Štandardy pre IS VS a ich aplikácia v praxi

Peter Bíro

Ministerstvo financií
Slovenskej republiky

Mojmírovce, máj 2009

Interoperabilita

- Interoperabilita je schopnosť informačných a komunikačných systémov spolupracovať t.j. vymieňať si údaje a spoločne ich používať
  - Organizačná interoperabilita (koordinácia a usporiadanie transakčných procesov a informačnej architektúry)
  - Sémantická interoperabilita (zabezpečenie, aby bolo presné znenie počas výmeny informácií zrozumiteľné pre osobu alebo aplikáciu prijímajúcu tieto údaje)
  - Technická interoperabilita (technológia fyzického prepájania informačných systémov za účelom výmeny informácií)
- Štandardy sú nástrojom interoperability
  - Štandardizácia je väčšinou chápaná iba ako striktne normatívna činnosť (STN, ISO, ETSI a podobne), ale štandardy sú často krát založené aj na nenormatívnych princípoch (WCAG, OECD, zaužívaná prax)

Činnosť na úrovni EÚ

- Európsky rámec interoperability 2.0 (vypracovaný v rámci pracovnej skupiny pod komunitárnym programom IDABC)
  - podpora poskytovania paneurópskych služieb pre občanov a podniky v rámci e-governmentu
  - Technické postupy a špecifikácie na pripojenie k ISVS v rámci EÚ
  - Podpora otvorených štandardov a „open source"
  - Dve nové úrovne interoperability:
    - Legislatívna interoperabilita (elektronické údaje vytvorené v jednom ČŠ majú rovnakú právnu silu a zavedenie aj v inom ČŠ)
    - Politická interoperabilita (horizontálna – kontext politík má pre spolupracujúcich partnerov kompatibilné vízie, harmonizované priority a je zameraný na rovnaké ciele)

Činnosť na úrovni EÚ

- Ďalšie projekty a iniciatívy na úrovni EÚ:
- Európska stratégia pre interoperabilitu
  - Najvyšší rámcový dokument – nadradený ERI 2.0
- CAMSS („štandardizácia štandardizácie")
  - definuje 4 hlavné kritériá – vhodnosť, potenciál, otvorenosť a podmienky na trhu
- SEMIC (www.semic.eu)
  - PS zameraná na sémantickú interoperabilitu
  - V súčasnosti najmä tvorba terminológie a oblasť multijazyčnosti
- OSOR (www.osor.eu)
  - Open Source Observatory and Repository – zameranie na otvorený zdrojový kód

Legislatíva v súvislosti so štandardizáciou

- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
  - účinný od 1. júna 2006
  - § 6 –Štandardom je súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných systémov verejnej správy, ktorý obsahuje charakteristiky, metódy, postupy a podmienky, najmä pokiaľ ide o bezpečnosť a integrovateľnosť s inými informačnými systémami.
  - **§ 13** - kompetencia MF SR vydávať štandardy
- Výnos MF o štandardoch pre ISVS (účinný od 1.10.2008)
- Metodický pokyn k výnosu o štandardoch pre ISVS
- Ďalšie metodické pokyny – dátové štandardy, terminológia
- Novela zákona po Legislatívnej rade Vlády SR

Koordinácia štandardizácie

- Ministerstvo financií SR (od 1.2.2007)
  - Kompetenčný zákon – MF SR ako gestor informatizácie spoločnosti
  - Zákon o ISVS - Právomoc stanovovať a vydávať štandardy
  - Kontrolný orgán
  - Na starosti má: Sekcia informatizácie spoločnosti – Odbor legislatívy, metodiky, štandardov a bezpečnosti SR
- Komisia pre štandardizáciu IS VS pri MF SR
  - Zastúpenie rezortov, súkromnej aj akademickej sféry
  - Pracovné skupiny pre jednotlivé oblasti štandardizácie
- Komunikácia:
  - web: www.informatizacia.sk (menu: eGovernment/Štandardy pre IS VS)
  - e-mail: standard@mfsr.sk

Koordinácia štandardizácie

- Pracovná skupina pre dátové štandardy (PS1)
- Pracovná skupina pre štandardy priestorovej identifikácie (PS2)
- Pracovná skupina pre prístupnosť webových stránok (PS3)
- Pracovná skupina pre štandardizáciu nových technológií (PS4)
- Pracovná skupina pre optimalizáciu existujúcich štandardov a procesov (PS5)
- Pracovná skupina pre štandardizáciu formulárov elektronickej verejnej správy (PS6)
- Pracovná skupina pre štandardizáciu terminológie v oblasti informatizácie spoločnosti (PS7) – február 2009
- Pracovná skupina pre základné číselníky (PS8) – marec 2009

