

Egovernment
elektronizace veřejné správy



**DOSÁHNEME UŽ
NA PLODY
ELEKTRONIZACE?**

MŮŽEME SI UŽ UTRHNOUT PLODY STROMU ELEKTRONIZACE?

Před půl rokem jsme v Mikulově na konferenci e-government 20:10 hovořili o posunu České republiky v oblasti elektronizace veřejné správy. Po dlouhé době jsme totiž zaznamenali v rámci některých mezinárodních srovnání výraznější změnu našeho umístění. Tedy výraznější změnu pozitivním směrem. A tak jsme využili příležitosti a ptali se přítomných odpovědných, zda se jedná o nahodilou událost, nebo jest oprávněné se domnívat, že by to mohl být již stálý trend. Všichni se radostně shodovali na tom, že se jedná o trend, který je výsledkem legislativních změn, které zde proběhly, i realizace konkrétních projektů. Tedy, že nyní již bude Česká republika bezpochyby jen stoupat.

Podle tohoto předpokladu bychom měli být tedy letos o něco výše než loni. Z mezinárodního hodnocení se to nedozvíme, to se realizuje ve dvouletých cyklech, a tak jsme se pokusili sami zamyslet nad tím, co vše máme k dispozici a čeho jsme dosáhli. Zda jsme se po „šprušlích“ legislativy a veřejných projektů vyšplhali tak vysoko, že můžeme sklízet plody, které elektronizace nabízí. Tedy užívat si efektivitu i pohodlí, které se s elektronickou veřejnou správou pojí.

Na následujících stránkách se proto věnujeme především dvěma základním „kamenům“, které jsme si opracovali a připravili na tento rok. Bankovní identitě a Katalogu služeb. Bankovní identita je dlouhodobě vyhlížena jako spasitelka, která nastartuje zájem klientů o nabídku služeb veřejné správy v elektronické podobě, neboť jim bude nabízet vlastně bezpracnou cestu k těmto službám. Katalog služeb pak navazuje, neboť má takto novým klientům ukázat pestrou paletu veřejných služeb, které mohu nyní, díky své elektronické identitě u vlastní banky, čerpat.

Po pravdě, ten žebřík, na kterém stojíme, když se snažíme dosáhnout na plody stromu elektronizace alespoň na těch spodních větvích, je trochu rozviklaný. Některé „šprušle“ jsou lehce naprasklé, sem tam nějaká chybí. Dá se tam vylézt, ne, že ne, ale je to trochu adrenalin. Bankovní identita tu je, to ano. Ale ještě ne u všech bank a překvapivě neumožňuje kontakt s celou veřejnou správou. Katalog služeb se pomalu plní. Tedy pomalu. A s popisy jednotlivých služeb je to ještě pomalejší.

Ale jak bylo řečeno, stojíce na špičkách, lehce balancující na nejistém žebříku, když se hodně natáhneme, na některé z těch plodů skutečně dosáhneme. I proto se v tomto čísle magazínu Egovernment dočtete o digitalizaci stavebního řízení, digitálním úřadu, elektronických podpisech a dalších tématech, díky kterým se ten žebřík stává pevnějším a stabilnějším.

Michal Jirkovský,
šéfredaktor

Redakce	ÚVODNÍ SLOVO	2
	OBSAH, TIRÁŽ	3

IDENTITA	4-7
JEŠTĚ NENAPLNĚNÝ KATALOG SLUŽEB VS	8-9
ELEKTRONICKÉ SLUŽBY V ČESKÉ REPUBLICE	10-11
POUŽÍVÁNÍ RŮZNÝCH TYPŮ ELEKTRONICKÝCH PODPISŮ	12-13
CESTA K ÚSPORÁM BEZ STAVEBNÍCH ÚPRAV	14-15
DIGITÁLNÍ ÚŘAD	16-18
DIGITALIZACE STAVEBNÍHO ŘÍZENÍ	20-21
KYBERNETICKÁ BEZPEČNOST V ROCE 2021	22-23
OTEVŘENÉ FORMÁLNÍ NORMY	24-25
ZONER SOFTWARE, A. S.	26-27

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
twitter: @EgovernmentMag
facebook: @EgovernmentMagazin

Šéfredaktor: Ing. Michal Jirkovský**Korektorka:** PhDr. Helena Veverková**Asistentka:** Kateřina Alexová**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

ISSN 1801-9420

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 **300 Kč** bez DPH/**výtisk, tj. 900 Kč** bez DPH **ročně**.

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



IDENTITA

Každý z nás máme svoji vlastní identitu, kterou se prokazujeme a považujeme to za něco naprosto samozřejmého. Z počátku se mohlo zdát, že je naprosto samozřejmé, a možná i triviální, její překlopení do digitálního světa, tedy že je naprosto samozřejmé, že tutéž identitu budeme vykazovat v rámci kyberprostoru. Ale ukázalo se, že to není tak triviální, že proces jejího překlopení je skutečně poněkud složitější. Řada věcí se postupně odladila a dnes patříme mez státy, jejichž občané se mohou, v zásadě bez větších problémů, prokazovat a identifikovat elektronicky. Díky tomu mohou čerpat elektronické služby od státu i soukromých subjektů. Pravda, jsou státy, kde to šlo i rychleji, ale jsou také naopak státy, kde to jde daleko hůře, nebo vůbec. Jak tedy na to?

KROK PRVNÍ – ZŘÍZENÍ IDENTITY

Elektronickou identitu nezískáváme automaticky, i když se i o tom uvažuje. Musíme si ji zajistit, požádat o ni. A to je, nebo by podle představ architektů z MV měl být, také poslední moment, kdy někam musíme osobně.

Musíte si vytvořit **profil** v tzv. **národním bodu** (<https://www.eidentita.cz/Home>). Aby se tak stalo, musí **kvalifikovaný správce** (tedy nějaký člověk v roli úředníka) ověřit Vaši totožnost a vytvořit Váš **identifikační prostředek** (kartu, USB klíč, kódy). Zvolit si můžete některý z produktů státu, nebo můžete vybírat z nabídky soukromých firem.

NABÍDKA STÁTU

- Založit si **eOP**, tzn. zajít na obecní úřad nechat si vydat elektronický občanský průkaz s čipem a nechat si aktivovat jeho elektronické funkce. Při tomto procesu jste identifikováni, bude Vám zřízen profil v národním bodu a získáte identifikační prostředek, kterým je eOP (navíc

prostředek s úrovní záruky vysoká – bude popsáno dále).

- Založit si **NIA ID**. Jedná se o identifikační prostředek, který sestává z kombinace jméno+heslo+SMS (tedy varianty, kdy svoji identitu budete prokazovat vepsáním jména a hesla do přihlašovacího formuláře (<https://www.eidentita.cz/ProfileRegistration>) a následným doplněním zaslaného jednorázového kódu prostřednictvím SMS). Zažádat si o založení NIA ID můžete prostřednictvím formuláře, který odnesete na Czech POINT, kde také proběhne ověření – ztotožnění. Následně je prostředek aktivován – výstupem budou příslušné údaje – hesla.
- **Mobilní klíč e-governmentu** je cílovým a nejmodernějším prostředkem. Jedná se o aplikaci pro mobilní telefony a tablety poskytovanou zdarma státem, která umožňuje přihlašování k elektronickým službám státu bez nutnosti čtečky čipových karet i bez zadávání dalších

ověřovacích kódů. Aplikaci si můžete stáhnout i před tím, než založíte svůj profil v národním bodu, a naopak jejím prostřednictvím o tento krok požádat (následuje uvedená návštěva Czech POINTu pro ověření).

A NEMUSÍ TO BÝT STÁTNÍ!

Může se ale stát, že již delší dobu používáte prostředky, které nabízejí soukromoprávní poskytovatelé a které jsou nyní použitelné i pro přístup ke službám státu. V tom případě není nutné, abyste si pořizovali „státní“ identifikační prostředky. Týká se to těch, kteří využívají:

- Čipovou kartu **Starcos** od I.CA – využívá se spíše jako „podniková“ karta (většinou k identifikaci pracovníků při přístupu ke konkrétnímu systému), ale jako identifikační prostředek je velmi dobře použitelná, navíc s úrovní záruky vysoká;
- FIDO klíč **MojeID** od sdružení CZ.NIC – služba, která už delší dobu umožňuje zřízení a správu elektronické identity – účet MojeID. Nyní je tato služba použitelná i ve vztahu k veřejné správě, díky bezpečnostnímu klíči (buď v **softwarové podobě** integrované s operačním systémem Windows 10 a Android 7+, nebo **hardwarové podobě** připojitelné k počítači přes USB a k mobilnímu telefonu přes NFC), Samozřejmě i zde je nutné ztotožnění (realizovatelné na Czech POINTu, nebo s využitím datových schránek či jiného existujícího elektronického prostředku);
- **bankovní identita** – pokud používáte elektronické bankovníctví, můžete nyní prostřednictvím svých přístupových údajů (hesel nebo klíčů) využívat i elektronických služeb státu. Klienti většiny bank obdrží e-mail informující o tom, že jim byl přístup do bankovníctví registrován jako identitní prostředek a mohou jej začít používat. V minoritním počtu bank je pak potřeba o zřízení prostředku banku požádat.

PRO KTEROU VARIANTU SE ROZHODNOUT

Zdá se, že chceme-li si zřídit elektronickou identitu, máme k dispozici širokou nabídku. Jak z ní tedy vybírat?

1. POHLED CENY

Jedním z hlavních pohledů by mohly být pořizovací náklady.

První pořízení a aktivace eOP jsou zdarma (platí se pouze při vydání nového eOP z důvodů ztráty, poškození či změny údajů na předchozím), nicméně je nutné počítat s dokoupením čtečky karet. Jedná se o jednoduché zařízení, které se k počítači připojí pomocí USB kabelu. Jeho cena se pohybuje mezi 150 až 200 Kč. Další prostředky státu (NIA ID, Mobilní klíč eG) jsou zdarma. Ze soukromoprávních prostředků je zdarma bankovní identita a za určitých okolností (viz dále) můžete zdarma získat i klíč MojeID. Přímou placenou je pouze karta Starcos od I.CA (cca 600 Kč).

Z uvedeného vyplývá, že cena nebude zřejmě tím nejzávažnějším kritériem.

