Egovernment
elektronizace veřejné správy

# ZPRÁVA Z KONFERENCE V MIKULOVĚ:

# STOUPÁME!

## BOD ZLOMU = BANKOVNÍ IDENTITA + KATALOG SLUŽEB

## MIKULOV 2020 – TO TU JEŠTĚ NEBYLO

Vždy jsme si přáli, aby byla naše konference výjimečná, řekněme až nezapomenutelná. Nečekali jsme, že se nám to někdy splní až takovým způsobem. Letošní ročník konference **e-government 20:10**, aneb žijem si jak na zámku, ať to trvá věčně se nám všem skutečně vryl do paměti. A upřímně doufám, že už se to opakovat nebude.

Z pohledu moderátora to vypadalo trochu jako na sjezdu chirurgů, sál plný zarouškovaných osob, všude stojany s desinfekcí a hlídání maximálního počtu osob v jednom sále (pro přebývající byl připraven přenos do sálu vedlejšího). Aby napětí z toho, jak s narůstajícími hygienickými požadavky bude konference nakonec vypadat, bylo co největší, v pátek, těsně před konferencí, MV ČR rozhodlo, že žádný z jejich vystupujících či účastníků nesmí do Mikulova přijet. Vzhledem k tomu, že MV ČR stabilně tvoří základní složku úvodního bloku konference, začal se produkční tým hroutit. Nutno v tomto směru poděkovat MV ČR a pochválit ho, protože přes víkend připravilo „vysílací" studio, z něhož bravurně odbavili jak jednotlivé prezentace, tak odpovědi na otázky. Zároveň dokázali rozsah prezentací přiměřeně upravit, aby vyhovovaly jiným nárokům, jež vyžaduje videoprezentování oproti klasické fyzické přítomnosti. I díky tomu jsme „sjeli" celou sekci vlastně téměř stejně, jako by byli zástupci MV ČR přímo v Mikulově.

Odpolední bloky konference opět nabízely řadu prezentací v oblasti e-governmentu, nebo kyberbezpečnosti. Na tu jsme pak v závěrečném workshopu navázali kyberbezpečností speciálně v oblasti zdravotnických zařízení. Mezičas mezi jednotlivými pracovními dny konference vyplnil koncert ABBY (Abba World Revival), který s ohledem na realizaci ve venkovním prostředí a našem celodenním zahalení do roušek byl skutečně příjemným osvěžením.

Vzhledem k tomu, že téměř ihned po mikulovské konferenci byla hygienická opatření ještě zpřísněna, zdá se, že to byla a bude jedna z mála konferencí, které se v letošním roce podařilo realizovat. Jak to přesně vypadalo a o čem všem jsme hovořili, naleznete na následujících stránkách, nebo na webové adrese www.egovernment.cz v sekci Mikulov, kde jsou k dispozici prezentace v PDF i videozáznamy jednotlivých vystoupení.

Přeji Vám vše dobré a těším se, že se setkáme na konferenci v čase bez roušek.

Michal Jirkovský,
šéfredaktor

# Obsah




**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:** Petra Němečková

**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




## 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 zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info◆com** s.r.o.

# MUSÍME PŘESVĚDČIT OBČANY

***V Mikulově jsme hovořili o klientsky přívětivě orientované veřejné správě. Zatím stále velmi často dochází k tomu, že jakákoliv žádost směřovaná na úřad musí být podložena vyplněným papírovým formulářem. Přitom kolonky se týkají dat, která už veřejná správa má. Kdy toto zmizí? Tzn., kdy bude možné požádat o něco s tím, že úředník si všechny údaje na základě ztotožnění „natáhne" automaticky? To jsou otázky, které jsme položili náměstkovi ministra vnitra pro řízení sekce informačních a komunikačních technologií Jaroslavu Strouhalovi.***

Nejdříve bych rád zmínil, že český e-government za posledních deset let udělal ohromný pokrok. Vybudoval základní pilíře digitalizace – základní registry, Informační systém datových schránek a síť kontaktních míst veřejné správy (Czech POINT). My jsme opravdu postavili velmi robustní a bezpečný backend pro digitalizaci. Druhá věc je ovšem legislativní rámec digitalizace. Zde musím upozornit, že ač my, jako Ministerstvo vnitra, digitalizaci zastřešujeme, nemohli jsme ovlivnit všechny legislativní procesy, které s tím souvisejí. V tomto ohledu je velkou změnou přijatý zákon o právu na digitální služby, který mimo jiné vyžaduje po veřejné správě, aby nepožadovala po uživatelích údaje, které již stát má. Tento zákon nabývá účinnosti 2. února 2021. Do té doby by měly být všechny služby, u kterých to lze provést, katalogizované. Zákon také umožňuje tzv. podání pomocí systému podporujícího vzdálené elektronické přihlášení občana. Předpokládám, že právě tento způsob podání pomocí tzv. portálových řešení konkrétních agend bude mít za následek výrazné navýšení počtu elektronických služeb. Díky němu nebude nutné státu opakovaně dokládat údaje, kterými již disponuje, ale hlavně půjde čerpat službu veřejné správy v místě a čase, které občanovi vyhovují, a nikoliv jen v úředních hodinách konkrétního úřadu. Vždy však budou úkony, u kterých bude nutná přítomnost občana na úřadě. Také bych zde rád uvedl, že ne vždy je nedostatek vůle na straně úřadů. Češi jsou na předních příčkách v Evropě ve využívání nákupů on-line, přesto však možností využívat elektronickou komunikaci se státem využívá jen zlomek obyvatel. „Papíru" před elektronickou komunikací dává přednost stále velká část občanů. My to však chceme a věřím, že dokážeme, změnit.

**Co vlastně takovému elektronickému sdílení dat brání? V Mikulově padlo, že legislativu i peníze už máme, přesto jsme velmi často stále v rovině papírového úřadování.**

Jak jsem již v předchozí otázce uvedl, dříve jsme se potýkali i s legislativními překážkami (nyní jich je většina vyřešena zákonem o právu na digitální služby). Náročné je však i samotné technické propojení mezi informačními systémy jednotlivých úřadů. Propojení informačních systémů veřejné správy (ISVS) řeší základní registry a Informační systém sdílených služeb, který umožňuje vzájemné sdílení dat. Tento propojený datový fond (PPFD) funguje na principu „Once-only" a „obíhají data, nikoli lidé". V reáli-

ích roku 2020 je ke službám PPDF připojeno cca 3 500 informačních systémů z celkového počtu cca 7 000. Základním cílem PPDF je kromě připojení všech informačních systémů veřejné správy také zajištění, aby připojení pro relevantní ISVS nebylo jen čtenářského typu (čerpání údajů), ale i publikátorského typu (poskytují své údaje). Teprve až budou všechny relevantní informační systémy veřejné správy čerpat a poskytovat služby PPDF, může se hovořit o propojeném datovém fondu.

Příkladem úspěšného sdílení dat může být propojení Centrálního registru řidičů s Portálem občana, díky čemuž zde můžete vidět své bodové hodnocení řidiče nebo také propojení Portálu občana s rejstříkem trestů, díky kterému si v Portálu občana můžete jednoduše, kdykoliv a zdarma obstarat výpis ve všech úředních jazycích EU.

**Podle zkušeností pracují úřady, kde to jde, alespoň z nějaké části elektronicky a jsou úřady, kde bez papíru ani krok. Znamená to, že není jednotný, závazný požadavek, jak tato služba má vypadat? Jak mohu vědět, jestli mě daný úřad může a musí obsloužit elektronicky, případně odkdy by takový požadavek byl sjednocen pro všechny úřady?**

Tuto informaci obsahuje připravovaný Katalog služeb VS. Podle zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, musí vláda do 1. 2. 2021 stanovit plán digitalizace. Cílem Katalogu služeb VS bude přehledně informovat klienta o všech dostupných službách veřejné správy (VS) a zároveň díky evidenci služeb VS, úkonů a jejich obslužných kanálů stanovit plán digitalizace a podpořit tím rozvoj e-governmentu. To vše bude dostupné na modernizovaném Portálu veřejné správy, který se aktuálně připravuje. Takže v blízké budoucnosti bude mít každý občan právo (nikoliv povinnost) komunikovat s úřady elektronicky, pokud to příslušná agenda umožňuje.

**V rámci diskuze jsme si vytkli, že do dvou let by ČR měla být dvacátá v hodnocení EGDI. Aby se tak skutečně mohlo stát, je vhodné směřovat k tomu, že se zbavíme dokladů v podobě množství kartiček a nahradit je přístupovým klíčem k datům (aplikací, generovaným kódem atp.). Máme v plánu v dohledné době takový krok?**

Ano, ale bohužel to nepůjde pro všechny, jak říkáte „kartičky", najednou. Budeme muset postupovat po jednotlivých krocích, protože každou z nich typicky řídí nějaký konkrétní právní předpis. Pro příklad nemusíme chodit daleko, konkrétně třeba řidičský průkaz. Jeho vydávání a nakládání s ním definuje zákon o provozu na pozemních komunikacích a v něm se říká, že řidič motorového vozidla musí mít při řízení u sebe technický průkaz. Pokud bychom tedy chtěli tento doklad převést do mobilní podoby, abychom jej nemuseli nosit u sebe fyzicky, je třeba změnit právní předpis. V tomto konkrétním případě by se to mohlo podařit už brzy, protože to je jeden z pozměňovacích návrhů k zákonu o další elektronizaci postupů OVM (tzv. „DEPO"), nicméně bude třeba ještě dořešit další otázky. Například nemožnost zadržení dokladu, přestože to v některých konkrétních situacích zákon dnes umožňuje. Ale zpět k Vaší otázce, u jiných než identifikačních dokladů (občanský průkaz, pas) to v principu půjde, jen to znamená nemalé legislativní změny. Co se týče základních osobních dokladů (občanský průkaz a cestovní pas), zde převládá nad výhodami jejich držení v mobilních aplikacích bezpečnostní riziko v případě jejich zneužití. MV v současné době pracuje na projektech, které si kladou za cíl výrazně omezit možnosti zneužití základních osobních dokladů pro trestnou činnost. Jde především o zavedení biometrických prvků do OP a zvýšení ochrany dokladů zavedením moderních ochranných prvků. Nahrávání těchto dokladů do mobilních zařízení považujeme k uvedeným aktivitám jako kontraproduktivní a jako cestu zcela opačným směrem.

**V porovnání například použití eOP a nového elektronického prostředku MojeID pro přístup k elektronickým službám veřejné správy vychází eOP poněkud těžkopádně až trochu starosvětsky. Do jisté míry je to charakteristika i pro ostatní prvky elektronizace veřejné správy. I takový náhled je součástí klientsky orientované VS. Dojde v tomto směru k nějakým změnám? Tedy nikoli pouze, že zde je elektronický přístup, ale že jeho forma odpovídá jakýmsi standardům či zažitým modelům, které známe například z komerční oblasti. Ve výsledku tedy bude elektronický kontakt s veřejnou správou stejně moderní, intuitivní a jednoduchý, jako tomu je například v rámci e-bankovnictví, e-shopů atp.?**

eObčanka je doklad, který stát vydává svým občanům jak pro fyzické prokázaní totožnosti, tak i pro elektronické prokázání totožnosti občana. eObčanka byla navrhována s ohledem na dosažení nejvyšší úrovně záruky prostředku elektronické identifikace (tj. nejvyšší míra důvěry v prokazovanou totožnost), aby mohla být použita pro přístup i ke službám, které vyžadují nejvyšší úroveň záruky. Z toho samozřejmě plyne i Vámi zmiňovaná „těžkopádnost", protože jsme dbali především na dodržení bezpečnosti pro uživatele a úřady.

eObčanka však není jediný státní prostředek pro elektronickou identifikaci. Občané mohou využít dále NIA ID, což je kombinace zadání uživatelského jména, hesla a jednorázového kódu, který přijde v SMS. Tento prostředek (úroveň záruky „značná") se velmi podobá prostředkům, které jsou používány například v bankovnictví pro účely přihlašování do internetového bankovnictví. Dále je vyvíjen prostředek „mobilní klíč e-governmentu", který je rovněž svým principem fungování blízký různým mobilním klíčům používaným např. v bankovnictví.

V neposlední řadě bych rád zmínil projekt bankovní identity, jehož idea spočívá v tom, že občané budou moci použít svoje přihlašovací údaje do internetového bankovnictví také k přihlášení k online službám veřejné správy, potažmo také k přihlášení ke službám dalších třetích stran (např. e-shopy). Uživatel internetového bankovnictví bude tedy moci používat stejné přihlašovací údaje jak k přihlášení do svého internetového bankovnictví, tak k přihlášení ke službám veřejné správy. V těchto dnech probíhá udělení akreditace ČSOB, která si jako první bankovní dům o akreditaci požádala. Další banky, které mají o akreditaci zájem, jsou: Air Bank a.s., Česká spořitelna, a.s., Komerční banka, a.s., (KB) a MONETA Money Bank.

**Má-li být dosaženo našeho posunu o dvacet míst ve zmiňovaném hodnocení EGDI, jaké jsou v oněch dvou letech, podle Vás, nejdůležitější a nevyhnutelné kroky, které musíme realizovat?**

Zcela klíčová je snadná dostupnost nástrojů e-governmentu pro každého občana umožňující elektronickou komunikaci se státem. K tomu v příštím roce přispěje již zmiňovaná bankovní identita, přes kterou bude možné si založit datovou schránku, přihlásit se do Portálu občana nebo portálu své obce. Situaci samozřejmě velmi ovlivní také zákon o právu na digitální služby, o kterém jsem již hovořil. V neposlední řadě je potřeba změnit i přístup občanů k nástrojům e-governmentu. Musíme je přesvědčit, že jejich využívání je oboustranně výhodné a především bezpečné. Ministerstvo vnitra na jaře tohoto roku spustilo dlouhodobou komunikační kampaň, která má veřejnost o výhodách e-governmentu nejen přesvědčit, ale především je naučit je využívat. Je to samozřejmě běh na delší trať, ale uvědomme si, že např. internetové bankovnictví nebo on-line nákupy, které jsou u nás dnes široce využívané, začínaly také na malých číslech a dnes jim většina občanů důvěřuje a využívá jejich výhod.


# Chystá se malý krok, který může znamenat významný skok v digitalizaci Česka

***Bude to zdánlivě drobná změna. Může však znamenat zásadní posun v další digitalizaci Česka.***

BANKOVNÍ IDENTITA

Od 1. ledna příštího roku se postupně lidé budou moci hlásit k elektronickým službám poskytovaným státem stejným způsobem, jakým se již dnes hlásí do elektronického bankovnictví – prostřednictvím bankovní identity. Tu v současnosti využívá již 5.5 milionu Čechů. Této možnosti bylo dosaženo díky spolupráci bank na půdě České bankovní asociace.

Až dosud bylo možné přistupovat k elektronickým službám státu s pomocí datové schránky nebo elektronické občanky (u té však byla potřeba čtečka čipových karet). Tyto přihlašovací metody však zatím přílišnou popularitu mezi občany nezískaly. Bankovní identita je oproti tomu průběžně využívaným nástrojem online identifikace. Díky rozšíření využití bankovní identity, která se stane běžným nástrojem pro online ověřování a elektronický podpis, získá každý druhý Čech snadný způsob, jak na internetu prokazovat svoji totožnost. To by mohlo výrazně „rozhýbat" další digitalizaci Česka (resp. veřejné správy České republiky).

Tři největší banky v České republice (Československá obchodní banka a.s., Česká spořitelna a.s. a Komerční banka a.s.) založili společný podnik – Bankovní identita, a.s. Tato společnost je vytvořena za účelem budování infrastruktury pro poskytování služeb bankovní identity a rozvíjení spolupráce s dalšími bankami. Tak, aby se bankovní identita postupně dále rozšiřovala a byla dostupná maximálnímu počtu uživatelů.

V první fázi, od počátku příštího roku 2021, budou například řidiči moci využít bankovní identitu k přihlášení se do Portálu občana a k ověření, kolik trestných bodů nasbírali. Dále také bude možné podávat daňová přiznání prostřednictvím chystaného portálu Ministerstva financí Moje daně. V další fázi budou moci využívat bankovní identitu i pro identifikaci klientů vůči poskytovatelům komerčních online služeb.

Záměrem je, aby bankovní identita byla snadná pro použití a stala se univerzálním prostředkem pro elektronické ověřování. Má k tomu všechny předpoklady. Potvrzují to zkušenosti ze zemí, kde už takové řešení funguje. Nejlepším příkladem je pro nás Skandinávie.

Severské země jsou lídrem v online komunikaci mezi občany a státem, jak dokazuje index digitální ekonomiky a společnosti DESI sestavovaný Evropskou komisí. V nejlepším Finsku vyšplhal podíl občanů ve věku od 16 do 74 let, kteří loni využili elektronickou formu komunikace se státem, 94,4 %. Česko bylo klasifikováno pod průměrem EU.

V severských zemích je bankovní identita využívána jako standardní identifikační metoda. Například ve Švédsku, kde vznikla služba Bank ID už v roce 2003, ji využívá ji 98 % lidí ve věku od 21 do 40 let. Lidé ve věkové skupině mezi 61 a 70 lety na ni spoléhají v 82 % případů.

Nové řešení, které banky uvedou na český trh, Bankovní identita, bude jak komfortní pro uživatele, tak bude zajišťovat vysokou bezpečnost. Nová bude ale jen v přístupu, neboť pro používání se uživatelů této identity nic, proti současnému stavu, nezmění.

ČSOB

Bankovní identita je podporována Československou obchodní bankou, dostala již akreditaci Ministerstva vnitra, a tím se posunula do závěrečné fáze testování.

# OBRAZ DOBY

***Náměstek ministra vnitra pro řízení sekce informačních a komunikačních technologií Jaroslav Strouhal pozdravil přítomné účastníky konference jménem svým i jménem ministra vnitra, který konferenci poskytl svoji záštitu. V komentáři k prezentovaným výsledkům ČR v rámci hodnocení OSN – EGDI 2020 uvedl, že náš posun směrem nahoru není rozhodně náhodný a jednorázový. Je to z jeho pohledu určitý obraz současné doby, kdy se zúročují kroky realizované v předchozích letech. Navíc se jedná o kroky, které jsou podpořeny potřebnými legislativními změnami. Tzv. střechová norma, tedy zákon o právu na digitální službu, už platí a v současné době se projednává doprovodná legislativa, což zahrnuje zhruba 150 zákonů tak, aby se filozofie zákona skutečně naplnila.***

Pozval rovněž účastníky k jednotlivým blokům konference tak, že upozornil na vystoupení ředitele odboru eGovernmentu Romana Vrby, který hovoří o **Portálu občana**, především pak o tom, jaké služby portál nabízí. Po dvou letech jeho existence je k dispozici více jak 130 služeb/agend, které je možné obsluhovat na dálku. Nicméně vyzval nejen účastníky konference jako potencionální klienty, ale především jako zástupce úřadů, tedy možné poskytovatele služeb, aby se připojili. Ministerstvo vnitra totiž připravilo zázemí, ale naplnit portál službami musí především ostatní úřady.

