



Úplné elektronické podání...

jedině přes síť



První polovina roku 2016 je skutečně, alespoň pokud jde o témata elektronizace veřejné správy, nabitá. Úplné elektronické podání, elektronická identita, registr smluv ... pojem vedle pojmu. Snažili jsme se je pojmut. Ne vždy se zadařilo, protože ještě není vše vyjasněno.

I tak jsme ale získali dostatek informací, abychom Vás informovali o tom, co je a co bude.

Dle všeho se zdá, že jsme již jen krůček od skutečné elektronické veřejné správy, tedy od stavu, kdy budou obíhat data, nikoli lidé. To si sice neříkáme poprvé, ale teď už to tak snad bude. Určitě k tomu stačí málo.

Posuďte sami, předkládáme Vám výstupy ze seminářů, které jsme na tato témata připravili a mnoho doplňujících informací.

Ing. Michal Jirkovský
šéfredaktor



e-government 20:10

aneb žijem si jak na zámku,
ať to trvá věčně

MIKULOV • 6. - 7. 9. 2016

ODBORNÝ PARTNER



PLATINOVÝ PARTNER



GENERÁLNÍ PARTNER



ZLATÝ PARTNER



... vše podstatné o eGovernmentu najdete v Mikulově.

Více naleznete na www.egovernment.cz/mikulov

Redakce	ÚVODNÍ SLOVO	2
	OBSAH, TIRÁŽ	4
Úplně elektronické podání	READY? PLAY!!!	6
	INFORMACE MV ČR	8-11
	INFORMACE SZR	12-13
	INFORMACE MMR	14-16
	ÚPLNĚ ELEKTRONICKÉ PODÁNÍ POMÁHÁ OBČANŮM I ÚŘEDNÍKŮM	18-19
	KYBERNETICKÁ BEZPEČNOST VERSUS ÚPLNĚ ELEKTRONICKÉ PODÁNÍ	20-22
eIDAS	PROČ SE ZAJÍMÁM O eIDAS?	24
	ELEKTRONICKÁ IDENTITA	26-28
	POSKYTOVÁNÍ DŮVĚRYHODNÝCH SLUŽEB PODLE eIDAS	30-31
	eIDAS NENÍ STRAŠÁK, UŽIVATELÉ SYSTÉMU GINIS SE HO OBÁVAT NEMUSÍ.....	32-34
Státní správa	ISOSS	36-37
	ISOSS JE PLNĚ FUNKČNÍ, ALE MŮŽEME JEJ ROZVÍJET	38-39
	CO PŘINESE DALŠÍ ROČNÍK KONFERENCE ISSS?	40-41
	AGENDOVÝ SYSTÉM - NEZBYTNOST	42-43

V rámci České a Slovenské republiky vydává:

info♦com s.r.o., Na Zatlance 10, 150 00 Praha 5
 www.infocom.cz
 IČO: 26426331
 zapsána u Městského soudu v Praze
 pod č. C - 81357
tel.: 241 412 518
e-mail: egovernment@egovernment.cz
http: www.egovernment.cz
 ISSN 1801-9420

Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Mgr. Kristýna Petrů

Grafika: PROPAGANDA, Malá Štupartská 7, Praha 1
Tiskárna: A. R. GARAMOND s.r.o., Belnická 758,
 252 42 Jesenice
Registrační číslo: MK ČR E 11364

Reprodukce celku ani jeho částí v jakémkoliv provedení
 není povolena bez výslovného souhlasu Egovernment
 - info♦com.

Registrace:

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**. Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **100 Kč (4 EUR)** bez DPH/**výtisk, tj. 400 Kč (16 EUR)** bez DPH **ročně**.

S registrací získáte, kromě pravidelného zaslání magazínu, i informace o dalších projektech, které realizuje společnost **info♦com s.r.o.**



I letos si Vás dovolujeme pozvat na konferenci **e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně**. Konference, kterou pořádá magazín Egovernment, proběhne tradičně na zámku Mikulov a to v termínu **6. - 7. 9. 2016**.



Součástí večera bude volba **Miss Egovernment**

- přihlašování soutěžících je již možné

Opět pro Vás bude připraven bohatý dvoudenní program stejně jako společenský večer.

(více na www.egovernment.cz/miss)

Vstupné na konferenci se mění v čase:

VEŘEJNÁ SPRÁVA (uvedené ceny jsou bez DPH):

registrace do 25. 5. 2016	600 Kč
registrace do 25. 6. 2016	700 Kč
registrace do 25. 7. 2016	1 000 Kč
registrace do 25. 8. 2016	1 200 Kč
registrace do 7. 9. 2016	1 500 Kč

KOMERČNÍ SFÉRA (uvedené ceny jsou bez DPH):

registrace do 25. 5. 2016	2 700 Kč
registrace do 25. 6. 2016	3 600 Kč
registrace do 25. 7. 2016	4 500 Kč
registrace do 25. 8. 2016	5 500 Kč
registrace do 7. 9. 2016	8 000 Kč



... vše podstatné o eGovernmentu najdete v Mikulově.

Přihlašování na konferenci je možné na www.egovernment.cz/mikulov

**Ready?
Play!!!**



Magazín Egovernment otevřel již tradičně v únoru v Jihlavě novou konferenční sezónu. Pro rok 2016 si jako zahajovací téma zvolil ÚPLNÉ ELEKTRONICKÉ PODÁNÍ.

Úplné elektronické podání – jako jeden ze základních strategických pilířů elektronizace veřejné správy – nabývá stále většího významu. Cíl, kdy občané budou při svém podání vůči veřejné správě doplňovat minimum dat, a to pouze ta, která veřejná správa nemá ve svých informačních systémech, by měl naplnit ono, dnes již okřídlené heslo Obíhají data, nikoli občané. Heslo, které sice symbolizuje podstatu elektronizace veřejné správy, nicméně stále není v ČR naplněno.

V Jihlavě jsme tedy chtěli zjistit, jak to vypadá s realizací úplného elektronického podání, jak se přibližujeme představě samoobslužného místa, konceptu sdílených služeb a elektronické identity občanů i úředníků, případně, jaká je možnost financování projektů směřujících k realizaci úplného elektronického podání.

Diskuze byla živá až bouřlivá. Jaké výstupy z ní vzešly, naleznete na následujících stránkách.

Cloud servery na SSD s výjimečnými parametry

Výkonné cloud servery do 55 sekund. To je ZonerCloud.cz!

Vyzkoušejte výkonné cloud servery na nejlepších technologiích světa.

ZonerCloud.cz nabízí opravdu výkonné cloud servery na špičkovém technologickém zázemí. **Včetně redundance, zálohování a nejlepších virtualizačních platforem světa - VMware a Hyper-V!** Jaké parametry a varianty serverů nabízí a za jaké ceny?

Výhody cloud serverů od Zoneru:

- ✓ Zřízení do 55 sekund
- ✓ Bez závazků
- ✓ Garance vrácení platby 14/365
- ✓ 99,99 % dostupnost
- ✓ 24/7 zákaznická podpora
- ✓ 100% na SSD storage



CLOUD SERVER LINUX

Počet přiřazených CPU:	2 core
Operační paměť RAM:	2 GB
Diskový SSD prostor:	30 GB
Přenos dat:	Neomezeně
Redundance:	Ano
Virtualizační platforma:	VMware
Operační systém:	Debian, Ubuntu, Centos, Fedora
Záloha 7/14	Ano



Výkonné cloud servery na systému Linux za výhodnou cenu.
od 290 Kč

CLOUD SERVER EKONOM

Počet přiřazených CPU:	3 core
Operační paměť RAM:	3 GB
Diskový SSD prostor:	30 GB
Přenos dat:	Neomezeně
Redundance:	Ano
RDP přístupy zdarma:	2
Účetní systém:	Money, Pohoda



Přesuňte účetnictví z fyzického serveru do bezpečí cloudu.
od 790 Kč

CLOUD SERVER WINDOWS

Počet přiřazených CPU:	2 core
Operační paměť RAM:	2 GB
Diskový SSD prostor:	30 GB
Přenos dat:	Neomezeně
Redundance:	Ano
Virtualizační platforma:	Hyper-V
Operační systém:	Windows Server 2012 R2
Záloha 7/14	Ano



Cloud Servery včetně licence Windows Server 2012 R2.
od 490 Kč

DISASTER RECOVERY

Chcete-li dosáhnout maximální úrovně dostupnosti služeb a eliminovat i riziko vyšší moci (živelné pohromy a katastrofy), Disaster Recovery společnosti VMware zajistí provoz cloudových služeb i v době náhlých a nečekaných událostí při kompletním výpadku primárního data centra.



Se službou disaster recovery budou vaše data v bezpečí.
cena individuálně

Vyzkoušejte špičkové cloud servery do 55 sekund
www.ZonerCloud.cz



Informace MV ČR

V rámci prezentace MV ČR měl hlavní slovo Ing. Roman Vrba, ředitel odboru e-governmentu. Spolu s ním se k pozdějším dotazům vyjadřovali Martin Kraus a Pavel Tesař. Martin Kraus je legislativec, který analyzuje registr smluv a podílel se na tvorbě zákona o službách vytvářejících důvěru. Pavel Tesař byl přítomen proto, že se podílel na technické části registru smluv.

Téma vystoupení mělo být zaměřeno především na úplné elektronické podání, což je podle Romana Vrby možné považovat za jakýsi svatý grál e-governmentu. Bavíme se o něm tak čtyři pět let, snažíme se jej všichni dosáhnout a objevit a pořád se nám to nedaří. Jeho koncepci shrnul tak, že byla postavena na CMS 2.0, Egon Service Bus, identitě a navíc registru smluv. Protože poslední jmenované je aktuální, předpokládal Roman Vrba, že bude posluchače zajímat nejvíc. Zdůraznil, že Ministerstvo vnitra je ve stejné situaci jako ostatní úřady, protože bude muset rovněž zveřejňovat smlouvy. Je to pro něj stejný problém jako pro ostatní, a navíc je ve schizofrenní roli, neboť je ze zákona zároveň správcem tohoto budoucího registru.

Uvedená témata spolu velice úzce souvisejí, když bez činnosti/provozu Egon Service Bus, CMS 2.0, e-Identity atp. nebude fungovat něco, co bychom mohli nazvat úplným elektronickým podáním. Protože diskutovaná problematika je skutečně aktuální a zásadní, rozhodli se pánové své vystoupení pojmout nikoli jako prezentaci, ale spíše diskusi. Jejím cílem bylo nejen informovat přítomné o současném stavu, ale zároveň získat co nejvíce dat o praktických potřebách úřadů tak, aby na nich mohlo MV ČR stavět svůj další postup. Níže tedy najdete text, který je stručným shrnutím toho, co v Jihlavě v úvodu semináře zaznělo.

Základní potřebou pro funkční elektronické podání je identifikovat konkrétní osobu. Doposud zde bylo pouze jediné, státem garantované, ověření identity, a to prostřednictvím datové schránky. Je tedy vhodné, aby začala fungovat i jiná cesta.

Alarmující je skutečnost, že zatímco v porovnání s evropskými státy jsme na předních místech ve využívání elektronických komerčních služeb, například elektronického bankovníctví či e-shopů, ve využívání elektronických služeb státu zaujímáme místo mezi posledními. Situace vyplývá z nabídky těchto služeb. Za základní okruh služeb státu můžeme považovat například daňové přiznání, nabídku úřadu práce, sociální benefity, osobní doklady, registraci vozidel, stavební povolení, doložení skutečností policií, veřejné knihovny, oddací nebo úmrtní listy, hlášení změn trvalého pobytu, zdravotní služby atp. V rámci těchto služeb však v ČR skutečně elektronicky funguje pouze daňové přiznání. Ostatní služby buď nejsou elektronické vůbec, či jen z části. Proto se MV ČR nyní zaměřuje na rozšíření nabídky elektronických služeb.

eIDAS

Jedná se o nařízení EU, které bude účinné od 1. 7. 2016, ovšem jen v některých částech – těch, které se týkají elektronických podpisů a elektronických značek. V části,



kteřá se týká elektronické identity, by měl být plně účinný od roku 2018. V Parlamentu ČR je nyní ve druhém čtení zákon o službách vytvářejících důvěru, který doplňuje zmiňované nařízení EU v našich podmínkách. Jako orgán dohledu je tímto zákonem určeno MV ČR.

Pro ČR, na rozdíl od některých jiných členských států, není novinkou elektronický podpis, který nařízení EU přináší, ale právě elektronická identita. Měla by být aplikovatelná od roku 2018, ale v ČR dojde k realizaci pravděpodobně daleko dříve, přičemž nositelem elektronické identity by měl být čip občanského průkazu.

DOTAZ: Jak konkrétně bude situace od 1. 7. 2016 vypadat, kdo bude „eidasový“ certifikát vydávat, kolik bude stát, bude s touto identitou kompatibilní Moje ID?

Od 1. 7. 2016 bude účinná regulace upravená nařízením EU a naším vlastním doplňujícím zákonem s tím, že od tohoto data bude možné vydávání elektronických podpisů kvalifikovat jako službu vytvářející důvěru podle nařízení eIDAS. Kvalifikaci či certifikaci bude provádět dohledový orgán – MV ČR – a takto certifikované úřady budou moci vydávat kvalifikované podpisové certifikáty. Zároveň budou ještě určitou dobu platit i certifikáty vydané podle dosavadní právní úpravy. Pokud jde o vydávání, pak MV ČR bude pouze orgánem dohledu. Přechné období, pravděpodobně 2 roky, bude umožňovat vznik nějaké nové národní certifikační autority, ale bezpochyby budou zachovány ty, které už zde fungují.

OPRAVDU SE NIC NEMĚNÍ, JEN SE VĚCI PŘEJMENOVÁVAJÍ – NOVĚ JE ZDE ZAVEDEN POUZE ELEKTRONICKÝ OBČANSKÝ PRŮKAZ S ČIPEM.

DOTAZ: Náš úřad by měl spravovat identitu vydanou v zahraničí, například v Estonsku. Jak to bude fungovat a jak bude fungovat federace identit, kdy elektronickou identitu vystaví třeba banka či jiný oprávněný poskytovatel?

To je dotaz směřující na budoucnost, zhruba na rok 2018. Můžeme však předpokládat, že filozofie bude nastavena podobně jako dnes u elektronických podpisů, tedy že bude nějaká databáze obsahující poskytovatele identit. Bude tak umožněno uznávání identit mezinárodně. Poskytovatelé identit budou procházet schvalovacím „kolečkem“, na jehož konci se stanou uznávanou autoritou poskytující elektronickou identitu pro použití napříč Evropou.

CMS 2.0, eGON Bus

Tyto projekty byly dokončeny, jsou akceptovány a běží. Oboje zaštiťuje odbor e-governmentu (p. Valenta lubomir.valenta@mvcv.cz). Zde budou sdružovány veškeré požadavky na využívání těchto služeb.

REGISTR SMLUV

Zákon schválený v prosinci loňského roku ukládá MV ČR vybudovat tento registr tak, aby byl funkční do 1. 7. 2016. Podstatné je, že smlouvy, které zde nebudou zveřejněny do 1. 7. 2017, nebudou platné. Veškeré vstupy do registru smluv budou realizovány prostřednictvím datové schránky. Pro ty, kteří používají svoje informační systémy, bude muset MV ČR nabídnout (patrně v březnu) rozhraní, aby se na budoucí informační systém mohli napojit. Zároveň bude existovat tzv. minimalistická varianta vstupu prostřednictvím formuláře Czech POINTu. Určitě bude včas připraven metodický návrh JAK ZVEŘEJŇOVAT.



DOTAZ: Jak bude vypadat aplikace registru smluv z pohledu občana, jak v ní bude možné vyhledávat? Nahradí publikaci smluv pro občany na vlastním webu úřadu?

Webová část aplikace musí být přístupná pro veřejnost bez registrace, tedy pro anonymní návštěvníky. Vyhledávání by zde mělo být podobné jako na Portálu veřejné správy, mělo by být:

- parametrické (vyhledání podle IČO, názvu subjektu, ID datové schránky, data zveřejnění, předmětu smlouvy);
- fulltextové (vyhledávání volného textu, a to i v textovém obrazu smluv, které zde budou).