2. SNADNOST NASAZENÍ – POUŽITÍ

Možná daleko důležitějším kritériem bude snadnost nasazení, respektive rychlost použití. V tomto směru je asi nejvíce těžkopádný **elektronický občanský průkaz**, jakkoliv je spolu s kartou Starcos výjimečně bezpečný, což je dáno mimo jiné i nutností použít čtečku čipových karet. Pro použití „v terénu“ mimo domov tedy musíme dopředu myslet na její přibalení, což není vždy příjemné, navíc použití na cizím počítači není doporučeno vůbec.

NIA ID je v tomto smyslu pohodlné, neboť nepotřebujete další externí zařízení (telefon předpokládáme, že má každý automaticky u sebe), ale musíte si pamatovat své jméno a heslo a ještě musíte opsat dlouhý kód z SMS.

V případě **Mobilního klíčeEG** stačí jediný kód pro přístup do aplikace a i ten je možné nahradit otiskem prstu či rozpoznáním Vašeho obličeje. Podmínkou pro jeho používání je pouze vlastnit chytrý mobilní telefon. Aplikace je k dispozici zdarma a pracuje rychle a spolehlivě.

Karty Starcos, podobně jako elektronického občanského průkazu, se týká nutnost vlastnit čtečku, stejně jako vlastnost nejvyšší bezpečnosti.

MojelID nabízí dvě různé možnosti:

- **Systémový softwarový FIDO klíč** v MojelID využívá přímo vlastností operačního systému. Pokud se například přihlašujete do Windows 10 pomocí systému Hello (PIN, otisk prstu nebo obličeje), nepotřebujete žádné další zařízení a můžete toto přihlášení spojit s účtem MojelID a přihlašovat se jím ke službám státu. Totéž platí pro interní klíč v platformě Android.
- **USB/NFC klíč MojelID** je dodatečné hardwarové zařízení, které je nutné k počítači připojit. Jedná se o další prvek, který nesmím doma zapomenout, pokud se chci připojit „kdekoliv“. Jeho velikost ale skutečně umožňuje zavěšení například na klíče, a tedy jej mít automaticky vždy s sebou. Navíc platí, na rozdíl od mobilní telefonu, že nemusíte hlídat jeho nabití.

Bankovní identita je nastavena v rámci našeho elektronického bankovníctví ve většině případů prostřednictvím aplikace elektronického klíče na mobilním telefonu.

Hodně se hovořilo o rychlosti přihlášení. Na sociálních sítích bylo diskutováno porovnání, respektive rozdíl doby, kterou trvá přihlášení klíčem MojelID a eOP. Tento časový rozdíl byl až 40 s, což by v případě opakování tohoto kroku konkrétní osobou mohlo znamenat během pracovní doby značnou časovou prodlevu. Doposud nebylo toto srovnání na místě s ohledem na rozdílné úrovně záruky obou prostředků. Od 10. 3. 2021 získala i služba MojelID akreditaci na úroveň vysoká, bude tedy jistě možné v brzké době používat některé klíče i pro požadavky s vysokou úrovní záruky. V tomto případě bude například nutné zadávat PIN, i tak však lze předpokládat, že se rychlost přihlášení příliš nezmění.

Více než rychlost nasazení bych možná hodnotil srozumitelnost informací, které je možné k jednotlivým prostředkům dohledat (z pohledu neznalé osoby). A zde státní prostředky proti komerčním skutečně pokulhávají. Jazyk, kterým jsou na internetu informace předkládány,

se stále drží jakési těžkopádné, úřednické verze. I když se v poslední době objevují videonávody, které se snaží tento deficit smazat.

3. MOŽNOSTI – SCHOPNOSTI

V této oblasti panují mezi jednotlivými prostředky patrně největší rozdíly. Veškeré prostředky elektronické identity se označují tzv. úrovní záruky, kterou poskytují. Podle té se liší i jejich využitelnost. Existují tři úrovně – **vysoká**, značná a nízká. Úroveň vysoká doposud nabízel **pouze elektronický občanský průkaz**, nebo karta **Starcos**. Jak již bylo uvedeno, 10. 3. 2021 akreditaci na úroveň vysoká získala i služba MojelID, a proto lze ve velmi krátké době očekávat nabídku nového (jiného než dosavadního) USB klíče s touto úrovní záruky. Všechny ostatní prostředky mají úroveň značná.

Co to znamená, respektive kdy a na co potřebuji vysokou úroveň a na co stačí značná? Většina agend, které chceme s veřejnou správou řešit elektronicky, vyžaduje identifikaci pomocí prostředků minimálně na úrovni značná. Dá se ale předpokládat, že v budoucnu se objeví i několik takových, ke kterým bude možné přistoupit pouze se zabezpečením vysoká. Konkrétní požadovaná úroveň pro konkrétní agendu není, až na několik výjimek, stanovena přímo zákonem, ale bude uvedena v Katalogu služeb, který je k dispozici od letošního roku a který bude každoročně aktualizován. V případě, že v katalogu není u dané agendy požadovaná konkrétní úroveň záruky uvedena, automaticky to znamená úroveň značnou.

Větší problém než úroveň záruky je však „dosah“ prostředku. Státní identitní prostředky jsou v tomto okamžiku využitelné **pouze pro služby státu**. To znamená, že například pomocí Mobilního klíče eGovernmentu nenakoupíte v e-shopu, nebudete moci komunikovat s dodavatelem energie atp., ale můžete využít všech služeb, které stát nabízí elektronicky. Samozřejmě o jejich šíři je možné diskutovat, ale lze předpokládat, že nabídka se bude postupně zvětšovat. (Pro představu seznam služeb, ke kterým se můžete přihlásit elektronickými identifikačními prostředky, naleznete **ZDE**: <https://info.eidentita.cz/sep/>.) Oproti tomu komerční identitní prostředky dosáhnou jak **do státní oblasti, tak do komerční**. To znamená, že například pomocí MojelID můžete čerpat služby od státu i od e-shopů či operátorů. Specifické jsou v tomto směru banky. Bankovní identita dosáhne do soukromé části i do státní, ale v té státní jen s určitým omezením. Služby přímo poskytované státem je možné vyřídit elektronicky pomocí bankovní

identity, ale služby, které bychom mohli nazvat doplňkové (školy, nemocnice atp.), nikoliv. Pokud ale chcete navazovat **přeshraniční kontakt** a čerpat nějakou službu veřejné správy ze zahraničí, pak budete muset použít pouze eOP. Jiný prostředek zatím takovou možnost nenabízí.

CO TEDY ZVOLIT?

Jaké by mohlo být doporučení na závěr? Víte-li, že budete chtít využívat pouze služeb státu a nechcete žádné další zařízení navíc, zdá se ideální volbou **mobilní elektronický klíč**. Jedná se o rychlý způsob přihlášení, který, pokud neztratíte mobilní telefon, máte stále po ruce. Pokud se budete chtít **přihlašovat i ke službám soukromého sektoru**, pak se zdá vhodným řešením **MojeID**. **Bankovní identita** je pak volbou pro pohodlné, kteří se nechtějí zaobírat objednáváním nějakého prostředku a ztotožňováním své osoby. Naskočí Vám automaticky (záleží na podmínkách stanovených Vaší bankou), ale s výše uvedeným omezením vůči některým službám, které zajišťuje stát.

-MJ-

	eOP	NIA ID	Mobilní klíč	Starcos	MojeID	Bankovní identita
CENA	cca 200 Kč*	0	0	cca 600 Kč	0 nebo 600 Kč**	0
POUŽITÍ	čtečka	hesla	klíč	čtečka	klíč	klíč
ZÁRUKA	vysoká	značná	značná	vysoká	značná nebo vysoká***	značná
SLUŽBY	státní	státní	státní	vše	vše	téměř vše
MEZINÁRODNĚ	ano	ne	ne	ne	ne	ne

* Výměna eOP z důvodu expirace starého dokladu je zdarma.

**V případě použití softwarového klíče je cena 0 Kč. To se týká těch, kteří používají OS Windows 10. Jinak platí, že cena USB/NFC klíče, který splňuje požadavky na zabezpečení pro úroveň záruky vysoká, je zhruba 600,- Kč. Může se Vám ale stát, že v rámci propagační akce společnosti CZ.NIC získáte ten správný klíč zdarma.

***FIDO klíč MojeID byl doposud na úrovni záruky značná, 10. 3. 2021 služba MojeID získala akreditaci na úroveň vysoká. Nové klíče (FIDO2) budou tedy nabízet tuto úroveň.

Oficiální seznam prostředků elektronické identifikace je uveden na:

<https://info.eidentita.cz/KvalifikovaniSpravci.aspx>

Odpovědi MV ČR na nejčastější dotazy v souvislosti s elektronickou identitou naleznete na:

<https://info.eidentita.cz/faq/>

A konečně, jak nejrychleji můžete získat státní identitu formou mobilního elektronického klíče se můžete dozvědět na:

<https://chciidentitu.gov.cz/>

JEŠTĚ NENAPLNĚNÝ KATALOG SLUŽEB VS

Podle zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, měla vláda do 1. 2. 2021 stanovit plán digitalizace, podle kterého by nejpozději do 1. 2. 2025 byly všechny služby nastaveny tak, aby je bylo možné vyřizovat digitálně (pokud je to účelné). Mělo se tak stát na základě naplnění Katalogu služeb, který je jakousi evidencí služeb VS a slouží k inventarizaci všech služeb, které stát poskytuje klientům. Cílem Katalogu služeb VS je tedy, mimo jiné, přehledně informovat klienta o všech dostupných službách veřejné správy (VS). Spolu se zmiňovaným plánem digitalizace by tak měl být podpořen rozvoj e-governmentu.

