

Potvrdzovanie elektronického dokumentu

Elektronická podateľňa

V životnom cykle elektronického dokumentu – podobne ako klasického dokumentu – hrajú významnú úlohu **úkony, ako je podanie** dokumentu podávateľom, **prevzatie** dokumentu adresátom, **overenie** dokumentu notárom a podobne. V záujme preukázateľnosti takéhoto úkonu je dôležité jeho potvrdenie vystavením potvrdenky – v prípade elektronického dokumentu tzv. **elektronickej potvrdenky**.

Podanie a prebratie elektronického dokumentu, ako aj vystavenie elektronickej potvrdenky umožňuje tzv. **elektronická podateľňa** (ďalej EPO). Elektronicкую podateľňu a elektronicкую potvrdenku v rámci orgánov verejnej moci alebo verejnej správy vymedzuje vyhláška NBÚ č. 542/2002 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku.

Aj keď ide o novú vyhlášku, problematika potvrdzovania príjmu elektronicých dokumentov má na Slovensku už niekoľkoročnú tradíciu a predstavuje jeden z významných prvkov bezpečnosti elektronickeho bankovníctva (R. Rexa a kol.: *Bezpečnosť elektronickeho bankovníctva v praxi*. PC REVUE č. 6/2001, s.102).

V článku porovnávame elektronicкую podateľňu podľa uvedenej vyhlášky s možnosťami elektronickej podateľne podľa reality dennej praxe.

Vyhláška NBÚ č. 542/2002 Z. z.

Obsah potvrdenky

Z § 6 ods. 2 písm. d) vyhlášky vyplýva, že elektronicкая potvrdenka je „elektronicкий документ выданный электронicкую подательню с использованием часовой печати“. Čo má byť obsahom tohto „dokumentu“ a ako má súvisieť s elektronickým dokumentom doručeným do podateľne, vyhláška nešpecifikuje. Zrejme je iba použitie časovej pečiatky, ale opäť chýba jasná informácia, načo má byť táto časová pečiatka vystavená. Možností je totiž viac.

Potvrdzovateľ

Aj keď nie je vo vyhláške explicitne uvedené, že elektronicкий документ – elektronicкая potvrdenka – má byť elektronicкую podateľňou podpísaný, povinnosť podateľne (§ 6 ods. 3 písm. c) „zverejniť kvalifikované certifikáty všetkých zamestnancov, ktorí zabezpečujú prevádzku elektronickej podateľne“, naznačuje, že ak uvedený dokument bude podpísaný, bude tam elektronicкий podpis niektorého zamestnanca podateľne.

Je škoda, že vyhláška nerieši podpisovanie elektronicých potvrdeniek automatizovanou elektronicкую podateľňou s bezpečným kryptografickým modulom podobne, ako je to v prípade podpisovania certifikátov certifikačnou autoritou. V modernom elektronickom svete, ktorý sa i vďaka

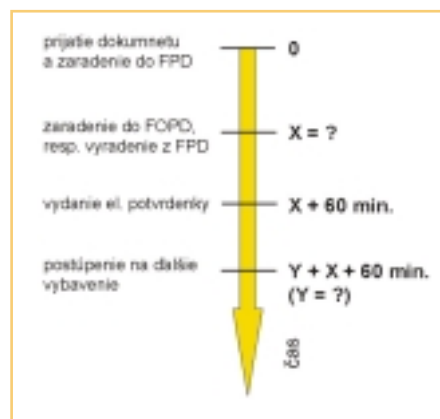


ka zákonu o elektronickom podpise začne úspešne rozbiehať aj na Slovensku, sa človek vykonávajúci určité operácie manuálne stáva zbytočnou brzdou.

Čas podania dokumentu

Vo vyhláške sa spomínajú štyri dôležité časové okamihy:

- prijatie dokumentu a jeho zaradenie do frontu prijatých dokumentov (ďalej FPD),
- zaradenie dokumentu do frontu overených prijatých dokumentov (ďalej FOPD), resp. jeho vyradenie z frontu prijatých dokumentov,
- vydanie elektronickej potvrdenky,
- postúpenie dokumentu na ďalšie vybavenie.



Nikde však nie je špecifikované, či vôbec, a ak áno, tak **aký čas má byť uvedený v potvrdenke** vystavenej elektronicкую podateľňou. Pre podávateľa dokumentu je určite najdôležitejší čas podania dokumentu.

