Úřad pro veřejné informační systémy
Havelkova 22
130 00 Praha 3

Standard ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu

016/01.01

Verze . modifikace standardu ISVS	Datum schválení verze / modifikace	Datum vyhlášení standardu ISVS	Datum zveřejnění na webu ÚVIS	Uveřejněn ve Věstníku ÚVIS
01.01	30. 4. 2002	25. 6. 2002	31. 5. 2002	2002/částka 1

Obsah

Standard ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu

016/01.01

Předmluva

Zřizování elektronických podatelen je jeden z konkrétních kroků při zkvalitňování výkonu veřejné správy, zejména s ohledem na zajištění permanentní možnosti podávat na orgány státní správy požadované dokumenty a žádosti.

Ve spojení s principem využívání zaručeného elektronického podpisu je vytvořen základ pro přechod (v případech, kdy je to pro občana výhodné) k bezpapírovému kontaktu občan – státní správa případně mezi orgány státní správy.

1 Předmět standardu

Standard je určen orgánům veřejné moci. Stanovuje organizačně technické předpoklady a podklady, které orgán veřejné moci rozpracuje do opatření k fungování pracovišť pro příjem a odesílání datových zpráv v orgánech veřejné moci (dále jen elektronických podatelen) v souvislosti s používáním elektronického podpisu podle zákona č. 227/2000 Sb., o elektronickém podpisu a návazných podzákonných norem.

Komentář: I když je elektronická podatelna součástí vnitřní organizační a funkční struktury orgánu veřejné moci, dotýká se její funkce nejen tohoto orgánu samotného. S elektronickou podatelnou se dostávají do styku ostatní orgány veřejné moci (o nichž je možné předpokládat, že jejich struktura a zejména informační systém odpovídají standardům ÚVIS), ale i komerční sféra a občané.

Standard se vztahuje povinně na orgány státní moci, pokud jde o podání podle zákona č. 337/1992 Sb., o správě daní a poplatků, zákona č. 71/1967 Sb., o správním řízení (správního řádu), zákona č. 99/1963 Sb., občanského soudního řádu a podle zákona č. 141/1961 Sb., o trestním řízení soudním (trestního řádu), dále jen podle zvláštních zákonů. Pro oblast samosprávy a pro oblast státní správy je pro jiná podání doporučený.

Elektronická podatelna splňuje ustanovení tohoto standardu tehdy, pokud splňuje požadavky kapitol 4., 5., 6. a 7.

2 Odkazy

- Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád).
- Zákon č. 99/1963 Sb., občanský soudní řád.
- Zákon č. 71/1967 Sb., o správním řízení (správní řád).
- Zákon č. 97/1974 Sb., o archivnictví.
- Zákon č. 337/1992 Sb., o správě daní a poplatků.
- Zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem.
- Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů.

- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).
- Zákon č. 240/2000 Sb., o krizovém zřízení.
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a změně některých dalších zákonů.
- Nařízení vlády č. 304/2001 Sb., kterým se provádí zákon o elektronickém podpisu.
- Vyhláška č. 116/1998 Sb., kterou se provádí zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem.
- Vyhláška ÚOOÚ č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.
- Standard ISVS pro komunikaci informačních systémů, 002/01.03., Věstník ÚVIS 2000/částka 2.
- Standard ISVS pro národní prostředí, 004/02.05, Věstník ÚVIS 2000/částka 4.
- Standard ISVS pro náležitosti životního cyklu informačního systému, 005/01.01, Věstník ÚVIS 2000/částka 5.
- Standard ISVS stanovující povinné požadavky na metodiku atestace shody IS se Standardem ISVS pro náležitosti životního cyklu IS, 017/01.01, Věstník ÚVIS 2002/částka 2.

  Komentář: Uvádí se citace právního předpisu bez ohledu na další legislativní vývoj.

3 Vymezení pojmů

Pro účely tohoto standardu se předpokládá význam pojmů a jejich definice podle zákona č. 227/2000 Sb., o elektronickém podpisu a navazujících podzákonných norem.

3.1 **Akreditovaný poskytovatel certifikačních služeb** – poskytovatel certifikačních služeb, jemuž byla udělena akreditace, (§ 2 písm. f) zákona č. 227/2000 Sb.).

3.2 **Certifikát** – datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost, (§ 2 písm. g) zákona č. 227/2000 Sb.).

3.3 **Čitelná zpráva** – zpráva, která je v některém z formátů akceptovaných elektronickou podatelnou a neobsahuje potenciálně škodlivé programy či makra (viry, trojské koně, červy).

3.4 **Elektronická podatelna** – pracoviště pro příjem a odesílání datových zpráv v elektronické podobě (nařízení vlády č. 304/2001).

3.5 **Elektronický podpis** – údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě (§ 2 písm. a) zákona č. 227/2000 Sb.).

3.6 **Informační systém** – funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností, (§ 2 písm. b) zákona č. 365/2000 Sb.).

3.7 **Informační systém elektronické podatelny** je informační systém veřejné správy zabezpečující funkce elektronické podatelny. Jedná se o souhrn technických a programových prostředků a organizačních pravidel pro zabezpečení funkce elektronické podatelny.