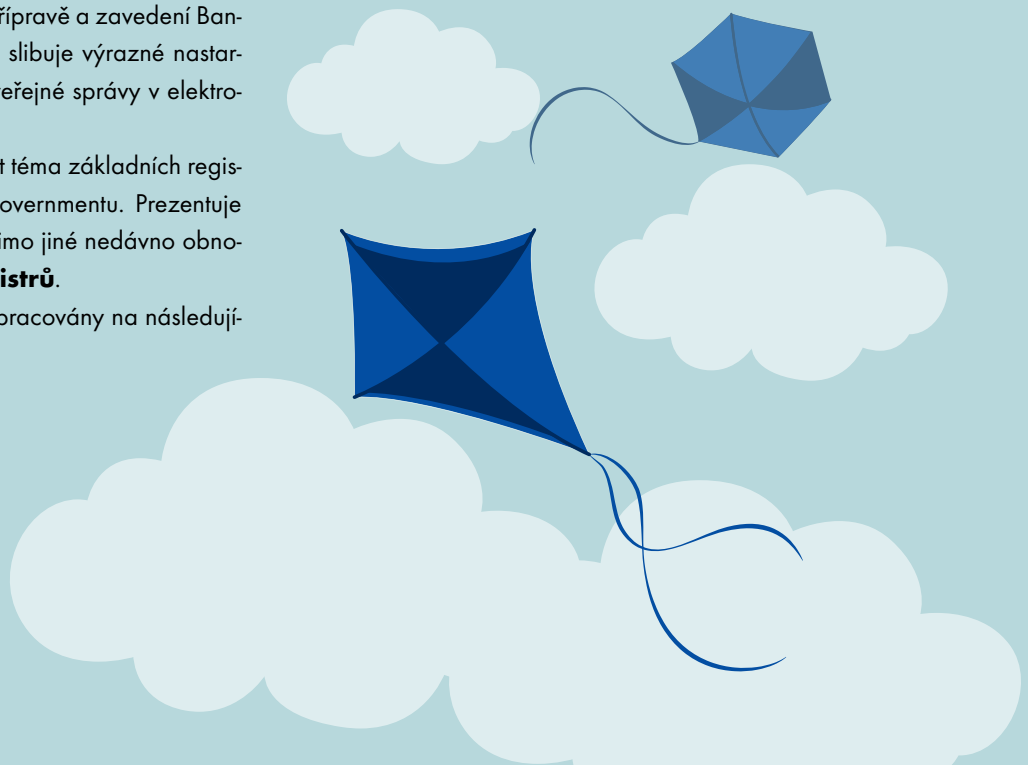
Další pozvánka směřovala k prezentaci ředitele odboru hlavního architekta e-governmentu Petra Kuchaře, který se věnuje tématu **mobilního prostředku**, který MV ČR vyvinulo jako identifikační platformu pro mobilní zařízení. Samozřejmě nevynechal ani eOP, kterých je nyní 300 000 aktivních. Související je i spolupráce s bankami, respektive Bankovní asociací na přípravě a zavedení BankID. Od jejího spuštění si MV ČR slibuje výrazné nastartování zájmu veřejnosti o služby veřejné správy v elektronické podobě.

Samozřejmě není možné vynechat téma základních registrů, které jsou pilířem celého e-governmentu. Prezentuje ředitel SZR Michal Pešek, který mimo jiné nedávno obnovil činnost rady **základních registrů**.

Všechny tyto prezentace jsou rozpracovány na následujících stránkách magazínu.

Zbývající prezentace najdete přímo na webové stránce konference. Obsahují informace k dalším důležitým a velice těsně souvisejícím tématům, jimž se věnují Igor Čermák z odboru kybernetické bezpečnosti MV ČR a **eGCloud**; Bohdan Urban, ředitel odboru provozu informačních technologií a komunikací MV ČR a aktuální fenomén, kterým jsou kvůli kovidu **videokonference**; Marek Beneš, nový ředitel odboru kybernetické bezpečnosti a koordinace komunikačních a informačních technologií seznámí s kyberútoky, kterým MV čelilo v době kovidové krize (včetně útoku na IS DS); Michal Kubáň z odboru hlavního architekta a téma otevřených dat.

Taková byla nabídka informací MV ČR na konferenci a většina z nich tvoří úvodní část tohoto čísla magazínu Egovernment.



# SOUHRNNÉ INFORMACE EGOVERNMENTU

***Ředitel odboru eGovernmentu MV ČR Roman Vrba uvedl, že se momentálně pracuje spíše na „backendových" záležitostech než na tom, co je vidět. Jedná se o produktové záležitosti, kdy je práce rozdělena na Portál veřejné správy a Portál občana, dále na Informační systém datových schránek, Czech POINT a RPP spolu s Katalogem služeb. V rámci svého vystoupení v Mikulově se věnoval především Portálu veřejné správy a Portálu občana.***

## Portál veřejné správy a Portál občana

Roman Vrba seznámil účastníky konference s tím, že na podzim bude spuštěna větší mediální kampaň, která bude pokračovat i v příštím roce. Mělo by se jednat o kampaň, která bude zahájena na sociálních sítích a následně se přesune na televizní obrazovky. Právě v době konání mikulovské konference se dodělávaly jednotlivé videoklipy a poslední přípravy. Měla by tak být zajištěna širší informovanost veřejnosti.


Základním propagovaným produktem bude **GOV.CZ** jako určitá vstupní brána a základní informace, jak se do Portálu občana dostat, jak si založit identitu, případně jak si založit datovou schránku a připojit se k ní, a to včetně podrobných videonávodů. V tomto smyslu není důležitý zvolený kanál, neboť podle slov Romana Vrby s datovou schránkou je možné zřídit identitu, naopak s identitou je možné zařídit datovou schránku.

PVS se nyní předělává a Roman Vrba ukázal novou verzi, která by měla být k dispozici v prosinci tohoto roku. Jak zdůraznil, do této verze bude již promítnut Katalog služeb. Nebude tedy nadále platit, že jednotlivé resorty musí aktualizovat konkrétní životní situace, ale data budou čerpána přímo z Katalogu služeb. Podrobnosti budou prezentovány ve vystoupení Šimona Trusiny (naleznete na str. 14).

V oblasti Portál občana se nyní hodně „ladí" backendové záležitosti jako příprava na masivní skokový nárůst uživatelů. K němu by mělo dojít díky změnám v oblasti datových schránek (například legislativní změny, nebo úpravy, o kterých v následujícím vystoupení hovoří Petr Kuchař (naleznete na str.12) a samozřejmě vstup bank (BankID) do oblasti identity a zajištění přístupu veřejnosti ke službám veřejné správy. Roman Vrba dále prezentoval jednotlivé možné služby, které by měly být na Portálu občana k dispozici již ke konci září.

## Informační systém datových schránek

Podle Romana Vrby se aktuálně vede diskuze o požadavku na neomezené velikosti příloh datových zpráv. Připustil, že se hledá vhodné řešení, ale je zřejmě nemožné, aby velikost takové přílohy přesahovala 50 MB. Varianta, která spíše přichází v úvahu, je pro větší soubory využít možnosti jejich upload na speciální úložiště. Další aktuální požadavek na zlepšení ISVS se týkal archivace. Ta by se však měla řešit pouze pro fyzické podnikající osoby, a to s největší pravděpodobností nikoli na úrovni DS, ale spíše na úrovni Portálu občana. Rozhodně se tedy nebude jednat o řešení, které by bylo k dispozici velkým firmám a právnickým osobám. Za velice důležité pak Roman Vrba považuje rozhodnutí, že by nemělo docházet k odstávkám ISVS, a to ani o víkendech.

## Katalog služeb

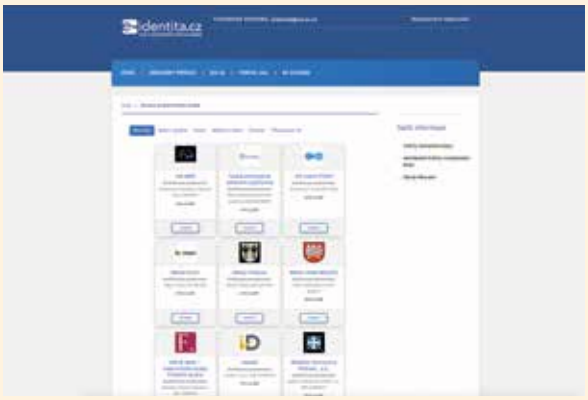
V závěru svého rychlého přehledu Roman Vrba považoval za důležité upozornit, že v případě prací na Katalogu služeb se nejedná „pouze" o samotný katalog, ale i o změnu zákona o přístupu k osobním údajům. Z toho pak vyplývá řada nových povinností především pro ohlašovatele agend. Stejně tak je součástí tohoto řešení tzv. jednotná digitální brána, která bude v prosinci funkční. Jedná se tedy o velký objem práce, který musí být dokončen před závěrem roku. Nicméně první ohlašovatelé již „přeohlašují" jednotlivé agendy tak, aby vláda mohla do 1. 2. 2021, podle plánu, rozhodnout o dalším postupu.

# NOVINKY V NÁRODNÍM IDENTITNÍM PROSTORU

***Ředitel odboru hlavního architekta eGovernmentu MV ČR Petr Kuchař se ve svém stručném vystoupení věnoval především té části identitního prostoru, která se týká poskytovatelů on-line služeb, poskytovatelů identitních služeb, a mezinárodní bráně.***

## POSKYTOVATELÉ ON-LINE SLUŽEB

V současné době se jedná přibližně o 50 portálů připojených k NIA. Na adrese **info.eidentita.cz/sep** je k dispozici jejich přehled. Jedná se tedy o portály, které jsou součástí identitní federace, a to v čele s Portálem občana. Vzájemně jsou propojeny tak, že mezi nimi funguje jednotné přihlášení (single sign on). Přihlášení na kterýkoliv portál je automaticky akceptováno těmi ostatními, není tedy, při přechodu mezi portály, nutno opětovné přihlašování.



## POSKYTOVATELÉ IDENTITNÍCH SLUŽEB

Jsou další důležitou součástí Národního identitního prostoru. Petr Kuchař prezentoval modelovou situaci, jak by seznam poskytovatelů mohl vypadat na jaře příštího roku, tedy v období, kdy bude připojena bankovní identita (místo doposud prezentovaného názvu BankID je nyní preferován pojem **bankovní identita**). To znamená, že k dnešním možnostem, kterými jsou eOP nebo jméno, heslo SMS, které nyní představují zhruba 360 000 identit, během podzimu přibude další, kterým je mobilní klíč e-governmentu. Zároveň je k dispozici mezinárodní brána, International ID Gateway, jejímž prostřednictvím připojujeme k našemu identitnímu prostředí jiné státy. V polovině roku 2020 získal certifikaci další prostředek StarCos (I.CA) a těsně před konferencí získal certifikaci prostředek MojeID (CZ.NIC), který je založen na USB tokenu. Tento stav bude platit do konce roku. Na jaře bude tedy spuštěna bankovní identita a to znamená, že současné statisíce uživatelů se skokově změní na miliony. Oprávněně je proto vhodné předpokládat i razantní zvýšení poptávky po on-line službách.

## MEP ISDS APLIKACE MOBILNÍ KLÍČ EGOVERNMENTU

Mobilní klíč funguje zhruba rok a používání je velice jednoduché a intuitivní. Jedná se o napárování mobilní aplikace pomocí běžného QR codu, přičemž následné přihlašování na stránky datových schránek probíhá mobilním klíčem. Právě s ohledem na jednoduchost a funkčnost tohoto přístupu bylo rozhodnuto, že nyní bude připojen k NIA. V současné době probíhá testovaní uvedené varianty. Výsledkem bude stejný postup, jaký byl doposud používán k přístupu do datových schránek, jen se bude tedy jednat o klíč k přístupu ke všem službám e-governmentu. Úroveň záruky takového přístupu bude značná. Podle situace existují tedy tři možné scénáře užití tohoto klíče. Pokud má uživatel profil v NIA, tedy pokud používá eOP, nebo jméno či heslo SMS, jednoduše si přiváruje další prostředek. Pokud je to uživatel systému DS, tak po přihlášení do DS si jedním tlačítkem převede tuto identitu do NIA. Pokud nemá ani to ani to, může si mobilní aplikaci registrovat osobně na Czech POINTu. Ostrý provoz aplikace MEP je očekáván na podzim.

# PRINCIPY BUDOVÁNÍ REFERENČNÍHO ROZHRANÍ PROPOJENÉHO DATOVÉHO FONDU

***Na Petra Kuchaře navazoval svým vystoupením Michal Pešek, ředitel SZR, který připustil, že se nacházíme v určitém mezním období, jež je charakterizováno novými možnostmi, které přináší eGovernment Cloud, a které dává možnost čerpání peněz z evropských fondů.***

Z pohledu SZR jsme dospěli do stádia, kdy máme téměř 3 miliardy transakcí od produkčního prostředí. Je ale nutné si uvědomit, že například díky zákonu o právu na digitální služby se začnou data ze základních registrů stále více využívat i v soukromoprávní sféře. Prvními, kteří tak začnou činit, budou na začátku roku 2021 banky. A SZR musí s takovým zvyšováním nároků počítat.

## CÍLE SZR V BUDOVÁNÍ REFERENČNÍHO ROZHRANÍ

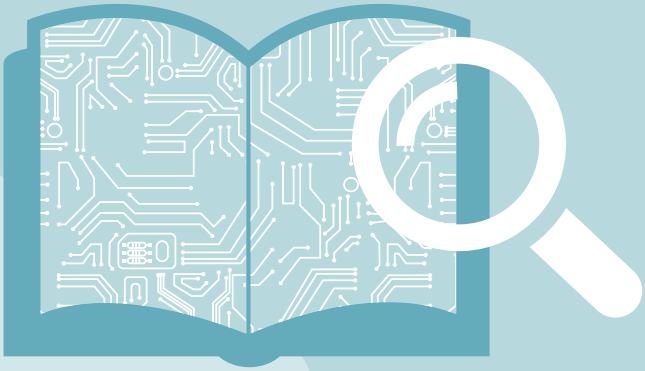
Vzhledem k tomu, že rozvíjející se e-government potřebuje stále rychlejší reakce a řekněme vyšší prostupnost dat, respektive transakcí, chce SZR zvýšit dostupnost a vybudovat referenční rozhraní. To by mělo fungovat od 1. 2. 2021. Mělo by také dojít ke sjednocení a standardizaci infrastrukturních systémů, tedy ke sdílení výkonu systémů, které má ve správě MV a SZR. Jako logické se proto zdálo využít primárně státní datová centra, je však nutné změnit přístup. Zatímco dnes je využívána tradiční vícevrstvá architektura, nyní přejdeme na model sdíleného výkonu. SZR proto hledá partnery v oblasti státní správy, respektive datových center, k co nejefektivnějšímu využití v rámci eGC.

## DOSAVADNÍ POSTUP

Byly vypracovány dopadové analýzy zákona o právu na digitální službu, aby bylo zřejmé, jaké změny a v jakých intervalech musíme implementovat. Jedná se o harmonogram až do roku 2025. Dále je vytvořena globální architektura propojeného datového fondu a nyní jsou připravovány principy referenčního rozhraní propojeného datového fondu. Tyto principy by měly ukázat, jaká legislativa tuto oblast nejvíce ovlivňuje a co je nutné realizovat s ohledem na plán rozvoje eGovernment Cloudu i na čerpání peněz.

Následně bude připravován prováděcí projekt (cca 6 měsíců) a další fází bude realizace. Od roku 2022 dojde na samotnou implementaci infrastruktury a migraci technologií.

Michal Pešek shrnul situaci konstatováním, že základní registry potřebují změnu technologií, která je vyvolána legislativou i aktuálními potřebami. To se zřetelně projeví už od prvního ledna příštího roku, kdy nás čeká sice postupný, ale trvalý nárůst uživatelů.



# KATALOG SLUŽEB A DALŠÍ ROZVOJ RPP

***Podle Šimona Trusiny z odboru eGovernmentu MV ČR má být tato prezentace pouze jakýmsi úvodem do problematiky Katalogu služeb. Pro podrobnější informace doporučil svoji odpolední prezentaci.***

## Co je Katalog služeb?

Vzniká na základě zákona o právu na digitální služby, a to v rámci ekosystému registru práv a povinností. Část těch údajů, které v něm jsou a budou vedeny, jsou referenční údaje, část nikoliv, což má své opodstatnění.

## Existují tři důvody, proč vzniká Katalog služeb:

### Evidence služeb veřejné správy a vytvoření kompletního inventáře toho, co vlastně dělá stát státem

Základní právní úpravou je v tomto případě zákon o základních registrech, který definuje výčet údajů, které se mají v rámci Katalogu vést. Zákon zároveň povinuje věcného gestora agendy – ohlašovatele, aby tuto svoji agendu inventarizoval a zveřejnil, jaké služby existují. Výstupem tak bude seznam služeb, které orgány veřejné moci poskytují klientům.

### Vytyčování plánu digitalizace

V tomto případě je stěžejním zákon o právu na digitální služby. Jedná se vlastně o plán digitalizace, který je velice konkrétní. Nastiňuje novou „pětiletku“, neboť zákon říká, že neexistuje-li k tomu nějaký rozumný (technický či jiný) důvod, tak by všechny služby, které budou obsaženy v Katalogu, měly být do pěti let digitální. Zákon rovněž pamatuje na situaci, kdy by ohlašovatel nesplnil svoji povinnost uvést službu v rámci Katalogu. I v takovém případě by měly být tyto služby nabízeny digitálně, pokud tomu něco nebrání. Klíčovou osobou je pro tuto situaci manažer ministerstva, nebo příslušného správního úřadu. On musí zajistit finanční prostředky i personální pokrytí ministerstva/správního úřadu kompetentními osobami, které digitalizaci zvládnou.

Výstupem budou digitální služby, a to v podobě, kdy je můžeme řešit (čerpat) z pohodlí domova. Současným výstupem bude skutečnost, že digitalizace bude řízená, bude prioritou vlády, tj. bude existovat jízdní řád toho, co, kdy a jak má být digitalizováno.

### Informování klienta o tom, jak využít tyto služby

V tomto směru mají vzniknout strukturované texty, které bude moci kdokoliv využívat, ať už z OVM, soukromoprávních uživatelů, či třetí strany. Nad těmito informacemi o službách bude možné stavět aplikace, které budou klienty provádět tím, jak danou službu řídit. Hlavním právním předpisem je zde zákon o svobodném přístupu k informacím. Ten povinuje změny, které proběhly ze zákona o právu na digitální služby, vystavovat. Vedle toho je zde důležité nařízení o jednotné digitální bráně, které ukládá členským státům Evropské unie, aby vytvořily popisy služeb, které jsou specifikovány v tomto nařízení, stejně jako popisy informací, které s těmito službami souvisejí. Hlavní tíha odpovědnosti leží na věcném gestorovi dané služby nebo agendy, který je schopen napsat uvedené texty. Protože se jedná o texty publikované navenek, je nutné, aby byly zpracovány přístupným jednoduchým jazykem (nikoli právnickým), a je rovněž nutno tyto informace přeložit. Výstupem jsou tedy srozumitelné informace jak v českém, tak anglickém jazyce.