ROZJEZD VYPADAL SLIBNĚ

Zákon sice stanovil termín pro vznik Katalogu služeb nejpozději do 1. 2. 2021, ale například ředitel odboru eGovernmentu MV ČR Roman Vrba už v září 2020 na konferenci **e-government 2010 v Mikulově** (<https://www.egovernment.cz/inpage/mikulov-2020/>) zdůraz-

nil, že takový katalog byl v podstatě již delší dobu budován, a to pod názvem Úkony na žádost. V první polovině loňského roku byly, podle jeho slov, práce na katalogu velice intenzivní, aby nic nebránilo jeho obsahovému naplňování. Stejně tak údajně běžela spolupráce s ohlašovatelí agend na jejich přípravě, především vysvětlo-

vání toho, co přesně je míněno terminologií Katalogu, co znamená služba, úkon atd. V pozdějším **rozhovoru** (<https://www.egovernment.cz/inpage/katalog-400/>) pro magazín Egovernment pak uvedl, že by byl rád, kdyby velká část evidence služeb vznikla o něco dříve, nejlépe k termínu spuštění nového Portálu veřejné správy, tedy v polovině prosince 2020. I plán digitalizace měl být podle těchto předpokladů stanoven kolem poloviny listopadu, aby bylo možné vyčíslit finanční dopady a prioritizaci vybraných služeb.

A JAKÁ JE SKUTEČNOST?

Podle informací, které nám v rámci svého vystoupení na konferenci **Bod zlomu** (<https://www.egovernment.cz/inpage/jihlava2021/>) sdělil ředitel odboru eGovernment MV ČR Roman Vrba, je Katalog služeb v současné době naplněn zhruba ze 46 %, což konkrétně znamená 171 agend z celkových 374. To nevypadá jako příliš rychlé tempo. Můžeme na to ale nahlížet pozitivně. Roman Vrba totiž přidává informaci, že nyní ještě 43 agend čeká na schválení a dalších 92 agend se upravuje dle připomínek, což by, i po jejich schválení, mělo znamenat už zhruba 70 % celkového počtu agend (ke konci března). Zároveň bylo, podle jeho slov, apelováno na ty, kteří ještě možné elektronizaci agend nevěnovali pozornost, aby tak začali činit.

PROČ JE TO DŮLEŽITÉ?

K čemu nám taková evidence služeb může být? Kromě přehledu o tom, které služby veřejná správa vlastně vykonává (kdo to dnes ví?), by tak mělo být zřejmé, které z nich jsou již vykonávány i elektronicky, které nelze vykonávat elektronicky a které lze, ale ještě tak poskytovány nejsou. A právě v jejich případě by měla vláda stanovit harmonogram jejich digitalizace tak, aby nejpozději do pěti let bylo digitalizováno 100 % těch, u kterých to možné a vhodné je. I proto poněkud zamrazilo, když v prvním harmonogramu, který na základě uvedených kroků vzešel, bylo pro letošní rok napláno-

váno digitalizovat dvě, zcela jistě velice důležité agendy: přijetí válečného veterána a pobyt nezletilé osoby. Nic víc. To nevypadá na překotně naplňování tak důležitého Katalogu.

A CO NA TO OBČAN?

Běžný občan výstup tohoto čížení zaznamená především na **Portálu veřejné správy**, kde jsou, tedy měly by být a snad i budou, postupně popisy všech elektronických služeb veřejné správy (to bude praktický výstup Katalogu služeb). S popisy je však ještě větší problém než se samotnou elektronizací služeb. Nyní je k dispozici popis pouze u 11 % z těch služeb, které jsou v Katalogu. Tedy 11 % ze 46 %, což znamená, že jako klienti veřejné správy v současné době vidíme pouze 5 % nabídky služeb (konkrétně je na gov.cz 193 popisů služeb).

DRUHÝ VÝKOP?

Ani ředitel eGovernmentu MV ČR Roman Vrba neskrýval, že situace neodpovídá očekávání. Problém především vidí ve skutečnosti, že sami gestoři agend často považují ze své strany úkol za splněný v případě, kdy příslušnou agendu je možné řešit s pomocí datové schránky. Cílem bylo však využít širšího spektra kanálů, a především pak nabídnout jejich popisy. MV ČR nyní s partnery připravuje příručku (měla by být hotova do konce dubna), která by měla vysvětlovat a navádět gestory k tomu, aby chápali, jaké typy agend jsou vhodné k umístění na portály, které na Czech POINTy atd. V polovině září bude pak následovat „druhý výkop“, kdy bude Katalog služeb znovu předložen vládě a Roman Vrba předpokládá, že evidenční část bude nyní již obsahovat 100 % agend a stejně tak věří v lepší vyznění digitalizačního plánu. Doufejme, že to tak bude a Katalog služeb bude tentokrát skutečně pozitivním tématem konference v Mikulově (7. – 8. 9. 2021).

-MJ-



Elektronické služby v České republice (otázky a odpovědi)

Elektronické služby. Toto sousloví se v sociální bublině informačních technologií rozrostlo tak, že se sem tam objeví i v místech, kde by jej člověk nečekal. Třeba ve veřejné správě. Mnohé ministerské resorty budují elektronické služby pro občany. Ministerstvo financí má portál MOJE DANĚ (přesněji z pohledu ministerstva: VAŠE DANĚ, naše radost). Ministerstvo vnitra provozuje PORTÁL OBČANA, který ale Národní kontrolní úřad alespoň za první roky provozu zcela sepsul. Prostředky vynaložené na počet občanů, kteří portál využívají, vycházejí tak, že by bylo levnější vozit občany na úřad taxíkem. Zdarma. Elektronické služby nejsou doménou jen centrálních úřadů, ale také samosprávy. Svůj portál s digitálními službami má přes 50 měst. To je opravdu hodně. Dá se však hovořit o úspěchu? Jak se vlastně využívají? To je nesmírně zajímavá otázka s jednoduchou odpovědí.

Jak se u nás elektronické služby využívají?

Nevyužívají se. Počty registrací jsou nicotné. Kdybychom prošli počty transakcí městských portálů a srovnali je s počtem transakcí elektronického obchodu na prodej mysliveckých huček z biobavlny, bude vítěz takové komparace jednoznačný. Proč tomu tak je? Protože zatímco prodejci mysliveckých huček chtějí prodat prostřednictvím elektronických služeb co možná nejvíce, četné obce se spokojí pouze s tím, že místo s elektronickými službami zbudovali. A tady veškerá snaha končí. Vydá se tisková zpráva, rozdají se ceny. Je jasné, že to nestačí na přijetí elektronických služeb občany.

Co mělo zajistit vyšší využívání elektronických služeb?

Bankovní identita. Slibujeme si od ní významný pokrok. Jednoduché, univerzální, automatizované přihlášení namísto složité NIA nebo fronty na České poště v případě získání datové schránky. Velmi komunikovanou výhodou je převod přihlášení ke službám mezi státní správou a samosprávou. Zní to krásně. Co ale bude realitou běžného dne? Myslí si někdo, že občané s tím, že získají bankovní identitu, začnou hned vyřizovat poplatek za psa elektronicky? Mohli by, kdyby o možnosti rychlé platby za psa věděli. Je docela dobře možné, že výhody bankovní identity bude spousta občanů využívat jen pro komerční aktivity - přihlášení v elektronickém obchodě, převod služeb u poskytovatelů energetických či telco služeb a podobně.

Kdo jim řekne, že stejným prostředkem mohou vyřídit novou popelnici na tříděný odpad nebo podat žádost o dotaci? Stát jede střídou kampaň na Twitteru. Některá města vytiskla letáčky. Nedostatek komunikace je zásadní riziko využívání elektronických služeb.

Co zajistí vyšší využívání elektronických služeb?

Obsah. Propagace a snaha informovat je jedním z nejdůležitějších bodů, ale **OBSAH je** zdaleka nejzávažnějším **slabým místem současných portálů občana**. Portály neumí nabídnout zásadní ulehčení komunikace s úřadem, mnoho z nich se shlédlo v úplném elektronickém podání, které je tak složité, že jej často (s nápovědou) provedou pouze zaměstnanci dodavatele či mimořádně informačně zdatní pracovníci úřadu. **Portály obsahují často až obskurní formuláře (např. žádost o poskytnutí kulturních vrstev půdy), které se doposud nikdy nepoužily a asi ani nepoužijí.** Vyhozené peníze. Proč někdo před implementací portálu neudělal analýzu nejpoužívanějších formulářů s možností jejich elektronizace? Protože takhle se to prostě dělá. Stěžejní agendou tak je vyřízení poplatků, ale to je prostě někdy málo. **Pokud budu vlastnit kamennou prodejnu s hučkami, budu moc stát o to, abych jich přes nově budovaný e-shop prodal co nejvíce.** Všechno tomu přizpůsobím. Stejně by měl přemýšlet i úřad. Udělat všechno pro to, aby elektronickou službu občanovi doručil v mašličkách, s nějakými výhodami. K elektronickému vyřízení zdarma kalendář obce. Cokoliv.

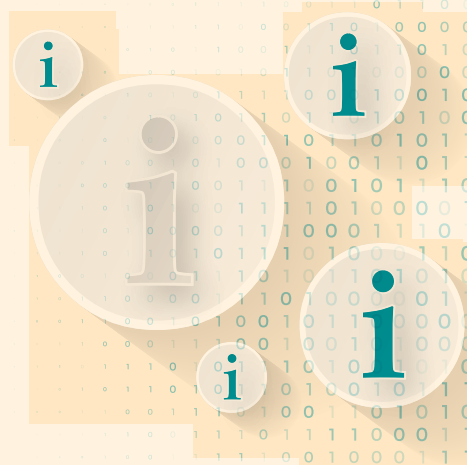
Jak začít plánovat portál občana v obci?

S rozmyslem a analýzou. Každý začátek je těžký, ale pokud je v České republice 50 portálů, tak je tu také dost inspirace, jak věci dělat i nedělat. **Velmi důležité je, zda se občanům bude líbit vizuální stránka portálu, a také to, jak rychle občan na webu města najde odkaz, který jej do portálu pustí.** Stěžejní je zapojit do přípravy odbory úřadu, kterých se nové služby mohou týkat. Jedním z prvních kroků je udělat řádnou interní analýzu nejpoužívanějších formulářů a služeb a na takových znalostech postavit návrh řešení. Společnost Marbes je často oslovována obcemi, aby poslala svou cenovou nabídku na průzkum trhu. Obsahem průzkumů jsou často funkcionality, které je třeba nacenit s vědomím, že je občané města nikdy nebudou používat. Správná cesta

vede přes rozvalu, koho a jak chci elektronickými službami oslovit. **Mnoho obcí má zpracovanou komunikační strategii, kde jsou data o obyvatelích obce, jejich preference ohledně digitální komunikace a jejich kanálů.** Ve stejném okamžiku je třeba začít plánovat propagaci portálu. Středobodem tak jsou uživatelské skupiny občanů, ke kterým je třeba doplnit to, jaké služby budou využívat a jak jim tyto služby bude obec propagovat.