3.8 **Kvalifikovaný certifikát** – certifikát, který má náležitosti stanovené zákonem č. 227/2000 Sb. a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty, (§ 2 písm. h) zákona č. 227/2000 Sb.).

3.9 **Poštovní klient** – programové vybavení pracovní stanice pro příjem, zpracování a odesílání elektronických zpráv.

3.10 **Provozovatel informačního systému veřejné správy** – subjekt, který provádí alespoň některé informační činnosti související s informačním systémem. Provozováním informačního systému veřejné správy může správce pověřit jiné subjekty, pokud to jiný zákon nevylučuje, (§ 2 písm. d) zákona č. 365/2000 Sb.).

3.11 **Správce informačního systému veřejné správy** – subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá, (§ 2 písm. c) zákona č. 365/2000 Sb.).

3.12 **Technický nosič dat** – materiál, do nějž, či na nějž lze zaznamenat data, a z něj je zpět získat.

3.13 **Veřejná moc –** taková moc, která autoritativně rozhoduje o právech a povinnostech subjektů, či už přímo, nebo zprostředkovaně. Subjekt, o jehož právech nebo povinnostech rozhoduje orgán veřejné moci, není v rovnoprávném postavení s tímto orgánem a obsah rozhodnutí tohoto orgánu nezávisí na vůli subjektu. (Usnesení Ústavního soudu České a Slovenské Federativní republiky ze dne 9. června 1992 sp. zn. l. ÚS 191/92).

3.14 **Veřejný informační systémem** – informační systém vedený správci uvedenými v § 3 odst. 2 zákona č. 365/2000 Sb. pro výkon veřejné správy nebo jiný informační systém poskytující služby veřejnosti, který má vazby na informační systémy veřejné správy, (§ 2 písm. u) zákona č. 365/2000 Sb.).

3.15 **Záhlaví zprávy** – sdělení, které je automaticky vygenerované poštovním klientem a které zpravidla obsahuje:

a) elektronickou adresu odesílatele
b) datum a čas odeslání zprávy
c) adresu příjemce
d) předmět zprávy
e) důležitost zprávy

3.16 **Zaručený elektronický podpis** – elektronický podpis, který splňuje následující požadavky:

a) je jednoznačně spojen s podepisující osobou,
b) umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
c) byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
d) je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat (viz § 2 písm. b zákona č. 227/2000 Sb.).

Komentář: V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (§ 11 zákona č. 227/2000 Sb.).

Význam použitých zkratek

IS	Informační systém
ISVS	Informační systém (y) veřejné správy
ÚVIS	Úřad pro veřejné informační systémy

4 Funkce elektronické podatelny

4.1 Úkoly elektronické podatelny

Funkce elektronické podatelny musí zahrnovat podle požadavku nařízení vlády č.304/2001 Sb.:

1. příjem a odesílání datových zpráv dálkovým přístupem i na technickém nosiči dat,
2. kontrolu, zda jsou zprávy čitelné a schopné dalšího zpracování v orgánu veřejné moci,
3. ověření platnosti certifikátu náležejícího k elektronickému podpisu,
4. předání ověřeného podání k dalšímu řízení.

Pro zajištění bezpečného využití elektronické podatelny orgán veřejné moci zveřejní (v přímo čitelné i elektronické podobě umožňujícím dálkový přístup):

a) seznam elektronických adres, jichž je možné pro styk s elektronickou podatelnou orgánu veřejné moci využívat, viz Standard ISVS pro komunikaci informačních systémů, 002/01.03., Věstník ÚVIS 2000/částka 2; *tato adresa musí být uvedena ve tvaru posta@<doména orgánu veřejné moci>.cz*,
b) seznam kvalifikovaných certifikátů zaměstnanců určených pro zajištění provozu elektronické podatelny (nebo elektronické adresy, na nichž se kvalifikované certifikáty nacházejí),
c) formát datových zpráv, jež je elektronická podatelna způsobilá přijmout na zveřejněných typech nosičů,
d) adresu umístění elektronické podatelny,
e) pravidla zasílání a potvrzování příjmu podání (musí se zohlednit postupy podle bodů 4.2.2 a 4.2.3),
f) seznam typů podání, které úřad přijímá a maximální přípustnou velikost přijímané elektronické zprávy včetně maximální velikosti příloh.

Všechny tyto úkoly musí plnit elektronická podatelna v návaznosti na existující organizační a funkční strukturu orgánu veřejné moci a bez ohledu na způsob nebo čas připojení elektronické podatelny ke službám elektronické pošty.

Komentář: Zde uvedené funkce jsou dále rozvedeny pro obě hlavní kategorie – podání elektronickou poštou a na technickém nosiči.

4.2 Podání učiněné elektronickou poštou

4.2.1 Charakteristika podání učiněného elektronickou poštou

Podání učiněné elektronickou poštou je zpráva zaslaná elektronicky zpravidla přes veřejnou datovou síť a přijatá elektronickou podatelnou prostřednictvím zvláštního programového vybavení (poštovního klienta elektronické podatelny). Zpráva může obsahovat přílohu.

