

Záznam
z 2. stretnutia pracovnej skupiny pre štandardizáciu nových technológií (PS4)
uskutočneného 3. decembra 2009 na MF SR

Zúčastnení:

Peter Bíro (MF SR), Ján Slovák (MZ SR), Peter Ivanič (ŠÚ SR), Ladislav Földessy (ŠÚ SR), Viktor Birmon (ÚGKK SR), Gabriel Vlk (Colné riaditeľstvo SR), Jiří Slynko (Únia miest Slovenska), Juraj Šitina (ITAS), Roman Fordinal (SKOSI), Štefan Szilva (nezávislý)

Program zasadnutia:

1. Úvod.
2. Diskusia a návrh odporúčaní PS4 k návrhom zmien a úprav predložených štandardov.
3. Ostatné.

Priebeh zasadnutia:

1. Úvod

Zasadnutie pracovnej skupiny viedol p. Bíro a úvodom privítal všetkých účastníkov. Následne v krátkosti zhrnul najmä pre nových zástupcov činnosť a cieľ PS4.

2. Diskusia a návrh odporúčaní PS4 k návrhom zmien a úprav predložených štandardov.

Na začiatku bola zhodnotený stav návrhov nových a úpravy existujúcich štandardov, ktoré boli Komisiou pre štandardizáciu IS VS (ďalej len „Komisia“) a MF SR predložené na posúdenie PS4, ich množstvo a spôsoby predloženia.

PS4 sa ďalej vyjadrovala k jednotlivým návrhom a to s nasledovnými závermi:

Návrhy z roku 2008

1. Zaradenie štandardu ISO/IEC 29500:2008 medzi štandardné formáty, platné pre verejnú správu Slovenskej republiky.

Stanovisko PS4:

Podľa informácií z diskusie bude formát nasadený v apríli 2010. Pre čitateľnosť bude vytvorený plugin, kedy je v súčasnosti otázne (zatiaľ nie je vytvorený), ale bude voľne dostupný. Vzhľadom na fakt, že rozšíriteľnosť tohto formátu teda zatiaľ prakticky neexistuje, navrhuje sa zaradiť iba do odporúčaných formátov. Do budúcnosti sa perspektívne očakáva jeho rozšírenie.

2. Vypustenie verzie 1.0 pri formáte ODF.

Stanovisko PS4:

Kancelárske aplikácie obvykle vytvárajú ODF súbory bez možnosti nastavenia verzie ODF a bez možnosti užívateľskej kontroly použitej verzie ODF. Bezplatné online

validátory pre formát ODF kontrolujú formáty "ODF 1.0/1.1" ako jeden formát. Kancelárske balíky OpenOffice.org, IBM Lotus Symphony a SUN ODF Plugin pre MS Office už budú v roku 2010 integrálne obsahovať aj verziu 1.2 a podpora tejto verzie sa očakáva aj v MS Office. PS4 sa konsenzom dohodla, že návrh je možné akceptovať.

Podľa informácií z diskusie je verzia 1.0 síce ISO norma, ale v praxi sa častejšie používa verzia 1.1 (vydaná začiatkom roka 2007), ktorá je opravnou verziou, rozširujúcou verziu 1.0 o prístupnosť pre zrakovo postihnutých. Kancelárske balíky MS Office 2007 už budú od roku 2010 integrálne obsahovať aj verziu 1.2. PS4 sa konsenzom dohodla, že návrh je možné akceptovať.

3. Do §19 vložiť medzi písmena d) a e) nový odsek:

e) vektorovú grafiku používanie formátu uvedeného v písmene d) bod 2 (SVG) pri odosielaní alebo zverejňovaní, ak je predpokladaná ďalšia úprava súboru

Stanovisko PS4:

Podľa informácií z diskusie je z vektorových formátov SWF neupraviteľné, jediným upraviteľným je formát SVG, takéto znenie preto iba explicitne potvrdí existujúci stav – zapracovanie návrhu je preto možné akceptovať.

Na zváženie sú aj požiadavky vyplývajúce z činností s danými formátmi - zobraziteľnosť a stiahnuteľnosť (ako súbor).

Vzhľadom na časté používanie a dodržanie otvorenosti a technologickej neutrality sa navrhuje aj zaradenie PDF od verzie 1.3 do verzie 1.5 ako vektorového grafického formátu, pri ktorom sa nepredpokladá ďalšia úprava súboru.