DOTAZ: Podle zákona má být smlouva zveřejněna v otevřeném a strojově čitelném formátu, jaký formát se tedy předpokládá?

Nebude stanoven jeden konkrétní formát, ale bude kontrolováno, zda příloha smlouvy má nějakou textovou vrstvu (tzn., že například PDF s textovou vrstvou je možné). Jedná se však o smlouvy nové, nikoli o zveřejňování historie. I proto je zde přechodné období jednoho roku, aby instituce mohly přizpůsobit workflow schvalování a zpracování smluv tomuto požadavku, včetně jejich dodavatelů. MV ČR je ovšem v tomto případě „pouze“ správcem tohoto informačního systému. Kontrolu obsahu a jeho správnosti musí provádět ten, kdo smlouvu zveřejňuje, na něm leží zodpovědnost za zveřejněné smlouvy.



DOTAZ: Smlouvy a objednávky nad 50 tisíc Kč zveřejňujeme v rámci našeho úřadu běžně, s tím problém nemáme, ale problémem může být posílání přes datovou schránku od 1. 7. 2016. Pokud není vyjasněno rozhraní a neznáme dodavatele, tak to může být zásadní problém.

Představa o fungování je následující.

Určitý registr smluv již dva roky funguje na Portálu veřejné správy. Nový způsob, o kterém tu hovoříme, bude velice podobný. Zveřejňování proběhne prostřednictvím datové zprávy, která bude mít přesně definovaný formát (popsán v provozním řádu datových schránek). Přílohou této datové zprávy budou xml data, která budou obsahovat:

- identifikaci pokynu, jaký registru dáváte (může jich být více);
- data k tomuto pokynu.

Nejčastějším pokynem bude zveřejnění konkrétní smlouvy, bude tedy nutné vložit xml strukturu metadat a přílohu (jednu nebo více smluv). Nyní není možné říci, jak přesně bude vypadat xml struktura, jak bude vypadat pokyn a jeho metadata, ale struktura by měla být k dispozici v průběhu března.

Podstatným rozdílem oproti stávajícímu stavu je přidání možnosti zveřejňování v zastoupení (požadavek krajů). Do metadat se tedy přidá ještě struktura, která říká, kdo zveřejňuje za koho (bude zařazen jednoduchý registrační proces). Další rozdíly již nebudou tak zásadní. Jedná se například o volitelnou položku hodnoty smlouvy v cizí měně (hodnota v korunách je povinná, ale bude možné zveřejnit i hodnotu v cizí měně). Dále bude zařazena položka identifikující plátce a příjemce a možnost zadání více smluvních stran.



Pokud jde o samotné pokyny, bude možný pokyn ke zveřejnění smlouvy a pokyn k modifikaci dat. V této souvislosti je důležité, že zveřejněná data není možné smazat, pouze modifikovat, původní verze je tedy dohledatelná. K dispozici bude rovněž servisní pokyn ke zmocnění k publikaci, případně zrušení tohoto zmocnění.

Podstatná je rovněž odpověď systému. Podle zákona má být odesláno potvrzení o zveřejnění. To bude obsahovat metadata, která byla odeslána, otisk přílohy, jednoznačný identifikátor záznamu a URL adresu záznamu pro případ evidence.

V další části vystoupení se rozvinula diskuze o rozdílu v přístupu ke smlouvám a objednávkám nad 50 000 Kč a dále pak o problematice dotačních smluv. Z diskuze vyplynulo, že MV ČR zatím nemá v tomto směru k dispozici žádný výklad zákona. MV ČR je sice zodpovědné za vybudování a správu informačního systému registru smluv, nikoli za jeho výklad. Protože zákon vznikl v Poslanecké sněmovně PČR, která zřejmě nebude realizovat jeho výklad, dá se usuzovat, že nakonec tato role stejně padne na MV ČR. I proto byla zvolena pro vystoupení forma diskuze, aby pracovníci ministerstva mohli posbírat potřebné připomínky a podněty, které jim usnadní přípravu tohoto výkladu.

ZÁVĚR

Závěrečná diskuze pak definovala některé připomínky a podněty ze strany posluchačů.

Především se jednalo o informaci, že pro některé úřady bude znamenat naplnění požadavků zákona další náklady, zejména v oblasti personální.

Praktická komunikace prostřednictvím datových schránek v případě rozsáhlých (například stavebních) dokumentací je téměř nemožná.

Je žádoucí, aby obce dostaly metodiku ke zveřejňování smluv.

Je nutné vyjasnit problematiku anonymizace smluv i to, zda bude software pro tuto činnost řešen centrálně, či každým úřadem samostatně.

I u problematiky jednotného číselníku smluv je nutno nastavit nějakou metodiku.

Zástupci MV ČR přivítali tyto podněty. Jak bylo řečeno, nyní je čeká setkání s tajemníky úřadů a dalšími osobami, od nichž mohou získat potřebné podněty. Jejich shrnutí a hlavně konkrétní zásadnější výstup bychom mohli očekávat na přelomu května a června. Slíbili jsme si, že se k tomuto tématu vrátíme ve dnech **1. – 3. 6. 2016 v rámci konference ROK INFORMATIKY**, která se bude konat v Náchodě.



INFORMACE SZR

Michal Pešek svým vystoupením navázal na MV ČR. Připomenul, že dochází ke změnám v legislativě a pro všechny, tedy nejen posluchače, zástupce úřadů, ale i pro samotné vnitro je to složité a náročné období. Jeho vystoupení mělo být prakticky zaměřeno na změny zákonů o základních registrech a o občanských průkazech, přičemž uvedl, že SZR ve spolupráci s ČP OZ realizují požadavky nařízení EU.

Všechny možnosti, které z uvedených změn a nařízení vyplývají, pokrývá, proto k jeho jednotlivým položkám – funkcionalitám – uvedl Michal Pešek aktuální informace.

ELEKTRONICKÁ IDENTIFIKACE

Od 1. 7. 2016, pokud bude schválen příslušný zákon, bude v ČR vydáván pouze čipový občanský průkaz, proto je nutné zvážit, co bude na tomto čipu vše uloženo. Nyní se pracuje na službách elektronické identifikace (společný tým SZR, MV ČR, ČP OZ). Součástí řídicího výboru je hlavní architekt e-governmentu a je tak zajištěn soulad se schválenými strategiemi státu v této oblasti.

INDIVIDUÁLNÍ VÝDEJ DAT

Je nutné, aby SZR uměla vydávat data z pohledu subjektu práva a tak podpořila projekt úplného elektronického podání.

HROMADNÝ VÝDEJ DAT

V souvislosti s hromadným výdejem dat budou vyzváni zástupci krajů, aby v průběhu dubna začali se SZR spolupracovat v technickém týmu tak, aby tento tým definoval především potřeby a nároky krajů.

ČÍSELNÍKY

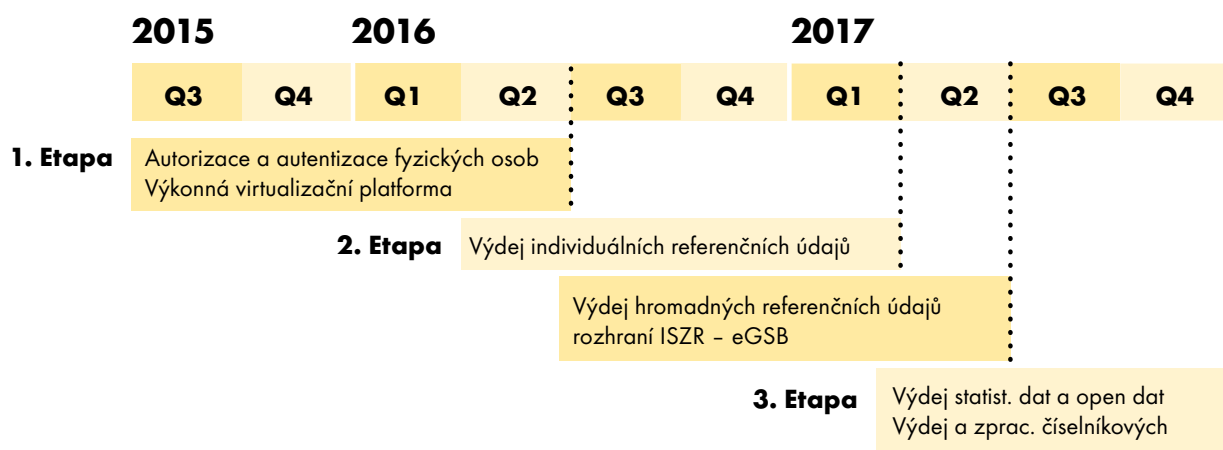
SZR bude spolupracovat s ČSÚ na dalším sčítání domů, lidu a bytů, a i proto je vhodné, aby byla schopna zpracovat Open Data a realizovat potřebné výpočty.

V současné době ZR vykazují 860 milionů transakcí, je k nim připojeno cca 3 000 OVM a 3 000 agendových informačních systémů. Cílem je počet připojených informačních systémů zmenšit (na straně území). Smyslem tohoto kroku je, aby byla garantována centrálně spravovaná data, která budou rychle přístupná všem. Taková možnost snižuje náklady a zvyšuje efektivitu.

V evidenci obyvatel je možné očekávat nový pojem – fiktivní adresa. Změna se týká registru obyvatel a jedná se reakci na neexistenci některých dat.

Nyní je schválena analýza, konstrukce procesů a je budován Front End pro národní identitní autoritu. Zbývá vyjasnit, jak přesně budou fungovat národní autority. Jedná se o dvě – autoritu identitní, která bude vázána s občanským průkazem, a klasickou certifikační autoritu. Musí být nastaveno jejich vytvoření, provozování a dohled. Samozřejmě občanské průkazy musí projít ještě legislativou a musí být nastaven jasný model. Cílem není, aby se certifikáty do čipu nahrávaly na výdejní přepážce. Možností je více, nyní je tato záležitost diskutována i se Státní tiskárnou cenin.

HARMONOGRAM



První etapa je autorizace a autentizace. V polovině letošního roku bude definováno, jak vypadá národní certifikační autorita. Buď se rozhodneme pro vybudování zcela nové, nebo vyjdeme z něčeho, co zde již funguje. V zákoně bude zároveň definováno, jak budou uznávány stávající autority, které se patrně budou muset technicky přizpůsobit. Rozhodně se ale jedná o plynulý přechod, žádné skokové řešení. Konkrétně 1. 7. 2016 se změní pouze to, že bude ukončena platnost starého zákona o elektronických podpisech a bude v platnosti zákon nový – o elektronické identitě a uznávání dat.

Druhá etapa je zaměřena na výdaje individuálních dat a výdaje hromadných referenčních údajů a nastartování eGON Service Bus. Zatím není domluveno, zda správcem a tím, kdo by měl řídit přístupy, bude MV ČR, nebo SZR.

Třetí etapa je vývoj statistických dat a Open Dat.

Určitý skluz do situace, kdy se zabýváme otázkami identity, vnesla i realizace zákona o státní službě. Pro řadu je věcí je nápomocen, v jistém smyslu se zároveň jedná o určitou komplikaci – přezkušování a náborů úředníků značně komplikují realizaci složitějších projektů. Důležitý je rovněž dopad zákona o kybernetické bezpečnosti. Vynucuje si certifikace a technické změny i změny v procesech, což jsou náročné kroky, které je však nutné prováďet důsledně. Zároveň, alespoň u SZR, dochází ke změně přístupu. Původní záměr při budování základních registrů byl, že data budou veřejná, nicméně provoz ukázal, že jsou části ZR, které používají například bezpečnostní složky státu, tedy části neveřejné. Pro SZR to znamená přechod z režimu vyhrazené na režim důvěrné.



Informace MMR

Vrchní ministerský rada MMR PhDr. Aleš Pekárek se ve svém vystoupení věnoval výzvě č. 4 IROP. Přiblížil historii a pozadí vzniku této výzvy, a to především z pozice toho, kdo je odpovědný za financování e-governmentu (IROP, prioritní osa 3, specifický cíl 3.2., celkově alokováno necelých 10 mld. korun na různé projekty elektronizace a kybernetické bezpečnosti veřejné správy).

Výzva č. 4 byla první výzvou ze specifického cíle 3.2, která byla vyhlášena již na podzim loňského roku. Stalo se tak na popud MV ČR, které tehdy považovalo úplné elektronické podání za naprostou prioritu. Výzva je vyhlášena a nyní záleží na MV ČR, kdy začne předkládat projekty. V této souvislosti musí útvar hlavního architekta především rozhodnout, jak bude jednotlivé projekty schvalovat. To, že je výzva již vyhlášena a nejsou zatím předloženy žádné projekty, neznamena zatím žádný problém, neboť výzva je otevřena až do června 2017.

IROP

Samotný IROP je druhým největším českým operačním programem s 85% kofinancováním regionálních projektů (pro celorepublikové projekty je kofinancování jiné). Dělí se na čtyři prioritní osy:

- **prioritní osa 1** se týká záchranných systémů, dopravy a telematiky;
- **prioritní osa 2** je zaměřena na sociální bydlení, sociální infrastrukturu a podnikání, podporu ZŠ, MŠ a SŠ;
- **prioritní osa 3** se týká e-governmentu a kultury;
- **prioritní osa 4** je zaměřena na komunitně vedený místní rozvoj.

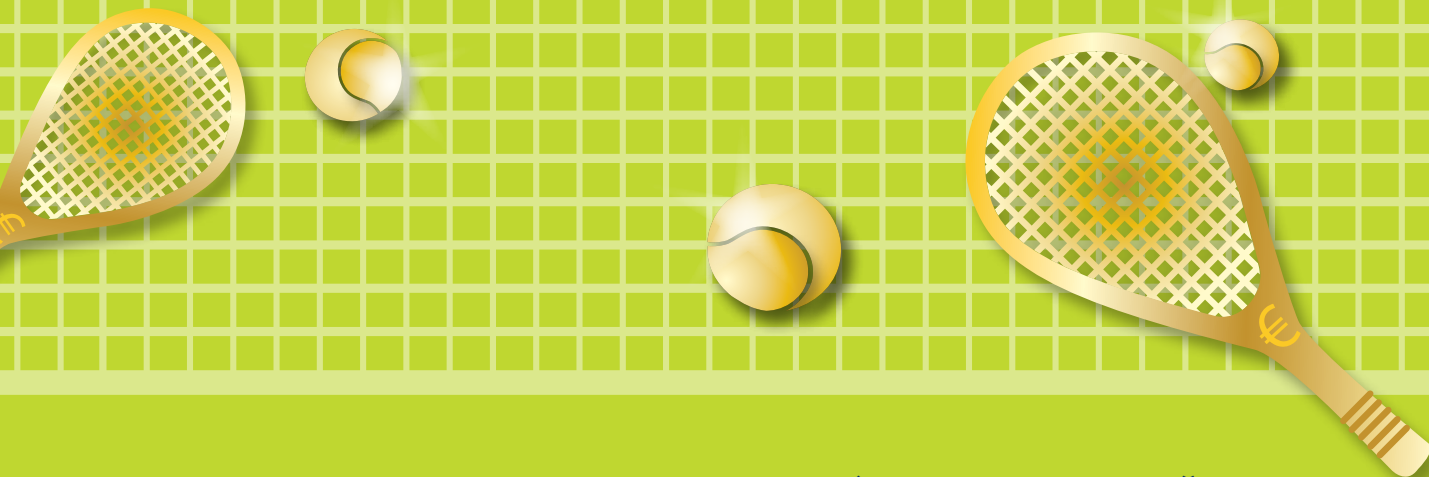
V rámci specifického cíle 3.2 byla tedy vyhlášena výzva na **úplné elektronické podání** a nyní jsou očeká-

vány projekty. Stejně tak byla již vyhlášena výzva č. 10 na **kyberbezpečnost**, zaměřená na významné informační systémy a kritické informační systémy, a rovněž výzva č. 17 **eLegislativa, eSbírka, Národní digitální archiv**. Zbylé výzvy (specifické informační systémy; eGovernment) by měly být vyhlášeny v průběhu března a dubna.