Komentář: Nevylučuje se možnost, že podání bude učiněno elektronickou poštou, ale nebude k tomu využito veřejného poskytovatele. Tento případ může nastat tehdy, jestliže se využije vnitřní elektronické pošty orgánu veřejné moci k sepsání podání a k jeho podepsání elektronickým podpisem, který si předkladatel podání pořídí pomocí podepisovacího prostředku z vlastní diskety.

Záhlaví zprávy není součástí zprávy.

Komentář: Záhlaví nelze podepsat. Není součástí vlastního podání, bude však archivováno.

Pokud zpráva obsahuje přílohu, může být zpráva s přílohou elektronicky podepsaná jako celek nebo příloha samostatně nebo obojí samostatně.

Pokud je zpráva elektronicky podepsána zaručeným elektronickým podpisem v souladu s § 11 zákona č. 227/2000 Sb., o elektronickém podpisu, postupuje se podle pokynů uvedených v článku 4.2.2. Není-li zpráva elektronicky podepsána a je předepsaným způsobem podepsána pouze příloha této elektronické zprávy, přičemž tato příloha tvoří podání učiněné orgánu veřejné moci, postupuje se podle článku 4.2.3.

Komentář: U podání formou podepsané přílohy k elektronické zprávě se a priori nepředpokládá, že osoba, která podepsala přílohu je totožná s odesílatelem zprávy.

4.2.2 Úkoly elektronické podatelny v souvislosti s přijetím podepsané zprávy

Elektronická podatelna musí:

1. Zajistit příjem podání ve formě zprávy elektronické pošty buď trvalým on-line připojením poštovního klienta k poskytovateli poštovních služeb nebo opakovaným off-line připojením nejméně na začátku a na konci pracovní doby orgánu veřejné moci.

Komentář: Bere se zřetel na orgány veřejné moci, které nejsou trvale připojeny k poskytovateli elektronické pošty ale i na situaci, že elektronická podatelna je z určitých důvodů (např. bezpečnostních) připojována jen na nezbytně nutnou dobu, danou příjmem a odesláním pošty, připojením k poskytovatelům certifikačních služeb apod.

2. Zapsat doručení poštovní zprávy (automaticky bez zásahu obsluhy) do archivu přijaté pošty. Zprávy uložené v archivu elektronické podatelny musí být zabezpečeny před modifikací nebo zničením v souladu se zákonem č. 97/1974 Sb., o archivnictví.

   Komentář: Archivace je nutná proto, aby bylo možné prokázat, jaká byla zpráva ještě před zahájením zpracování. Např. antivirová kontrola by mohla v určitých situacích, daných nastavením, způsobit destrukci zprávy nebo elektronického podpisu. Rovněž to, že zpráva je doručena v nezpracovatelném formátu, který však nese vnější znaky formátu povoleného (např. přípona souboru) musí být průkazně dokumentováno.

3. Zapsat podání do evidence doručených elektronických podání (ručně nebo automatizovaně).

   Komentář: To, jak je zpráva zapsána a jaká je podoba výsledného zápisu, je určeno stávající úrovní automatizace práce s dokumenty v orgánu veřejné moci. Důležité je, aby byl zápis učiněn a bylo možné jej v případě potřeby přečíst nebo doplnit. Je zřejmé, že v některých systémech může být kniha došlých elektronických podání reprezentována záznamem z tzv. poštovního serveru. Všechny údaje o došlé elektronické poště však v takovém případě musí být dostatečně průkazné, s potřebnou mírou podrobností a musí být zajištěna požadovaná bezpečnost (tzn. dostupnost, důvěrnost a integrita záznamů).

4. Ověřit, jsou-li zpráva a případné přílohy čitelné a bezpečně zpracovatelné v orgánu veřejné moci. Součástí je i kontrola na přítomnost virů, trojských koňů, červů apod. či maker (dále jen potencionálně škodlivých programů). V případě, že byl zjištěn potenciálně škodlivý program či makro nebo zpráva nebyla čitelná, další zpracování elektronického podání se v orgánu veřejné moci zastaví a elektronická podatelna uvědomí předkladatele podání nejpozději následující pracovní den, že podání nemůže být přijato z technických příčin. Důvod nepřijetí se zapíše do knihy došlých elektronických podání. Je-li podání zasláno z veřejného místa (internetový kiosek, internetová kavárna), splní podatelna tento požadavek pouze v případě, že předkladatel uvedl zpětnou adresu (elektronickou nebo poštovní).

   Komentář: Výskyt škodlivých programů znamená, že zprávu elektronické pošty a tedy i podání učiněné jejím prostřednictvím, nelze v orgánu veřejné moci „standardním způsobem" zpracovat, dokonce pokus o zjištění, zda se skutečně jedná o podání, může vést k nevratným poškozením ostatních částí systému. Z tohoto důvodu je tato kontrola zcela zásadní a její výsledek ovlivňuje další činnost. Snaha o odstranění škodlivého programu vede v každém případě k porušení integrity původní zprávy (jejíž originál je podle bodu 2 archivován) a výsledek není zaručen. Zpráva, u níž není možné zaručit další bezpečné zpracování v orgánu veřejné moci, je tedy z těchto příčin odmítnuta.