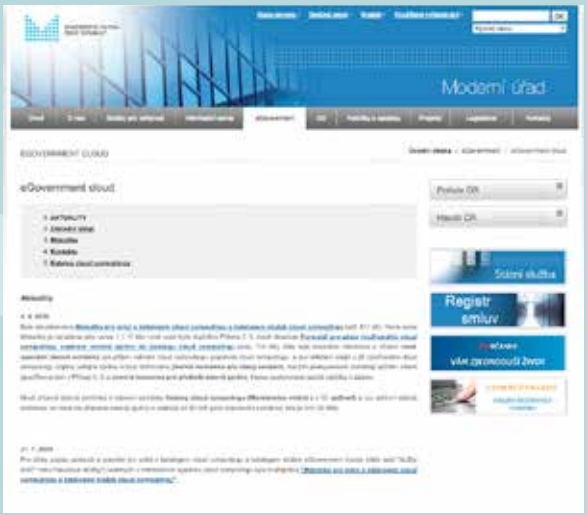
# EGOVERNMENT CLOUD

***Základní informaci k aktualitám v oblasti eGovernment Cloudu podal na konferenci Igor Čermák z odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií MV ČR.***

K 1. 8. 2020 totiž došlo k nabytí účinnosti některých odložených ustanovení zákona o informačních systémech veřejné správy (ZoISVS), které byly novelizovány v zákoně o právu na digitální služby. Byl tedy zaveden koncept Cloud Computingu a katalog Cloud Computingu. Nyní je dokončován legislativní proces vydání vyhlášky o údajích vedených v katalogu Cloud Computingu. Předpokládaný termín vydání vyhlášky je 1. 10. 2020. Nicméně, s ohledem na kontinuitu všeho, co se týká nabídek a poptávek Cloud Computingu, připravilo MV ČR a k 31. 7. 2020 vydalo Metodiku pro práci s katalogem Cloud Computingu a katalogem služeb Cloud Computingu. V těchto metodikách je popsán postup, který je od 1. 8. 2020 využíván, a to zejména vzhledem k poskytovatelům CC, tedy pro zápis nabídky či poptávky. Zápis nabídky je totiž nutnou podmínkou pro možnost využívání služeb CC pro orgány veřejné správy (pokud již příslušným orgánem nebyl Cloud Computing využíván před 1. 8. 2020). Přílohou této metodiky jsou rovněž bezpečnostní kritéria formulována ve spolupráci s NÚKIB.

Z uvedeného vyplývá, že nyní bylo připraveno základní prostředí pro možnost využívání CC po 1. 8. 2020 tak, že pro nové nabídky je potřeba, aby poskytovatel zaslal žádost o zápis do katalogu CC MV ČR. Po posouzení, zda nabídka splnila veškeré náležitosti, je zapsána do katalogu. Podobně může každý orgán veřejné správy zaslat poptávku na CC, pokud takové poptávce nebudou ještě existovat nabídky. Poskytovatelé následně mohou reagovat.

Veškeré tyto informace jsou podrobněji popsány na webových stránkách ministerstva v sekci pro eGovernment Cloud:
https://www.mvcr.cz/clanek/egovernment-cloud.aspx



# VIDEOKONFERENČNÍ ŘEŠENÍ MV ČR

***Ředitel odboru provozu informačních technologií a komunikací MV ČR Bohdan Urban připustil, že na začátku koronavirové krize mělo MV ČR, oproti ostatním resortům a úřadům, dvě podstatné výhody. Především již byl ve výstavbě videokonferenční systém Policie ČR a zároveň byl realizován projekt VCI pro OAMP, který byl financován z programů EU. V tomto okamžiku se MV ČR tedy podařilo vytvořit funkcionalitu videořešení, která je dostupná jak v rámci resortní sítě, tak i pro policii ČR a Hasičský záchranný sbor (end to end šifrování).***

Nyní je tedy MV ČR schopno poskytovat videokonferenční služby jak uvnitř sítě MV, tak i z vnějšku. Pro komunikaci jsou v tomto smyslu využívány dedikované aplikace, ale je možné provozovat i přes webové prohlížeče rovněž vzdálené videokonference. V místech, kde v rámci resortu byl již zaveden standard Ip Telefonie, je tak možné připojit účastníky i audio, stejně tak je možné připojit účastníky i z veřejné telekomunikační sítě.

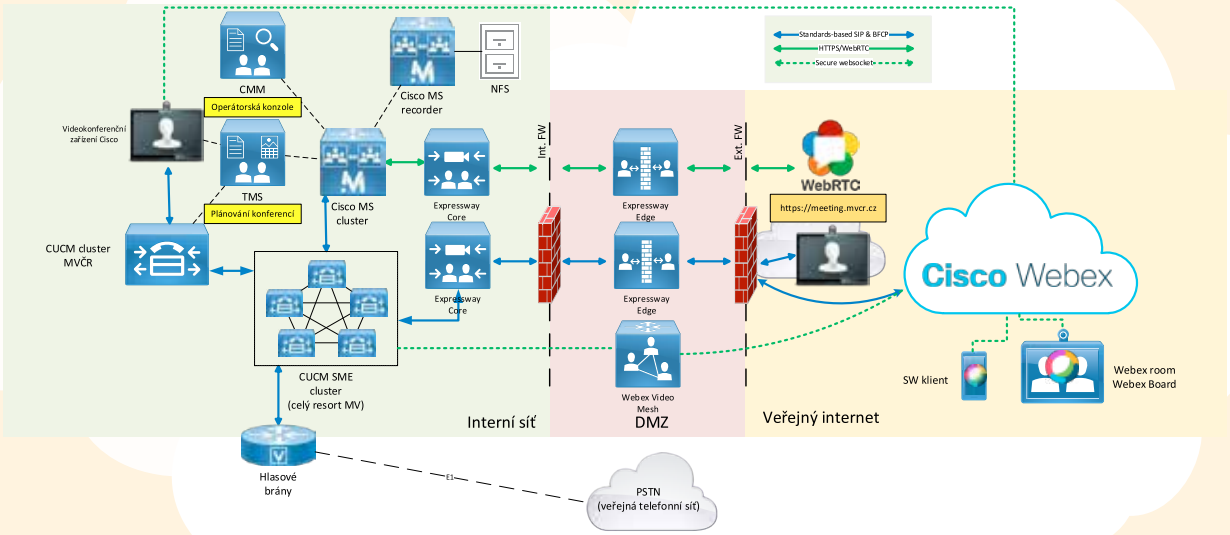
Při výstavbě videokonferenčního řešení se MV ČR rozhodlo postupovat cestou on premise. MV ČR má tedy jednotlivá zařízení a obecně celé videokonferenční prostředí plně pod kontrolou. Používá vlastní síťovou infrastrukturu, která je pod kompletní dohledem a patřičně zajištěna smlouvami. Toto řešení přináší výhody stability (v případě přetížení internetu, nebo jiných krizových scénářích), zároveň je toto řešení integrováno na stávající realizované projekty v oblasti iP Telefonie. Využívá tedy síťové prostředí, které je v rámci MV dedikováno pro multimediální komunikaci.

Vedoucí oddělení realizace komunikačních systémům MV ČR **Roman Martiňák** představil blokové schéma ON-PREMISE videokonferenčního řešení. Jak bylo řečeno, je plně v prostředí MV ČR a vychází ze zkušeností z provozu videokonferenčního řešení PČR. Snahou MV je pojmout celou záležitost jako hybridní řešení tak, aby bylo možné do ON–PREMISE infrastruktury zakomponovat ty nejlepší služby, které nabízí CISCO WEBEX CLOUD. Jedná se především o ovládání konferenčních jednotek pomocí mobilních zařízení, dále možnost malování a sdílení obsahu, možnost interaktivních školení, velkokapacitních vzdálených schůzek a možnost jmenovek účastníků schůzky.

V dalších krocích se uvažuje o tzv. duální registraci, tzn. že konkrétní videokonferenční jednotky by byly registrovány jak ve vnitřním prostředí MV ČR, tak na Webex Cloudu, a tedy i v případě výpadku jednoho z těchto prostředí by byla i nadále zajištěna konektivita. Patrně největším přínosem cloudového řešení je pak možnost registrace desítek zařízení v řádech minut kdekoliv, kde je připojení k internetu.

Bohdan Urban v závěru ještě doplnil, že směřujeme k udržení/zvýšení bezpečnosti provozu videokonferencí a snahou MV je dostat do oběhu ještě několik mobilních videokonferenčních jednotek.

**Cíl: hybridní řešení**



MĚSTO
POD PALCEM

Powered by ETERNAL

# Město pod palcem

## RYCHLÁ A DYNAMICKÁ KOMUNIKACE S OBČANY

Město pod palcem je nejucelenější řešení pro komunikaci mezi městem a občany. Není to jen mobilní aplikace, ale **komplexní systém, který funguje jako komunikační platforma a agregátor informací.**


HLAVNÍ DŮVODY

## Proč si pořídit naše řešení

+ Mobilní aplikace je snadno identifikovatelná a vyhledatelná občany – respektuje design města a nese jeho název
+ Zcela modulární – je na Vás, zda si vyberete všechny moduly a funkce, nebo jen některé z nich
+ Podporuje správu podnětů občanů
+ Umožňuje informování občanů prostřednictvím SMS
+ Zahrnuje vlastní redakční systém – pro případnou potřebu pořízení a správu nového obsahu aplikace
+ Podporuje integraci na provozní IT systémy města – využívá obsah, se kterým již město pracuje

DOPRAVA · ANKETY · JÍZDNÍ ŘÁDY · MAPY · FOCENÍ ZÁVAD · KALENDÁŘ · NOTIFIKACE · KONTAKTY

PRŮVODCE · BLOKOVÉ ČIŠTĚNÍ · KAMERY · ŽIVOTNÍ SITUACE · ÚŘAD · PŘIHLÁŠENÍ · KRIZOVÁ SMS · ZASÍLÁNÍ SMS

**NAPIŠTE SI O NABÍDKU NEBO NÁM ZAVOLEJTE**


+420 736 606 350

mestopodpalcem@eternal.cz


www.mestopodpalcem.cz

# Studio Egovernment

elektronizace veřejné správy

# 8. 9. 2020

***„Vysílání" našeho nepravidelného STUDIA EGOVERNMENT bylo tentokráte výjimečné hned v několika aspektech. Především jsme jej „nevysílali" z našeho obvyklého studia na Barrandově, ale přímo z konferenčního pódia na zámku Mikulov. Byli jsme tak obklopeni zarouškovanými účastníky konference e-government 20:10. Neplatilo to ale pro všechny účastníky STUDIA, neboť s ohledem na hygienická opatření nemohli zástupci MV ČR na konferenci přijet. A tak jsme se s nimi museli propojit videokonferenčně. V Mikulově tedy seděli na pódiu Zdeněk Zajíček, prezident ICT Unie, a Ivan Bartoš, předseda výboru pro veřejnou správu a regionální rozvoj PSP ČR. Na velké projekční ploše pak byli vidět náměstek ministra vnitra Jaroslav Strouhal a vládní zmocněnec pro IT a digitalizaci Vladimír Dzurilla.***

Naše debata se odvíjela od letošních výsledků průzkumu EGDI (e-government Development Index) OSN. V porovnání, které je realizováno ve dvouletém cyklu, jsme letos mezi 193 hodnocenými zeměmi obsadili **39. příčku**. To možná nevypadá oslnivě, ale znamenalo to, po dlouhém, několikaletém poklesu, poprvé **vzestup, a to o 15 pozic**. Byla to jen náhoda, nebo je možné považovat tento posun za trend, který by mohl v příští letech pokračovat?

Náměstek ministra vnitra **Jaroslav Strouhal** se domnívá, že se bezpochyby jedná o trvalý trend. Česká republika podle jeho mínění učinila za poslední roky na poli e-governmentu řadu důležitých kroků. Tento postup byl sice pomalý, za což bylo ministerstvo vnitra často kritizováno, ale jak náměstek Strouhal zdůraznil, bylo potřeba dát dohromady schopné lidi, peníze a hlavně zákony. Zákony nyní máme. Zákon o právu na digitální služby, často zmiňovaný na mikulovské konferenci, je k dispozici. Na něj navazuje rozsáhlá novela agendových zákonů, která je v současné chvíli v Poslanecké sněmovně. Dá se tedy říci, že to jsou kroky, které onen zmiňovaný trend nastartovaly, a lze předpokládat, že je nyní budeme vylepšovat.


Jaroslav Strouhal rovněž připomenul několik let starou aktivitu prezidenta ICT Unie, kterou byla **iniciativa 202020**. Její podstatou bylo aktivovat budování e-governmentu v ČR tak, abychom v hodnocení EGDI byli do roku 2020 na dvacátém místě. To se sice nepovedlo, ale vzestup byl nyní odstartován. Je tedy potřeba požádat o trpělivost, ale bezpochyby je posunutí ČR na dvacátou pozici reálné, a to právě například díky připravovanému Bank ID a dalším nástrojům, které jistě napomohou digitalizaci. Je samozřejmé, že to nejde bez spolupráce s ostatními úřady, a je zřejmé, že změnit myšlení některých lidí jde pomaleji, ale trend je podle náměstka Strouhala nastaven správně.

Vládní zmocněnec pro IT a digitalizaci **Vladimír Dzurilla** je přesvědčen nejen o tom, že naše posouvání v žebříčku bude trend, ale protože bez digitální identity nejsou digitální služby, je přesvědčen, že se tyto služby nyní rozvinou právě na základě požadavku samotných lidí–klientů. Zdůraznil, že máme k dispozici jak zákon, tak harmonogram, a dokonce by neměly chybět ani peníze. Nyní by tedy náš posun měl být skutečně rychlejší.

Předseda výboru pro veřejnou správu a regionální rozvoj PSP ČR **Ivan Bartoš** uvedl, že byly schváleny tři důležité zákony a je velice dobře, že jsme to takto zvládli. Věří tedy, že jsme si „vyšlápli" dobře, ale radovat bychom se měli až v okamžiku, kdy budou konkrétní služby skutečně uvedeny do praxe. Koronavirus podle jeho slov ukázal, jak špatně sdílíme data (MPSV například nedokáže použít data z FÚ atp.) Přitom je zřejmé, že řada agend může být realizována nikoli v papírové, ale elektronické podobě. Bylo by tedy vhodné podívat se na jednotlivé procesy, které odpovídají oněm službám, a co nejvíce zjednodušovat. Mělo by dojít k propojování jednotlivých agend tak, aby se nám zjednodušil život. Jako příklad uvedl situaci, kdy by, je-li možné se prokázat OP na poště, neměl existovat důvod, proč by nebylo například možné si zde vyzvednout zaslaný řidičský průkaz místo toho, abych musel osobně chodit na vzdálený úřad. Stejně tak považuje za zbytečné prokazování se dvěma doklady (OP a ŘP), když by mohl stačit jeden z nich (data by měla být sdílena). V samotné elektronizaci veřejné správy by tedy nemělo jít o pouhou digitalizaci starých procesů, ale o modernizaci a zjednodušování těchto procesů.

Prezident ICT Unie **Zdeněk Zajíček** uvedl, že zmiňovanou **iniciativou 202020** chtěli upozornit právě na naše zbytečně nízké umístění v jednotlivých žebříčcích. Je jisté, že umístění samo o sobě nevypovídá o úrovni služeb v konkrétním státě. Jde tu ale o určitou míru naší hrdosti a zároveň i o úroveň marketingu, který stát navenek realizuje. Konkrétně 50. a vyšší umístění v mezinárodním hodnocení bylo rozhodně nepříjemné. I proto ona výzva, nebo cíl, že bychom se do roku 2020 měli posunout na 20. místo. Nepodařilo se to do roku 2020. Jsme 39. Zdeněk Zajíček proto znovu vyzval, abychom udělali všechno pro to, aby ČR za dva roky, až vyjde další hodnocení EGDI, na oné dvacáté příčce byli. Je to podle jeho mínění reálné. Je přesvědčen, že musíme mít takové cíle a vložit veškerou energii do jejich splnění. Nyní jsou podle něj všichni zainteresovaní nastaveni tak, že chceme spolupracovat a posouvat se. Ta realizace sice musí ležet na straně VS, neboť to jsou zadavatelé, ale bylo dobré, kdyby soukromý sektor dostal větší prostor pro spolupráci s VS. Bank ID je dobrým příkladem toho, kdy soukromý sektor bude poskytovat služby, které stát akceptuje, a je to inovace, kterou potřebuje a která je přínosná pro stát i jeho klienty. I proto připomenul **DNA – Digitální národní aliance**, která je hledáním platformy pro komunikaci potřeb VS a spolupráce se soukromým sektorem, protože taková spolupráce má, podle jeho mínění, benefity, které výrazně převyšují možná rizika.

**Vladimír Dzurilla** je přesvědčen, že ve chvíli, kdy každý, kdo bude chtít, bude mít přístup ke službám státu, bude zcela automaticky tlačit na jejich kvalitu. Zároveň připustil, že za naším umístěním je i **špatný reporting**. I proto vyzval odborné asociace, aby v propagaci e-governmentu státu pomohly. Aby se doplňovaly nejen samotné služby, ale i informace o nich.

Že o jednotlivých službách, které jsou k dispozici, ví málo lidí, připustil jako problém i náměstek **Strouhal**. Bylo to zřejmé v rámci první vlny omezení v souvislosti s COVID – 19, kdy občané teprve objevovali, co a jak už funguje. Je

to dáno i **chybějící propagací**. Vždyť poslední masivní kampaň se týkala datových schránek a Czech POINTů. MV ČR proto nyní připravuje **novou kampaň**, která by měla být realizována na podzim a bude stávající možnosti a služby přibližovat.

**Ivan Bartoš** ale vidí problém v tom, že i kdyby lidé o existujících službách již věděli, jsou tyto služby docela složité na obsluhu. Kromě subjektivního vnímání - designu jde i o změnu pohledu především na sdílení dat mezi resorty. O běžném občanovi – zaměstnanci se dá říci, že o něm FÚ má k dispozici veškerá potřebná data pro daňové přiznání. Ve Skandinávii běžně tamní FÚ vypočítá a zašle občanům návrh jejich daně právě na základě zřejmých a známých údajů. Ti jej mohou akceptovat a pouze v případě, že s ním nesouhlasí, předkládají vlastní daňové přiznání. To jsou přesně formáty služeb, které si Ivan Bartoš slibuje od masivní digitalizace služeb a procesů, která musí nastat.

**Zdeněk Zajíček** souhlasil s tím, že se jedná o změnu paradigmatu, kdy se na veškeré tyto změny uvnitř VS musíme dívat **očima klienta**. To zde nebylo zvykem. V oblasti využití e-shopů se ČR pohybuje zhruba na třetím místě v Evropě. Naši občané tedy nemají žádný blok vůči

využívání e-služeb. Pravdou ale je, že soukromý sektor má k potřebám klienta podstatně blíž, než mohou mít úřady, a dokáže jim lépe nabídnout, co odpovídá jejich potřebám. I proto je spolupráce veřejné správy a soukromého sektoru zcela přirozená a důležitá. Podle Zdeňka Zajíčka by se mělo jednat o **cílený program spolupráce**, jehož výsledkem bude daleko snazší oslovení klientů.

S tím souhlasil i **Vladimír Dzurilla**. Když budou jednotlivé služby VS prezentovány i komerčními partnery, bezpochyby poroste tlak na vznik dalších služeb, stejně jako na jejich „přívětivost" či uživatelský komfort. Právě sestavovaný Katalog služeb VS je pak již jen nástroj, který bude brán jako samozřejmost.

**Jaroslav Strouhal** v souvislosti s Katalogem uvedl, že každé ministerstvo, každý úřad si jednoznačně určí, kterou agendu chce digitalizovat. V návaznosti na státní rozpočet pak bude tuto digitalizaci schvalovat vláda. Zároveň zdůraznil, že na MV ČR už tři roky běží procesní modelování agend, které sleduje myšlenku **klientsky zjednodušit** a zpřístupnit stávající procesy. Ze strany MV ČR bude uplatňován tlak na to, aby docházelo k onomu zjednodušování, ale jedná se především o **odpovědnost jednotlivých resortů**.