Pomůže dotace z IROP?

Pomůže, pokud budou podmínky dotace napsány rozumně. Podle dosavadních informací MMR budou moci čerpat obce i kraje na spuštění svých elektronických služeb. Klíčové bude, zda způsobilými náklady budou moci být výdaje na propojení služeb portálu s agendovými systémy města. Velmi by pomohlo, kdyby část hrazených nákladů mohl beneficiant využít na propagaci služeb.



Kde rychle najít informace?

Kvalitních informací a rad není nikdy dost. **Společnost Marbes pro současné dlouhé a opakující se dny připravila malá vytrhnutí ze šedi v podobě odborných webinářů. Samozřejmě ZDARMA.** Portálu občana a zkušeností z provozu portálu se věnuje hned několik těchto kurzů. Více informací najdete na adrese:

<https://www.marbes.cz/novinky>

Michal Karvánek





Používání různých typů elektronických podpisů

Často se při vydávání certifikátů setkáváme s otázkou, jaký typ podpisu má být v konkrétní situaci použit. Pracovníci I.CA mohou svým klientům poskytnout doporučení, která vycházejí z platných právních předpisů, odborných textů, výroků soudů různých stupňů a z poznatků z praxe. Tyto dotazy jsou čtenější v době, kdy v důsledku nepříznivé epidemiologické situace výrazně stoupá zájem o elektronickou komunikaci, a tedy i o použití elektronického podpisu.

Zpravidla je možné na tyto dotazy kvalifikovaně odpovědět, zůstává však i oblast, ve které v současné době nepanuje mezi právníky ve výkladu úplná shoda.

Podle našich poznatků nečiní v praxi téměř žádné problémy situace, kdy je nejméně jedním z komunikujících orgán veřejné moci. K tomu je k dispozici „Metodický pokyn k elektronickým podpisům a pečetím pro veřejnoprávní původce“, doplněný odpověďmi na časté dotazy. To vše je dostupné na webových stránkách Ministerstva vnitra v sekci Služby vytvářející důvěru a elektronická identifikace.

V těchto situacích platí, že:

- pokud právně jedná orgán veřejné moci, musí být použit **kvalifikovaný elektronický podpis**;
- pokud kdokoliv jedná vůči orgánu veřejné moci, musí použít **zaručený elektronický podpis založený na kvalifikovaném certifikátu nebo kvalifikovaný elektronický podpis** (zákon oba typy souhrnně nazývá „uznávaný elektronický podpis“).

Při jednání vůči orgánu veřejné moci se tedy bezpodmínečně nevyžaduje použití kvalifikovaného prostředku pro vytvoření podpisu (tj. hodnocená čipová karta, token), to platí jen u kvalifikovaného elektronického podpisu. Tento český „uznávaný podpis“ je českou národní výjimkou

a nařízení eIDAS takový pojem nezná. Příslušná ustanovení obsahuje v § 5 a 6 zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „zákon č. 297/2016 Sb.“).

Připomeňme si, co nařízení eIDAS v čl. 25 stanoví ohledně právních účinků elektronických podpisů:

- elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nespĺňuje požadavky na kvalifikované elektronické podpisy;
- kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu;
- kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

Tato ustanovení je žádoucí mít na paměti zejména v situacích, kdy si nemůžeme být jisti, zda elektronicky podepsaný dokument nebude předán do jiného členského státu, případně tam použit při dokazování.

Pro zjednodušení je použit pojem „orgán veřejné moci“, podle zákona č. 297/2016 Sb. označovaný jako „veřejnoprávní podepisující“, kterým jsou stát, územní samosprávné celky, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávním celkem nebo právnickou osobou zřízenou zákonem, nebo jiná osoba při výkonu své působnosti. Pokud není ani jedním z komunikujících orgánů veřejné moci, aplikuje se § 7 zákona č. 297/2016 Sb., který stanoví, že: „k podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1.“

Pokud se tedy elektronicky podepisuje ve všech dalších situacích, tedy především při podepisování soukromých listin, zákon připouští použití „jiného typu elektronického podpisu“. Tím může být téměř cokoliv, například i z klávesnice napsané „Tvůj strýc Karel“.

Tento jiný typ elektronického podpisu bývá označován jako „prostý“ elektronický podpis. V nařízení eIDAS ani v českém právu není nijak dále upravován, neexistují pro něj žádné obecné normy ani technické standardy, nejsou zde žádné služby vytvářející důvěru (při vytváření, uchování či ověřování).

Podle zveřejněných právních názorů patří k těmto metodám podpisu zejména napsání jména a příjmení na konci dokumentu nebo v e-mailové zprávě, zaškrtnutí políčka „souhlasím“ na webové stránce (např. „souhlasím s obchodními podmínkami“), ale i vložení obrázku s naskenovaným vlastnoručním podpisem (např. na konci dokumentu), vzor podpisu vytvořený elektronickou tužkou a další. Tento typ elektronického podpisu najde uplatnění zejména mezi dvěma soukromoprávními subjekty. Záleží však vždy na samotných stranách, jaké podmínky pro elektronický podpis si nastaví. Mohou se také dohodnout, že pro uskutečnění právního jednání budou vyžadovat některou z následujících „vyšších“ forem elektronického podpisu.

Prostý elektronický podpis je možné použít zejména v případech, pokud je k dispozici něco navíc, čím si příjemce ověří, kdo je skutečným podepisujícím. To může být například osobní známost, kdy se jedná o dlouhodobou opakovanou komunikaci, nebo BankID, pomocí kterého si spo-

léhající se strana může ověřit identitu podepisující osoby. Uplatnění může najít i v případě hromadných návrhů (formulářů) na webových stránkách, v hromadné elektronické korespondenci, na elektronických fakturách apod.

Kvalifikovaný elektronický podpis i ryze český uznávaný elektronický podpis s vysokou úrovní důvěry „zaručuje“ integritu podepsaných dat a identitu podepsané osoby. Kvalifikovaný certifikát je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru konkrétní osobě proti ověření její totožnosti. Podpis se pak vytváří jen z iniciativy podepsané osoby a až v souvislosti se zobrazeným obsahem jednání. Takto vytvořený podpis nelze nepoznatelně vyjmout a přenést jinam, např. připojit k jinému dokumentu. V případě „zaručeného“ elektronického podpisu je to se zárukou identity podepsané osoby problematické a nelze na ni bez dalšího spoléhat. V případě „prostého“ elektronického podpisu chybí jak záruka integrity podepsaných dat, tak identity podepsané osoby. Pokud se jedná o biometrický podpis, resp. dynamický biometrický podpis, někteří právníci jej pokládají za „prostý“ elektronický podpis, jiní za „zaručený“.

Je nutné vzít v potaz, že právníci, kteří se dané problematice věnují, a ani soudy ještě nejsou při posuzování různých typů podpisů zcela jednotní, což se týká především tzv. prostého elektronického podpisu. Pokud se chce klient vyvarovat jakýchkoliv rizik, pak i v případě, že právní předpisy nestanoví jako povinný určitý typ podpisu, použije „uznávaný elektronický podpis“, tj. buď zaručený elektronický podpis založený na kvalifikovaném certifikátu, nebo kvalifikovaný elektronický podpis. V případě, že může být podepsaný dokument použit za hranicemi České republiky, je žádoucí použít v každém případě kvalifikovaný elektronický podpis (řada států jiný typ neuznává).

Použití kvalifikovaného časového razítka stvrdí, že podpis byl vytvořen v době platnosti kvalifikovaného certifikátu, což případně dokazování ještě usnadní a činí podpis ještě důvěryhodnějším.

Roman Kučera
obchodní ředitel, veřejná správa



Cesta k úsporám bez stavebních úprav

Cesta k úsporám bez nákladných rekonstrukcí. Přesně tak by šlo popsat volbu bezdrátové zónové regulace vytápění známé jako IQRC. Pro její využití se rozhodl i Magistrát města Prostějova. Dlouhodobá udržitelnost a snižování nákladů i dopadů na životní prostředí jsou zde prioritou. Právě systém IQRC dodaný firmou HDL Automation s.r.o. s ní dokonale ladí a současně jeho nasazení díky využití bezdrátových termostatických hlavic nevyžaduje žádné větší stavební úpravy, které by uvnitř historické budovy úřadu ani nebyly povoleny. Tím však výčet výhod bezdrátové zónové regulace vytápění rozhodně nekončí.

Centrální dohled i ovládání systému

Kromě zmíněných povinností splnil systém IQRC i mnohé další energetické požadavky. Klíčová je možnost individuální regulace teplot v jednotlivých místnostech rozsáhlé budovy. Ta dovede zajistit vytápění pouze v obsazených kancelářích v pracovní době. Na regulaci lze dohlížet vzdáleně, což samozřejmě nevyklučuje dočasné změny teploty prováděné pracovníky přímo v kancelářích. V místech objektu, kde se pohybuje veřejnost, je možné této manipulaci zamezit a předejít tak neoprávněným zása-

hům na termostatických hlavicích (TRV) pomocí speciálního krytu hlavice nebo uzamčením kláves regulátoru. Ve vybraných prostorách sociálního zařízení byla tato varianta využita a teploty jsou řízeny na základě hodnot uvedených v hygienické normě přes TRV hlavice. Díky centrálnímu ovládání se lze jednoduše přizpůsobit například i dočasné změně úředních hodin, aniž by servisní pracovník musel fyzicky na magistrát přijít a obcházet teplotně regulované místnosti.



Nová radnice v Prostějově s prvky historismu a secese je cenným dokladem stavebního a uměleckého řemesla počátku 20. století

Specifikace magistrátu

Již v úvodu zaznělo, že úřad sídlí v historickém areálu, zástupci magistrátu proto uvítali možnost barevného sladěni exponovaných prvků systému s dřevěným obloženi interiéru historické budovy úřadu. Pro bližší představu o rozsahu i specifikách realizace si dovolíme popsat i další detaily. Instalace bezdrátové zónové regulace vytápění IQRC probíhala ve dvou administrativních budovách.

