

Verejná elektronická podateľňa

V klasickom papierovom svete je každému z nás jasné, čo predstavuje **podací listok** k doporučenému listu, resp. **doručenka** k listu určenému do vlastných rúk. Máme takisto skúsenosti s preberaním takýchto zásielok, resp. ich podávaním na pošte či v klasickej podateľni úradu a vieme si predstaviť, čo všetko s tým súvisí.

V článku sa prenesieme z klasického papierového sveta do toho elektronického a budeme sa venovať podávaniu a preberaniu elektronických dokumentov prostredníctvom elektronickej podateľne.

Čo je to elektronická podateľňa?

Elektronická podateľňa (ďalej EPO) je informačný systém s komplexom bezpečnostných, organizačných, obchodných, právnych opatrení, ktorého základnou úlohou je umožniť podávateľom **podávať** elektronické dokumenty určené určitým adresátom a, naopak, adresátom umožniť **preberať** nimi určené elektronické dokumenty. Ďalej je úlohou systému **ochrániť** **súkromie** oboch strán (podávateľ, adresát) a poskytnúť im hodnotné **podklady**, použiteľné na **riešenie** prípadného sporu.

Elektronická podateľňa môže existovať ako **verejná** (VEPO), v rámci ktorej môže byť podávateľom, resp. adresátom ktokoľvek, kto má dostatočný počet kreditov, a ako **vnútro podniková**, ktorá slúži bez kreditácie pre potreby určitého podniku, resp. úradu na vnútro podnikovú výmenu elektronických dokumentov alebo na styk úradu s verejnosťou. V ďalšej časti sa budeme venovať VEPO.

Zatiaľ čo pri klasickej pošte, resp. podateľni je dôležitá ich fyzická dostupnosť, v prípade VEPO nie je až také podstatné, kde sa nachádza. Dôležitá je

jej **dostupnosť cez internet**, prípadne iné komunikačné médium.

Dôveryhodnosť VEPO značne závisí od spoľahlivosti služieb a údajov, ktoré VEPO poskytuje. Časový údaj je jedným z najvýznamnejších. Hodiny VEPO sú synchronizované so zdrojom atómového času s odchýlkou na úrovni 0,1 s.

Aktuálny čas VEPO sa klientovi zobrazí po úspešnej autentifikácii (obr. 1). Nepresnosť **časového komponentu** na obrazovke klienta, synchronizovaného s hodinami VEPO, závisí od kolísania priestupnosti spojenia klienta s VEPO, pričom odchýlka je na úrovni 1 s. K štandardným službám VEPO, založeným na vlastnom zdroji presného času, môže klient využívať aj časové pečiatky od poskytovateľa tejto služby.

Prístup do VEPO je možný na základe súkromného kľúča a **platného certifikátu** klienta, vydaného uznávanou certifikačnou autoritou na účely autentifikácie a šifrovania. V prípade, že majiteľ platného certifikátu pristupuje do VEPO po prvýkrát, má možnosť rozhodnúť sa, či bude využívať služby VEPO a nechá sa zaviesť do systému (obr. 2).

Po zavedení klient ešte nemá **kredity** a môže využívať výmenu dokumentov s obchodným oddelením VEPO, prípadne ďalším tzv. verejným adresátom. Až po získaní kreditov môže využívať v plnom rozsahu základné, prípadne doplnkové služby VEPO.

Podávanie dokumentu

Ako prvé pri podávaní dokumentu podávateľ vyberá **adresáta** (obr. 3). Pri tomto výbere podávateľ určuje certifikát adresáta, ktorému dôveruje. Má možnosť vybrať si tzv. verejného adresáta (ob-