Používanie formátu PDF per rastrovú grafiku PS4 zamietla.

Pre krátkosť času bolo len veľmi okrajovo informatívne prediskutované možné zaradenie verzií 1.6 a 1.7 PDF do Výnosu o štandardoch, kde je možné uvažovať o ich zaradení na špecifický účel prezentácie (vizualizácie) elektronických formulárov. Ide o jediné verzie PDF, ktoré umožňujú priamy export a import XML dát z/do PDF vizualizácie formulára. Touto otázkou sa ešte MF SR bude zaoberať a bude potrebné stanovisko Komisie.

Zástupca MF SR vyjadril názor, že by mal výnos vo všeobecnosti pristupovať k verziám formátov jednotne a neuvádzať rozličné verzie pre rôzne účely, pretože v praxi to môže spôsobovať zámieny a zmatečnosť pri snahe o dodržiavanie.

4. Uvádzanie protokolu IMAP v povinnej verzii IMAP4rev1.

Stanovisko PS4:

Praktická aplikácia protokolu IMAP v súčasnosti nepoužíva nižšiu verziu ako IMAP4 resp. revidované znenie IMAP4rev1, ktoré je spätne kompatibilné (je to v podstate iba doplnenie vysvetlenia a drobné opravy). Návrh sa odporúča akceptovať.

5. Predpísanie S/MIME minimálne vo verzii 3, prípadne vo verzii 3.1.

Stanovisko PS4:

Uvedený návrh podlieha Komisii pre informačnú bezpečnosť a nie je predmetom PS4. Podľa informácií z diskusie však napr. Národný bezpečnostný úrad SR v súčasnosti

vyžaduje verziu 3 v rámci vyhlášky 136/2009 Z.z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku.

6. K § 19 V písmene c) sa odporúča doplniť bod 4 formát OpenGIS Geography Markup Language (GML) Encoding Standard.

Stanovisko PS4:

Nie je zrejmé odôvodnenie a dopady prípadnej implementácie. Vzhľadom na špecifickosť je potrebné doplnenie týchto faktov zo strany predkladateľa (ÚGKK SR) a posúdenie aj v PS2.

7. Doplnenie formátu PCM/LPCM (Linear Pulse Code Modulation) pre nekomprimované audio a formátu FLAC (Free Lossless Audio Codec).

Stanovisko PS4:

Formát LPCM sa navrhuje doplniť ku kontajnerovým formátom pre audio WAVE (.wav) a AIFF (.aif) a zapracovať.

Flac je otvorený formát na bezstratovú kompresiu audia. Tento formát sa vzhľadom na nedostatočné rozšírenie, pomernú neznámosť aplikácií, ktorého ho vedia čítať (nepodporuje ho však napr. Flash) t.j. chýbajúcu analýzu jeho podpory odporúča zatiaľ zaradiť iba do odporúčaných štandardov.

K formátu Flac boli v rámci diskusie uvedené aj nasledovné informácie:

- *Umožňuje zmenšiť nekomprimované LPCM audio približne o 50%.*
 - *Niektorí členovia PS4 vyjadrili názor, že bezstratová kompresia audia sa vo verejnej správe pravdepodobne príliš často nepoužíva.*
 - *Výnos o štandardoch už od roku 2006 vyžaduje od verejnej správy používanie celej rodiny MPEG-4 formátov, ktoré obsahujú aj bezstratové kompresie MPEG-4 ALS, MPEG-4 SLS a MPEG-4 DST. Tieto MPEG-4 formáty sa však ani vo svete takmer vôbec nevyužívajú a je pre ne dostupná len veľmi malá podpora, pretože prišli na trh až okolo roku 2006, kedy tu už niekoľko rokov existovali viaceré bezstratové audio kompresie.*
 - *Flac má podľa niektorých verejne dostupných informácií najlepšiu hardvérovú a softvérovú podporu spomedzi užívateľsky orientovaných bezstratových kompresí audia.*
 - *Flac je obvykle podporovaný vo väčšine prehrávačov, ktoré podporujú formáty Ogg. Na prehrávanie formátu FlacC je napríklad v MS Windows možné nainštalovať kodeky alebo univerzálny prehrávač (napr. VLC), čo je však potrebné pri veľkej časti audio a video formátov uvedených vo Výnose o štandardoch.*
8. §20 sa navrhuje upraviť na „prijímanie a čítanie všetkých doručených formátov audio a video súborov, ktorými sú
- *kontajnerový formát OGG (.ogg, .oga, .ogv) pre audio, video, audio spolu s videom - s použitím video kompresí x264, XVID, Theora alebo Huffiyuv a audio kompresie MP3, Vorbis alebo Flac.*