## REPORTOVÁNÍ

V rámci diskuze jsme se ještě jednou vrátili ke zmíněnému problému s reportováním našich výsledků na mezinárodní úrovni. **Zdeněk Zajíček** je přesvědčen, že řada států nemá například základní registry a sdílení dat na takové úrovni jako my. Tuto výjimečnost však **nedokážeme** v žádném hodnocení **zviditelnit**. Dá se tedy říci, že řada zemí, které jsou v žebříčku před námi, má skutečně dobře nastaven marketing a my jej naopak nezvládáme. I v tomto směru vidí prostor pro spolupráci státu a komerčního sektoru. Jsme nyní v situaci, kdy díky Katalogu služeb můžeme udělat ve veřejné správě pořádek. Jakmile bude Katalog hotov, mohou jednotlivé životní situace tvořit privátní subjekty, neboť jak bylo již řečeno, mají ke klientovi blíž. Mají s ním nějaký vztah, který je provázaný právě s onou životní situací, jsou tedy schopné definovat jeho potřeby.

Shoduje se s ním i **Vladimír Dzurilla** a jako precedens úspěšného převzetí něčeho, co bylo vyvinuto komerčním sektorem a úspěšně implementováno do veřejné správy, připomenul **bankovní identitu** a **chytrou karanténu**. Podle jeho slov je důležité, aby ve veřejné správě byli **lidé**, kteří **jsou schopní takové spolupráce**, a zároveň, abychom měli **legislativu**, která to umožňuje. V souvislosti s reportováním uvedl, že jsme skutečně specialisté, protože to, co funguje, si často sami dokážeme pohanit, ale přitom **se neumíme chlubit** svými výsledky. Problém tedy vidí v tom, že nejsou vytahovány vzory ze státní správy. Je potřeba daleko více propagovat nejen jednotlivé kroky, ale i osoby, které je reprezentují a realizují.

Náměstek ministra vnitra **Jaroslav Strouhal** s uvedeným souhlasil a doložil to známým faktem, že média prodávají špatné zprávy a s tím se těžko bojuje. Hodí se ale podle jeho mínění poděkovat. Pokud jde o **MV ČR**, má pocit, že se zde podařilo vybudovat velice **zajímavý a kvalitní tým lidí**, stabilizovat lidský potenciál na ministerstvu, nastavit spolupráci se soukromým sektorem, a to vše považuje za velice důležité a příslibné pro budoucí výsledky.

V souvislosti s naším hodnocením jsme se rovněž zeptali všech čtyř pánů, zda se skutečně domnívají, že ČR může, například i díky zlepšenému marketingu, být v příštím hodnocení EGDI – 2022 na oné vysněné dvacáté příčce. Bez váhání se shodli, že ano. **Plán na příští dvouletku je tedy jasný, uchvátíme dvacáté místo.**

# KATALOG SLUŽEB

***O Katalogu služeb se v současné době velice často hovoří jako o zásadní záležitosti pro další vývoj českého e-governmentu. Díky němu bychom mohli získat přehled o jednotlivých službách veřejné správy, zjistit, které jsou podstatné, a možná i to, které jsou zbytečné, a najít způsob oceňování výkonů těchto služeb. Ředitele odboru eGovernment MV ČR Ing. Romana Vrby jsme se proto zeptali, co přesně si je možné a vhodné pod označením Katalog služeb veřejné správy představit?***

Katalog služeb veřejné správy (VS) vzniká primárně na základě zákona o právu na digitální služby. Současně je ale navržen tak, aby jednotlivým ministerstvům a dalším ústředním správním úřadům pomáhal plnit či přesněji sjednotit část jejich informačních povinností.
Katalog služeb tak bude sloužit k evidenci služeb, poskytování informací o jednotlivých službách a k jejich digitalizaci. Tuto evidenci služeb je možné si představit jako generální inventarizaci služeb poskytovaných jednotlivými úřady externímu klientovi. Žijeme v jednadvacátém století, ale stále nemáme jednotný pohled na to, co pro nás stát dělá – jaké služby, kdo a jakým způsobem poskytuje. V základní podobě to bude služba spíše pro stát, aby tuto znalost získal a poskytování služeb i jejich digitalizaci mohl lépe řídit.

**Předpokládám, že inventarizací to ale nekončí.**
Nekončí. Inventarizace je předpokladem pro další dva kroky: digitalizaci služeb a jejich srozumitelné popsání pro klienty. Z hlediska digitalizace je důležité rozdělit tyto služby na jednotlivé úkony neboli transakce, ke kterým musí mezi úřadem (orgánem veřejné moci) a klientem dojít. Pro každou transakci pak budeme z evidence vědět, jakými prostředky (obslužnými kanály) ji lze dnes realizovat. Například pro výpis bodového hodnocení řidiče bude evidován Portál občana, datová schránka nebo Czech POINT.

**Budoucí forma znamená, že Katalog služeb ještě není hotový?**
Z hlediska jeho naplňování jsme spíše na začátku, ale záleží, o jakém z uvedených bodů se bavíme. Každopádně, když se vrátím k té digitalizaci, jednotlivé rezorty dle zákona o právu na digitální služby mají povinnost všechny služby, kde to dává smysl, digitalizovat do čtyř let od schválení plánu digitalizace vládou. A k tomu má dojít do 1. února 2021.

**Jak se bude určovat, kdy to dává smysl?**
To bude na každém z rezortů. Své rozhodnutí bude ale muset odůvodnit. V zásadě jde o dva případy. Prvním je hledisko technických možností, například nemá smysl digitalizovat službu, pokud se v rámci žádosti sbírají biometrické údaje. Druhým typem je počet uživatelů. Pokud existuje služba, která má omezený počet klientů, není ekonomické ji (minimálně nyní) digitalizovat.
Zde si dovolím malou odbočku – řadu služeb lze již dnes vyřídit, nebo alespoň o ně zažádat, pokud máte datovou schránku či uznávaný elektronický podpis, ale málokdo to používá. Nechci se teď bavit o tom, čím je to způsobeno. Rozhodně ale platí, že je třeba zlepšit informovanost našich klientů, a k tomu má sloužit právě třetí bod katalogu služeb.

**A to bude poskytování informací o službách.**
Přesně tak. Pro všechny služby, kde je na začátku rozhodující iniciativa klienta (služby iniciované klientem), mají vzniknout textové popisy. Mají být psané srozumitelným popisem, budou jednotně strukturované a budou dostupné na novém Portálu veřejné správy, který plánujeme spustit v polovině prosince.
Zde je také důležité upozornit, že popisy se (po přeložení) využijí i pro plnění informační povinnosti dané nařízením EU o jednotné digitální bráně.
Tím to ale nekončí. Protože si uvědomujeme význam vznikajícího datasetu, snažíme se i o jeho co největší šíření mezi další zájemce. Proto bude publikovaný formou otevřených dat, a hlavně k němu vytváříme rozhraní (API), které bude dostupné nejen pro úřady (orgány veřejné moci), ale i pro další zájemce - soukromý sektor, neziskový sektor, prostě pro kohokoliv.

**K čemu konkrétně to pak povede?**
Pokud se na to budeme dívat v krátkodobém horizontu, bude to jednoznačně jeden ze způsobů, jak zlepšit infor-

movanost našich klientů. V horizontu několika let je stěžejní digitalizace. Stát si udělá doma pořádek, rozhodne se, co, kdy a jak bude digitalizovat, a podle zákona by nejpozději během roku 2025 měly všechny služby, kde to dává smysl, existovat i v digitálu.

Na Ministerstvu vnitra si s pokorou říkáme, že vlastně nelze odhadnout, k čemu všemu může být dataset dobrý, byť samozřejmě máme řadu případů užití, jako je benchmarking, digitalizace jednotlivých agend a úřadů, optimalizace poskytování služeb v území, odstraňování duplicit či zbytečných služeb, jako jsou ohlašovací povinnosti základních údajů vedených v základních registrech atd. Když ale mám použít nějakou analogii, může to být podobné jako s daty o jízdních řádech: než vznikly centrální, všichni jsme s tím dokázali žít a hledat v jízdních řádech dle lokality nebo typu prostředku. Dnes, po centralizaci, kdy vyhledáváme pouze v jedné aplikaci, nedokážeme pochopit, jak jsme mohli fungovat bez nich.

**Rozumím přínosu pro stát. Jak to ale bude se službami poskytovanými obcemi?**

Zde je důležité rozumět dělení působnosti v České republice. Ve stručnosti, pokud jdete na úřad, službu vám poskytuje buď v rámci výkonu státní správy, nebo přenesené působnosti, kdy stát deleguje poskytování určité služby na samosprávu (jde o obce a kraje), anebo o výkon samostatné působnosti. S evidencí služeb v rámci prvních dvou možností nebude problém. V případě služeb poskytovaných samosprávou k nim musí existovat zákonné zmocnění, tedy agenda, jinak je dle platné legislativy není možné evidovat.

Znovu zopakuji, že kdokoli bude moci data přebírat, tedy i obce, a zobrazovat na svých webových stránkách, případně v mobilní aplikaci. Zobrazení na webových stránkách bude o to snazší, že vydáme jako open source i vizualizační komponentu, takže připojení a zobrazování dat bude opravdu hračka.

**Jaká bude propagace?**

Propagace zatím probíhá uvnitř státu. Jde o to, aby na každém ministerstvu pochopili význam celého, protože pokud bude katalog prázdný, bude k ničemu. Evidencí služeb vlastně jednotlivá ministerstva vytváří produkt, o který se (nejpozději) od teď budou muset starat a neustále jej zlepšovat. Digitalizací to totiž nekončí, ale spíše začíná, protože stále je co zlepšovat a na co reagovat. Ale zpátky k Vaší otázce, přiznáváme, že propagace je něco, co neumíme a musíme se to naučit. Každopádně na podzim bude spuštěna velká reklamní kampaň a pevně věřím, že se její výsledky projeví.

**Na konferenci v Mikulově jsme hovořili o nutnosti těsné spolupráce státu se soukromým sektorem. Jak bude vypadat v této oblasti?**

Naše data/řešení budou od počátku otevřená i pro soukromý sektor. Co se týče přímé spolupráce, dokáži si představit, že podobný katalog by dobrovolně mohl vznikat i nad službami poskytovanými soukromou sférou a náš katalog by se tak zajímavě rozšířil, ale nechci moc předjímat.

**Zní to zajímavě. V podstatě se jedná o základ oné uživatelsky přívětivé veřejné správy, která byla tématem kulatého stolu v Mikulově. Bude ale realita skutečně taková?**

Již jsem o tom trochu mluvil. Někdo to musí vyplňovat a udržovat aktuální, jinak to vše bude k ničemu. A je fér říci, že zákon o právu na digitální služby pro úřady znamená řadu nových povinností, ale nedošlo k navýšení personálních kapacit ani k přidělení finančních prostředků na jeho implementaci.

Ohledně digitalizace služeb navíc platí, že evidovat je a naplánovat (časově) jejich digitalizaci je jedna věc, ale správně a včas ji uskutečnit je úplně jiná problematika. Doufám, že nikoho neurazím, když podotknu, že umět digitalizovat a navrhovat věci opravdu uživatelsky přívětivě je věc, kde mají rezervy i podobně velké organizace ze soukromého sektoru.

**Jaký je tedy jízdní řád – harmonogram?**

Evidencí služeb to začíná, a abychom v lednu mohli jít s materiálem na vládu, musí být v polovině listopadu hotová. Jakmile bude služba evidována, mohou vznikat její popisy. Zákon stanoví termín pro jejich vznik nejpozději do 1. 2. 2021. My bychom ale byli rádi, kdyby jich už velká část vznikla dříve, k termínu spuštění nového Portálu veřejné správy, tedy v polovině letošního prosince. Ohledně plánu digitalizace je to podobné jako s evidencí, měl by být stanoven kolem poloviny listopadu, protože ten bude vládu zajímat kvůli finančním dopadům a prioritizaci vybraných služeb.

# GORDIC na konferenci e-government 20:10 – naučme se více naslouchat potřebám uživatelů

***První vlna pandemie Covid-19, kterou jsme si před několika měsíci prošli, ovlivnila nejen životy nás všech, ale také více upozornila na nutnost uspíšení digitalizace agend. Ze dne na den jsme ztratili osobní kontakt s úřady a většina komunikace se přesunula do online prostředí. Jak ale praví známé pořekadlo, „všechno zlé je pro něco dobré". Mimořádná situace nám ukázala, že dokážeme být daleko flexibilnější, než jsme si na první pohled mysleli. Věci, které jsme dříve řešili několik měsíců a možná i let, jsme najednou zvládli v horizontu týdnů. Mimořádná situace měla také vliv na priority mnohých úřadů.***


I na to se zaměřili bratři Marek a Michal Řezáčovi ze společnosti Gordic ve svém vystoupení na 12. ročníku konference E-government v Mikulově. *„Řekli jsme si, že to nejlepší, co teď můžeme dělat, je probírat s jednotlivými zákazníky, jak v současné době jejich pracoviště fungují. V našem rozsáhlém průzkumu jsme zjistili, že úřady vnímají digitalizaci často odlišně než stát nebo IT firmy,"* vysvětluje ředitel pro strategický rozvoj a IoT **Marek Řezáč**. Během svojí prezentace na výroční konferenci apeloval na organizace státní správy, samosprávní celky i dodavatele digitálních technologií, aby vnášeli do otázek digitalizace více pohledy koncových uživatelů.

Pokračovatelé rodinné firmy Gordic taktéž upozornili na nutnost zjednodušení komunikace mezi občanem a úřady. Podle nich města sice provozují Portál občana, nevyužívají ho ale zdaleka tak efektivně, jak by mohla. *„V mnoha případech je odkaz na Portál občana na jejich webových stránkách těžko dohledatelný. Navíc jsou formuláře natolik složité a psané formálně, že člověk bez znalosti legislativy není schopen jim porozumět. Je proto nejenom na vládních institucích, ale také na nás – dodavatelích, abychom se zaměřili na skutečné přínosy pro občany a úřady,"* dodal Marek Řezáč.

Nutnost zjednodušení komunikace mezi občanem a úřady potvrzuje také ředitel pro strategický rozvoj a kybernetickou bezpečnost **Michal Řezáč**. Podle něj musí být digitální služby veřejné správy z Portálu občana snadno dosažitelné a uživatelsky stejně přívětivé jako v komerční oblasti. Na konferenci představil mimo jiné možnosti Portálu občana GINIS. *„Chceme, aby se díky responzibilitě a designu aplikace i samotných formulářů lidé cítili komfortně, ať už si chtějí vyřídit své záležitosti z mobilu, počítače, nebo tabletu."*

Všechny tyto náležitosti splňuje Portál občana GORDIC. Díky němu lze efektivně komunikovat s úřady online. Nástroj umožňuje například platit za veřejné služby přes mobilní telefon platební kartou, řešit životní situace, zvládnout žádosti o dotace atd. Navíc v době, kdy je kvůli pandemii ohrožena možnost návštěv na úřadech, je Portál občana důležitým prvkem pro zajištění nepřetržité komunikace mezi občanem a veřejnou správou.

## Portál do světa digitálních služeb

Pořídíte-li si například mobilní telefon nebo televizi od značky, která většinu kapacit soustředí do vývoje a mezi prioritami má i možnosti integrace (propojení) se systémy třetích stran, máte jistotu, že získáváte špičkový produkt. Totéž platí i pro nástroj Portál občana GINIS od společnosti GORDIC, jehož prostřednictvím poskytují města a kraje občanům širokou škálu digitálních služeb.

Zjišťování úředních hodin, čekání ve frontách, listování ve formulářích a žádostech, nutnost platit na přepážkách pokladen, nebo zjišťování, zda byl požadavek vyřízen – opravdu někdo touží po těchto „zážitcích"? Přitom je lze pořízením Portálu občana ze životů obyvatel jednou pro vždy odstranit. Nástroj však umí zbavovat některých komplikací i samotné úředníky. Asi nikdo netouží po frontách nervózních lidí, přepisu dat z papírových žádostí a formulářů do informačního systému nebo práci s větším objemem hotovosti. A na všechny tyto nepříjemnosti fungují právě kouzelná slova „Portál občana". K jeho využití lidé potřebují pouze webový prohlížeč a přístup k internetu.

## Digitální formuláře

Města mohou svým občanům na portálu zpřístupnit libovolné elektronické formuláře. Na základě analýzy jsme sestavili sadu 10 formulářů, která zohledňuje četnost využití i další faktory. Data jsou následně automatizovaně vytěžována do informačního systému GINIS. I formuláře, které byly vyplněny ve webové podobě, může úředník


exportovat v jednotné přehledné podobě (shodné s papírovou verzí).

Portál zajistí hladké zpracování jakéhokoliv počtu současně podaných žádostí i při větších nárocích na přílohy, objem či formu údajů. Nástroj je připraven i na typy žádostí o dotace, u kterých vyhodnocení a následné přidělování závisí na pořadí při podání. V minulosti tak byl například využíván krajskými úřady při sběru žádostí o kotlíkové dotace. I přes velký nápor v každé vlně sběru Portál občana obstál.

## Online platby

Co může být snadnější než se přihlásit do Portálu občana a vidět splatnost jednotlivých místních poplatků. Pak už stačí jen příslušnou položku rozkliknout a zvolit, zda chci platbu provést platební bránou, příkazem nebo načtením QR kódu do bankovní aplikace. Pokud tak člověk nechce, už nikdy se při úhradě místních poplatků nemusí utkat s růžovým nepřítelem: složenkou.

Vedle výše uvedených životních situací a správě plateb se Portál občana GINIS rozšiřuje o řadu dalších funkcí, například rezervaci času úředníka, sběr návrhů pro participativní rozpočet atd. Nezáleží přitom, z jakého zařízení se člověk přihlásí. Díky responzivitě se portál automaticky přizpůsobí dostupnému prostoru na obrazovce uživatele. Lidé tak mohou plnohodnotně pracovat s PC, notebookem, tabletem či mobilním telefonem. Rychlou orientaci jim zajistí i řada prvků, na které jsou zvyklí z poštovních klientů, sociálních sítí či dalších oblíbených aplikací.

Více informací o Portálu občana najdete na https://www.gordicportalobcana.cz/

GORDIC

# Videokonference pro vládu aneb Zázraky na počkání, nemožné do 4 dnů

***Když nás vláda oslovila s tím, abychom během několika dní zajistili její virtuální fungování, znamenalo to pro nás, že jsme v Ciscu vzali videokonferenční vybavení nejen ze skladů, ale i to vlastní ze svých kanceláří a dali jsme ho k dispozici vládě. Naši partneři udělali v podstatě totéž a díky tomu mohla česká vláda od 16. března začít fungovat zcela virtuálně.***

Od pokynu k tomu, že máme videokonferenční řešení začít připravovat na míru potřeb vlády, přes sestavení konceptu, až po plné fungování videokonference, uběhlo 6 dní. Projekt byl specifický tím, že vzhledem k situaci u něj neexistovalo přesné zadání, ale zároveň byl dán přesný termín, kdy musí stoprocentně fungovat. Ve čtvrtek 12. března jsme sestavili jednoduchý koncept tak, aby bylo pro uživatele co nejsnazší se v něm ihned zorientovat a začít ho naplno používat, aby všichni věděli, co mají stisknout, jak se ke konferenci připojit a jak z ní odejít. Pátek jsme věnovali instalaci videokonferenční technologie. Tady skvěle zafungovala IT oddělení jednotlivých

ministerstev, kde nám opravdu skvěle vycházeli vstříc. Měli jsme k dispozici týmy lidí, které videokonferenční řešení rozvážely na místa a vše proběhlo včas a hladce. O víkendu jsme se zabývali analýzou řešení, která vedla k tomu, že původní koncept bylo potřeba změnit a upřesnit. Ukázalo se totiž, že původně zamýšlený rozsah by byl naprosto nedostatečný. Přes videokonference se totiž měla vést kompletní vládní agenda. To znamenalo nejen jednání vlády, ale i konzultace s externisty, tiskové konference, či ad hoc jednání s různými týmy, které se budou teprve vytvářet. Přešli jsme proto na mítinky realizované v nástroji Webex Teams. Ten disponuje pracovními místnostmi, do kterých jsou přizváni vždy konkrétní lidé, kteří se na dané problematice, k níž je místnost určena, podílejí. Tento způsob umožnil velkou variabilitu v počtu konferencí i ve způsobu jejich startování. Nic se nemuselo plánovat vyloženě dopředu, stačilo, když poskládaná skupina dostala pokyn, aby klikla na zeleně svítící tlačítko a účastníci se připojili.