Koordinácia štandardizácie

- Ďalšie oblasti tvorby špecifickej štandardizácie:
  - Zdravotníctvo (MZ SR – NCZI)
  - Priestorové informácie (ÚGKK SR)
  - Elektronický podpis (NBÚ SR)
  - Kybernetický priestor?? (NBÚ SR)

Štandardizácia - úvod

- Životný cyklus štandardov:
  1. Odporúčaný (príloha metodického pokynu)
  2. Povinný (výnos)
  3. Zrušený (príloha metodického pokynu)
- Schvaľovací procesov vydávania štandardov
  1. Príslušná PS
  2. Komisia pre štandardizáciu IS VS
  3. VPK MF SR
  4. MPK
  5. Technická komisia pri Legislatívnej rade Vlády SR

Základné oblasti štandardizácie

1. Skupina - vydané
   - Technické štandardy (pre prepojenie, pre prístup k elektronickým službám, pre webové služby, pre integráciu dát)
   - Štandardy prístupnosti a funkčnosti webových stránok
   - Štandardy použitia súborov
   - Štandardy názvoslovia elektronických služieb
   - Bezpečnostné štandardy (štandardy pre architektúru riadenia, štandardy minimálneho technického zabezpečenia)
   - Dátové štandardy

Základné oblasti štandardizácie

2. Skupina - pripravované

- Štandardy pre elektronické formuláre (t.j. formuláre elektronickej verejnej správy)
- Štandardy pre priestorovú identifikáciu
- Štandardy pre procesné riadenie
- Terminologické štandardy v oblasti informatizácie spoločnosti
- Štandardizované číselníky (čiastočne vydané)

3. Skupina – zatiaľ nezačaté prípravné procesy

- Štandardy pre metadáta

Princípy implementácie

- Všeobecné princípy:
  - Zmluvy, zmluvy, zmluvy! - dodávatelia majú dodržiavať platnú legislatívu, odporúča sa explicitne uvádzať samotný zákon 275/2006, prípadne platný výnos o štandardoch
  - Čítanie metodík
  - Komunikácia s kontrolným orgánom (MF SR) – standard@mfsr.sk a s ostatnými povinnými či inými osobami navzájom
  - Zdravý rozum – informácie a služby sú poskytované pre ľudí a to spôsobom, aby sa k nim dostali, pochopili ich a použili a nie iba preto, lebo „tak je písané"
  - Kritériá hodnotenia dodržiavania štandardov zohľadňujú istú mieru tolerancie
- Cieľom nie je rozdávať pokuty, ale zabezpečiť, aby boli štandardy skutočne implementované.

Princípy implementácie

- Výnos obsahuje už iba povinné požiadavky resp. štandardy
- § 1 - Vzťah k zákonu
- § 2 - Definície
  - Webová stránka; webové sídlo
  - Správca obsahu; technický prevádzkovateľ
  - Bezpečnostný incident
  - Technické komponenty IS VS; zariadenia IS VS

Technické štandardy

- § 3 - § 13 – Technické štandardy
  - § 3 - § 8 – Štandardy pre prepojenie (UDP, IPv4 + IPv6, FTP, DNS, SMTP, POP3, IMAP, MIME)
  - § 9 - § 10 – Štandardy pre prístup k elektronickým službám (HTTP, XHTML, LDAP)
  - § 11 – Štandardy pre webové služby (SOAP, HTTP, WSDL, UDDI, WMS)
  - § 12 - § 13 – Štandardy pre integráciu dát – podporné štandardy pre dátové štandardy (XML, XSD, UTF)
  - Pri všetkých podpora bezpečnostných protokolov (SSL, TLS, IPSEC, S/MIME)

Štandardy prístupnosti (a funkčnosti) webových stránok

- § 14 + príloha 1 – Štandardy prístupnosti webových stránok
  - Tieto štandardy sú monitorované od roku 2005, metodika finalizovaná začiatkom roku 2008
  - Narastajúci tlak EÚ na ich dodržiavanie (presadzovanie najmä WCAG 2.0)
  - Žiadny z týchto ani nasledujúcich štandardov neurčuje mať webové sídlo
  - Požadovaná úroveň je 90%:

2008	VS (310)	13,55%	ŠS (148)	13,51%	ÚS (162)	13,58%
2009 I	VS (150)	29,21%	ŠS (89)	14,75%	ÚS (61)	23,33%

  - Situácia sa pomaly zlepšuje, ale monitorovania zatiaľ stále ukazujú nie veľmi pozitívne výsledky

Priemerné hodnoty pre prístupnosť

2008 - Celkovo (493) 75,47%							
Verejná správa (310)	75,2%						
Štátna správa (148)	76,1%	ÚOŠS (24)	77,1%				
Samospráva (162)	75,9%	VÚC (8)	80,9%	Mestá (73)	75,8%	Ostatné obce (68)	74,5%
Sektor zdravotníctva (25)	75,9%						
Nákupné centrá a sprostredkovateľské služby (23)	75,9%						
Sektor školstva (35)	75,1%						
Médiá (12)	74,1%						
Poisťovne (14)	68,8%						
Banky (13)	64,6%						
2009 - Celkovo (150) 77,76%							
Verejná správa (150)	77,76%						
Štátna správa (89)	79,4%	ÚOŠS (23)	77,1%				
Samospráva (61)	76,1%	VÚC (8)	83%	Mestá (34)	73,4%	Ostatné obce (17)	76,7%

Štandardy prístupnosti (a funkčnosti) webových stránok

- Najčastejšie chyby:
  - Nesprávne alebo chýbajúce popisy (pravidlo 1, najmä bod 1.1)
  - Zlý kontrast (bod 2.1)
  - Chýbajúce nadpisy (tam, kde majú existovať) (bod 3.5)
  - Chýbajúce zoznamy (tam, kde majú existovať) (bod 3.6)
  - Systémovo nepopísané formuláre a aktívne prvky (bod 12.4)
  - Nenastavený alebo nesprávne nastavený jazyk stránky v kóde (SK / EN) (bod 4.3)
  - Nenastavená hlavička tabuliek (bod 5.1)
  - Flash (bod 7.3), závislosť od myši (Java) (pravidlo 8)
  - Neoznačené ciele odkazov (bod 13.1), neoznačené otváranie ne-HTML súborov (bod 13.11) – tieto sú nepovinné
- „Záchranné pravidlo" (bod 11.4) – ak niečo neviete urobiť prístupné, poskytnite alternatívu

Štandardy (prístupnosti a) funkčnosti webových stránok

- Predbežné monitorovanie nasledovných štandardov prebehlo v januári až marci 2009, po prejdení prechodného obdobia 1. októbra 2010 bude „ostré" monitorovanie
- § 15 – Štandardy pre obsah webového sídla
  - Najkomplikovanejšia požiadavka – angličtina, postačuje však informácia komu web patrí, aký je jeho účel, aké sú kompetencie resp. služby danej osoby a najmä kontakty
  - Najčastejšie „porušenia" – existencia vyhlásenia o prístupnosti (je možné využiť hodnotenie MF SR) a úradných hodín v angličtine
- § 16 – Štandardy pre komponenty a funkcionality webových sídiel
  - Štátna správa (89) 69,1%, samospráva (13) 66,67%
  - RSS iba 57 zo 110 subjektov, vyhľadávanie 93

Štandardy pre použitie súborov

- Prvé monitorovanie v júli-septembri 2008, najbližšie od júna 2009
- § 17 - § 23 – použitie súborov (textové, grafické, audio a video, audio a video streaming, tabuľky, kompresia)
- § 17 – „všeobecná výnimka"
  - a) ak sa (vopred!) dohodneš, môžeš používať čo chceš
  - b) nezaradené typy súborov (napr. mapy) sú neobmedzené
- § 17 – väčšinou odsek c) – „špecifická výnimka"
  - Na webe / pri komunikácií musíš použiť aspoň jeden povinný, zároveň však môže byť použitý aj relevantný iný (napr. PDF + DOC)
- Všeobecne: Byť schopný prijať všetky povinné typy súborov (najmä odseky a)) a odoslať jeden, ktorý si vyberiem (najmä odseky b))
- Nie je povinnosť vedieť súbory spracovávať.
- Text v PDF ako text a nie skenovaný obrázok!
- Tolerancia do 10 súborov daného typu (web)