Stanovisko PS4:

Uvedený návrh už je súčasťou existujúceho výnosu okrem formátu Flac a Huffvov. K formátu Flac platí stanovisko z pripomienky 7. Formát Huffvov je formát bezstratovej kompresie videa, vzhľadom na nízke rozšírenie využívania videa vo verejnej správe sa tento zatiaľ neodporúča zaradiť.

Formáty x264 a XVID uvedené v návrhy sú konkrétne softvérové aplikácie – x264 je určený na vytváranie (enkódovanie) videa vo formáte H.264 (MPEG-4 Part 10) a XVID je určený na vytváranie a dekódovanie videa vo formáte MPEG-4 Part 2.

9. K §6, §7, §9 a všeobecne k šifrovaniu

Pri zabezpečenom prenose dát a zabezpečených protokoloch sa navrhujú uvádzať minimálne povinné vlastnosti šifrovania/zabezpečenia:

- SSL - minimálne verzia SSLv3
- pri používaní "public-key cryptography" dĺžka kľúča musí byť minimálne 1024bit, odporúča sa 2048bit
- pre symetrické šifrovanie je povinné používať jeden z algoritmov AES128, AES256, Triple DES, Blowfish448bit ... atď.
- pre hash funkcie je povinné používať jeden z algoritmov MD5, SHA-256 ... atď.

Stanovisko PS4:

Uvedený návrh podlieha Komisii pre informačná bezpečnosť a nie je predmetom PS4.

Vo všeobecnosti je možné konštatovať, že v prípade používania krátkych dĺžok SSL/TLS kľúčov, prelomených hash algoritmov použitých v kľúčoch a slabých šifrovacích algoritmov nie je možné hovoriť o skutočne zabezpečenom prenose dát. PS4 navrhuje zaviesť do odporúčaných štandardov opačný princíp – uvádzanie tých algoritmov, ktoré sa už nemajú používať.

PS4 nenavrhuje zmenu v požiadavkách ohľadom SSL 3.0.

Podľa informácií z diskusie je TLS 1.0 jemne modifikovanou podobou SSL 3.1.

Predbežné stanovisko Komisie pre IB (informatívne):

V návrhu 5 sa odporúča doplniť verziu pre SSL v 3 na SSL v3.1, a zväžiť použitie algoritmu MD5 (bol už rozbitý).

10. K §8 sa navrhuje doplniť:

"c) podpora formátu OpenPGP (Pretty Good Privacy) pri chránenom prenose elektronických poštových správ"

Stanovisko PS4:

Uvedený návrh podlieha Komisii pre informačná bezpečnosť a nie je predmetom PS4. PS4 odporúča zaviesť uvedenú požiadavku iba ako odporúčaný štandard.

Predbežné stanovisko Komisie pre IB (informatívne):

S formátom OpenPGP je pravdivé čo sa týka dostupnosti, ale je treba uvážiť jeho použitie kvôli nižšej dôveryhodnosti (je tam prenášaná dôveryhodnosť, neexistuje tam centrálna autorita).

Odporúča sa vypustiť hash algoritmus MD5 a orientovať sa na hash algoritmy z rodiny SHA2 (t.j. SHA256, SHA384 a SHA512).

Navrhuje sa, aby 1. Boli odporúčanými štandardmi počas prechodného obdobia (napríklad počas dvoch rokov). 2. Boli povinnými štandardmi po uplynutí prechodného obdobia uvedeného bode 1., uvedenom vyššie.