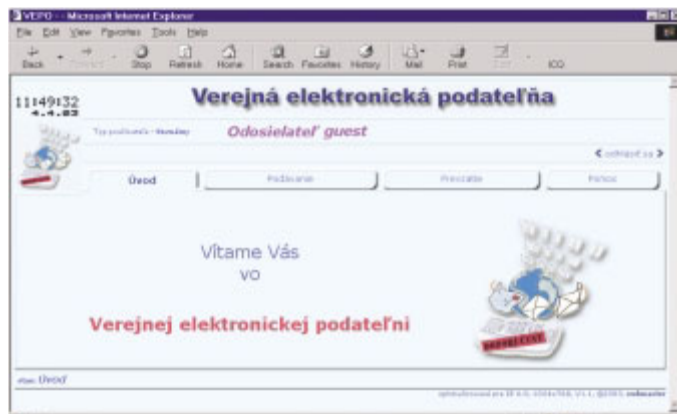
chodné oddelenie VEPO, prípadne ďalší nadštandardní klienti), resp. si môže vybrať adresáta zo svojho súkromného zoznamu. Do tohto zoznamu sa automaticky ukladajú adresáti, ktorých certifikát odosielať už aspoň raz použil pri odosielaní elektronických dokumentov.

V druhom kroku (obr. 4) klient vyberá súbor s **elektronickým dokumentom**, ktorý bude podávať. K dokumentu môže pridať súbor s **elektronickým podpisom**, ktorý k danému elektronickému dokumentu vytvoril pomocou tzv. **podpisovacieho** súkromného kľúča a lokálnej aplikácie, prípadne ešte aj súbor s **časovou pečiatkou**, ktorú získal u poskytovateľa služby časovej pečiatky. V prípade, že klient nemá k dispozícii lokálnu aplikáciu na vytvorenie podpisu, môže využiť **podpisovací komponent**, ktorý sa mu po výbere príslušnej voľby stiahne a spustí na počítači. Tento komponent pri podpisovaní využíva čas synchronizovaný s hodinami VEPO.

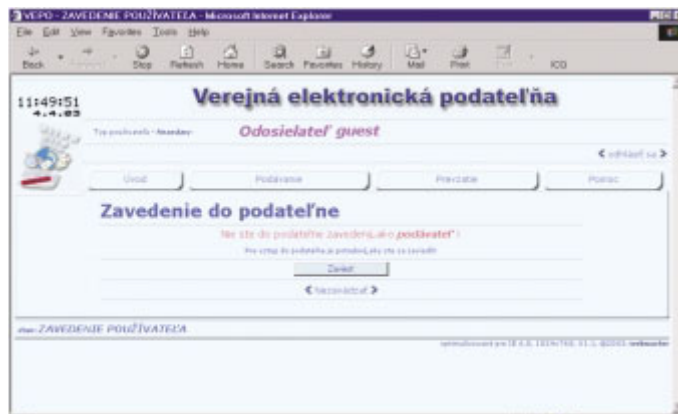
Po odoslaní podpísaného dokumentu VEPO informuje podávateľa (obr. 5) o úspešnosti podania, prípadne o dôvode jeho odmietnutia. Podrobnejšie informácie o úspešnom podaní spolu s prideleným **podacím číslom** a **časom podania** dokumentu obsahuje **elektronický podací listok**, ktorý sa nachádza v zozname dokumentov podaných klientom (obr. 6). Vydala ho elektronická podateľňa v momente prijatia elektronického dokumentu do VEPO (čas podania). Je v záujme podávateľa **overiť si platnosť** elektronického podacieho listka (obr. 7) a **uchovať si ho** spolu s príslušným elektronickým dokumentom a súvisiacimi súborami (podpis, prípadne časová pečiatka) pre prípad sporu.

Overovanie platnosti certifikátu

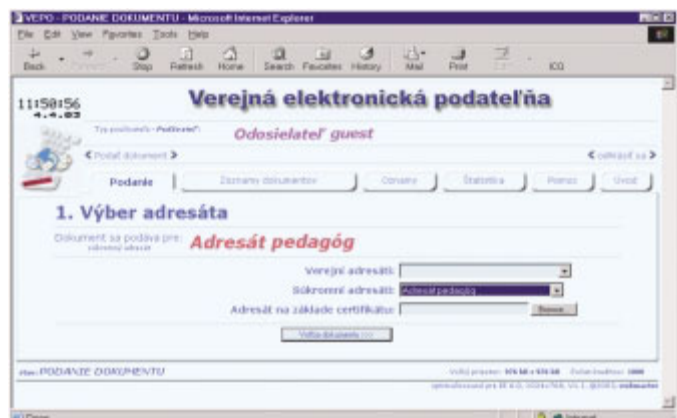
Pri overovaní platnosti elektronického podacieho listka (všeobecne akéhokoľvek podpisu) vytvoreného určitým súkromným kľúčom je potrebné



