Ministerstvo informatiky
České republiky

**Ministerstvo informatiky**
**Havelkova 2**
**130 00 Praha 3**

# Best practice
# Jak vyřizovat elektronickou poštu

Verze 2.0

# Obsah:

# Předmluva

Zásady pro vyřizování elektronické pošty, které Ministerstvo informatiky vydává jako „best practice", jsou určeny zejména orgánům státní správy a samosprávy, jakož i dalším právním subjektům, které rozhodují jako orgány veřejné moci (dále „úřady") a kterým jsou doručovány písemnosti ve smyslu zákona o archivnictví a spisové službě [6] prostřednictvím elektronické pošty.

Elektronická pošta se stále více prosazuje jako prostředek doručování písemností veřejné správě na úkor listovní pošty. Po novele hlavních procesně právních předpisů je nutné vzít v úvahu i to, že takto doručené písemnosti mají stejný význam a plynou z nich stejné právní důsledky jako z podání doručených v listinné podobě. Některé z těchto písemností jsou zároveň elektronicky podepsány. Je proto nezbytné, aby se pracovníci úřadů naučili s písemnostmi v elektronické podobě zacházet a používat prostředky elektronické komunikace k jejich přijímání a doručování. Význam a množství úřední korespondence v elektronické podobě bude v budoucí době pouze narůstat.

V současnosti upravuje postupy úřadů při přijímání elektronických písemností pouze vyhláška o elektronických podatelnách [12] a nařízení vlády, kterým se provádí zákon o elektronickém podpisu [10]. Oba předpisy nabyly účinnosti dnem 1. ledna 2005 a ukládají úřadům některé nové povinnosti. Hlavním úkolem těchto předpisů je poskytnout návod pro úřady, které mají jinými předpisy uloženou povinnost přijímat a vypravovat elektronické úřední písemnosti. Tyto zásady navazují na oba zmíněné předpisy.

Nový správní řád [2], který nabude účinnosti dnem 1. ledna 2006, ještě značně rozšíří možnosti elektronické komunikace s úřady. V současné době upravují předpisy především komunikaci osob vůči úřadům, od uvedeného data budou mít správní orgány povinnost vydávat veřejné listiny (tedy především rozhodnutí) v elektronické podobě.

Elektronický podpis (dále „e-podpis") je velmi častou povinnou náležitostí právních úkonů, které osoby činí vůči úřadům v elektronické podobě. Mezi uživateli ale panuje značná nejasnost v tom, jak s e-podpisem zacházet, jak využít všech jeho vlastností a zároveň splnit požadavky na něj kladené zákonem o elektronickém podpisu [4]. Odpověď zkušenějším uživatelům by měly dát oba výše zmíněné prováděcí předpisy vydané k elektronickým podatelnám (dále „e-podatelnám"). I tyto zásady se soustřeďují na popis úkonů, které je s e-podpisem třeba provést při jeho přijetí. Čtenář se ovšem neobejde bez základních technických znalostí nebo schématického manuálu k aplikačnímu vybavení, které používá k přijímání pošty. Tento dokument se nesnaží být návodem k aplikačnímu softwaru, kterým mohou být uživatelé vybaveni, na vhodných místech je jen formou příkladu ukázáno, jak je možné daný krok provést v nejběžnějším programovém vybavení.

# Úvod

Zásady uvedené v tomto dokumentu jsou zpracovány tak, aby příslušné postupy byly v souladu se zákonem o elektronickém podpisu [4], vyhláškou o elektronických podatelnách [12] a nařízením vlády, kterým se provádí zákon o elektronickém podpisu [10]. Tyto předpisy upravují postup úřadů při přijímání a odesílání elektronicky podepsané písemnosti prostřednictvím e-podatelny, pokud pro ně ze zvláštních právních předpisů taková povinnost vyplývá. Pro tyto úřady je výhodné, aby tak činily u všech písemností v elektronické podobě, tedy i u těch, které elektronicky podepsané nejsou.

E-podatelna je informační systém (tedy technické vybavení, jeho obsluha, pravidla pro jeho fungování a vlastní data), který plní úlohu přijetí datové zprávy, jejího uložení, evidence, ověření některých náležitostí a předání k dalšímu vyřízení, a na druhé straně uložení a evidenci vypravovaných datových zpráv, jejich podepisování a odeslání. V tomto ohledu je efektivní přirovnání k běžné listovní podatelně. Zde se přijaté písemnosti evidují v podacím deníku, opatřují se podacím razítkem a předávají se k dalšímu vyřízení. Přirovnání e-podatelny k listovní podatelně může čtenáři pomoci pro vytvoření představy o pravidlech jejího fungování, neboť obě dvě odlišuje de facto pouze forma zpracovávaných písemností.

Uvedené právní předpisy nekladou na technické vybavení e-podatelny vysoké nároky. Zároveň upouští od konceptu zrušeného Standardu ISVS č. 016/01.01, tedy od požadavku, aby toto technické vybavení bylo atestováno. Nároky na jeho kvalitu si stanoví každý úřad. Jediné, co je třeba vzít v úvahu při jeho pořizování nebo vývoji, je to, zda daný informační systém:

- umožňuje přijímat datové zprávy prostřednictvím veřejné datové sítě ve zvoleném formátu a pomocí zvoleného protokolu,
- je možné navázat na antivirový systém ochrany,
- umožňuje ověřit e-podpis v souladu s vyhláškou o elektronických podatelnách [12],
- umožňuje ukládat datové zprávy, evidovat je a zobrazovat jejich obsah,
- je možné udržovat a jsou-li pro jeho obsluhu k dispozici příslušné návody,
- zaručuje přiměřenou úroveň ochrany zpracovávaných informací.

Některé požadavky, jako pořizování elektronického identifikátoru nebo evidování došlé pošty, je možné zajistit administrativně, některé lze provádět jen prostřednictvím IT. Je nutné, aby si profil požadavků na ICT e-podatelny stanovil každý úřad podle svých potřeb a možností.

Tento dokument má sloužit jako pomůcka pro ty e-podatelny, které budou fungovat na bázi přijímání e-mailových zpráv. Domníváme se, že v současné době se bude jednat o nejčastější případ. Cílem tohoto dokumentu ale není vyloučit jakékoliv jiné varianty fungování e-podatelny.

Na druhé straně budou ovšem existovat e-podatelny, které budou umožňovat přijímání XML struktur z webové aplikace, CRL a kvalifikované certifikáty budou stahovány automaticky do LDAP i vícekrát denně a programové vybavení e-podatelny bude distribuováno do serverových a klientských částí.

Tento dokument neřeší návaznost e-podatelny na ostatní ICT systémy organizace, jako je např. spisová služba.

Novela zákona o elektronickém podpisu [4], která stanovila povinnost úřadů přijímat a odesílat datové zprávy opatřené zaručeným e-podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem prostřednictvím e-podatelny, nabyla účinnosti 26. července 2004, vyhláška o elektronických podatelnách [12] a nařízení vlády, kterým se provádí zákon o elektronickém podpisu [10] jsou účinné od 1. ledna 2005. Plná

znění těchto právních předpisů jsou dostupná na webových stránkách Ministerstva informatiky.

Zde uváděné zásady vycházejí z praxe Ministerstva informatiky a z poznatků, které ministerstvo získalo od jiných subjektů. Ministerstvo informatiky uvítá Vaše případné zkušenosti a náměty, které můžete zasílat na adresu posta@micr.cz.

Návrh tohoto dokumentu byl zveřejněn na webových stránkách Ministerstva informatiky k veřejným připomínkám. Na jejich základě byly provedeny dílčí změny. V úvahu byly vzaty i příspěvky reagující na tento dokument, které byly zveřejněny na některých serverech, a dotazy, které ministerstvo obdrželo k e-podatelnám. Zohledněny byly i zkušenosti ministerstva s provozováním vlastních e-podatelen. Dále byly provedeny některé stylistické úpravy.

**Poznámka:**

Tento dokument není závazný a jeho charakter je pouze doporučující[1)].

Pokud jsou v tomto dokumentu použity pojmy „musí" nebo „je nutné" eventuelně „je nezbytné", pak se jedná:

- o povinnost stanovenou právním předpisem; v takovém případě je zpravidla uveden odkaz na příslušný právní předpis,
- o popis postupu, který nelze zajistit jiným způsobem.

[1)] Metodické dokumenty typu „best practice" jsou založeny na principu, že nejlepší cesta k poznání vede přes zkušenosti jiných. Ukazují cestu, jak něco konat na základě obecně přijímaného názoru, že určitý způsob řešení je z hlediska praxe považován za nejlepší. Dokumenty typu „best practice" však nevylučují, aby k dosažení cíle byla použita i jiná cesta.

# 1 Jak vyřizovat elektronickou poštu

## 1.1 Elektronická podatelna a spisový a skartační řád úřadu

### 1.1.1 E-podatelna je efektivním nástrojem pro přijímání/odesílání elektronické pošty.

E-podatelna je místem, které slouží k přijímání/vstupu a vypravování/výstupu elektronických písemností do/z úřadu. Pro úřady je klíčové nahlížet na e-podatelnu jako na alternativu listovní podatelny, neboť zde naleznou odpověď na většinu otázek, které pojem e-podatelny v uživatelích často vyvolává.

E-podatelnou je v kontextu tohoto dokumentu souhrn technického vybavení, umožňujícího připojit se prostřednictvím sítě na poštovní server e-podatelny, stáhnout elektronickou poštu do své e-mailové schránky v poštovním klientu, uložit a evidovat doručenou elektronickou poštu a postoupit ji k dalšímu vyřízení, dále obsluha e-podatelny a pravidla pro zacházení s elektronickými písemnostmi, nejčastěji ve formě spisového řádu a návodů pro obsluhu technického vybavení.