FINANCOVÁNÍ

Věcným garantem je MV ČR. MMR funguje v pozici „peněženky“, která vypisuje výzvy na témata a okruhy podle doporučení MV ČR a Rady vlády pro informační společnost. MMR tedy hlídá pravidla čerpání a MV ČR zodpovídá za rozvoj e-governmentu, tedy za zaměření projektů. Ke specifickému cíli 3.2 byl vytvořen pracovní tým MMR, MV ČR, Asociace krajů, v případě kyberbezpečnosti i NBÚ.

Podstatné je, že v rámci specifického cíle 3.2 musí všechny projekty být v souladu se Strategickým rámcem rozvoje VS a jeho projektovými okruhy. Žádný projekt, který by s tímto rámcem nebyl v souladu, nemůže být financován pomocí ESIF. Je tedy nutné, aby projekty měly souhlasné stanovisko odboru hlavního architekta e-governmentu. Netýká se to ale všech projektů. Obecní a krajské pro-



jekty do 15 mil. Kč, které se nevážou na centrální systémy státu, tuto povinnost nemají.

NÁVAZNOST NA IOP

Panuje obecné přesvědčení, že projekty, které byly již v minulosti financovány z IOP, není možné dále touto cestou podporovat. Je tedy nutné zdůraznit, že je možné platit další rozvoj takových projektů, ale za předpokladu, že se skutečně jedná o jejich **další rozvíjení**. Tedy například v případě, kdy je zřejmé, že projektu přibyly nové funkcionality, které jsou aktuálně potřeba a v předchozím „kole“ nebyly implementovány.

NEJČASTĚJŠÍ PROBLÉMY IOP

Byl realizován horizontální audit páteřních projektů z MV ČR, jehož výsledkem jsou doporučení, čeho se vyvarovat, aby se autoři projektů vyhnuli problémům s auditory. MMR v blízké době vydá k tomuto tématu podrobnější tiskovou zprávu se seznamem těchto doporučení.

PROJEKTOVÉ OKRUHY

Úplné elektronické podání mělo jednoznačnou prioritu, bylo tedy již vyhlášeno, podobně jako okruh eLegislativa, eSbírka a NDA. Další „elektronizace“ odvětví bude vyhlášena v březnu (eCulture, eHealth, eEducation, eJustice...) a žádosti zde budou moci podávat jak centrální instituce, tak kraje či obce. eEducation a eCulture jsou priority stanovené Radou vlády pro informační společnost, eHealth by mělo být výrazně lákavé pro kraje.

Stanovena nebyla priorita zpřístupnění obsahu, transparentnost a Open Data. Bude vyhlášeno příští rok.

V rámci ostatních projektových okruhů (elektronická identita, eIDAS) bude SZR podávat navazující projekt MORIS. V dubnu pak bude vyhlášena výzva na specifické informační systémy státní správy.

4. VÝZVA IROP PODROBNĚ

Vyhlášení výzvy: **17. 9. 2015**

Příjem žádostí: **od 17. 9. 2015 do 30. 6. 2017, příjem může být při vyčerpání alokace ukončen dříve nebo může být alokace navýšena.**

Průběžná výzva – hodnocení projektů probíhá průběžně podle data podání žádosti.

Datum zahájení realizace projektu: **od 1. 1. 2014**

Datum ukončení realizace projektu: **do 30. 6. 2019**

Realizace projektu nesmí být ukončena před datem podání žádosti o podporu.

K dispozici jsou přesné popisy, co je úplné elektronické podání, eIDAS, datový fond...

Alokace činí **400 mil. Kč** a zahrnuje jak páteřní projekty MV ČR, tak zároveň možnosti pro obce i kraje. Lze předpokládat, že ty si budou chtít podat své vlastní projekty na elektronické podání v rámci agend, které mají ve své působnosti. I proto je minimální hranice nákladů stanovena na **3 000 000 Kč**.

Podporované aktivity v rámci této výzvy jsou rozděleny na hlavní a vedlejší.

Hlavní podporovanou aktivitou je pořízení upraveného, konfigurovaného, nebo nově vybudovaného informačního systému, který splňuje jeden, nebo více následujících parametrů:

- vytvoření podpůrných služeb pro úplné elektronické podání;
- vytvoření samoobslužného místa pro subjekt práva v české i anglické verzi, prostřednictvím kterého bude možné realizovat úplné elektronické podání;
- elektronizace formulářů veřejné správy a zajištění anglické verze;
- zajištění úplného elektronického podání;
- implementace identifikace a autentizace pomocí identifikačních prostředků ve smyslu nařízení eIDAS pro



využívání služeb e-governmentu prostřednictvím kontaktních míst;

- podpora sdílení identitních služeb na národní a regionální úrovni;
- vytvoření bezpečného mechanismu poskytování a využívání údajů jako součást referenčního rozhraní ISVS z jednotlivých agendových systémů v návaznosti na referenční údaje základních registrů s využitím funkcionality EGON Service Bus;
- vytvoření mechanismu pro odstraňování nekonzistencí nereferenčních údajů o subjektech práva v jednotlivých agendových systémech.

Pořízený informační systém musí zajišťovat **minimálně tři nové funkcionality**, pokud v upravovaném informačním systému v době podání žádosti o podporu neexistují.

Pokud funkcionality v upravovaném informačním systému existuje, **není možné ji započítat**. Jedná se o následující funkcionality:

- **samoobslužný proces veřejné správy** (není nutné chodit na úřad);
- **propojování datového fondu veřejné správy** (využití údajů centrálních registrů);
- **zajištění provozní spolehlivosti a bezpečnosti**;
- **dostupnost služeb veřejné správy** (dálkový přístup);
- **interoperabilita na území státu s přesahem v rámci EU** (identifikace, autentizace a autorizace v rámci EU dle eIDAS);
- **celoplošná dostupnost** (dostupnost na území ČR i EU v režimu 24/7).

Organizační složky státu (SZR, MV ČR atp.) mohou žádat dotace na projekty, které řeší problematiku výkonu státní správy, včetně přenesené působnosti. Kraje a obce mají vymezeno, že mohou žádat na projekty, které řeší problematiku podání v rámci samostatné působnosti.

Z pohledu územního vymezení je toto rozdělení jednoduché a logické. Státní instituce mohou žádat na projekty v rámci celé ČR, včetně Prahy. Projekty krajů se týkají kraje a projekty obcí území obce.

POVINNÉ PŘÍLOHY

Důležité je, že v rámci povinných příloh žádosti o podporu musí být předloženo **souhlasné stanovisko hlavního architekta e-governmentu**. Podrobnější informace ke stanovisku jsou k nalezení na stránkách MV ČR. Novou přílohou je **průzkum trhu**. Musí být zřejmé, jak žadatel k uvedené ceně dospěl, zda nad cenou přemýšlel a prostředky byly vynaloženy účelně. Forma tohoto prokázání je na uvážení žadatele (otisky webových stránek, komunikace s dodavateli, srovnávání cen atp.).

DALŠÍ VÝZVY

Výzva č. 23 byla vyhlášena 24. 2. 2016 - specifické informační a komunikační systémy a infrastruktura pro centrální instituce (týká se projektového okruhu 9, 6.1, 6.2 a 6.3 - veškeré informační systémy, které jsou potřeba pro chod úřadu).

V březnu by měla být vyhlášena výzva e-government I - pro všechny centrální instituce, kraje a obce (eHealth, eCulture, eEducation...).

V dubnu by měla být vyhlášena výzva pro specifické informační a komunikační systémy a infrastrukturu pro obce a kraje. Jedná se hlavně o příležitost modernizace agendových záležitostí v rámci obcí a krajů.

KONFERENCE PRO MUNICIPALITY A BANKY

O ČEM?

Seminář nabídne praktické pohledy na finanční služby nabízené samosprávám. Představeny budou také zkušenosti obcí, které modernizovaly v nedávné době své služby a efektivně a úsporně využívají nové bankovní služby. Co za možnosti nabízejí banky samosprávě? Jaké služby mohou obce využívat? Za jakých podmínek lze zavést placení kartou na městských a obecních úřadech? Jak si říct o lepší podmínky? Jaké jsou možnosti financování investic? Jakou úlohu sehraje problematika chytrých měst a jak mohou být využita?

KDY?

8. června 2016, 8:30–14:30

KDE?

Kongresové centrum
České národní banky

REZERVUJTE SI SVÉ MÍSTO NA

BANKYAOBCE.CZ



POŘADATELÉ

Bankovníctví.



POD ZÁŠTITOU PŘEDSEDY SMO

**ING. FRANTIŠKA
LUKLA**

PARTNEŘI



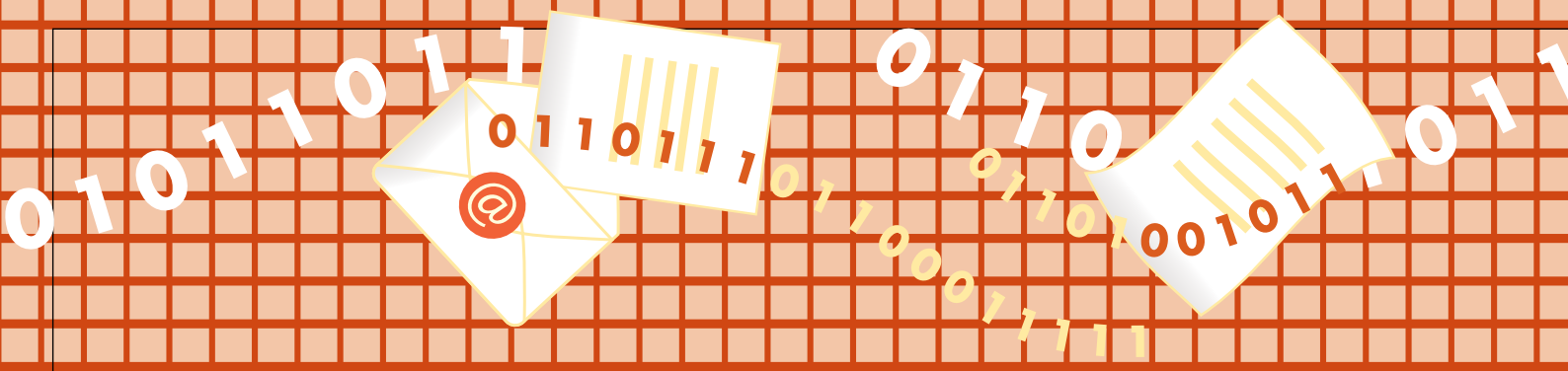
(ZA ODBORNÉ PODPORY)
B ČESKÁ BANKOVNÍ ASOCIACE

MEDIÁLNÍ
PARTNEŘI

**moderní
obec**

fininvestičníweb

Egovernment



Úplné elektronické podání pomáhá občanům i úředníkům

Není zcela jednoduché pojmut mnohokrát komunikované téma zcela jinak, neotřele. Rozhodnutí však bylo tentokrát jednoznačné – shrnout do jednoho článku to nejdůležitější z dané problematiky. Oblast elektronického podání je aktuálně v další fázi svého vývoje a v průběhu následujících měsíců snad konečně dojde k vytouženému průlomu. Pro pořádek je třeba říci, že řada uvedených informací je čerpána z oficiálních materiálů MV ČR nebo prezentací hlavního architekta e-governmentu.

ÚEP a možnosti dotace

Na úvod si připomeňme, co to vlastně úplné elektronické podání (ÚEP) je. ÚEP představuje stav, kdy při elektronickém podání dle většiny agend dokládá osoba pouze údaje, které jsou mimo informační systémy veřejné správy, a to pokud možno opět v elektronické podobě. Toto podání umožní sdílení získaných údajů i ostatními orgány veřejné moci nebo subjekty, které takto jednájí se souhlasem občana. K zajištění ÚEP je využíván koncept sdílených služeb a v souvislosti s principy činností veřejné správy se i v rámci ÚEP zachová princip digitálního dokumentu, který bude tvořen z dat publikovaných informačními systémy k danému času prostřednictvím stanovených služeb.

ÚEP je postaveno na 4 klíčových komponentách, které lze sdílet:

- elektronické formuláře;
- elektronická identita klientů veřejné správy i úředníků veřejné správy;
- propojený datový fond jako datový zdroj pro předvyplňování formulářů obsahující referenční údaje ze základních registrů (ZR), nereferenční údaje editorů ZR, nereferenční údaje agendových informačních systémů (AIS) publikované na eGSB (eGON Service Bus) a vlastní nereferenční údaje AIS;
- elektronické podání.

Nesmíme také opomenout možnosti získání finančních prostředků na realizaci ÚEP. Aktuálně je otevřená výzva č. 4 integrovaného regionálního operačního programu (IROP) s názvem Aktivita vedoucí k úplnému elektronickému podání. Čas kvapí a poslední žádosti budou přijaty 30. 6. 2017.

Zasazení do strategického plánu

V kontextu ÚEP je zásadní projektový okruh č. 3.1 Úplné elektronické podání, nicméně v širším rámci je vhodné respektovat další projektové okruhy, především pak:

- rozšíření, propojení a konsolidace datového fondu veřejné správy a jeho efektivní a bezpečné využívání dle jednotlivých agend;
- služby technologické infrastruktury, které lze sdílet;
- elektronická identita;
- elektronické doručování a ekvivalence dokumentů (eIDAS);
- elektronizace podpůrných procesů.

Vzhledem ke skutečnosti, že ÚEP veřejnost vnímá spíše pohledem řešení životní situace, je vhodné při konceptu ÚEP respektovat rovněž výstupy a doporučení projektu Ministerstva vnitra „Optimalizace životních situací ve vztahu k registru práv a povinností“.

Pohled ICZ – oproti architektonickým vzorům

Při schvalování projektů z oblasti ÚEP je zásadní získání kladného stanoviska odboru hlavního architekta

e-governmentu Ministerstva vnitra, který zkoumá shodu projektových záměrů (ve formě studie proveditelnosti) s pravidly, jež stanovil. V tomto kontextu jsou klíčové zejména vytvořené architektonické vzory sdílených služeb e-governmentu, které reprezentují současný, ale zejména budoucí stav problematiky úplného elektronického podání. Vyjadřují tak možné přístupy a druhy podání do AIS. Pro vyhovění AIS úplnému elektronickému podání je nutné mít zajištěné propojení se spisovou službou a podatelnou. Zde lze doporučit rozšíření komunikace i o další AISy ve smyslu samostatných evidencí dokumentů tak, jak je definuje Národní standard pro elektronické spisové služby.

Řešení ICZ: iPoint

A jaké jsou možnosti řešení z pohledu společnosti ICZ? Ta dlouhodobě vyvíjí a dodává standardizovaný produkt iPoint. Jedná se o ucelený systém pro realizaci úplného elektronického podání, který aktuálně využívá již několik organizací v rámci České republiky a Slovenské republiky, především statutární města a městské části, ale například i takové organizace, jako je Úřad priemyselného vlastníctva Slovenskej republiky, kde jsou využívány již velmi pokročilé a rozsáhlé formuláře, které nejsou pouze statické. Z pohledu uživatele je iPoint v základu velmi jednoduchou webovou aplikací, která obsahuje funkce, jako nepovinná registrace uživatele a editace uživatelského profilu, strom životních situací a výběr relevantního interaktivního formuláře, včetně validace jednotlivých polí a závislostí, které uživateli pomáhají formulář správně vyplnit, výběr komunikačního kanálu a možnost sledovat historii podání. Z uživatelského pohledu jde o velmi jednoduché a přehledné řešení, čímž se zvyšuje šance, že uživatel nebude odrazen realizovat samotné elektronické podání. Právě v tomto případě dvojnásob platí, že v jednoduchosti je síla. Z pohledu informačních systémů jsou na druhou stranu důležité integrační vazby a maximalizace automatizace zpracování podání. Velmi důležitou oblastí je integrace na Autentizační službu PVS (kterou mnozí znáte jako přihlašovací obrazovku ISDS), jež dokáže jednoznačně identifikovat patřičného uživatele. Dále tato služba umí

předat relevantní atributy o přihlašované osobě, čímž lze například automatizovaně předvyplnit vybraný elektronický formulář. Další velmi důležitá integrační vazba je se spisovou službou, která elektronické podání přijme a eviduje, stejně tak zpětně komunikuje s iPointem ohledně stavu relevantního elektronického podání. Ideální automatizací je pak předvyplnění všech potřebných metadat pracovníkovi organizace tak, že již vyplňuje naprosté minimum potřebných informací k danému podání. Podobně pak funguje možnost integrace s agendovými informačními systémy. Výše uvedené integrace dnes využívají bez rozdílu všichni stávající zákazníci. Kromě samotného provedení ÚEP si může uživatel ve webovém rozhraní zobrazit aktuální finanční závazky vůči dané organizaci (včetně kompletní platební historie), což lze realizovat opět díky jednoznačné identifikaci uživatele.

