

Stanovisko k § 17 ods. 2 zák. č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej len „zákon“)

Elektronické podpisy by mali umožniť aj komunikáciu prekračujúcu hranice. Na tento účel je potrebné zabezpečiť, aby slovenské elektronické podpisy mali medzinárodnú platnosť a opačne, stanoviť podmienky, za ktorých bude možné v Slovenskej republike uznávať zahraničné elektronické podpisy.

Podľa Smernice Európskeho parlamentu a Rady 199/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (ďalej len „smernica EÚ“) si podmienky pre platnosť cudzích elektronických podpisov na svojom teritóriu stanovuje každý štát sám; smernica EÚ v tomto smere dáva iba odporúčania.

Zákon o elektronickom podpise v ustanovení § 17 ods. 2 zákona (Uznávanie zahraničných certifikátov) túto skutočnosť upravuje nasledovne: „*Dňom vstupu Slovenskej republiky do Európskej únie sa certifikát vydaný certifikačnou autoritou majúcou sídlo v niektorej z krajín Európskej únie, ktorého platnosť možno overiť v Slovenskej republike, stáva rovnoprávnym certifikátu vydanému v Slovenskej republike. Kvalifikovaný certifikát vydaný uvedenou certifikačnou autoritou bude mať rovnakú právnu účinnosť ako kvalifikovaný certifikát vydaný v Slovenskej republike.*“

Pre overenie zaručeného elektronického podpisu vydaného zahraničnou akreditovanou certifikačnou autoritou je rozhodujúca možnosť overiť platnosť certifikátu príslušného verejného kľúča.

Proces overenia zaručeného elektronického podpisu v Slovenskej republike podlieha režimu právnych predpisov *Slovenskej republiky* a bez ohľadu na to, či sa jedná o kvalifikovaný certifikát domácej alebo zahraničnej certifikačnej autority, proces overenia musí byť v oboch prípadoch zhodný. Je tomu tak z toho dôvodu, lebo v konečnom dôsledku majú oba rovnakú platnosť a rovnakú právnu silu v *Slovenskej republike*.

Overovateľ overuje zaručený elektronický podpis prostriedkami na overovanie elektronického podpisu využitím podpísaného elektronického dokumentu a verejného kľúča patriaceho udávanému podpisovateľovi. Overenie zaručeného elektronického podpisu znamená overenie toho, či zaručený elektronický podpis spĺňa formálne požiadavky (schválené formáty dokumentov a podpisov) a či je platný. Podľa § 5 ods. 4 zákona „*pri overovaní zaručeného elektronického podpisu overovateľ na základe kvalifikovaného certifikátu verejného kľúča overí, či verejný kľúč na overenie zaručeného elektronického podpisu patrí podpisovateľovi.*“

Postup overovania zaručeného elektronického podpisu upravuje vyhláška Národného bezpečnostného úradu č. 135/2009 Z. z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky (ďalej len „vyhláška“).

Podľa § 11 ods. 5 vyhlášky na „overenie platnosti zaručeného elektronického podpisu overovateľ používa:

- a) elektronický dokument, pre ktorý sa zaručený elektronický podpis vyhotovil,
- b) zaručený elektronický podpis elektronického dokumentu,
- c) verejný kľúč z platného kvalifikovaného certifikátu prislúchajúci k súkromnému kľúču, ktorého pomocou sa zaručený elektronický podpis vyhotovil,
- d) podpisovú politiku, ktorej objektový identifikátor je uvedený v zaručenom elektronickom podpise alebo platný objektový identifikátor ním akceptovanej podpisovej politiky zo zoznamu podľa § 4 ods. 7 vyhlášky,
- e) platné verejné kľúče prislúchajúce k súkromným kľúčom, ktorých pomocou sa vyhotovili podpisy certifikátov a zoznamov certifikátov v certifikačnej ceste,

f) zoznamy zrušených certifikátov pre všetky certifikáty v certifikačnej ceste, prípadne informáciu o stave certifikátov v certifikačnej ceste získanú z potvrdenia o existencii a platnosti certifikátu.“

Na overenie zaručeného elektronického podpisu sa vyžaduje, aby boli dostupné a úplné informácie, ktoré sú potrebné a nevyhnutné na jeho overenie v zmysle zákona a vyhlášok. V zmysle vyhlášky úplnosť informácií znamená pripojiť k zaručenému elektronickému podpisu „úplné informácie o všetkých certifikátoch verejných kľúčov potrebných na overenie platnosti daného zaručeného elektronického podpisu, ako aj úplné informácie o zoznamoch zrušených certifikátov alebo informácie o stave certifikátov, ktoré sú rozhodujúce na overenie platnosti daného zaručeného elektronického podpisu“. Na overenie platnosti zaručeného elektronického podpisu teda nepostačuje overiť iba verejný kľúč podpisovateľa dokumentu.