První jednání vlády proběhlo v pondělí 16. března v devět hodin ráno, odpoledne se pak uskutečnila první tisková konference s novináři na dálku. Instalace a zaučení uživatelů trvalo několik málo hodin a první den využívání videokonferenčních zařízení proběhl bez problému. Následující dva dny jsme instalovali další potřebná zařízení a od 18. března běžely virtuální vládní mítinky v rutinním provozu asi dva a půl měsíce. V té době jsme uživatelům samozřejmě poskytovali průběžnou vzdálenou podporu. V tom nám velmi pomohly Webex Teams. Pomocí textové komunikace, sdílení souborů nebo obrazovky jsme mohli rychle reagovat na žádosti o podporu. Protože Webex Teams fungují stejně uvnitř organizace i mezi nimi, mohli uživatelé okamžitě komunikovat s kýmkoli. Mobilem nebo e-mailem by to bylo zdlouhavější. Tady v praxi vidíte, jak může vypadat projekt, který se realizuje pomocí cloudové služby, a jaké jsou jeho výhody: velmi rychlé nasazení, možnost škálování řešení a efektivní komunikace.

## Jednoduchost jako základ

V Ciscu je pro nás vždy nejdůležitější onboarding uživatelů, protože využívání videokonferenčních řešení musí být pro lidi jednoduché. Na prvotní seznámení jsme měli jen hodinu, přesto se start podařil. Jedním z důvodů byla aplikace Webex Teams na mobilech. S mobilem umí zacházet každý a akce, jako sestavení skupiny (založení Space) a nastartování online schůzky, je intuitivní. Mobil se také používá jako dálkové ovládání k videokonferenčním zařízením Cisco (Intelligent Proximity). Největší zátěž byla kladena na asistentky a IT oddělení. Mezi úlohy asistentek patřilo vytvářet skupiny uživatelů a poté je spojovat dohromady právě přes videokonference. Od samotných účastníků se neočekávalo, že do tohoto procesu budou nějakým způsobem zasahovat. Asistentky využívaly Proximity na mobilech jako dálkové ovládání k videokonferencím. Dalším jejich úkolem bylo řídit samotnou konferenci, vpouštět do ní jen plánované účastníky, řídit promítání prezentací a podobně. Samotný uživatel se tedy nemusel vůbec ničeho dotýkat, o nic se starat a mohl se plně soustředit na průběh videokonference. Co se týče vzdálené podpory, ta probíhala také přes místnosti ve Webex Teams. IT zde například využívalo jednoduché možnosti sdílení obrazovky nebo chat. Ve srovnání s e-mailovou podporou se rychlost odezvy při řešení požadavků a podpoře uživatelů zněkolikanásobila.

## Hybridní mítinky jako nová forma schůzek

Virtuální mítinky se přes letošní léto staly novým normálem. Ukazuje se, že řada lidí si na fungování v práci na dálku zvykla, anebo to vnímají jako přínos. Najednou se schůzka, která se dříve konala v jedné místnosti, kde museli být přítomni všichni účastníci dohromady, daleko častěji konala jako schůzka kombinovaná. Takové setkání označujeme jako hybridní mítink – část lidí se schůzky účastní na dálku a část lidí je přítomna fyzicky na místě. U takového hybridního mítinku ale nestačí, že postavíte doprostřed stolu počítač a sednou si k němu čtyři lidé dohromady. Je potřeba řešit náležité vybavení místnosti, kde by videokonferenční zařízení mělo splnit především tři základní vlastnosti. Zaprvé, automatické zaměření mluvčího a jeho přiblížení. To znamená, že technologie zabere zrovna toho, kdo v daném momentě mluví, a ne tři lidí okolo. Zadruhé, pokud se v místnosti vyskytuje více displejů, tak je nejlépe využít celé jejich plochy – uživatelé na místě schůzky mohou vidět všechny účastníky, kteří jsou připojeni na dálku, nejen jejich část. Další možností využití více ploch je sdílet obsah v reálném čase na jednom z displejů. A do třetice je důležité zajistit co nejjednodušší možnost promítání, ideálně bezdrátově, například přes již zmiňovanou Proximitu. S tímto souvisí i nutnost jednoduchého ovládání – videokonferenční technologie by měla být někde v pozadí a nenutit účastníka, aby se jí neustále věnoval.

Řešení, které jsme v Ciscu přizpůsobili podle potřeb vlády, umožnilo institucím fungovat ve virtuálním prostoru v horizontu několika dní. Naprosto klíčovými vlastnostmi byly jednoduchá aplikace, která usnadnila adopci, a to, že videokonferenční zařízení uživatel vnímal jako televizi. Nestaral se o to, že se jedná o počítač, využívající umělou inteligenci. Poučení, které jsme si z této doby vzali, je, že řešení pro vzdálenou spolupráci se má zakládat na otevřených standardech, protože nikdy nevíte, koho budete chtít v budoucnu ke konferenci připojit, s kým budete chtít komunikovat. V tomto případě to může být nejen komunikace uvnitř vlády, ale i mezi rezorty, napříč státními organizacemi, úřady či samosprávou. V případě mezinárodní komunikace mezi státními představiteli pak jde o prostředí, které už nemůžeme mít pod kontrolou. Na otevřených standardech se ale vždy všichni shodnou a nic nebrání snadnému spojení.

## S výzvami práce na dálku se nepotýkala jen vláda

S nastalou situací se museli vypořádat všichni, nejen vláda, ale i jednotlivci, firmy a samozřejmě i školy. Dle mého názoru právě ve školách proběhla velká změna, protože potřebovaly pomoct se vzdálenou komunikací. A dost možná ještě budou potřebovat pomoct řešit toto nějak koncepčně. Proto jsme jim nabídli možnost používat Webex s rozšířenými funkcemi zdarma. Díky tomu mohli učitelé zakládat virtuální školní třídy, kde viděli žáky před sebou na obrazovce a poznali tak, jak kdo výklad vnímá. Učitel mohl k videokonferenci využít i digitální tabuli, a tak svůj výklad doprovodit i psanými poznámkami nebo jinak graficky. Umožnili jsme tak školám učit přes Webex na dálku v situaci, kdy se nikdo nemohl osobně setkávat se studenty. Všichni tak dostali možnost učit se stejně, jako by spolu seděli v jedné místnosti. Všichni účastníci také mohli sdílet v reálném čase dokumenty, zkrátka měli k dispozici vše potřebné. Chtěl bych také zdůraznit, že při jakékoliv práci na dálku je důležité používat technologie, které jsou zabezpečené, a to nejen v případě nasazení na úrovni veřejné správy, ale i ve školách. V Cisco Webex je proto od základu veškerá komunikace šifrovaná, a tak se nikdo z účastníků nemusí bát, že by jeho data nebyla chráněna.

Pro videokonference bylo období od letošního března velmi důležité a práce na dálku se do povědomí lidí dostala více než za předchozích deset let. Mezi březnem a květnem jsme například zaznamenali pětinásobný nárůst provozu Webexu v České republice, v absolutních číslech mluvíme o 300 000 video schůzkách za měsíc květen, ke kterým se připojil milion lidí. V únoru, tedy před zavedením karanténních opatření, to bylo 60 tisíc schůzek.

## Naučte se komunikovat na dálku

Vzdálená komunikace, jak vidíme, zažívá období rozkvětu a stává se standardem, ale to, co zde ještě trochu zaostává, jsou návyky lidí související s jejím využíváním. Chybí zde jakási komunikační gramotnost. Schopnost, jak vést videokonferenci, se na školách neučí, ale osvojit bychom si ji měli. Důležitá je dochvilnost i zapnutá kamera. Lidé často chtějí vidět ostatní, sami ale nechtějí být vidět. Uvědomme si, že jde vlastně o komunikaci přes stůl a tam byste svému protějšku také oči nezavazovali. Navíc význam nonverbální komunikace a mimiky je pro snadnost porozumění a hladký průběh komunikace výrazný. Ti pokročilejší by měli zvládat také vedení diskuze na dálku – zaměřit se více než jindy na srozumitelnost a strukturovanost svého sdělení. Pokud i v tomto dokážeme udělat alespoň malý krok kupředu, mohou nám videokonference ušetřit spoustu času i stresu a pomoct rychle reagovat, což se ukazuje být v řadě oblastí lidské činnosti klíčové pro úspěch.

Jaroslav Martan

CISCO

axians

The best of ICT with a human touch

# Chráníme Vaši organizaci

Nebojíme se jakékoliv výzvy – efektivně a účinně Vám pomáháme ve všech oblastech kybernetické bezpečnosti.

## Hlavní oblasti:

- Řízení zranitelností
- Penetrační testování
- Síťová bezpečnost
- Ochrana koncových zařízení
- Security Operation Center
- Governance, Risk, Compliance
- Konzultace kybernetické bezpečnosti
- Odborná školení a vzdělávání

Více o kybernetické bezpečnosti a našich dalších službách najdete na **www.axians.cz**

VINCI ENERGIES

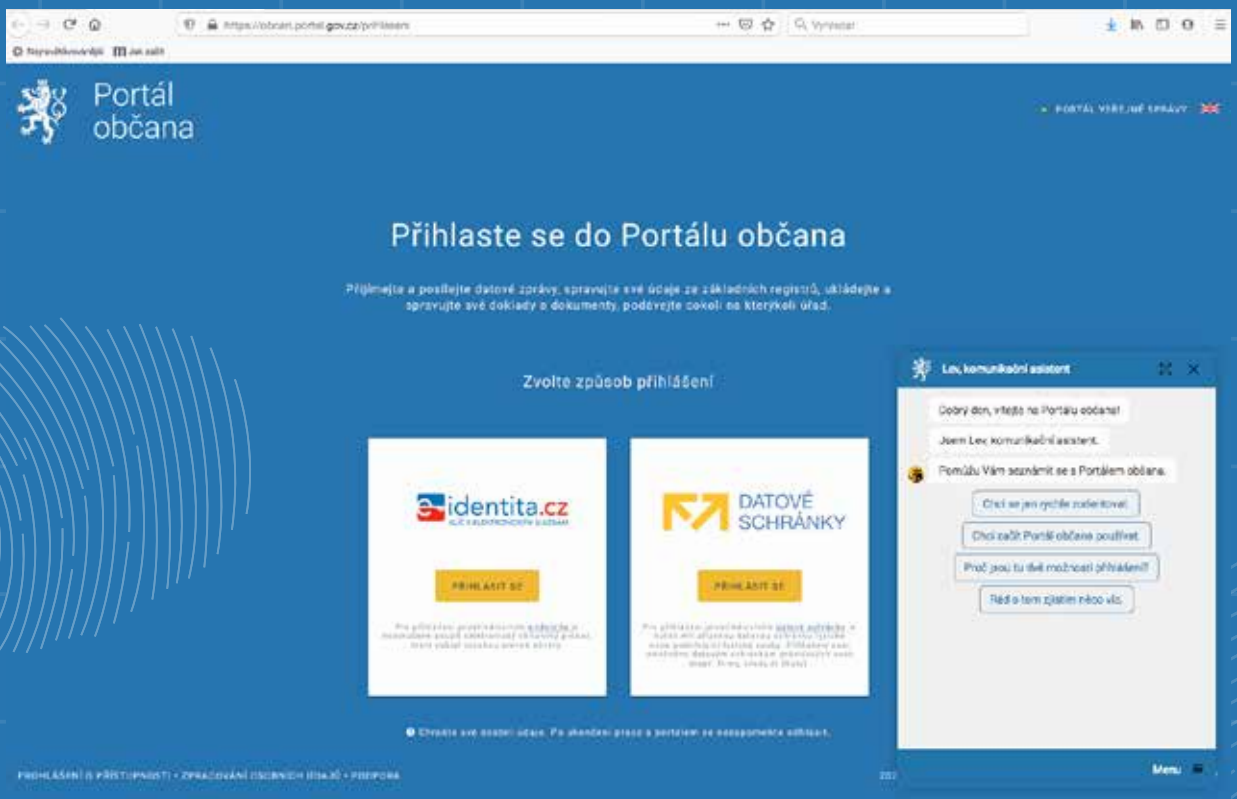
# Certifikáty pro elektronickou identifikaci vydává První certifikační autorita, a.s., jako kvalifikovaný správce kvalifikovaného systému elektronické identifikace

***Certifikáty, jejichž náležitosti a použití jsou upraveny právními předpisy, je možné rozdělit z pohledu uživatelů na dvě hlavní skupiny. První, které jsou označovány jako kvalifikované, jsou určeny pro vytváření elektronického podpisu jako projevu vůle, kdy se má za to, že podepisující se seznámil s obsahem podepisovaného dokumentu. Podepisujícím je vždy fyzická osoba, ať už jedná svým jménem, nebo v zastoupení právnické osoby. Obdobou jsou certifikáty pro vytváření elektronických pečetí, kdy se k dokumentu hlásí konkrétní právnická osoba.***

Druhou skupinou jsou certifikáty, které umožňují vzdálené ověření identity fyzické osoby, které byl certifikát vydán. Ty nejsou na rozdíl od první skupiny označovány jako kvalifikované, ale jako identitní, případně komerční identitní či komerční certifikáty pro elektronickou identifikaci.

Zákon o elektronické identifikaci stanoví, že „vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace". Například je v současné době možné takto prokázat totožnost vůči Portálu občana, bráně k elektronickým službám státu. Počet takto dostupných služeb se stále rozšiřuje, novinkou je možnost použití tohoto způsobu identifikace pro vstup do Zákaznického systému elektronického mýtného, Informačního systému technických prohlídek či podání žádosti COVID – nájemné Ministerstva průmyslu a obchodu.

Prokázání totožnosti s využitím identitního certifikátu I.CA ve spojení s čipovou kartou Starcos 3.5 a vyšší představuje nejvyšší stupeň úrovně záruky prostředku pro elek-




tronickou identifikaci ze stupnice nízká – značná - vysoká. Certifikát i čipovou kartu nabízí všem zájemcům První certifikační autorita, a.s., která jako první soukromoprávní subjekt získala v lednu tohoto roku akreditaci pro správu kvalifikovaného systému elektronické identifikace.

Na rozdíl od běžných komerčních certifikátů určených pro autentizaci je vydání a používání identitních certifikátů spojeno s ověřováním u tzv. identity providera. Realizuje se prostřednictvím Národního bodu pro identifikaci a autentizaci Národní identitní autority (NIA) provozované Správou základních registrů. Pouze při takovém postupu se má za to, že se jedná o nepopiratelné prokázání identity žadatele o službu v on-line komunikaci s poskytovateli jednotlivých služeb.

Čipová karta Starcos 3.5 a vyšší je tedy stejně jako občanské průkazy, vydávané od 1. 7. 2018,nástrojem, kterým se prostřednictvím NIA prokazuje, že přihlašující se uživatel je skutečně tím, za koho se vydává.

Z hlediska uživatele je proces získání identitního certifikátu obdobný jako při vydání kvalifikovaného certifikátu pro elektronický podpis s uložením soukromého klíče v bezpečném hardwarovém prostředku, tj. čipové kartě nebo tokenu. Stejně tak je jednoduché jeho používání. Certifikáty vydávají tytéž registrační autority I.CA, které vydávají jiné typy certifikátů. Jejich aktuální seznam je na webových stránkách První certifikační autority, a.s.

Výhodou kombinace kvalifikovaného komerčního identitního certifikátu a čipové karty Starcos 3.5 a vyšší je skutečnost, že čipová karta je současně certifikována jako QSCD zařízení, tj. umožňuje při uložení kvalifikovaného certifikátu pro elektronický podpis vytvořit nejvyšší úroveň podpisu, kvalifikovaný elektronický podpis, který je dle nařízení eIDAS postaven na úroveň vlastnoručního podpisu. Uživatel má tedy možnost použít jeden prostředek jak pro on-line prokázání identity, tak i pro elektronický podpis.

Kvalifikovaný prostředek pro elektronickou identifikaci, kterým je identitní certifikát ve spojení s čipovou kartou Starcos 3.5, však není vázán pouze na použití při komunikaci s e-governmentem, a tak se brzy určitě dočkáme jeho širšího uplatnění.

Roman Kučera
obchodní ředitel veřejná správa
První certifikační autorita, a.s.

# Otevřená data a otevřené formální normy

***Pro mnoho veřejných institucí se poskytování otevřených dat stalo běžným způsobem sdílení informací s veřejností. S rostoucím počtem poskytovatelů otevřených dat a s různorodostí dat, která jsou takto poskytována, se ukazuje, že nutným předpokladem použitelnosti dat je sjednocování jejich podoby. Na to pamatuje i legislativa, která v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím zavádí pojem otevřené formální normy (OFN) jako „písemně vydanou specifikaci požadavků na zajištění schopnosti různých programových vybavení vzájemně si poskytovat služby a efektivně spolupracovat".***

V tomto článku pojem otevřené formální normy rozvedeme. Na příkladu cestování po ČR ukážeme, proč jsou OFN v praxi důležité, a popíšeme, jak k OFN přistupuje Ministerstvo vnitra jako koordinátor oblasti otevřených dat veřejné správy v ČR.

## Motivace

Průzkum iniciativy Zachraňme turismus „Dovolená v Česku 2020" zjistil, že dovolenou v Česku plánuje 9 z 10 občanů, že nejoblíbenější formou dovolené jsou poznávací výlety a že při jejich výběru je pro 83 % dotázaných rozhodující lokalita, stravování a možnosti provozování dalších aktivit, tedy turistické cíle. Obce by rády návštěvníky přivítaly ve svých zařízeních a turistických lokalitách. K tomu ale musí potenciální návštěvníky co nejlépe informovat a zajistit, aby se o zajímavých místech dozvěděli.

Turisté získávají informace o tom, co je kde zajímavého, z portálů, jako např. Mapy.cz, Google mapy, CzechTourism, Kudy z nudy, Tipy na výlety atd. Stávající praxe naplňování těchto portálů je bohužel taková, že každý portál používá jinou podobu zveřejňovaných informací. Obce tak musí turistické cíle zaznamenávat ručně na každý portál zvlášť, což bývá pro ně často velmi pracné.

Praktickým řešením tohoto problému je publikace dat o turistických cílech v podobě otevřených dat. Obce mohou snížit své náklady na šíření informací tím, že svá otevřená data budou katalogizovat v Národním katalogu otevřených dat (NKOD). Ten provozovatelům portálů umožní snadno (automatizovaně) zjistit, které obce otevřená data o turistických cílech poskytují. NKOD obsahuje též informaci, jak k datům přistoupit a strojově je konzumovat. Publikovaná data tedy mohou provozovatelé jednotlivých portálů přebírat, aniž by obce musely připravovat a dodávat data jednotlivým portálům.