První z nich se nachází v ulici Demelova, druhá je přímo radnici města Prostějova. Obě sestávají z desítek místností, rozsáhlých společenských prostor, zasedacích místností i reprezentativních míst. Požadavkem tedy bylo, aby každá budova disponovala svojí řídicí jednotkou. Počet regulačních jednotek zajišťujících bezdrátovou komunikaci mezi termostatickými hlavici a řídicí jednotkou přesáhl hranici stovky a samostatných hlavice bylo v rámci tohoto projektu využito hned tři sta. Dále se v seznamu položek objevily snímače teploty, prodlužovače signálu a přes sto pevných hlavice s antivandal krytkami.

Nečekaně snadná instalace

Máte-li představu, že změna systému vytápění musí obnášet hromady prachu, suši a početnou skupinu pánů vyzbrojených úhlovými bruskami a svářečci technikou, rozhodně byste neměli následující řádky přeskakovat – spolehlivě vás vyvedou z omylu. Instalaci systému IQRC lze shrnout do několika kroků. Výměna regulačních radiátorových ventilů, kvůli které je nutné vypustit, napustit a odvzdušnit otopný systém. Dále samotné osazení motorických a TRV hlavice na ventily. Osazení a elektrické zapojení prostorových regulátorů, prodlužovačů signálu a teplotních čidel. A nakonec parametrování, oživení a otestování provozu celého systému pomocí software IQRC. Díky zmíněné bezdrátové metodě mizí nutnost interiérových úprav, stavební zásah je tak omezen na elektroinstalační práce z důvodu nutného přívodu 230 V k napájení regulačních jednotek. To je samozřejmě možné zajistit i z již instalovaných ovladačů osvětlení nebo zásuvek. Klíčovým faktorem doby instalace se tak stává množství hlavice, které je nutné vyměnit za bezdrátové – v případě Magistrátu města Prostějova nebylo rozhodně malé. I tak se s dobou instalace vešli pracovníci HDL Automation s.r.o. do vymezeného prázdninového období, které je charakteristické menším vytížením a samozřejmě i tím, že nezasahuje do topné sezóny.



Jednotlivé prvky systému jsou sladěny s dřevěným obloženi interiéru historické budovy

Smyslné využití technologií

S nadsázkou se dá říci, že nejlépe ušetřená energie je ta, co se vůbec nemusí vyrobit. A právě i díky bezdrátové regulaci vytápění se Magistrát města Prostějova řadí mezi zodpovědné úřady, které budují Smart City s rozmyslem, prokazatelnými přínosy a nehledají pouze libivá řešení k chlubení. Udržitelnost je značně abstraktní pojem, úspory jsou však hmatatelné a nezpochybnitelné. Jakých přesných hodnot dosáhnou v Prostějově, zjistí správce systému nejdříve na konci topné sezóny. Při správném nastavení však lze předpokládat, že by výsledná čísla měla potvrdit zlepšení alokace tepla a snížení plýtvání. Nejinak tomu bylo i v řadě jiných areálů a budov, které bezdrátovou regulaci vytápění již disponují – například 1. ZŠ Hořovice, Obchodní akademie Sereď, ZŠ Dr. Edvarda Beneše Čakovice, Ministerstvo školství Slovenské republiky nebo Nemocnice Vranov nad Topľou.

HDLA

Jak bude vypadat úřad budoucnosti? Projekt digitalni-urad.cz ukazuje, co lze pro digitalizaci udělat už teď.

V posledním díle studia eGovernment jsme s hosty diskutovali na téma, které je v současné době vysoce aktuální. Jak by měl vypadat moderní úřad a jaké služby by měl občanům nabízet? Na tyto otázky přišli odpovědět Ing. Roman Vrba, ředitel odboru eGovernmentu Ministerstva vnitra, Mgr. Martin Kupka, poslanec, zastupitel Středočeského kraje a starosta Libeznic, Ing. Marek Řezáč, ředitel pro strategický rozvoj společnosti Gordic, a Ing. Václav Koudele, Industry Executive ve společnosti Microsoft a jeden z hlavních autorů nového projektu [digitalni-urad.cz](#). Ten na názorných příkladech ukazuje, že přerod na moderní úřad nemusí být ani náročný, ani nákladný, hlavně ale že ze změny budou profitovat jak samotní úředníci, tak hlavně občané.



Digitalizovaná veřejná správa umožní občanům vyřizovat svou agendu z pohodlí domova.

„Karlovi se blíží konec platnosti občanského průkazu, na což ho upozorní notifikace od digitálního asistenta v mobilním telefonu. To je Karlův osobní asistent a také součást Portálu občana. Pomáhá Karlovi se vším, co potřebuje od úřadů, a má k tomu od něj přístup i k informacím, jaké o Karlovi jednotlivé úřady mají. Díky tomu umí digitální asistent včas upozornit na blížící se konec platnosti dokladů, technickou kontrolu auta nebo na důležité termíny, které by Karel neměl zmeškat. Karel tak nezapomene zaplatit daně ani na možnost požádat si například o dotaci na opravu domu. S digitálním asistentem také Karel vyřeší vše potřebné pro prodloužení platnosti svého řidičského průkazu. A i když si ho musí vyzvednout osobně, může si dopředu rezervovat preferované datum a čas tak, aby na úřadě nemusel trávit delší dobu, než je nezbytně nutné.“

Digitalni-urad.cz: řešení, která pomohou úředníkům i občanům

Výše popsaný příběh se někomu může zdát jako vize daleké budoucnosti. Pro nový projekt digitalni-urad.cz, který byl spuštěn v těchto dnech, jde jen o jeden z mnoha pří-

kladů, jak efektivně digitalizovat státní správu. Prostor pro využití projektu digitalni-urad.cz je navíc obrovský – ve studiu eGovernment na úvod zaznělo, že je stále velká část úřadů, krajů a obcí, které v oblasti digitalizace zaostávají. „**Nacházíme se v situaci, kdy jsme v některých věcech**

velmi pokročili. Na centrální úrovni jsme už zavedli celou řadu vyspělých nástrojů, jako je například Portál občana, které jsou srovnatelné i v rámci EU. Zároveň jsou ale úřady i města, která nemají digitalizaci jako prioritu a nechtějí se jí zabývat, řekl ředitel odboru eGovernmentu Ministerstva vnitra Roman Vrba.

Diskutující se shodli, že ač koronakrizy v mnoha oblastech hlavně bere, digitalizaci jak soukromé sféry, tak i veřejné správy ale pomohla posunout vpřed. Poslanec, zastupitel a starosta Martin Kupka uvedl, že celá řada krajů využila poslední měsíce k digitalizaci nebo zajištění optických sítí. Zároveň ale zdůraznil, že stát v digitalizaci zaostává za soukromým sektorem a musí ho dohnat.

Občané jsou na realitu digitálního úřadu připraveni

Online komunikace s institucemi i firmami, ale i nákupy jak přes počítač, tak přes mobil nebo tablet jsou v dnešní době zcela samozřejmé pro velkou část občanů, konstatoval Václav Koudele z Microsoftu. **„Většina občanů je už dávno připravená na realitu digitálního úřadu. Internet a komunikační technologie jsou všeobecně rozšířené a lidi si navykli komunikovat s komerční sférou online. Spotřebitelské chování nám tedy ukazuje, že digitalizace státní správy je tím správným krokem vpřed, který má navíc potenciál zajistit větší transparentnost a spolehlivost,**“ doplnil.

K urychlení procesu digitalizace státní správy slouží několik nástrojů a opatření, které byly v nedávné době zave-

deny. Klíčovými jsou zákon o právu na digitální služby a také nová bankovní identita. Zákon je podstatný hlavně kvůli změně uvažování úředníků. Předtím, než vstoupil v platnost, si každý úřad digitalizoval více méně podle svého uvážení. Zákon o právu na digitální služby ale jasně uvádí, že vše, co lze digitalizovat, digitalizováno být má. Pohodlnou digitální komunikaci s úřady pak přineslo zavedení bankovní identity. V současnosti k ní má přístup zhruba dva a půl milionu občanů a s přibývajícím bankovními domy, které ji zavádějí, bude toto číslo dále růst. Další občané, kteří budou připraveni s úřady komunikovat digitálně, přibudou díky chystaným změnám u datových schránek.

Portál občana přináší úřady do počítačů i telefonů

„V minulosti jsme často slýchávali, že na digitální služby nejsou občané, kteří by je využívali, což se právě díky bankovní identitě zásadně změnilo,“ říká Václav Koudele z Microsoftu. Tento technologický lídr se mimo jiné spolu s Ministerstvem vnitra podílel na vzniku Portálu občana. Přes tuto službu, dostupnou jak na počítači, tak i v telefonu s operačním systémem Android, si občan už dnes může vyřídit celou řadu úkonů, kvůli kterým musel v minulosti fyzicky dojít na úřad či vyplnit papírový formulář. Portál občana běží na cloudovém řešení Microsoftu a jde navíc o otevřenou platformu, již mohou (stejně jako v případě Portálu Pražana) jednoduše implementovat další úřady či samosprávy.



Cloudová řešení jsou postavená tak, aby šla rychle začlenit do běžného fungování úřadů.



Digitální úřad

Veřejná správa může fungovat podobně digitálně jako jiné, uživatelsky přívětivé komerční služby. Díky digitalizaci úřadů můžeme občanům ušetřit vzácný čas i případné starosti a zároveň lépe využít veřejné prostředky. Ukážeme vám, jak na to.

Vydejte se na prohlídku >

Virtuální prohlídka



Fyzická návštěva úřadu

Fyzická návštěva úřadu je klasika, kterou zná každý občan. Návštěva se může zrychlit a zjednodušit, pokud úřady používají současné digitální nástroje.

Přejít na prohlídku >



Digitální služby veřejné správy

Stejně jako jste zvyklí vyřadit většinu vašich potřeb v bance pomocí elektronického bankovníctví, lze i k službám státu přistupovat vzdáleně.

Přejít na prohlídku >



Digitalizovaný úřad

Nestačí digitalizovat služby směrem k občanovi. Aby vše správně fungovalo, je důležité provést změnu a digitalizaci interních postupů a procesů úřadu.