Aktuální limitace řešení

Jaké jsou však aktuální limitace řešení? Kromě chybějícího článku eGON Service Bus je z pohledu uživatele i poskytovatele služby zásadním a významným handicapem realizovat úplné elektronické podání bez nutnosti využití či aktivace datové schránky, případně elektronického podpisu. Ačkoli je k dispozici Autentizační služba PVS, tak ji nelze samostatně využít právě bez aktivace datových schránek, což je obrovská škoda. Dle MV ČR by v roce 2016 měla být dokončena platforma pro jednoznačnou identifikaci osob, včetně možnosti využití nového občanského průkazu s čipem. Stále ale není jasné, zda identifikace na nejvyšší úrovni bude možná pouze s pomocí nového OP, nebo bude možné na stejné úrovni využít i jiných služeb pro identifikaci osob. Ať tak či onak, pevně věříme ve světlé zítřky a brzy se určitě dočkáme zcela elektronické komunikace s veřejnou správou.

Luděk Louda a Tomáš Hrabík





Kybernetická bezpečnost versus úplné elektronické podání

Uvedená témata spolu neoddělitelně souvisejí a při jejich návrhu, budování a realizaci je nelze taxativně oddělit. Vzájemně se prolétají až do jemných souvislostí technického či procesního rázu.

Tolik teoretický pohled na věc a názor profesionála. Jak už to tak bývá u nás v českém království a markrabství moravskoslezském zvykem, každé téma si žije svým životem a svými problémy a na konec vždycky nějak dopadne. Díky našim dlouhodobým osobním zkušenostem jak ve veřejné správě, tak i v komerční sféře se na uvedená témata díváme komplexně ... upřesním, pokoušíme se je řešit komplexně a připravujeme se i na eventualitu takzvaně z druhé strany. Naše strana je v tento okamžik řešení kybernetické bezpečnosti v rámci provozu infrastruktury. Hledíme tedy skrze vize a představy či existující řešení z pozice správy infrastruktury na aplikační vrstvu a pokoušíme se o integraci bezpečnostních nástrojů a pravidel tak, aby úplná elektronická podání probíhala v legislativně definovaném a garantovaném prostoru. Zde je nutno podotknout, že cesta k zajištění kybernetické bezpečnosti je neméně trnitá a křivolaká stejně jako byla při vývoji aplikací pro úplná elektronická podání.

Snaha o rozvoj aplikací či prostředí pro realizaci úplných elektronických podání je tu již poměrně dlouhou dobu a může být tedy obecně vnímáno, že aplikace kybernetické bezpečnosti tuto snahu komplikuje a poněkud prodlužuje cestu k její realizaci. Odborníci vědí, že toto tvrzení lze stejně tak podpořit jako zamítnout. Před krátkým

časem, kdy se bezpečnost aplikací řešila pouze v kontextu „je to potřeba“ a na úrovni minimálně nutné, osvětlení architekti řešení a vizionáři se pokoušeli zvýšeným úsilím o šíření myšlenky bezpečného prostředí e-governmentu a strašili odbornou veřejnost historkami, která ve se Spojených státech hackeři tu a tam prolomili do státních systémů, poukazovali na thrillery typu „Síť“ a podobné. Nebylo to nic platné, stále vítězila myšlenka nikde otevřeně nevytvořená, „je to zbytečně drahý“ a „to se tady nemůže stát“. Boj proti větrným mlýnům je od časů dona Quijota stále beznadějnou disciplínou.

Čas však trhnul oponu, máme tu zákon č. 181/2014 Sb. a obec „kyberbezpečáků“, právníků, osvětlených „ajťáků“ a výrobců bezpečnostních technologií společně zajásala. Najednou se kybernetická bezpečnost dostala do oficiální role jako hlavní téma v oblasti elektronizace státní správy a samosprávy. Jenže ono se opravdu nestalo nic jiného, než že se z polohy „mělo by se“ stala poloha „musíš“. Z odborného hlediska nepřinesl zákon o kybernetické bezpečnosti nic nového. Učinil však důležitý posun v tom, že standardní kroky vedoucí k bezpečnému provozování ICT direktivně nařídil, a to v oblastech, které považuje zákonodárce za klíčové – slovy zákona za kritické a významné.



Zajištění bezpečnosti elektronického podání, resp. elektronické agendy má tři významné oblasti. Je to zabezpečení přístupu z veřejného internetu, zabezpečení přístupu zpracovatele a konečně zabezpečení dat. Napříč těmito oblastmi je dobré vždy zkoumat, jak hovoří legislativa, které náležitosti vyžaduje a jak přesně charakterizuje konkrétní úřední úkon, který hodláme převést do elektronické podoby. S touto problematikou má již dost subjektů veřejné správy své zkušenosti díky plošné snaze a trendu nasazovat AISy. Je však nutno ctít, že se jedná o základní bezpečnostní předpoklad – beze zbytku naplnit požadavek zákona.



Ing. Luděk Tichý

je absolventem VUT Brno, FS, obor měření, regulace a automatizace. Dvacet let pracoval na různých manažerských pozicích v oblasti ICT, z toho osm let v oblasti státní správy a samo-

správy. Prošel významnými firmami v oblasti vývoje SW a telekomunikací a několik let podnikal v oblasti kybernetické bezpečnosti. Od roku 2001 se zabývá kybernetickou bezpečností, v současné době jako vedoucí oddělení bezpečnosti ČP OZ ICTs.

Další bezpečnostní otázkou je kapacitní připravenost ve všech třech uvedených oblastech. Zajistit dostatečnou kapacitu s ohledem na vždy útlý rozpočet bývá složité, a proto je lepší odhadnout či odvodit přibližně vyhovující kapacitu a nasadit prostředky na její sledování a regulaci a dle zjištěných trendů kapacitu navyšovat. Tento postup se týká jak komunikačních, tak i úložných kapacit. V obou případech se sledováním uvedeného dostáváme ke klasické bezpečnostní disciplíně, kdy se pokoušíme vyhodnotit, zda je nárůst vytížení přirozený, nebo jedná-li se o formu útoku, pokus o destabilizaci a následnou kompromitaci systému. Tyto formy útoků jsou zaměřeny obvykle na napadení rozhraní mezi uvedenými oblastmi.

Uvedené skutečnosti nás vedou k opatřením, kterými dokážeme minimalizovat rizika narušení integrity a důvěryhodnosti dat v aplikacích pro elektronická podání. Základem je dnes již samozřejmé opatření perimetru firewally, IDS/IPS sondami, software na ochranu proti škodlivému obsahu a DDoS útokům. Mezi poměrně mladou, nicméně velmi účinnou disciplínu patří monitorování toků na data, a to nejen v síti, ale i v aplikacích. Výsledkem je poměrně účinný nástroj nejen pro optimalizaci infrastruktury či aplikace, ale i pro účinná a včasná bezpečnostní opatření.

Pokud jsme schopni výstupy z monitoringu napojit na nástroj SIEM a průběžně vylepšovat kombinace nastavení, určitě tím nadstandardně napomáháme bezpečnosti provozu veřejně dostupných aplikací. Stinnou stránkou je však vysoká cena SIEM a v neposlední řadě akutní nedostatek odborníků, kteří jsou schopni efektivně nasadit a následně vytěžit uvedená řešení. Dalším standardním nástrojem je Vulnerability scanning, který by měl umožnit nejen periodickou kontrolu odolnosti infrastruktury proti



bezpečnostním hrozbám, ale i ad hoc testování a vyhodnocování úrovně zabezpečení.

Oba tyto nástroje je teoreticky možno použít na vybudování tzv. Security operation center (užívaná zkratka SOC), což není úplně běžná disciplína, ale velmi účinná. Takovéto pracoviště proaktivního dohledu je na úrovni státní správy nutné právě proto, aby bylo vytvořeno bezpečné prostředí pro vznik aplikací podporujících elektronická podání. Nyní je toto téma akcelerováno přijetím evropské normy eIDAS, která otevírá možnost vzniku právní platformy pro komunikaci prostřednictvím sítě internet. Vznik státem garantované bezpečné platformy pro ochranu identity občana na internetu vytvoří poměrně značný prostor pro prudký nárůst aplikací, které jsou určeny k elektronické komunikaci mezi státem, občany, firmami a ostatními subjekty. Ochrana dat tímto postoupí do vyšší úrovně, neboť masovost sdílení dat vytvoří strmý nárůst pravděpodobnosti bezpečnostních hrozeb a rizik z toho vyplývajících.

V předchozím textu jsem velmi obecně uvedl běžná bezpečnostní opatření, nicméně zkušenost existuje na úrovni proprietárních řešení, která lze ohraničit. Je třeba se připravit na vznik diametrálně jiných hrozeb, umocněných právě zmíněnou masovostí. Pak bude nutno řešit úroveň investic do zabezpečení vůči socioekonomickým přínosům vlastní elektronizace. Tato cesta má totiž jeden silný aspekt, a to je nevratnost procesu. Jakmile stát poskytne elektronickou agendu, obávám se, že přechod zpět na papírové podání nebude možný. Tudíž je nutno smířit se s kontinuálními investicemi a koncepčně je zakotvit do zajištění ochrany dat.

Již existuje náznak záměru vydat se touto cestou, nicméně investice, které nás čekají, budou velké. Dovolil bych si předjímat, že role státu se bude muset v tomto tématu posí-

lit, protože na úrovni samosprávy nebude možno řešit tuto otázku dostatečně účinně. Samospráva zde bude v roli jen dalšího uživatele a množství napojených aplikací umožňujících elektronická podání bude minoritní. Je to z důvodu nutnosti nejen vlastního napojení, ale i efektivního využívání a sdílení systému státních registrů a možná i v blízké budoucnosti elektronické identity, což z pozice bezpečnosti je logické. Nejsem si však jistý z pozice laika, zda je legislativa, která toto umožní efektivně spravovat, kompletní.

Pochopitelně existuje spousta dalších drobných překážek a komplikací, nicméně jsem chtěl prokázat, že z pohledu aplikací existuje spousta příznivých předpokladů pro rychlé a masové rozšíření elektronických podání. Problémy jsou a budou v oblasti kybernetické bezpečnosti a je třeba se k nim postavit konstruktivně. Mnohé by vyřešilo, pokud by stát setrval delší dobu v jakési koncepci budování a rozšiřování ICT nástrojů pro komunikaci s občany a pokud by důsledně dbal na vznik a trvalé prosazování standardů nejen v oblasti kyberbezpečnosti, ale i infrastruktury pro provoz aplikací potřebných k rozvoji elektronizace státní správy a samosprávy.

Na závěr bych rád vyjádřil velká očekávání, která s sebou nesou témata eIDAS a kyberbezpečnost, jež jsou dnes státem již podporovaná a mají prioritu. Doufám, že stát nepoleví v důsledné podpoře rozvoje těchto témat a bude jim dopřávat jak finanční, tak i realizační podporu.

Ing. Luděk Tichý

Česká pošta, s.p., Odštěpný závod ICT služby

 **Česká pošta**
odštěpný závod **ICT služby**



ROK INFORMATIKY 2016

NÁCHOD 1. - 3. 6. 2016

Již tradičně si Vás dovolíme pozvat na pracovní setkání **všech**, pro které je důležitá
či zajímavá elektronizace veřejné správy v ČR.

V rámci jedné konference zde spolu mohou diskutovat zástupci ministerstev, krajů,
měst a obcí. Celý program, který je rozložen do tří dní, je koncipován tak,
aby si v něm každý z nich našel, co je pro jeho práci podstatné a důležité.

Letos poprvé budou v rámci konference ROK INFORMATIKY
vyhlášeny výsledky soutěže **eOSOBNOST EGOVERNMENTU**

Většina bodů programu se bude odehrávat přímo ve městě Náchod.

Odborná část všech tří dní v prostorách hotelu U Beránka.

Společenský večer prvního dne konference proběhne
v prostorách **vojenské pevnosti Dobrošov**.

Společenský večer druhého dne - slavnostní vyhlásování,
je umístěn do prostor **státního zámku Náchod**.

Více informací a registrační formulář na www.egovernment.cz/rok

Proč se zajímám o eIDAS?

Magazín Egovernment pořádá v roce 2015 seminář na téma eIDAS a záštitu mu tehdy poskytl místopředseda Poslanecké sněmovny Parlamentu ČR pan Jan Bartošek. Magazín Egovernment pokračoval dalším seminářem na téma eIDAS i v roce 2016 a opět pod záštitou místopředsedy Bartoška. Je tedy zřejmé, že právě problematika elektronické identity občanů je jeho tématem.



Místopředseda Poslanecké sněmovny Parlamentu ČR při zahajování semináře na téma eIDAS v roce 2015 uvedl:

„Žijeme v době kartové a internetové. Stát by měl dát občanovi jeden jediný doklad, který v sobě sloučí všechny

potřebné funkce pro identifikaci v reálném i kybernetickém prostoru.“ I proto jsme chtěli vědět, proč je pro něj toto téma důležité.

Jsem velký fanda všeho, co usnadní a zpříjemní lidem život. Když si vzpomenu na dlouhé fronty a nutnost dojíždění za každým výpisem z rejstříku trestů, z katastru, z obchodního nebo živnostenského rejstříku, jsem rád, že toto jsou věci, které od nás v minulém desetiletí odvál projekt Czech POINT, a cítím velkou vděčnost ke všem propagátorům elektronizace státní správy a samosprávy. Nakonec státní agendy nejsou nic jiného než jedna velká počítačová databáze a v dnešní době jsme zvyklí vyřizovat vše po internetu. Tak proč by občan měl běhat za úředníky, když je pro obě strany lepší zprostředkovat vše co nejbližší občanovi. Nejlépe je, aby občan vůbec nikam chodit nemusel, tedy myslím ani na Czech POINT, i když jich je dnes více než 7000, a vše mohl vyřídit odkudkoliv po internetu. Stát ale potřebuje u některých typů služeb vědět, že jedná opravdu s určitým občanem, a k tomu je nutné dát mu nějakou „internetovskou občanku“ a to zajistí právě eIDAS.

Takže Vy chápete eIDAS jako další logický krok v elektronizaci státu?

Jistě. V tuto chvíli máme nějaké průkopníky, například Českou správu sociálního zabezpečení, kde již před více než rokem zprovoznili pohodlnou komunikaci s jejich portálem po internetu, a to po ověření přes datovou schránku.

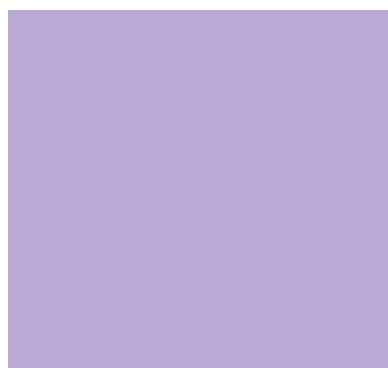
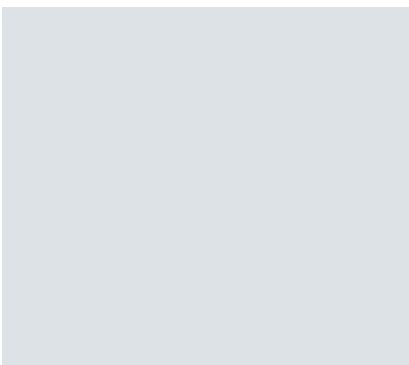
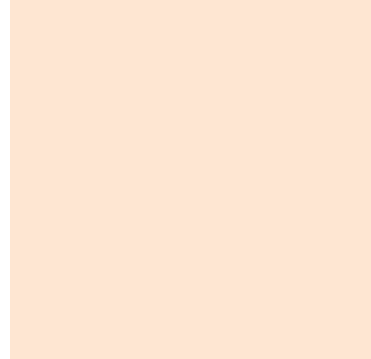
Živnostníci a firmy již dlouho komunikují zase s finančním úřadem přes internet a do papírové podoby komunikace by se asi vracet nechtěli. eIDAS není žádná vymyšlenost našich politiků, ale nařízení Evropské komise, a tak nepřinese našim občanům pouze možnost využívání systému našeho státu, ale systémů institucí i komerčních subjektů celé EU.