11. K §15 sa navrhuje doplniť:

"h) zverejnenie minimálne jedného verejného kľúča spolu s e-mailovou adresou pre chránený prenos elektronických poštových správ vo formáte S/MIME alebo OpenPGP a zverejnenie adresy alebo telefónneho čísla, na ktorých je možné overiť pravosť tohto kľúča s pomocou odtlačku prsta kľúča (fingerprint)"

Bolo zaevidovaný aj upravený návrh, ktorý znel nasledovne:

Znenie pôvodného návrhu: Do §15 Obsah webového sídla sa navrhuje doplniť:

Variant A

"g) zverejnenie minimálne jedného verejného kľúča spolu s e-mailovou adresou pre chránený prenos elektronických poštových správ vo formáte S/MIME (§8 písm. b), Variant B

"g) zverejnenie minimálne jedného verejného kľúča spolu s e-mailovou adresou pre chránený prenos elektronických poštových správ vo formáte S/MIME (§8 písm. b), ak správca obsahu chránený prenos elektronických poštových správ používa,

Stanovisko PS4:

Táto problematika patrí do kompetencie Komisie pre IB, PS4 však vecne s návrhom súhlasí. Zo zavedenia uvedenej požiadavky PS4 neočakáva administratívne ani finančné dopady.

12. K §15 sa navrhuje doplniť :

"i) zverejnenie adresy alebo telefónneho čísla, na ktorých je možné overiť pravosť certifikátov a verejných kľúčov (pre SSL, TLS, OpenPGP) používaných organizáciou verejnej správy pre elektronické služby."

Bolo zaevidovaný aj upravený návrh, ktorý znel nasledovne:

Znenie pôvodného návrhu: Do §15 Obsah webového sídla sa navrhuje doplniť:

"h) zverejnenie adresy alebo telefónneho čísla, na ktorých je možné získať kontrolné číslo (tzv. "fingerprint") pre overenie pravosti certifikátov a verejných kľúčov (SSL, TLS, S/MIME) používaných organizáciou verejnej správy pre elektronické služby a elektronické poštové správy."

Stanovisko PS4:

Táto problematika patrí do kompetencie Komisie pre IB, PS4 však vecne s návrhom súhlasí. Zo zavedenia uvedenej požiadavky PS4 neočakáva administratívne ani finančné dopady.

Vzhľadom na rozšírenosť používania vlastných bezplatných šifrovacích certifikátov a verejných kľúčov (tzv. "self signed"), ktoré neboli vydané certifikačnou autoritou, má tento štandard umožniť overenie ich pravosti.

- 13.** V § 20 sa odporúča štandardy pre audio a video súbory vo verzii 1. 1 uvedené v písm. a) rozšíriť o ďalšie body, a to o formát súborov Windows media ...(.wm, wma,wmv) a Wave sound (.wav) z dôvodu, že ide o celosvetovo bežne používané typy súborov.

Stanovisko PS4:

Formáty triedy Windows media... sú proprietárne formáty OS Windows a z tohto dôvodu sa neodporúča ich zaradenie.

Navrhuje sa zapracovať formát WAVE do novely spolu s časťou požiadavky podľa vyššie uvedenej pripomienky 7, nakoľko je to základný formát pre nekomprimované audio.

- 14.** V § 18 Textové súbory, písm. c) sa navrhuje vložiť za slovo „.doc“ čiarku a za ňu slovo „.docx“.

Stanovisko PS4:

Návrh výnosu z dôvodu nezachovávanie technologickej neutrálnosti neobsahuje formát .doc a z rovnakého dôvodu sa odporúča nezaraďovať ani formát .docx.

- 15.** K § 1 – Odporúča sa rozšíriť rozsah ustanovených štandardov pre informačné systémy verejnej správy o štandardy pre riadenie IT služieb (napr. ITIL a pod.)

Stanovisko PS4:

Nie sú zrejmé dopady prípadnej plošnej implementácie. Vzhľadom na vecný obsah sa odporúča posúdiť v PS5. Uvedený štandard je potrebné zvážiť aj v súlade s navrhovaným štandardom pre riadenie IT projektov.

- 16.** V § 11 navrhuje sa doplniť písmená g), h) a i), ktoré znejú:

- „g) Web Feature Service a Web Coverage Service na poskytovanie priestorových údajov
- h) Web Catalogue Service na vyhľadávanie údajov a služieb na základe popisných informácií – metaúdajov
- i) protokol „Networked Transport of RTCM via Internet Protokol“ (NTRIP) na prenos údajov globálnych navigačných satelitných systémov (GNSS) cez internet (použitím HTTP), obzvlášť diferenciálnych korekcií pre statických ako aj mobilných používateľov GNSS“.