Z uvedeného vyplýva, že na to, aby sme mohli hodnoverne a bezpečne overiť platnosť zaručeného elektronického podpisu v *Slovenskej republike*, potrebujeme poznať úplnú informáciu o kvalifikovanom certifikáte verejného kľúča podpisovateľa, úplnú informáciu o certifikáte akreditovanej certifikačnej autority a úplnú informáciu o certifikáte Národného bezpečnostného úradu. Musíme poznať celý reťazec certifikátov verejného kľúča: *kvalifikovaný certifikát verejného kľúča podpisovateľa – certifikát verejného kľúča akreditovanej certifikačnej autority – certifikát verejného kľúča Národného bezpečnostného úradu*. Kvalifikovaný certifikát používateľovi musí byť vydaný hodnovernou inštitúciou - akreditovanou certifikačnou autoritou a preto znalosť certifikátu verejného kľúča akreditovanej certifikačnej autority je pre overenie podpisu nevyhnutná. Tu sa však reťaz overovania nekončí, pretože v hierarchii infraštruktúry verejného kľúča (PKI) je akreditovanej certifikačnej autorite nadradená koreňová certifikačná autorita Národného bezpečnostného úradu a preto je potrebné overiť aj certifikát verejného kľúča Národného bezpečnostného úradu, teda certifikát, za ktorý ručí štát. Ak by ktorýkoľvek z týchto certifikátov nebol platný, prípadne bol zrušený a nachádzal by sa v zozname zrušených certifikátov, nebolo by možné overovaný podpis považovať za hodnoverný a nebolo by možné spoliehať sa na jeho platnosť v právnych úkonoch.

Platnosť kvalifikovaného certifikátu sa overuje nasledovnými spôsobmi:

1. Kontrolou platnosti kvalifikovaného certifikátu používateľa podľa časového údajá uvedeného v tele certifikátu, ktorý tam uviedol vydavateľ certifikátu, čiže akreditovaná certifikačná autorita. (Platnosť od – do),
2. Kontrolou možného predčasného zrušenia kvalifikovaného certifikátu používateľa na tzv. zozname zrušených certifikátov (CRL), ktorý vydáva vydavateľ certifikátov (akreditovaná certifikačná autorita),
3. Kontrolou pravosti kvalifikovaného certifikátu používateľa, t.j. kontrolou podpisu certifikátu, teda či certifikát bol vydaný dôveryhodným poskytovateľom - akreditovanou certifikačnou autoritou.

Platnosť certifikátu akreditovanej certifikačnej autority sa overuje nasledovnými spôsobmi:

1. Kontrolou platnosti certifikátu akreditovanej certifikačnej autority podľa časového údajá uvedeného v tele certifikátu, ktorý tam uviedol vydavateľ certifikátu, čiže Národný bezpečnostný úrad (Platnosť od – do),

2. Kontrolou možného predčasného zrušenia certifikátu akreditovanej certifikačnej autority na tzv. zozname zrušených certifikátov (CRL), ktorý vydáva vydavateľ certifikátov (Národný bezpečnostný úrad),
3. Kontrolou pravosti certifikátu akreditovanej certifikačnej autority, t.j. kontrolou podpisu certifikátu, teda či certifikát bol vydaný Národným bezpečnostným úradom.