Co si od zavedení eIDAS slibujete Vy osobně?

Jako občan si představuji, že má šílená pracovní doba „od nevidím do nevidím“ již nebude překážkou v tom, abych si v klidu z domova nevyřídil své pochůzky po úřadech pěkně v kybernetickém prostoru po internetu a to klidně o půlnoci nebo o víkend. A jako politik si představuji spokojené občany, kteří si tyto technologie široce osvojí stejně tak jako ostatní internetové technologie. Císař Josef II. řekl: „Buď vládcem občanů, ne otrokům!“ a tak si hlavně slibuji zažít tu svobodu, kterou nám dává internet např. při nakupování, také v jednání s úřady, a protože to technika umí, nevidím důvod, proč občana honit někam k přepážce.

Kam jsme se za ten rok, kdy se konal náš první seminář s tématem eIDAS, podle Vás posunuli?

U nás v Parlamentu proběhly jen další semináře, ale hlavní práci má na bedrech Ministerstvo vnitra. Jsem moc rád, že pan náměstek Strouhal přijal mou nabídku a já se mohu aktivně účastnit přípravy legislativní části. Ono už je málo času, a pokud máme dodržet termíny nařízené Evropskou komisí pro zavedení eIDAS, pak je nutné, aby celý legislativní proces proběhl bez zádrhelů, a tomu bych velice rád dopomohl. I to jsou důvody, proč jsem podpořil seminář magazínu Egovernment s tématem eIDAS v roce 2015 a proč jsem tak učinil i letos.



ISSS 2016

DOPROVODNÁ MEZINÁRODNÍ KONFERENCE **V4DIS**

4.–5. DUBNA 2016 HRADEC KRÁLOVÉ

KONGRESOVÉ CENTRUM ALDIS, ELIŠČINO NÁBŘEŽÍ 375

- ... 19. ročník renomované konference – jedné z největších evropských akcí svého druhu
- ... Mimořádná příležitost k setkání se špičkami domácí politické scény, ministry, zástupci státní správy a samospráv z ČR i zahraničí, krajskými či městskými informatiky, vysokými manažery renomovaných firem i nezávislémi odborníky
- ... Přes 200 přednášek a vystoupení během dvoudenního programu, více než 100 partnerů a firem ve výstavní části
- ... Průběžné zpravodajství na **www.issc.cz**

Registrujte se již nyní na www.issc.cz/registrace

Do 31. 12. 2015 účastnický poplatek za zvýhodněnou cenu

issc
LOCAL AND REGIONAL INFORMATION SOCIETY
V4DIS

Elektronická identita

V celé Evropské unii se radikálně změní nakládání s elektronickými dokumenty. To je základní zpráva, kterou sebou přináší nařízení Evropského parlamentu pro služby vytvářející důvěru a elektronický dokument.

Konkrétně po 1. 7. 2016, kdy toto nařízení vstoupí v účinnost bude platit, že:

- elektronický dokument opatřený kvalifikovaným elektronickým podpisem se stane ekvivalentem listiny s vlastnoručním podpisem;
- nikdo **nebude** moci odmítnout **elektronický dokument**, který bude splňovat náležitosti dané nařízením eIDAS;
- tímto krokem dojde k odbourání **bariéry v elektronickém styku** mezi jednotlivými členskými státy EU.

Právě důležitosti tohoto tématu se v programu semináře **eIDAS – jarní pohled, aneb máme to už za pár**, který magazín Egovernment pořádal v Poslanecké sněmovně Parlamentu ČR, věnovali ve svých vystoupeních Robert Piffll, poradce náměstka ministra, Michal Pešek, ředitel SZR, a Petr Budiš z I. CA. Každý ze svého pohledu hovořil o zásadních momentech, které nařízení přináší, i o dalších krocích, které budou, či musí následovat.

Prezentace Roberta Pifflla byla, z důvodu nemoci, v zastoupení realizována Michalem Peškem a byla doplnována a komentována Petrem Kuchařem, ředitelem odboru hlavního architekta e-governmentu. Ten se rovněž zapojoval do diskuze, která byla charakteristická pro celý program semináře.

ROVNOST, ODPOVĚDNOST, POVINNOST

Nařízení přináší skutečné zrovnoprávnění elektronického dokumentu s papírovým.

Pro elektronický dokument je nyní charakteristické, že:

- podepsaný kvalifikovaným elektronickým podpisem platí, že se na něj nahlíží stejně jako na dokument v listinné podobě podepsaný vlastnoručním podpisem;
- opatřený kvalifikovanou elektronickou pečeti platí domněnka integrity dat a správnosti původu dokumentu, se kterým je pečeť spojena;

- opatřený kvalifikovaným elektronickým časovým razítkem platí domněnka správnosti data a času, které udává, a integrity elektronického dokumentu;
- doručení službou elektronického doporučeného doručování platí domněnka integrity dat, odeslání a přijetí těchto dat identifikovaným odesílatelem a příjemcem, správnosti data a času odeslání a přijetí.

Podstatnou novinkou, kterou nařízení přináší, je odpovědnost za škodu, protože ji určuje všem, kteří budou provozovat elektronické služby veřejné správy. Ti nyní musí zvažovat, jak dalece mohou občanovi způsobit určitou škodu. Konkrétně tedy platí:

- členské státy, ale i poskytovatelé služeb vytvářejících důvěru mají odpovědnost za škodu při provozování služeb vytvářejících důvěru a v některých případech i jejich nedostupnosti;
- kombinace skutečnosti, že elektronický dokument podepsaný kvalifikovaným podpisem na kvalifikovaném certifikátu je rovnocenný listině s vlastnoručním podpisem a odpovědnost za škodu definované v nařízení eIDAS, bude velmi pozitivním katalyzátorem elektronizace veřejné správy v celé EU.

Nástroje pro vytváření kvalifikovaných podpisů na kvalifikovaném certifikátu budou k dispozici ihned od 1. 7. 2016 – od tohoto data nemůže veřejná správa požadovat pouze listinou podobu.

K zajištění uvedených služeb je nutné, aby členské státy EU měly:

- fungující a právně zakotvený orgán dohledu nad poskytovateli služeb vytvářejících důvěru (v ČR je to MV ČR);
- připraveny národní akreditační ústavy k akreditaci subjektů posuzování shody;
- zajištěno oznamovat služby vytvářející důvěru podle prováděcího aktu 2015/1505 k nařízení eIDAS;



- oznámit seznam QSCD komisi EU dle nařízení eIDAS
- **veřejnou správu připravenou akceptovat formáty zaručených elektronických podpisů** a zaručených elektronických pečeti v souladu s prováděcím aktem 2015/1506 tam, kde je vyžadován zaručený elektronický podpis nebo pečeť;
- systém dohledu s efektivními sankcemi a pokutami.

Pokud jde o samotnou otázku identity, stát nyní plánuje státního identity providera, který bude mít jako identitní prostředek občanský průkaz. Do budoucna bude možné, aby existovali i soukromoprávní identity provideři. Vzhledem k tomu, že stát ručí za správnou identifikaci, bude nutné doladit přenesení uvedené odpovědnosti, a tedy možných právních potíží v případě chybné identifikace, či špatného použití identitního prostředku, na tento soukromoprávní subjekt či subjekty.

JAK VZNIKÁ DŮVĚRA?

Základním principem nařízení eIDAS jsou zcela jasně definované a rozdělené, ale vzájemně se doplňující služby, a to podle jejich účelu, v nichž je pro správné využívání služeb vytvářejících důvěru zcela zásadní nezaměňovat jejich primární účel:

- eID a služby poskytující důvěru pro identifikaci obecně slouží k identifikaci pro autentizaci v rámci on-line služeb;
- podpisy a pečete slouží k projevu vůle podepisující nebo pečeti osoby;
- služby elektronického doporučeného doručování slouží k doručování.

Podstatné je, že elektronické doručování a eID samo o sobě **nemůže ani prostřednictvím jiných služeb vytvářejících důvěru nahradit projev vůle**. Ten může být vyjádřen pouze podepsáním elektronickým podpisem nebo označením elektronickou pečeti. K projevu vůle je tedy nutné vždy využít elektronický podpis nebo elektronickou pečeť.

Samotný elektronický dokument podepsaný kvalifikovaným podpisem na kvalifikovaném certifikátu je možné

doručit libovolným způsobem a je rovnocenný listině s vlastnoručním podpisem. Důležitým nástrojem v procesu identifikace je občanský průkaz. Ten by nově měl mít, kromě autentizační funkce, rovněž funkci podepisovací. Pravděpodobně po roce 2017 by tak občané měli díky svému OP k dispozici plnou kryptografickou výbavu pro vzdálené přihlášení k portálům veřejné správy, případně i k soukromým portálům, a zároveň nástroj k projevení vůle, tedy možnost podepsat dokument svým elektronickým podpisem. V ČR je nyní ustaven poradní orgán ministra – řídicí výbor eIDAS, jehož věcným garantem je odbor hlavního architekta. MV nyní upravuje životní situace tak, jak se změni po 1. 7. 2016.

I PŘES UVEDENÉ REALIZOVANÉ KROKY A TECHNOLOGIE BUDE MOŽNÉ, ABY OBČAN PŘI PŘEVZETÍ OBČANSKÉHO PRŮKAZU JEHO ELEKTRONICKÉ FUNKCE ODMÍTL.

Z diskuze rovněž vyplynulo, že určité mezinárodní rozdíly budou existovat. Poprvé od roku 1999 vzniká nová směrnice a v místních legislativách se „vyrábějí“ prováděcí zákony. Ty nesmí být v rozporu s touto směrnicí, tedy pouze regionálně rozšiřují nařízení. I když nemohou být s tímto nařízením v rozporu, určité budou rozdíly mezi státy v určitých detailech a interoperabilita bude určitým problémem.

Ze stávajících služeb lze kontinuálně poskytovat pouze službu vydávání kvalifikovaných certifikátů pro elektronický podpis. **Zahájení poskytování dalších služeb je podmíněno provedením posouzení shody** (audit). Audit mohou provádět pouze k tomu **oprávněné subjekty, určené Českým institutem pro akreditaci (ČIA)**. Je otázka, zda takové subjekty včas vzniknou a zda pokryjí potřeby tří stávajících akreditovaných poskytovatelů. Je nutné, aby alespoň ty služby, pro které český zákon stanoví dvouletý odklad, bylo možné poté návazně poskytovat.



TECHNICKÉ NORMY, KTERÉ BY MĚLY ZAJISTIT JISTOTU OVĚŘOVÁNÍ, TJ. STANOVIT PŘÍSLUŠNÉ POŽADAVKY, MAJÍ DOSUD NEJASNÝ STATUT „ZÁVAZNÉ/DOPORUČUJÍCÍ“. ROVNĚŽ DOSUD NENÍ K DISPOZICI JEJICH FINÁLNÍ ZNĚNÍ.

PROBLÉM KOMUNIKACE PŘES HRANICE ČLENSKÝCH STÁTŮ

Pokud bude nutné zaslat do jiného členského státu dokument, který bude podepsán během dvouletého přechodného období uznávaným elektronickým podpisem (bez QESCD), patrně nebude v jiném členském státu podpis akceptován, neboť se nebude jednat o kvalifikovaný elektronický podpis podle eIDAS („změkčení“ požadavku platí jen pro ČR).

eIDAS prováděcí akty

1. Prováděcí rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti **elektronické identifikace** podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
2. Prováděcí nařízení Komise (EU) 2015/806 ze dne 22. května 2015, kterým se stanoví specifikace týkající se podoby **značky důvěry EU** pro kvalifikované služby vytvářející důvěru
3. Prováděcí rozhodnutí Komise (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro **formáty zaručených elektronických podpisů a zaručených pečeti uznávaných subjekty veřejného sektoru** podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
4. Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví **technické specifikace a formáty důvěryhodných seznamů** podle čl. 22 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
5. Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví **minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci** podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
6. Prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o **rámci interoperability** podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
7. Prováděcí rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví **okolnosti, formáty a postupy pro oznamování** podle čl. 9 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

MISS EGOVERNMENT 2016

Magazín Egovernment spustil přihlašování do nového ročníku soutěže o nejsympatičtější dámu ve veřejné správě. Jste sympatická a komunikativní, nebo máte kolem sebe takové kolegyně? Stačí vyplnit on-line formulář.

CO JE MISS EGOVERNMENT



Jedná se o soutěž, kterou vyhlašuje magazín Egovernment a která je určena všem sympatickým dámám, které pracují v rámci elektronické veřejné správy. Díky zprovoznění základních registrů je možné tvrdit, že na výkonu elektronické veřejné správy se nyní podílí úplně každý pracovník veřejné správy a proto je i tato soutěž určena všem dámám, které v ní pracují. To znamená, že soutěžít může referentka, tisková mluvčí, vedoucí odboru, obsluha Czech POINTu, starostka, pracovnice spisové služby ... prostě každá dáma, která pracuje ve veřejné správě. Věková hranice není nijak omezena. Stačí, když se jedná o sympatickou, komunikativní dámu.

Soutěž je poděkováním všem, kteří se věnují výkonu elektronické veřejné správy. Zároveň chceme představit sympatické dámy, neboť převážně ony ve veřejné správě pracují, a také trochu navodit příjemnou a zábavnou atmosféru jako poděkování za jejich práci.



2009



2010



2011



2012



2013



2014



2015

Přihlásit se mohou jak přímo samotné dámy, nebo je mohou přihlásit jejich kolegové. Podrobné informace a registrační formulář naleznete na www.egovernment.cz/miss

Finále se koná 6. 9. 2016 na zámku Mikulov v rámci společenského večera konference **e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně** (www.egovernment.cz/mikulov).
Vítězku čeká tradičně hodnotná a zajímavá cena.



WWW.EGOVERNMENT.CZ/MISS

Poskytování důvěryhodných služeb podle eIDAS

Již za několik měsíců, konkrétně 1. 7. 2016, vejde ve všech členských státech EU v účinnost nová právní úprava některých elektronických služeb. Vztahuje se především na oblasti, ve kterých jsou vyšší nároky na bezpečnost, na identifikaci komunikující osoby, na prokázání identity původce dokumentu a možnosti zjištění, zda dokument nebyl po jeho vzniku změněn. Bude se tedy týkat zejména úřadů a těch, kteří s nimi komunikují, finančních institucí a jejich klientů a dalších podnikajících subjektů. Můžeme se těšit i na zcela nové služby, které uživatelům usnadní práci s elektronickými dokumenty a výrazně přispějí k vyšší bezpečnosti elektronické komunikace a učiní ji ještě více důvěryhodnou. Naopak nijak významně se neprojeví v oblastech, ve kterých tyto atributy nehrají stěžejní roli, tj. v běžné e-mailové komunikaci a na sociálních sítích.

Evropské nařízení, pro které se užívá zkratka „eIDAS“¹⁾ a které má právní sílu stejnou jako jakýkoliv náš zákon publikovaný ve Sbírce zákonů, upravuje jednak oblast elektronické identifikace osob (pro nás novou) a dále náležitosti některých nástrojů elektronických služeb, které mají vykazovat nejvyšší záruku kvality a spolehlivosti. Mají být na takové úrovni, že budou použitelné pro elektronické transakce na celém vnitřním trhu EU. Jedná se především o elektronické podpisy a služby s nimi spojené, dále o elektronické doručování a elektronické dokumenty.

Co k této nové právní úpravě evropské instituce vedlo?