Stanovisko PS4:

Nie je zrejmé odôvodnenie a dopady prípadnej implementácie. Vzhľadom na špecifickosť je potrebné doplnenie týchto faktov zo strany predkladateľa (ÚGKK SR) a posúdenie aj v PS2.

- 17.** V § 39 navrhuje sa doplniť písmeno k), ktoré znie:

„k) špecifikácia OpenGIS Geo Digital Rights Management na poskytovanie geografických informácií z informačných systémov verejnej správy“

Stanovisko PS4:

Nie je zrejmé odôvodnenie a dopady prípadnej implementácie. Vzhľadom na špecifickosť je potrebné doplnenie týchto faktov zo strany predkladateľa (ÚGKK SR) a posúdenie aj v PS2.

18. V § 13 písmeno a) navrhujeme rozšíriť o „XML stylesheet language transformation (XSLT)“.

Stanovisko PS4:

Vzhľadom na bežné používanie tohto jazyka a dôležitosť pre elektronické formuláre a používanie dátových prvkov sa odporúča zaviesť. Jazyk spĺňa aj pravidlá otvorenosti a technologickej neutrality.

XSLT je W3C štandard platný od roku 1999 a je založený na XML.

19. V § 19 písmeno a) navrhuje sa doplniť bod 6, ktorý znie:

„ 6. Rastrový monochromatický obraz s kompresiou CCITT“

Stanovisko PS4:

Nie je zrejmé odôvodnenie a dopady prípadnej implementácie. Vzhľadom na špecifickosť je potrebné doplnenie týchto faktov zo strany predkladateľa (ÚGKK SR) a posúdenie aj v PS2.

20. V § 19 písmeno c) navrhuje sa doplniť body 4 a 5, ktoré znejú

„4. Výmenný grafický interfejs (VGI)

5. Extensible Markup Language (XML,GML)“.

Stanovisko PS4:

Nie je zrejmé odôvodnenie a dopady prípadnej implementácie. Vzhľadom na špecifickosť je potrebné doplnenie týchto faktov zo strany predkladateľa (ÚGKK SR) a posúdenie aj v PS2. VGI je špecifický formát, vyvinutý pre potreby ÚGKK SR, jeho otvorenosť je PS4 neznáma. GML je možné v súlade so všeobecnou akceptáciou XML uvažovať, avšak odporúča sa overiť vhodnosť umiestnenia tohto návrhu ako príslušného bodu resp. úprava formulácie.

21. Za § 21 navrhujeme vložiť nový paragraf, ktorý znie:

„§ X

Formáty údajov na určenie polohy použitím globálnych navigačných satelitných systémov
(1) Štandardom na poskytovanie diferenciálnych korekcií GNSS v reálnom čase je formát RTCM.

(2) Štandardom na poskytovanie údajov o čase a polohe určenej použitím GNSS v reálnom čase je NMEA GGA.“

Stanovisko PS4:

Nie je zrejmé odôvodnenie a dopady prípadnej implementácie. Vzhľadom na špecifickosť je potrebné doplnenie týchto faktov zo strany predkladateľa (ÚGKK SR) a posúdenie aj v PS2.

22. V § 23 odsek 1 písmeno a) navrhujeme doplniť body 4 a 5, ktoré znejú:

„4. CAB (.cab)

5. RAR (.rar)“

Stanovisko PS4:

Obidva formáty sú proprietárne, čo odporuje požiadavkám interoperability a požiadavkám na otvorenosť štandardov. CAB je navyše veľmi špecifický typ archivačného formátu pracujúci s viacerými metódami kompresii. Formát RAR je možné vytvárať iba s pomocou proprietárnych aplikácií, ktoré získali potrebný súhlas od autora tohto formátu. Návrh sa neodporúča zapracovať.