Obecně lze říci, že:

a) čím více úřad sjednotí postupy zpracování pošty v listinné podobě s postupy při zpracování elektronické pošty, tím srozumitelnější prostředí pro své pracovníky vytvoří,
b) čím více elektronické pošty bude do úřadu vstupovat prostřednictvím e-podatelny, tím menší budou „ztráty" této pošty, neboť došlá pošta bude podléhat jedné evidenci a bude s ní manipulovat omezený a kontrolovaný počet pracovníků, které není problém vyškolit. Obdobně to platí i pro poštu odesílanou. Bude-li došlá i odesílaná pošta procházet tímto jedním kanálem, bude možné jednoduše zkontrolovat, jak je došlá pošta vyřizována.

### 1.1.2 Nakládání s elektronickou poštou musí být upraveno ve spisovém a skartačním řádu [2)].

Spisový a skartační řád, jako základní předpis upravující oběh písemností v úřadu, je základním dokumentem, který definuje postupy pro práci s elektronickými písemnostmi. Je třeba, aby v něm úřad upravil, které datové zprávy jsou v působnosti spisového řádu a stávají se písemnostmi úřadu a které nikoli[3)]. Množinu těchto písemností můžeme definovat jako elektronickou poštu, která souvisí s výkonem kompetencí daného úřadu. Mezi datové zprávy, které není třeba považovat za písemnosti určené úřadu, bezpochyby patří soukromá sdělení adresovaná zaměstnancům úřadu, spam nebo interní e-mailová komunikace (např. komunikace mezi nadřízenými a podřízenými).

Elektronickou poštu nelze ze spisového řízení vyčlenit a považovat ji za zvláštní kategorii komunikace. Naopak je s ní třeba nakládat stejně obezřetně, a v souladu se spisovým a skartačním řádem, jako s poštou v listinné podobě. Pokud spisový a skartační řád nebo jiné

---

2) Zákon o archivnictví a spisové službě [6] § 66 odst. 2: „Určení původci vydají vnitřní předpis pro výkon spisové služby, který obsahuje základní pravidla pro manipulaci s dokumenty u určeného původce (dále jen „spisový a skartační řád")..."

3) Vyhláška o podrobnostech výkonu spisové služby [11] § 2 odst. 2: „...Určený původce uvede ve svém spisovém a skartačním řádu seznam dokumentů, které z hlediska jeho činnosti nejsou úředního charakteru; tyto dokumenty pak nepodléhají evidenci."

interní směrnice elektronickou poštu ignorují a příslušné postupy neupravují, nelze očekávat, že s ní bude náležitě nakládáno.

Vymezení toho, jaké datové zprávy podléhají spisovému řízení, je jistě prvním úkolem spisového řádu. Dalším úkolem je určení postupů pro jejich evidenci a vyřizování.

### 1.1.3 Postupy musí být upraveny jak pro poštu, která do úřadu vstupuje prostřednictvím e-podatelny, tak pro poštu, která dochází jednotlivým pracovníkům na jejich jména do jim přidělených e-mailových schránek[4)].

E-podatelna by měla být hlavním místem, kudy vstupují do úřadu elektronické písemnosti. Někdy se stává, že podání (žádosti, oznámení, stížnosti) doručují osoby nikoliv na adresu e-podatelny (např. posta@micr.cz), ale přímo do e-mailových schránek zaměstnanců. I v takovém případě musí písemnost projít e-podatelnou, protože právě zde musí dojít k její evidenci a k ověření e-podpisu, pokud je k datové zprávě přiložen [12]. Spisový a skartační řád musí pamatovat i na tuto situaci a ukládat zaměstnancům, aby písemnost do e-podatelny sami doručili. Zpráva musí být přeposlána včetně všech jejích součástí, kterými mohou být přílohy, ale i e-podpis, pokud jím je zpráva opatřena, a certifikát, je-li ke zprávě přiložen.

Přeposlání lze provést uložením dané datové zprávy ve formátu, který zachovává všechny její součásti (např. standardizovaný formát .eml, případně formát .msg), a následným odesláním této zprávy v příloze.

Přeposílat naopak není nutné datové zprávy, které jsou svým obsahem a rozsahem obdobou telefonického rozhovoru. Taková pošta se neeviduje. Pokud však má úřad zájem, aby určitý přehled o této poště existoval, může vést její evidenci například v rámci jednotlivých organizačních útvarů na nižší úrovni řízení (např. oddělení). Tato evidence může posloužit pro kontrolu, zda bylo na došlou poštu reagováno a zda se tak stalo bez zbytečného prodlení, nebo pro namátkovou kontrolu, jakým způsobem jsou požadavky, dotazy apod. vyřizovány. Je vhodné, aby tato došlá i odeslaná pošta byly ukládány tak, aby k nim měl přístup bezprostředně nadřízený pracovník (např. k tomuto účelu vyhrazený adresář se sdíleným přístupem).

Na straně zaměstnanců je pak třeba dbát na to, aby byly správně rozlišeny datové zprávy, které mají být evidovány a ukládány a které nikoliv. Spisový a skartační řád by měl toto rozlišení formulovat co nejjasněji, aby každý pracovník uměl bez problémů rozlišit, která z doručených zpráv podléhá spisové evidenci (zejména podání podle správního řádu či jiného předpisu, žádost o informaci podle zákona o svobodném přístupu k informacím [5], stížnost apod.) Dosavadní praxe ukazuje, že takových zpráv není mnoho. E-mailová komunikace je v převážné míře skutečně spíše obdobou uvedeného telefonického hovoru.

Doručování dokumentů či písemností, které mají úřední charakter, do e-mailových schránek zaměstnanců, je vždy komplikací a zbytečným zatížením úředního procesu. Vyloučit však tyto případy v praxi nelze. Navíc zde vždy existuje nebezpečí, že v důsledku nepřítomnosti pracovníka zůstane doručená datová zpráva po určitý čas nepovšimnuta. Preventivním opatřením je v této věci dobrá informovanost těch, kteří úřadu podání zasílají. Na webových stránkách úřadu je třeba jasně deklarovat, že pro doručování se používá daná

[4)] Vyhláška o podrobnostech výkonu spisové služby [11] § 1 odst. 6: „Pokud je v adrese na obálce dokumentu uvedeno na prvním místě jméno a příjmení fyzické osoby, předá se adresátovi, popřípadě jím určené osobě, neotevřená. Zjistí-li adresát po otevření zásilky, která mu byla takto doručena, že obsahuje dokument úředního charakteru, zabezpečí jeho dodatečné zaevidování a dále postupuje podle spisového a skartačního řádu určeného původce. Pokud je dokument úředního charakteru doručen v digitální podobě přímo do e-mailové schránky adresáta, postupuje se podle věty druhé obdobně."

adresa e-podatelny, jak tato e-podatelna na podání odpovídá apod. Občan tak získá konkrétní představu o způsobu, jak je jeho podání zpracováno, a má větší motivaci jej zaslat právě na tuto adresu místo odesílání dokumentů konkrétnímu zaměstnanci. O účinnosti podání doručených do personalizovaných e-mailových schránek zaměstnanců pojednává 1.1.4.

### 1.1.4 Úřad má možnost zřídit více e-podatelen pro příjem datových zpráv různého obsahu.

Úřad má možnost se rozhodnout, že zřídí více e-podatelen, z nichž každá je učena pro příjem datových zpráv předem stanoveného obsahu (např. pro příjem podání podle správního řádu, pro příjem žádostí o informace podle zákona o svobodném přístupu k informacím [5], pro příjem dotazů atd.) [10]. Dosavadní praxe však ukazuje, že takové opatření nemusí vždy přinést očekávaný efekt. Odesilatelé zpráv se často nezabývají tím, zda má úřad více e-podatelen, a zprávu zašlou na elektronickou adresu, kterou znají, nebo na první, kterou mají k dispozici (zpravidla na webových stránkách úřadu).

V této souvislosti je nutné si uvědomit, že odesilatel nemá zákonnou povinnost zasílat datové zprávy úřadu výlučně prostřednictvím e-podatelny, případně jedné z několika e-podatelen[5)]. Podání je zásadně učiněno v okamžiku, kdy se o něm úřad dozví, a tímto okamžikem se stává účinným[6)]. To znamená v době, kdy je přijato na jakoukoliv elektronickou adresu úřadu, nikoliv až tehdy kdy jej obdrží e-podatelna, případně e-podatelna, kterou úřad zřídil pro příjem zpráv určitého obsahu. Jiný postup by připadal v úvahu jen tehdy, pokud by některý zákon stanovil, že podání je účinné pouze tehdy, pokud je doručeno konkrétní e-podatelně.

Určitou výhodu mají úřady, které postupují podle právních předpisů stanovujících, že podání je možné podat pouze na jimi zveřejněném tiskopisu (např. daňová přiznání). E-podatelna (resp. aplikace), která taková podání přijímá, má možnost prakticky neumožnit zaslání jiného podání a naopak nabízí výhodu (zveřejněný formulář, event. další služby aplikace) těm, kteří ji využijí.

Pokud se tedy úřad rozhodne provozovat více e-podatelen, měl by najít způsob, jakým zainteresovat odesilatele, aby zaslal datovou zprávu na „správnou" e-podatelnu. Může to být forma adresy (stavebni_rizeni@urad.cz), příslib rychlé reakce (např. pokud svůj dotaz zašlete na adresu dotazy@urad.cz, vyřídíme jej do tří dnů) aj. Praktické zkušenosti při uplatnění takových postupů však prozatím nejsou.

