



## KONFERENCE MIKULOV e-government

„Žijem si jak na zámku, ať to trvá věčně.“

# Slavili jsme 10 let



Digitální  
česko



Portál  
občana



Elektronická  
občanka

## KONEC DESETILETKY

Letošní výroční konference e-government 20:10, aneb žijeme si jak na zámku, ať to trvá věčně, kterou jsme pořádali počátkem září na zámku Mikulov, byla desátá, tedy pro nás skutečně výroční. Končili jsme desetileté období existence, stejně jako například internetový prohlížeč Chrome. Ostatně společnost Google vznikla přesně v den konání letošní konference před dvaceti lety a v den konference se roku 1927 narodil John McCarthy – autor pojmu umělá inteligence. Tedy výročí spojených s elektronizací dost a dost. A k tomu jsme se potkali v roce 100letého výročí naší republiky. Výročnější naše setkání už snad ani nemohlo být.

Odpovídala tomu nejen atmosféra, ale i „napěchování“ programu. Rozsáhle jsme hovořili o Portálu občanu, projektu MV ČR, který odstartoval 1. 7. 2018, a strategii Digitální Česko. Oboje je pro další vývoj elektronizace v ČR důležité a určující. Nevynechali jsme ale ani elektronickou identitu a nezapomněli ani na legislativu. Dali jsme si tím vším naději, že úroveň našeho e-governmentu bude nyní, v porovnání s ostatními zeměmi, jen a jen stoupat. Věřím, že pokud jsme v mezinárodním hodnocení končili v našem desetiletí na 54. místě, budeme při příštím jubileu, za deset let, na místě 4., tedy v TOP FIVE. Máme na to. Mohou Vám to ukázat informace z Mikulova, které naleznete na následujících stránkách.

Hezké čtení.

Ing. Michal Jirkovský  
šéfredaktor

<b>Redakce</b>	ÚVODNÍ SLOVO .....	2
	OBSAH, TIRÁŽ .....	3
<b>e-government 20:10</b>	DEVELOPMENT NEBO DEPRESE? .....	4-6
	ÚVOD MV ČR .....	8-9
	VZDĚLÁVÁNÍ, PROPAGACE A GOV.CZ .....	10-11
	PROPOJUJME SE .....	12-13
	JAK SE IDENTIFIKOVAT? .....	14-16
	NÁRODNÍ BOD A JAK S NÍM PRACOVAT .....	18
	SYSTÉMY JSOU BEZPEČNÉ .....	20-21
	DIGITÁLNÍ ČESKO .....	22-24
	ČESKO V DIGITÁLNÍ EVROPĚ .....	26-27
	PILÍŘ Č. 3 DES - DIGITÁLNÍ EKONOMIKA A SPOLEČNOST .....	28-29
	ZÁKON O PRÁVU NA DIGITÁLNÍ SLUŽBY .....	30-33
	MEMORANDUM O SPOLUPRÁCI .....	34-35
	OZNÁMENÁ ELEKTRONICKÁ IDENTITA .....	36-40
	CISCO NETWORKING ACADEMY .....	42-44
	JEDNOTNÝ EKONOMICKÝ SYSTÉM KRÁLOVÉHRADECKÉHO KRAJE .....	46-47

**V rámci České a Slovenské republiky vydává:**

info♦com s.r.o, Na Zatlance 10, 150 00 Praha 5  
 www.infocom.cz  
 IČO: 26426331  
 zapsána u Městského soudu v Praze  
 pod č. C - 81357

**tel.:** 241 412 518  
**e-mail:** egovernment@egovernment.cz  
**http:** www.egovernment.cz  
 ISSN 1801-9420

**Šéfredaktor:** Ing. Michal Jirkovský  
**Korektorka:** PhDr. Helena Veverková  
**Asistentka:** Patricie Stránská

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

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

**Registrace:**

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**. Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **100 Kč (4 EUR)** bez DPH/**výtisk, tj. 400 Kč (16 EUR)** bez DPH **ročně**. S registrací získáte, kromě pravidelného zaslání magazínu, i informace o dalších projektech, které realizuje společnost **info♦com s.r.o.**



# Development nebo deprese?

**Konference e-government 20:10, aneb žijeme si jak na zámku, ať to trvá věčně se letos konala již po desáté. Deset let se v Mikulově scházíme, abychom diskutovali o úrovni elektronizace veřejné správy v ČR, hodnotili realizované projekty a hledali cestu dalšího vývoje. V rámci těchto diskuzí se shodujeme v tom, že náš e-government je dobrý, zajímavý, přínosný atp. Každoročně! Každoročně se totiž najde něco, co stojí za zmínku, co je možné nazvat určitým posunem, podnětem a úspěchem. A tak postupně, rok od roku, roste pocit, že je všechno, jak má být.**

Pokud ale vykukneme z ulity, trochu se porozhlédneme, a nedej bože hledáme určité srovnání, není důvod k radosti a uspokojení. Neznamena to, že bychom u nás nerealizovali zajímavé projekty, nebudovali e-government a neposouvali se. Jen ve srovnání s ostatními zeměmi možná ne stejným tempem.

Od roku 2001 vydává ve dvouletých periodách Organizace spojených národů žebříček srovnávající jednotlivé země (celkem 193) právě co do úrovně e-governmentu (e-government Development Index OSN - zkr. EGDI). Pokud bychom se podívali jen na ono desetileté období trvání naší konference, zjistíme z pohledu ČR brutální sešup. V roce 2009, kdy se konference konala poprvé, jsme se nacházeli na 25. příčce (hodnocení roku 2008).

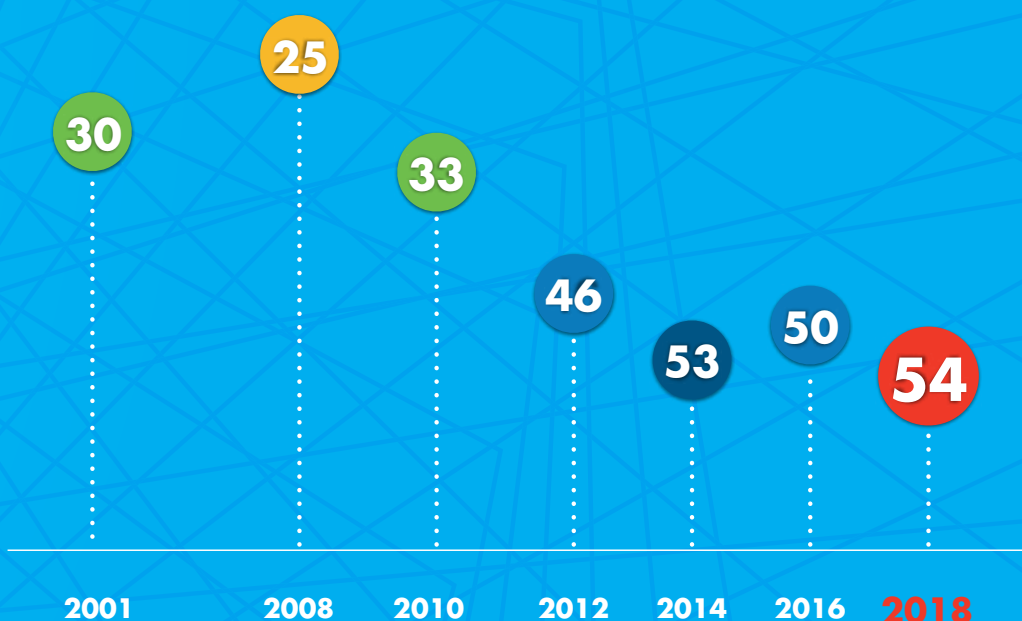
O deset let později, naplněných radostným budováním a množstvím diskuzí nejen na naší konferenci, je možné vidět ČR na 54. pozici, tedy o 29 příček níže!!! Prostý pohled na takový graf říká, že s naší elektronizací veřejné správy to nijak růžové není. Přesto i letos v Mikulově zněla slova chvály, optimismu a přesvědčení o kvalitě českého e-governmentu.

Kde je tedy pravda?

## ÚSPĚŠNÝ ZAČÁTEK

Úplně první hodnocení EGDI se odehrálo v roce 2001. Tehdy jsme ještě možná od jeho výsledku, ve vztahu k naší elektronizaci, mnoho nečekali. A tak jsme byli mile překvapeni pěkným 30. místem. Mohlo se to stát například díky dobře připravenému a především on-line obchodnímu

## E-GOVERNMENT DEVELOPMENT INDEX OSN – POZICE ČR



rejstříku. To byla ukázka, jak asi má vypadat správná on-line služba veřejné správy. Dech jsme neztráceli, protože v následujících deseti letech jsme postupně produkovali základní registry, Czech POINTy a datové schránky. Nejenže se jednalo o jednotlivě zajímavé projekty, smysl a kouzlo jim dávalo především jejich propojení. Vše vypadalo, že máme „našlápnuto“ na to stát se jednou z těch zemí, které budou určovat trendy v elektronizaci.

### NĚJAK TO „ZAMRZLO“

Ale pak, jakoby se kola naší elektronizace zastavila. Zatímco jsme pořád sledovali ty před sebou - Velkou Británii nebo Austrálii, skoro jsme si nevšimli, že kolem nás profičeli ti, co se zpočátku dívali závistivě na nás. Speciálně skok Estonska byl neuvěřitelný. Dnes je právě ono země, která pro nás může být vzorem, především přístupem a nasazením státu. Naše realizační cesta musí být trochu jiná, neboť i naše situace byla jiná. Pro Estonsko platí, že jako země odtržená od Sovětského svazu, bez funkční vlastní infrastruktury veřejné správy měla vlastně ideální možnost udělat vše elektronicky, protože to bylo nejrychlejší a nejlevnější. Ale i my jsme si na počátku libovali, že vlastně ten určitý skluz v 90. letech, který tady oproti západním zemím byl, je výhodou. Že můžeme stavět na zelené louce. A snažili jsme se, když v roce 2007 byly slavnostně spuštěny Czech POINTy, v roce 2009 datové schránky a od roku 2010 (vznik SZR) jsme budovali základní registry - dokončeno a spuštěno v roce 2012.

A pak, alespoň při pohledu zvenčí, jako kdybychom ztratili dech. Ne, že by se nedělo vůbec nic - byly rozšiřovány a vylepšovány uvedené služby (registr smluv, nabídka Czech POINTů i datových schránek atp.), začínalo se mluvit o nových tématech (Government Cloud, otevřená data, on-line služby, elektronická identifikace) - ale nebyly spuštěny žádné projekty, které by byly „převratné“ a posouvaly nás na přední příčky hodnocení, a tak jsme se postupně propadali až na ono 54. místo.

### ODRÁŽÍME SE ODE DNA?

Bylo by možné toto období nazvat obdobím příprav. Alespoň tak vyznívá nálada některých prezentací z konference v Mikulově. Postupně jsme připravili vše potřebné a nyní tedy startujeme další etapu našeho e-governmentu. Tématy letošní konference proto byl Portál občana, elektronická identifikace či strategie Digitální Česko. Není podstatné, jestli se jedná o projekty realizované z vlastní vůle, nebo donucení například EU. Podstatné je, jaký budou mít dopad na úroveň našeho e-governmentu a jak nás případně mohou v příštím hodnocení EGDÍ 2020 posunout.

**Elektronická identifikace** - je naprosto stěžejní záležitost, pokud míníme slovem e-government vyřizování záležitostí mezi občanem a státem elektronicky. Stát musí vědět, že ten, kdo sedí někde u druhého počítače, je skutečně tím, za koho se vydává, jedině tak jej může obsloužit. Podstatné

je, že tato identifikace se neomezuje pouze na naše hranice, ale platí pro celou Evropskou unii.

**Portál občana** – je vstupní branou do elektronické veřejné správy. Je to místo, kde se mi v podobě dlaždic budou nabízet jednotlivé služby veřejné správy a já se tudy snadno dostanu přímo k té, kterou potřebuji. Soudě podle počtů, v jakých Češi využívají mobilní služby bank či mobilních operátorů, jak jsou schopni nakupovat v internetových obchodech, orientovat se na App, Google a dalších storech, by to nemělo být něco, co by je zaskočilo, ba naopak.

**Digitální Česko** – je strategie, která toto vše propojuje a provazuje i se záměry EU, dává do souvislosti s vizí „lepších digitálních zítřků“. Realizace jednotlivých bodů, respektive naplňování cílů jednotlivých pilířů Digitálního Česka by mělo zajistit realizaci potřebných a efektivních projektů, které nás budou posouvat.

Vypadá to tedy, že máme nastartováno.

## ZAUJETÍ A PROPAGACE

Pro realizaci projektů, plánů a strategií je potřeba „nasazení“ a schopnosti strhnout ty ostatní. Ideální je, pokud takto vyjadřuje podporu elektronizaci například premiér. Pokud porovnáme zaujetí a veřejnou podporu projektů e-governmentu, jakou dával najevo například britský premiér, ať již Tony Blair, nebo David Cameron či estonský premiér Juri Ratas a vzpomene na „zaujetí“, s jakým se tomuto tématu věnovali někteří z našich dřívějších premiérů, je možná 54. pozice ještě dost dobrá.

Současný premiér Andrej Babiš vyjádřil ve videovstupu konference v Mikulově podporu elektronizaci a speciálně pak vyzdvihl projekt Digitálního Česka. Vyjádřil rovněž podporu digitálnímu zmocněnci Vladimírovi Dzurillovi a jeho postupu. Vznik funkce zmocněnce vlády pro IT a digitalizaci je bezpochyby dobrým signálem, stejně jako jmenování právě Vladimíra Dzurilly do této pozice. Je tu však drobný problém, podobně jako na vojně, v kombinaci funkční x hodnostní postavení. Vladimír Dzurilla by měl „dirigovat“ resorty, ale je zmocněncem vlády. Tedy vláda - ministři jej zmocnili. Navíc se jedná zároveň o generálního ředitele státního podniku, jehož zřizovatelem je MV ČR. A tak, když dojde na lámání chleba, je otázkou, kdo koho poslouchá.