23. Vzhľadom na rast elektronických služieb všetkých typov, objem a význam elektronických dát nielen novovytvorených, ale vytvorených aj procesom masovej digitalizácie navrhujeme zvýrazniť a doplniť § 36 a § 37 pre zálohovanie a fyzické ukladanie záloh aj s uvedením štandardov / napr. ISO 14721:2003 pre OASIS, ISO 15489-2001, EAC, EAD, DPE, BRAMBORA/

Stanovisko PS4:

Zástupca MF SR skonštatoval, že uvádzanie noriem sa na základe stanoviska Legislatívnej rady Vlády SR v predchádzajúcom schvaľovacom procese výnosu používa v metodickom pokyne a nie v znení výnosu. Predložené štandardy sa týkajú archivácie, ktorú bude najprv potrebné prediskutovať s gestorom príslušnej legislatívy (MV SR).

24. Používanie písiem (fontov) v značnej miere ovplyvňuje prenositeľnosť dokumentov, a to nielen medzi rôznymi platformami, ale aj rôznymi počítačmi s rovnakým operačným systémom. Ak potrebné písmo nie je na danom počítači dostupné, môže dôjsť k narušeniu formátovania alebo aj k nesprávnemu zobrazeniu znakov. Navrhujeme preto, aby Výnos predpísal aj sadu písiem, ktoré sa smú používať. Akceptovateľným kandidátom by mohla byť trojica písiem Arial (bezpätkové písmo), Times New Roman (pätkové písmo) a Courier New (písmo s pevnou šírkou znakov). Tieto, bohužiaľ, nie sú licenčne celkom voľne prístupné, existuje však sada písiem Liberation Sans, Liberation Serif and Liberation Mono, ktorá je s uvedenými písmami metricky kompatibilná. Do Výnosu navrhujeme doplniť nasledujúci paragraf:

Štandardom v textových dokumentoch, prezentáciách a ďalších súboroch, ak to je technicky relevantné, je

- a) používanie písiem Arial (bezpätkové písmo), Times New Roman (pätkové písmo) a Courier New (písmo s pevnou šírkou znakov) alebo im metricky kompatibilných písiem Liberation Sans, Liberation Serif and Liberation Mono,
- b) vkladanie (embedding) použitých písiem v prípade súborov vo formáte .pdf

Bod b) umožňuje v pdf súboroch používať ľubovoľné písma, pokiaľ sú v samotnom súbore vložené.

Stanovisko PS4:

Vzhľadom na časté komplikácie napr. pri zverejňovaní tlačív verejnou správou a "rozhádzania" ich vzhľadu v dôsledku použitia neštandardných fontov sa uvedený návrh odporúča zapracovať.

Z diskusie vyšiel návrh, aby štandard predpisoval, že pri zverejňovaní niektorých typov informácií (napríklad texty právnych predpisov a pod.) majú byť používané navrhnuté základné 3 fonty alebo ich náhrady. Keďže však z legislatívneho hľadiska nie je možné všeobecne špecifikovať účel použitia, MF SR sa pokúsi navrhnúť vhodnú formuláciu.

K návrhu boli ďalej uvedené nasledovné fakty:

- *Metricky kompatibilné písma zachovávajú základné rozmery písma (šírka, výška), vďaka čomu je pri ich použití možné zachovať vzhľad tlačiva alebo iného zverejneného dokumentu.*
- *Pri otvorení napr. formátu HTML, používajúceho fonty, ktoré nie sú k dispozícii štandardne prichádza k ich nahradeniu inými fontami, ktoré sú k dispozícii (ak je tak HTML vytvorené).*
- *Fonty Times New Roman, Arial a Courier New sú v základe komerčné, nie sú však známe prípady, že by ich komerčnosť bola riešená. Existujú aj rôzne špecifické fonty, ktoré majú licenčné obmedzenia.*
- *Fonty Liberation a rôzne ďalšie bezplatné a voľne šíriteľné fonty sa v niektorých aplikáciách a operačných systémoch používajú ako predvolené náhrady za Times New Roman, Arial a Courier New.*
- *Niektoré interné pravidlá organizácií verejnej správy, ale aj štandardizované procesy (napr. Legislatívne pravidlá vlády SR alebo tvorba diplomových prác) už dnes vyžadujú, aby boli určité materiály vytvárané s použitím predpísaných fontov (často je to font Times New Roman).*

25. V §20, písm. a) doplňte bod 5 v znení:

5. nekomprimovaný formát audio (.wav) s parametrami

Stanovisko PS4:

Stanovisko totožné so stanoviskom k pripomienke 13.