V niektorých prípadoch je presne stanovená hodina, dokedy možno podanie urobiť. Nedodržanie tohto termínu podania, resp. neschopnosť dokázať jeho splnenie, môže mať pre podávateľa za následok značné straty. Preto zvlášťne pôsobí „voľné tempo“ pri vystavovaní elektronicých potvrdeniek v elektronickej podateľni podľa uvedenej vyhlášky: „Overenie a následné prijatie elektronickeho dokumentu elektronicкая podateľňa potvrdí vydaním elektronickej potvrdenky... a to najviac 60 minút od zaradenia elektronickeho dokumentu do frontu overených prijatých dokumentov“. Pritom sa už nehovorí, za aký čas od príjmu má byť dokument preradený do FOPD. Pretože v klasickej podateľni, resp. na pošte nehrozí 60-minútové zdržanie vydania doručenej k prevzatému dokumentu, je nevhodné niečo podobné zavádzať v elektronickej podateľni.

Časová pečiatka

Podľa § 6 ods. 4 vyhlášky: „Pri manipulácii s elektronickým dokumentom, najmä pri potvrdzovaní jeho

prijatia alebo postúpení na ďalšiu manipuláciu, využíva elektronickú podateľňu službu časovej pečiatky.“

Je záhadou, prečo na získanie informácie o čase je v elektronickej podateľni možné využívať iba časové pečiatky, ktoré podľa zákona č. 215/2002 Z. z. môže poskytovať iba akreditovaná certifikačná autorita. Určite ste už aspoň raz boli svedkom ochromenia práce pokladní v hypermarkete v súvislosti s prerušením spojenia s ACS – poskytovateľom služieb súvisiacich s platobnými kartami. V hypermarkete naštastie okrem platenia platobnou kartou cez ACS máte možnosť platiť aj v hotovosti. V elektronickej podateľni podľa uvedenej vyhlášky alternatíva neexistuje. Z formulácie uvedeného paragrafu nie je vylúčené, že pri podaní elektronického dokumentu a ďalšej manipulácii s ním nemusí stačiť iba jedna časová pečiatka.

Úvaha o vyhláške

Uvedená vyhláška nešpecifikuje obsah elektronickej potvrdenky, takže v nej môžu chýbať tie najpodstatnejšie prvky:

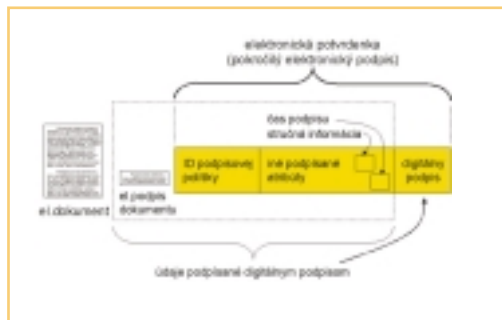
- osoba, ktorá úkon (podanie dokumentu) potvrdzuje,
- obsah úkonu (spojenie potvrdenky s konkrétnym podaným dokumentom),
- čas úkonu.

To, čo vyhláška „zabetónovala“ dôkladne, je využívanie časovej pečiatky, aj keď ide o prvok ohrozujúci plynulosť poskytovania elektronických potvrdeniek.

Na doplnenie predstáv o potvrdzovaní príjmu elektronických dokumentov podľa uvedenej vyhlášky sa v nasledujúcej časti budeme venovať elektronickým potvrdenkám a elektronickej podateľni podľa reality dennej praxe.

Elektronická potvrdenka

Aby mala potvrdenka právnu silu a bolo ju možné použiť ako dôkaz pri prípadnom spore, musí z nej byť zrejmé, kto daný úkon potvrdil, kedy a čo bolo obsahom tohto úkonu.



Potvrdenka je určená tomu, koho má chrániť – kto v prípade potreby bude musieť dokazovať, že sa daný úkon uskutočnil. Napríklad:

- **elektronická potvrdenka o podaní dokumentu podávateľom** je určená podávateľovi daného dokumentu,
- **elektronická potvrdenka o prevzatí dokumentu adresátom** je určená doručovateľovi
- a pod.

Elektronická potvrdenka je elektronický dokument informujúci o úkone s iným elektronickým dokumentom, je k tomuto inému dokumentu pripojená alebo s ním logicky súvisí a slúži ako metóda overenia. Pod overením sa myslí:

- kto úkon potvrdil – **potvrdzovateľ**,
- kedy úkon potvrdil – **čas potvrdenia**,
- o aký úkon a v súvislosti s akým elektronickým dokumentom išlo – **obsah úkonu**,
- a pod.