V případě, že úřad provozuje více e-podatelen, může s ohledem na úspornost provozu interně stanovit, že pouze jedna z podatelen provede předepsané postupy při doručování datových zpráv (odeslání potvrzení o doručení apod.). V takovém případě, na těch e-podatelnách, které nebudou předepsané postupy provádět, musí dojít k uložení datové zprávy ve formátu, který zachová všechny její součásti (viz výše), a k jejímu odeslání na e-podatelnu, která tyto postupy provádět bude, ve formě přílohy.

---

5) Zákon o elektronickém podpisu [4], v § 11 odst. 3 stanoví, že orgán veřejné moci přijímá a odesílá datové zprávy prostřednictvím e-podatelny. Jedná se tedy o povinnost úřadů, nikoliv těch, kteří jim zprávy zasílají. Podle zákona č. 500/2004 Sb., správní řád, platí od 1. 1. 2006, že se podání činí u orgánu věcně a místně příslušného, přičemž e-podatelna není „orgánem", ale souborem technicko-organizačních pravidel (viz nařízení vlády, kterým se provádí zákon o elektronickém podpisu č. 495/2004 Sb.).

6) Zákon správní řád [2] § 37 odst. 6: „…Podání je učiněno dnem, kdy tomuto orgánu došlo."

### 1.1.5 Ve spisovém řádu je vhodné upravit nakládání s poštou, která je dodána na technickém nosiči (disketě, kompaktním disku atd.).

Je-li technický nosič přílohou pošty doručené v listinné podobě, je nezbytné, aby byl evidován jako její nedílná příloha a tak s ním bylo i nakládáno. Je-li doručen pouze technický nosič, je vhodné, aby byl evidován „klasickou" podatelnou jako zásilka, a předán e-podatelně ke zpracování datové zprávy uložené na tomto nosiči. S datovou zprávou se dále manipuluje obdobně, jako by byla doručena e-podatelně prostřednictvím sítě.

## 1.2 Životní cyklus doručené datové zprávy

### 1.2.1 Mezi odesilatelem datové zprávy a e-podatelnou musí být na straně úřadu „kontrolní mechanismus", kterým je antivirová ochrana včetně ochrany proti datovým zprávám, které mají chybný formát[7)].

Internet, který je hlavním prostředím pro připojení e-podatelen, je velmi málo regulovaným médiem. Každý z připojených uživatelů se zde vystavuje riziku neoprávněného přístupu do systému nebo zasažení škodlivým kódem[7)], a proto je nutné se těmto hrozbám bránit.

Úřad musí tedy před přijetím jakékoli datové zprávy do e-podatelny ověřit, zda daná zpráva neobsahuje škodlivý software nebo zda její formát nemůže poškodit její aktiva. Pokud by k této kontrole nedošlo a zprávy zasažené viry nebo jiným škodlivým kódem byly e-podatelnou přijaty, mohly by způsobit nenapravitelné škody. Takto zasažené zprávy mohou být uloženy jen mimo e-podatelnu, a to pouze tehdy, není-li tím ohrožena bezpečnost informačního systému úřadu ani bezpečnost zpracovávaných informací. Pokud je v možnostech úřadu tyto zprávy odděleně a bezpečně uložit, například do antivirových trezorů, je vhodné, aby uloženy byly, a tak byly k dispozici pro možnost případného řešení sporů a dokazování.

Je na uvážení úřadu, zda bude informovat odesilatele o přijetí takto poškozené datové zprávy. Doporučuje se však maximální obezřetnost, neboť řada „zavirovaných" zpráv při doručení „maskuje" elektronickou adresu odesilatele. V takovém případě by prosté „odpovězení" bylo zasláno na elektronickou adresu, ze které zpráva nebyla odeslána.

Datové zprávy, které neprošly úspěšně výše uvedenou kontrolou, nejsou považovány za doručené.

### 1.2.2 U doručených datových zpráv je nezbytné stanovit a zaznamenat čas jejich doručení.

V okamžiku, kdy datová zpráva dojde e-podatelně, je jí tzv. dostupná. To znamená, že e-podatelna zprávu přijala a může s ní dále nakládat (např. evidovat ji, ověřit e-podpis, pokud je připojen atd.). Za dostupnou se tedy považuje datová zpráva, pokud je uložena již na e-mailovém serveru ve schránce e-podatelny.

Pro některé další úkony je nutné určit a zaznamenat přesný čas doručení [12]. Jedná se o čas **doručení**, nikoliv čas počátku zpracování. Časem doručení může být například pátek 20:00:00 SEČ[8)], kdy byla datová zpráva e-podatelně doručena, i když bude poprvé otevřena až v pondělí na začátku pracovní doby. Úřad tedy musí počítat veškeré lhůty od času doručení.

---

7) Podle vyhlášky o elektronických podatelnách [12] se kontroluje výskyt počítačového programu, který je způsobilý přivodit škodu na informačním systému nebo na informacích zpracovávaných orgánem veřejné moci, nebo chybný formát přijaté datové zprávy (souhrnně „škodlivý kód").

8) Středoevropský čas, též CET (Central European Time).

Organizačně ani technicky nelze se 100% úspěšností zajistit, že podání budou na úřad docházet výhradně na e-podatelnu. Jak je popsáno v 1.1.3, bude se stávat, že podání přijdou přímo do e-mailové schránky zaměstnance úřadu. Tento zaměstnanec má pak povinnost přijatou datovou zprávu zaslat e-podatelně k zaevidování. Časem doručení bude i v tomto případě čas, kdy datová zpráva došla na e-mailový server, ze kterého si datovou zprávu do své e-mailové schránky zaměstnanec stáhl.

### 1.2.3 Způsob zacházení s nevyžádanými obchodními sděleními [3] (spam) by měl být upraven spisovým a skartačním řádem. Obecně platí, že nemusí podléhat spisovému řízení.

Zákon o některých službách informační společnosti [3] zakazuje všem subjektům, až na malé výjimky, šířit bez souhlasu adresáta obchodní sdělení. Tento nešvar způsobuje v současné době velmi podstatné zvýšení objemu dat přenášených po Internetu. Zpracování těchto dat v e-podatelnách může znamenat zbytečné zatížení jak technického vybavení, tak jeho obsluhy. Uvedený zákon o některých službách informační společnosti [3] nemůže ale spam z prostředí českého Internetu zcela odstranit, a proto je třeba problém řešit. Jednou z možností, která je v souladu s legislativou, je nastavit e-podatelnu tak, aby odmítala nevyžádaná obchodní sdělení a tyto datové zprávy nebyly e-podatelnou ukládány a evidovány. Podmínkou je, aby antispamový filtr byl dobře nastavený, a nemohlo se stát, že dojde k odmítnutí důležité písemnosti (např. podání).

Ačkoli se to může zdát jednoduché, vždy zde bude určité riziko odmítnutí platného podání, a proto může úřad uvážit také druhou variantu. Tou je přijímání i obchodních sdělení od odesilatelů, kteří nejsou na tzv. opt-in seznamu, a následné posouzení těchto sdělení, tj. zda se budou dále zpracovávat nebo budou odmítnuta a případně bude upozorněn Úřad pro ochranu osobních údajů na jejich doručení. V každém případě se doporučuje použít určitý filtr, který rozdělí doručenou poštu na platné písemnosti a spam (ten poté může být předmětem posouzení, odstranění, nebo i následného zpracování). Zvolené řešení je vhodné popsat ve spisovém a skartačním řádu. Pro použití konkrétního filtru a jeho nastavení je nutné se dobře seznámit s funkcemi daného filtru, případně konzultovat použití s dodavatelem.

### 1.2.4 Doručené datové zprávy se ukládají do úložiště doručených datových zpráv ve tvaru, ve kterém byly přijaty, včetně všech příloh a případných jiných součástí.

Je-li k datové zprávě připojen kvalifikovaný certifikát a zaručený e-podpis založený na tomto certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále „uznávaný e-podpis“) nebo kvalifikovaný systémový certifikát[9]) a elektronická značka založená na tomto certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále „uznávaná e-značka“), ukládají se spolu se zprávou [12].

Používá-li úřad pro stažení pošty z poštovního serveru např. poštovní klient MS Outlook Office, je třeba pro uložení datové zprávy použít formát, který zachovává všechny vlastnosti dané zprávy. V tomto případě se jedná o formát .msg. Při použití ostatních e-mailových klientů je možno zprávu uložit ve formátu .eml.

Pokud je k datové zprávě připojen jiný druh e-podpisu nebo certifikátu, je vhodné je také uložit spolu se zprávou (jsou její součástí), i když není nutné s nimi dále pracovat a ověřovat jejich platnost.

[9]) Zjednodušeně: kvalifikovaný certifikát je vydáván pro fyzickou osobu, která se bude jménem úřadu podepisovat. Kvalifikovaný systémový certifikát se vydává (resp. bude vydávat, dosud se nevydávají) pro úřad. Je obdobou razítka úřadu.

Pro zajištění bezpečnosti úložiště a datových zpráv, které jsou v něm uloženy, je nutné aby:

- byla data zálohována a zabezpečena proti ztrátě a neoprávněnému pozměnění,
- byli určeni pracovníci, kteří mají do úložiště přístup a odpovídají za ně.

### 1.2.5 Datové zprávy se v e-podatelně evidují a opatřují identifikátorem e-podatelny.

Doručené datové zprávy se v e-podatelně evidují v souladu se spisovým a skartačním řádem úřadu. Kromě obvyklých náležitostí takové evidence se zaznamenává přesný čas doručení, a to s přesností na sekundu. Tento údaj má zásadní význam při ověřování platnosti uznávaného kvalifikovaného certifikátu[10)], jak je vysvětleno v 1.2.7.