26. K § 4 - Prenos dát

- a) Štandardom pre prenos dát vo verzii 1.0 je používanie protokolu File Transfer Protocol (FTP) alebo protokolu Hypertext Transfer Protocol (HTTP).
- b) Podpora chráneného prenosu dát cez kryptografický protokol vo verzii 1.1 je secure shell verzia 2(SSHv2) alebo protokolu SSH File Transfer Protocol (SFTP).

Stanovisko PS4:

Pre zavedenie štandardu chýba podrobnejšie zdôvodnenie vzhľadom na už platné štandardy IPSEC a SSL/TLS. Predkladateľ (ÚV SR) by mal doplniť zdôvodnenie a analýzu kritérií. PS4 sa bude prípadným schvaľovaním štandardom zaoberať až po doplnení zdôvodnenia.

Zatiaľ sa neodporúča uvedený návrh zaviesť, odporúča sa však zváženie Komisiou pre informačnú bezpečnosť. K návrhu boli ďalej uvedené nasledovné fakty:

- *SSH (Secure Shell Protocol) je sieťový protokol pre zabezpečené vzdialené prihlásenie/pripojenie a pre zabezpečené používanie sieťových služieb cez nezabezpečenú sieť. Najčastejšie sa používa napríklad na vzdialené používanie a správu počítačov a serverov, na zabezpečený prenos súborov a podobne.*
- *SSH je štandard definovaný v RFC (4250-4256, 4335, 4344, 4345).*
- *SSH je najviac používaný v unixových technológiách.*
- *SSL je omnoho rozšírenejší.*
- *SSH a SSL sú navzájom nekompatibilné, čo môže spôsobiť veľké problémy v interoperabilite a obvykle sa používajú pre rozdielne účely*
- *SFTP je sieťový protokol pre zabezpečený prenos súborov a pre zabezpečený vzdialený prístup k súborovému systému*
- *Pre SFTP zatiaľ neexistuje ISO a existuje iba návrh RFC (posledný z roku 2006), pričom oficiálna verzia RFC zatiaľ nebola vydaná.*
- *SFTP je možné používať aj bez SSH, s pomocou iných kryptografických protokolov (napr. TLS, SILC)*
- *SFTP používaný s protokolom SSH je často podporovaný užívateľským softvérom ktorý zároveň podporuje protokol FTPS*
- *SSH využíva napr. MV SR, CR SR zase využíva najmä SSL.*

27. V § 19 písm. c) Odporúčame pridať formát pre technické výkresy CAD, napríklad ".dxf".

Stanovisko PS4:

Uvedený formát nie je bežne používaný a môže vyžadovať proprietárny softvér, zavedenie všeobecnej povinnosti sa preto neodporúča. Jeho použitie je možné požadovať na špecifické účely, ktoré však musí definovať predkladateľ (Sociálna poisťovňa), vo všeobecnosti je možné na jeho použitie využiť všeobecnú výnimku § 17. Drawing Exchange Format (DXF) je podľa dostupných informácií proprietárny formát.

Návrhy z roku 2009

1. Navrhuje sa vypustenie samorozbal'ovacieho ZIP.

Stanovisko PS4:

Vzhľadom na proprietárnosť aplikácií, umožňujúcich plnohodnotné používanie samorozbal'ovacích ZIP súborov a ich vzájomnej nekompatibility PS4 odporúča návrh akceptovať.

Samorozbal'ovací ZIP nie je podporovaný v množstve aplikácií, ktoré však samotný formát ZIP podporujú. Samorozbal'ovací ZIP je aplikácia (program), ktorá po svojom spustení rozbalí ZIP súbor v nej obsiahnutý. Funkčnosť takejto aplikácie nie je v špecifikácii ZIP formátu plne zdokumentovaná, čo je v rozpore s požiadavkou otvorenosti a platformovej neutrality. Podľa špecifikácie používa príponu .exe, ktorá ako taká prislúcha spúšťačným (vykonateľným) typom súborov.

2. Potreba definovať štandardy pre informačné systémy na správu elektronických registratúrnych záznamov a to najmä v súvislosti s pripravovanou realizáciou spoločného modulu ÚPVS - Modulu dlhodobého ukladania elektronických registratúrnych záznamov

Stanovisko PS4:

Z uvedeného nie je zrejmé aké štandardy má predkladateľ na mysli. Odporúča sa v súlade so stanoviskom k pripomienke 23 z roku 2008.