Aby bylo sdílení informací pro obce i poskytovatele portálů možné, je nutná jednotnost i v samotné publikaci otevřených dat. Bez jednotné definice požadavků na podobu (strukturu, sémantiku, granularitu atd.) poskytovaných dat o turistických cílech by každá obec publikovala data ve své vlastní podobě. Provozovatel služby, který by mohl data využít, by tak musel pro každou obec zpracovávat data speciálním způsobem, což by bylo pro většinu zpracovatelů dat drahé a neudržitelné.

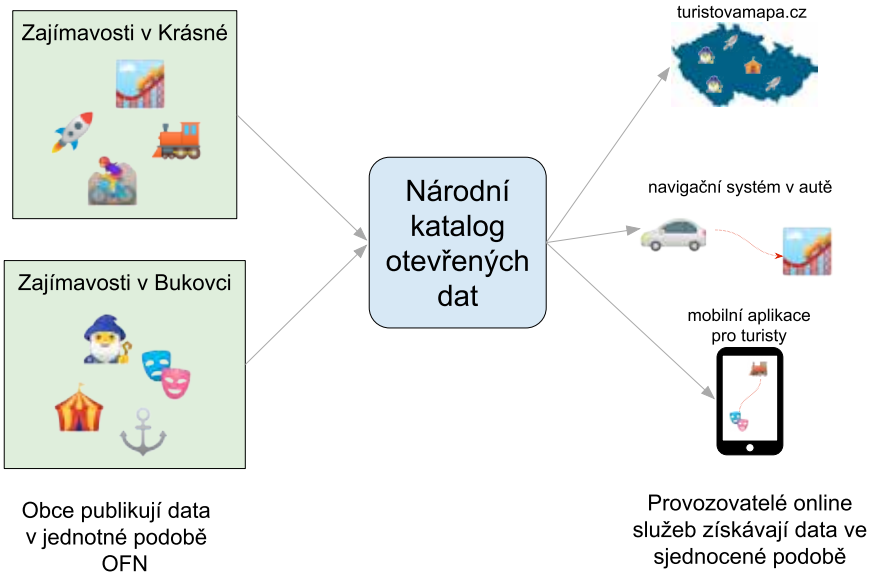
Řešení je jednoduché a spočívá v tom, že všichni poskytovatelé dat o turistických cílech (např. všechny obce) poskytnou data v jednotné, předem dohodnuté podobě. K jejímu zajištění jsou určeny právě OFN, které specifikují strukturu publikovaných informací, jejich význam a vazby na jiné (publikované) související informace. Součástí OFN jsou také předepsané informace nutné k registraci do NKOD sloužící k dohledání publikovaných dat. Takovým sjednocením bude zajištěno, že obce budou s minimálními náklady a jednoduchým způsobem poskytovat data různým zpracovatelům, kteří informace o zajímavých turistických cílech dostanou k široké veřejnosti prostřednictvím jimi provozovaných služeb (webových portálů, mobilních aplikací, navigačních systémů v automobilech atd.).

Tento přístup není omezen pouze na turistické cíle, ale je vhodný pro jakákoliv data určená veřejnosti a je plně v duchu definice OFN v zákoně č. 106/1999 Sb., která hovoří o OFN jako o nástroji pro zajištění schopnosti vzájemně si poskytovat služby a efektivně spolupracovat.

## Přístup Ministerstva vnitra k OFN a možnost účasti na jejich tvorbě

Teoreticky můžeme jako OFN chápat každou písemně vydanou specifikaci, kterou může vydat jak MV ČR, tak i jiný subjekt. Při zveřejnění velkého množství různých specifikací by se v nich poskytovatelé otevřených dat vyznali jen obtížně. Proto z komunikace MV ČR se zástupci několika obcí vzešel jasný požadavek, aby MV ČR koordinovalo tvorbu a doporučování OFN a sjednotilo jejich podo-

**Obrázek 1: Národní katalog otevřených dat a OFN propojují poskytovatele a zpracovatele dat a minimalizují jejich náklady**




bu napříč různými doménami, od turistických cílů, přes sportoviště a pořádané akce až po aktuality nebo úřední desky. Obce požadují jednoduché a návodné řešení, které pro daný typ dat (např. turistické cíle) stanoví jasné doporučení podoby dat, ve které mají být poskytována.

V reakci na tento požadavek MV ČR vytvořilo na Portálu otevřených dat (POD) sekci věnovanou OFN na adrese https://ofn.gov.cz a stanovilo podobu OFN doporučovaných MV ČR. Jako další krok byl vytvořen návrh čtyř OFN: turistické cíle, sportoviště, události a aktuality. Návrhy byly připomínkovány obcemi a po zapracování připomínek je MV ČR vydalo jako první OFN v rámci koordinace prostředí otevřených dat v ČR. V současné době pracuje několik obcí na přípravě publikace dat dle těchto OFN.

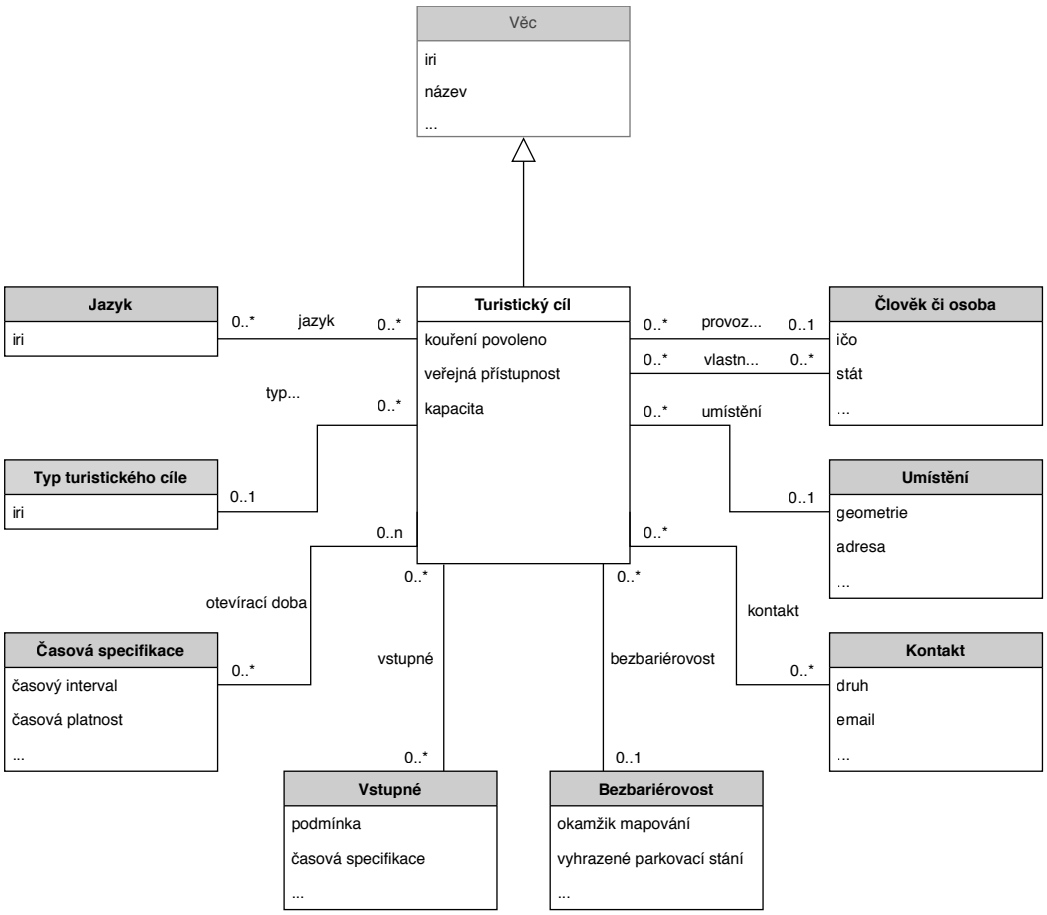
## Co obsahuje otevřená formální norma

Vydané OFN mají jednotnou formu, kterou bude MV ČR aplikovat i u všech dalších vydávaných OFN. Každá OFN začíná popisem důležitých pojmů pro danou datovou sadu, čímž sjednocuje to, jak data chápeme. Pro turistické cíle je to jistě samotný pojem turistický cíl a jeho vlastnosti, jako kapacita či veřejná přístupnost. Dále to jsou pojmy, jako např. umístění turistického cíle či vstupné. Zde využíváme standardní prostředek softwarového inženýrství zvaný konceptuální modelování. Důležité pojmy jsou znázorněny v podobě konceptuálního schématu, který pojmy modeluje jako třídy, jejich vlastnosti a vztahy mezi nimi. Také je graficky znázorňuje. Tímto způsobem je sjednocena základní sémantika dat.

Důležitou vlastností OFN je, že třídy, které se vyskytují ve více různých OFN, např. kontakt, vstupné či umístění, jsou specifikovány na jednom místě, v tzv. sdílených specifikacích. To zajistí, že např. vstupné na festival (událost) bude reprezentováno stejně jako vstupné na hrad či zámek (turistický cíl), což usnadní zpracování dat dle různých OFN. Dále využití těchto sdílených specifikací umožňuje publikovat data, pro která ještě OFN neexistuje, alespoň podobným způsobem. V obrázku 2 jsou třídy vyskytující se ve více různých OFN označeny šedým rámečkem. Můžeme zde vidět i třídu Vstupné označenou šedým rámečkem. To znamená, že třída vstupné je specifikována ve sdílené specifikaci a v OFN pro turistické cíle je použita stejně jako v jiných OFN, které potřebují pracovat se vstupným.

Již existující pojmy lze dále specifikovat. To je vidět na příkladu v obrázku 2, kde vlastnosti, které má téměř každá třída, jako třeba identifikátor či název, jsou popsány ve třídě Věc. Specifičtější třídy, jako např. turistický cíl, pak specializují obecnější třídu věc a tím získávají její vlastnosti. Toto reprezentujeme vazbou s trojúhelníkovou šipkou na jednom konci. Jedná se o běžný prostředek konceptuálního modelování zvaný generalizace (někdy také specializace nebo dědičnost).

**Obrázek 2: Konceptuální model otevřené formální normy turistické cíle**




Dále OFN sjednocuje datový formát a konkrétní datové struktury. V našem příkladu specifikuje, že turistické cíle mají být poskytovány ve formátu JSON-LD, a určuje konkrétní JSON strukturu pro reprezentaci turistických cílů a souvisejících pojmů dle konceptuálního schématu ve formě JSON schématu, které lze použít pro validaci dat. Tím sjednocuje syntaxi a zajišťuje plnou syntaktickou interoperabilitu.

Použití formátu JSON-LD také sjednocuje sémantiku a zajišťuje plnou sémantickou interoperabilitu díky tomu, že formát JSON-LD je jedním z formátů datového modelu RDF (Resource Description Framework), který sémantický popis umožňuje pomocí navázání jednotlivých položek na slovníky široce používané na webu. Příkladem takového slovníku může být http://schema.org, kterému rozumí webové vyhledávače, jež pak umožňují data lépe zobrazit v jejich výsledcích.

OFN také poskytuje vzorový katalogizační záznam do Národního katalogu otevřených dat tak, aby záznamy o datech turistických cílů jednotlivých poskytovatelů vypadaly stejně a bylo je možné stejným způsobem vyhledávat.

## Publikace otevřených dat dle otevřených formálních norem

Při poskytování informací podle zákona č. 106/1999 Sb. má formát co nejvíce splňovat OFN. To se týká i poskytování informací v podobě otevřených dat. Aby byl maximalizován užitek otevřených dat, doporučuje MV ČR postupovat dle OFN vydávaných na zmíněné adrese https://ofn.gov.cz. Není ale samozřejmě možné a ani účelné vydat najednou OFN pro všechny typy dat ve všech doménách, ve kterých je možné otevřená data poskytovat. OFN vznikají na základě poptávky poskyto-

vatelů nebo konzumentů otevřených dat, kteří také dávají požadavky na jejich podobu. Při publikaci dat dle OFN má tak poskytovatel jistotu, že formátuje svá data správně, jednotně s ostatními poskytovateli a očekávatelně pro zpracovatele.

Pokud poskytovatel dat, např. obec, plánuje publikaci otevřených dat nějakého typu, např. o turistických cílech, zjistí na POD, zda pro taková data již OFN existuje. Pokud ano, poskytne data tak, jak OFN definuje. Může se stát, že nemůže publikovat všechny údaje popsané v OFN. Potom poskytne pouze část, kterou publikovat může. Jednotlivé části formátu popsaného v OFN jsou totiž nepovinné. Musí ale počítat s tím, že přílišné omezení poskytovaných údajů datovou sadu znehodnotí. Poskytovatel také může chtít publikovat data nad rámec toho, co je v OFN sjednocené. Pak může datovou strukturu rozšířit za předpokladu, že tak učiní v souladu s existujícími sdílenými specifikacemi a že své rozšíření vhodně dokumentuje formou webové stránky a strojově čitelných schémat tak, aby jeho rozšíření bylo snadno pochopitelné a validovatelné. Struktura takové dokumentace je pak stejná jako struktura OFN.

## Možnost účasti na tvorbě otevřených formálních norem

Tvorba a konzultace OFN probíhá na platformě GitHub https://github.com/opendata-mvcr/otevrene-formalni-normy, což je verzovací systém běžně používaný vývojáři softwaru a autory webových stránek. OFN lze tedy jednak sledovat v celém průběhu jejich tvorby a také lze jejich podobu aktivně ovlivnit. To lze buď formou diskuze o konkrétním problému (GitHub Issue), nebo přímo příspěvkem do kódu či textu (Pull Request).

Stejným způsobem může libovolný poskytovatel požádat o tvorbu nové OFN, kterou vytvoří ve spolupráci s MV ČR. Alternativně může publikovat datovou sadu i bez konzultace s MV ČR. V takovém případě ale je nutné využívat sdílené specifikace, které již pro některé části dat existují stejně jako v případě publikace dat nad rámec již existující OFN. I v tomto případě je nutné vzniklou datovou sadu řádně dokumentovat tak, aby mohla sloužit alespoň jako základ pro budoucí OFN.

## Zpracování otevřených dat dle OFN

Zpracovatelé dat, jako například portály s informacemi o turistických cílech, mohou všechny datové sady odpovídající OFN najít strojově, automatizovatelně a opakovatelně pomocí API Národního katalogu otevřených dat. Dohromady s jednotným formátem, který specifikuje OFN, je pak již snadné data od jednotlivých poskytovatelů pravidelně stahovat a zpracovávat. MV ČR připravuje ukázkovou open-source aplikaci, která tento proces a následné využití dat dle OFN názorně ukáže.

## Závěr

Otevřené formální normy (OFN) jsou specifikace syntaktické a sémantické podoby datových sad publikovaných jako otevřená data, které se řídí moderními webovými standardy. Jejich využíváním benefitují jak poskytovatelé dat, kteří svá data musí publikovat pouze jednou, tak jejich zpracovatelé, kteří dostanou data od mnoha poskytovatelů ve stejné podobě, a tedy je nemusí složitě integrovat. Ministerstvo vnitra publikovalo OFN pro 4 datové sady – turistické cíle (obrázek 2), aktuality, sportoviště a události a koordinuje tvorbu OFN i pro další datové oblasti. Do tvorby OFN se může zapojit libovolný poskytovatel či zpracovatel dat pomocí GitHubu https://github.com/opendata-mvcr/otevrene-formalni-normy

Více informací naleznete na webu https://ofn.gov.cz.

Jakub Klímek, Martin Nečaský

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

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_025/001398, který zastřešuje odbor hlavního architekta e-governmentu, Ministerstvo vnitra ČR.

# Digitální služby a bankovní identita: praktický příklad digitálního stavebního řízení

***V pondělí 15. 6. 2020 schválila vláda České republiky aktualizované implementační plány a další dokumenty programu Digitální Česko. Tím se definitivně přihlásila k závazku digitalizovat do 5 let veškeré služby státu, které je z podstaty možné realizovat online. Povinnost provést v tomto termínu digitalizaci plyne ze zákona o právu na digitální služby, sám zákon však proměnu českého e-governmentu neprovede – nezbytné je velké úsilí veřejné správy k jeho naplnění.***

Prvním krokem k naplnění zákona je sestavení tzv. katalogu služeb. Ten bude součástí stávajícího přehledu agend v registru práv a povinností a bude zachycovat všechny úkony, které veřejná správa provádí navenek nebo jsou vůči ní činěny. Ty úkony, které v tomto přehledu budou označeny jako elektronické, bude muset stát poskytovat navenek jako digitální službu, resp. bude muset umožnit jejich činění ve formě digitálního úkonu.

Vedle stávajících portálových řešení Finanční správy a Správy sociálního zabezpečení bude muset vzniknout řada nových digitálních služeb. Branou k těmto službám by měl být především stávající Portál občana a také připravovaný Portál podnikatele. Zatímco některé oblasti státní správy si musí na plán, jak a kdy budou digitalizovány, ještě počkat (vláda jej má vydat do 1. 2. 2021), některé oblasti již mají detailní právní úpravu se stanoveným termínem účinnosti.

Příkladem je digitalizace stavebního řízení a územního plánování, upravená novelou stavebního zákona a zákona o zeměměřictví, přijatou v únoru tohoto roku. Podle dat Světové banky trvá v ČR v současné době vyřízení stavebního povolení 247 dní. Novela si klade za cíl tuto situaci změnit; příslušné systémy by měly být plně funkční 1. 7. 2023, kdy novela nabývá účinnosti. Nic by na tom neměl změnit ani připravovaný nový stavební zákon, protože ten příslušné systémy v plném rozsahu přebírá a jeho účinnost je právě s ohledem na digitalizaci z velké části nastavena k 1. 7. 2023.

Základním pilířem digitalizace stavebního řízení je Portál stavebníka, který bude občanům sloužit jako jednotný přístupový bod k datům ve všech systémech stavebního řízení a územního plánování. Prostřednictvím tohoto portálu tak bude možné podávat žádosti o stavební povolení a činit i další elektronické úkony vůči stavebním úřadům, sledovat průběh řízení a nahlížet do evidencí. Interaktivní formuláře usnadní podání vůči orgánům stavební správy, a to v souladu se zákonem o právu na digitální služby. Páteří digitálního stavebního řízení budou evidence stavebních řízení a evidence elektronických dokumentací. V evidenci stavebních postupů budou dostupné veškeré úkony, které budou v daném řízení či postupu činěny elektronicky. Díky tomu bude v rámci Portálu stavebníka možné podrobně sledovat aktuální stav řízení a nahlížet do klíčových dokumentů, jako jsou rozhodnutí a stanoviska dotčených orgánů. Právě integrace dotčených orgánů do systémů digitálního stavebního řízení je klíčová, protože díky ní bude žadatel moci činit veškeré potřebné úkony z jednoho místa – přes Portál stavebníka – a na tomtéž místě sledovat průběh příslušných postupů.

Evidence elektronických dokumentací pak bude digitálním úložištěm elektronicky zpracovaných projektových dokumentací. Drtivá většina projektových dokumentací zpracovaných profesionály již dnes vzniká elektronicky a stavebnímu úřadu se poskytuje na listině, případně hmotném nosiči jako DVD, jen proto, že prakticky není možné ji doručit jinak (objem dat zpravidla výrazně přesahuje nastavené limity pro zaslání datovou schránkou). Z toho důvodu bude do budoucna povinné takovou dokumentaci zpracovanou profesionálem odevzdat stavebnímu úřadu elektronicky právě pomocí evidence elektronických dokumentací, konkrétně vložením přes Portál stavebníka. Možnost listinného podání občanů však zůstane i v těchto případech zachována – stavebník bude moci projektanta pověřit, aby dokumentaci vložil do evidence a sdělil mu unikátní odkaz generovaný Portálem stavebníka. Odkaz se následně uvede v příslušném listinném podání a dokumentace se tak stane jeho přílohou.