5. Ověřit, zda elektronicky podepsaná zpráva má náležitosti požadované zvláštními zákony. Ověřit elektronický podpis a platnost certifikátu náležejícího k elektronickému podpisu odesílatele.

   Komentář: Pro obce 1. a 2. typu je nutné ověřovat seznam zneplatněných certifikátů aspoň 1 x denně vytvořením kopie seznamu CRL, ostatní orgány veřejné moci jsou povinny zajišťovat platnost certifikátu on-line.

6. Poté, co elektronická podatelna ověří čitelnost podání, musí potvrdit příjem odesílateli, bez ohledu na to, generuje-li poštovní klient potvrzení o doručení zprávy. Součástí tohoto potvrzení příjmu musí být konstatování, zda elektronicky podepsaná zpráva má všechny náležitosti stanovené zvláštními zákony, konstatování o výsledku kontroly elektronického podpisu a platnosti certifikátu.

   Je-li potvrzení o přijetí podání odesláno elektronickou poštou na adresu toho, kdo podání zaslal, bude toto potvrzení zasláno jako zpráva podepsaná elektronicky zplnomocněným zaměstnancem orgánu veřejné moci nejpozději následující pracovní den poté, co bylo podání přijato. Je-li podání zasláno z veřejného místa (internetový kiosek, internetová kavárna), splní podatelna tento

požadavek pouze v případě, že předkladatel uvedl zpětnou adresu (elektronickou nebo poštovní). Pokud si odesílatel vymínil zaslání potvrzení o přijetí podání písemně, elektronická podatelna zajistí vydání potvrzení cestou listovní podatelny.

Komentář: Ve smyslu tohoto standardu je elektronická podatelna jediným místem, které zajišťuje styk mezi orgánem veřejné moci a předkladatelem podání podepsaného elektronickým podpisem. Tím není dotčena možnost ostatních pracovníků orgánu veřejné moci elektronický podpis používat v souladu s vnitřními předpisy orgánu veřejné moci.

7. Předat podání k vyřízení podle interních předpisů orgánu veřejné moci cestou listovní podatelny (elektronická podatelna podání vytiskne, ověří a opatří náležitostmi podle vnitřních předpisů orgánu veřejné moci) nebo vnitřním elektronickým systémem zpracování dokumentů (elektronická pošta převede zprávu v elektronické podobě do systému práce s dokumenty a učiní v dokumentu poznámku o tom, že byl ověřen elektronický podpis).

   Komentář: Zde se musí provázat činnost elektronické podatelny s ostatními funkcemi orgánu veřejné moci. Není vhodné, aby elektronická podatelna pracovala s vlastními kanály pro pohyb dokumentů, je naopak žádoucí (i s ohledem na nařízení vlády č. 304/2001 Sb., §1 odst. 1 písm. b) aby činnost elektronické podatelny probíhala v souladu s organizačním řádem orgánu veřejné moci.

   Nedostatky zjištěné kontrolami probíhajícími v průběhu elektronického zpracování nebo při zpracování dokumentů přímo čitelných, se kvalifikují a řeší podle zvláštních právních předpisů jako vada podání.

   Elektronická podatelna plní funkce obdobné podatelnám listovním, není-li uvedeno jinak.

   Příjem podání v elektronické podobě je spojen s jistými administrativními úkony, které jsou vesměs definovány ve vnitřním předpisu o listovní podatelně.

4.2.3 Úkoly elektronické podatelny v souvislosti s přijetím zprávy s podepsanou přílohou

Elektronická podatelna musí:

1. Zajistit příjem podání ve formě zprávy elektronické pošty buď trvalým připojením poštovního klienta k poskytovateli poštovních služeb nebo opakovaným připojením nejméně na začátku a na konci pracovní doby orgánu veřejné moci.
2. Zapsat doručení poštovní zprávy (automaticky bez zásahu obsluhy) do archivu přijaté pošty. Zprávy uložené v archivu elektronické podatelny musí být zabezpečeny před modifikací nebo zničením v souladu se zákonem č. 97/1974 Sb., o archivnictví.
3. Zapsat každou samostatně podepsanou přílohu do evidence elektronických doručených podání (ručně nebo automatizovaně). Pro každou samostatně podepsanou položku se dále postupuje podle odstavce 4.2.2 bodů 4., 5., 6. a 7.

4.2.4 Doba přijímání zpráv obsahujících podání

Příjem a odesílání elektronické pošty musí být elektronickou podatelnou zajištěn pomocí připojení datové sítě každý pracovní den nepřetržitě nebo opakovaně a to nejméně jednou na počátku a jednou před ukončením pracovní doby.

Provoz elektronické podatelny musí být zahrnut do vnitřních organizačních předpisů orgánu veřejné moci.