3. Zavedenie princípu špecifickej výnimky pre zverejňovanie na webovom sídle pre:
 - prezentačné súbory
 - tabuľkové súbory

Zdôvodnenie: dvojakosť používaných princíпов

Stanovisko PS4:

Vzhľadom na dodržanie jednotnosti princíпов štandardizácie odporúča PS4 návrh akceptovať.

4. Vysporiadanie problematiky grafických súborov s textovým obsahom (skenované vzory, plagáty) a to v súlade s princípmi pre PDF

Zdôvodnenie: variabilnosť súčasného výkladu a problém určovania porušovania / dodržiavania

Stanovisko PS4:

PS4 vzhľadom na už existujúci princíp pre PDF odporúča návrh akceptovať.

Textový obsah by mal byť kopírovateľný a vyhľadávateľný. Za textový obsah, ktorý je potrebné poskytovať vo formáte textu sa bude štandardne považovať len tlačené písmo a ručne písané písmo môže zostať v podobe grafiky. Tento štandard sa týka najmä všetkých zoskenovaných textových dokumentov. Plagáty, ktoré nespĺňajú definíciu úradných dokumentov alebo dôležitých verejných oznamov a neobsahujú čitateľné tlačené formáty, je možné považovať za grafiku, pri ktorej nebude potrebná prístupnosť textu. Na prevod obrázkov zoskenovaných dokumentov do textového obsahu sa najčastejšie používa softvér označovaný ako OCR - Optical Character Recognition.

V rámci diskusie zazneli aj upozornenia, že PDF formát má rôzne možnosti ochrany svojho obsahu. Je možné napríklad použitie ochrany PDF súboru proti kopírovaniu textu, vypnúť prístup k textu pre nástroje prístupnosti, zakázať tlač alebo vyplňanie polí.

5. Do §14 Prístupnosť webových stránok navrhujem doplniť medzi povinné body z pravidiel prístupného webu aj: "bod 3.2"

Stanovisko PS4:

Uvedená problematika nie je predmetom PS4, spadá do kompetencie PS3.

Vzhľadom na nedostatok času, veľký rozsah a veľmi neskoré predloženie sa na tomto stretnutí PS4 nezaoberala návrhmi p. Szilvu, ktoré ním boli predložené niekoľko dní pred stretnutím PS4. Členovia PS4 boli zástupcom MF SR informovaní, že prípadné zaradenie niektorého z ďalších návrhov štandardov do súčasnej novely bude podľa uváženia ponechané

na MF SR resp. Komisiu, ostávajúce návrhy budú predmetom diskusie ďalšieho stretnutia PS4.

Zástupca MF SR požiadal prítomných, aby mu v rámci možností e-mailom zaslali vyjadrenia k štandardom, ktoré sa nestihli prebrať na zasadaní.

Návrhy smerujúce k Metodickému pokynu k Výnosu o štandardoch ešte budú môcť byť prerokované neskôr, keďže Metodický pokyn bude vydaný až po ukončení celého legislatívneho procesu novely výnosu.

3. Ostatné

P. Bíro informoval o predpokladanom časovom harmonograme novely Výnosu o štandardoch pre IS VS.

Záver:

1. Zpracovať stanoviská PS4 do návrhu novely výnosu a upravené znenie predložiť na stretnutie Komisie dňa 9. decembra 2009.
T: 8.12.2009
2. Zástupca ÚGKK SR spracuje požadované informácie k vecne príslušným návrhom štandardov a zástupca ÚGKK SR v PS2 ich predloží PS2 na prerokovanie.
T: 28.2.2010
3. Návrhy vyžadujúce si doplňujúce informácie zo strany ostatných predkladateľov budú s nimi relevantne prediskutované.
T: na zvážení MF SR v súlade s procesmi štandardizácie
4. Návrhy vyžadujúce si stanoviská iných pracovných skupín budú nimi relevantne prediskutované.
T: v súlade so stretnutiami jednotlivých pracovných skupín
5. Zaslanie pripomienok k návrhom štandardov, ktoré neboli prebrané na stretnutí.
T: 15.1.2010