V prípadnom spore za dostatočne dôveryhodný dôkaz je možné považovať elektronickú potvrdenku, ktorá umožňuje overiť **jednoznačné spojenie** potvrdenky s potvrdzovateľom, časom potvrdenia a obsahom úkonu. V tomto prípade možno v súlade s terminológiou smernice EÚ hovoriť o **pokročilej** (zaručenej) **elektronickej potvrdenke**, zatiaľ čo v prípade nejednoznačnosti ktoréhokoľvek z uvedených spojení ide o „obyčajnú“ **elektronickú potvrdenku**, ktorú v prípadnom spore bude potrebné doplniť o ďalšie dôveryhodnejšie dôkazy.

Jednoznačnosť spojenia elektronického dokumentu (v tomto prípade obsahu úkonu) s osobou (potvrdzovateľom), ktorá daný úkon v danom čase (čas potvrdenia) urobila, umožňuje zaistiť elektronický podpis potvrdzovateľa k obsahu úkonu, prípadne v kombinácii s časovou pečiatkou k tomuto podpisu. Táto jednoznačnosť platí za predpokladu splnenia troch základných predpokladov (elektronický podpis je na báze digitálneho podpisu, ide o jednoznačné spojenie verejného kľúča s jeho majiteľom – potvrdzovateľom, súkromný kľúč potvrdzovateľa je pod jeho výlučnou kontrolou).

A. Potvrdzovateľ

Potvrdzovateľom úkonu – príjmu elektronického dokumentu – je fyzická osoba, ktorá dokument preberá manuálne.

V prípade automatizovaného príjmu dokumentov je potvrdzovateľom elektronická podateľňa. V tomto prípade nejde o podpis konkrétneho pracovníka, ale o podpis elektronickej podateľne, ktorý je potrebné chápať podobne ako podpis certifikačnej autority na certifikáte verejného kľúča.

B. Čas potvrdenia úkonu

V klasickom papierovom svete dochádza k potvrdzovaniu príjmu dokumentu v momente jeho príjmu, prípadne s miernym predstihom, resp. oneskorením. V elektronickej svete, hlavne vďaka automatizácii a vysokému výkonu použitej výpočtovej techniky, je možné v zlomku sekundy okrem príjmu dokumentu a potvrdenia jeho príjmu vykonať ešte množstvo ďalších úkonov, ktoré pri manuálnej manipulácii s dokumentom s ohľadom na ich časovú náročnosť nie je možné vykonávať.

Je niekoľko možností zaznamenania času, keď daný úkon (príjem elektronického dokumentu) nastal:

a) Čas podpisu (signing time)

Čas podpisu je jedným z atribútov elektronického podpisu, ktorého integrita je kontrolovaná samotným digitálnym podpisom spolu s integritou podpísaného elektronického dokumentu.

Pri manuálnej manipulácii s elektronickým dokumentom za správnosť uvedeného atribútu zodpovedá konkrétna fyzická osoba – potvrdzovateľ, pričom je väčšinou odvodený od systémového času prostriedku použitého na vytvorenie elektronického podpisu potvrdzovateľa.

Pri automatickej manipulácii s elektronickým dokumentom je čas podpisu odvodený od systémového času bezpečného kryptografického modulu, prípadne bezpečného zariadenia presného času, ktoré sú súčasťou elektronickej podateľne.

b) Časová pečiatka (time stamping)

Ide o časový údaj, ktorý je jednoznačne priradený k podpisu potvrdzovateľa na elektronickej potvrdenke a ktorého správnosť svojím podpisom garantuje poskytovateľ časovej pečiatky.

Spôľahlivosť poskytovania elektronických potvrdeniek elektronickej podateľňou bude v tomto prípade silne závisieť od spoľahlivosti poskytovania časových pečiatok

poskytovateľom časových pečiatok a od spoľahlivosti spojenia s ním. Je rozumné, aby si podávateľ obstaral časovú pečať iba k tým elektronickým potvrdenkám, pri ktorých bude vyžadovať dlhodobú platnosť.