Propagace by měla být nedílnou součástí tak závažných záležitostí, jakou je realizace a uvádění projektů elektronizace veřejné správy do provozu. Poslední propagační kroky, podle mého mínění, byly ze strany státu, ministerstva nebo vlády učiněny v souvislosti s Czech POINTy a datovými schránkami. Logo Czech POINT jsme tehdy viděli téměř všude a troufám si tvrdit, že si je stále uvědomujeme. Současné logo Portálu občana vypadá možná státotvorně, ale je až příliš nenápadné. A jeho propagace je opatrná, možná stejně nenápadná. Bylo by dobré, aby informace o Portálu občana, Digitálním Česku i elektronické identifikaci padaly na občany, ale i úředníky doslova ze všech stran. Jedině propagační kampaní, chcete-li mediální masáží, naučíme jak občany, tak úředníky, že tu jsou možnosti elektronické komunikace, že skutečně stát už dnes řadu dat má k dispozici a může je sdílet, že toto sdílení bude nabývat na rozsahu a občan skutečně bude mít možnost a právo vyřizovat své záležitosti se státem osobně či elektronicky, podle vlastní vůle.

Aby uvedené skutečně fungovalo, je potřeba upravit zákony, které mnohdy a mnohde s elektronickou variantou stále nepočítají. Nejvíce je však nutné přesvědčit úřady a úředníky. Především musí začít naplňovat Portál občana svými službami. Žebříček EGDÍ nás posadil na tu nelichotivou 54. příčku hlavně proto, že nemáme dostatečnou nabídku on-line služeb veřejné správy pro občany. Jenže to není tak úplně pravda. Na jednom z předchozích ročníků konference, konkrétně v roce 2016, upozorňoval prezident ICT Unie Zdeněk Zajíček, že jen centrální úřady tehdy poskytovaly 735 on-line služeb, kraje 150 on-line služeb a obce několik tisíc. Problém tedy zdaleka není v jejich neexistenci, jako spíše v tom, že o nich nevíme. Nejsou propagovány a nedokážeme je dohledat. I tomu by měly uvedené projekty napomoci, a i o tom jsme se v Mikulově bavili.

Na následujících stránkách naleznete extrakty toho nejzajímavějšího, co v Mikulově zaznělo. Všechny prezentace, stejně jako fotogalerie z konference jsou k dispozici na [www.egovernment.cz](http://www.egovernment.cz) pod záložkou MIKULOV.

Michal Jirkovský



Reliable Security Always™

## THUNDER ADC

APPLICATION DELIVERY CONTROLLER (ADC)  
& WEB APPLICATION FIREWALL (WAF)

### Vysoká dostupnost a bezpečnost aplikací

Platforma ACOS (Advanced Core Operating System) je postavená na inovativním konceptu architektury SSMP (Scalable Symmetrical Multi-Processing). Navíc proti ostatním výrobcům nepoužívá statickou, ale sdílenou paměť, což umožňuje vynechat IPC (meziprocesovou komunikaci). Při takto odlišné architektuře má řada Thunder od A10 Networks při stejném počtu jader více než dvojnásobnou propustnost a obsluhuje více než třikrát větší počet transakcí za sekundu oproti konkurenci.

A10 Networks přináší celou paletu řešení od fyzických zařízení přes možnost instalace na vybrané bare-metal platformy po virtuální instance na nejznámější virtualizační platformy VMware, KVM, MS Hyper-V a kontejnery Docker/Kubernetes. Samozřejmě je i virtualizace uvnitř těchto platform – rozdělení do tzv. Application Delivery Partitions (ADP), samostatných oblastí s možností oddělené správy, oddělených výkonových parametrů i směrovacích modulů (VRF).

Bezpečný chod aplikací zajišťuje integrované řešení ochrany Web Application Firewall, DNS Application Firewall a AntiDDoS. Další vestavěné moduly umožňují chráněný přístup ke službám, inspekci SSL provozu včetně podpory nejmodernějšího šifrování založeného na eliptických křivkách. Hardwarovou akceleraci SSL zajišťují dedikované čipy Nitrox V.

### Snadná správa včetně možností automatizace

Pro správu řešení a konfiguraci pravidel využívá platforma A10 intuitivní grafické rozhraní GUI s přehledným zobrazením stavu nakonfigurovaných ADC a jejich součástí. Dále je k dispozici běžně používaná řádková konfigurace CLI, podobná příkazové řádce Cisco. Je vhodná pro migraci a optimalizaci konfigurací i pro vytváření a správu velkého množství pravidel. Zařízení se spravují přes zabezpečené protokoly a přístupová oprávnění se rozdělují dle funkcí. Možné je oddělení správy jednotlivých ADP.

A10 Networks používá velmi účinný nástroj pro tvorbu složitějších pravidel ADC – skriptovací jazyk aFleX vycházející z TCL. Existuje celosvětová komunita tvůrců, na jejímž webu je možné najít již hotová, nejčastěji používaná pravidla (včetně konkurenčních výrobců), která nejsou součástí operačního systému. Rovněž lze využít univerzální programovací rozhraní REST API (aXAPI), díky kterému je možné řešení integrovat s procesy DevOps. I zde existuje hodně již připravených receptů Chef, Puppet a Ansible.

### Kvalitní monitoring a vysoká úroveň podpory

Řídicí nástroj pod označením Harmony Controller je určený pro správu i monitoring výkonu aplikací a většího množství zařízení (fyzických i virtuálních). Aplikační monitoring nabízí detailní informace o transakcích při průchodu jednotlivými síťovými prvky. Zařízení je možné rozdělovat do skupin dle libovolných kritérií včetně hromadné konfigurace vybraných parametrů, např. nahrání SSL certifikátů na vybranou skupinu zařízení jedním kliknutím.

Kvalitní podporu zajišťuje celosvětově rozmístěný TAC za účasti předních odborníků. Z reálného provozu je ověřeno, že během velmi krátké doby dostáváte skutečné řešení nebo workaround, což umožňuje garantovat vysoké SLA. Standardní součástí podpory je i zpracování konfiguračních požadavků včetně tvorby aFleX pravidel na míru.

Distribuce a servis



Akreditované školicí centrum



A10 Affinity Platinum partner



A10 Affinity Gold partneři



VÍCE INFORMACÍ NALEZNETE NA [WWW.A10NETWORKS.COM](http://WWW.A10NETWORKS.COM)



## ÚVOD MV ČR

***JUDr. Jaroslav Strouhal, náměstek vnitra pro řízení sekce informačních a komunikačních technologií v úvodu svého vystoupení reagoval na souhrnné informace k tématu, které byly prezentovány na začátku programu. Především připustil, že graf e-government Development Index dle OSN je pro Českou republiku poněkud pesimistický. Toto hodnocení má tři části – lidské zdroje, infrastrukturu a e-government. A především v oblasti e-governmentu, jak se náměstek Strouhal domnívá, jsme udělali vše pro to, abychom se posunuli na čelní příčky. A právě na tyto kroky měl být na konferenci zaměřen blok MV ČR.***

Jeho tématem byla **elektronická identita, Portál občana a elektronický občanský průkaz (eOP)**. Všechny tři tyto nesmírně důležité záležitosti jdou ruku v ruce se skutečností, že 1. 7. 2018 nabyly účinnosti dva významné právní předpisy – **novela zákona o občanských průkazech a zákon o elektronické identifikaci a autentifikaci** (zcela nový právní předpis).



*JUDr. Jaroslav Strouhal,  
náměstek ministra vnitra pro řízení sekce  
informačních a komunikačních technologií*

### **CO?**

**Elektronický občanský průkaz s čipem** – jedná se o elektronickou kartu, která je součástí implementace nařízení **eIDAS**. Hovořilo se o ní velice intenzivně v posledních dvou letech. Je to brána k elektronickým službám, prostředek jednotné identifikace pro občany ČR a bezpečný klíč k nabízeným elektronickým službám. Ke dni konání konference (4. 9. 2018) bylo vydáno již téměř **180 000 eOP**. U celé třetiny tohoto množství byla aktivována veřejná část občanského průkazu.

Náměstek Strouhal rovněž poukázal na skutečnost, že zákon o elektronické identifikaci a autentizaci zavádí tzv. **Národní bod pro identifikaci a autentizaci**. Jak řekl, jedná se o vrstvu informačního systému, která je schovaná na pozadí a uživatelům eOP umožňuje bezpečnou autentizaci do Portálu občana a dalších informačních systémů, které jsou ze strany MV ČR, respektive orgánů veřejné správy postupně představovány. (Národní bod byl v rámci samostatné prezentace představen ředitelem SZR Michalem Peškem a Petrem Kuchařem, ředitelem odboru hlavního architekta.)



## PROČ A NAČ?

**Portál občana** vznikl jako jednotný rozcestník pro obsluhu agend veřejné správy, tedy jakási samoobsluha. Uživatelům, občanům, byl představen 8. 7. 2018, téměř souběžně se startem eOP. V současné době Portál nabízí, podle slov Jaroslava Strouhala, cca 40 služeb veřejné správy. Namátkou ČSSZ, výpisy ze systému Czech POINT a další postupně přibývají. Aktuálně byla „oživena“ **karta** finančního generálního ředitelství, respektive **finanční správy**. Díky tomu je již nyní možné podávat na dálku elektronicky některá **daňová přiznání**. Současně, protože je systém napojen na registr obyvatel a pomocí občanského průkazu je občan jedinečně identifikován, systém umožňuje pracovat s tzv. **inteligentními formuláři**. To znamená, že občané neobtěžuje tím, že by museli vyplňovat data, která již stát vlastní – jsou doplněna automaticky.

Na přelomu září/října by se, dle informací náměstka Strouhala, na Portálu občana měla objevit **karta řidiče**, to tedy znamená možnost kontroly osobního bodového konta a sledování seznamu vlastních dopravních přešupků. Během října, maximálně v listopadu by měla být na Portálu občana zaktivněna **karta Českého úřadu zeměměřického a katastrálního**, jejímž prostřednictvím bude možné obsluhovat agendy, které souvisejí se **správou nemovitostí** a které jsou vedeny v tomto systému.

## KOMPLIKOVANOST = BEZPEČNOST

Jak náměstek Strouhal zdůraznil, aby systém fungoval, vyžaduje určitou míru komplikovanosti, jejímž účelem je zajistit určitou míru kybernetické bezpečnosti. Připustil, že MV ČR je občas kritizováno, že systém je komplikovaný. Ale právě tato komplikovanost přináší potřebnou bezpečnost. Naopak výhodou zmiňovaného propojení eOP a Portálu občana je právě jednoduchost „jedné stránky“. Není tedy nutné se několikrát identifikovat do několika informačních systémů několika úřadů. Jednou jedinkrát se občan zaručeně identifikuje prostřednictvím elektronické-

ho občanského průkazu a pak již „konzumuje“ nabízené služby.

Jaroslav Strouhal v závěru svého vystoupení připustil, že v rámci elektronizace veřejné správy byla výrazná propagační kampaň realizována naposledy v době spuštění Czech POINTů. I proto MV ČR nyní připravilo kampaň zaměřenou na eOP a Portál občana. Ta směřuje na sociální síť a weby veřejné správy. Náměstek Strouhal při této příležitosti prezentoval jeden z propagačních šotů.

Mimo hlavní téma připomenul práce na finalizaci strategického dokumentu Digitální Česko, nebo přípravu tendru na nákup produktů Microsoft, který bude zahrnovat až 700 pověřujících zadavatelů.

Své vystoupení Jaroslav Strouhal uzavřel shrnutím, že přestože jsme v roce 2008 byli v rámci uvedeného hodnocení rozvoje elektronizace veřejné správy na 33. místě na světě a v roce 2018 až na 54. místě, věří, že díky prezentovaným nástrojům e-governmentu dojde nyní k výraznému posunu našeho umístění směrem nahoru. Jak řekl, MV ČR přichystalo vše, co bylo potřeba - jednotnou identifikaci, nosič pro tuto identifikaci a rozcestník pro úřady, tedy Portál občana. Nyní záleží především na ostatních úřadech, municipalitách, krajích, firmách a dalších subjektech, aby se připojovaly do Portálu a zvětšovaly jeho nabídku.



## VZDĚLÁVÁNÍ, PROPAGACE A GOV.CZ

*Ředitel odboru eGovernmentu MV ČR Roman Vrba svým vystoupením navazoval na náměstka Strouhala a upozornil na projekt VAPEG – vzdělávání a propagace v oblasti e-governmentu. Jedná se o projekt financovaný z evropských peněz, který se skládá ze tří částí – analýza, vzdělávání – e-learning a PR. MV ČR v letošním roce realizovalo první krok, tedy analýzu, abychom věděli, jak na tom český e-government ve skutečnosti je.*

Kromě uvedeného porovnání (eGovernment Development Index) existují další hodnocení a MV ČR rovněž disponuje vlastními daty o mínění českých občanů. Podle těchto dat **pouhých 9 %** občanů přesně ví, co je e-government. Přitom ale **85 % občanů** e-government chce a myslí si, že je správné, aby se rozvíjely elektronické služby tak, aby občané mohli s veřejnou správou komunikovat z domova. To doplňuje ještě skutečnost, že 75 % občanů si myslí, že elektronizace veřejné správy jim zjednoduší vyřizování na úřadech, tedy že jim zjednoduší život, a plných 71 % občanů má pocit, že nejsou o mož-



Roman Vrba, ředitel odboru eGovernmentu

nostech veřejné správy dobře informováni. Podle Romana Vrby ta čísla jednoznačně ukazují, že v povědomí občanů je co zlepšovat, zároveň jsou jasným signálem, že občané e-government skutečně chtějí. Proto tedy vznikl projekt VAPEG. V jeho rámci bude pokračovat snaha o vzdělávání především úředníků v obcích s rozšířenou působností, neboť ti mají přímý kontakt s občany. Tento způsob si MV ČR, podle slov Romana Vrby, již vyzkoušelo v rámci eOP,

kdy byly například vytištěny brožurky, které se předávají lidem při vyřizování občanského průkazu tak, aby si mohli během doby, než jim je nový eOP vydán, nastudovat vše potřebné. Pokud jde o PR, snaží se MV ČR využít všechna media, která jsou k dispozici tak, aby se povědomí občanů o e-governmentu prohlubovalo.

Roman Vrba se rovněž krátce věnoval problematice identity CZ. Protože legislativním souvislostem se ve svých vystoupeních věnovali Petr Kuchař a Michal Pešek, pouze poděkoval realizátorům, protože jak řekl, bez projektu identity CZ by celý Portál občana nebyl k ničemu. Je proto rád, že se povedlo obojí nastartovat v jeden den a na začátku července bylo možné Portál občana skutečně spustit.

### eOP

V souvislosti s eOP vidí Roman Vrba jako velice pozitivní, a možná i docela překvapivé, že během dvou prázdninových měsíců si občané aktivovali **35 000 občanek**. Porovnává-li to s datovými schránkami fyzických osob, kterých je cca 100 tisíc, znamená to, že nyní má eOP více jak třetina těchto osob. V rámci budoucí elektronické komunikace se státem to Roman Vrba vnímá jako velice pozitivní.