Obr. 1



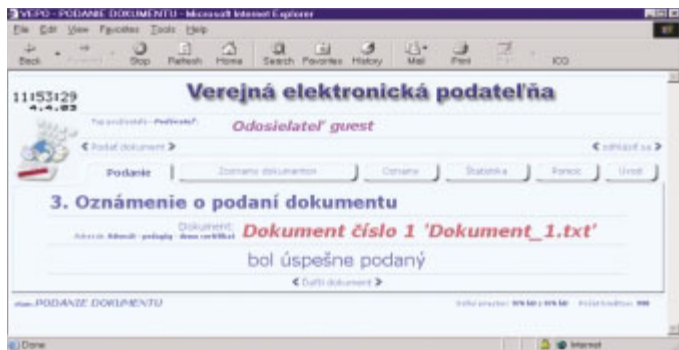
Obr. 2



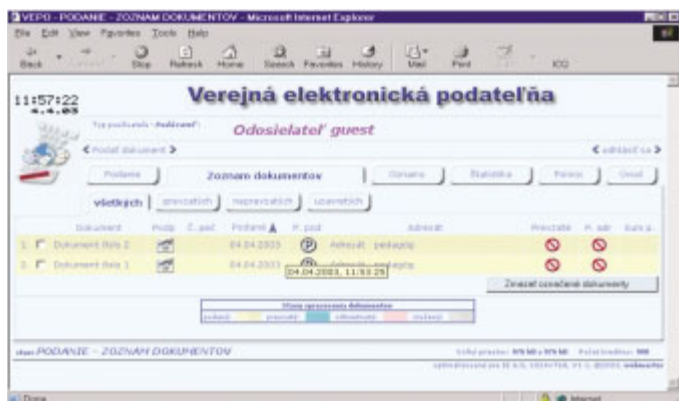
Obr. 3



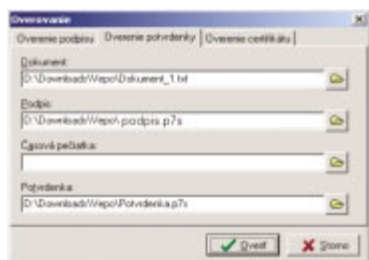
Obr. 4



Obr. 5



Obr. 6

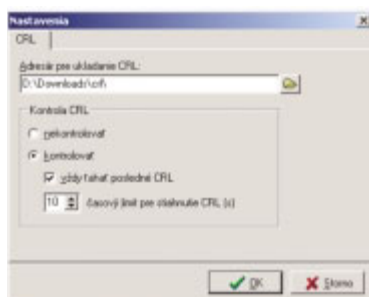


Obr. 7

zistiť, či príslušný certifikát, ktorým sa overuje platnosť podpisu, rovnako ako všetky nadradené certifikáty, nebol predčasne zrušený a nebol zaradený na zoznam zrušených certifikátov (CRL). Komponent na overovanie podpisu umožňuje nastaviť 3 hladiny režimu kontroly platnosti certifikátu (obr. 8):

- nekontroluje CRL,
- kontroluje CRL,
- kontroluje CRL a sťahuje posledné CRL pri overovaní platnosti každého podpisu.

Pri nastavení prvej voľby sa nekontroluje možnosť predčasného zrušenia certifikátu. V ďalších dvoch prípadoch sa táto kontrola vykonáva, pričom v prvom z nich sa CRL občerstvuje až po uplynutí platnosti predchádzajúceho CRL, v druhom prípade sa CRL občerstvuje pri overovaní platnosti každého podpisu. Výhodou poslednej voľby je možnosť využívať služby tej certifikačnej authority, ktorá okrem periodicke vydávaných CRL vydáva CRL aj po každom požiadaní klienta o zrušenie certifikátu.