Dosud platná evropská směrnice²⁾, na kterou eIDAS navazuje a kterou nahrazuje, upravovala jen jeden nástroj elektronické komunikace – elektronický podpis, který při splnění podmínek stanovených evropskou směrnicí je uznáván ve všech členských státech EU, bez ohledu na to, ve kterém členském státu se člověk elektronicky podepsal. Evropská směrnice je platná od roku 1999 a logicky pokulhává za potřebami praxe. Členské státy na to reagovaly tak, že postupně zaváděly a legislativně upravovaly další elektronické služby, které ale nemohly být bez dohody komunikujících stran akceptovatelné za jejich hranicemi. V České republice byly například zavedeny a legislativně upraveny elektronické značky, u nichž na rozdíl od elektronického podpisu nebyl požadavek na

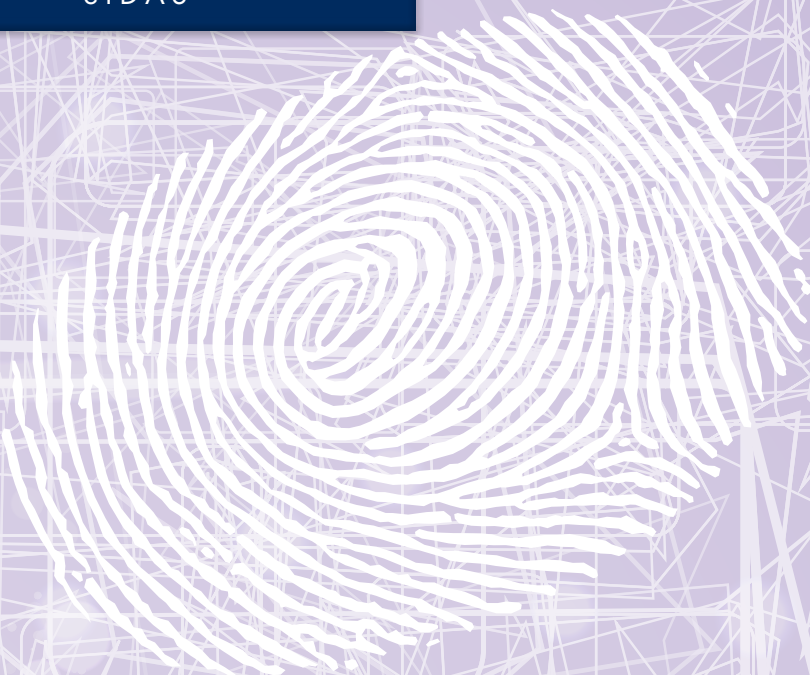
seznámení se s označovaným dokumentem a ke kterým jsou certifikáty vydávány i pro právnické osoby. Stejně tak byla uvedena do praxe časová razítka, která potvrzují existenci dokumentu v určitém čase. eIDAS tyto nebo obdobné nástroje a s nimi spojené služby upravuje pro celounijní použití.

eIDAS je možné z hlediska jeho obsahu rozdělit do tří tematických částí – elektronická identifikace, služby vytvářející důvěru/kvalifikované služby vytvářející důvěru a elektronický dokument. Služby poskytovatelů certifikačních služeb se vztahují zejména ke druhé oblasti, tj. službám vytvářejícím důvěru. Přibližme si tedy, jak to s těmito službami bylo, je a bude.

V České republice byla evropská směrnice implementována zákonem č. 227/2000 Sb., o elektronickém podpisu. V následujících letech se elektronický podpis začal ve stále větší míře uplatňovat v praxi, a to i v oblastech, ve kterých to žádný právní předpis sice nevyžadoval, ale jevílo se jako výhodné využít vlastnosti elektronického podpisu – především zajištění integrity dokumentu a nepopíratelnosti jeho původu. S rozšířením používání elektronického podpisu nutně dochází – i když v menší míře, než se předpokládalo – k pokusům o podvodné jednání. Oproti původním obavám z prolomení algoritmů jsou tyto pokusy zcela „obyčejně“, zpravidla se jedná o snahu získat

¹⁾ Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

²⁾ Směrnice Evropského parlamentu a Rady 99/93/ES o zásadách Společenství pro elektronické podpisy.



certifikát na základě zfalšovaných dokumentů kvůli používání tohoto certifikátu k nezákonné činnosti (vydávání se za někoho jiného). S cílem maximálně dosažitelné míry bezpečnosti reaguje eIDAS tak, že výslovně stanoví, že pouze „kvalifikovaný elektronický podpis“ má právní účinek rovnocenný vlastnoručnímu podpisu, tj. jedná se o zaručený elektronický podpis založený na kvalifikovaném certifikátu a použit je kvalifikovaný prostředek pro vytváření elektronických podpisů. V České republice jsou takové prostředky k dispozici již nyní, jedná se o čipové karty Starcos 3.0 a 3.2, které svým zákazníkům poskytuje První certifikační autorita, a.s. (I.CA) a používá je celá řada úřadů i komerčních subjektů.

Jaké služby podle eIDAS budou moci nabízet dnešní akreditovaní poskytovatelé certifikačních služeb?

Z těch kvalifikovaných, tj. požívajících nejvyšší stupeň důvěry, jsou to kromě vydávání kvalifikovaných certifikátů pro elektronické podpisy rovněž vydávání kvalifikovaných certifikátů pro elektronické pečeti (obdobu elektronické značky, ovšem použitelná pouze na straně původce dokumentu), dále kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů/pečetí, kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů/pečetí, vydávání kvalifikovaných elektronických časových razítek, vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek. U nových služeb je v současné době ze strany uživatelů největší zájem o službu ověřování platnosti kvalifikovaných elektronických podpisů.

Bohužel z uvedených nových služeb bude možné bezprostředně po 1. 7. 2016 využívat pouze vydávání kvalifikovaných certifikátů pro elektronický podpis. Tuto službu mohou naši stávající akreditovaní poskytovatelé i nadále poskytovat. Pro poskytování ostatních služeb je podmínkou provedení auditu podle eIDAS, který logicky může být proveden, až eIDAS nabude účinnosti a budou k tomu vytvořeny příslušné nástroje (například určení subjektů, které budou audit provádět). Doufejme, že v dohledné době budou vydány i veškeré relevantní evropské technické normy. Jak v České republice překleneme přechod od režimu zákona o elektronickém podpisu k režimu eIDAS, a to zejména u elektronických značek a časových razítek, stanoví připravovaný adaptační zákon o službách vytvářejících důvěru pro elektronické transakce, který je v gesci Ministerstva vnitra.

Očekávat můžeme i další nové služby, které eIDAS výslovně neupravuje, ale vytváří pro ně právní prostředí a shledává je perspektivními – podepisování prostřednictvím mobilního telefonu a podepisování v cloudech nebo vytváření elektronického podpisu na dálku.

Mgr. Dagmar Bosáková,
První certifikační autorita, a.s.



eIDAS není strašák, uživatelé systému GINIS se ho obávat nemusí

Stále častěji se setkáváme s novou zkratkou „eIDAS“, která se mnohdy stává tak trochu neoprávněným strašákem. Co si zase ten Brusel na nás vymyslel? Jak „to“ splnit co nejjednodušeji? Podívejme se tedy stručně, o co jde a co to bude znamenat pro uživatele systému GINIS.

Novinky v elektronických transakcích

Nařízení Evropské unie eIDAS si klade za cíl vytvořit jednotné celoevropské prostředí, v němž bude rutinně fungovat elektronická identifikace (elektronické prokazování totožnosti) a další služby vytvářející důvěru pro elektronické transakce na vnitřním trhu EU. Do této oblasti spadají také služby pro vytváření a ověřování elektronických podpisů, pečeti a časových razítek.

A právě zde se zakotvuje celoevropský princip, že důvěryhodnost digitálního dokumentu musí primárně vycházet z dokumentu samotného a z jeho atributů. Z tohoto důvodu prováděcí rozhodnutí EU 2018/1506 zavádí povinnost používat zaručené elektronické podpisy a zaručené elektronické pečeti v souladu se specifikací ETSI (PADES, XAdES, CAdES), tedy tzv. dlouhodobě ověřitelné (LTV – Long-Term Validation), což je samo o sobě řešitelné soft-

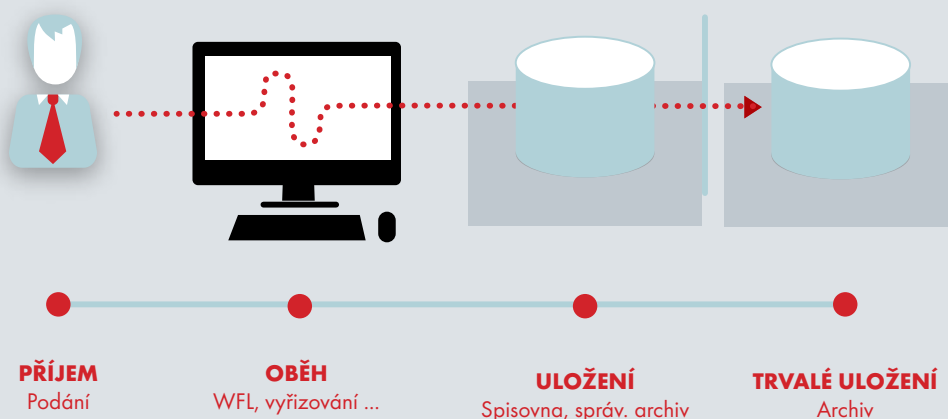
warovou úpravou tvorby elektronického podpisu a běžného uživatele se v podstatě nijak nedotkne.

Jeden drobný zádrhel to však přece jen přináší – uvedený dlouhodobě ověřitelný elektronický podpis pro PDF dokumenty (PADES) je možné plnohodnotně vložit pouze do „novějšího“ formátu PDF/A-2 a vyššího (založeného na PDF verzi 1.7). Doposud běžně užívaný formát PDF/A-1 (založený na PDF verzi 1.4) bude již nedostatečný. Původci tedy musí mimo jiné inovovat své nástroje na tvorbu PDF/A, včetně konverzních nástrojů.

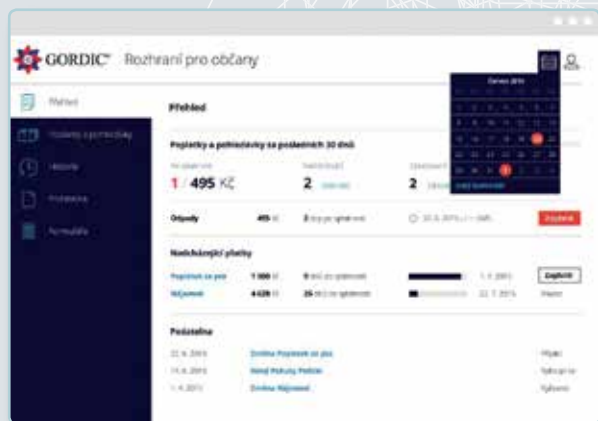
Zákonná úprava od 1. července

Nařízení eIDAS je s ohledem na smlouvu o fungování Evropské unie přímo platné ve všech zemích EU (od 1. 7. 2016), a není tedy nutné jej transponovat do naší legislativy. Bylo by ale nepříjemné, kdyby byl eIDAS

Oběh elektronických dokumentů v organizaci



Přehled pohledávek občana prostřednictvím aplikace systému GINIS



v rozporu s naší legislativou (pak by eIDAS „přebil“ naši legislativu, což by mohlo vést k chaotickému stavu). Proto se již nyní pracuje na novém zákonu „o službách vytvářejících důvěru pro elektronické transakce a o změně některých zákonů“, který bude platný také od 1. 7. 2016.

Tento zákon zcela nahradí (a tím i zruší) současný zákon č. 27/2000 Sb., o elektronickém podpisu. Ale také, jak již jeho název naznačuje, přinese „legislativní smršť“ drobných i větších změn v mnoha jiných zákonech a samozřejmě i v prováděcích vyhláškách. Dotčen bude například i zákon č. 499/2004 Sb., o archivnictví a spisové službě, zákon č. 300/2008 Sb., o elektronických úkonech

a autorizované konverzi dokumentů, zákon č. 500/2004 Sb., správní řád atp. Polovina roku 2016 bude tedy opět legislativně velice zajímavá.

GINIS v souladu s eIDAS

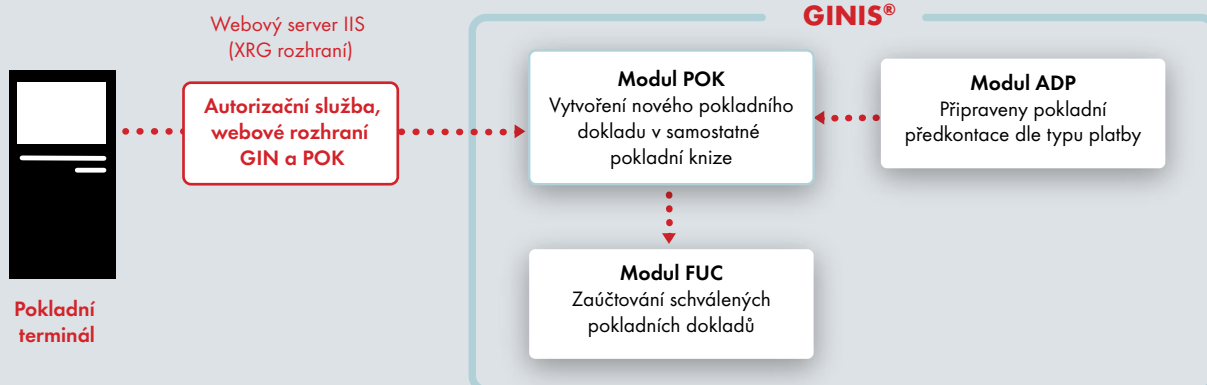
Tým odborníků společnosti GORDIC samozřejmě tento vývoj aktivně sleduje a připravuje pro Vás již tradičně nejlepší softwarové produkty na českém trhu, po právu označované jako „pozoruhodné“, navíc podpořené špičkovou metodikou. Ne jinak tomu je i v tomto případě. Aktuální distribuční verze systému GINIS již dnes obsahuje možnost práce s digitálními dokumenty a elektronickými podpisy v plném souladu s nařízením eIDAS.

Pro zvýšení jistoty svých zákazníků navíc právě završujeme nezávislou certifikaci produktu GINIS na soulad s eIDAS a příslušnou technickou specifikací ETSI.

Portál občana: poplatky lze zaplatit i přes telefon

Současně s připravovanou změnou legislativy v oblasti autentizace reaguje společnost GORDIC také na aktuální výzvu k překládání projektů na aktivity podporující úplné elektronické podání. Informační systém GINIS vytváří podporu samoobslužných procesů veřejné správy, které občané nebo firmy využívají bez nutnosti osobní návštěvy na úřadu a bez nutnosti zprostředkování služby veřejné správy úředníkem.

Komunikace platebního terminálu s ekonomickým systémem



Nikoliv nevýznamnou roli v této nabídce hraje řešení rozhraní pro občany, prověřené již v praxi. Tato aplikace umožňuje komunikaci občana s úřadem bez nutnosti jeho osobní návštěvy. Data jednotlivých pohledávek občana jsou načítána přímo z informačního systému GINIS a jsou tedy v každém okamžiku aktuální. Platbu lze zadat i sejmutím QR kódu v mobilní aplikaci internetového bankovníctví. Vedle pohledu na stav pohledávek je v nabídce i možnost zasílání upozornění na blížící se splatnost předpisu formou e-mailu nebo SMS zprávy.

Kromě výhody samoobslužné služby vede tato služba ke snížení administrativní zátěže měst a obcí spojené s rozesíláním upomínek a k posílení pravidelného příjmu z poplatků. Občané zase mohou kdykoliv zkontrolovat svoje platby vůči městu a předejít tak případným potížím s řešením nedoplatků a případných exekucím.

Plaťme i mimo úřední hodiny

Podporu samoobslužných procesů představují stále častěji také samoobslužné platební terminály. Terminál je onli-

ne propojen s informačním systémem GINIS, vzájemná komunikace je zajištěna pomocí online webových služeb. Je tak zajištěno okamžité zaúčtování transakce. Platby se automaticky načítají do modulu pokladna, kde je vytvořen nový platební doklad, a dále jsou již standardní cestou účtovány. Lidé mohou tímto způsobem platit poplatky za řidičské a profesní průkazy, poplatky taxislužby, výpisy z evidence řidičů, poplatky spojené se stavebním řízením, zvláštním užíváním pozemku atd., a to i ve dnech či hodinách, kdy je klasická pokladna zavřena.

Miroslav Čejka
GORDIC spol. s r. o.



GORDIC[®]

Přehled pojmů, užitečné odkazy

eIDAS – Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Podle článku 52 odst. 2 se toto nařízení použije od 1. 7. 2016.

EU 2015/1506 – Prováděcí rozhodnutí Komise (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle čl. 27 odst. 5 a čl. 37 odst. 5 eIDAS.