Platnosť certifikátu Národného bezpečnostného úradu sa overuje nasledovnými spôsobmi:

1. Kontrolou platnosti certifikátu Národného bezpečnostného úradu podľa časového údajá uvedeného v tele certifikátu, ktorý tam uviedol vydavateľ certifikátu, čiže Národný bezpečnostný úrad (Platnosť od – do),
2. Kontrolou možného predčasného zrušenia certifikátu Národného bezpečnostného úradu na tzv. zozname zrušených certifikátov (CRL), ktorý vydáva vydavateľ certifikátov (Národný bezpečnostný úrad),
3. Kontrolou pravosti certifikátu Národného bezpečnostného úradu, t.j. kontrolou podpisu certifikátu, teda či certifikát bol vydaný Národným bezpečnostným úradom. Z toho dôvodu je verejný kľúč Národného bezpečnostného úradu k dispozícii priamo na Národnom bezpečnostnom úrade a zároveň sa zverejňuje vo viacerých informačných zdrojoch, tak ako to ustanovuje zákon.

Národný bezpečnostný úrad je certifikačnou autoritou najvyššej úrovne – tzv. koreňovou certifikačnou autoritou (KCA) v Slovenskej republike, preto proces overovania zaručeného elektronického podpisu musí byť vždy zavŕšený overením certifikátu verejného kľúča Národného bezpečnostného úradu.

Celý reťazec overovania kvalifikovaného certifikátu verejného kľúča, začínajúc kvalifikovaným certifikátom verejného kľúča podpisovateľa, končiac certifikátom verejného kľúča koreňovej certifikačnej autority musí byť dodržaný a zachovaný aj v prípade zahraničných certifikátov.

Národný bezpečnostný úrad je podľa § 34 zákona č. 575/2001 z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy ústredným orgánom štátnej správy pre elektronický podpis a teda garantom, ktorý vykonáva kontrolu nad dodržiavaním zákona a jeho vykonávacích predpisov, čo znamená že je garantom bezpečnosti prostredia elektronického podpisu. Národný bezpečnostný úrad však nemôže ručiť za zahraničné akreditované certifikačné autority a nimi vydané kvalifikované certifikáty, na ktoré nemá dosah (právo kontroly), a o ktorých nevie za akých legislatívnych, technických, organizačných, bezpečnostných a iných podmienok poskytujú svoje služby.

Jediným možným riešením ako uznať platnosť zahraničného kvalifikovaného certifikátu v Slovenskej republike je uzavretie medzinárodnej dohody alebo prijatie legislatívy v rámci Európskej únie, ktorá jednotlivé štáty zaviazze dodržiavať porovnateľné pravidlá a akreditačné postupy pre posúdenie dôveryhodnosti poskytovateľov certifikačných služieb (Akreditované certifikačné autority). Toto riešenie zároveň pokrýva recipocitu uznávania kvalifikovaných certifikátov. Prípadné uznanie zahraničného kvalifikovaného certifikátu bez splnenia uvedených podmienok by vnieslo nerovnoprávnosť do prostredia elektronického podpisu, pretože na domáce akreditované certifikačné autority by bolo možné uplatniť všetky požiadavky zákona avšak na zahraničné akreditované certifikačné autority len niektoré ustanovenia.

V rámci Európskej únie je proces posudzovania hodnovernosti akreditovanej certifikačnej autority ošetrený rozhodnutím Európskej komisie 2009/767/ES zo 16. 10. 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“, podľa smernice Európskeho parlamentu a

Rady 2006/123/ES o službách na vnútornom trhu. Týmto dňom vznikla pre orgány verejnej moci povinnosť uznávať kvalifikované certifikáty vydané poskytovateľmi certifikačných služieb členských krajín Európskej únie, za predpokladu, že príslušná členská krajina zverejní zoznam dôveryhodných poskytovateľov služieb – Trusted List (TL).

Na záver treba preto opätovne zdôrazniť, že aby platnosť zahraničného kvalifikovaného certifikátu bolo možno hodnoverne overiť, je nutné, aby:

- a) akreditovaná certifikačná autorita z členskej krajiny Európskej únie bola uvedená v zozname dôveryhodných poskytovateľov služieb danej členskej krajiny,*
- b) bola uzavretá medzinárodná dohoda medzi Slovenskou republikou a príslušným štátom (štát, ktorý nie je členským štátom Európskej únie; v súčasnosti Slovenská republika nemá uzavretú takúto dohodu so žiadnym štátom), v ktorej sa oba štáty po porovnaní príslušných právnych noriem a akreditačných schém recipročne zaviazajú, že si budú vzájomne uznávať vydávané kvalifikované certifikáty.*