Komentář: Provozní doba elektronické podatelny se nemusí krýt s dobou, kdy je elektronická podatelna přímo spojena s poskytovatelem poštovních služeb. Elektronická podatelna zajišťuje např. i přípravu zpráv, komunikaci s ostatními organizačními útvary orgánu veřejné moci, příjem a odbavení přímo doručených technických nosičů apod.

4.3 Podání na technických nosičích dat

4.3.1 Charakteristika podání předaného elektronické podatelně na technických nosičích dat

Podání předané elektronické podatelně na technickém nosiči dat je soubor informací, zapsaný na technický nosič technickým a programovým vybavením, jehož uživatelem je předkladatel podání.

Komentář: Je možné, aby předkladatel podání dočasně využil např. počítač orgánu veřejné moci, který k tomu účelu orgán veřejné moci dá k dispozici např. v předsíni podatelny, v hale apod.

Podání může být tvořeno jedním souborem nebo několika soubory, z nichž jeden je zpravidla vlastní podání a ostatní jsou jeho přílohami. Na technickém nosiči dat nesmí být soubory, které s podáním nesouvisí. Elektronický podpis může být připojen ke všem souborům nebo jen k některým z nich. Nejsou-li elektronicky podepsány všechny soubory, nelze existenci elektronického podpisu u jednoho z nich vztahovat na ostatní.

Komentář: To znamená, že o tom, který z dokumentů (přeneseně „souborů“) na technickém nosiči bude podepsán, rozhoduje předkladatel podání podle jeho obsahu.

Na jednom technickém nosiči smí být pouze jedno podání, které je elektronickou podatelnou označeno jedním číslem jednacím.

Komentář: Tento požadavek sice poněkud omezuje předkladatele více podání současně, ale vzhledem k administrativnímu postupu listovní podatelny se jedná o běžnou praxi.

4.3.2 Úkoly elektronické podatelny při příjmu podání na technických nosičích

Elektronická podatelna musí:

1. Zapsat přijaté podání manuálně spuštěným procesem do archivu přijatých podání. Zprávy uložené v archivu elektronické podatelny musí být zabezpečeny před modifikací nebo zničením. Z archivu přijatých podání lze podání vyjmout pouze při zachování zvýšených bezpečnostních zásad a se současným ověřením, zda podání neobsahuje škodlivé programy či makra (viz bod 3 dále).

   Komentář: Protože podání na technickém nosiči je doručeno osobně, musí se ručně zahájit i jeho zpracování. Požadavek na primární archivaci je zde, narozdíl od elektronické pošty (která se archivuje automaticky), explicitně vyjádřen.

   Při vyjmutí podání z archivu je třeba uplatnit zvýšené bezpečnostní požadavky, protože zpráva může být nositelem nebezpečných programů (např. virů). V praxi to bude znamenat, že při vyjmutí z archivu se podání předá ke kontrole stejně, jako při obdržení od předkladatele podání.

2. Zapsat doručení podání do evidence elektronických podání.

   Komentář: Tato kniha je analogická knize pošty. Opět je požadavek vyjádřen explicitně, protože u elektronické pošty se automaticky pořizuje záznam o došlých poštovních zprávách.

3. Ověřit, jsou-li zpráva a případné přílohy čitelné v orgánu veřejné moci. Součástí je i kontrola na přítomnost potenciálně škodlivých programů či maker (tzv. antivirová kontrola). V případě, že byl zjištěn škodlivý program či makro, další zpracování elektronického podání se v orgánu veřejné moci zastaví a elektronická podatelna uvědomí předkladatele podání, že podání nemůže být přijato z technických příčin. Pokud doručil podání osobně, bezprostředně, pokud podání doručil poštou, pak na poštovní adresu nejpozději následující pracovní den, se sdělením. Příčina se zapíše do evidence došlých elektronických podání.

4. Pořídit z podání na technickém nosiči pracovní kopie na paměťové médium informačního systému elektronické podatelny; další operace nad elektronickým podáním provádí elektronická podatelna s touto pracovní kopií.

   Komentář: Archivovaný originál musí zůstat nedotčen a musí se zabránit jeho poškození při dalších operacích (např. kontrola na přítomnost škodlivých programů a pokus o přečtení nosiče).

5. Ověřit, zda elektronicky podepsaná zpráva má náležitosti požadované zvláštními zákony. Ověřit elektronický podpis a platnost certifikátu náležejícího k elektronickému podpisu odesílatele.

Komentář: Pro obce 1. a 2. typu je nutné ověřovat seznam zneplatněných certifikátů aspoň 1 x denně vytvořením kopie seznamu CRL, ostatní orgány veřejné moci jsou povinny zajišťovat platnost certifikátu on-line.

K ověření se musí použít speciálního programového vybavení nebo se podání musí konvertovat tak, aby bylo možno použít standardních mechanismů poštovních klientů nebo prohlížečů. Tento bod bude v praxi tvořit nejproblematičtější část řešení elektronické podatelny.