ETSI (European Telecommunications Standards Institute) – organizace zabývající se standardizací ICT v Evropě. Její technické specifikace pro zaručené elektronické podpisy a zaručené elektronické pečeti (PAdES, XAdES a CAdES – LTV, tzv. dlouhodobě ověřitelné) představují základ pro definici služeb vytvářejících důvěru, definovaných v eIDAS a EU 2015/1506.



OSOBNOST

eGOVERNMENTU 2016



eOSOBNOST EGOVERNMENTU

Hledáme osobnosti, které se nejvíce zasloužily o rozvoj a popularizaci elektronizace veřejné správy v ČR

v kategoriích:

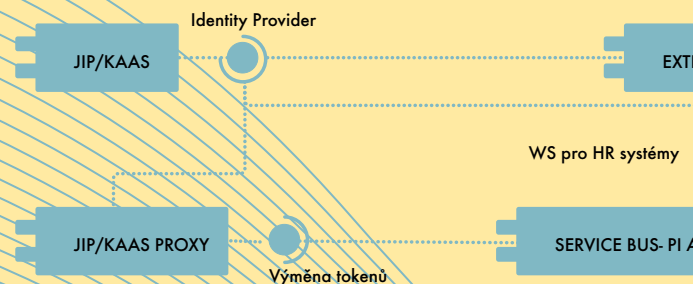
- eOsobnost centrálních úřadů/institucí;
- eOsobnost krajů;
- eOsobnost Měst (MČ);
- eOsobnost obcí.

POD ZÁŠTITOU

RNDr. Josef Postránecký,
náměstek ministra vnitra
pro státní službu

Mgr. Jana Vildumetzová,
náměstkyně ministra vnitra
pro řízení sekce veřejné správy

Své kolegy, vedoucí, šéfy úřadů a další můžete a musíte do soutěže nominovat VY.
Více informací a nominační formulář na www.egovernment.cz/eOSOBNOST



ISoSS

Od 1. července 2015 zahájilo Ministerstvo vnitra provoz Informačního systému o státní službě (ISoSS). Stalo se tak o rok a půl dříve, než bylo stanoveno zákonem o státní službě, a po 6 měsících vývoje. ISoSS obsahuje údaje nezbytné pro správu organizačních věcí služby a správu služebních vztahů a provádění úkonů stanovených zákonem o státní službě. Tvoří jej čtyři moduly - rejstřík státních zaměstnanců, evidence obsazovaných služebních míst, portál pro přihlašování na úřednickou zkoušku a evidence provedených úřednických zkoušek. ISoSS je primárně určen pro úřady, ale s vybranými údaji se může seznamovat i veřejnost, proto se dělí na veřejnou část a část přístupnou pouze uživatelům přihlášeným přes JIP/KAAS.

Rejstřík státních zaměstnanců obsahuje základní údaje o státních zaměstnancích a jejich služebním poměru. Modul evidence obsazovaných služebních míst obsahuje údaje o volných služebních místech a vyhlášených výběrových řízeních, která jsou také přístupná ve veřejné části portálu ISoSS. Portál pro přihlašování na úřednickou zkoušku slouží k organizaci a zajištění úřednické zkoušky a modul evidence provedených úřednických zkoušek je určen k evidenci a analýze dat o úřednických zkouškách, přičemž část z těchto dat je také přístupná veřejnosti.

Příprava a náběh do produktivního provozu

Pro zajištění plynulého náběhu a potřebné podpory uživatelů byl od 1. 7. 2015 do 30. 9. 2015 naplánován postupný náběh plné funkcionality ISoSS ve 3 vlnách a po jednotlivých modulech. V první vlně byla převedena data Ministerstva vnitra, ve druhé vlně data pilotních úřadů, kterými bylo Ministerstvo financí, Ministerstvo životního prostředí, Ministerstvo spravedlnosti a Správa státních hmotných rezerv, a ve třetí vlně dalších 227 služebních úřadů.

ISoSS se stal plně funkčním již 22. 9. 2015, kdy byla ve veřejně přístupné části ISoSS otevřena evidence obsazovaných služebních míst.

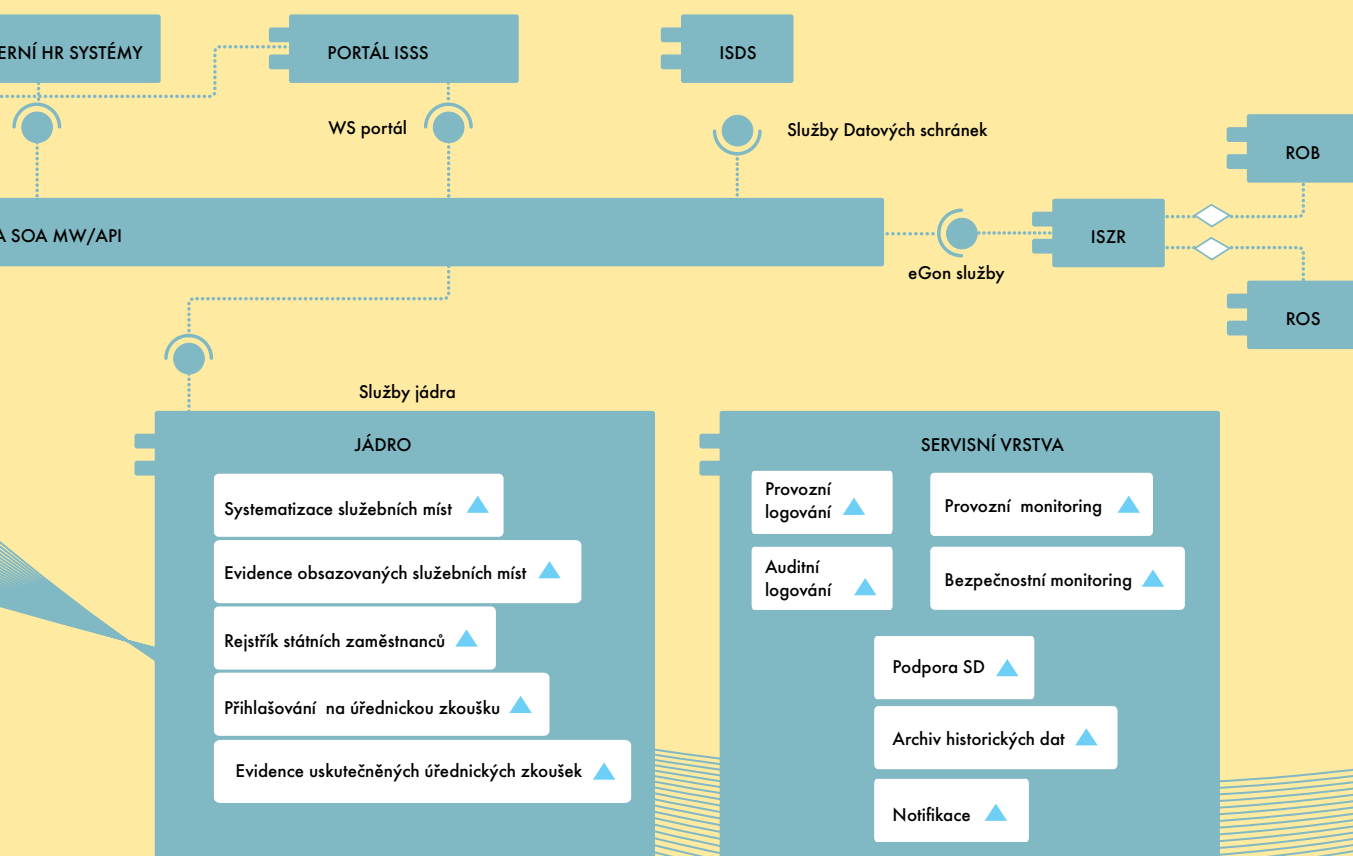
Před zahájením produktivního provozu intenzivně probíhaly přípravné práce, včetně metodické podpory služebních úřadů ze strany Ministerstva vnitra. Napojení na ISoSS vyžadovalo také úzkou spolupráci uvnitř služebních úřadů a zapojení dodavatelů personálních systémů, které služební úřady používají.

Spolupráce se služebními úřady

Služební úřady od zahájení příprav ISoSS aktivně spolupracují a v současnosti velmi dobře činnost se systémem zvládají. Postupné spouštění a zapojování služebních úřadů umožnilo odzkoušet systém a odladit tak problémy, se kterými se úřady z počátku potýkaly, zejména při nastavení zaslání dávek dat.

Údaje se do ISoSS mohou zadávat 3 způsoby: přímo, nebo posílat dávkou přes Portál ISoSS, nebo s využitím webových služeb při napojení personálních systémů úřadů na ISoSS. Je potěšující, že se stále zvyšuje počet úřadů, které zasílají data dávkou, a to s využitím webových služeb. Dosud bylo zasláno 11 872 dávkových souborů, z toho 1 293 poslaných přes Portál ISoSS a 10 579 přes webové služby.

V současné době zasílá do rejstříku státních zaměstnanců 39 služebních úřadů dávkové soubory přes Portál a 52 služebních úřadů odesílá dávkové soubory přes webové služby. Jako první se se svým personálním systémem



Základní architektura aplikací IS o státní službě

napojilo Ministerstvo vnitra, které celý systém testovalo, a velmi rychle následovala Česká správa sociálního zabezpečení, Archiv bezpečnostních složek a Ministerstvo financí.

Modul evidence obsazovaných služebních míst, který rovněž umožňuje dávkové zasílání dat, je dosud využíván formou přímé editace dat v Portálu ISOSS, ale řada úřadů již zasílání dávek testuje. Zbývající dva moduly lze obsluhovat pouze prostřednictvím Portálu ISOSS.

Aktuální využití

Vedle každodenní komunikace s uživateli pořádá Ministerstvo vnitra workshopy pro zástupce úřadů i firem, které spravují personální systémy služebních úřadů, a také tematicky zaměřené konzultační dny. ISOSS vychází ze zcela nové právní úpravy, proto také Ministerstvo průběžně reaguje na podněty úřadů a poznatky z praxe a systém dále zlepšuje a vyvíjí další služby pro uživatele.

Využití ISOSS je nejvíce patrné v následujících číslech.

K 1. 3. 2016 je v ISOSS evidováno 53 033 státních zaměstnanců.

V roce 2015 se konalo 15 úřednických zkoušek, při kterých vykonalo obecnou část úřednické zkoušky 323 osob. Pro období leden až březen 2016 bylo vypsáno již 172 termínů úřednických zkoušek a jen v lednu a únoru konalo úřednickou zkoušku 1 325 osob.

V evidenci provedených úřednických zkoušek, která obsahuje i údaje o úřednických zkouškách uznaných na základě zákona, je evidováno na 47 000 záznamů.

V evidenci obsazovaných služebních míst je dosud evidováno 4 300 výběrových řízení.

Rozvoj ISOSS

Druhá etapa ISOSS, která byla zahájena v letošním roce, se věnuje vytvoření nového modulu pro systemizaci služebních úřadů a dalšímu rozvoji stávajících modulů. Modul systemizace bude spuštěn od 1. 7. 2016 prozatím pilotně pro tvorbu návrhu systemizace na rok 2017.

Ing. Kateřina Vojtková, MPA,
sekce pro státní službu, MV ČR

ISoSS je plně funkční, ale můžeme jej rozvíjet

Od září 2015 je v provozu a plně funkční Informační systém o státní službě (ISoSS). Půl roku je tedy dostatečná doba na to hodnotit, jak systém funguje, jak je využíván, případně v čem je dobré jej vylepšit. Ptali jsme se osoby nejpovolanější – náměstkyně ministra vnitra pro státní službu RNDr. Josefa Postráneckého – a zajímalo nás, mimo jiné, jestli je možné celý ISoSS považovat za jakýsi personální systém veřejné správy?



Ano, zjednodušeně se systém dá takto vysvětlit. Informační systém o státní službě, který je definován přímo služebním zákonem, může považovat za jeden z klíčových nástrojů pro řízení státní služby a to speciálně v oblas-

ti lidských zdrojů. Služební zákon stanovuje čtyři stěžejní funkcionality tohoto systému. Tou asi nejrozsáhlejší je **informační systém o státních zaměstnancích**. Druhou funkcionalitou je **evidence obsazovaných služebních míst**, již se vyhláší výběrová řízení na obsazení buď volných míst, nebo nyní při náběhu zákona na tzv. „přesoutěžení“ vedoucích zaměstnanců. Zbývající dvě funkcionality jsou pak vázány na oblast vzdělávání úředníků. Jedná se o **evidenci úřednických zkoušek**, která umožňuje jak úředníkům, tak občanům přihlásit se na úřednickou zkoušku v daném oboru státní služby a následně jejich výsledky evidovat.

Hovoříte nejen o úřednících, ale rovněž o občanech. ISoSS není tedy určen výhradně pro státní správu?

Samotný ISoSS je z principu rozdělen na dvě části, přičemž jedna je neveřejná – úřední a druhá je skutečně veřejná, tedy přístupná všem. Jedná se například o informace o volných služebních místech, vyhlášených výběrových řízeních a nárocích na ně. Systém také umožňuje přihlásit se do příslušného výběrového řízení na obsazení volného služebního místa a rovněž přihlásit se ke slo-

žení příslušné úřednické zkoušky. To je důležité v případě, že občané uvažují o tom, že by se chtěli o konkrétní místo ucházet a mohou si tak s předstihem udělat zkoušku nezbytnou pro výkon státní služby.

Co vlastně ISoSS obsahuje, aby splnil vše, co od něj požadujeme?

Systém bude obsahovat informace o **všech** státních zaměstnancích, kteří jimi jsou **dle služebního zákona**. V současné době probíhalo „překlápění“ dosavadních úředníků pod režim zákona o státní službě, proto systém ještě neobsahuje údaje o všech. K dnešnímu datu (polovina února 2016) jsou v ISoSS informace o 52 000 státních zaměstnanců z těch necelých 70 000 úředníků, kteří spadají pod státní službu. Zbývá nám tedy ještě doplnit chybějící údaje, ale systém obsahuje již většinu potřebných dat.

Naplňování ISoSS daty vyžadovalo spolupráci s řadou institucí. Probíhala bezchybně, nebo se vyskytovaly nějaké komunikační problémy?

Poskytnutí potřebných dat je povinností, která vyplývá ze služebního zákona. Znamená to, že jsme na úřady nijak v tomto směru tlačit nemuseli. Je pochopitelné, že někdy nastávají určité technické problémy, ale nejedná se o nic zásadního. Je dobré upřesnit, jak se data o státních zaměstnancích do informačního systému dostávají. Jsou možné dva způsoby. Jednak prostřednictvím vlastního portálu tohoto informačního systému, kdy úřady v dávkách za určitou skupinu státních zaměstnanců potřebná data do ISoSS vkládají. Mohou ovšem rovněž využít

webových služeb. V takovém případě napojí svůj dosavadní systém s informacemi o svých úřednících na ISoSS a touto cestou zmiňovaná data přenesou do nového informačního systému.

Rád bych upozornil, že i když zákon ukládal MV ČR vytvoření ISoSS do dvou let od účinnosti zákona, bylo přijato rozhodnutí, že jej vybudujeme už k 1. 7. 2015, tedy do doby, kdy bylo zahájeno překlápění podstatné části státních úředníků pod služební zákon. Šlo nám především o to, aby se nemusela připravovat nějaká přechodná řešení k jejich evidenci. Znamená to, že za půl roku jsme připravili s kolegy ze sekce komunikačních a informačních technologií MV ČR a odštěpného závodu ČP, kteří měli na starosti technické řešení, systém tak, aby jeho fungování nabíhalo postupně od 1. 7. 2015. Od září loňského roku je pak plně funkční a přístupný příslušným úřadům.

System je k dispozici již půl roku, je tedy možné hodnotit, jak pravidelně je využíván, případně s jakou očekávanou intenzitou?

Neveřejná část, která je určena pouze úřadům a slouží jejich potřebám v personální oblasti, je využívána v souladu se zákonem a řekl bych poměrně aktivně.

