávanie zoznamu zrušených certifikátov a potvrdzovanie existencie a platnosti kvalifikovaných certifikátov používať hašovaciu funkciu SHA1 a algoritmus RSA s parametrom MinModLen nižším ako 2048 bitov do 31. decembra 2010.

E: Zasielanie zoznamu vydaných a zrušených kvalifikovaných certifikátov

Podľa §14 ods.3 písm e) je od 1.1.2009 akreditovaná certifikačná autorita povinná zasielať úradu zoznamy vydaných kvalifikovaných certifikátov a zoznamy zrušených kvalifikovaných certifikátov, pričom formát, spôsob a periodicitu zasielania týchto zoznamov ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.

Vzhľadom na viazanie finančných prostriedkov rozpočtu úradu sa dosiaľ nerealizovalo vybudovanie potrebnej technológie. Dokument „Technická špecifikácia...“, ktorý upravuje danú činnosť nie je v súčasnosti relevantný. Vydavateľom kvalifikovaných certifikátov bude zaslané usmernenie ako uvedenú povinnosť reálne vykonať.

F: Informácia o podmienkach použitia rodného čísla v kvalifikovaných certifikátoch pre zaručený elektronický podpis v administratívnom styku

Zákon č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov (ďalej len „zákon“) umožňuje používať v styku s orgánmi verejnej moci „obyčajný“ elektronický podpis aj zaručený elektronický podpis. Pre vytvorenie zaručeného elektronického podpisu je povinné použitie kvalifikovaného certifikátu vydaného akreditovanou certifikačnou autoritou, ktorý musí obsahovať rodné číslo držiteľa, bezpečného zariadenia pre uloženie súkromného kľúča a certifikovanej aplikácie pre vytvorenie a overenie podpisu.

Znenie § 6 zákona definuje certifikát ako elektronické osvedčenie, ktoré potvrdzuje totožnosť osoby podpisovateľa. Kvalifikované certifikáty vydané do 31.12.2008 neobsahovali žiaden identifikačný údaj, ktorý by jednoznačne identifikoval držiteľa certifikátu (podpisovateľa) v styku s orgánmi verejnej moci. Bez jednoznačnej identifikácie podpisovateľa nie je možné v administratívnom styku podpis akceptovať, preto v elektronickej komunikácii niektoré orgány verejnej moci uplatnili doplnkové formy overenia totožnosti držiteľa certifikátu pre identifikáciu podpisovateľa.

V zmysle § 5 ods. 1 zákona v znení účinnom do 31. decembra 2008 sa v styku s orgánmi verejnej moci alebo orgánmi verejnej správy používal elektronický podpis alebo zaručený

elektronický podpis, pričom kvalifikovaný certifikát zaručeného elektronického podpisu musela vydať akreditovaná certifikačná autorita.

V zmysle § 5 ods. 1 zákona v znení účinnom od 1. januára 2009 sa v styku s orgánmi verejnej moci aj naďalej používa elektronický podpis alebo zaručený elektronický podpis, ktorého kvalifikovaný certifikát vydala akreditovaná certifikačná autorita. Avšak od 1. januára 2009 sa vyžaduje, aby kvalifikovaný certifikát zaručeného elektronického podpisu obsahoval aj rodné číslo držiteľa certifikátu.

Vzhľadom na vyššie uvedené ako aj na absenciu právnej úpravy, ktorá by zrušila platnosť a možnosť používania kvalifikovaných certifikátov, ktoré boli vydané podľa právnej úpravy účinnej do 31. decembra 2008 a neobsahovali rodné číslo, konštatujeme, že **kvalifikované certifikáty bez rodného čísla vydané podľa právnych predpisov účinných do 31. decembra 2008 možno v styku s orgánmi verejnej moci využívať aj naďalej, pokiaľ neuplynie ich platnosť.**

Avšak v prípade ak kvalifikovaný certifikát bol vydaný po 1. januári 2009 je nevyhnutné, aby obsahoval aj rodné číslo. Ak by takýto kvalifikovaný certifikát neobsahoval rodné číslo nebolo by ho možné použiť v styku s orgánmi verejnej moci.

K podmienkam použitia rodného čísla v kvalifikovaných certifikátoch bolo na spoločnom rokovaní zástupcov NBU a Úradu na ochranu osobných údajov (ÚOOÚ) 3. novembra 2008 prijaté nasledovné stanovisko:

a) k porušeniu generálneho zákazu zverejňovania rodného čísla (resp. všeobecne použiteľného identifikátora) uvedeného v § 8 ods. 2 zákona č. 428/2002 Z.z. nedochádza, za predpokladu, že kvalifikovaný certifikát sa nikde nezverejňuje. Podpisovateľ (ako držiteľ kvalifikovaného certifikátu) zasiela overovateľovi kvalifikovaný certifikát obsahujúci rodné číslo spolu s podpisom, resp. s elektronicky podpísaným dokumentom. Ak je prijímateľom elektronicky podpísaného dokumentu orgán verejnej moci, ktorý **použitie kvalifikovaného certifikátu s rodným číslom v komunikácii vyžaduje ako povinné**, predpokladá sa, že už do tohto času vedie databázu rodných čísel, má určený účel spracovania tohto osobného údaju a má vypracovaný bezpečnostný projekt alebo bezpečnostné smernice. **Takýto informačný systém overovateľa musí spĺňať požiadavky zákona o ochrane osobných údajov.**

Z hľadiska bežných používateľov, ktorí sú príjemcami elektronicky podpísaných dokumentov, pričom **nevyžadujú použitie kvalifikovaného certifikátu s rodným číslom ako povinné**, vzťahuje sa na nich negatívne vymedzenie pôsobnosti zákona č. 428/2002 Z.z., t.zn. že ak boli takéto údaje (v tomto prípade kvalifikovaný certifikát s rodným číslom) získané bez predchádzajúceho určenia účelu a prostriedkov spracovania a bez zámeru ich ďalšieho spracovania **ustanovenia zákona o ochrane osobných údajov sa na nich nevzťahujú.**

b) ACA **nesmie** na svojich stránkach publikovať vydané kvalifikované certifikáty obsahujúce rodné číslo držiteľa, ale iba zoznamy týchto certifikátov.