Obr. 8

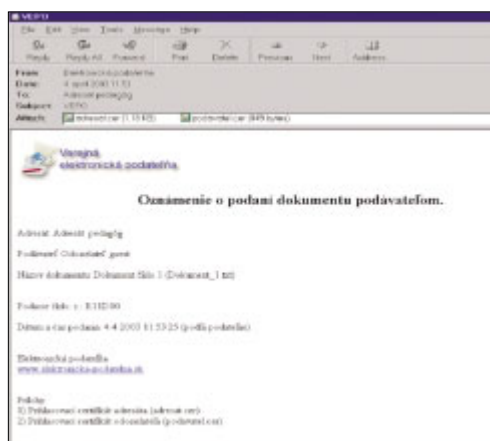
Počet CRL použitých pri overovaní platnosti podpisu je zrejme z informácie o výsledku overovania (obr. 7). Overovanie je vzťahované k času v časovej pečiatke, resp. k tzv. času podpisu (Signing Time), resp. k aktuálnemu času.

Storno dokumentu

VEPO prostredníctvom e-mailu (prípadne prostredníctvom SMS, faxu atď.) automaticky informuje adresáta o tom, že do jeho schránky daný podávateľ v danom čase podal daný dokument, ktorý je v podateľni evidovaný pod daným podacím číslom (obr. 9). Do doby prevzatia dokumentu adresátom môže podávateľ príslušný dokument stornovať. Predtým však musí podpísať **elektronické potvrdenie storna dokumentu** (obr. 10), ktoré si uchová podateľňa pre prípad sporu. O stornovaní dokumentu VEPO adresáta tiež informuje.

Štatistika

Na rýchly prehľad o aktivitách v schránke klienta slúži jednoduchá štatistika (obr. 11).

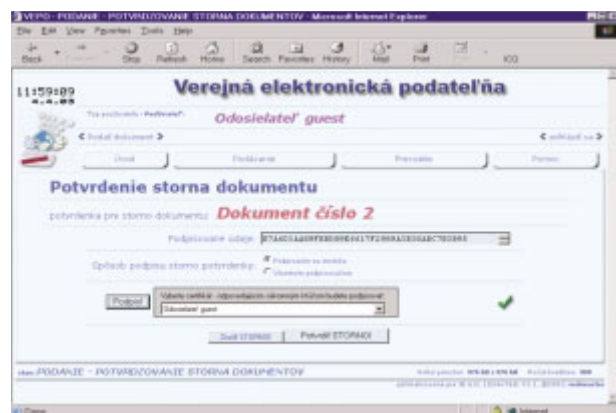


Obr. 9

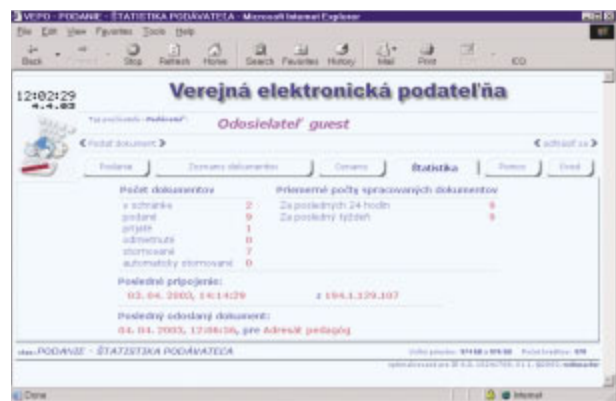
Zvýšenie diskrétnosti podávaných elektronických dokumentov

Aj keď komunikácia podávateľa i adresáta s VEPO je šifrovaná, má podávateľ možnosť zvýšiť diskrétnosť podávaného dokumentu využitím „digitálnej obálky“ – zašifrovaním elektronického dokumentu so súvisiacimi súborami pomocou verejného kľúča adresáta, resp. ďalších vybraných osôb (obr. 12). Túto digitálnu obálku môže otvoriť (rozšifrovať) iba adresát, prípadne ďalšia vybraná osoba vlastniaca súkromný kľúč zodpovedajúci verejnému kľúču použitému na šifrovanie (obr. 13).