Speciální funkcionalitou Portálu stavebníka bude také možnost z jednoho místa požádat vlastníky sítí o vyjádření k ochranným pásmům a stavebnímu záměru jako celku. Díky digitálním technickým mapám jednotlivých krajů, kde budou jednotlivé sítě a další technická infrastruktura zachyceny, se nejen usnadní samotné projektování, ale zároveň budou stavebníci přesně vědět, koho se svou žádostí oslovit.

Praktickým předpokladem širokého a plnohodnotného využití Portálu stavebníka je široce dostupná a důvěryhodná digitální identita – taková, kterou budou moci snadno a bezpečně využívat miliony občanů. Právě takovou digitální identitu slibuje projekt bankovní identity, ke kterému byla potřebná legislativa přijata rovněž v únoru tohoto roku. Podstatou bankovní identity je využití stávajícího přístupu klientů bank do internetového bankovnictví jako prostředku pro elektronickou identifikaci vůči státu i soukromému sektoru. Bankám bude nově od 1. 1. 2021 povoleno poskytovat elektronickou identifikaci na komerční bázi, podmínkou však bude zpřístupnění této identity bezplatně pro stát, obce a kraje v rámci Národního bodu pro elektronickou identifikaci a autentizaci.

Díky tomu může snadný přístup k elektronickým službám veřejné správy okamžitě získat až 5,5 milionů občanů, kteří dnes využívají elektronické bankovnictví. Tento přístup přitom bude jak pro občany, tak pro stát a samosprávu bezplatný. Ve spojení s úpravou digitálních úkonů v zákoně o právu na digitální služby přitom bankovní identita umožní občanům právní jednání online přímo v informačních systémech veřejné správy, bez nutnosti používat elektronický podpis či datovou schránku.

Zákon o právu na digitální služby by tak ve spojení s bankovní identitou měl do 5 let přinést plně digitální formu všech myslitelných služeb veřejné správy, přístupnou pro miliony občanů díky jednoduše použitelné a široce rozšířené elektronické identitě. Příkladem oblasti, pro kterou již má postup digitalizace konkrétní obrysy, je stavební řízení a územní plánování, které bude zpřístupněno přes jednotné rozhraní Portálu stavebníka.

JUDr. Josef Donát, LL.M.,
Advokát / Partner, ROWAN LEGAL,
advokátní kancelář s.r.o.

ROWAN LEGAL

# Otevřená data: základní přehled právní úpravy

***Otevřená data jsou fenomén, který se v posledních letech pomalu zabydluje v českém prostředí, a hlavně českém právním řádu. Věcně navazují na problematiku informací veřejného sektoru (spíše známou pod zkratkou „PSI" z anglického „Public Sector Information"), kterou nalezneme zakotvenou v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím. Tradičně můžeme rozeznat dva základní účely, mezi kterými je právní úprava PSI rozkročena.***

Prvním účelem je přístup k informacím jako projev základního politického práva na informace. Právo na přístup k informacím se řídí obecným principem publicity veřejné správy, který stanoví, že nikdo nemusí prokazovat právní zájem pro to, aby mu byl přístup k informacím umožněn a povinný subjekt musí poskytnout dožadované informace s výhradou výjimek předvídaných zákonem . Toto právo je nedílnou součástí práva na svobodu projevu, které není možné plně vykonávat bez řádné možnosti být informován o veřejném dění. Kořeny právní úpravy tohoto cíle pak nalezneme zejména v ústavněprávní rovině a lidskoprávních mezinárodních smlouvách, kterými je Česká republika vázána.

Druhým základním účelem právní úpravy PSI je účel ekonomický, naplňovaný možností opětovného užití PSI pro další účely nedefinované předem , včetně užití komerčního. Tento přístup vhodně demonstruje výrok zakladatele Open Knowledge Foundation Rufuse Pollocka: „Nejzajímavější způsob využití vašich dat vymyslí někdo jiný." Ekonomická hodnota opětovného užití PSI spočívá například ve vytváření ekonomických příležitostí při vývoji nových aplikací a služeb, případně v úspoře získané díky možnosti propojení jinak separátních dat. Z toho důvodu se do regulace opětovného použití PSI s cílem podpory evropského digitálního trhu pustil evropský zákonodárce. Byla tak přijata směrnice 2003/98/ES, o opakovaném použití informací veřejného sektoru, která následně prošla novelou prostřednictvím směrnice 2013/37/EU.

Obě směrnice je možné shrnout do hlavní zásady: členské státy mají zajistit, aby PSI, které poskytují, byly poskytovány co nejotevřenějším způsobem, který maximálně usnadní jejich další užití. To znamená, že informace mají

být poskytovány online v otevřených a strojově čitelných formátech a zároveň mají co nejvíce odpovídat tzv. otevřeným formálním normám, tedy technickým specifikacím popisujícím způsob poskytování určitých typů informací.

Implementace směrnic do českého právního řádu pak byla provedena do zákona č. 106/1999 Sb. Je zajímavá zejména tím, že se v celém zákoně pojem opětovné užití prakticky neobjevuje. Možnost opětovného užití PSI je v Česku založena zásadou legální licence, a je tedy limitována jen výjimkami a omezeními vyplývajícími z právních předpisů, jako je například ochrana osobních údajů, obchodní tajemství, nebo duševní vlastnictví. Zákon stanoví prostřednictvím § 4b odst. 1 jen povinnost dodržet při poskytování PSI minimální technickou kvalitu poskytovaných informací.

Otevřená data představují maximálně efektivní způsob poskytování PSI. Koncept otevřených dat neřeší, jaké informace jsou poskytovány, ale jakým způsobem se tak děje. Obvyklými předpoklady otevřených dat jsou zveřejnění PSI online v otevřeném a strojově čitelném formátu, s minimálními právními překážkami a s takovými podmínkami užití, které nijak neomezují způsob a účel jejich dalšího využití. Tomu rovněž odpovídá zákonná definice v podobě § 3 odst. 11 zákona č. 106/1999 Sb., která navíc přináší podmínku registrace zveřejňovaných otevřených dat v Národním katalogu otevřených dat. Jde o informační systém veřejné správy ve správě Ministerstva vnitra, jehož účelem je umožnit efektivní vyhledávání mezi publikovanými otevřenými daty. Vedle zavedení definice a zakotvení Národního katalogu přinesla tzv. Open Data novela, provedená zákonem č. 298/2016 Sb., třetí zásadní novinku v podobě tzv. povinných otevřených dat, která jsou určena nařízením vlády č. 425/2016 Sb. Povinné subjekty podle zákona č. 106/1999 Sb. však mohou poskytovat jako otevřená data i jiné informace než jsou ty vyjmenované v tomto nařízení, a to na základě obecné diskrece vyplývající z § 5 odst. 6 zákona.

Česká právní úprava otevřených dat však dozná v blízké době několika změn. V roce 2019 byla přijata směrnice EU č. 2019/1024, o otevřených datech a opakovaném použití informací veřejného sektoru (tzv. OD směrnice), která s účinností od července 2021 nahradí výše zmíněnou směrnici z roku 2003 a její novelu. OD směrnice dále prohlubuje důraz na poskytování PSI v co nejotevřenější podobě a oproti své předchůdkyni přináší tři zásadní novinky.

První z nich spočívá v rozšíření působnosti směrnice na veřejné podniky ve smyslu definice vycházející ze směrnice 2014/25/EU, tedy na obchodní společnosti podnikající v klíčových oblastech fakticky ovládané státem.

Druhá novinka spočívá v zavedení tzv. datových sad s vysokou socioekonomickou hodnotou, které budou stanoveny prováděcím předpisem k OD směrnici a které budou povinně zveřejňovány napříč EU. V současné době nejsou známy konkrétní informace, které budou takto zveřejňované. OD směrnice nicméně stanoví alespoň obecné kategorie, z nichž mají být vybrány. Jedná se o informace o pozorování Země a životním prostředí, meteorologii, statistické údaje, nebo údaje o vlastnictví společností.

Konečně třetí zásadní novinka spočívá ve výslovném zahrnutí údajů z vědeckého výzkumu prováděného z veřejné podpory do aplikačního rozsahu směrnice.

V současné době probíhá mezirezortní připomínkové řízení k návrhu implementačního předpisu, který krom změn v zákoně č. 106/1999 Sb. předpokládá rovněž změny v zákoně č. 123/1998 Sb., o právu na informace o životním prostředí, které jsou nezbytné vzhledem k nutnosti narovnání regulace otevřených dat v těchto velmi blízkých předpisech. O výsledcích legislativního procesu tzv. Open Data novely pak budeme samozřejmě v budoucnu na těchto stránkách referovat.

Jakub Míšek

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

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_025/001398, který zastřešuje odbor hlavního architekta eGovernmentu, Ministerstvo vnitra ČR.

# Cloud pomáhá zmírnit omezení způsobená koronavirem

***Je to jen pár měsíců, kdy jsme se poprvé setkali s novým fenoménem dneška, tedy omezeními způsobenými koronavirem. Kvůli tomu, že se aktuálně potýkáme s nástupem druhé vlny, nám může doba té první připadat už vzdálená. Ale všichni z „IT branže" si pamatujeme, že to byl největší akcelerátor digitalizace společnosti nejen za poslední roky, ale i obecně. Nikdy předtím se lidstvo nevěnovalo tak agilně a masivně elektronizaci jako právě na jaře tohoto roku. A proč? Protože informační a komunikační technologie pomáhaly zmírňovat následky koronakrize. Nebál bych se označit informační technologie za největšího pomocníka v krizovém stavu tohoto období – samozřejmě hned po lékařích a vědcích.***

Největším pomocníkem v oblasti IT technologií byly především cloudové služby. Proč právě cloud? Především díky tomu, že jeho nasazení je extrémně rychlé. Mnohem rychlejší, než když si vše stavíme sami ve své serverovně nebo v datovém centru. Ve chvíli, kdy bylo třeba mít rychlý výpočetní výkon nebo nástroj pro online komunikaci, všichni sáhli logicky právě po cloudovém řešení. A jak to v době krize vypadalo ve veřejném sektoru? Veřejná správa, která je obvykle stabilní a rozvážná, dokázala v této situaci zabrat a předhonit ve spoustě oblastí digitalizace i komerční sektor. Doufejme, že do budoucna se toto stane novým standardem a nevrátí se zpět do svých stabilních vod.

## Online výuka a online komunikace

Pojďme se podívat na pár konkrétních příkladů. Určitě si všichni vzpomenete na zavřené školy, což s sebou přineslo velké výzvy spojené s výukou dětí, které se ze dne na den ocitly doma. Školy se nové situaci postavily čelem. Sáhly po cloudových řešeních pro online spolupráci a komunikaci a začaly žáky užit na dálku. A jaká to byla řešení? Někteří z vás si možná z dětství pamatují seriál z roku 1968 o klokanovi Skippy. Tam se hlavní dětský hrdina žijící s rodiči v australské pustině učil také na dálku, a to prostřednictvím vysílačky. Školy na jaře samozřejmě nesáhly po vysílačkách, ale využily cloudová řešení, která v některých případech dokázaly pro celou školu nasadit takřka přes noc. Velká část škol zvolila řešení Microsoft Teams, jež je pro školy zdarma a jež umožňuje nejen online komunikaci, sdílení souborů a zadávání úkolů, ale také vytvářet online třídy, hromadně ztlumit mikrofon všem žákům, jednotlivé hodiny nahrávat a mnoho dalšího. Microsoft Teams jsou navíc součástí celého balíku služeb Office 365, který je ve verzi A1 školám poskytován bezplatně i v běžných časech a jež nabízí další cloudové služby pro učitele a studenty.

Podobnou situaci tou dobou řešila i veřejná správa. I úřady se musely naučit pracovat online a začaly využívat tzv. homeoffice. Velmi rychle zjistily, že pokud nezavedou homeoffice, výrazně zvyšují riziko paralýzy činnosti úřadu. Začala tedy doba, kdy se úřady začaly učit organizovat interní porady sekcí, odborů nebo oddělení videokonferenčně. Velké množství úřadů mělo Microsoft Teams již zakoupené v rámci licencí Office 365, jen je ještě nestihlo začít používat. Tyto úřady tak byly ve velké výhodě. Instituce, které licence ještě neměly, měly možnost začít Office 365 využívat na půl roku zdarma. Z letošního jara tak máme zkušenost s několika ministerstvy a úřady, které začaly Teamsy využívat doslova během několika málo dní. Jen namátkově bych jmenoval například Ministerstvo průmyslu a obchodu nebo Ministerstvo zahraničních věcí. Právě zmiňované MPO dokázalo díky platformě Teams hned od samého začátku krize koordi-

novat Covid manuál a jeho využívání nejen v rámci svého resortu, ale i s ostatními ministerstvy.
Rád bych ještě upozornil, že úřady, které již mají nasazenu platformu Microsoft Teams a další cloudové služby z balíčku Office 365, mohou významným způsobem optimalizovat provozní náklady na IT. Tím, že začnou online služby naplno využívat, mohou optimalizovat – snížit – množství provozovaných a nakupovaných serverů do vlastní serverovny.

## Online komunikace s občany a klienty

Další výzvou byla pomoc s online vyřizováním potřeb klientů veřejné správy. Tedy odbavit velké množství dotazů občanů a jejich problém i pomoci vyřešit. Zde přicházejí na řadu chatboti, které jsme pomáhali nasadit hned několika resortům. Ty se staly opravdu obrovskými pomocníky, kteří jako virtuální roboti odváděli rutinní práci za úředníky a šetřili jim tak čas potřebný na řešení těžších a náročnějších úkolů. Příkladem je opět Ministerstvo průmyslu a obchodu či Ministerstvo práce a sociálních věcí a Česká správa sociálního zabezpečení. A jak chatboti fungovali? Ano, opět jako cloudová služba. V našem případě v cloudovém prostředí Microsoft Azure. Zmíněné úřady si ověřily hlavní výhodu chatbota, tedy že dokáže v jeden okamžik vyřizovat požadavky a dotazy velkého množství občanů současně. Díky tomu dokáže nahradit hned několik úředníků, což se plně projeví nejen při vypjatých a krizových situacích, ale i v běžné činnosti úřadu. A co nás čeká dále? Chatboti se začínají měnit v osobní digitální asistenty a začínají si s námi nejen psát, ale i mluvit. To pomůže v digitální komunikaci např. seniorům, kterým se digitální asistent bude jevit jako virtuální člověk, který s nimi mluví a pomůže jim vše vyřídit.
Další krok, který měly úřady před sebou, bylo spuštění systémů pro elektronické vyřizování a žádání o cokoliv. Jedním příkladem za všechny je opět Ministerstvo průmyslu a obchodu a žádosti o ošetřovné pro OSVČ. Úkol byl nelehký - spustit za 5 dnů systém na žádosti OSVČ o ošetřovné, včetně elektronického podání a vazby na další systémy ministerstva. V klasickém IT světě by toto zadání bylo nemyslitelné, ale právě cloudové služby to umožnily. Dnes je systém vybaven dokonce prvky umělé inteligence, které úředníkům pomáhají kontrolovat velkou masu povinných příloh.

## Chrání sebe, chrání mě

Bezpečnost je pro Microsoft na prvním místě. Je pro nás zásadní budovat vztah důvěry v naše služby. Může to znít na první pohled jako marketingová fráze, ale je za tím skutečně obrovské množství úsilí a nepřetržité práce. Na cloudové služby je vedeno každý den, každou hodiny, minutu i vteřinu množství kybernetických útoků. Naše týmy neustále pracují na rozvoji nástrojů a postupů, které umožňují efektivní obranu a které jsou k dispozici nejen nám, ale i uživatelům našich cloudových služeb. A jak to souvisí s tématem? Koronakrize je doprovázena masivními kybernetickými útoky. Útočníci cílí na IT infastruktury úřadů, které jsou pro fungování státu, ale i pro zdravotnictví a sociální služby v takové době důležitější než kdy jindy. Spousta úřadů využívá naše cloudové systémy, jejichž výhodou je, že jsou okamžitě aktualizovány a chráněny proti novým útokům. Můžete si proto s klidem říci, že tím, že Microsoft chrání sebe, chrání i vás.

## Budoucnost cloudů

Cloudové technologie jsou hojně využívány veřejnou správou, o svém přínosu již přesvědčily. Online veřejná správa se aktuálně stává realitou a pomáhá tomu i zákon o právu občanů na digitální službu. Jen potřebujeme znát odpověď na to, jak toto právo naplnit. Po zkušenostech s Portálem občana a dalšími systémy, které cloudové služby využívají již několik let, je vidět, že cloud je rychlá, jednoduchá, přímá a ekonomicky výhodná cesta k cíli. A když už bude občan potřebovat mluvit s úředníkem, bude to čím dál častěji videokonferenčně. Věřím, že stát bude nadále pokračovat ve své cloudové strategii, kterou si stanovil již před třemi lety, a že bude i nadále vnímat nejen výhodnost, ale i špičkovou bezpečnost, kterou je ve vlastních datových centrech finančně velmi náročné docílit. Cloudové služby jsou připraveny pomoci nejen v aktuální situaci, ale v digitalizaci a zjednodušení veřejné správy obecně.

Václav Koudele,
architekt strategických řešení
pro veřejný sektor, Microsoft

Microsoft

# Covid i post-Covid: Jak chránit data před kybernetickými útoky

***Během posledních několika měsíců zaznamenal tým FortiGuard Labs značný nárůst bezpečnostních hrozeb v souvislosti s pandemií COVID-19. Právě takovéto události bývají historicky katalyzátorem vzniku nových hrozeb. Jaké to jsou a jak se bránit? Ochrana proti hackerům není složitá, stačí použít správné nástroje a dodržovat následující postupy.***

Určitě vás hned napadne: Proč hackeři stupňují útoky – a zrovna v během krizového stavu? Útočníci jsou si velmi dobře vědomi, že v takových chvílích se společnosti potýkají s množstvím náhlých změn, na které nejsou připraveny. Takové chvíle často vyústí v rychlosti vymyšlené provizorní řešení ve snaze udržet byznys v chodu. Tak vznikají mezery v zabezpečení interních dat a otevírají se nové možnosti pro kybernetické útoky. Často jde o sofistikované nebo skryté útoky, které na první pohled zmatou uživatele.

## Podvodné reklamy

Snaha identifikovat nejnovější trendy, formy a témata kybernetických útoků odhalila například alarmující množství reklamních prvků, které inzerují podvody související s pandemií COVID-19. Mezi nejčastější patří ty apelující na strach plošně panující ve společnosti – finance či léky a zdravotnické potřeby coby nedostatkové zboží. Všeobecný hlad po informacích či panika přinesla hackerům obrovské množství obětí. Jeden klik na podvodný odkaz v emailu a uživatelův systém byl infikován. A infekce se mohla rozšířit až nečekaně daleko...

## Z domácnosti až do firem

Vlivem vládních nařízení z posledních měsíců se tak ocitlo dříve těžko představitelné množství nechráněných uživatelů a jejich zařízení online – připojených denně k interním serverům prostřednictvím domácího internetového připojení. Domácí síť se najednou ocitla pod náporem: Dospělí ji využívali k práci, děti ke vzdělání – a celá rodina potom ke kontaktu s příbuzenstvem a přáteli – všichni chatují, streamují, posílají data, sdílí na sociálních sítích.... Ideální podhoubí pro kybernetické útoky a jejich šíření! A jak to funguje?