C. Obsah úkonu

Aby elektronická potvrdenka umožnila jednoznačne určiť obsah úkonu (prijatie/odmietnutie konkrétneho elektronického dokumentu), je podpis potvrdzovateľa na elektronickej potvrdenke vytvorený k podpisu doručeného podpísaného elektronického dokumentu a k stručnej informácii potvrdzovateľa (o aký úkon ide – prijatie dokumentu, zamietnutie z dôvodu... a pod.). Je vhodné, aby stručná informácia potvrdzovateľa bola ďalším podpísaným atribútom elektronického podpisu potvrdzovateľa, ktorého integritu – podobne ako integritu času podpisu – kontroluje digitálny podpis elektronickej potvrdenky.

Pokročilá elektronická potvrdenka

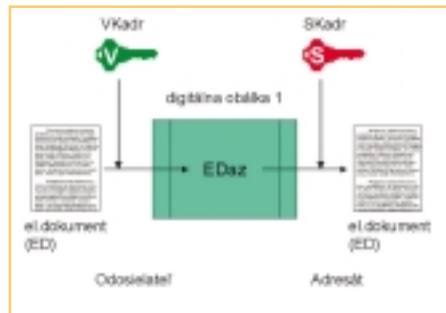
Z uvedeného sa môžeme dopracovať k nasledujúcej definícii: **pokročilá (zaručená) elektronická potvrdenka** je vlastne pokročilým (zaručeným) elektronickým podpisom potvrdzovateľa k podpisu doručeného elektronického dokumentu. Čas prijímu elektronického dokumentu zachytáva atribút čas podpisu v elektronickej potvrdenke potvrdzovateľa, resp. ho približuje časová pečať k tomuto podpisu. V druhom prípade ide o tzv. **elektronickú potvrdenku s dlhodobou platnosťou**.

Digitálna obálka

Zachovať dôvernosť obsahu elektronického dokumentu umožňuje tzv. **digitálna obálka**. Tá zabezpečuje utajenie obsahu dokumentu jeho kryptovaním. Ku kryptovaniu dochádza na strane autora dokumentu a k odkryptovaniu zase na strane adresáta. Na kryptovanie elektronického dokumentu, prípadne podpísaného elektronického dokumentu sa využíva asymetrická kryptografia, prípadne v kombinácii so symetrickou kryptografiou.

Asymetrická kryptografia – digitálna obálka 1

V tomto prípade autor zakryptuje elektronický dokument (ED) verejným kľúčom adresáta (VKadr). Odkryptovať takýto dokument (EDaz) je možné iba pomocou zodpovedajúceho súkromného kľúča (SKadr). Znamená to, že okrem adresáta, ktorý má



súkromný kľúč pod svojou výlučnou kontrolou, nikto iný nemá možnosť otvoriť digitálnu obálku s elektronickým dokumentom.

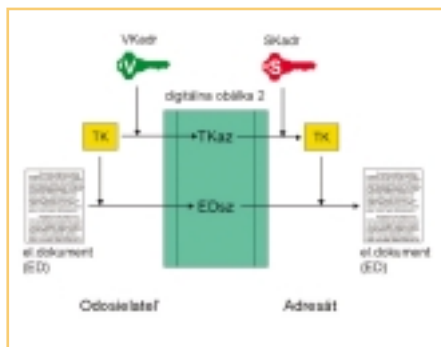
Nevýhodou tejto čisto asymetrickej metódy je časová náročnosť kryptovania, resp. dešifrovania

hlavne dokumentov s väčším objemom. Túto časovú náročnosť eliminuje kombinácia asymetrickej kryptografie so symetrickou kryptografiou.

Asymetrická kryptografia v kombinácii so symetrickou kryptografiou – digitálna obálka 2

V tomto prípade autor správy použije náhodne vygenerovaný tajný kľúč (TK) na symetrické kryptovanie elektronického dokumentu a súčasne pomocou verejného kľúča adresáta (VKadr) zakryptuje tajný kľúč (TK). Digitálnu obálku predstavuje asymetricky zakryptovaný tajný kľúč (TKaz) spolu so symetricky zakryptovaným dokumentom (EDsz).

Adresát najprv pomocou svojho súkromného kľúča (SKadr) odkryptuje zakryptovaný tajný kľúč (TKaz) a následne pomocou tohto kľúča (TK) odkryptuje zakryptovaný elektronický dokument.



Tajný kľúč má malý objem, preto jeho asymetrické kryptovanie, resp. dešifrovanie nie je časovo náročné, rovnako ako symetrické kryptovanie a dešifrovanie väčšieho dokumentu.