### Datové schránky

Je podle jeho mínění stále jeden z nejdůležitějších projektů e-governmentu i proto, že Portál občana je bude využívat jako zásadní komunikační kanál. Navenek žádná zásadní změna není patrná, ale podstatné je, že **MV ČR datové schránky koupilo**, je tedy nyní jejich vlastníkem a může je rozvíjet podle svého. Tou první změnou bude plná responzivita datových schránek. Bude tedy možné je bez omezení používat jak v mobilním zařízení (tabletu), tak i v počítači. Designově vykazují jistou podobnost s grafikou Portálu občana. Je to dáno, podle slov Romana Vrby, strategií MV ČR při budování webů pod hlavičkou GOV.CZ. V příštím roce by mělo dojít ještě k doplnění formulářů. To však bude moment, kdy dojde v rámci této nabídky k určitému profesnímu rozdělování, když se počítá s tím, že datové schránky budou více využívat spíše podnikající osoby.

### GOV.CZ

To by měla být, podle Romana Vrby, do budoucna značka pro skupinu webů veřejné správy, která se v základu skládá z informační a transakční části. Transakční část je nyní zastoupena Portálem občana. Zatímco s ním panuje spokojenost, je zřejmé, že v informační části je co dohánět. V tomto směru se jako velice důležitý prvek jeví tzv. životní událost. Občanům je v zásadě jedno, kolik a jakých agend ve veřejné správě existuje. Podstatné pro něj jsou konkrétní události, které musí řešit. Na seznamu životních událostí se tedy nyní intenzivně pracuje a přichází kritický okamžik komunikace s gestory jednotlivých částí, z nichž se určitá životní událost skládá. Roman Vrba to považuje za nejtěžší část celého procesu, protože jde o dohodu, jak přeložit určité paragrafové znění, tedy jak upravit úřednický a právnícký jazyk do tvaru přívětivého a srozumitelného běžným občanům. Dosažení shody je podle Romana Vrby velice složité. MV ČR se o to snaží a v momentě, kdy se tak stane, budou tyto texty jako universální uloženy na jednom místě tak, aby kdokoliv, kdo bude používat životní události nejenom v rámci Portálu občana nebo dalších webů GOV.CZ, ale i v rámci jakéhokoliv jiného portálu či webu, mohl tyto informace jako definice použít a nemusel je znovu vymýšlet. Jde o to, aby se jednalo o určitý obsahový standard. K tomu slouží, podle jeho slov, i do jisté míry zatracovaný projekt PMA3. V této souvislosti demonstroval provázanost jednotlivých agend a množství kroků, které musí při řešení některých životních situací občané podniknout.

Roman Vrba připustil, že určitým vzorem pro GOV.CZ je přístup Nového Zélandu, který je v řešení životních situací velice návodný a srozumitelný, a přál by si, abychom se k takovému webu veřejné správy postupně dopracovali i my.

V závěru svého vystoupení zdůraznil, že máme-li změnit fungování veřejné správy, musíme změnit svoje myšlení, musíme změnit procesy a následně změnit legislativu. Pokud na tyto tři body nepřistoupíme, tak k žádnému výraznějšímu posunu nedojde. To je důvod, proč MV ČR nyní vysvětluje ostatním resortům, že potřebujeme postupovat koordinovaně a vzájemně se doplňovat.

## PROPOJUM SE

**Digitální šampion České republiky Ondřej Felix se ve svém vystoupení pokusil zasadit jednotlivé informace, které doposud zazněly, do určitého širšího kontextu českého e-governmentu.**

Jak uvedl, ono zmiňované 54. místo v celkovém hodnocení e-government Development Index má zcela zásadní důvod v definici toho, co je to e-government. Jak řekl, v takovýchto mezinárodních průzkumech se e-government poslední dobou měří především jako **dostupnost online služeb**. Z toho vyplývá, že elektronizace veřejné správy se nepočítá, back-office veřejné správy se nepočítá. Zohledňuje se pouze snadná orientace občanů v online službách, které jim veřejná správa poskytuje.

Podle Ondřeje Felixe je takový postoj správný. Podle něj má každá inženýrská služba zcela bezpochyby komplikovanou infrastrukturu, ale to klienta, který konzumuje jejím prostřednictvím nějakou službu, většinou vůbec nezajímá. Občan očekává srozumitelnou nabídku a určitě ho nezajímá, kolik tisíc úřadů vlastně tvoří naši veřejnou správu, v kolika agendách a s kolika úředníky tyto služby poskytuje. Občan se potřebuje pouze co nejsnadněji dostat ke konkrétní informaci, co musí udělat, koho kde a jak požádat, pokud něco potřebuje mít schváleno či povoleno od veřejné správy.

Podle Ondřeje Felixe je možné konstatovat, že jsme se konečně s českým e-governmentem dostali do stádia, kdy tzv. nasazujeme pokličku na hrnec, jinými slovy to, co jsme dosud budovali, začínáme konečně sjednocovat jednoduchým uživatelským rozhraním. Dostali jsme se tedy do stádia, kdy 6500 nebo 7000 existujících informačních systémů veřejné správy určitým způsobem propojíme a díky tomu začneme skutečně poskytovat on-line služby. I proto je Ondřej Felix přesvědčen, že nyní bychom z 54. místa měli velmi rychle akcelarovat nahoru a nejen proto, že autoři citovaných průzkumů, se například dosud nedostali do našich datových schránek a nemohli například zohlednit miliony podání vůči veřejné správě, která byla učiněna právě cestou datových schránek.



Ondřej Felix

### POSLEDNÍCH DESET LET Z POHLEDU OF

Někdy v roce 2008 byl jediným informačním systémem veřejné správy, o kterém jsme se bavili, izolovaný informační systém, sedící uvnitř úřadu a obsluhující úředníky. Dnes, máme ve výkonu VS takových systémů 7000 a Ondřej Felix odhaduje, že jako provozní informační systémy veřejné správy funguje (spisové služby, účetnictví, správa majetku ...) dalších 5 až 6000. Všechny jsou schovány „uvnitř“ úřadu a slouží k jeho potřebě. Klient tyto systémy využívat doposud nemohl, neboť přístup k nim byl vždy prostřednictvím úředníka. Celá elektronizace byla schována uvnitř a týkala se především jakéhosi standardizování procesů VS.

Po roce 2008 jsme začali startovat druhou iniciativu, která z těchto „izolovaných ostrovů“ měla pomocí sdílených služeb udělat propojenou síť informačních systémů veřejné správy. Tím startem byly Czech POINTy, tedy pokus o univerzální front-end veřejné správy. Druhou centrální službou byly datové schránky a třetí pak byly základní registry. Dnes tedy máme, jak referoval digitální šampion ČR, na základní registry připojeno 4000 informačních systémů veřejné správy a zásada „neobíhají lidé, ale data“ mezi ZR a klientskými systémy skutečně funguje. Co podle Ondřeje Felixe ještě nefunguje, je dostatečně rychlá úprava legislativy tak, aby přes uvedené, klienti nebyli neustále nuceni obíhat úřady.

Sdílené služby mají podle Ondřeje Felixe společný jeden základní implementační princip – někdo dostal zákonem uloženo vybudovat sdílenou službu, jedna rozpočtová kapitola ji financuje a všichni ji nadále bezplatně používají. To je jediná metoda sdílení ve veřejné správě, která je správná a nosná, ale je nutné se posunout ještě o další krok dále.

## PROPOJENÝ DATOVÝ FOND

Od sdílených systémů veřejné správy (nejen ZR, ale rovněž agendových systémů, jako např. živnostenský rejstřík...) je podle slov Ondřeje Felixe nutné **přejít k propojeným informačním systémům**. Tedy v zásadě to, co jsme si ve sdílených systémech doposud vytvořili (například pro registry jako editory, publikátory údajů a čtenáře údajů), začít provozovat jako propojený systém, který umožní před klientem veřejné správy schovat komplexnost. Budeme tak moci jednat, jako kdyby se jednalo o jednu homogenní veřejnou správu. Můžeme pak záležitosti řešit od jednotlivých uživatelských agendových potřeb, i když se úřadovat musí v rámci jednotlivých agendových informačních systémů veřejné správy.

I proto nyní, jak řekl Ondřej Felix, ukazujeme způsob, jak propojovat jednotlivé informační systémy veřejné správy a na bázi základních registrů jdeme budovat propojený datový fond. Základní registry + eGon ServiceBus + publikující evidenční zdroje autoritativních údajů, tedy ti, kdo jsou nositeli právně závazných údajů, a ZR spojené s údaji vedenými v evidencích veřejné správy (registri řidičů, registr motorových vozidel) jsou všechny propojeny do jednoho komplexu a vytváří datovou základnu pro subjekty a objekty práva, které se tak mohou dopracovat ke svým životním situacím a svým právům. To je tzv. propojený datový fond. Propojené portály pak umožňují přístup ke každému z nich s jednou identitou a jedním způsobem přihlášení.

## OTEVŘENÝ DATOVÝ FOND

Otevřený datový fond je, jak Ondřej Felix upozornil, založen na iniciativě, která nezačala v Česku. V zásadě říká, že všechna data, která se vytvářejí a používají ve veřejné správě, by měla být dostupná ve veřejné správě i mimo ni. A zároveň platí, že se budeme snažit produkovat co nejvíce datasetů, které jsou veřejně použitelné a může s nimi pracovat i veřejná správa.

## PROPOJUJTE SE A MNOŽTE SE

Portál občana je první ukázkou základní komponenty propojených informačních systémů veřejné správy. Ondřej Felix zdůraznil, že v Portálu občana nevznikají žádné nové údaje, žádné v něm nejsou uloženy, Portál občana pouze publikuje údaje ostatních systémů veřejné správy, zpřístupňuje funkce úplného elektronického podání, zpřístupňuje výpisy z informačních systémů veřejné správy. Je to tedy základní brána vstupu k údajům a podáním v celé veřejné správě. Abychom byli schopni jej rozvíjet, musíme se propojovat – doposud jsme podle slov Ondřeje Felixe udělali, co jsme mohli ve sdílené infrastruktuře, teď se musí jednotlivé orgány veřejné moci se svými agendami připojit do sdílené infrastruktury, ať jako datové zdroje či jako prezentátoři údajů pro občany či plnitelé úplných elektronických podání. Celý systém bude fungovat jako federace, která před občany schová komplexnost veřejné správy. Pojďme se tedy propojovat.

0100 01100011  
1010000101000000  
1000100000011000  
01001000011  
00100000  
0100 0110001  
11110 00100000



01100010 01101  
011011101001001  
00110101011  
1101001001001  
11011011001  
01100010110100  
01100010110100  
11010010110110  
01101111 0110

## JAK SE IDENTIFIKOVAT?

**Petr Kuchař, ředitel odboru hlavního architekta MV ČR, byl dalším řečníkem v řadě, který se ze svého pohledu věnoval problematice Portálu občana. Připomenul, že OHA má za úkol budování sdílených služeb centrálního charakteru a jednou takovou sdílenou službou, kterou se nyní povedlo vybudovat, je Národní identitní autorita. Podle Petra Kuchaře je svým významem srovnatelná se základními registry, datovými schránkami, nebo Czech POINTy. Jedná se o čtvrtou, velice důležitou službu, na které pak budou navazovat všechny další služby, o nichž se na konferenci hovoří.**

Petr Kuchař definoval Národní identitní prostor jako ledovec, kdy část služeb je schovaná pod hladinou (principy funkce, stroje atp.). O jejich existenci my, jako uživatelé, vlastně nemusíme vědět. Nad hladinou jsou pak služby poskytovatelů on-line služeb, které nalezneme na jejich portálech, a na pomezí hladiny jsou poskytovatelé identitních služeb.

### PRINCIP NIP

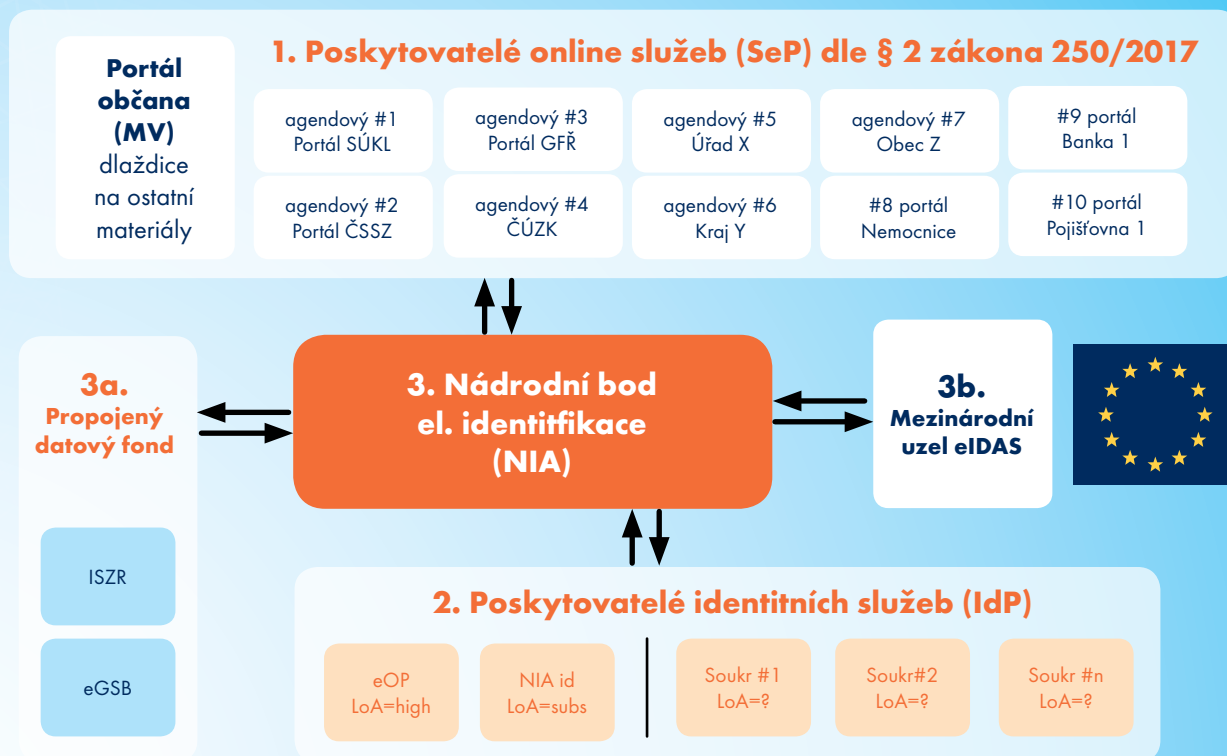
Celá identitní autorita je postavena na základě § 2 zákona č. 250/2017 Sb., který říká, že „vyžaduje-li právní předpis, nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace **pouze** prostřednictvím kvalifikovaného systé-



Petr Kuchař, ředitel odboru hlavního architekta MV ČR

mu elektronické identifikace“. Elektronická identita každé fyzické osoby je uložena v registru obyvatel, k jedné identitě může být připojeno neomezeně identifikačních prostředků, přičemž každý z nich má jinou úroveň důvěry.