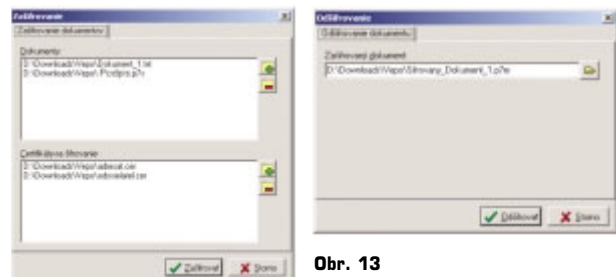
Poznámka: Pri využívaní digitálnych obálok VEPO nemôže pre adresáta zabezpečovať niektoré nadštandardné služby – kontrolu na prítomnosť škodlivých kódov a bitových sekvencií a pod.



Obr. 10

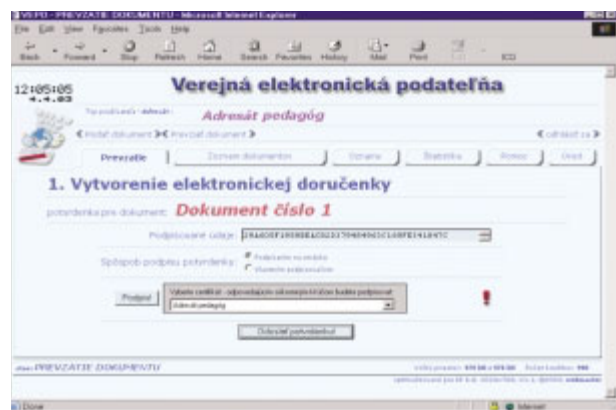


Obr. 11

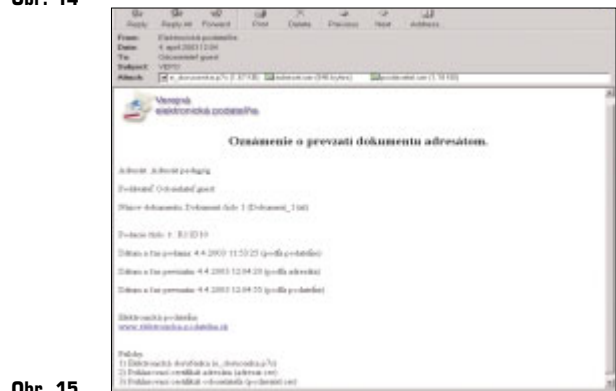


Obr. 13

Obr. 12



Obr. 14



Obr. 15

Prevzatie dokumentu

Ako už bolo uvedené, VEPO cestou e-mailu, resp. ďalších kanálov informuje adresáta o tom, že do jeho schránky pribudol nový dokument. Na základe príslušného súkromného kľúča má adresát možnosť vstúpiť do svojej schránky a prevziať si príslušný elektronický dokument so súvisiacimi súborami. Predtým však musí podpísať **elektronickú doručku** k elektronickému odtlačku elektronického dokumentu a všetkých s ním súvisiacich súborov (obr. 14). Elektronická doručka podpísaná adresátom sa uchováva vo VEPO pre prípad sporu a zároveň sa odosiela podávateľovi elektronického dokumentu so súhrnnou informáciou o podaní i prebratí dokumentu (obr. 15).

Tieto údaje informatívneho charakteru sú zároveň obsiahnuté v tzv. sumárnej elektronickej potvrdenke, ktorú vystavuje a potvrdzuje VEPO po prevzatí dokumentu adresátom, po odmietnutí prevziať dokument adresátom, resp. po stanovenom čase (7 dní), ak adresát dokument neprevzal.

Elektronické dokumenty so súvisiacimi súborami sa v podateľni neuchovávajú. Má ich možnosť zo svojej schránky zmazať podávateľ i adresát, resp. neprevzaté dokumenty sa zmažu automaticky po uplynutí stanoveného času. V podateľni sa uchovávajú iba potvrdenia storna, resp. elektronické doručky, ako dôkaz o tom, že podateľňa vydala daný dokument iba osobe, ktorej bol určený. Všetky ďalšie elektronické podklady (dokument, podpis, časová pečiatka, podací listok, resp. sumárnu potvrdenku) musí v prípade sporu predložiť reklamujúci.