Přejít na prohlídku >

Prozkoumejte digitální řešení pro veřejnou správu na webu <https://digitalni-urad.cz/#/>

V případě nového projektu digitalni-urad.cz se k ustavené spolupráci Microsoftu a Ministerstva vnitra přidala ještě městská část Praha 5, Digitální Česko a NAKIT – Národní agentura pro komunikační a informační technologie. Marek Řezáč, ředitel pro strategický rozvoj společnosti Gordic, jejíž řešení je v rámci digit-urad.cz prezentováno, ve studiu eGovernment připomněl, že každý úřad má překážky v digitalizaci někde jinde, a je tak v první řadě třeba individuální přístup. „**Neexistuje univerzální řešení ani pro stejně velké úřady, všechny mají jiné problémy. Cestou ke zrychlení digitalizace je najít a vyřešit specifický problém daného úřadu. Důležitá je ale také adopce, když se něco zavádí, je nutné jak úředníkům, tak i občanům vysvětlit, co to znamená a jaké výhody z toho pro ně plynou,**“ řekl Marek Řezáč.

Digitální-urad.cz ukazuje, jak jednoduchá cesta k digitalizaci může být

I na specifické problémy jednotlivých úřadů myslí nový web digitalni-urad.cz. Jedná se o zcela unikátní projekt jak v regionu středovýchodní Evropy, tak i v celosvětovém měřítku, který za pomoci 360° videí a doprovodných audiokomentářů představuje reálné situace ze života občanů i úředníků. Zároveň přibližuje, jakým způsobem jim představená řešení pomohou. Projekt je určen především manažerům ze státní správy, jimž chce ukázat digi-

tální řešení, která mohou už dnes implementovat do fungování svého úřadu. A protože jsou tu prezentována už existující a odzkoušená řešení, jejich zavádění je nejen rychlé, ale šetří se při něm také náklady. Nedílnou součástí online prezentace dostupné na digitalni-urad.cz jsou pak konkrétní řešení 33 partnerů, která mohou úředníkům s digitalizací významně pomoci.

Součástí prezentace na webu digitalni-urad.cz je také videonávod pro veřejnou správu, jak si postavit vlastní digitální službu z komponent, které jsou k dispozici od Ministerstva vnitra. Za pomoci jednotlivých komponent, tedy služeb, jako je Portál občana, platební identita, eldentita, či například modul kalendář sloužící k zobrazování termínů agend, lze jednoduše a rychle poskládat celý systém plně funkčního e-governmentu na míru každému úřadu. Za centrální služby navíc instituce veřejné správy ministerstvu vnitra neplatí.

„**Byl bych rád, kdyby se všichni manažeři ze státní správy, kteří uvažují o digitalizaci, přišli podívat na internetové stránky Digitálního úřadu, protože tu zjistí, že jde všechno udělat opravdu jednoduše,**“ řekl na závěr Václav Koudele ze společnosti Microsoft.





ROK INFORMATIKY 2021

Speciální setkání úplně všech, pro které je důležitá
informatika a elektronizace veřejné správy
na úrovni krajů, měst a obcí.

Plzeň – Darovanský dvůr, 2. – 4. 6. 2021

Zhodnocení vývoje ICT na krajích, městech i obcích
a diskuze o přístupu státu k eGovernmentu.



Informace a registrace na:

www.egovernment.cz

ICTU a příprava digitalizace stavebního řízení

Jakkoliv se v uplynulých letech podařilo realizovat řadu projektů, které přispěly k elektronizaci a digitalizaci veřejné správy a rozvoji e-governmentu (vzpomeňme jen datové schránky, Czech POINT, základní registry, Portál občana, elektronickou identitu...), v oblasti stavebního řízení na tom stále nejsme nejlépe. Česká republika je podle žebříčku Světové banky až na 157. místě s průměrnou délkou trvání stavebního řízení 246 dní.

Je jasné, že na tomto stavu se podílí více faktorů, ale nedostatečná úroveň digitalizace patří mezi ty podstatné. Pokud chcete získat stavební povolení, je lhostejné, jak moderní a skvělý software Vám pomáhá při vytváření projektové dokumentace. Nakonec ji stejně musíte vytisknout a odnést na stavební úřad. Ještě předtím to však znamená oběhnout celou řadu úřadů a institucí k získání příslušných stanovisek. Dnes, když chcete stavět, nemáte jedno místo, kam se podívat a zjistit, odkud kam vede která trubka a kabel. Musíte proto obeslat všechny vlastníky všech infrastruktur po celé republice, jestli tam nějaký kabel nemají. A mohli bychom pokračovat dále...

ICT Unie se vždy snažila být nejen respektovanou profesní organizací, ale i partnerem a oponentem vlády v projektech moderní informační společnosti. Proto již řadu měsíců spolupracuje s Ministerstvem pro místní rozvoj (MMR) na přípravě rozsáhlého projektu digitalizace stavebního řízení, který by výše uvedené nedostatky odstranil.

V roce 2020 se podařilo společným úsilím zajistit řadu nezbytných kroků, díky nimž je možné celý projekt realizovat. Především díky skvělé komunikaci se skupinou poslanců v čele s Martinem Kupkou, Ondřejem Profanem, Barborou Kořanovou, Jiřím Běhounem a dalšími byla v Parlamentu ČR schválena novela zákona o zeměměřičství, stavebního zákona a zákona o výkonu povolání autori-

zovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě, která položila legislativní základy digitalizace stavebního řízení.

Ve spolupráci s MMR a širokou škálou odborníků se podařilo připravit architekturu celého řešení a připravit vše potřebné pro podání projektů na financování z prostředků Integrovaného regionálního operačního programu.

Koncept počítá se vznikem několika informačních systémů, které usnadní a zjednoduší celý proces.

Mezi základní cíle patří:

- zjednodušit opatřování podkladů před zahájením řízení;
- zajistit vedení elektronického správního spisu s veškerými dokumenty;
- zjednodušit podání prostřednictvím interaktivních formulářů;
- umožnit získávání informací o stavu řízení;
- umožnit správu projektových dokumentací staveb ve standardizovaných formátech (pdf, dwg a BIM), aby bylo možné jejich další využití;
- umožnit oprávněným osobám přístup k těmto strukturovaným datům pro využití pokročilejších funkcí, jež propojí data o územním plánování, data o území a infrastruktúře s daty stavbách a řízeních.



Digitální mapa veřejné správy, tvořená propojením digitálních technických map krajů, přinese informace o zařízení dopravní a technické infrastruktury, včetně údajů o jejich ochranných a bezpečnostních pásmech, údaje o vlastnících, správcích a provozovatelích infrastruktury.

Portál stavebníka bude základním a přehledným rozhraním pro stavebníky, kterým kromě všeobecných informací umožní podávat své žádosti na interaktivních formulářích, zobrazovat informace o stavu řízení, o rozhodnutích a jiných opatřeních. Prostřednictvím Portálu stavebníka bude možné nahrávat dokumenty a projektovou dokumentaci do specializovaných úložišť a rovněž s využitím informací z digitálních technických map žádat dotčené vlastníky a správce technické infrastruktury o jejich stanoviska k záměrům, a to vše na několik kliknutí.

Aby byly všechny dokumenty přehledně na jednom místě, vznikne **evidence stavebních postupů a evidence elektronických dokumentací**, která bude umět pracovat s moderními datovými formáty, včetně dat z BIM, a umožní na tyto soubory odkazovat místo složitého přeposílání velkých souborů.

Samostatným informačním systémem pak bude **Národní geoportál územního plánování**, který bude sloužit ke zveřejnění výstupů z územně plánovací činnosti orgánů územního plánování, k zabezpečení přístupu k evidenci územně plánovací činnosti, k poskytování prostorových dat k tématu plánované využití území a k zpřístupňování a poskytování dalších dat, která souvisejí s územním plánováním.

Ostrý start všech systémů byl naplánován na 1. 7. 2023. Jakkoliv se může zdát, že toto datum je ještě velmi vzdálené, bude třeba zvládnout do té doby obrovské množství práce. ICT Unie je připravena být nadále partnerem vládě při realizaci tohoto projektu, který Českou republiku může významně posunout dopředu.

Zdeněk Zajíček
prezident ICT UNIE

a

Petr Stiegler
koordinátor projektu

Digitalizace stavebního řízení
ICT UNIE





JAKÉ NOVÉ HROZBY ČEKÁJÍ KYBERNETICKOU BEZPEČNOST V ROCE 2021?

V důsledku šířící se pandemie muselo velké množství zaměstnanců v roce 2020 pracovat z domu. V rámci těchto změn došlo i v oblasti kybernetických hrozeb k výraznému rozvoji. Útočníci jsou si velmi dobře vědomi, že v takových chvílích se společnosti střetávají s množstvím náhlých změn, na které nejsou připraveny. Je proto třeba zvážit nasazení vhodných nástrojů a zároveň i možná rizika. Pojďme se podívat na to, o jaká rizika jde a jak se s nimi vypořádat.

Předpovědi hrozeb z dílny **FortiGuard Labs** pro rok 2021 odhalily strategie, které budou kybernetičtí zločinci využívat i v následujících letech. Patří sem mimo jiného předpovědi a informace o Intelligent Edge Computing (kombinace výpočetního výkonu, umělé inteligence, analýzy dat a konektivity), zařízeních s podporou 5G a pokrocích v oblasti výpočetního výkonu, ale také o nové vlně pokročilých hrozeb, se kterými se bude kybernetická bezpečnost potýkat.

Jak posun v oblasti sociálního inženýrství ovlivní kybernetické útoky?

Většina technik sociálního inženýrství nevyžaduje žádnou odbornou zručnost ze strany útočníka, proto se o takový útok může pokusit opravdu každý – od drobných zlodějíů až po ty nejrefinovanější útočníky. V oblasti kyberne-

tické bezpečnosti existuje mnoho technik, které spadají pod sociální inženýrství. Mezi nejznámější patří spam a phishing. Trendem se stávají inteligentní zařízení či jiné domácí systémy, které integrují s uživatelem. V budoucnu už nebudou pouze terčem útoků, ale i kanálem pro hlubší útoky.

Lze očekávat i invazivní útoky pomocí trojských koní?