Principem Národního identitního prostoru je propojení fyzické osoby, on-line služby, identitní autority a poskytovatele identitní služby. Pokud občan chce využít nějakou službu, například přes Portál občana, může se zde přihlásit tlačítkem a je odeslán na Národní identitní autoritu. Zde vybere poskytovatele identitní služby, jehož identitní prostředek využívá. Národní identitní autorita na příslušné úrovni ztotožnění potvrdí a sdělí poskytovateli on-line služby bezvýznamový identifikátor. Portál tento identifikátor obdrží a převede na agendový identifikátor fyzické



osoby. Občan v tom okamžiku může ve své agendě realizovat úkony, které potřebuje (lhostejno, zda se jedná o Portál občana, Portál ČSSZ atp., princip je stále stejný).

## AKTUÁLNÍ STAV NIP

Národní identitní prostor sestává z několika skupin subjektů – **poskytovatelé identitní služby** (nyní máme dva a další testujeme – jednáme s bankami, telefonními operátory i certifikačními autoritami). Vypadá to, že kromě dvou státních **poskytovatelů elektronické identity** (eOP a uživatelské jméno+jednorázové SMS heslo) budou i některé komerční.

Dále je v NIP pět poskytovatelů on-line služeb – Portál občana, Portál NIA, Portál státního úřadu pro kontrolu léčiv – eRecept, Portál ČSSZ a Portál GFŘ. O dalším rozšíření se nyní jedná.

Vedle toho patří do Národního identitního schématu i **mezinárodní brána**. Elektronická identita není totiž projektem jen České republiky, ale je založena na nařízení eIDAS. Jde tedy o propojení na národní brány ostatních států. Zde nabývají důležitosti tzv. **notifikované systémy** – evropské státy musí notifikovat svůj identitní systém Evropské komisi, tím se informace poskytne všem ostat-

ním zemím na vědomí a dojde k mezinárodnímu propojení. V září proběhla notifikace SRN a následují další státy, jako Itálie, Belgie, Estonsko atp. (více informací ve vystoupení Roberta Piffly). I Česká republika bude u Evropské komise usilovat o notifikaci našeho Národního identitního prostoru, aby v evropských státech bylo možné u on-line služeb použít naše české identitní prostředky. Potřebnou dokumentaci nyní připravujeme a zahájíme proces notifikace do konce roku.

V současné době existuje tedy velká skupina poskytovatelů on-line služeb, postupně se k ní budou připojovat agendové systémy dalších ministerstev a úřadů, municipality, kraje, obce atd. Díky tomu, že celá veřejná správa se musí do dvou let připojit k Národní identitní autoritě, bude tato skupina skutečně velmi velká. Je velice pravděpodobné, že se zde objeví i soukromoprávní společnosti (pojišťovny, banky), kterým zákon nějakým způsobem přikazuje identifikovat klienta. Nepočítáme však s tím, že by se do NIP připojovaly soukromé společnosti typu internetových obchodů, především proto, že zákon tak nepraví. Uprostřed struktury je Národní bod elektronické identifikace (NIA), propojený na mezinárodní uzel eIDAS. V pozadí NIA je systém základních registrů, zejména pak registr obyvatel (ROB). Jedinou službou, kterou uživatel na chvíli vidí, je Portál identitní služby v okamžiku připojení.

## KDO JE KDO?

Podle zákona č. 250/2017 Sb., o elektronické identifikaci, může být kvalifikovaným správcem pouze státní orgán, nebo osoba, které byla udělena akreditace (seznam těchto kvalifikovaných správců vede SZR).

Provozovatel on-line služby je takový poskytovatel, který umožňuje v rámci svého portálu prokázání totožnosti podle zákona č. 250/2017 SB., o elektronické identifikaci. Seznam těchto kvalifikovaných poskytovatelů vede SZR (nyní se jedná např. o ePortál ČSSZ, ePreskripce SÚKL, Daňový portál, Portál občana ...)

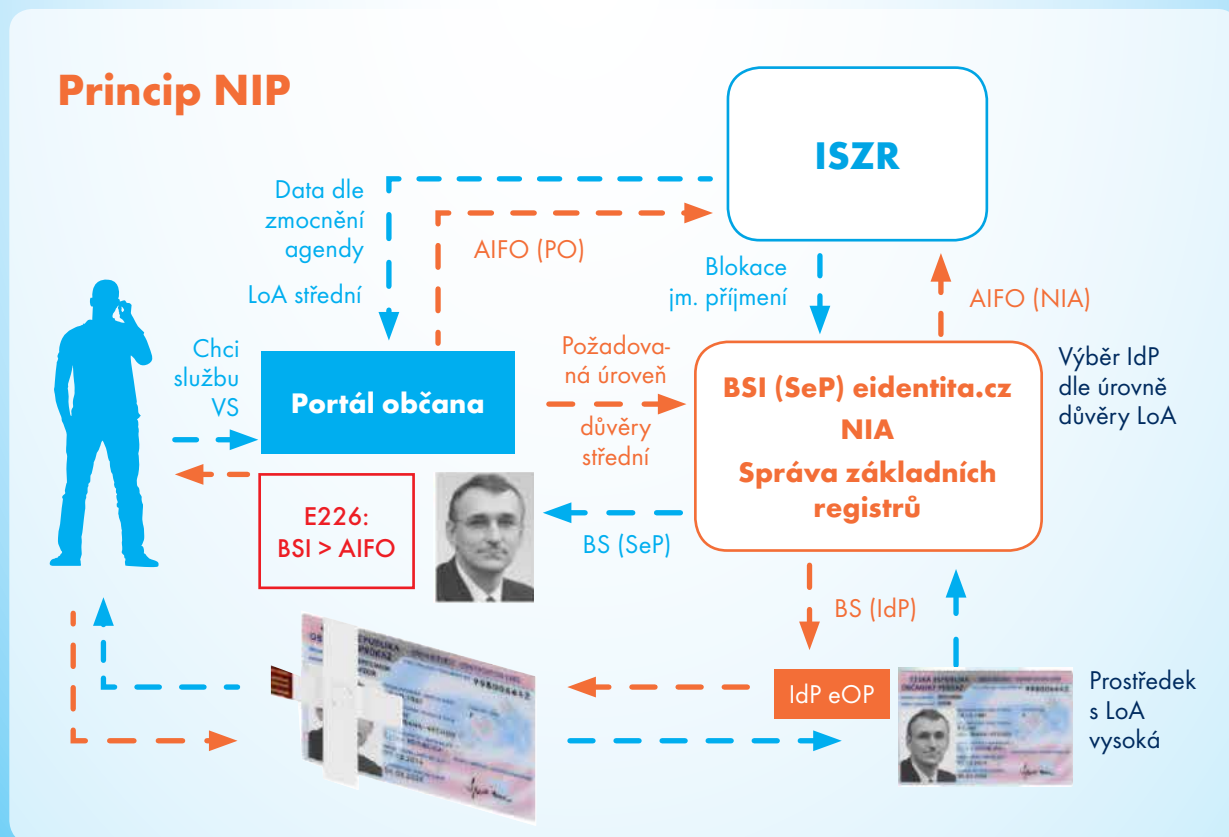
## JAK NA TO?

**Elektronický občanský průkaz** nově obsahuje identifikační aplikaci. Elektronické funkce eOP si mohou, ale nemusím občané aktivovat při přebírání průkazu. Nicméně eOP vyžaduje znalostní kódy právě proto, že odemká přístup k identifikačnímu certifikátu. Úroveň ověření díky tomuto prostředku je vysoká. Aby bylo možné eOP použít, je potřeba instalovat tzv. obslužný software (Middleware), který je ke stažení na stránkách eldentita.cz.

V současné době je k dispozici Middleware pro platformu Windows. Do konce října by podle smlouvy se STC měl být k dispozici pro MacOS, Linus, iOS i Android.

Pro práci s kontaktním čipem eOP je nutné kartu vsunout do čtečky čipových karet, která je připojena buď prostřednictvím USB se stolním počítačem (čtečka musí splňovat ISO/IEC 7816 a k dostání je v ceně do 200 Kč), nebo případně čtečky, kterou je možné připojit pomocí Bluetooth k mobilnímu zařízení. Cena čteček je v řádu několika set korun a podporovány jsou všechny značky, které se momentálně na trhu vyskytují. **Čtečku si musí občan pořídit sám.**

Protože eOP může z výrobních důvodů dostat maximálně 1,5 mil. lidí za rok, tak pro ostatní, kteří nemají eOP buď proto, že nechtějí, nebo se na ně hned nedostane, je k dispozici druhá forma identifikace – JménoHesloSMS. Fakticky se jedná o uživatelský účet v NIA, kam se přihlásím, a druhý faktor ověření je SMS kód, který obdržím do mobilního telefonu. Tento prostředek poskytuje střední úroveň ověření.





## Platební karty jako základ Smart Cities

S konceptem Smart Cities neboli chytrých měst se setkáváme stále častěji. Definovat je můžeme např. jako cestu k udržitelnému rozvoji měst s využitím moderních technologií nebo jako město, kterému se povedlo využít stávající digitální technologie pro lepší služby obyvatel a dostupné zdroje s minimalizací negativních dopadů na životní prostředí. Vedle technologického vývoje jsou důležitým hybatelem Smart City projektů demografické pohyby a s nimi související dopady na dopravu.

## Role dopravy

Doprava a dopravní obslužnost tvoří jednu z klíčových oblastí Smart Cities, ale je třeba ji vnímat jak z hlediska veřejné, tak i individuální automobilové dopravy. V rámci veřejné dopravy je naprosto dominantní městská hromadná doprava, která každoročně přepraví přes 81 % všech cestujících veřejné dopravy. Automobilová přeprava ve městech zvyšuje požadavky na organizaci dopravy, řešení ucpaných silnic a environmentálních otázek a především na oblast parkování a parkovacích služeb. Funkční a efektivní doprava je kritickým předpokladem úspěšného fungování chytrého města. V tuzemských podmínkách se nyní nedílnou součástí dopravních řešení stávají platební karty.

## Platební karty základem chytrých měst

Předpokladem úspěchu projektů Smart Cities je nutnost využít běžně dostupné a široce využívané technologie, což jsou i platební karty, mobilní aplikace nebo online platby. V České republice je nyní v přepočtu 1,1 platební karty na občana a devět z deseti karet je bezkontaktních. Občané si již zvykli platit kartou všude tam, kde je terminál k dispozici, a očekávají platbu kartou i na dalších místech, např. v dopravě, při parkování nebo u lékaře. Platební karty již nepředstavují pouze nástroj, se kterým lze pohodlně, rychle a bezpečně zaplatit. Rozmanitost a šíře jejich využití dále roste a vyvíjí se. Platební funkce zůstává základním stavebním parametrem karet v rámci projektů Smart Cities, karta ale může sloužit i jako identifikátor k zakoupené službě, třeba k jízdě na veřejnou dopravu, vstupence do kina, na festival nebo do zoo. Obrovskou devízou platebních karet je jejich vysoká bezpečnost (zaručená mezinárodními bezpečnostními standardy) a již vybudovaná a plně funkční infrastruktura, která je ve správě bank a platebních společností.

## Funkční projekty

Smart City projektů je poměrně dost, jednoznačně nejdále je oblast dopravy. Příkladem může být Ostrava, kde byla v roce 2016 všechna vozidla MHD plně vybavena bezkontaktními čtečkami, takže pro cestování stačí připsat platební kartou a systém sám určí optimální cenu jízdného, a to bez tisku papírového lístku. Jedná se o první projekt v České republice a druhý v Evropě po Londýně, který zahrnuje i zastropování jízdného. V případě nákupu více jednorázových jízdenek během jednoho dne činí maximální částka cenu jednodenní jízdenky. Platební karta může úspěšně sloužit i jako vstupenka (využita byla na festivalech Burgerfest nebo Svět knihy), využívána je také jako klubová karta

ČSOB ve sportovních klubech Slovan Liberec nebo HC Pardubice. Z úspěšných mobilních aplikací lze zmínit Můj Vlak Českých drah, která umožňuje vedle vyhledání spojení pohodlný nákup jízdního dokladu a jeho úhradu platební kartou nebo mobilní peněženkou Mastercard. Zakoupený lístek je poté uložen v mobilní aplikaci a pomocí QR kódu průvodčím kontrolován. Mobilní aplikace ClickPark zase umožňuje nákup parkování v Berouně, Blansku, Chrudimi nebo Sázavě.



 banka  
i pojišťovna

## NÁRODNÍ BOD A JAK S NÍM PRACOVAT

**Ředitel Správy základních registrů Michal Pešek v úvodu svého krátkého vstupu zdůraznil své přesvědčení, že z onoho 54. místa hodnocení rozvoje e-governmentu, které bylo prezentováno v úvodu konference, se určitě posuneme výrazně nahoru. Po letech příprav řady projektů totiž nyní, podle jeho slov, došlo ke skutečnému průlomu.**

Správa základních registrů je nově správcem Národního bodu pro identifikaci a autentizaci, který zahrnuje uživatelské rozhraní, uživatelský účet, informační web, poskytovatele služeb, SZR atd. Propojuje tedy uživatele a poskytovatele služeb i poskytovatele identit, což sebou nese velkou odpovědnost. Michal Pešek je však přesvědčen,



Michal Pešek,  
ředitel Správy základních registrů

Národní bod nejenže propojuje poskytovatele služeb a poskytovatele identit, ale zároveň aproximuje nařízení eIDAS do českého právního řádu. V této souvislosti je tedy v rámci Národního bodu nutné zajistit propojení v rámci EU. Michal Pešek ujistil, že nyní probíhá závěrečná fáze testování tak, abychom skutečně byli schopni uznávat všechny nahlášené prostředky, které veškeré státy EU oznámí.