Elektronická potvrdenka

Pri práci s elektronicou podateľňou sme sa stretli s pojmami ako elektronický podací listok, elektronické potvrdenie storna dokumentu, elektronická doručka, resp. sumárna elektronická potvrdenka. Vo všetkých týchto prípadoch ide o pokročilú elektronickú potvrdenku, z ktorej je zrejmy **obsah** úkonu (podanie, stornovanie, prevzatie akého konkrétného elektronického dokumentu), **kedy** a **kto** (podateľňa, podávateľ, adresát) svojím zarúčeným elektronickým podpisom tento úkon potvrdil. Podrobnejšie pozri [1].

Spôľahlivosť a bezpečnosť služieb VEPO

Z hľadiska kvality služieb VEPO hrá kľúčovú úlohu spoľahlivosť a bezpečnosť celého systému. So spoľahlivosťou úzko súvisí presnosť jednotlivých operácií a poskytovaných údajov (napr. **presnosť času**), stabilita a priepustnosť celého systému.

Kľúčovým prvkom bezpečnosti je **elektronický podpis a PKI**, na základe ktorých sa riadi prístup k jednotlivým službám VEPO, overuje sa oprávnenosť vykonať určitú transakciu (podanie, prevzatie,

storno dokumentu), potvrdzuje sa vykonanie určitej transakcie a zaisťuje sa dôverynosť a integrita vymieňaných informácií (elektronických dokumentov, elektronických potvrdeniek a pod.).

S ohľadom na počet podateľňou potvrdzovaných transakcií nie je reálne, aby ich potvrdzovala fyzická osoba svojím súkromným kľúčom, ktorý má udržiavať pod svojou výlučnou kontrolou. Tieto operácie sa robia automatizovane pomocou **bezpečného kryptografického jadra**. Bezpečnosť celého systému VEPO vychádza z bezpečnostnej politiky VEPO, ktorá je rozpracovaná v bezpečnostnom projekte s bezpečnostným zámerom, analýzou bezpečnosti, bezpečnostnými smernicami a havarijným plánom.

VEPO garantuje:

1. správny čas podpísaných elektronických potvrdeniek,
2. zachovanie súkromia (podávateľa i adresáta). Podaný elektronický dokument so súvisiacimi súborami VEPO vydá iba adresátovi, ktorého si odosielateľ zvolil výberom jeho certifikátu. Po stanovenom termíne dokument a súvisiace súbory nenávratne zlikviduje.

VEPO nezodpovedá za:

1. jednoznačné spojenie verejného kľúča s jeho majiteľom, za to zodpovedá príslušná certifikačná a registračná autorita; podávateľ určuje, ktorému certifikátu adresáta dôveruje;
2. spôsob udržiavania súkromného kľúča majiteľa certifikátu (podávateľ, resp. adresát) pod jeho výlučnou kontrolou; za bezpečnosť súkromného kľúča zodpovedá majiteľ príslušného certifikátu.

Klasická verzus elektronická podateľňa

K porovnaniu výhod, resp. nevýhod elektronickej podateľne aspoň niekoľko parametrov na zamyslenie:

- Čas – rýchlosť doručenia dokumentu a získania doručky
- Spojenie potvrdenky s dokumentom (integrita dokumentu)
- Dôverynosť
- Kontrola dokumentu pri jeho podávaní
- Oznámenie o podaní, prevzatí
- Lokalizácia podateľne
- Prevod dokumentu papierový < - > elektronický
- Prácnosť
- Cena

Aj vám vyšlo, že elektronická podateľňa je podstatne výhodnejšia než klasická „papierová“ podateľňa, resp. pošta?

Literatúra:

- [1] REXA, R.: Elektronický podpis – kľúč k moderným elektronickým službám. Elfa, Košice 2002.