Pokud jde o veřejnou část, jak bylo již řečeno, je možné se jejím prostřednictvím hlásit na úřednické zkoušky. Do této chvíle bylo vypsané více jak 100 termínů úřednických zkoušek, na které se přihlásilo a zkoušku složilo kolem 1000 osob. Náběh systému je postupný, ale z našeho pohledu je podstatné, že všechny čtyři funkcionality plně běží.

ISoSS tedy splnil Vaše očekávání, nebo máte pocit, že je potřeba například přidat nějakou funkcionality?

Naším úkolem bylo zabezpečit funkčnost oněch čtyř funkcionalit, které předpokládá přímo zákon. Vnímáme však tento systém skutečně jako určitý nástroj pro řízení celé státní služby. Proto pro jeho rozvoj v letošním roce připravujeme některé doplňkové funkcionality, které více umožní

jeho provázání například s přípravou systemizace. Ta je dalším klíčovým nástrojem státní služby, kterým se zabezpečuje její organizační a personální chod. Systemizaci schvaluje vláda vždy koncem roku na příští rok a rozděluje počty služebních (a rovněž i pracovních) míst mezi jednotlivé úřady. Obsahuje rozdělení na představené, tedy vedoucí zaměstnance, řadové zaměstnance a další strukturální charakteristiky. Pro toto rozdělování by ISoSS měl poskytnout veškeré potřebné údaje, abychom například některé kroky nečinili dvakrát atp. Protože v rámci státní služby je nutné plánovat rozvoj lidských zdrojů, například s ohledem na věkovou strukturu, úroveň a typ jejich vzdělání, bude ISoSS získávat stále větší důležitost. Naši úlohu pro nejbližší dobu tedy vidíme v jeho rozvoji. Může se totiž stát, že některému úřadu v rámci státní služby hrozí „zestárnutí“ úředníků a bude potřeba včas připravit generační obměnu. Zatím u nás takové signály nemáme, ale v zahraničí už tyto situace nastávají, a pokud nejsou včas identifikovány, pak příslušný úřad stojí před výraznou obměnou svých zaměstnanců, aniž by na to byl včas připraven. ISoSS by tedy měl pomoci plánovat lidské zdroje ve státní službě a právě k tomu bude směřovat i jeho další rozvoj.

Model, který jsme použili, je čistě naším nápadem, nebo jste přejímali zkušenosti ze zahraničí?

Pokud se podíváme, jak fungují obdobné IS o státních úřednících v jiných státech, tak náš systém je velmi podobný. Obsahuje všechny nezbytné údaje o úřednících tak, jako kdekoli jinde. To co nebývá vždy pravidlem, ale rozhodně je přínosné, je právě možnost hlásit se prostřednictvím tohoto systému například na vykonání úřednických zkoušek. Systém ISoSS tedy nejen dává přehled o personálním stavu státní služby, ale rovněž usnadňuje její řízení a rozvoj.

-MJ-

Nabíý sál sleduje slavnostní zahájení ISSS 2015



Co přinese další ročník konference ISSS?

Ve dnech 4.–5. dubna 2016 se v kongresovém centru Aldis v Hradci Králové uskuteční již 19. ročník renomované konference zaměřené na reformu veřejné správy, rozvoj e-governmentu a informatizaci společnosti, tradičně doprovázený visegrádkou konferencí V4DIS (Visegrad Four for Developing Information Society). V posledních letech se na akci pravidelně registruje více než 2300 hostů, během programu proběhne zhruba 200 přednášek a diskusí a ve výstavní části se představí přes sto dodavatelů technologií a služeb.

Akce se každoročně koná pod oficiální záštitou několika členů vlády ČR, včetně premiéra, místopředsedů obou komor Parlamentu a Asociace krajů ČR. Mezi aktivními účastníky se vedle stovek zástupců veřejné správy, odborníků i zástupců dodavatelů technologií a služeb objeví i letos řada vrcholných politiků, náměstků ministerstev, hejtmanů, primátorů, šéfů státních organizací, zástupců obou komor Parlamentu ČR i desítky zahraničních návštěvníků. Nebudou chybět ani hosté z Bruselu – osobní účast potvrdila eurokomisařka Věra Jourová, delegace členských zemí Visegrádky čtyřky a řada dalších osobností. Letos se zde díky dlouhodobé spolupráci s Krajem Vysočina prezentuje i delegace tchajwanských dodavatelů do segmentu veřejné správy, a to pod hlavičkou státní agentury pro podporu podnikání a investic TAITRA.

Nabíý dvoudenní program

Nadcházející ročník určitě nebude nudný. Kromě tradičního hodnocení aktuálního stavu informatizace na národní i evropské úrovni, zdůraznění co největší transparentnosti veřejné správy nebo otázek spojených s financováním

ICT projektů proběhnou i tradiční odborné bloky věnované GISům, e-health nebo kybernetické bezpečnosti. Asi nejvíce se ale bude probírat elektronická identita, unijní směrnice eIDAS, úplné elektronické podání a poskytování důvěryhodných elektronických služeb. Přítomnost eurokomisařky Věry Jourové určitě vynese do popředí také unijní vizi jednotného digitálního trhu. Program ovlivní i fakt, že v posledních měsících výrazně roste zájem o záležitosti



Výkonný ředitel konference RNDr. Tomáš Renčín je u akce od samotného začátku



Součástí programu pondělního galavečera je i slavnostní vyhlášení soutěže Zlatý erb

ti spojené s „internetem věcí“ – v souvislosti s tím tak posílí blok věnovaný konceptu „smart cities“ a nejnovějším trendům v komunikaci státu, samospráv, občanů i dodavatelů služeb.

Kterým směrem v příštích letech?

Slovy dlouholetého programového ředitele ISSS Vojtěcha Dvořáčka „zkoušet si hrát na vizionáře je úloha těžká a nevděčná a je rozhodně lepší se do větších spekulací nepouštět“. Z programu posledních ročníků lze však vypozařovat stále větší důraz na mobilitu úředníka, propojení občana s úřadem, ale i využití machine-to-machine komunikace v rámci správy věcí veřejných. Následující ročníky v tom budou určitě pokračovat, spousta otevřených otázek zatím stále zůstává okolo dalšího rozvoje cloudových řešení.

Pro příznivce moderního e-governmentu mají pořadatelé přece jen jednu dobrou zprávu. S účastí na jubilejním dvacátém ročníku v příštím roce předběžně počítá místopředseda Evropské komise a tvůrce estonského elektronického zázraku Andrus Ansip. Uvidíme, zda jeho případná přítomnost na konferenci podníká větší snahu o rychlejší dotažení některých projektů na domácí scéně. Jedním z největších problémů je totiž přetrvávající setrvačnost v přijímání nových trendů a technologií ze strany veřejné správy a zájmy jednotlivých resortů, které jsou většinou nadřazený zájmům občanů.

Bez partnerů a spolupracovníků by to nešlo

Konference ISSS, jejíž první ročník se uskutečnil v roce 1998 v Praze a již od následujícího roku pravidelně hostí Hradec Králové, je již řadu let samozřejmou součástí programu všech, kdo se podílejí na reformě a informatizaci veřejné správy – ať už jde o politiky, pracovníky státních orgánů či zástupce samospráv nebo odborníky, kteří se informatizaci veřejné správy profesně věnují. Na přípravě programu i na organizaci akce se zpravidla podílí vedle Ministerstva vnitra ČR několik dalších resortů, Kraj Vysočina, asociace, svazy a profesní sdružení a řada dalších subjektů. Významnou roli hraje i hostitelské město Hradec Králové, fond Regina a partneři konference v čele s Českou spořitelnou.

Celá rozsáhlá akce je v posledních letech stále vyhledávanější příležitostí také pro prezentaci firmy, produktů a služeb či úspěšných projektů. Účastníci konference se stávají aktivní součástí procesu, v němž se představují klíčové novinky a strategie v oblasti e-governmentu a kde se zároveň tvoří, diskutují a často i schvalují další postupy.

Více informací včetně kompletního archivu minulých ročníků lze najít na www.issc.cz.

Agendový systém – nezbytnost

Vize úplného elektronického podání nemůže být naplněna bez fungujícího integrovaného systému podporujícího výkon agend. Samotné pěkné inteligentní formuláře a graficky vyšperkovaný portál občana zajistí jen vstup nových podání, ale nikoli poskytování průběžných informací o stavu podání či o dlouhodobých vztazích občana s organizací. Nemluvě o efektivitě zpracování podání uvnitř organizace.

Úplné elektronické podání má zajistit elektronické vyřízení životní situace a poskytnout přehled o řešených životních situacích, ať již byly realizovány čistě elektronickou cestou, nebo dnes obvyklou cestou fyzického dokumentu či osobním podáním.

Téma úplného elektronického podání zahrnuje:

- vstup elektronického podání (dokumentu) prostřednictvím formuláře nebo i bez něho;
- promítnutí dat z podání do odpovídající agendy bez jejich přepisování „automaticky“;
- průběžné automatické poskytování informací občanovi (obecně podatelí) o stavu vyřizování podání;
- informace o vyřízení podání občanovi.

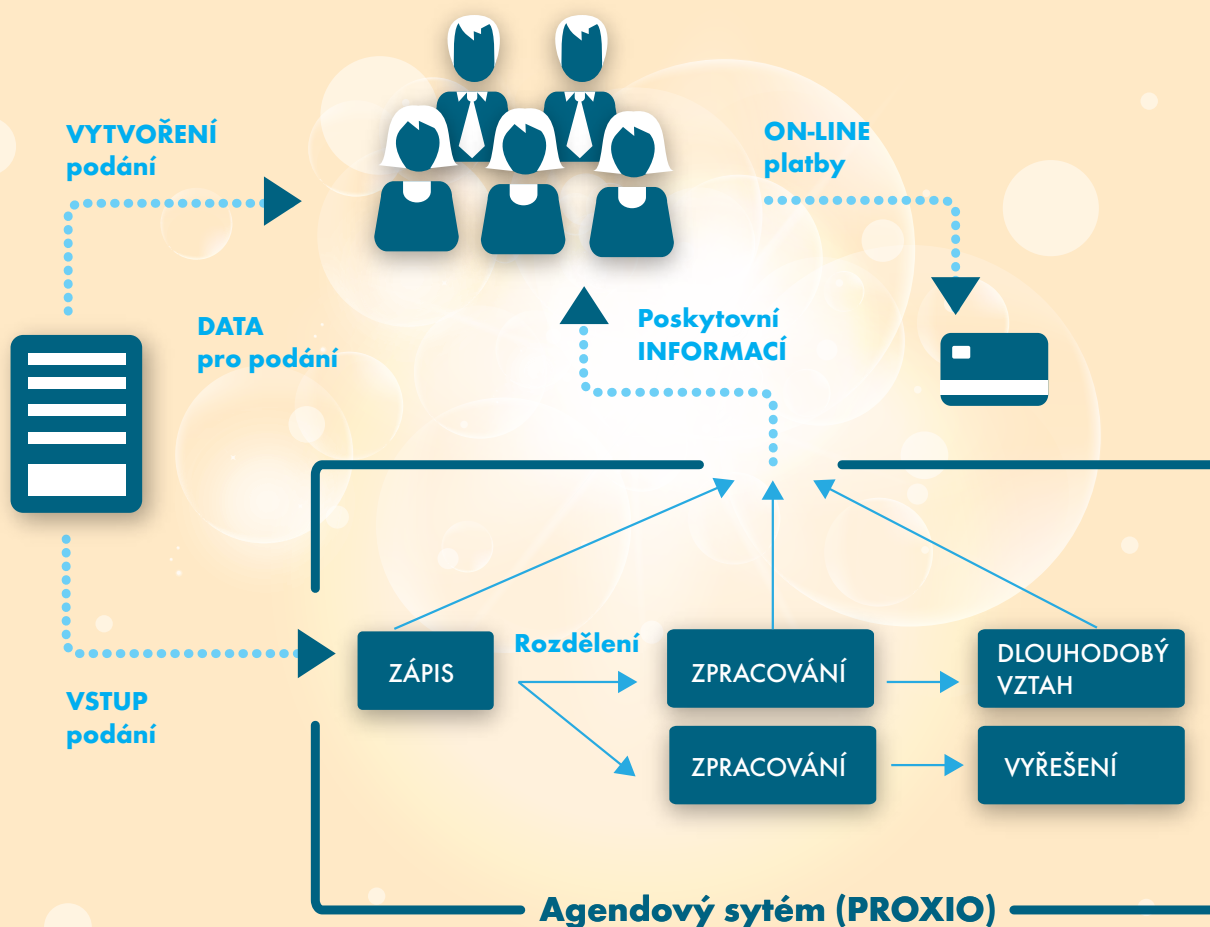
Celý mechanismus úplného elektronického podání musí mít oporu především v jednoznačné a bezpečné identifikaci občana a zpracování takového podání pak v celostátním sdíleném datovém fondu, stojícím zejména na datech základních registrů a propojených agendových systémech (např. AISC, AISEO, ISKN) a samozřejmě také na vlastním datovém fondu organizace.

Zajištění **vstupu elektronického podání** začíná u přesného a aktuálního popisu životních situací a musí být podpořeno odpovídajícím formulářem. Formuláře podání, kterým se zahajuje životní situace a vzniká „vztah“ občana s organizací, si mohou vystačit bez dat agendového systému. Formuláře podání, kterým se doplňuje nebo mění již probíhající životní situace nebo existující vztah občana s organizací, jsou však na datech agendového systému silně závislé.

Co je mi jako občanovi platné, že mohu např. požádat o změnu nádoby na komunální odpad nebo o četnost jejího svozu, když musím zadat všechny informace znovu jako při prvotním podání. Mnohem raději bych jen upravil existující vztah ve formuláři, ve kterém je stávající nádoba a četnost svozu již vyplněna.

Data z podání učiněného prostřednictvím formuláře by měla být automaticky promítnuta do agendového systému pro zpracování v příslušné agendě nebo agendách. V případě komplexních podání zajistí agendový systém jejich rozdělení do příslušných agend. Tím dojde ke zjednodušení vstupu a zmenší se i riziko chyb při přepisu dat ze vstupních podkladů. Zvýší se také efektivita zpracování podání na straně organizace.

Elektronizace zpracování podání v agendovém systému umožní **průběžné poskytování informací z agendového systému** občanovi o průběhu a výsledku zpracování podání, a to nezávisle na vystavovaných dokumentech a dlouhodobě. Dlouhodobé poskytování aktuálních informací je důležité zejména pro déletrvající vztahy občana s organizací, např. v agendách místních poplatků či nájemních vztahů. Lze tak na portálu města např. upozorňovat na splatnost poplatku s možností přímé platby. Nezávislost poskytovaných informací na vystavovaných dokumentech umožní jemněji členit proces zpracování životní situace občana a informovat i o změnách procesu, při kterých žádný dokument nevzniká. Poskytované informace jsou důvěrné a musí být poskytovány adresně pouze občanovi (subjektu), jehož se týká, a to bez ohledu na způsob jejich poskytování.



Nesmírně důležité je zde hledisko automatizace poskytování informací, která zajistí správnost, důvěryhodnost a včasnost informací a nezpůsobí zvýšení pracnosti zpracování agendy.

Agendový systém PROXIO umožňuje automatický vstup dat z formuláře nezávisle na použitém formulářovém systému. Formulář může pocházet z interního formulářového systému PROXIO nebo z jiných systémů, jako je Adobe LiveCycle či formuláře Software602. PROXIO podporuje různé formy poskytování informací a upozorňování nezávisle na použitém portálovém řešení.

Nezbytnou podmínkou pro drtivou většinu podání je jednoznačná a bezpečná identifikace občana, podatele, tedy subjektu, který podání provedl. Stejně tak je bezpečná identifikace nezbytná pro poskytování důvěrných informací adresně konkrétnímu občanovi. Systém PRO-

XIO obsahuje nástroje pro jednoznačné provázání občana s „jeho daty“ v systému, ať již tato data vznikla z elektronického podání nebo jiným způsobem (například již aktuálně v systému existují).

Téma úplného elektronického podání je komplexní a není možné podcenit žádnou jeho část. Velmi pravděpodobně nedojde k podcenění významu formulářů jako nositelů podání, ale snadno může být podceněn význam agendového informačního systému. Ten je přitom pro úspěch tohoto tématu zcela zásadní.

Máte své uživatele pod kontrolou?

NEWPS.CZ

Správa identit a kontrola přístupů.