Celý portál je, podle jeho slov, provozován v bezpečném prostředí centrálního místa služeb, přesto je vhodné zdůraznit, že **pracuje pouze s údaji**, které jsou poskytovány **ze základních registrů na základě souhlasu občanů**.

Michal Pešek dále ukázal, jak vypadá uživatelské prostředí portálu eldentita.cz, tedy určitého back office ke službám, o nichž se již hovořilo. Ukázal, že je možné zvolit přihlášení ke službám Portálu občana pomocí datových schránek nebo e-identitou. Zároveň má občan po přihlášení možnost zvolit a vyplnit údaje, které „státu“ dále poskytne – telefon, e-mail atp. Mimo jiné mohou občanům touto cestou přicházet avíza o nových službách, které jsou k dispozici, a další důležité informace.

Informační web info.eidentita.cz umožňuje uživatelům orientaci tak, aby chápali jednotlivé použité zkratky a pojmy. V případě nejasností, nebo potřeby pomoci je k dispozici komunikační linka 225 514 777, která funguje 24 hodin 7 dní v týdnu.

že to, co bylo vybudováno, je bezpečný nástroj pro ověření totožnosti. Jedná se o systém, který využívá propojený datový fond, tedy základní registry. Základním zdrojem informací pro Národní bod je registr obyvatel. Občan se může rozhodnout, jakým identitním prostředkem se přihlásí, zda eOP či prostřednictvím jména a hesla.

**info.eidentita.cz**  
**225 514 777**



## Cena magazínu Egovernment

**V rámci konference e-government 20:10 udělil Magazín Egovernment ocenění za přínos elektronizaci veřejné správy ČR náměstkovi ministra vnitra Jaroslavu Strouhalovi**

**Ocenění bylo uděleno nejen v souvislosti se zavedením a spuštěním Portálu občana ale především vzhledem k tomu, že náměstek Strouhal:**

- na ministerstvu vnitra vede tým, který dokončil vytvoření robustní komunikační infrastruktury,
- díky jeho práci a lidí, které vede, se podařilo spustit pro občany systém digitálních služeb,
- podařilo se mu také prosadit potřebnou legislativu (zákon o elektronické identifikaci a novela zákona o občanských průkazech), bez které by nebylo možné nic z toho realizovat.
- dobré výsledky hlásí také jemu podřízený odbor, který kontroluje velké ICT projekty a realizuje výrazné úspory prostřednictvím centrálním nákupům.

## SYSTÉMY JSOU BEZPEČNÉ

*Miroslav Tůma, ředitel odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií MV ČR, se ze svého, tedy kyberbezpečnostního pohledu věnoval všem projektům, které byly doposud prezentovány. Všechny přítomné ubezpečil o tom, že tyto systémy jsou funkční nejenom z pohledu občana, ale rovněž z pohledu kyberbezpečnosti a MV ČR dělá vše pro to, aby nebyly napadeny. V případě, že by na ně bylo útočeno, aby těmto útokům odolaly. MV ČR vnímá podle Miroslava Tůmy systémy e-governmentu jako klíčové, i proto jejich zabezpečení neustále zdokonaluje, neustále probíhá jeho vyhodnocování, ať již na bázi organizačního charakteru, tak na bázi technického opatření.*

Z pohledu definičního rámce kybernetické bezpečnosti MV ČR zabezpečuje informace, které jsou uloženy v rámci kybernetických systémů. V rámci digitálních informací je tento pohled samozřejmě širší a zahrnuje i aktiva, na kterých vše „běží“ a bez kterých by nebylo možné systémy provozovat. To znamená, že kyberbezpečnost, respektive její zajištění, zahrnuje i ostatní informace, které jsou nutné pro fungování systému. Rámec, na který se zaměřuje MV ČR, zahrnuje kontext celé bezpečnosti a bezpečnostních informací, se kterými MV ČR pracuje a jichž má nejvíce v celé státní správě. MV ČR se tedy v rámci své působnosti v souvislosti s kybernetickou bezpečností zaměřuje nejen na vlastní perimetr, ale ten záběr je daleko širší. V rámci systémů MV ČR se jedná konkrétně o 58 organizací a následně 30 systémů, které se pohybují v oblasti e-governmentu a v rámci kritické informační infrastruktury. Od vydání zákona přibýlo 5 systémů v oblasti významných nebo kritických systémů. To se, podle slov Miroslava Tůmy, týká například i Portálu veřejné správy a Portálu občana, který je zařazen mezi významné informační systémy a už od příštího roku bude překlasifikován do kritické informační infrastruktury.



*Miroslav Tůma, ředitel odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií MV ČR*

ry. Objevuje se tu rovněž další systém – NIA, neboť probíhá právě jeho klasifikace, která rozhodne, zda bude významným systémem a nebo systémem kritické informační infrastruktury. Dostáváme se tedy na magické číslo **30 systémů**.

Miroslav Tůma zdůraznil, že odbor kyberbezpečnosti pracuje v cyklu neustálého zdokonalování – systém řízení je nastaven ve dvou rovinách, existují jasně definovaná pravidla a jasně definované standardy, které se snaží v rámci jednotlivých systémů standardizovat a unifikovat tak, aby všechny systémy fungovaly jednotlivě. Aby se tedy nejednalo o unifikovaný ostrov, ale využívaly se nejen synergie mezi systémy, ale i jednotlivé přístupy, které jsou platné pro všechny systémy. To znamená, že je zaváděn organizační systém i v rámci systému ISVS a následně je vše monitorováno prostřednictvím poměrně masivního dohledového centra.

Porovnáme-li meziroční nárůst kybernetických hrozeb, tak počet útoků stále roste. Podle Miroslava Tůmy se daří nekopírovat tento negativní trend – tzn. útoky, které



0100 01100011  
 1111000011000000  
 11000001000011000011  
 1100010000000000  
 11001100011  
 11010010111010001100  
 110000000000  
 0100001100001  
 1111000011000000  
 11000001000010000  
 1100000000000000

se prosadily, nerostou stejným tempem jako počet útoků samotných. Pokud jde o kybernetické bezpečnostní incidenty, daří se je podle Miroslav Tůmy držet v řádech jednotek – v letech 2016–2017 byly tři, v letošním roce máme 2 kybernetické incidenty. Důležité je, že ani **tyto incidenty nezpůsobily žádný dopad**, ať už na úrovni technickou, materiální, nebo únikem informací, tzn. podařilo se nám vše zachytit a zastavit včas.

V závěru vystoupení Miroslav Tůma zdůraznil, že počet útoků stále roste a bude růst. MV ČR se adekvátně tomu snaží systémy, na které dohlíží, zabezpečovat a toto zabezpečení neustále zdokonalovat. I proto může všechny ujistit, **že systémy jsou funkční a bezpečné.**

## DIGITÁLNÍ ČESKO

**Zmocněnec vlády pro IT a digitalizaci Vladimír Dzurilla svým vystoupením na konferenci přiblížil, co vše bylo již v rámci strategie Digitální Česko realizováno, co je naplánováno a jak vlastně bude informační koncepce ČR, o které hovořilo i MV ČR, zakomponována do této strategie. Zmínil také, jak digitalizaci veřejné správy ovlivňují například požadavky EU, nebo jaký dopad má digitalizace na takové oblasti, jako je průmysl, či digitální společnost. Přítomné rovněž seznámil s názory a postoji některých členů vlády.**

Podle Vladimíra Dzurilly je základem pro uvedenou koncepci programové prohlášení. To současně je druhým v pořadí, obsahuje několik změn, ale z našeho pohledu je důležité, že digitalizace opět zůstala prioritou vlády. Nacházela se dokonce mezi šesticí priorit, s nimiž premiér předstoupil před Sněmovnu, když žádal o vyslovení důvěry. Z koncepčního pohledu byla podstatná snaha o vytvoření strategie, která bude mít víceletou „trvanlivost“. Jak Vladimír Dzurilla upozornil, historicky existují v ČR možná desítky usnesení vlády k tématu IT, stejně jako byla postupně vypracována řada strategií. Problém je, že většinou nejsou nijak uzavřené. Současná vláda by je proto ráda nějak smysluplně provázala.

Vladimír Dzurilla následně zdůraznil, že digitalizace a elektronizace neznamená primárně pouze úspory. Je podle něj jasné, že minimálně na počátku někte-



Zmocněnec vlády pro IT a digitalizaci  
Vladimír Dzurilla

rých projektů jsou potřebné rozsáhlé investice, musí být však vždy vynaloženy účelně. I proto vznikla zmiňovaná koncepce Digitální Česko. Ta byla na počátku stavěna skutečně pouze jako informační koncepce v přímé souvislosti s budováním e-governmentu. Ukázalo se ale, že její dosah je daleko širší. Že je a bude přímo ovlivňována tlaky zvenčí, především z EU. Zároveň ale musí respektovat nové možnosti a požadavky jiných oblastí, například průmyslu. V souvislosti s vlivem a množstvím nových technologií, které realizaci strategie ovlivňují a budou ovlivňovat, vyvstala důležitost standardizace a sdílení informací tak, aby nedocházelo k duplicitním řešením téhož na různých úřadech. Jedna ze zásad strategie tedy říká – **je nutné sdílet, abychom se propojili.**

## STRATEGIE

Samotná strategie obsahuje řadu z toho, co prezentovalo Ministerstvo vnitra. Například on-line služby pro občany a firmy či centrálně a efektivně řízené IT je obojí zahrnuto v cílech strategie. Obsahuje samozřejmě další body a cíle, přičemž jedním z těch nejdůležitějších je **legislativa a personální záležitosti**. Důvodem je skutečnost, že bez legislativy respektující možnosti a nároky digitálního prostředí není možné rozvíjet veřejnou správu, stejně jako to není možné bez schopných lidí. Strategie Digitální Česko by měla všechny tyto cíle či požadavky pospojovat a provázat. Stejně tak by měla sledovat vlivy na současnou legislativu, tedy především, jaké jsou aktuální trendy a jaké jsou regulační kroky ze strany EU. Je to podstatné pro vyjasnění toho, co potřebujeme prosazovat ve vztahu k EU, a naopak, co je nutné implementovat jako požadavek EU. A samozřejmě se strategie dotýká i oblasti průmyslu a vlastně všeho, co má označení 4.0, přičemž řeší, jak právě tato problematika zapadá či navazuje na e-government.

## JEDNÁ SE TEDY CELKEM O 4 DOKUMENTY – PILÍŘE:

- ČDE** – Česko v digitální Evropě;
- IK ČR** – informační koncepce ČR;
- DES** – digitální ekonomika a společnost;
- d;Č** – Digitální Česko (zastřešující projekt).

Tyto pilíře jsou dohromady popsány na **47 stranách**. Nejedná se tedy o nijak rozsáhlou a detailní koncepci. Je zde ale popsáno celkem **43 principů**, které vznikly buď v reakci na požadavky EU či Tallinnské deklarace. Materiál tak rozpracovává **15 hlavních cílů** a **115 dílčích cílů**, které v současné době dále rozepisujeme do **21 příloh**. Vznikají přitom implementační plány tak, aby hlavní cíle, dílčí cíle i cíle zpracované v rámci jednotlivých dokumentů byly vzájemně propojené, provázané.

## SITUACE

Koncepce je hotová, prošla připomínkovým řízením a máme za sebou úspěšně vypořádané první kolo, jsme ve druhém a očekáváme, že velmi brzo bude tato koncepce schválena vládou (schváleno 3. 10. 2018 – pozn. redakce) a že můžeme s jednotlivými ministerstvy a úřady na základě této koncepce začít pracovat tak, aby vše, co se bude dít dál, bylo na ni navázáno. Jak Vladimír Dzurilla uvedl, nyní je v přípravě metodika řízení programu. Byly zmapovány stávající projekty, které prošly OHA tak, aby byl ověřen jejich soulad s informační koncepcí. Stav je takový, že na rozvoj on-line služeb, což je cíl 1, jsme vymezili 142 projektů, ohledně digitalizace dosud nedigitalizovaného obsahu 140 projektů. Zlepšení katalogu otevřených dat se týkalo 54, veřejného datového fondu 51 a propojeného datového fondu 48 projektů. Vladimír Dzurilla to považuje za dostatečný důkaz toho, že koncepce funguje a že jsme schopni jednotlivé projekty reálně mapovat.

## RVIS

Důležitým momentem je **nový statut Rady vlády pro informační společnost (RVIS)**. Vše v souvislosti s Digitálním Českem prochází přes RVIS, který je poradním orgánem vlády. Podstatné je, že nyní jsou do tohoto procesu zapojeni i IT náměstci ze všech resortů. Postupně by měli být zapojeni i náměstci ostatních oblastí tak, aby se nejednalo pouze o IT komunitu, ale byla pokryta i oblast digitální ekonomiky a digitální společnosti atp. Vladimír Dzurilla považuje za velice přínosné, že se podařilo navázat spolupráci rovněž se soukromým sektorem, kraji atp.

## CO PŘIPRAVUJEME?

Jak bylo již řečeno, jsou nyní zpracovávány implementační plány (celkem 21), které vycházejí přímo z informační koncepce. Při navazování na jednotlivé projekty je sledován výsledný efekt projektu v souvislosti s vynaloženým úsilím při jeho realizaci. Projekty, které mají sice velký dopad, ale zároveň vyžadují značné úsilí, by měly vznikat koordinovaně (například eGovernment Cloud). Naopak projekty, které mají značný efekt s vynaložením nižšího úsilí (např. Portál občana a následné připojení), mohou vznikat samostatně v rámci resortů. Z těch **významných, či náročných projektů**, kterých je nyní 32, uvedl Vladimír Dzurilla například společný notifikační server, společné call centrum, které by vzniklo pro všechny, sandboxy, tzn. testovací prostředí, platební brána, eGovernment Cloud atd.

Mezi **projekty realizované s nižším úsilím**, ale velkým dopadem, které by měly být realizovány v rámci jednotlivých resortů, se jedná například o on-line služby, metodiku pro veřejné zakázky, realizaci veřejného datového fondu, propojený datový fond atp. Představa je podle Vladimíra Dzurilly taková, že by bylo najednou realizováno 14 projektů – každý resort jeden projekt, který se jednou zaplatí a je 13x poskytnut v rámci tohoto balíku ostatním.