## Cílem jsou citlivá data

Nejprve je potřeba si říct, o co vlastně útočníkům jde. Cílem je obecně získat vzdálený přístup k citlivým datům a osobním údajům v koncových systémech. Použít k tomu mohou nejrůznějších prostředků – včetně virů, trojských koní (RAT, etc.) nebo ransomware. Útočníkům nahrál také fakt, že ne všechny společnosti byly schopny zajistit dostatečné množství laptopů pro veškeré své zaměstnance, kteří po dobu státem vyhlášeného omezení pohybu osob pracovali z domova.

Mnohdy tak byli zaměstnanci nuceni využívat k připojení do firemní sítě svých soukromých zařízení. Tedy právě TĚCH, která za normálních okolností využívají k přístupu na sociální sítě, e-shopy nebo třeba ke streamování audia a videa na internetu. Navíc jsou tato zařízení zpravidla mnohem hůře chráněna, a tedy mnohem zranitelnější vůči všem možným hrozbám.

## Hrozba pro všechny

Není přitom třeba napadnout přímo laptop s přístupem do firemní sítě. Hackerům postačí využít jedno z dalších zařízení propojených společným domácím internetovým připojením. Tablet, herní zařízení nebo dokonce některý z prvků chytré domácnosti jako domovní zvonek, alarm, termostat či osvětlení. I tyto zdánlivě nevinné doplňky poskytnou stejně prostupný přístup k interní síti a citlivým datům společnosti. Vzhledem k faktu, že v době pandemie jsou veškeré helpdesk služby dostupné vzdáleně, zařízení infikovaná ransomware či virem mohou odstavit zaměstnance i na několik dní. Ohroženy jsou nejen nadnárodní společnosti enormních rozměrů, ale především malé a střední podniky (SMB).

## PREVENCE JE NEJLEPŠÍ OBRANOU – JAK NA TO?

Události posledních měsíců jasně dokázaly, že zabezpečení domácích zařízení i sítí je nezbytné. S nadsázkou zaujměte stejnou strategii vůči virům a ohrožení jako v reálném světě – udržujte sociální (kybernetický) odstup, nasaďte roušku (bezpečnostní nástroje) a rozpoznávejte rizika. V praxi si pod tím představte tyto kroky:

- Zkontrolujte, zda je dostatečně chráněna firemní síť – kromě FortiToken a FortiAuthenticator umožňujících multifaktorové ověřování a jednotné přihlášení, můžete zvážit i nasazení řešení FortiGate pro kontrolu provozu v síti, či FortiNAC pro správu autentizovaných zařízení a jejich přístupů pouze k těm síťovým prostředkům, které reálně potřebují.
- Vzdělávejte o rizicích i možnostech ochrany své zaměstnance, vzdálené pracovníky i jejich rodiny – začít můžete například s NSE training program, vzdělávacím programem sestaveným společností Fortinet.
- Zajistěte všem zaměstnancům, kteří pracují vzdáleně, přístup k bezplatnému řešení FortiClient VPN a zvažte i pokročilejší zabezpečení přidáním FortiEDR detekující a eliminující živé hrozby. Informujte je, jak povolit zabezpečení i na routerech a bezdrátových AP.
- Eliminujte vstup kybernetických trendů skrze e-mail pomocí FortiMail, který nabízí široké spektrum možností ochrany. Bezpečná e-mailová brána musí být schopna detekovat a spolehlivě filtrovat phishingové útoky a spam, ale i zneškodnit závadné přílohy.
- Zkontrolujte vzájemnou symbiózu bezpečnostních nástrojů.

FORTINET

# Ochrana proti kyberútokům nejen ve zdravotnictví: klíčový je nový pohled na zabezpečení

***Nebezpečí kyberútoků neustále roste a bohužel stále častěji je to viditelné ve zdravotnictví. Rostoucí trendy v mobilitě a cloudu učinily nová místa kybernetických útoků i z koncových zařízení. Tyto útoky obchází tradiční ochranu a bezpečnostní týmy často nedokáží dostatečně rychle reagovat. Provozy informačních systémů řady institucí tak byly i v České republice v posledních letech a měsících ochromené počítačovým kryptovirem. Přitom existují sofistikovaná řešení, která dokáží podobným útokům předcházet.***

## Nejviditelnějším příkladem jsou nemocnice

Zdravotnické organizace jsou stále častěji cílem kybernetických útoků zejména kvůli množství osobních údajů, které vlastní. Zpravidla jsou i tím typem zařízení, kde jsou kybernetické útoky nejvíce vidět a mohou mít i největší dopad. Příkladem jsou nejen útoky s celosvětovým dopadem, jako WannaCry a NotPetya ransomware útoky z roku 2017, ale i ty lokální z nedávné doby. Není to tak dávno, kdy byl v České republice velmi sledovaný kybernetický útok zaměřený na nemocnici v Benešově. Čerstvým případem je pak incident z doby vypuknutí koronavirové epidemie, kdy hackeři zaútočili na počítačovou síť brněnské fakultní nemocnice v Bohunicích.

Kybernetičtí útočníci mohou získat přístup k informacím o pacientovi, ukrást je a prodat je na „dark webech". Kromě toho umí vypnout či omezit přístup nemocnic ke klíčovým systémům a k záznamům o pacientech, což prakticky znemožní efektivní péči o pacienty.

*„Kdyby na nemocnici proběhl kybernetický útok, mělo by to významný dopad, ze všeho nejdřív na poskytnutí služeb. Ano, doktor by vás stále mohl prohlédnout, ale jeho schopnost objednat testování, zaznamenat léčbu nebo domluvit další schůzku by byla značně narušena. Ale také by pacienti a veřejnost ztratili důvěru, protože bychom pro ně nebyli bezpečným a zabezpečeným místem,"* vysvětluje David Wall, ICT ředitel Tallaghtské univerzitní nemocnice v Dublinu.

Se zvýšeným používáním lékařských zařízení v rámci internetu věcí jsou možnosti napadení celých systémů stále větší. Problému nepomáhá ani nedostatek IT pracovníků zodpovědných za kyberbezpečnost, natož stagnující rozpočet na zabezpečení v tomto odvětví.

## Výzkum potvrzuje nárůst kyberútoků ve zdravotnictví

Zajímavé údaje o tomto segmentu přináší loňská zpráva o stavu kybernetické bezpečnosti ve zdravotnictví, která vznikla pod hlavičkou VMware Carbon Black a na které spolupracovali přední odborníci na bezpečnostní technologie. 83 % dotázaných zdravotnických organizací uvedlo, že za poslední rok zaznamenaly nárůst kybernetických útoků. Dvě třetiny (66 %) dotázaných zdravotnických organizací uvedly, že se kybernetické útoky staly za poslední rok složitějšími.

Možná ještě hrozivější je zjištění, že téměř polovina (45 %) dotázaných zdravotnických organizací uvedla, že se setkaly s útoky, jejichž hlavním cílem bylo právě zničení dat, což by bylo obrovským problémem nejen ve zdravotnictví. A protože plné dvě třetiny (66%) dotázaných zdravotnických organizací uvedly, že jejich organizace byla cílem kybernetického útoku během uplynulého roku, je třeba, aby se všechny instituce a zařízení – nejen ty zdravotnické – na podobné útoky co nejlépe připravily.

## Tallaghtská univerzitní nemocnice se na bezpečnost soustředí

Příkladem, jak situaci řešit, může být Tallaghtská univerzitní nemocnice v Dublinu. *„Měli jsme mnoho problémů s předchozím prostředím. Běželi jsme na velmi stárnoucí infrastruktuře a neměli jsme dostatek počítačové techniky,"* vysvětluje Ricky McKenna, manažer ICT infrastruktury této nemocnice. Ta již technologie VMware v minulosti využívala a byly pro ni spolehlivé, takže se rozhodla je používat i nadále. *„VMware má ve zdravotnické péči dobré výsledky, proto jsme cítili, že bude dobrou volbou pro naši nemocnici,"* říká ICT ředitel David Wall.

Tallaghtská univerzitní nemocnice používá VMware vRealize Operations Manager ke správě a monitoringu a VMware vSphere k virtualizaci serverů. Dále pak VMware Log Insight Manager, který sbírá protokoly z celého prostředí pro diagnostické účely. *„Technologie VMware spolu velmi dobře pracují. Je skvělé mít jednotné rozhraní pro správu práce na různých komponentech z řešení VMware,"* říká Ricky McKenna.

Přestože nemocnice má za sebou v oblasti zabezpečení již hodně práce, i tak nechce riskovat, že by nebyla v této oblasti úspěšná a nějaký malware se do nemocnice dostal. VMware NSX a funkce mikro-segmentace izoluje aplikace tak, že v případě, kdy je jedna aplikace napadnuta, nebude schopna napadnout i ostatní.

Stephen O'Herlihy, CTO největší irské společnosti poskytující ICT a managed služby PFH Technology Group přirovnává řešení k hotelu. *„V hotelu mají ochranu zabezpečující celý obvod, ale všechny dveře odemčené nenechávají. To stejné dělá NSX: uzamkne každý individuální virtuální stroj. Pro Tallaghtskou univerzitní nemocnici jsou prioritou číslo jedna pacienti a bezpečnost jejich dat, takže to z tohoto pohledu byla perfektní volba,"* říká.

*„Naše bezpečnost je pro nás nesmírně důležitá. Pracujeme s množstvím různých informací – od dat našich pacientů, která jsou velmi citlivá, až po finanční údaje. Takže ochrana těchto informací je opravdu zásadní,"* uzavírá příběh dublinské nemocnice David Wall.

## Vhodná je kombinace více technik zabezpečení

Tým globální technologické společnosti VMware má bohaté zkušenosti s pomocí svým klientům s obnovou po útoku a ochranou proti kybernákazám. VMware nabízí pro ochranu sítě dvě základní techniky. První je antivir nové generace VMware Carbon Black s účinností 99,78 %. Druhým klíčovým nástrojem je segmentace a virtualizace síťové infrastruktury pro karanténu nakažených systémů a možnost obnovy produkčních systémů.

Útoky v dnešní době většinou vedou přes uživatelskou stanici do vnitřní sítě a VMware Carbon Black právě na toto myslí. Pomáhá zákazníkům s komplexním zabezpečením koncových bodů a pracovních zátěží, pokročilou bezpečnostní analýzou na ochranu proti sofistikovaným kybernetickým útokům a se zkrácením reakční doby. Služba VMware Carbon Black aplikuje analýzu big data ve všech koncových bodech, aby předpovídala a tím poskytovala ochranu před současnými, budoucími i neznámými útoky.

## Problémům je třeba předcházet

Všechny instituce spravují velké množství citlivých dat a kritických systémů. I proto by měly využívat možnosti moderních technologií a předcházet bezpečnostním problémům. A transformace kybernetické bezpečnosti pomocí řešení společnosti VMware je navržena tak, aby před těmi nejpokročilejšími hrozbami ochránila.

vmware®

# DOBRÝ POCIT

***Jestliže jste letos zavítali do Mikulova na naši konferenci e-government 20:10, nebo si ji pustili ze záznamu, který je k dispozici na stránkách konference (můžete najít na www.egovernment.cz), pak jste museli mít docela dobrý pocit. Po letech neustálého poklesu se Česká republika v hodnocení OSN – EGDI posunula o patnáct příček nahoru. Všichni přítomní (fyzicky či videokonferenčně) zainteresovaní nás ubezpečovali, že toto není náhodné a ojedinělé, ale že se jedná o trend, který bude rozhodně trvalý. A navíc přidali věštbu, že za dva roky (hodnocení EGDI se realizuje vždy jednou za dva roky) budeme jisto jistě na pozici dvacáté (což by znamenalo skok téměř o dvacet pozic). Při těchto projevech bylo hojně používáno sousloví „klientsky orientovaná", nebo „přívětivá veřejná správa". Jak říkám, člověk z toho musel mít dobrý dojem.***

Není nad osobní zkušenost. Patrně, abych se probral z ohromení, kterým na mě tato diskuze zapůsobila, podařil se mi husarský kousek. Ztratil jsem osobní doklady. Ale tak, že všechny. Tedy občanský průkaz, řidičský průkaz, technický, průkaz pojištěnce, lítačku na MHD, platební karty. Prostě když něco, tak pořádně. A tak mě čekalo úřední kolečko. Víte, už dvacet let, co vydáváme magazín Egovernment a organizujeme konference s tématikou elektronizace veřejné správy, slýchávám heslo „obíhat mají data, ne občané". Tak trochu jsem tušil, že stále ještě, i po těch dvaceti letech, není plně v platnosti. Přesto jsem byl překvapen. A neměl jsem z toho dobrý pocit.

## PLATEBNÍ KARTY

Peníze na prvním místě, že? A tak volám do banky, jaký jsem šikula a že potřebuji zablokovat sbírku karet. Identifikace/autentizace po telefonu, karty zablokovány. O nové si mohu požádat rovnou, nebo si sednout k počítači a vyřídit to ve svém internetovém bankovnictví. Radši takové věci vidím, takže děkuji. Zatím mi stačí jistota, že karty nefungují. Odpoledne pak usedám k počítači, volím typ karet a rozsah služeb. Hotovo, celkově cca 15 minut. Karty by poštou měly dorazit do pěti dní, přes internet je následně aktivuji.

## OBČANSKÝ PRŮKAZ

Pro občanský průkaz si musím dojít osobně. Vzal jsem s sebou rodný list, strávil 30 minut na cestě a díky nulové frontě byl hned na řadě. Vyplnil papírové formuláře s informacemi, které už veřejná správa skutečně má k dispozici, nechal se vyfotit a dostal papírovou náhradu, která však není plnohodnotnou náhradou. Navíc informaci, že OP budu mít za tři týdny a ať si do té doby rozmyslím, jestli tam chci aktivovat nějaký ten elektronický čip.

## ŘIDIČSKÝ PRŮKAZ

Vzal jsem papírový leták, který měl být úředním dokladem o momentální neexistenci mého OP, a vyrazil na jiný úřad v jiné části města řešit řidičský průkaz. Přece jezdit se musí, ne? Cesta dalších třicet minut, fronta na 90 minut. Klika, že jsem ještě ve vyvolávacím systému vylosoval číslo pro dnešní den – a hlavní cenu vyhrává ... tak nic, tombola se nekonala. Sličná slečna v roušce byla neoblomná. Bez dalšího dokladu s fotografií nebude nic. „Ale já mám papírek o občance a rodný list. A fotografii máte v počítači, tak se jukněte, vždyť poznáte, že jsem to já," říkám si, že se nedám a že jsem šikula, když poukazuji, že data, včetně mé fotografie, jsou v té bedně, která stojí mezi námi. „Kdepak, to nejde, musím Vás ztotožnit podle nějakého dokladu," omlouvá se mi, usmívá se na mě (tuším ten milý úsměv pod rouškou), skoro mě chlácholí. Nakonec z toho vycházím alespoň s remízou, když získám náhradní řidičský průkaz (tedy vlastně zase potvrzení o tom, že ten skutečný jsem ztratil a ten další skutečný teprve dostanu), ale alespoň s tím mohu jezdit a ten původní je označen jako neplatný, kdyby jej chtěl někdo nějak zneužít. Jsou tři odpoledne, to už na žádný další úřad nemá cenu jezdit, jdu domů.

## LÍTAČKA

Abych mohl po těch úřadech cestovat s klidným svědomím, volám na „lítací" linku – Operátor ICT. Ptám se, kam a kdy nejlépe bych měl zaběhnout, abych si ji obnovil, a jak tak asi dlouho to bude trvat (už jsem po zkušenostech s řidičským a občanským průkazem trochu opatrněj-

ší). Slečna na druhém konci mi říká, ať nejsem „debil“ (tedy samozřejmě kulantnější formulací), ať nikam nechodím, že bych tam stál zbytečně frontu. Že když si do telefonu stáhnu aplikaci Lítačka a sednu k počítači, kde se připojím ke svému účtu (pidlitacka.cz), který u Operátora ICT mám, mohu si nahrát svůj kredit do mobilu, tedy mít lítačku v mobilu a tu původní zneplatnit. Funguje to. Zabralo to 10 minut.

## ZDRAVOTNÍ POJIŠŤOVNA

S novou vírou v dobré výsledky se přihlašuji do svého účtu u zdravotní pojišťovny. Tady to není tak přehledné a intuitivní jako u lítačky, a tak prošťourávám různé varianty, až vypadne jako nejrozumnější e-mail. Výsledkem elektronické komunikace je informace, že nový průkaz pojištěnce obdržím poštou. Za dva, až tři týdny. Tak jo. Je 17:00, dnes už nic.

## TECHNICKÝ PRŮKAZ

Další den vyrazím na další (v pořadí již třetí) úřad s papírovým velkým technickým průkazem, papírovou náhražkou občanky a sebedůvěrou, že to dám. Nakonec se ukázalo, že největším problémem bylo trefit do správných dveří (vyvolávací systém zuřivě bliká moje číslo) a vyplnit papírovou žádost s údaji, které už mají ve svých počítačích (jen abych tam nenapsal něco blbě). Malý technický průkaz je nakonec vypečen (zataven) během 5 minut, celková doba na úřadě asi 45 minut. To se dá vzít jako pozitivní.

## CO DÁL

Celkem zatím, a to jsem v mezičase, jsem strávil běháním po úřadech cca 8 hodin, tedy jeden pracovní den. Až dostanu OP, pro kterou si musím opět osobně, budu moci zaskotačit za tou smutnou princeznou a požádat ji o řidičský průkaz, ona si vezme do ruky můj nový OP, vyťuká potřebné údaje a zjistí, že jsem to skutečně já. Možná budu muset vyplnit další papírovou žádost, a hlavně budu muset čekat další lhůtu, než si budu moci zase osobně pro průkaz dojít.

## ČAS JSOU PENÍZE

No, nejsem žádný vrcholový manažer, takže mi tím časem, kdy jsem obíhal a ještě budu obíhat úřady, žádné velké miliardy neutekly. Ale tak trochu mi připadá, že mě tím někdo pekelně potrestal za všechny ty prezentace o světlých zítřcích, které nám elektronizace přináší. Každopádně, jednoznačným vítězem mého soukromého průzkumu se stala Lítačka a Operátor ICT. A já si tak říkám, proč to podobně nejde i ve věcech úředních?

Proč není OP, ŘP a další v podobě nějaké aplikace, kterou mohu mít, díky autorizaci, ať již přes DS, či dvoufaktorově přes mobil, právě v mobilu? Proč data, která jsou uvnitř veřejné správy (OP, ŘP, TP), musím znovu a znovu psát na papírovou žádost? Proč vůbec je to tak složité, stačil by přece jeden identifikátor (třeba OP), který může být kartičkou, nebo kódem v mobilu, a tím se mohu prokazovat komukoliv, kdo má příslušnou čtečku? Možná jsem naivní idealista odtržený od reality, a v tom případě budu rád za umírnění svých představ, ale měl jsem dojem, že žijeme v době, kdy jsou naše data kdesi shromážděna a podle autorizace a míry oprávnění mohou být sdílena tím či oním kontrolním orgánem. Pokud to nebude takto fungovat, domnívám se, že neposkočíme o oněch dvacet pozic v mezinárodním hodnocení. Ale snad, tak jak v úvodu vyplývá z vyjádření a prezentací MV ČR, se vše začne měnit po 1. 2. 2021. Máme se tedy nač těšit.

Michal Jirkovský, šéfredaktor

GORDIC

# Digitální služby Portálu občana GINIS

Komunikace s úřadem

Elektronické podání žádostí

Pohodlná platba poplatků

Řešení životních situací

www.gordic.cz