6. Poté, co elektronická podatelna ověřila čitelnost podání a elektronický podpis, potvrdit předkladateli příjem na počkání nebo poštou na adresu uvedenou v podání. V případě, že šlo o podání podle zvláštních zákonů, informuje navíc předkladatele o výsledku kontroly podle bodu 5. Potvrzení předkladateli se odešle v případě, že si předkladatel podání potvrzení vyžádal, nebo je-li to požadavek plynoucí z jiných zákonných nebo podzákonných norem.
7. Je-li potvrzení o přijetí podání odesláno elektronickou poštou na adresu toho, kdo podání zaslal, zaslat toto potvrzení jako zprávu podepsanou elektronicky zplnomocněným zaměstnancem orgánu veřejné moci nejpozději následující pracovní den poté, co bylo podání přijato. Pokud si odesílatel vymínil zaslání potvrzení o přijetí podání písemně, elektronická podatelna zajistí vydání potvrzení cestou listovní podatelny.
8. Předat podání k vyřízení podle interních předpisů orgánu veřejné moci zpravidla cestou listovní podatelny (elektronická podatelna podání vytiskne a opatří náležitostmi podle vnitřních předpisů orgánu veřejné moci) nebo vnitřním elektronickým systémem zpracování dokumentů (elektronická podatelna převede podání z elektronické podoby do systému práce s dokumenty).
9. Vrátit technický nosič, pokud o to předkladatel podání požádá, neprodleně nebo v dohodnutém termínu.

4.3.3 Doba přijímání podání na technických nosičích

Příjem podání na technickém nosiči zajistí elektronická podatelna v úředních hodinách orgánu veřejné moci při osobní návštěvě předkladatele podání nebo osoby doručující zásilky.

Elektronická podatelna přijme také technický nosič s podáním, který byl zaslán orgánu veřejné moci poštou jako součást zásilky podané zejména podle zvláštních zákonů cestou listovní podatelny. Těmito zákony se podatelna řídí také při vystavení potvrzení o přijetí takového podání.

4.4 Návaznost elektronické podatelny na organizační strukturu orgánu veřejné moci

Práce v elektronické podatelně musí respektovat vnitřní předpisy orgánu veřejné moci a navazovat na jeho organizační strukturu.

4.5 Požadavky na technické a programové vybavení elektronické podatelny

4.5.1 Soulad se standardy ÚVIS

Technické a programové vybavení elektronické pošty slouží jako informační systém veřejné správy nejen uvnitř orgánu veřejné moci, ale i pro styk s ostatními subjekty. Proto musí informační systém elektronické podatelny jako celek splňovat závazné požadavky standardů ISVS vydané Úřadem pro veřejné informační systémy ve Věstníku ÚVIS.

4.5.2 Technické a programové vybavení pro podání doručené elektronickou poštou nebo na technických nosičích

Technické a programové vybavení elektronické podatelny musí umožnit realizaci všech činností, které jsou požadovány podle nařízení vlády nařízení vlády č. 304/2001 Sb., kterým se provádí zákon o elektronickém podpisu.

Každá elektronická podatelna proto musí zajistit zejména bezpečné uložení:

a) zpráv, které byly do orgánu veřejné moci doručeny jako podání učiněné elektronickou poštou nebo na technickém nosiči,
b) zpráv, které byly odmítnuty, protože byly nečitelné,

c) zpráv, které byly elektronickou poštou přijaty,
d) kopií potvrzení o přijetí a vyřízení podání,
e) archivních záznamů týkajících se podání.

Komentář: Realizace uložení se zajistí:

podle bodu a) – klientskou nebo serverovou částí zpracování elektronické pošty pro podání učiněné elektronickou poštou nebo programovým vybavením pro pořízení kopie podání z technického nosiče,

podle bodu b) – programovým vybavením, jímž se realizuje kontrola podání (tzv. antivirová kontrola) v elektronické poště nebo na technickém nosiči (tzv. karanténní oblast), přičemž tato kontrola může probíhat v klientské nebo serverové části elektronické pošty nebo jako část pracoviště elektronické pošty,

podle bodu c) – programovým vybavením pro pořízení kopie zprávy do bezpečného úložiště přijatých podání nebo programovým vybavením, jímž se realizuje zpracování dokumentů v elektronické podobě,

podle bodu d) – programovým vybavením jímž se vede agenda elektronické podatelny,

podle bodu e) – programovým vybavením pro pořizování kopií souborů do archivu nebo jako součást programového vybavení pro zpracování dokumentů v elektronické podobě.

4.5.3 Technické a programové prostředky pro příjem a odesílání elektronické pošty

Technické a programové prostředky pro příjem a odesílání elektronické pošty musí umožnit zpracování nejméně ve vazbě na SMTP a POP3 s tím, že další rozšíření zveřejní elektronická podatelna spolu s ostatními specifikacemi (na místě veřejně přístupném a to i způsobem umožňujícím dálkový přístup).

4.5.4 Požadavky na kódování znaků národního prostředí

Znaky českého národního prostředí musí být kódovány v souladu se Standardem ISVS pro národní prostředí.

4.5.5 Formáty a mechanizmy pro podání učiněné v elektronické poště

Zpráva elektronické pošty nebo její příloha, obsahující podání, musí být přijímána v textové podobě (formátu *.txt) nebo jako hypertextový dokument (formát *.htm, *.html). Elektronická podatelna může určit další možné přijímané formáty, jejichž seznam zveřejní předepsaným způsobem. Předkladatel podání musí zachovat uvedené přípony jmen souborů.