## PODPORA MINISTRŮ

Vystoupení Vladimíra Dzurilly bylo proloženo videovstupem některých ministrů:

Premiér vlády ČR **Andrej Babiš** pozdravil účastníky mikulovské konference a zdůraznil, že digitalizace je prioritou vlády, a proto podporuje Digitální Česko, a to nejen proto, že je to zřejmá cesta k efektivitě a úsporám. Vítá odstartování projektu eOP a Portálu občana, ale doufá, že postupně nabídku rozšíříme ze současných 37 na daleko větší počet služeb. I proto avizoval listopadovou konferenci, na které bude estonský premiér prezentovat jejich situaci, kde mají k dispozici zhruba 170 služeb.

Ministr vnitra **Jan Hamáček** zdůraznil, že elektronizace veřejné správy je z jeho pohledu nedílnou součástí resortu a že ji považuje za stejně důležitou jako ostatní oblasti, které řeší. Ministryně financí **Alena Schillerová** potvrdila nutnost vynaložit peníze na realizaci konkrétních projektů, ale zároveň zdůraznila nutnost sledovat jejich účelnost. Ministryně průmyslu a obchodu **Marta Nováková** vnímá význam Digitálního Česka jako velkou výzvu a byla by ráda, pokud by MPO bylo leadrem v této oblasti.

Vladimír Dzurilla vysvětlil, že důvodem, proč oslovil jednotlivé ministry, je skutečnost, že programové prohlášení je stále jen „pouhý“ dokument. Na jeho základě byla zpracována koncepce Digitální Česko, kterou samozřejmě ministři viděli a budou schvalovat (schváleno 3. 10. 2018), ale je dobré vědět, zda ji podporují. Jen tak můžeme vědět, jakou míru zapojení od nich můžeme očekávat. Ministři, se kterými o tom hovořil, Vladimíru Dzurillovi vyjádřili podporu. Vědí, že v digitalizaci je budoucnost, a jsou ochotni a připraveni podporovat jak tvorbu konkrétních služeb, tak jejich napojení na ostatní služby veřejné správy a realizovat Digitální Česko.



THE  
BEST  
2018

Sbírka projektů elektronizace Veřejné správy  
Uzávěrka přihlášek projektů 30. 10. 2018  
Vyhlášení výsledků – Obecní dům 19. 11. 2018

Více informací a přihláška na:

**[www.egovernment.cz](http://www.egovernment.cz)** pod záložkou Best 2018

## ČESKO V DIGITÁLNÍ EVROPĚ

**Ředitel odboru koordinace hospodářských politik EU z Úřadu vlády ČR Zbyněk Smetana představil jeden z pilířů Digitálního Česka, který se týká především evropské roviny. Jak uvedl, jedním z klíčových témat, kterým se s kolegy věnuje, je koordinace digitální agendy, především v kontextu jednotného digitálního trhu (tzv. Single Digital Market). Je to jedním z prioritních témat současné Evropské komise a jedno z hlavních témat diskutovaných na evropské úrovni obecně.**

V rámci Digitálního Česka mají na Úřadu vlády na starosti část Česka v digitální Evropě. Jde o nastavení základní ucelené koncepce, která by zajistila jednotný aktivní přístup České republiky v rámci struktur EU a zároveň zajistila provázání na existující struktury na národní úrovni. Jak řekl, navazují na řadu materiálů, které zde byly již vytvořeny (např. koncepce působení ČR v EU, rámcová pozice ke strategii pro jednotný digitální trh v Evropě atp.).

### JEDNA VIZE, DVĚ MOTIVACE

Zbyněk Smetana vidí pro Digitální Česko dvě motivace.

**1** První je potřeba koordinace. Digitální agenda je specifická, nedá se zcela jednoduše zarámovat do struktur státní správy. Zde platí, že většinou jde o jeden konkrétní materiál, který dostane jeden konkrétní resort a ten jej řeší od začátku do konce. Digitalizace je však horizontální, průřezová záležitost, která se z pravidla týká vždy všech. Proto na Úřadu vlády cítili potřebu koordinace tak, aby spolu jednotlivá ministerstva, ale i hospodářští a sociální partneři, profesní sdružení, podniky atp. komunikovali. Jde o to, aby probíhala výměna názorů, idejí, myšlenek a přístupů. S tím rovněž souvisí potřeba stanovení cílů na národní úrovni. Právě v oblasti digitalizace totiž řada agend vzniká tak, že se objeví určitá nová technologie a v souvislosti s ní vyvstanou otázky, zda je potřeba určitá regu-



Zbyněk Smetana, ředitel odboru koordinace hospodářských politik EU z Úřadu vlády

lace, nebo ne. Z národního pohledu je dobré, pokud si dokážeme vytvořit názor či postoj k takovému problému co nejdříve. Můžeme jej pak propagovat i na nadnárodní, tedy evropské úrovni. Pokud se naopak, v rámci evropských procesů, dostaneme „ke slovu“ v okamžiku, kdy už existuje nějaký konkrétní legislativní návrh, je to vlastně konec procesu, kdy mnoho neovlivníme. Jak zdůraznil Zbyněk Smetana, je nutné vystoupit s jasným názorem v momentě, kdy probíhá jednání o tom, zda nějaký členský stát má s konkrétním problémem konkrétní zkušenost, národní přístup, regulaci, protože pak se zvažuje, do jaké míry je možné tento „lokální“ postoj aplikovat nadnárodně. Je tedy potřeba, aby ČR dokázala formulovat co nejdříve vlastní přístup, vlastní pozici. A právě to je záležitost, která by se neměla odehrávat v úřednické kanceláři, ale měla by vycházet ze široké diskuse a na základě určité zpětné vazby.

**2** Druhou motivací byla potřeba provázanosti evropské agendy s národní úrovni. O tom hovořil podrobněji ve svém vystoupení Vladimír Dzurilla. Znamená to z našeho pohledu zajistit, aby evropská rovina byla provázána s národním vývojem.

## DVA CÍLE

Byly stanoveny dva základní cíle, jejichž dosažení je nezbytné pro zajištění institucionální koordinace a případně souvisejícího financování celé koncepce a komunikace o aktuálních tématech a příležitostech v digitální agendě. První cíl souvisí s horizontální povahou digitální agendy s tím, že je potřeba zajistit horizontální koordinaci, spolupráci resortů, proto jeho hlavním výstupem by mělo být **vytvoření výboru pro jednotný digitální trh**. Výbor by zahrnoval nejen ministerstva, ale i hospodářské a sociální partnery, profesní sdružení atp. tak, aby vznikla platforma pro diskusi nad uvedenými tématy, stejně jako konkrétními legislativními návrhy. S tím podle Zbyňka Smetany velmi úzce souvisí potřeba zajistit **lidské i finanční zdroje**. Jak uvedl, bude požadováno, aby každé ministerstvo vytvořilo určitého „styčného důstojníka“, který bude zajišťovat komunikaci výboru směrem do resortu. Návazně pak jde o již uvedené rozpracování principů tvorby a prosazování pozic České republiky a jejich provázanost s ostatními cíli Digitálního Česka.

Principiálně jde o to, že chceme-li se ve státní správě věnovat nějaké nové technologii, musíme nejprve ostatním resortům vysvětlit, co je její podstatou, jak se týká konkrétního resortu a proč by se technologií vlastně měl zabývat a věnovat jí pozornost. To vše je rovněž důležité i proto, že v roce 2022 bude ČR předsedat EU. Budeme tedy v pozici, kdy budeme nastolovat agendu, určovat, o čem se bude diskutovat a na co se bude klást důraz. Za tímto účelem si samozřejmě musíme definovat, co by ČR v rámci těchto měsíců chtěla primárně posunout dále.

## PRINCIPY

Zbyněk Smetana uvedl, že součástí připravovaných materiálů je i stanovení určitých principů. Zdůraznil ale, že to neznamená, že bychom nyní žádná pravidla, jak nakládat s evropskými návrhy, neměli. Spíše jde o to, že v rámci digitální agendy má i tento postup určitá specifika, která je nutné zohledňovat. Tím klíčovým specifikem je slovo **spolupráce**, respektive **horizontální spolupráce**. Představa je tedy taková, že pokud se objeví nějaké nové téma nebo nějaký nový legislativní návrh, tak prvním krokem by měla být vždy široká diskuse. Podstatné je vyslechnout co nejširší spektrum názorů a teprve na jejich základě rozhodovat, o jak zásadní téma se jedná. S tím souvisí i další z principů, a to **zaujmout včasný přístup** k for-

mulování evropské debaty. Dochází často k tomu, že EK píše návrhy zákonů, které se pak my snažíme více či méně úspěšně změnit, modifikovat, nebo zabránit jejich přijetí. To je ale v podstatě konec celého procesu. Ten začíná podle Zbyňka Smetany mnohem dříve, často na různých neformálních setkáních, kdy se začne diskutovat o tom, že se objevuje nějaké nové téma (nyní například umělá inteligence, blockchain). Debatuje se zde o tom, jestli by se Evropská komise měla zapojit, měla hledat regulační nástroje, či nikoliv. A právě v tomto momentu je potřeba pracovat na formulaci toho názoru, abychom byli případně schopni nabídnout podklady pro legislativní návrh. Klíčová otázka zní – k čemu by to vše mělo směřovat? Primárním cílem je **efektivní vystupování a prosazování zájmů** České republiky v rámci EU. Druhým cílem je pozitivní příspěvek k probíhajícímu procesu digitalizace v rámci České republiky.

## JAK DÁL?

Nyní by měla vláda schválit dokumenty Digitální Česko (stalo se 3. 10. 2018, pozn. redakce). Pak přijde na řadu rozpracování implementačních plánů. Aktivně se věnujeme vytvoření výboru pro jednotný digitální trh, který bychom rádi ustanovili v průběhu podzimu. Dalším okruhem je oblast umělé inteligence. Ve spolupráci s technologickou agenturou ČR je zpracovávána analýza současného stavu ohledně umělé inteligence v ČR. Výsledkem by mělo být doporučení pro státní správu, jak se k tomuto tématu stavět. Úřad vlády navazuje kontakty s digitálními inovačními centry, zjišťuje, co tato centra v současnosti dělají, jestli něco z těch zamýšlených evropských aktivit je vhodné k rozpracování atp.

V současnosti je také předmětem našeho zájmu program **Digitální Evropa** – součást nového víceletého finančního rámce. Není to program zaměřený na výzkum a vývoj, ale na implementační složku a měl by podporovat několik oblastí, jako jsou superpočítače, umělá inteligence, kybernetická bezpečnost, digitální dovednosti a zajištění širokého využití digitálních technologií v ekonomice a společnosti. Zbyněk Smetana upozornil, že za tím vším se skrývá několik miliard euro, které budou dostupné členským státům, aby pomohly zvýšit implementaci moderních digitálních technologií v praxi. Nyní se snažíme zjistit potenciál ČR v této oblasti.



## PILÍŘ Č. 3 DES – DIGITÁLNÍ EKONOMIKA A SPOLEČNOST

***Jak v úvodu svého vystoupení zdůraznil, nemohl na konferenci Pavel Hrabě skutečně plnohodnotně zastoupit náměstka Petra Očka z MPO a jeho zodpovědnost za koncept digitální ekonomiky a společnosti. Nicméně, protože Pavel Hrabě je architekt e-governmentu a člen týmu MV ČR a měl možnost být členem autorského týmu, pokusil se představit zásady koncepce DES – digitální ekonomiky a společnosti***

V souvislosti s e-governmentem upozornil na to, že jeho zásadní inovace nevznikají ve veřejné správě. Ta se v této souvislosti naopak opírá o výsledky digitální ekonomiky společnosti, tedy o to, co bylo objeveno a vymyšleno mimo veřejnou správu. Musí zvážit, zda takovým prostředkům a postupům poskytne podporu, případně jakou, zda se tyto nové objevy mají nějak regulovat a samozřejmě se je snažit co nejlépe využít pro sebe a pro zpřístupnění veřejné správy občanům. Je tedy podstatné, že e-government se odehrává v prostředí digitální ekonomiky a společnosti a obě tato témata spolu úzce souvisejí.



Pavel Hrabě



## CÍLE DES

1. funkční finanční a nefinanční podpora výzkumu, vývoje a inovací;
2. zralost a připravenost sektorů ekonomiky na digitální transformaci;
3. připravenost občanů na změny na trhu práce, vzdělávání a rozvoj digitálních dovedností;
4. podpora konektivity a infrastruktury digitální ekonomiky a společnosti;
5. zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti;
6. legislativa podporující všechny aspekty digitální ekonomiky a společnosti;
7. optimální systém financování digitální ekonomiky a společnosti;
8. institucionální zajištění centrální koordinace politik na podporu digitální ekonomiky a společnosti.

Základním cílem koncepce digitální ekonomiky a společnosti je tedy **odstraňovat překážky** (cíl 1) a vytvořit předpoklady pro dlouhodobou udržitelnost a rozvoj české společnosti v prostředí digitální transformace. To znamená na jedné straně objevovat digitální inovace a na druhé straně umožnit firmám, které byly jejich tvůrci, aby je mohly použít, aby rostla jejich **digitální zralost** (cíl 2), která je podstatná pro cíl 3. Jedná se tedy o úlohy, které jsou průřezové – jdou napříč všemi sektory stejně tak jako o samostatné sektorové cíle, například pro průmysl či zdravotnictví. Podle Pavla Hraběte jsou zde však zastoupeny i méně obvyklé sektory, které bychom v této souvislosti možná nečekali, jako je stavebnictví, zemědělství a další. Jak ale upozornil, dlouhodobá udržitelnost digitálního rozvoje spočívá v tom, že umožníme občanům, aby přijímali a využívali výhody digitalizace a vyhnuli se jejich negativům, jako je například závislost na instancích informacích a zážitcích. Právě skupinu dobře připravených, vyškolených a zanícených uživatelů chce oslovit český e-government.

Důležité je, že celý tento proces se musí odehrávat v prostředí **dostupné infrastruktury**, ať už je to infrastruktura komunikační, nebo je to infrastruktura inovační. Následné tři cíle (4, 5, 6) vytvářejí prostředí v tom smyslu, že musíme být schopni si digitální informace poskytovat bezpečně, musíme mít speciální právo – je zjevné, že právě inovativní charakter digitalizace předbíhá legislativu, a jak už o tom hovořil Zbyněk Smetana, následně musíme zaujmout pozici, jak podpořit, nebo regulovat takové věci, jako síťová ekonomika, nebo umělá inteligence.

A protože uvedených cílů je hodně, tak samozřejmě potřebujeme ještě poslední dva (7, 8) – **koordinovat všechny prostředky** na financování a podporu těchto cílů a **koordinovat sami sebe**.