Reálna elektronická podateľňa

Základnou úlohou elektronickej podateľne je **prijímať, resp. umožniť prevziať elektronický dokument** a zabezpečiť pre odovzdávajúcu stranu (podávateľa, resp. elektronickú podateľňu) **pokročilú (zaručenú) elektronickú potvrdenku**, ktorá umožní jednoznačne overiť, ktorý dokument, kto a kedy od odovzdávajúcej strany prevzal.

Podávateľ môže elektronický dokument doručiť do podateľne:

- prostredníctvom verejného poskytovateľa (poskytovateľ prístupu na internet, poskytovateľ WAP služby a pod.) s využitím štandardnej aplikácie typu e-mail, WWW prehliadač, WAP prehliadač,
- prostredníctvom pevného alebo dial-up pripojenia k podateľni s využitím špeciálnej aplikácie,
- osobne na niektorom z dohodnutých médií.

V prípade emailového podania v súvislosti s možným oneskorením doručenia e-mailu do podateľne môže byť čas uvedený na potvrdenke oproti času odoslania e-mailu podávateľom takisto oneskorený. V ostatných uvedených prípadoch, pretože ide o on-line komunikáciu, podávateľ dokumentu súčasne s podaním dostane od podateľne pokročilú (zaručenú) elektronickú potvrdenku.

Vďaka automatizácii jednotlivých operácií vykonáva elektronická podateľňa súčasne s prijímom dokumentu aj nastavené kontroly (na platnosť certifikátu, platnosť podpisu, prítomnosť škodlivých kódov a bitových sekvencií, dodržanie ustanovených

formátov a pod.). V prípade, že sa doručený dokument nachádza v digitálnej obálke, niektoré kontroly sa nevykonávajú.

Súčasne s prijímom dokumentu a jednotlivými kontrolami podateľňa vydá príslušnú pokročilú (zaručenú) elektronickú potvrdenku. Súčasťou potvrdenky okrem certifikátu je aj CRL použité na overenie platnosti certifikátu podávateľa dokumentu. Čas prijímu dokumentu a vystavenia elektronickej potvrdenky poskytuje bezpečné zariadenie so zdrojom presného času, ktoré je súčasťou elektronickej podateľne a nachádza sa v elektronickej potvrdenke ako atribút „čas podpisu“. Podateľňa má možnosť vystavovať aj elektronické potvrdenky s dlhodobou platnosťou s využitím časových pečiatok od poskytovateľa takejto služby.

Preberateľ môže v podateľni prebrať iba jemu určené dokumenty, prípadne dokumenty určenej skupine, do ktorej patrí, alebo dokumenty určené všetkým preberateľom podateľne. Pred prevzatím elektronického dokumentu musí preberateľ podpísať elektronickú potvrdenku o prevzatí dokumentu. Až po jej overení sa preberateľovi sprístupní príslušný dokument.

Okrem uvedených základných úloh môže elektronická podateľňa poskytovať správu dokumentov (**Document management**), definovanie postupu práce s dokumentom (**Workflow**), skladovanie dokumentov (**Storage**), prevod klasických dokumentov do elektronickej formy (**Capture**) a pod.

Z bezpečnostného hľadiska automatizovaného podpisovania elektronických potvrdeniek je táto elektronická podateľňa podobne ako certifikačná autorita na automatizované podpisovanie certifikátov vybavená kryptografickým modulom podľa CEN/ISSS CWA 14167-2 a umožňuje auditovateľnosť preddefinovaných operácií.

Pokročilé elektronické potvrdenky (v terminológii podľa smernice EÚ, nie však v terminológii „zdeformovaného“ slovenského zákona č. 215/2002 Z. z.) pri svojich platobných príkazoch využívajú tisíce klientov jednej banky na Slovensku už od roku 1996. Opísanú elektronickú podateľňu si prakticky môžete vyskúšať na adrese:

www.elektronicka-podatelna.sk.

ZHRNUTIE

1. Pre podávateľa elektronického dokumentu má význam iba taká elektronická potvrdenka, ktorá je jednoznačne spojená s obsahom úkonu, jeho potvrdzovateľom a časom, keď úkon nastal.

2. Je vhodné, aby si k potvrdenke, ktorá má mať dlhodobú platnosť, podávateľ obstaral aj časovú pečať.

3. Používanie časových pečiatok ku každému podaniu je nelogické. Závislosť elektronickej podateľne od tretej strany zníži jej pružnosť a spoľahlivosť.

R.Rexa@e-unicom.sk