Zatímco koncoví uživatelé a jejich domácí zařízení se již stali cílem počítačových zločinců, sofistikovaní útočníci je používají jako odrazový můstek. Útoky na podnikové sítě spuštěné z domácí sítě vzdáleného pracovníka – a to zejména v případech, kdy má útočník v trendech užívání jasno – je možné pečlivě koordinovat tak, aby nevyvolaly podezření. Pokročilý malware může nakonec odhalit ještě cennější data a trendy pomocí nových EAT virů (Edge

Access Trojans) a provádět invazivní kroky – patří k nim například zachycení požadavků z lokální sítě s cílem narušit další systémy či vložení dalších příkazů pro útok.

5G může poskytnout prostor pro pokročilé swarm útoky. Kompromitace a využití nových zařízení s podporou 5G otvírá nové příležitosti k pokročilejším hrozbám. Kybernetičtí zločinci pokračují ve vývoji a spouštění swarm útoků. Takové útoky lze rozdělit do podskupin dle napadených zařízení, z nichž každá má odlišnou specializaci. Zaměřují se na síť či zařízení, jako je integrovaný systém, a sdílejí informace v reálném čase, aby svůj útok zdokonalili přímo v akci. Swarm technologie si žádají velké množství výpočetního výkonu, aby umožnily fungování jednotlivým swarmbotům a efektivně sdílely informace ve skupině botů. To jim pomáhá rychle odhalit, sdílet a spojit zranitelná místa a poté přeskupit svoje metody útoku tak, aby lépe využily to, co objevily.

Nové způsoby využití ransomwaru v kritických infrastrukturách

Ransomware se neustále vyvíjí, a jelikož IT systémy stále více konvergují se systémy provozních technologií (OT), zejména s kritickou infrastrukturou, bude narůstat také množství dat a zařízení vystavených ohrožení.

„Je důležité pochopit, vůči komu se musíte chránit a jaké taktiky používá. Kybernetičtí zločinci jsou dobře financováni a při rozsáhlých útocích jde o znemožnění fungování celé vaší infrastruktury. Na to, aby vás přinutili uhradit výkupné, použijí různé donucovací metody v závislosti na ceně dat. Mimo zašifrování vašich dat je také zkopírují (ukradnou) a budou vám vyhrožovat zveřejněním těchto údajů. Pokud jste doteď byli odhodlaní neuhradit výkupné, tak právě zveřejnění dat vás může dostatečně motivovat k přehodnocení vašeho postoje,“ dodává Ondřej Šťáhlavský, Sr. Regional Director CEE ze společnosti Fortinet.

Kvantová počítačová hrozba

Budou-li v budoucnu kvantové počítače schopné zpochybnit účinnost šifrování, mohly by z hlediska kybernetické bezpečnosti vytvořit nové riziko. Obrovský výpočetní výkon kvantových počítačů by mohl způsobit, že někte-

ré asymetrické šifrovací algoritmy budou řešitelné. Výsledkem bude nutnost připravit organizace k přechodu na odolné kryptografické algoritmy pomocí principu krypto-agility, za účelem zabezpečení a ochrany současných i budoucích údajů a informací. I když průměrný počítačový zločinec nemá přístup ke kvantovým počítačům, některé státy jej mít budou. Pokud se již teď nezavedou opatření přijetím krypto-agility, hrozba se stane reálnou.

Klíčem bude umělá inteligence, která drží krok s dobou

Technologie s pokročilou umělou inteligencí, které dokážou vidět, předvídat a čelit útokům, se v budoucnu stanou nutnou realitou, neboť kybernetické útoky budoucnosti budou otázkou mikrosekund. Primární úlohou lidí bude zajistit bezpečnostním systémům dostatek informací na to, aby nejen aktivně čelily útokům, ale ve skutečnosti i předvídalily útoky natolik, že jim bude možné předejít.

Organizace na to nemohou být samy

Není možné od organizací očekávat, že se budou samy schopny bránit proti kybernetickým protivníkům. Budou potřebovat vědět, koho mají v případě útoku informovat, aby bylo možné efektivně sdílet „otisky prstů“ a příslušné správní orgány tak mohly vykonat svoji práci. Prodejci kybernetické bezpečnosti, organizace zabývající se výzkumem hrozeb i další hráči v odvětví musí navzájem spolupracovat na sdílení informací, ale i při vymáhání práva tak, aby pomohli rozložit infrastruktury zločinců a zabránili budoucím útokům. Jen společnou prací je možné přívalovou vlnu kyberzločinců zastavit.

The logo for Fortinet, featuring the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is stylized with a red and white grid pattern.

OTEVŘENÉ FORMÁLNÍ NORMY: FLEXIBILNÍ NÁSTROJ STANDARDIZACE

Orgány veřejné správy pracují při výkonu svých agend s velkým množstvím dat. Kromě primárního využití pro činnosti předvídané zákonem však jejich data mohou být sekundárně využita kýmkoli dalším pro libovolné zákonné účely. Tato data totiž představují značný potenciál, a to jak společenský, například v podobě zajištění efektivnější kontroly veřejné správy nebo participace občanů na věcech veřejných, tak ekonomický, zejména v podobě otevírání možností pro vznik nových služeb a produktů. Právě to je pak hlavním principem právní úpravy informací veřejného sektoru, kterou nalezneme v zákoně č. 106/1999 Sb. Ten je vystavěn na principu *publicity veřejné správy* a umožňuje povinným subjektům, aby zveřejňovaly jakékoli informace¹⁾, s výhradou těch, o kterých zákon specificky uvádí, že jejich zveřejnění není možné.²⁾

Pro efektivní vytváření služeb pracujících s daty veřejného sektoru je nezbytné, aby data byla poskytována v takové podobě, která maximálně usnadní následnou práci s nimi. Když přeskočíme nezbytné podmínky, jako že data musí být zveřejněna online a bez přidáných právních překážek, zcela zásadním požadavkem je technická interoperabilita. Bez ní je totiž jen velice obtížné propojovat data z různých zdrojů, kvůli čemuž se ztrácí značná část již zmiňovaného potenciálu poskytovaných dat. Obzvláště významně se tento problém projevuje tehdy, když typově totožnou datovou sadu publikuje větší množství různých institucí. Typickým příkladem takové situace jsou data z úředních desek, protože v zásadě každý povinný subjekt musí publikovat svoji úřední desku online. Mezi další podobné situace patří například seznamy volných pracovních míst, případně seznamy zájmových bodů v obcích, jako jsou parkoviště (a jejich zaplněnost), umístění kontajnerů na tříděný odpad (a data jejich svozů) nebo turistické cíle (a detaily k nim). Můžeme si snadno představit službu, která bude agregovat všechny úřední desky z celé republiky. Pokud ale každý povinný subjekt bude svoje informace z úředních desek poskytovat, byť jen maličko, odlišně, například rozdílně označí položky v databázi, nebo bude pracovat s rozdílnými číselníky, je jakákoli interoperabilita výrazně ztížena. Tvůrce takové

agregované služby by pak musel vynaložit značné úsilí a náklady na to, aby rozříznutý způsob publikace ve své službě sjednotil, místo toho, aby se zaměřil na nové užitečné funkcionality. Aby se podobným situacím předcházelo, obsahuje zákon č. 106/1999 Sb. koncept tzv. „otevřených formálních norem“.

Otevřená formální norma (dále „OFN“) je v zákoně definována v § 3 odst. 9 jako „*pravidlo, které bylo vydáno písemně a obsahuje specifikace požadavků na zajištění schopnosti různých programových vybavení vzájemně si poskytovat služby a efektivně spolupracovat*“. Tato textace představuje trochu rozpracovanější verzi definice OFN, která se vyskytuje ve směrnici 2013/37/EU³⁾ a zní: „*Norma, která byla písemně stanovena a obsahuje specifikace požadavků na zajištění interoperability softwaru*“. Evropský zákonodárce si totiž uvědomoval nezbytnost zajištění technické standardizace poskytovaných informací, bez které by šlo jen o prázdnou snahu bez reálného výsledku. Zároveň se však projevila racionální obava, že není možné na evropské úrovni normovat každý detailní standard různých typů informací. Kromě toho bylo nezbytné zachovat technologickou neutralitu předpisu a vzít v potaz probíhající technologický vývoj. Výsledkem je tak definice OFN, jež je na první pohled poměrně nejasná.

¹⁾ Ve smyslu zákona č. 106/1999 Sb. se informacemi obecně rozumí jakýkoli obsah na jakémkoli nosiči, tedy včetně dat. Definice je tak v rozporu s většinou teoretických přístupů k informační vědě (srovnej např. Floridi, L. *Information: a very short introduction*. Oxford; New York: Oxford University Press, 2010. *Very short introductions* 225), je však nezbytné s ní v tomto smyslu pracovat.

²⁾ Viz § 5 odst. 6 zákona č. 106/1999 Sb.

³⁾ Tato směrnice provedla novelizaci tzv. PSI směrnice 2003/98/ES, která tvoří evropský základ pro opětovné užití informací veřejného sektoru.