Příloha zprávy elektronické pošty musí být ve formátu prostého textu (*.txt), nebo hypertextového dokumentu (*.htm, *.html). Elektronická podatelna může určit další možné přijímané formáty, jejichž seznam zveřejní předepsaným způsobem.

*Komentář: Formáty, v nichž je elektronická podatelna povinna podání přijmout, musí být nezávislé na tom, kdo vytvořil program, zařízení atd. Tato produktová nezávislost vede k tomu, že nesmí být stanoven pouze formát odvozený od proprietárních produktů konkrétních firem. Zejména v případě občanů, malých podniků a místních – obecních – samospráv nelze předpokládat, že budou vybaveny jistým technickým nebo programovým vybavením. Formát text (stejně jako hypertextový formát) je obecný, mezinárodně standardizovaný a není vázán na žádný softwarový produkt, lze jej pořídit na prakticky libovolném počítači. Otázka formátu textu se formátu elektronického podpisu netýká. Podatelna může stanovit i další přijímané formáty jako např. *.rtf , *.doc, *.pdf, *.tex, *.602,* .jpg apod.*

Zpráva elektronické pošty obsahující podání musí být zakódována metodou MIME nebo S/MIME. Elektronická podatelna může určit další možné přijímané formáty připojení elektronického podpisu, jejichž seznam zveřejní předepsaným způsobem.

Komentář: Podepisování v souladu s S/MIME je jediným praktickým a standardizovaným postupem. Používání jiných formátů (např. PGP) je sice možné, ale zaručený elektronický podpis je v těchto případech pouze teoretickou možností.

Ověření elektronického podpisu zprávy elektronické pošty se provede mechanizmy tzv. poštovního klienta, případně jinými softwarovými prostředky.

Komentář: Tato funkce je standardní součástí poštovních klientů bez ohledu na výrobce.

4.5.6 Formáty a mechanizmy pro podání na technickém nosiči

Elektronická podatelna musí minimálně zajistit příjem podání v elektronické podobě na technickém nosiči formou diskety s kapacitou 1.44 MB se souborovým systémem FAT16. V případě, že se očekávají ve formě podání rozsáhlé soubory, doporučuje se, aby elektronická podatelna zařadila do přijímaných technických nosičů dat též CD a ZIP, včetně jejich souborového systému. Jejich seznam zveřejní elektronická podatelna předepsaným způsobem.

Elektronická podatelna musí přijímat podání v podobě textu (soubory formátu *.txt) nebo hypertextového dokumentu (soubory formátu *.htm nebo *.html). Elektronická podatelna může určit další možné přijímané formáty, jejichž seznam zveřejní předepsaným způsobem.

Zpráva musí být podepsána elektronickým podpisem v souladu s metodou PKCS#7. Elektronická podatelna může určit další možné přijímané formáty elektronického podpisu, jejichž seznam zveřejní předepsaným způsobem.

Ověření elektronického podpisu zprávy se provede zvláštním programovým vybavením elektronické podatelny k tomu určeným. To musí umožňovat používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

4.5.7 Prostředky pro vytváření a ověřování zaručeného elektronického podpisu

Prostředky pro vytváření a ověřování zaručeného elektronického podpisu musí minimálně vyhovovat podpisovému schématu 1,2 nebo 5 s délkou klíče do 2048 b podle Vyhlášky ÚOOÚ č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

5 Správa prostředků pro vytváření a ověřování elektronického podpisu

Manipulovat s prostředky pro vytváření a ověřování elektronického podpisu:

1. smí pouze fyzické osoby určené pro tuto činnost orgánem veřejné moci, které byly o používání podepisovacích dat, podepisovacích prostředků a o důsledcích takového jednání proškoleny,
2. lze pouze v místnosti, která je pro tuto činnost zabezpečena prostředky technické a objektové bezpečnosti,
3. lze jen v souladu s bezpečnostní dokumentací elektronické podatelny.

Organizačně a technicky musí být zabezpečeno, že elektronická podatelna bude disponovat takovými prostředky, které umožní kdykoliv ověřit elektronický podpis a certifikát s ním spojený.

Za ověřený se v orgánu veřejné moci bude pokládat takový elektronický podpis, jehož připojený certifikát byl kontrolován proti seznamu zneplatněných certifikátů (tzv. CRL), který vydal poskytovatel certifikačních služeb jako poslední předtím, než bylo podání zapsáno do knihy došlé elektr. pošty manuálně nebo automatizovaně.

Elektronická podatelna ověřuje certifikát spojený s elektronickým podpisem jen v tom případě, byl-li vydán akreditovaným poskytovatelem certifikačních služeb. V obráceném případě má elektronická podatelna za to, že elektronický podpis nebyl ověřen.