Štandardy názvoslovia elektronických služieb @

- Prvé monitorovanie v júli-septembri 2008, najbližšie od júna 2009
- § 24 – personálne e-maily
  - Povinný tvar „meno.priezvisko@", pokiaľ je nutné definovať ďalší parameter pre spoločný e-mailový server rôznych úradov, je výnimočne možné použiť aj tvar „meno.priezvisko.parameter@"
- § 25 – generické e-maily
  - Musia existovať „info@", „webmaster@", „podatelna@" (ak existuje), „nazovfunkciepredstaveneho@"
  - „skratkautvaru@" je skôr odporúčaná
  - Tvar za znakom @ nie je predpísaný!
- § 26 – domény – týka sa iba uzlov GOVNET

Bezpečnostné štandardy

Krásny, ale ťažko chrániteľný

Bezpečnostné štandardy

Funkčný, ale ťažko dosiahnuteľný

Bezpečnostné štandardy

- § 29 – manažment rizík pre oblasť informačnej bezpečnosti
  - Spolu s definíciou aktív základ nastavovania politiky a opatrení
  - Dodržiavanie veľmi nedostatočne
- § 30 – kontrolný mechanizmus
  - Nie sú vyžadované nutne audity certifikovanou osobou
  - Všeobecný princíp kontroly – každé „teoretické" opatrenie, cieľ či úloha by mali byť kontrolovateľné, t.j. mať známe ukazovatele kontroly
- § 31 + § 34 – Ochrana proti škodlivému kódu + Aktualizácia softvéru
  - Aktualizovaný bezp. softvér, legálny softvér a obsah, šifrovanie

Bezpečnostné štandardy

- § 32 – sieťová bezpečnosť
  - Firewally, chránené uzly siete
- § 33 – fyzická bezpečnosť a bezpečnosť prostredia
  - Audity certifikovanou osobou nie sú vyžadované
  - Všeobecný princíp kontroly – každé „teoretické" opatrenie, cieľ či úloha by mali byť kontrolovateľné, t.j. mať známe ukazovatele kontroly
- § 35 – Monitorovanie a manažment bezpečnostných incidentov
  - Povinná osoba zodpovedá za bezpečnosť IS VS (zákon)
  - Monitorovanie, evidencia a riešenie bezpečnostných incidentov – najviac absentuje práve evidencia

Bezpečnostné štandardy

- § 36 – Periodické hodnotenie zraniteľnosti
  - Hodnotenie slabých miest systému
- § 37 – Zálohovanie
  - Archívna kópia (2x, podľa § 38 nie na tom istom mieste), prevádzková (1x) – rozsah daný bezp. politikou
  - Testy obnovy médií a IS VS
- § 38 – Fyzické ukladanie záloh
  - Uzamykateľný priestor

Bezpečnostné štandardy

- § 39 – Riadenie prístupu
  - Meno, heslo, ďalšie ochranné prvky (najmä pre mobilné pripojenie)
  - Logovanie prístupov (odporúča sa aj činnosti), logovanie zmien oprávnení
  - Pravidlá pre mobilné pripojenie (úplné zakázanie je nevhodné, lepšie je nastavenie pravidiel)
  - Systémový admin nemá vidieť údaje v databáze (šifrovanie, iná rola typu správca obsahu t.j. vecný pracovník)
- § 40 – Aktualizácia IKT
  - Schvaľovanie pre zmeny a nové systémy (už zahŕňa bezpečnosť)
  - Dostatočné testovanie
  - Dokumentácia (používateľská, administrátorská, prevádzková) – dodáva dodávateľ

Bezpečnostné štandardy

- § 41 – Účasť tretej strany
  - Analýza rizík zahŕňa aj tretie strany (najmä dodávateľov)
  - Bezpečnostné požiadavky do zmlúv s dodávateľmi (autorské práva, nevyžiadané funkcie, dodržanie bezp. politiky, odpočet dodržania bezp. štandardov)
  - Pri nedodržaní bezpečnostných požiadaviek možnosť sankcií, neprebrania diela, vypovedania zmluvy
  - Prístup k „živým" údajom podobne ako systémový admin (za konkrétne určených okolností)

Dátové štandardy

- § 42 + príloha 2 – Dátové štandardy
  - Výmena dát musí dodržiavať definovanú štruktúru, v prípade neexistencie požadovaných dát je možné rozšíriť
  - Pri prenose XML (podľa § 13)

Záver

Čo dodať záverom?

Pomaly, ale isto...

Ďakujem za pozornosť

Ing. Peter Bíro

Odbor legislatívy, metodiky, štandardov a bezpečnosti informačných systémov

Sekcia informatizácie spoločnosti

Ministerstvo financií SR

peter.biro@mfsr.sk / standard@mfsr.sk

+421/2/595 82 426