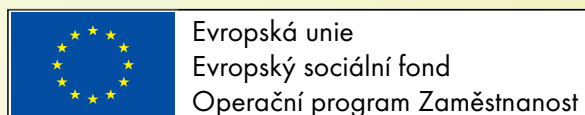
OFN ve smyslu zákona č. 106/1999 Sb. je písemně stanovené pravidlo či specifikace, která může poměrně přesně určit konkrétní technický způsob, jakým mají být určité informace poskytovány, včetně detailního popisu sémantické struktury poskytovaných dat. Zároveň není nutné, aby se jednalo o právní předpis. Zákon ani nijak nepředepisuje, kdo může OFN vydávat. Obecně se však předpokládá, že OFN budou publikovat instituce, které mají v dané oblasti určitou autoritu, byť striktně vzato ne nutně formálně stanovenou. Jako příklad je tak možné uvést standardizační organizace vydávající ISO normy, případně instituce, do jejichž působnosti dané typové informace věcně patří. V České republice začala systematická příprava OFN na půdě Ministerstva vnitra, konkrétně v rámci odboru hlavního architekta eGovernmentu a kanceláře národního koordinátora otevřených dat. V současné době jsou hotové OFN například pro data z registru práv a povinností, data o turistických cílech a data o aktualitách. Na dalších OFN, včetně té pro úřední desky, se pracuje.⁴⁾

Zákon č. 106/1999 Sb. ve svém § 4b odst. 1 stanoví povinnosti, které musí každý povinný subjekt splnit, pokud poskytuje informace zveřejněním, tedy rovněž v případě, kdy publikuje data online a jako otevřená data. Nezáleží, zda ke zveřejňování dochází na základě právní povinnosti, nebo na základě dobrovolného uvážení povinného subjektu. § 4b odst. 1 kromě požadavků na publikaci metadat, otevřenost a strojovou čitelnost formátu poskytované informace rovněž uvádí, že „formát i metadata by měly co nejvíce splňovat otevřené formální normy“. Jedná se o poměrně měkkou formulaci, kterou je však vzhledem k obecným zásadám dobré správy a publicity veřejné správy, stejně jako vzhledem ke standardizačnímu účelu této právní úpravy, nezbytné interpretovat tak, že pokud existuje OFN k informaci, kterou povinný subjekt zveřejňuje, má povinnost se jí řídit a při přípravě publikace dat ji

zohlednit. Tato interpretace navíc odpovídá rovněž posunu k většímu důrazu na dodržování OFN, který je možné sledovat v textaci nové evropské směrnice o otevřených datech (č. 2019/1024) a jejího implementačního návrhu, který v aktuální verzi výslovně zakládá povinnost dodržovat existující OFN. Ačkoli zákon č. 106/1999 Sb. nezavádí žádné přímé sankce pro případy, kdy by povinný subjekt při publikaci dat nedodržel existující OFN, je nezbytné vzít v úvahu, že existence OFN má za cíl standardizaci a lepší interoperabilitu existujících publikovaných dat. Pokud povinný subjekt zveřejní data bez přihlídnutí k OFN, podryvá tento cíl a investice vynaložené na zveřejnění dat a jejich následnou opravu budou spadat do kategorie nevhodného nakládání s veřejnými prostředky.

OFN představují zatím spíše opomíjený, ale do budoucna zásadní prostředek pro zajištění standardizace poskytovaných informací veřejného sektoru a tím i zvýšení jejich kvality, interoperability a využitelnosti. Pro efektivní rozvoj v oblasti informací veřejného sektoru a zajištění jejich další využitelnosti je nezbytné, aby povinné subjekty jejich existenci lépe reflektovaly a přispěly tak ke kvalitnějšímu datovému prostředí české veřejné správy.

JUDr. MgA. Jakub Míšek, Ph.D.



Tento článek vznikl v rámci projektu „Rozvoj datových politik v oblasti zlepšování kvality a interoperability dat veřejné správy“ OPZ č. CZ.03.4.74/0.0/0.0/15_025/0 013983, který zastřešuje odbor hlavního architekta eGovernmentu Ministerstva vnitra ČR.

⁴⁾ Více informací viz online: <https://data.gov.cz/ofn/>.

ZONER Software, a. s.

SVĚŘTE SE DO RUKOU PROFESIONÁLŮ

Společnost ZONER Software, a. s., má více než 25 let zkušeností s vývojem softwaru a poskytováním internetových služeb v oblasti e-commerce. Zoner nabízí celou škálu služeb spojených s provozem a zabezpečením on-line projektů, registrací a správou domén, serverhosting a nejširší nabídku elektronických certifikátů všeho druhu.

Zoner je evropskou společností s hlavním sídlem v Brně a pobočkami na Slovensku, v Maďarsku, Japonsku a USA. Společnost se dělí na čtyři samostatné divize – internetové služby, on-line bezpečnost, fotografický software a vydavatelství.

ZONER PHOTO STUDIO

Program pro zpracování fotografií a fotografické dokumentace **Zoner Photo Studio X** je ústředním produktem divize Software. Využívají ho tisíce firem i veřejných institucí, jejichž uživatelům poskytuje nástroje ke zpracování celého životního cyklu fotografií. Za zajímavých licenčních podmínek nabízí vhodnou alternativu pro širokou skupinu řešení – od bezplatných až po drahé komerční aplikace.

Pro účely zpracování fotodokumentace jsou v programu doplněny **speciální nástroje**, které usnadní uživatelům její rutinní zpracování, ale i nástroje, které jsou specifické pro segment pracovníků ve veřejném sektoru (např. anonymizace obrazu v souvislosti s GDPR, spolupráce programu s katastrálními mapami nebo databází RÚIAN pro poloautomatické popisování fotodokumentace metadaty, nejrůznější grafické anotace apod.). Kromě klasické orga-

nizace a ukládání fotografií na lokální disky uživatelů poskytuje Zoner Photo Studio X také týmovou spolupráci prostřednictvím služby **Zoner Photo Cloud**, která je plně integrovaná do prostředí programu. Vedle toho existuje několik zákaznických instalací *on demand* vytvořené speciální fotodatabáze **Zoner Photo Depository**, jakožto součást širšího projektu Zoner DAM. Zoner Photo Cloud nabízí specializované nástroje pro ukládání fotografií a propracovaný systém ukládání fotografií s metadaty. Kromě zpracování fotografií je v Zoner Photo Studio X pilotně integrován vícestopý střih videa, což rozšiřuje jeho možnosti právě při zpracování obrazové dokumentace v situacích, kdy série fotografií nahrazuje videozáznam.

ELEKTRONICKÉ CERTIFIKÁTY A SPRÁVA DOMÉN

Bezpečnostní SSL/TLS certifikáty Vás denně chrání před různými kyberhrozbami. Díky nim víte, že je Vaše internetová komunikace chráněna, máte jistotu, kdo Vám píše, kdo vytvořil daný dokument, případně Vás upozorní i na phishing. Nejlepší certifikáty poskytuje jednoznačně **projekt SSLmarket.cz**, který je největším prodejcem těchto



certifikátů v Evropě, jak potvrzuje i **ocenění Partner roku 2019** od společnosti DigiCert, největší CA na světě. SSLmarket.cz má v nabídce několik druhů webových certifikátů, tím nejdůvěryhodnějším je EV – rozšířené ověření. V rámci této úrovně je oblíbeným produktem **EV certifikát od GeoTrustu**. Je doporučován pro společnosti a organizace, které kladou požadavky na nejvyšší stupeň důvěryhodnosti a dbají na vysokou úroveň zabezpečení.

SSLmarket.cz se zaměřuje jen na ty nejkvalitnější produkty, proto v jejich nabídce najdete i oblíbené certifikáty Thawte od společnosti DigiCert. Kromě tradičních SSL/TLS certifikátů pro webové servery a služby můžete získat osobní certifikáty pro elektronický podpis (S/MIME), kvalifikované certifikáty splňující požadavky e-IDAS, certifikáty pro podpis dokumentů a certifikáty pro podpis zdrojových kódů aplikací.

Jako pracovníci ve veřejném sektoru jistě oceníte i možnost **zabezpečení domén DNSSECem** (rozšíření systému doménových jmen DNS, které zvyšuje jeho bezpečnost). Registraci a správu zabezpečených domén poskytuje další z projektů ZONER Software, **CZECHIA.COM**. Je prvním registrátorem, který má na svých DNS zabezpečeno 100 % .cz domén technologií DNSSEC.

CZECHIA.COM poskytuje nejširší nabídku doménových jmen k registraci na trhu.

U většiny domén jsou v nabídce i **víceleté registrace**, které jsou výhodnější pro Váš rozpočet. Při registraci domény také automaticky získáváte bonus ve formě HTTPS zabezpečení svého webu s certifikátem Basic DV od DigiCertu, e-mailovou schránku na vlastní doménu zcela zdarma v rámci služby inPage mini a možnost vytvořit si základní webové stránky, fotogalerie nebo e-shop díky službě inPage mini.

SERVERHOSTING A HOSTING

Rychlost načítání webových stránek do značné míry ovlivňuje výkon serveru, na kterém jsou data webu a jeho funkční scripty uloženy a které zabezpečují jeho chod. Existuje několik možností, jak bezproblémový provoz webového projektu zajistit. Od webhostingu, přes pronájem virtuálních serverů až po provoz vlastního zařízení.

Projekt ZonerCloud.cz společností ZONER Software, a. s., nabízí nejvýkonnější virtuální servery na trhu zapojené v cloudové infrastruktuře. Jednou z mnoha výhod serverů od ZonerCloud.cz je, že nedochází k žádným latencím a případným výpadkům spojení, protože všechny servery jsou umístěny v ČR. Aby ZONER svým kli-



entům zajistil absolutní komfort a bezchybnost služeb, postavil nové datové centrum v klasifikaci TiER III. Obsahuje ty nejmodernější technologie od nejspolehlivějších dodavatelů na trhu, jako jsou DELL a CISCO. Stavba tohoto moderního datacentra vyšla společnost ZONER Software na desítky milionů Kč. Zoner může svědomitě prohlásit, že je Green providerem, na střeše svého sídla vybudoval vlastní solární elektrárnu o výkonu 60 kWp, která slouží pro napájení datacentra. Veškerou další potřebnou energii dále nakupují od společnosti E.ON jen z obnovitelných zdrojů. Že má ZonerCloud.cz ty nejvýkonnější servery, dokazuje i velké výkonnostní srovnání, ve kterém ZonerCloud.cz porazil přední konkurenty. ZONER Software, a. s., Vám pomůže i s **hostováním** Vašeho webu. Vybírat můžete z webhostingových variant pro Windows, Linux, WordPress, Drupal, Joomla a další. Výhodou je bezproblémová a intuitivní instalace – stačí jedno kliknutí.

Jejich webhosting běží na nejnovější distribuci Debian ve verzi 10.2 (Buster), webserver je Apache 2.4. Podporujeme http/2 (pro rychlejší načítání šifrovaného obsahu), nejnovější verzi protokolu TLS 1.3 a nejnovější rodinu šifer využívajících eliptické křivky ECDH x25519.

Nedílnou součástí webhostingových profesionálních služeb jsou i e-mailová řešení s trojí ochranou (antispam, antivir, antiphishing), kde např. u nejoblíbenějšího programu Linux Plus máte k dispozici neomezený počet e-mailových schránek a 20 GB prostoru.

Paolína Malachová
obchodní oddělení internet divize





e-government
20:10 aneb žijem si jak na zámku,
ať to trvá věčně

MIKULOV • 7. - 8. 9. 2021

13. ročník výroční konference e-governmentu 7. - 8. 9. 2021

Platinový partner:



Generální partner:



GORDIC



www.egovernment.cz