Evidence může být jak v elektronické (v praxi častější, jelikož ji lze nezpochybnitelným způsobem navázat na elektronickou poštu), tak i v listinné podobě, pokud je úřad schopen zajistit jednoznačný vztah mezi listinnými záznamy o elektronické poště a elektronickou poštou jako takovou (odkazem na číslo hlavičky datové zprávy, identifikací jejího odesilatele a přesného času doručení apod.).

Následně je datová zpráva opatřena identifikátorem e-podatelny [12], který je obdobou podacího razítka. Jeho účelem je zachytit informace o dané zprávě pro další řízení, a to zejména informace týkající se e-podpisu, případně časového razítka. Důležité je, aby identifikátor obsahoval výsledek ověření platnosti e-podpisu (viz 1.2.8) a zmíněný čas doručení. Je žádoucí, aby zaznamenání uvedených informací proběhlo co nejdříve po doručení datové zprávy. Nezjistí-li úřad předmětné skutečnosti a nezaznamená je do identifikátoru, bude je následně velmi obtížně získávat, eventuelně dokazovat.

Forma identifikátoru není předepsána, ale je výhodné, pokud je v elektronické podobě. Úřady, které přijímají datové zprávy ojediněle, jej mohou pořizovat i v listinné formě v rámci jejich listinné evidence. V každém případě je nutné dbát na bezpečnost údajů, které jsou v identifikátoru uvedeny. Platí zde stejné zásady jako pro úložiště doručených zpráv.

### 1.2.6 Doručení datové zprávy e-podatelna potvrzuje odesilateli zasláním zprávy o doručení.

Učiní tak v případě, že je možné z doručené datové zprávy zjistit elektronickou adresu odesilatele.

Potvrzení musí obsahovat [12]:

- datum a čas s uvedením hodiny, minuty a sekundy, kdy byla datová zpráva doručena (čas doručení včetně sekundy je uveden v hlavičce zprávy, většinou ji lze zobrazit v možnostech dané zprávy),
- charakteristiku doručené datové zprávy umožňující její identifikaci (např. číslo jednací nebo jiný identifikační znak, hash, případně i plný text doručené zprávy).

Potvrzení by mělo být podepsáno uznávaným e-podpisem pracovníka e-podatelny nebo uznávanou e-značkou úřadu[11)]. Toto je důležité pro právní jistotu odesilatele. Prostředí

---

10) V oblasti orgánů veřejné moci lze podle §11 zákona o elektronickém podpisu [4] za účelem podpisu používat jen kvalifikované certifikáty vydané akreditovaným poskytovatelem certifikačních služeb.

11) Ne všechny produkty, které jsou pro elektronickou poštu užívány, umožní podepsání/označení datové zprávy ve smyslu zákona o elektronickém podpisu. Používáte-li například e-mailovou schránku na webu freemailu (např. na Seznamu, Centru, Atlasu apod.), kontaktujte provozovatele a vyžádejte si příslušné informace. Pokud na svém webovém rozhraní provozovatel tyto služby neposkytuje, je možné použít pro stažení a další práci se zprávami prostřednictvím těchto serverů e-mailový klient-např. MS Outlook, Mozilla Thunderbird, které již podepisování a ověřování podpisu umožňují.

Internetu nedává záruky za doručení, proto by mělo být doručení pokaždé potvrzeno. Je to obdoba potvrzení doručení listovního podání "klasické" podatelně, například ve formě razítka podatelny na kopii písemnosti.

V případě, že je takto reagováno na datovou zprávu, která byla doručena s uznávaným e-podpisem nebo uznávanou e-značkou, je toto podepsání/označení podle vyhlášky o elektronických podatelnách [12] povinné.

Příklad datové zprávy, kterou se doručení potvrzuje, je uveden v Příloze č. 2.

### 1.2.7 E-podatelna zjišťuje a zaznamenává náležitosti doručených datových zpráv, tedy především vlastnosti e-podpisu. Pro tento krok musí být obsluha e-podatelny proškolena.

Tato činnost je pro pracovníky e-podatelen poměrně nová a v řadě případů je dosud prováděna nesprávně nebo neúplně. Z tohoto důvodu je zde popsána detailně. Je třeba poznamenat, že následující řádky jsou určeny především poučeným laikům, projektantům softwaru pro e-podatelny nebo informatikům, kteří by měli nastavit software e-podatelny ke správnému fungování a proškolit obsluhu. Méně zkušený čtenář si bude muset vzít na pomoc příručky nebo osobu uvedenou v předchozí větě.

**Zjišťuje se, zda datová zpráva odpovídá technickým parametrům, které úřad stanovil jako přípustné.**

Každá e-podatelna má určité programové vybavení, které ve větší nebo menší míře omezuje škálu datových zpráv, které je schopná zpracovávat. Je tedy důležité, aby každý úřad popsal, jaké technické náležitosti musí mít doručované písemnosti, a tuto informaci zveřejnil na svých webových stránkách nebo na jiném veřejném a navštěvovaném místě [10]. Mezi tyto informace musí bezpochyby patřit formát datových zpráv, případně jejich velikost. Každý úřad vybavený ICT by jistě měl umět otevřít a pracovat se soubory ve formátu pdf, txt, html.

**Zjišťuje se, zda je k datové zprávě připojen uznávaný e-podpis nebo uznávaná e-značka[12)], případně zda je připojeno kvalifikované časové razítko.**

Uznávaná e-značka a kvalifikované časové razítko budou v současné době k datovým zprávám připojeny pouze výjimečně, protože novela zákona o elektronickém podpisu [4] jejich užívání umožnila, ale žádný jiný právní předpis zatím nestanovil povinnost jejich užívání pro konkrétní typy podání. E-podpis bude stále běžnější součástí přijímaných datových zpráv. E-podatelna by za účelem práce s e-podpisem měla být vybavena aplikací, která dokáže pracovat s kryptografickými funkcemi operačního systému, uloženými v tzv. kryptografickém jádře OS, a která umí pracovat s formátem .p7s podle normy PKCS#7. Běžné kancelářské softwarové balíky, které v sobě mají poštovního klienta, tyto požadavky bez problémů splňují. V návodu k nim je možné nalézt i popis kroků vedoucích ke zjištění, zda je e-podpis k doručené zprávě připojen, či nikoliv.

---

12) Novela zákona o elektronickém podpisu [4] zavedla pojem „uznávaný elektronický podpis" pro zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Protože nejde ověřit uznávaný elektronický podpis jako celek, ale je nutné zvlášť ověřit zaručený elektronický podpis a zvlášť kvalifikovaný certifikát, je v dalším textu používán při ověřování pojem „zaručený elektronický podpis". Obdobně platí pro „uznávanou elektronickou značku", tj. elektronickou značku založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

**Zjišťuje se, zda je zaručený e-podpis platný a zda jeho kvalifikovaný certifikát nebyl zneplatněn nebo e-značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn, případně zda je platné kvalifikované časové razítko.**

Řada produktů, které jsou popsané výše v textu, umožňuje, aby ověření platnosti zaručeného e-podpisu nebo e-značky provedla aplikace sama a ohlásila, pokud podpis platný není[11)].

Naopak to, jestli kvalifikovaný certifikát nebyl zneplatněn, musí ověřit u každé datové zprávy samostatně pracovník e-podatelny. Dále uvádíme, jakým způsobem se toto ověření může provést[13)].

Kvalifikované certifikáty vydávají poskytovatelé certifikačních služeb[14)] s platností na jeden rok a doba platnosti je v nich v vyznačena v okem čitelné podobě[15)].

Pokud by byl k datové zprávě přiložen certifikát starší než jeden rok, aplikace sama ohlásí, že na certifikát nelze spoléhat.

Ten, komu byl certifikát vydán, však může poskytovatele požádat, aby v průběhu tohoto roku jeho certifikát zneplatnil. Údaj o zneplatnění se v certifikátu neobjeví, tj. doba platnosti zůstane vyznačena tak, jak byla uvedena při vydání certifikátu (jeden rok). Jediným zdrojem, ze kterého je možné věrohodnou informaci o zneplatnění získat, je Seznam zneplatněných kvalifikovaných certifikátů, často označovaný jako CRL. I.CA tento seznam zveřejňuje na adrese http://www.ica.cz/seznam_znepl_cert.html (klikněte na uvedené webové stránce na „Žádosť"), a na dalších adresách, uvedených v certifikátu, v položce Distribuční místo seznamu odvolaných certifikátů. U každého certifikátu, který byl zneplatněn, se zveřejňuje jeho číslo a dále datum a čas, kdy byl zneplatněn. Záznam vypadá následovně:

Serial Number: 989F37
Revocation Date: Jul 25 07:58:30 2003 GMT

Z tohoto záznamu vyplývá, že od uvedeného data a času (včetně) nelze na certifikát uvedeného čísla spoléhat, a nelze tedy e-podpis vytvořený po tomto čase považovat za platný. Proč? Protože existuje reálné nebezpečí, že se podepisovacího prostředku někdo neoprávněně zmocnil a „podepsal" se místo oprávněného majitele tohoto prostředku. Právě ztráta kontroly nad tímto prostředkem je nejčastějším důvodem pro zneplatnění certifikátu.

Seznam zneplatněných certifikátů je možné i přímo nainstalovat do operačního systému, i v tomto případě je však nutné zkontrolovat, kdy byl daný seznam vydán ve vztahu k času doručení datové zprávy.

Čas, ke kterému se platnost kvalifikovaného certifikátu ověřuje, je čas doručení datové zprávy. Je to totiž jediný čas, který může pracovník e-podatelny brát jako důvěryhodný.

---

13) Pokročilejší uživatelé, a především obsluha e-podatelen, které přijímají větší objemy elektronicky podepsaných zpráv, si s největší pravděpodobností nastaví pravidelné stahování CRL.