Jedná se tedy o problematiku, která jde přes celou společnost a je potřeba zajistit její dlouhodobě udržitelný rozvoj. To znamená, že zainteresována a zapojena bude spousta lidí, úřadů a organizací, proto musíme vytvořit určité institucionální předpoklady, aby se koncepce digitální ekonomiky a společnosti mohla implementovat.

# ZÁKON O PRÁVU NA DIGITÁLNÍ SLUŽBY

*Prezident ICT Unie Zdeněk Zajíček zahájil své vystoupení odkazem na prezentace MV ČR, v nichž bylo několikrát zmíněno, že veřejná správa je extrémně složitá či spleťtá. Návrh zákona o právu na digitální službu by, podle jeho slov, měl pomoci tuto spleťtost rozmotávat. Je nutné provázat nejen možnosti a schopnosti resortů, ale nastartovat spolupráci i ostatních orgánů veřejné moci a zástupců veřejné správy tak, abychom skutečně mohli sdílené služby e-governmentu poskytovat. Zdeněk Zajíček zdůraznil, že je zcela evidentní, že procesy ve veřejné správě se neupravují ničím jiným než zákony a že i když na jednotlivých úřadech existuje vůle, tak v mnohých případech nám právě zákony, vyhlášky či podzákonné akty brání v tom, abychom mohli elektronizaci dotáhnout do konce.*

Zdeněk Zajíček v loňském roce na konferenci hovořil o tom, že občan, nebo firma má právo na některé služby. Nyní je takovým právem možnost vyřizovat si své záležitosti ve vztahu k veřejné správě digitálně a nejlépe on-line. Je to základní právo, které bychom měli mít.

## CO NÁM BRÁNÍ?

Nejsou to ani občané, ani firmy, co by bylo překážkou. Například občanů, kteří jsou uživateli internetového bankovníctví, jsou v tuto chvíli 4 miliony. Jedná se tedy o masu lidí, která by si pravděpodobně stejným způsobem, tedy elektronicky, vyřizovala i svoje záležitosti se státem, ale nejde to. Nyní sice nově máme Portál občana, přesto se Zdeněk Zajíček domnívá, v rámci celé veřejné správy to prostě nefunguje. Překážkou nejsou ani technologie, úředníci či organizace veřejné správy, pokud tedy mluvíme o elektronizaci veřejné správy jako budování jakési virtuální přepážky či virtuálních úřadů. Nebrání nám v tom dokonce ani finance, i když je zřejmé, že nějaká finanční injekce je potřeba, nicméně z dlouhodobého pohledu by mělo dojít k úsporám. Brání nám však **legislativa**.



Zdeněk Zajíček, prezident ICT Unie

## JAK NA TO?

Je pravdou, tak jak o tom mluvili zástupci MV ČR, že již dnes jsou některé služby poskytovány digitálně a elektronicky, například prostřednictvím Portálu občana. Ale není nikde deklarováno a zakotveno, že takové právo na poskytnutí služby mám. Podle Zdeňka Zajíčka by bylo vhodné, aby občané a firmy měli toto právo zakotveno v našem právním řádu. Proto je nutné udělat změnu vyhlášek a zákonů, které se přímo týkají e-governmentu, a také změnu agendových zákonů. V některých agendových zákonech je totiž výslovně napsáno, že obslužení klienta se děje v papírové, respektive fyzické podobě. Takovou formulaci tedy musíme upravit.

Zároveň bude podle Zdeňka Zajíčka nutné zajistit jednoznačnou metodiku zadávání veřejných zakázek, případně upravit samotný zákon o veřejných zakázkách, neboť pro možnost rychlého zavádění nových služeb a technologií musíme být rovněž schopni nakupovat rychle a efektivně.

## CO BYLO UDĚLÁNO?

Byl zpracován první návrh zákona o právu na digitální služby a zaslán do připomínkového řízení, zatím neformálního, a to členům Rady vlády pro informační společnost (RVIS), členům pracovního výboru pro digitálně přívětivou legislativu a zástupcům soukromého sektoru. Zároveň, protože se jedná o legislativu, byli osloveni zástupci poslaneckých klubů zastoupených v PČR, konkrétně v Poslanecké sněmovně. Jejich reakce byla vstřícná a všechny poslanec-

ké kluby přislíbily podíl na diskusi a spoluvytvoření prostředí pro přijetí takového zákona. Někteří z nich byli přítomni konferenci, protože jedním z jejích pracovních, neveřejných bodů byl seminář s tématem návrhu zákona.

Jak dále Zdeněk Zajíček referoval, nyní probíhá analýza a zpracování námětů k tomu, které zákony by mohly být a jak novelizovány, počínaje zákonem o základních registrech, zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, a zákonem č. 300/2008 Sb. o elektronických úkonech, právě proto, aby některé z těch práv mohly být bez problému realizovány. Zároveň bylo zadáno zpracování objektivní RIA (Regulatory Impact Assessment). Nyní Zdeněk Zajíček předpokládá prezentaci tohoto záměru, jeho projednání s vládou, jednotlivými resorty a se zástupci politických stran v Parlamentu. Zároveň očekává jednání se zástupci Asociace krajů a Svazu měst a obcí, protože jak uvedl, bez spolupráce s nimi se nic v oblasti e-governemntu nedá dotáhnout do úspěšného konce.

## JAKÁ PRÁVA BY MĚLA BÝT ZAKOTVENA?

Zákon o právu na digitální služby by měl stanovovat:

- **Právo být obslužen digitálně, pokud tomu povaha agendy nebrání**

Je to něco, co v tuto chvíli u mnoha agend sice již funguje, ale mělo by se jednat o univerzální pravidlo. Samozřejmě, že úkony typu převzetí OP musí být provedeny osobně, ale řada předcházejících kroků (žádost, doložení údajů atp., či celková komunikace) může probíhat v elektronické podobě, pokud o to občan stojí. Tedy jaké si základní pravidlo – DIGITAL BY DEFAULT.

- **Právo na poskytnutí údajů pouze jednou**

Je připraveno z hlediska základních registrů. Je ovšem nutné postoupit do další fáze – **propojený datový fond**. Pak budou skutečně úřady mezi sebou sdílet informace, a to na základě zákona, nebo na základě souhlasu občana. To musí být umožněno legislativně, abychom tím dali oprávnění jak občanům, tak institucím.

- **Právo využívat identitní prostředek dle své volby, pokud zákon nestanoví jinak**

Existuje zákon o elektronické identifikaci, ale je potřeba do právního řádu zakotvit i onu možnost volby.

Občan si pak může zvolit dle svého uvážení prostředek s požadovanou mírou záruky.

- **Právo na digitální právní jednání**

Zdeněk Zajíček upozornil na skutečnost, že náš právní řád žádné taková ustanovení zatím neobsahuje. Můžeme je sice dovozovat z některých zákonů o e-governemntu a občanského zákoníku, ale taková komplexní úprava neexistuje. Bylo by tedy dobré ustanovení zapracovat do jednoho zákona.

- **Právo na digitální projev vůle**

Stejně tak by měla vzniknout úprava práva na digitální projev vůle.

- **Právo na záznam o digitálním právním jednání a projevení vůle**

Občané a firmy jsou při jednání s úřady v podstatě ve slabší pozici. I proto by mělo být garantováno, že záznam o proběhnutém jednání by měl být uchováván podobně, jako je uchováván například v datových schránkách. Zde platí, že mám možnost získat potvrzení – záznam o realizované transakci. Něco takového by tedy mělo být samozřejmě i u všech ostatních digitálních služeb.

- **Právo na poskytnutí informace ze všech ISVS**

Základ už v tuto chvíli máme v zákoně č. 365/2000 Sb. o informačních systémech veřejné správy, v podobě

výstupů z každého informačního systému veřejné správy. Stačí tedy tento princip prohloubit, respektive rozšířit.

- **Právo na zaslání výpisu do datové schránky o tom, KDO, KDY a PROČ využíval mé údaje do DS**

Zatím funguje pouze u základních registrů. Kdokoli má datovou schránku, takový výpis pravidelně dostává. Cílem návrhu je, abychom dostávali výpisy ze všech informačních systémů veřejné správy, v nichž jsou naše údaje vedeny.

- **Právo na zápis údajů a skutečností vyplývajících z dokladů, průkazů, osvědčení a veřejných listin do RPP**

Je bohužel výjimka, že v současné době i na základě tlaku náměstka Strouhala začíná Ministerstvo dopravy uvažovat o tom, že propojí datový fond MD s Portálem občana a dalšími informačními systémy. Návrh předkládá, že by se jednalo o pravidlo. Zároveň by každý občan měl možnost, pokud příslušný úřad sám není aktivní, si do registru práv a povinností svoje právo zapsat.

- **Právo nenosit, nepředkládat doklad, osvědčení, průkazy a veřejné listiny**

Mnoho našich oprávnění musíme dokládat různými průkazy, doklady a potvrzeními (zdravotní, řidičský, zbrojní průkaz, vysvědčení a další). Všechny tyto informace jsou přitom dnes vedeny v centrálních systémech jednotlivých resortů a je možné zajistit, aby do nich oprávněné osoby mohly nahlížet. Proto není důvod, abych osobně musel tyto dokumenty předkládat nebo je u sebe nosit.

- **Právo na interaktivní formulář, který se sám předvyplní**

Tedy formulář, který podle příslušné agendy „natáhne“ údaje, které jsou o mně již vedeny a mají souvislost s touto agendou. Občan tak nevyplňuje dokola totéž, ale pouze dopíše, co je nad rámec. To je princip založený na základních registrech, tedy od roku 2009. Mimo jiné toto ustanovení říká, že k registraci agendy každý úřad, který poskytuje služby v oblasti veřejné správy, má dodat do registru práv a povinností elektronický formulář. Zdeněk Zajíček si podle vlastních slov není úplně jistý, ale je přesvědčen, že žádný úřad nevzal tuto povinnost vážně. Je tedy nutné upozornit, že i na toto mají občané právo.

- **Právo na notifikaci o končící platnosti průkazu, dokladů, osvědčení a veřejné listiny 30 dnů před uplynutím platnosti do DS (SMS, e-mailem)**

Platí to nyní pro občanský průkaz a začíná to platit pro některé další průkazy (zbrojní, řidičské), ale měl by to být obecný princip. Pokud už stát vydává nějaké osvědčení, průkaz či listinu, vydává ji buď na neomezenou dobu, nebo ji vydává s určitou dobou platnosti. Pokud na omezenou dobu, pak zná termín ukončení platnosti, a je tedy možné, aby byl občan notifikován, že se blíží konec platnosti tak, aby mohl včas činit příslušné kroky.

- **Právo na otevřená data, s nimiž stát disponuje a nepodléhají utajení, či zvláštní ochraně**

V tomto směru se podle Zdeňka Zajíčka hodně učinilo. Vláda sestavuje seznam otevřených dat a tato problematika je vnímána jako důležitá. I tak by bylo vhodné ukotvit to jako právo.

- **Právo na přístupnost digitální služby pro osoby s hendikepem**

To by měla být naprostá samozřejmost, stejně jako následující bod.

- **Právo, aby důkazní břemeno nesl ten, kdo službu neposkytl**

Úřad či instituce by měla dokládat, že existují oprávněné důvody, proč nebyly služby poskytnuty.

## NA KOHO BY SE TO MĚLO VZTAHOVAT?

Zdeněk Zajíček poděkoval všem, kteří už svoje připomínky k těmto návrhům zaslali, a i na jejich základě si troufá odhadovat směr dalšího vývoje.

### Podmínky stanovené tímto zákonem by měly splňovat:

- **OVM na úrovni státu, které vykonávají působnost státní správy, nebo podle zvláštních zákonů, zvláštní kompetence**, nejpozději do dvou až tří let.
- **Kraje a obce** by měly sladit kroky s orgány státní správy, a to v oblasti přenesené působnosti. Zde sehrávají ústřední správní orgány důležitou roli, když přenášejí kompetence na lokální úřady.



- **Kraje a obce** při výkonu samostatné působnosti, samosprávy nejpozději do 3–5 let. Zde není takový tlak, je tedy možné poněkud delší období.

V návrhu byly původně i soukromoprávní poskytovatele digitálních služeb. Nicméně byli vyjmuti vzhledem k tomu, že na rozdíl od státu tyto kroky již dávno naplňují. Dokazují to i čísla, kdy ČR je například na třetím místě z hlediska objemu obchodování na internetu či využívání internetového bankovníctví atd. Možná až stát v tomto smyslu dožene soukromý sektor, pak bude vhodné uvažovat o úpravě. V současném návrhu nebudou tedy soukromé služby zahrnuté.

## CO DNES MÁME?

Co z toho, co již máme k dispozici, může pomoci naplnit uvedený cíl? Máme evidenci agend a rolí v RPP dle platných zákonů. Evidence se stále zpřesňuje, což je dobré, ale chybí evidence služeb, které se v rámci jednotlivé agendy poskytují. Pokud bychom takovou evidenci dokázali sestavit, identifikovali bychom, které z těchto služeb mají být poskytovány digitálně a které digitálně poskytovat nejde z principu. Ideálně by se pak do jednoho roku od vydání uvedeného zákona přijalo nařízení vlády, kterým by se stanovil seznam služeb, které veřejná správa dělá v jednotlivých agendách. Byl by to jakýsi benchmark, z něhož by bylo naprosto jasné, z čeho vycházíme. Seznam by se pak každoročně aktualizoval, neboť bezpochyby budou přibývat další a další služby, které se do něj dají zařadit. Na tomto základě by bylo zcela

jednoznačné, kde má úřad povinnost a na co mají občané, nebo firmy právo, protože je-li v nabídce státu služba, která se poskytuje digitálně, nemůže se poskytnutí takové služby odmítnout.

Celá tato aktivita je vedena vírou, že občan a firma mají právo pořídit si své záležitosti se státem digitálně a nejlépe on-line. Překážkou je jednoznačně naše legislativa. Mluvíme-li o digitálně přívětivé legislativě, je vhodné upozornit, že se nejedná pouze o zákon o právu na digitální služby. Bude totiž nutné i do všech nových právních předpisů vnést tyto principy, aby nevznikaly bariéry a mohlo se skutečně digitálně obsluhovat. Zdeněk Zajíček proto poděkoval poslancům, kteří do Mikulova na konferenci přijeli, protože jak zdůraznil, bez Poslanecké sněmovny a celkově bez Parlamentu se při změnách právních norem v ČR skutečně neobejdeme. Doufá, že se podaří najít společnou řeč jak s tvůrci koncepce Digitální Česko, tak s MV ČR, poslanci i se soukromým sektorem.