6 Bezpečnost provozu elektronické podatelny

6.1 Požadavky na bezpečnost

Bezpečnost elektronické podatelny vychází z bezpečnostní politiky orgánu veřejné moci. Pro bezpečnost elektronické podatelny musí být zpracován bezpečnostní projekt (nebo jiný dokument stejné právní síly) v souladu se Standardem ISVS pro náležitosti životního cyklu informačního systému, 005/01.01, Věstník ÚVIS 2000/částka 5. U osobních údajů se musí postupovat podle zákona č. 101/2000 Sb., o ochraně osobních údajů.

Bezpečnostní projekt musí zajistit:

a) ochranu informací, které se zpracovávají v elektronické podatelně,
b) dostupnost těchto informací v souladu s organizačním řádem orgánu veřejné moci.

Bezpečnostní opatření musí vynutit zejména bezpečné nakládání s kvalifikovanými certifikáty, zaručeným elektronickým podpisem a také s podáními (nebo jejich náležitostmi) v přímo čitelné podobě.

Musí být definovány bezpečnostní požadavky v oblastech:

a) administrativní,
b) personální,
c) technické a objektové (jinak zvané též bezpečnost fyzická),
d) informačních systémů a komunikací.

6.2 Řešení typických situací

Plán pro zvládání nestandardních situací stanoví postupy které se uplatní v případě ohrožení úkonů spojených s používáním elektronické podatelny.

Tento plán musí být zpracován v souladu se standardem ÚVIS pro náležitosti životního cyklu informačního systému, 005/01.01, Věstník ÚVIS 2000/částka 5. Součástí plánu pro zvládání nestandardních situací je plán obnovy řádné funkce elektronické podatelny a plán náhradního provozu.

7 Atestace produktů

Elektronická podatelna je informační systém veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Při její implementaci jsou orgány veřejné správy povinny dodržovat standardy ISVS, zejména Standard ISVS pro náležitosti životního cyklu IS. Ten předepisuje povinný rozsah a strukturu dokumentace, která musí být před uvedením do provozu zpracována. Její součástí jsou i Evidenční list pro projekt akvizice a Evidenční list uvedení do provozu, které se zasílají na ÚVIS. Velmi významné je zpracování bezpečnostního projektu podle kapitoly 6 tohoto standardu při uplatnění struktury požadované Standardem ISVS pro náležitosti životního cyklu IS.

Pro prokazování shody elektronické podatelny orgánu veřejné moci s ustanoveními tohoto standardu se nepožaduje atestační řízení. Orgány veřejné moci, které informační systém elektronické podatelny zřizují, jsou povinny při akvizici technického vybavení elektronické podatelny vyžadovat od dodavatele atest na shodu s technickými požadavky obsažené v článku 4.5 tohoto standardu a jakosti dokumentace dodávané jako součást akvizice, tj. systémové příručky, uživatelské příručky a školících a učebních textů v rozsahu a struktuře vyžadované Standardem ISVS pro náležitosti životního cyklu IS.

Atestační řízení bude prováděno podle Standardu stanovujícího povinné požadavky na atestace shody se standardem ISVS pro náležitosti životního cyklu informačního systému (projekt akvizice) a metodik atestace jakosti produktů zpracovaných atestačními středisky a zaregistrovaných Úřadem pro veřejné informační systémy.

Předmětem atestace (objednává ji dodavatel) bude:

a) dokumentace požadovaná Standardem ISVS pro náležitosti životního cyklu IS,
b) technické podmínky vymezené tímto standardem,
c) prohlášení dodavatele o tom, že zprávy elektronické podatelny jsou archivovány, kopírovány a poskytovány oprávněným osobám v souladu se zákonem č. 97/1974 Sb., o archivnictví.

Podmínky shody se Standardem ISVS pro náležitosti životního cyklu IS budou dodavatelem produktu splněny, pokud k atestaci předloží dokumenty: systémová příručka, uživatelská příručka a školící a učební texty ve struktuře požadované Standardem ISVS pro náležitosti životního cyklu IS.

Splnění technických podmínek tohoto standardu bude ověřováno s využitím metodiky atestace jakosti s tím, že předmětem atestace bude pouze funkčnost produktu vymezená v kapitole 4.5 tohoto standardu. Doporučuje se, aby součástí atestu bylo i ověření bezporuchovosti a použitelnosti.

Elektronická podatelna musí u podepsaných zpráv nebo příloh zejména umožnit:

a) Zapsat doručení poštovní zprávy (automaticky bez zásahu obsluhy) do archivu přijaté pošty. Zprávy uložené v archivu elektronické podatelny musí být zabezpečeny před modifikací nebo zničením v souladu se zákonem č. 97/1974 Sb., o archivnictví.
b) Zapsat podání do evidence doručených elektronických podání (ručně nebo automatizovaně).
c) Provést kontrolu na přítomnost virů, trojských koňů, červů apod. či maker.
d) Ověřit elektronický podpis a platnost certifikátu náležejícího k elektronickému podpisu odesílatele.

Elektronická podatelna musí u podání na technických nosičích zapsat toto podání pouze **manuálně** spuštěným procesem do archivu přijatých podání.

V případě, že správce orgánu veřejné moci pořídí technické a programové vybavení elektronické podatelny bez atestu, je povinen tento atest zajistit vlastními prostředky.