14) Též: certifikační autority. Pro komunikaci „v oblasti veřejné moci" stanoví zákon o elektronickém podpisu povinnost používat pouze kvalifikované certifikáty nebo kvalifikované systémové certifikáty, které vydal akreditovaný poskytovatel. Tím je v současné době pouze První certifikační autorita, a. s. (I.CA).

15) Součástí údaje o době platnosti je časový údaj uvedený s přesností na sekundu. Je-li u časového údaje zkratka GMT (Greenwich Mean Time), jedná se o čas na nultém poledníku v Greenwichi (Londýn). GMT je univerzální časová jednotka, jednotlivé časové zóny se určují posunem proti času GMT. Hodnota SEČ (středoevropský čas, také CET – Central European Time) je GMT+1. Letní čas je oproti běžnému času posunutý o 1 hodinu dopředu. K přechodům mezi časy dochází poslední neděli v říjnu (-1 h) a poslední neděli v březnu (+1 h).

Upozornění! I.CA vydává Seznam zneplatněných kvalifikovaných certifikátů každých 12 hodin[16)]. Uveďme si příklad: certifikát byl zneplatněn v 10 hodin, následně byl použit (patrně neoprávněně) a zaslán spolu s datovou zprávou e-podatelně. Ta jej ověřuje například v 11 hodin. Je bezpředmětné hledat v seznamu, který I.CA vydala ve 4 hodiny, logicky zde tato informace ještě nemůže být. Je tedy nutné s ověřením počkat, až bude vydán seznam v 16 hodin, ve kterém naopak příslušná informace být musí.

Pokud tedy pracovník e-podatelny zjistí, že:

- aplikace (poštovní klient) ohlásila, že e-podpis je neplatný, protože došlo ke změně obsahu podepsaných dat, neboli k porušení integrity, nebo
- certifikát, na jehož základě je e-podpis vytvořený, přestal být platný ještě před časem doručení datové zprávy, nebo
- certifikát se nachází na seznamu zneplatněných certifikátů s časem zneplatnění, který předchází času doručení, nebo
- aplikace ohlásí, že certifikát není důvěryhodný, protože nejsou důvěryhodné certifikáty v jeho certifikační cestě, nebo
- CRL není důvěryhodné, protože certifikáty v jeho certifikační cestě nejsou důvěryhodné,

pak je výsledkem ověření e-podpisu výrok, že e-podpis je neplatný a tuto skutečnost je nutné napsat do identifikátoru e-podatelny. I v tomto případě je nutné zaznamenat údaj o tom, zda certifikát podepisující osoby je kvalifikovaný a zda jej vydal akreditovaný poskytovatel certifikačních služeb. Tyto informace jsou uvedeny v certifikátu.

Důsledky neplatnosti e-podpisu dovodí odborný referent, který danou písemnost zpracovává. Nutné však je, aby se o této skutečnosti dozvěděl. Zdrojem informací jsou pro něj údaje zaznamenané v identifikátoru (viz 1.2.8).

Pokud všechna uvedená ověření skončí dobře, tj. s kladným výsledkem, je možné považovat e-podpis za platný.

Veškerému výše popsanému ověřování předchází jeden krok, který spočívá v instalaci certifikačních cest. Jedná se o instalaci certifikátů, které jsou nadřazeny certifikátu podepisující osoby a příslušnému CRL.

Jak už bylo uvedeno, čas, ke kterému se platnost certifikátu ověřuje, je čas doručení datové zprávy. Ojediněle může dojít k situaci, že e-podatelna zjistí, že kvalifikovaný certifikát byl v době doručení datové zprávy neplatný, ale lze usuzovat, že zaručený e-podpis byl vytvořen v době platnosti tohoto certifikátu. Například: v podepsané zprávě je uvedeno, že byla odeslána v 8:00 hodin (z toho usuzujeme, že podpis byl vytvořen před tímto časem), certifikát byl zneplatněn v 8:03 a ověřování probíhá 8:10 hodin. Úřad nemůže na takový certifikát spoléhat, protože nemá k dispozici věrohodný údaj, kdy byla skutečně zpráva podepsána (s časem odeslání lze lehce manipulovat, takže podpis mohl být vytvořen i v 8:05).

V tomto případě by úřad mohl na certifikát spoléhat, pokud by bylo k datové zprávě připojeno platné kvalifikované časové razítko a toto razítko by bylo vytvořeno před okamžikem zneplatnění certifikátu datové zprávy (pro uvedený příklad dříve než v 8:03).

Pokud by platné časové razítko k datové zprávě připojeno nebylo, úřad uvědomí podepsanou osobu, že nemá možnost provést veškeré úkony potřebné k tomu, aby ověřil, že zaručený e-podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn před vytvořením zaručeného e-podpisu. Se zprávou je tedy nutné nakládat tak, jako by podepsána nebyla.

---

16) Nejedná se o nedostatek na straně I.CA, ale o běžnou praxi. Standardy EU dokonce připouštějí vydávání těchto seznamů každých 24 hodin. V budoucnu se patrně rozšíří používání OCSP (Online Certificate Status Protocol), který umožní zjišťovat aktuální stav jednotlivých certifikátů bez zpoždění.

Ověření platnosti e-značky a kvalifikovaného systémového certifikátu probíhá obdobně jako ověření platnosti e-podpisu a kvalifikovaného certifikátu.

Výjimečně se může stát, že datová zpráva je podepsána zaručeným e-podpisem, ale kvalifikovaný certifikát připojen není. V takovém případě je odesilatel povinen uvést akreditovaného poskytovatele, který certifikát vydal a vede jeho evidenci. V současné době je určení akreditovaného poskytovatele jednoduché – akreditaci získala pouze I.CA. Seznam kvalifikovaných certifikátů, které vydala, je dostupný na adrese http://www.ica.cz/seznam_ver_cert.html a zde je možné si certifikát prohlédnout.

**Zjišťuje se, zda kvalifikovaný certifikát obsahuje údaje, na jejichž základě je možné osobu, která podepsala datovou zprávu, jednoznačně identifikovat.**

Toto ověřování má smysl pouze v případě uznávaného e-podpisu, tedy v případě kvalifikovaného certifikátu. V současné době se jako tento údaj používá pouze identifikátor Ministerstva práce a sociálních věcí, který I.CA bezplatně do kvalifikovaných certifikátů vkládá[17)], pokud o to žadatel o certifikát požádá. Identifikátory tohoto ministerstva má I.CA k dispozici.

### 1.2.8 Výsledky jednotlivých zjištění se zapisují do identifikátoru e-podatelny.

V souhrnu si můžeme vyjmenovat, které údaje se do identifikátoru musí zaznamenávat [12]:

- datová zpráva odpovídá technickým parametrům – ANO x NE
- je připojen uznávaný elektronický podpis – ANO x NE
- je připojena uznávaná elektronická značka – ANO x NE
- je připojeno kvalifikované časové razítko – ANO x NE
- zaručený elektronický podpis[12)] je platný – ANO x NE
- jeho kvalifikovaný certifikát nebyl zneplatněn – ANO x NE x zatím nebyl vydán odpovídající CRL
- elektronická značka je platná – ANO x NE
- její kvalifikovaný systémový certifikát nebyl zneplatněn – ANO x NE x zatím nebyl vydán odpovídající CRL
- připojené kvalifikované časové razítko je platné – ANO x NE
- je připojen kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát – ANO x NE
- je uveden akreditovaný poskytovatel, který certifikát vydal a vede jeho evidenci – ANO x NE
- obsahuje kvalifikovaný certifikát údaje, na jejichž základě je možné osobu, která podepsala datovou zprávu, jednoznačně identifikovat – ANO x NE

případně:

- bylo odesláno potvrzení o doručení datové zprávy – ANO x NE
- bylo odesláno sdělení, že úřad nemá možnost provést veškeré úkony potřebné k tomu, aby ověřil, že zaručený elektronický podpis nebo elektronická značka jsou platné a jejich kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nebyly zneplatněny před vytvořením zaručeného elektronického podpisu nebo elektronické značky – ANO x NE.

17) Tento údaj je uveden v alternativním názvu předmětu v certifikátu, v položce „jiné jméno".

E-podatelna tyto skutečnosti zjistí a zapíše do identifikátoru, ale dále se jimi nezabývá. Pokud úřad nestanoví interním předpisem jinak, e-podatelna tedy nezjišťuje, zda datová zpráva měla být podle zvláštního právního předpisu podepsána uznávaným e-podpisem, zda mělo být připojeno kvalifikované časové razítko atd. Pouze uvedené skutečnosti konstatuje a předává je k řešení příslušným útvarům, které se vyřízením obsahu zprávy zabývají. Údaj o skutečnosti, jestli se certifikát nenachází na CRL, může být v průběhu vyřizování obsahu zprávy doplněn, aby nedošlo ke zbytečným prodlevám. V takovém případě by však neměla z úřadu odejít odpověď na danou zprávu dříve (pokud právní předpis vyžaduje uznávaný e-podpis nebo uznávanou e-značku), než dojde ke správnému ověření (pokud neexistuje nebezpečí z prodlení, např. ohrožení života).

### 1.2.9 Po splnění všech výše uvedených úkonů e-podatelna předává datovou zprávu příslušným útvarům úřadu k vyřízení.

Je na rozhodnutí úřadu, a tedy úpravě ve spisovém a skartačním řádu, zda je datová zpráva předána v elektronické podobě nebo vytištěna a předána v listinné podobě. V takovém případě musí být vytištěn a ke zprávě připojen i identifikátor e-podatelny, ve kterém jsou uvedeny všechny předepsané údaje. Údaje o času doručení, ověření e-podpisu a jiné údaje, které identifikátor obsahuje, totiž mohou mít pro další vyřizování zásadní význam.

V každém případě musí být datová zpráva uložena v elektronické podobě ve tvaru, ve kterém byla přijata [12].

## 1.3 Životní cyklus odesílané datové zprávy

### 1.3.1 Datová zpráva, která je z úřadu odesílána, se v e-podatelně ukládá do úložiště vypravených datových zpráv ve tvaru, ve kterém byla odeslána.

Pokud je k datové zprávě připojen uznávaný e-podpis oprávněného zaměstnance úřadu a jeho kvalifikovaný certifikát nebo uznávaná e-značka úřadu a její kvalifikovaný systémový certifikát, ukládají se spolu se zprávou [12].

Podepsat datovou zprávu uznávaným e-podpisem může pouze zaměstnanec, který je k tomu oprávněn. Na rozdíl od podepisování potvrzení o doručení zprávy, které bude zpravidla podepisovat pracovník e-podatelny, se zde bude jednat o podpis pracovníka, který je oprávněn takto stvrdit určitý úkon úřadu[18)]. Pokud tak úřad stanoví, může být odesílaná zpráva včetně tohoto podpisu, „přepodepsána" jako celek pracovníkem e-podatelny. Tím stvrdí, že zprávu z e-podatelny odeslal se všemi jejími součástmi.

Před odesláním z úřadu prochází datová zpráva kontrolou, zda neobsahuje škodlivý kód[7)].

Odesílaná datová zpráva se v e-podatelně eviduje v souladu s vnitřními předpisy úřadu, které upravují evidenci vypravovaných písemností. Čas odeslání zprávy je zaznamenán s přesností na sekundu.

[18)] Vydávání rozhodnutí a jiných obdobných úkonů v elektronické podobě a elektronicky podepsaných připadá v úvahu po nabytí účinnosti nového správního řádu [2].

## 1.4 Zveřejňování údajů

### 1.4.1 Aby ti, kdo elektronickou poštu na úřady zasílají, měli k dispozici potřebné údaje, ukládá nařízení vlády, kterým se provádí zákon o elektronickém podpisu [10], úřadům povinnost příslušné údaje zveřejnit.

Jedná se o tyto údaje:

a) elektronická adresa e-podatelny (e-mail, případně url) a informace o tom, zda je e-podatelna určena výhradně pro příjem datových zpráv určitého obsahu (např. daňová přiznání), nebo nikoliv,
b) kontaktní údaje pro přijímání datových zpráv na technických nosičích (adresa, úřední hodiny apod.),
c) případné další možnosti doručování datových zpráv (pokud existují), zejména prostřednictvím technického zařízení v sídle úřadu nebo v jeho organizačních jednotkách,
d) pravidla pro potvrzování doručení datových zpráv (např. max. doba, která může uplynout od přijetí zprávy do odeslání potvrzení) a vzor zprávy, kterou se doručení potvrzuje,
e) technické parametry:
   - datových zpráv, pro jejichž přijetí má e-podatelna technické a programové vybavení (např. rtf, doc, pdf, jpg nebo html, dále se může jednat o komunikační protokoly); některé úřady preferují jimi zveřejněné elektronické formuláře (např. Automatizovaný daňový informační systém, žádosti o dávky státní sociální podpory) – nastavení se odvozuje od vybavení daného úřadu a od požadavků (např. bezpečnostních) na provoz ICT,
   - technických nosičů, na nichž lze předávat datové zprávy,
f) postup v případě, že u přijaté datové zprávy je zjištěn škodlivý software nebo chybný formát zprávy,
g) způsob, jakým jsou vyřizovány dotazy týkající se provozu e-podatelny, včetně kontaktních údajů (e-mailová adresa, telefon apod.),
h) aktuální seznam zaměstnanců, kterým byly vydány kvalifikované certifikáty,
i) seznam právních předpisů, podle kterých je možné vůči úřadu činit právní úkony v elektronické podobě a náležitosti těchto úkonů, zejména náležitosti týkající se použití uznávaného e-podpisu.

Podle dosavadních zkušeností s provozem e-podatelen není jejich vnějším uživatelům často zřejmé, jaké právní úkony lze vůči úřadu činit elektronicky, má-li být použit e-podpis, a pokud ano, jaký typ e-podpisu a certifikátu musí pro daný účel použít (je vždy upraveno příslušným právním předpisem, který se daného úkonu týká). Příklad zveřejňovaných informací je uveden v Příloze č. 2.

V této souvislosti je nutné zdůraznit, že úřad není oprávněn omezovat druhou stranu v úkonech, které hodlá činit elektronicky. Pokud tedy právní předpis stanoví, že určitý úkon vůči úřadu je možné činit elektronicky, úřad musí pro příjem takových datových zpráv vytvořit příslušné podmínky. Na druhé straně není úřadu bráněno v tom, aby umožnil příjem i jiných datových zpráv, například takových, jejichž náležitosti nejsou právními předpisy upraveny. Naopak v elektronické podobě nelze přijímat taková podání, u nichž právní předpis výslovně stanoví povinnost přijímat je pouze v klasické listinné podobě, nebo stanoví takové podmínky, že je nelze provést elektronicky (např. úředně ověřený podpis).

# Seznam použitých právních předpisů


1. Zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění zákona č. 29/2000 Sb., zákona č. 227/2000 Sb., zákona č. 226/2002 Sb. a zákona č. 309/2002 Sb.
2. Zákon č. 500/2004 Sb., správní řád.
3. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).
4. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb., zákona č. 517/2002 Sb., zákona č. 440/2004 Sb., zákona č. 635/2004 Sb. a zákona č. 501/2004 Sb.
5. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím ve znění zákona č. 101/2000 Sb., zákona č. 159/2000 Sb. a zákona č. 39/2001 Sb.
6. Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.
7. Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění zákona č. 273/2001 Sb., zákona č. 450/2001 Sb., zákona č. 320/2001 Sb., zákona č. 313/2002 Sb. (část), zákona č. 311/2002 Sb., zákona č. 313/2002 Sb., zákona č. 59/2003 Sb., zákona č. 22/2004 Sb., zákona č. 216/2004 Sb., zákona č. 257/2004 Sb., zákona č. 421/2004 Sb., zákona č. 626/2004 Sb., zákona č. 501/2004 Sb.
8. Zákon č. 565/1990 Sb., o místních poplatcích, ve znění zákona č. 184/1991, zákona č. 338/1992 Sb., zákona č. 48/1994 Sb., zákona č. 305/1997 Sb., zákona č. 149/1998 Sb., zákona č. 185/2001 Sb., zákona č. 274/2001 Sb., zákona č. 320/2002 Sb., zákona č. 229/2003 Sb.
9. Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění zákona č. 35/1993 Sb., zákona č. 157/1993 Sb., zákona č. 302/1993 Sb., zákona č. 315/1993 Sb., zákona č. 323/1993 Sb., zákona č. 85/1994 Sb., zákona č. 255/1994 Sb., zákona č. 59/1995 Sb., zákona č. 118/1995 Sb., zákona č. 323/1996 Sb., zákona č. 61/1997 Sb., zákona č. 242/1997 Sb., zákona č. 168/1998 Sb., zákona č. 91/1998 Sb., zákona č. 29/2000 Sb., zákona č. 159/2000 Sb., zákona č. 227/2000 Sb., zákona č. 218/2000 Sb., zákona č. 367/2000 Sb., zákona č. 492/2000 Sb., zákona č. 120/2001 Sb., zákona č. 271/2001 Sb., zákona č. 320/2001 Sb., zákona č. 226/2002 Sb., zákona č. 320/2002 Sb., zákona č. 322/2003 Sb., zákona č. 354/2003 Sb., zákona č. 438/2003 Sb., zákona č. 479/2003 Sb., zákona č. 440/2003 Sb., zákona č. 19/2004 Sb., zákona č. 237/2004 Sb., zákona č. 254/2004 Sb., zákona č. 436/2004 Sb., zákona č. 554/2004 Sb., zákona č. 501/2004 Sb.
10. Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.
11. Vyhláška č. 646/2004 Sb., o podrobnostech výkonu spisové služby.
12. Vyhláška č. 496/2004 Sb., o elektronických podatelnách.
13. Vládní vyhláška č. 150/1958 Ú. l., o vyřizování stížností, oznámení a podnětů pracujících.

# Slovník použitých pojmů a zkratek

**Akreditovaný poskytovatel certifikačních služeb** – poskytovatel certifikačních služeb, který získal od Ministerstva informatiky akreditaci podle zákona o elektronickém podpisu; pouze akreditovaný poskytovatel může vydávat certifikáty pro vytváření takových e-podpisů a e-značek, které lze používat v oblasti orgánů veřejné moci (§ 11 zákona o elektronickém podpisu). Důvodem udělování akreditace je, aby měl stát možnost ověřit, zda činnost poskytovatelů certifikačních služeb je dostatečně důvěryhodná.

*též*[19]*: Zákon o elektronickém podpisu [4] § 2 písm. j), § 10, § 10a*

**Poskytovatel certifikačních služeb** (též: certifikační autorita, poskytovatel) – obecně subjekt, který vydává certifikáty a případně zajišťuje další služby spojené s e-podpisy a/nebo e-značkami. Na poskytovatele se zákon o elektronickém podpisu vztahuje pouze tehdy, pokud vydávají kvalifikované certifikáty a/nebo poskytují další kvalifikované služby podle tohoto zákona.

*též: Zákon o elektronickém podpisu [4] § 2 písm. h)*

**Kvalifikovaný poskytovatel certifikačních služeb** – poskytovatel certifikačních služeb, který oznámil Ministerstvu informatiky, že vydává kvalifikované certifikáty, případně poskytuje jiné kvalifikované služby podle zákona o elektronickém podpisu. Certifikáty kvalifikovaného poskytovatele certifikačních služeb nelze používat za účelem podpisu při komunikaci s úřady, dokud tento poskytovatel nezíská akreditaci.

*též: Zákon o elektronickém podpisu [4] § 2 písm. i)*

**Antivirový trezor** (též: virový trezor) – místo (adresář), kam lze přesunout infikované či podezřelé soubory nalezené testem a kam systém případně odkládá záložní kopie „léčených" objektů.

**CRL (**angl. **C**ertificate **R**evocation **L**ist**)** – seznam certifikátů, které byly zneplatněny. Certifikáty jsou vydávány na určité období, např. na dobu jednoho roku. Tato doba (od-do) je v certifikátu uvedena. V průběhu uvedené doby může nastat okolnost, která vlastníka certifikátu vede k tomu, že musí poskytovatele požádat, aby certifikát zneplatnil. Takovými okolnostmi jsou například: změna údajů, které jsou v certifikátu uvedeny (např. změna příjmení u provdaných žen nebo změna funkce v rámci organizace) nebo situace, kdy má vlastník certifikátu obavu, že jeho podepisovací data mohou být zneužita (např. ztráta notebooku, na jehož pevném disku byla tato data uložena). Pokud poskytovatel certifikát zneplatní, zařadí příslušnou informaci do seznamu certifikátů, které byly zneplatněny. Ve vlastním certifikátu však v údaji o době platnosti k žádné změně nedojde. Seznam zneplatněných certifikátů obsahuje sériová čísla zneplatněných certifikátů, přesnou dobu zneplatnění certifikátu a údaj o době, kdy byl příslušný seznam zneplatněných certifikátů vydán. Tento seznam je elektronicky označen e-značkou poskytovatele certifikačních služeb.

*též: Zákon o elektronickém podpisu [4] § 6a odst. (1) písm. f)*

**Certifikační cesta** – hierarchie certifikátů, kterou je nutné postupovat při ověřování certifikátu. Certifikát, který přijde spolu s datovou zprávou, je elektronicky označen elektronickou značkou poskytovatele. Ten, kdo bude na certifikát spoléhat, bude k ověření platnosti přijatého certifikátu potřebovat další veřejný klíč uložený v nadřazeném certifikátu poskytovatele. I jeho certifikát je podepsán další, například kořenovou certifikační autoritou. Tzv. kořenový certifikát certifikační autority již bude „self-signed" (podepsán, resp. označen „sám sebou"). Tvoří tedy vrchol této hierarchické struktury. Pro ověření platnosti certifikátu je nutné provést ověření platnosti všech certifikátů v certifikační cestě, až po kořenový certifikát. V praxi neověřujeme manuálně jeden certifikát za druhým, ale provádí to za nás

[19] Je-li u odkazu uvedeno „též", je pojem definován v uvedeném právním předpisu a zde je objasněn v širších souvislostech. Pokud u odkazu není uvedeno „též", jedná se o přesnou citaci.

programové vybavení (např. e-mailový klient). Pokud uplyne doba platnosti některého z nadřazených certifikátů, není považován za platný žádný z podřízených certifikátů a tato informace je uživateli zobrazena.

**Elektronická značka** – umožňuje jednoznačnou identifikaci subjektu (orgánu veřejné moci, firmy apod.), který datovou zprávu označil, a zaručuje, že každá následná změna označených dat bude zjistitelná. Z technologického hlediska se jedná o digitální podpis (stejně jako v případě zaručeného elektronického podpisu). E-značky jsou určeny především pro automatizované označování datových zpráv v případě, kdy je nutné odesílat velké objemy těchto zpráv (např. při odesílání potvrzení o doručení datové zprávy v případě e-podatelen ústředních orgánů veřejné správy, výpisy z registrů aj.).

*též: Zákon o elektronickém podpisu [4] § 2 písm. c)*

**Uznávaná elektronická značka** – legislativní zkratka pro e-značku založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem.

*též: Vyhláška o elektronických podatelnách [12] § 2 odst. 3*

**Zaručený elektronický podpis** – umožňuje jednoznačnou identifikaci fyzické osoby, která data v elektronické podobě podepsala, a zaručuje, že každá následná změna podepsaných dat bude zjistitelná. Z technologického hlediska se jedná o digitální podpis.

*též: Zákon o elektronickém podpisu [4] § 2 písm. b)*

**Uznávaný elektronický podpis** – legislativní zkratka pro zaručený elektronický podpis, který je založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem. Pouze uznávané elektronické podpisy lze používat v oblasti orgánů veřejné moci.

*též: Zákon o elektronickém podpisu [4] § 11*

**Certifikát** – datová zpráva, kterou vydává poskytovatel a která obsahuje zejména jméno vlastníka certifikátu, sériové číslo certifikátu, veřejný klíč (díky veřejnému klíči lze podpis ověřit), dobu jeho platnosti, případně název organizace, kde vlastník certifikátu působí aj. Poskytovatel v rámci procesu vydávání označuje certifikát svou e-značkou (viz certifikační cesta). Certifikát slouží k ověřování e-podpisu.

*též: Zákon o elektronickém podpisu [4] § 2 písm. k)*

**Kvalifikovaný certifikát** – označení pro certifikát, který byl vydán podle zákona o elektronickém podpisu; je spojen s používáním e-podpisu.

*též: Zákon o elektronickém podpisu [4] § 2 písm. l)*

**Kvalifikovaný systémový certifikát** – označení pro certifikát, který byl vydán podle zákona o elektronickém podpisu; je spojen s používáním e-značky.

*též: Zákon o elektronickém podpisu [4] § 2 písm. m)*

**Identifikátor e-podatelny** – obdoba podacího razítka; je určen pro zaznamenávání informací o doručené zprávě, a to zejména informací týkajících se ověření elektronického podpisu. Identifikátor může existovat v elektronické i papírové podobě.

*též: Vyhláška o elektronických podatelnách [12] § 2 odst. 9*

**Elektronická podatelna** – pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv.

*Zákon o elektronickém podpisu [4] § 2 písm. y)*

**Hash, Hashovací funkce –** matematická funkce, jejímž vstupem je libovolně velký datový blok a výstupem je datový řetězec pevné délky. V oblasti digitálních podpisů se hashovací funkce obvykle používají k výpočtu tzv. otisku podepisované zprávy. Namísto původní zprávy tak podepisujeme její podstatně „kratší" otisk, neboli hash (délky např. 128 nebo 160 bitů). Vlastnosti takových hashovacích funkcí navíc zaručují, že je prakticky nemožné vytvořit k určité zprávě jinou zprávu, která by měla stejný otisk. Pokud tedy ve zprávě provedeme byť jen nepatrnou změnu, otisk na výstupu bude zcela odlišný. Mezi nejznámější a nejpoužívanější hashovací funkce patří SHA-1 (Secure Hash Algorithm, otisk délky 160 bitů) a MD5 (Message Digest, otisk délky 128 bitů).

**Identifikátor Ministerstva práce a sociálních věcí** – číselný znak, který Ministerstvo práce a sociálních věcí přiděluje příjemcům sociálních dávek. V některých agendách (např. elektronická daňová přiznání) je využíván k další identifikaci podepisující osoby. Může být obsažen v kvalifikovaných certifikátech.

**Časové razítko** – datová zpráva, kterou vydala důvěryhodná třetí strana a která stvrzuje, že data, ke kterým je časové razítko připojeno, existovala dříve, než bylo toto razítko vytvořeno.

**Kvalifikované časové razítko** – časové razítko vydané podle zákona o elektronickém podpisu.

*též: Zákon o elektronickém podpisu [4] § 2 písm. r)*

**LDAP** (angl. **L**ightweight **D**irectory **A**ccess **P**rotocol) – protokol používaný pro přístup do adresářů přes Internet, který zprostředkovává tzv. adresářové služby. V e-mailových klientech se tento protokol používá pro vyhledávání informací o uživatelích. Nejčastěji se u hledané osoby vyhledávají informace o e-mailové adrese nebo kontaktu. Tento protokol je však možné také použít pro stahování libovolných dat (konfigurace, nastavení) ze serveru podporujícího tento protokol. Kompletní popis tohoto protokolu můžete nalézt v dokumentu RFC 1777.

**Poštovní klient** (též: e-mailový klient) – je program, který zajišťuje „klientskou část" systému elektronické pošty. Pomocí něj uživatelé píší nové zprávy, stahují ze serveru příchozí zprávy, čtou je, případně je mažou, ukládají nebo jinak zpracovávají. Poštovní klient také zprostředkuje odeslání nové zprávy tím, že předá její obsah spolu s požadavkem na odeslání SMTP (poštovnímu) serveru, a ten se postará o faktické doručení zprávy. Nejrozšířenějším klientem je Outlook (MS Outlook Express a MS Office Outlook), jeho nejpoužívanější alternativou je Mozilla Thunderbird.

**Protokol SMTP** (angl. **S**imple **M**ail **T**ransfer **P**rotocol) – protokol, který slouží k přenosu e-mailových zpráv.

**Spam –** nevyžádaná pošta, zpravidla reklamního charakteru. Obvykle přichází z adres, které příjemce nezná, a pro její odesílání jsou často využívány freemailové servery (např. hotmail.com či yahoo.com). V ČR existuje právní úprava týkající se nevyžádaných obchodních sdělení [3].

**Elektronická pošta** – textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.

*Zákon o některých službách informační společnosti [3] odst. 2 písm. b)*

**Formáty souborů**

- formát .eml – formát pro ukládání kompletních e-mailových zpráv ve většině e-mailových klientů definovaný v RFC 2822;
- formát .msg – formát pro ukládání kompletních e-mailových zpráv v MS Office Outlook;
- formát S/MIME (angl. Secure/Multipurpose Internet Mail Extensions) – může sloužit k bezpečnému posílání e-mailů, v našem případě spíše k posílání podepsaných e-mailů. Při použití tohoto postupu se zpráva uloží do tzv. S/MIME obálky a takto se posílá většinou přes internetový SMTP protokol. Definice S/MIME zprávy je v RFC 3851;
- formát .p7s – soubor s podpisem ve formátu PKCS #7;
- formáty .pdf, .txt, .jpg, .doc, .rtf .html, .xml – běžně používané formáty souborů známé většině uživatelů.

# 2 Změny

## 2.1 Změnové řízení

| Status | Datum | Popis | Garant | Schválil |
|---|---|---|---|---|
| Verze 1.0 (interní návrh) | 19.11.2004 | Best practice – Jak vyřizovat elektronickou poštu | Sekce 5 | ředitel odboru elektronického podpisu |
| Verze 1.1 (zveřejněný návrh) | 29.11.2004 | Best practice – Jak vyřizovat elektronickou poštu | Sekce 5 | ministr |
| Verze 2.0 | 31.3.2005 | Best practice – Jak vyřizovat elektronickou poštu | Sekce 5 | ministr |

# Příloha č. 1

## Doporučení pro obce

Povinnost zřídit e-podatelnu je úzce spjata s povinností přijímat/odesílat elektronicky podepsané písemnosti. Povinnost přijímat/odesílat takové písemnosti je stanovena v předpisech, které upravují výkon konkrétní agendy.

Pro obce v rámci výkonu samostatné působnosti připadá v úvahu příjem/odesílání elektronických písemností elektronicky podepsaných v souvislosti s řízením:

- o uložení pokuty (správní sankce) podle § 58 a 59 zákona č. 128/2000 Sb. o obcích, (obecní zřízení) [7],
- ve věcech poplatků podle zákona č. 565/1990 Sb., o místních poplatcích [8],
- poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím [5].

Na postup podle těchto zákonů se vztahují právní předpisy, které upravují přijímání datových zpráv v elektronické podobě. Těmito předpisy jsou zákon č. 71/1967 Sb., o správním řízení [1] (od 1. 1. 2006 zákon č. 500/2004, správní řád [2]) a zákon č. 337/1992 Sb., o správě daní a poplatků [9].

Protože tyto předpisy předpokládají, že tato řízení budou vedena i v elektronické podobě, tj. obec bude muset písemnosti zasílat elektronicky nebo občané budou požadovat, aby tuto formu komunikace mohli použít, musí obec zřídit a provozovat e-podatelnu podle nařízení vlády č. 495/2004, kterým se provádí zákon o elektronickém podpisu [10] a vyhlášky č. 496/2004, o elektronických podatelnách [12], případně dohodnout s jiným úřadem, že bude přijímat/odesílat datové zprávy prostřednictvím jeho e-podatelny.

V případě, že obec nemá prostředky ke zřízení a zajištění chodu vlastní e-podatelny, je žádoucí, aby zajistila přijímání datových zpráv veřejnoprávní smlouvou s jiným orgánem veřejné moci podle nařízení vlády.

Toto ustanovení nařízení vlády je modifikováno zákonem č. 500/2004 Sb., správní řád [2], který s účinností od 1. 1. 2006 stanoví, že osoba, jejíž je správní orgán součástí, která není schopná zajistit činnost e-podatelny uzavře s obcí s rozšířenou působností, v jejímž správním obvodu má sídlo, veřejnoprávní smlouvu o provozování elektronické podatelny.

I v případě, že se obec zbaví své povinnosti zřídit e-podatelnu veřejnoprávní smlouvou, je stále žádoucí, aby obec občanům umožnila alespoň základní formu elektronické komunikace, tj. zveřejnila elektronickou adresu, na kterou je možné datové zprávy zasílat, a došlou poštu průběžně vyřizovala tak, aby byla schopná adekvátně reagovat na oznámení občanů, i když elektronická komunikace bude převážně obsahovat dotazy, stížnosti a náměty, které nemusí být elektronicky podepsány a nemusí být přijímány a vyřizovány pouze prostřednictvím e-podatelny.

# Příloha č. 2

## Příklad informací zveřejňovaných k e-podatelně

**Elektronická podatelna obecního úřadu Stupná**

**Elektronická adresa:** posta@stupna.cz

Tato elektronická podatelna a uvedená adresa je určena pro příjem veškerých datových zpráv doručovaných obecnímu úřadu Stupná.

**Adresa pro osobní a poštovní přijímání datových zpráv na technických nosičích:** Obecní úřad Stupná, podatelna, Janáčkova 22, 777 26 Stupná

Úřední hodiny podatelny: pondělí – pátek 7:30 – 11:00 13:00 – 15:00

**Pravidla potvrzování doručení datových zpráv:**

Úřad potvrzuje, že datová zpráva byla doručena elektronické podatelně, zasláním této zprávy (vzor):

| Potvrzení doručení datové zprávy |
| --- |
| Datová zpráva byla doručena elektronické podatelně Obecního úřadu Stupná posta@stupna.cz DD/MM/RRRR v HH/MM/SS. |
| Identifikátor dokumentu:[20)] |
| Jméno a příjmení oprávněného zaměstnance |

Tato datová zpráva musí být podepsána zaručeným elektronickým podpisem oprávněného zaměstnance úřadu.

Úřad zasílá datovou zprávu o doručení nejpozději v první pracovní den, který bezprostředně následuje po dni doručení. Úřad zprávu zasílá na elektronickou adresu, ze které byla zpráva odeslána, pokud odesilatel výslovně nepožádal o zaslání na jinou elektronickou adresu. Pokud se zpráva potvrzující doručení vrátí úřadu jako nedoručitelná, úřad učiní ještě jeden pokus o její doručení.

**Technické parametry přijímaných datových zpráv:**

Datové zprávy jsou přijímány ve formátech: html, pdf, doc, jpg, rtf , případně dalších běžně používaných formátech datových zpráv. V případě pochybností vzneste dotaz na naši e-podatelnu, kde Vám naši pracovníci sdělí, zda je daný formát akceptovatelný.

**Technické parametry fyzických nosičů, na nichž lze předávat datové zprávy:**

Datové zprávy jsou přijímány na 3,5" disketách zformátovaných pro některý z „windowsovských" systémů souborů (FAT), dále na CD, ZIP, případně dalších technických nosičích. V případě pochybností vzneste dotaz na naši e-podatelnu, kde Vám naši pracovníci sdělí, zda jsou technické parametry daného fyzického nosiče akceptovatelné.

[20)] Vyhláška o elektronických podatelnách [12], v § 2 odst. 5 písm. c) stanoví, že součástí zprávy o potvrzení doručení je „charakteristika doručené datové zprávy umožňující její identifikaci". Touto jednoznačnou charakteristikou může být úplná přijatá datová zpráva, identifikační číslo (číslo jednací), pod kterým je zpráva elektronickou podatelnou vedena, případně jednoznačná reprezentace zprávy ve formě jejího otisku (hash).

**Postup v případě zjištění škodlivého softwaru nebo chybného formátu u přijaté datové zprávy:**

Datová zpráva, u které byl zjištěn škodlivý software nebo chybný formát, není zpracovávána. Pokud odesilatel neobdrží zprávu potvrzující doručení (viz výše), je pravděpodobné, že se jednalo o takto poškozenou zprávu, kterou nelze zpracovat.

**Vyřizování dotazů týkajících se provozu elektronické podatelny:**

Vaše dotazy týkající se provozu elektronické podatelny zasílejte na elektronickou adresu posta@stupna.cz nebo na adresu novakk@stupna.cz případně na poštovní adresu úřadu. Dotazy úřad vyřizuje do 3 pracovních dnů ode dne jejich doručení.

**Seznam jmen oprávněných zaměstnanců úřadu, kterým byl vydán kvalifikovaný certifikát:**

| Jméno/Název (CN) |
|---|
| Karel Novák |
| Jana Svobodová |

**Seznam právních předpisů, podle kterých je možné vůči úřadu činit právní úkony v elektronické podobě a náležitosti těchto úkonů:**

**Žádost o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím** nemusí být podepsána zaručeným elektronickým podpisem.

Podle § 14 odst. 2 zákona č. 106/1999 Sb. musí být z podání zřejmé, kterému povinnému subjektu je určeno a kdo jej činí. U podání prostřednictvím telekomunikačního zařízení musí být uvedena rovněž příslušná identifikace žadatele (například elektronická adresa). Neobsahuje-li žádost tyto údaje, není žádost podáním ve smyslu tohoto zákona a žádost se odloží.

**Podání podle zákona č. 71/1967 Sb., o správním řízení (správní řád)** (§ 19)**:**

- musí být podepsáno zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb; současně musí být uveden poskytovatel certifikačních služeb, který certifikát vydal a vede jeho evidenci, nebo musí být certifikát k podání připojen, nebo
- nemusí být podepsáno zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb; v takovém případě musí být do 3 dnů doplněno – viz výše.

Podle § 19 odst. 2 zákona č. 71/1967 Sb. musí být z podání patrno, kdo je činí, které věci se týká a co se navrhuje. Zvláštní právní předpisy mohou stanovit jeho další náležitosti.

**Stížnosti, oznámení a podněty podle vyhlášky č. 150/1958 Ú.l.** nemusí být podepsány zaručeným elektronickým podpisem.

**Datové zprávy zaslané úřadu, jejichž náležitosti neupravuje právní předpis**, nemusí být podepsány zaručeným elektronickým podpisem. Jedná se například o běžnou e-mailovou komunikaci mezi pracovníky úřadu a občany.