Jako důkaz, že když je vůle, jdou dělat velké věci, bylo na závěr vystoupení Zdeňka Zajíčka slavnostně podepsáno Memorandum o spolupráci při zajištění podpory vzniku Digitální technické mapy České republiky. Přímo na pódiu jej podepsali náměstek ministra vnitra pro ICT Jaroslav Strouhal, vládní zmocněnec pro IT a digitalizaci Vladimír Dzurilla, prezident ICT Unie Zdeněk Zajíček a předseda Asociace podnikatelů v geomatice Martin Hrdlička. Ostatní signatáři se připojí následovně (Memorandum na straně 34).

## MEMORANDUM O SPOLUPRÁCI

**při zajištění podpory vzniku Digitální technické mapy České republiky sloužící k systematické a jednotné správě geografických dat o umístění sítí elektronických komunikací a dalších infrastrukturních sítí (dále jen „technická infrastruktura“) včetně poskytování informací o technické infrastruktuře orgánům veřejné moci, vlastníkům nemovitostí, investorům a veřejnosti zejména pro územně plánovací činnost a územní a stavební řízení podle stavebního zákona a zajištění činnosti jednotného informačního místa podle zákona o opatřeních ke snížení nákladů na zavádění vysokorychlostních sítí elektronických komunikací.**

Níže podepsaní signatáři tohoto memoranda si uvědomují, že v České republice doposud neexistuje ucelený a důvěryhodný systém pro správu a využívání údajů o technické infrastruktuře na území České republiky (dále jen „DTM“), který by efektivně sloužil jak orgánům veřejné moci pro výkon jejich pravomocí v oblasti územního plánování, územního a stavebního řízení, tak také vlastníkům pozemků a nemovitostí, stavebníkům a široké veřejnosti pro ochranu jejich práv a zájmů.

Neexistence DTM zamezuje urychlení výstavby technické infrastruktury, zejména infrastruktury elektronických komunikací pro gigabitové služby, zvyšuje náklady na straně veřejné správy a soukromého sektoru a udržuje nadměrnou byrokratickou zátěž pro stavební úřady, dotčené orgány a účastníky územního nebo stavebního řízení.

### **Signatáři proto podporují DTM, která bude vytvořena na následujících principech:**

- DTM bude integrální součástí elektronizace územně plánovacího, územního a stavebního řízení;
- DTM je významným nástrojem k zefektivnění (tedy usnadnění, zkrácení a zlevnění) procesu přípravy a realizace územně plánovacího, územního a stavebního řízení pro stavebníky, tedy zejména občany a právnické osoby;
- DTM je vhodným nástrojem k získání dalších územně analytických podkladů, nezbytných pro územně plánovací činnost nebo územní a stavební řízení;
- DTM je nezbytným předpokladem pro efektivní využívání stávající technické infrastruktury a zároveň efektivní plánování budoucí výstavby tak, aby bylo zabráněno nadbytečným investičním překryvům a zároveň byla minimalizována administrativní zátěž stavebníka vyplývající z irelevantních žádostí o vyjádření o existenci a podmínkách ochrany technické infrastruktury;
- DTM je efektivním nástrojem pro ochranu vlastnických a jiných práv na ochranu realizovaných, či plánovaných investic do technické infrastruktury.
- DTM je základem pro efektivní pasportní úlohy státu i územních samospráv a jsou významným zdrojem dat a informací, zejména pro bezpečnost státu, krizové řízení a Integrovaný záchranný systém;
- Pořizování údajů pro DTM je postaveno na principu nezvyšování stávající administrativní zátěže vlastníků technické infrastruktury. Základem jsou primárně údaje již dnes předávané úřadům územního plánování.
- DTM je datovou bází o objektech technické infrastruktury a patří mezi základní geografická data, která jsou využívána při správních a rozhodovacích činnostech veřejné správy nebo správce technické infrastruktury.
- Řešení DTM představuje komplexní informační systém, který slouží pro její efektivní správu a údržbu pomocí prostředků výpočetní techniky;
- DTM obsahuje nejpodrobnější reálné dosažitelný a trvale aktualizovaný popis skutečného stavu v území, včetně technické infrastruktury v České republice a poskytuje tak nezbytné údaje, které jednoznačně vymezují její umístění v terénu;
- DTM je upravena v legislativě tak, aby byly jasně definovány podmínky provozování a správy informačního systému a zároveň umožněn bezpečný přístup pro pořizování a využívání údajů z DTM pro různé skupiny editorů a uživatelů. DTM je výkonem přenesené působnosti státní správy s odpovídajícími finančními nároky;
- DTM bude zákonem definováno jako jednotné digitální mapové dílo velkého měřítka včetně souvisejících služeb, které se skládá z digitálních technických map krajů, které je provozují v rámci přenesené působnosti výkonu státní správy;
- DTM bude součástí Národního architektonického plánu ČR jako jedna z centrálních sdílených digitálních služeb

eGovernmentu, kde stát nese odpovědnost za enterprise architekturu DTM v návaznosti na jiné centrální sdílené digitální služby, informační systémy (například informační systém technické infrastruktury veřejné správy) a další digitální služby eGovernmentu; legislativně bude garantováno, že právní úprava bude definovat závazný rozsah digitálních služeb poskytovaných DTM a souvisejících informačních systémů, například Informační systém technické infrastruktury veřejné správy v návaznosti na jednotné technické řešení DTM byt zajišťované v přenesené působnosti jednotlivými kraji a pro účely správy a provozu DTM bude vydána jednotná metodika.

### **Signatáři memoranda se v zájmu urychlení procesu vytvoření DTM shodují na následujících opatřeních, která je nezbytné urychleně realizovat pro vznik DTM:**

- 1) urychleně zpracovat a předložit signatářům k podmínkám návrh právní úpravy, aby byly vytvořeny odpovídající legislativní, ekonomické a další předpoklady pro vytvoření, správu a užívání DTM

*KT: nejpozději do 31. října 2018*

*Koordinuje a odpovídá: RVIS*

*(Pracovní výbor pro digitálně přívětivou legislativu)*

- 2) urychleně navrhnout a prosazovat při jednání s odpovědnými národními i unijními institucemi nalezení vhodných zdrojů pro financování vzniku DTM a pořízení dat do DTM, např. s využitím dosud nevyužitých finančních prostředků evropských strukturálních fondů (např. IROP nebo OPPIK) a zároveň připravit návrh nároku na personální zajištění a financování provozu DTM v rámci výkonu přenesené působnosti kraji

*KT: nejpozději do 31. října 2018*

*Koordinuje a odpovídá: MMR, MPO a MV*

- 3) urychleně zpracovat a předložit návrh architektury a podmínek správy a provozu DTM v návaznosti na centrálně sdílené digitální služby eGovernmentu a další poskytované digitální služby

*KT: nejpozději do 31. října 2018*

*Koordinuje a odpovídá: MV, MMR, AK ČR, ICT Unie, HK ČR, SPD*

### **SIGNATÁŘI MEMORANDA:**

#### **Ministerstvo vnitra**

zastoupené náměstkem JUDr. Jaroslavem Strouhalem

#### **Předseda Rady Vlády pro informační společnost**

Ing. Vladimír Dzurilla

#### **Ministerstvo pro místní rozvoj**

zastoupené náměstkem člena vlády Bc. Václavem Nebeským

#### **Ministerstvo průmyslu a obchodu**

zastoupené náměstkem člena vlády Mgr. Ondřejem Malým

#### **Český úřad zeměměřický a katastrální**

zastoupený předsedou Ing. Karlem Večeřem

#### **Český telekomunikační úřad**

zastoupený předsedou Ing. Jaromírem Novákem

#### **Asociace krajů České republiky**

zastoupená předsedkyní Mgr. Janou Vildumetzovou

#### **Svaz měst a obcí České republiky**

zastoupený předsedou Mgr. Františkem Luklem, MPA

#### **ICT UNIE**

zastoupená prezidentem Mgr. Zdeňkem Zajíčkem

#### **Hospodářská komora České republiky**

zastoupená viceprezidentkou Ing. Irenou Bartoňovou Pálkovou

#### **Svaz průmyslu a dopravy České republiky**

zastoupený viceprezidentkou Mgr. Milenou Jabůrkovou, MA

#### **Asociace podnikatelů v geomatice**

Zastoupená předsedou Ing. Martinem Hrdličko

#### **Česká asociace pro geoinformace**

zastoupená předsedou Ing. Karlem Janečkou, Ph.D.

#### **Český svaz geodetů a kartografů**

zastoupený předsedou Ing. Václavem Šandou

#### **Česká komora autorizovaných inženýrů a techniků**

zastoupená předsedou Ing. Pavlem Křečkem

#### **Česká komora architektů**

zastoupení předsedou Ivanem Plickou

#### **Odborná rada pro BIM**

zastoupená předsedou Petrem Vaňkem

#### **Česká asociace provozovatelů mobilních sítí**

zastoupená prezidentem Jiřím Šuchmanem

#### **Česká asociace elektronických komunikací**

zastoupená předsedou JUDr. Zdeňkem Vaníčkem



## OZNÁMENÁ ELEKTRONICKÁ IDENTITA

**Poradce náměstka ministra vnitra Robert Píffl na konferenci hovořil o záležitostech, které budou v následujících týdnech a měsících velice důležité, a to nejen v souvislosti s tématem eIDAS. Konkrétně se jedná o plné spuštění systému oznámené elektronické identifikace v rámci Evropské unie.**

Upozornil, že v této souvislosti je velice důležité, abychom správně porozuměli jednotlivým pojmům tak, aby nedocházelo ke zmateným výstupům. V našem právním řádu je jednoznačně definována elektronická identifikace a věci související nařízením eIDAS.

### Toto nařízení rozpoznává tři různé druhy identifikace:

1. identifikace fyzické osoby;
2. identifikace právnické osoby;
3. identifikace fyzické osoby, která zastupuje právnickou osobu.

Elektronická identifikace je definována v nařízení eIDAS – článku 3 jako „postup používání osobních identifikačních údajů v elektronické podobě, které jednoznačně iden-



Robert Píffl,  
poradce náměstka ministra vnitra

tifikují určitou fyzickou, či právnickou osobu, nebo fyzickou osobu zastupující právnickou osobu“. Netýká se tedy pouze nějakého fyzického prostředku, týká se obecně použití osobních identifikačních údajů v elektronickém světě. Právě v souvislosti s tímto ustanovením je velice často možné narazit na nevhodné implementace a nesprávné použití. Jako typický příklad uvedl Robert Píffl snahu využít elektronický podpis jako nástroj identifikace.

## V rámci svého vystoupení zopakoval a ujasnil následující pojmy:

### Údaje a prostředky

Osobní identifikační údaje rovněž jasně vymezuje článek 3 nařízení eIDAS, a to v odstavci 3. Zároveň definuje, co jsou prostředky pro elektronickou identifikaci a jaké existují záruky elektronické identifikace. Prostředky mohou být hmotné, ale rovněž nehmotné, to znamená, že jsme schopni fungovat ryze virtuálně. Podstatné je pouze to, že takový prostředek identifikace (hmotný či nehmotný), který obsahuje identifikační údaje, jež se používají k autentizaci, byl vydán za určitých předpokladů konkrétní fyzické osobě.

### Autentizace

Je elektronický postup, který v elektronickém světě umožňuje potvrdit identifikaci fyzické (právníkové, či fyzické zastupující právníkou) osoby, původ a integritu dat. Autentizace tedy zabezpečuje **věrohodnost původu a neporušitelnost obsahu** – nic jiného. Je velice důležité si uvědomit, že **o případném projevu vůle autentizace vůbec nehovoří**.

### Spoléhající strana a záruky

Dalšími důležitými termíny, které zavádí nařízení eIDAS, je například **spoléhající strana**. Jde o situaci, kdy máme dvě strany – jedna, která je držitelem toho prostředku (virtuálního, nebo fyzického), a protistrana, která se bude spoléhat na systémy, jejich ověření a záruky. Díky tomu bude spoléhající strana předpokládat, že na vzdálené straně skutečně sedí konkrétní identifikovaná osoba.

Spoléhající osobou může být fyzická, nebo právníká osoba, nebo veřejnoprávní sektor. I z tohoto důvodu je v celém procesu identifikace nejkritičtější moment prvotního ztotožnění. Právě proto existují tři stupně záruk – nízká, značná a vysoká. Jsou popsány v prováděcích nařízeních eIDAS a jejich úroveň závisí na tom, jak kvalitně a jednoznačně se při tomto prvotním ztotožnění prokáže totožnost osoby, která poprvé zřizuje nějaký identifikační prostředek, tedy osoby, která zřizuje svoji elektronickou identitu. Od toho se tedy odvíjejí právní důsledky.

### Normy

**Prováděcí akty eIDAS, které se opravdu týkají přímo elektronické identifikace jako takové, jsou:**

- prováděcí rozhodnutí komise EU 2015/2016 ze dne 24. 2. 2015;
- prováděcí nařízení komise EU 2015/1501 ze dne 8. 9. 2015;
- prováděcí nařízení komise EU 2015/1502 ze dne 8. 9. 2015;
- prováděcí nařízení komise EU 2016/1984 ze dne 3. 11. 2015.

V ČR upravuje zákon č. 250/2017 Sb., o elektronické identifikaci, **pouze elektronickou identifikaci fyzických osob**. Zároveň zahrnuje dvouleté přechodné období – pokud zákon nařizuje určité postupy, má veřejná správa čas do 1. 7. 2020, aby mohla upravit veškeré informační systémy podle tohoto zákona. Pokud ale někdo již provozoval on-line službu, která splňovala zákon č. 250/2017 Sb. i nařízení eIDAS, má k dispozici lhůtu 6 měsíců (od 1. 7. 2018), aby nahlásil na SZR podrobnosti o těchto systémech.

## CO ELEKTRONICKÁ IDENTIFIKACE PŘINESE?

### Bezpečnost

Nejedná se o pouhé technické požadavky vyplývající z prováděcích aktů. Elektronická identifikace by měla zásadním způsobem zvýšit bezpečnost elektronických transakcí. Jak z našeho zákona, tak z nařízení eIDAS jednoznačně vyplývá **odpovědnost za škodu**. Ta nově otáčí důkazní břemeno. Pokud v rámci elektronické identifikace bude nyní občan tvrdit, že mu vznikla škoda, je na protistraně, aby prokázala opak. Pokud se jí to nepodaří, bude na situaci pohlíženo, jako by ke škodě skutečně došlo. Je to tedy ustanovení, které bude všechny provozovatele tlačit ke zvyšování bezpečnostních požadavků na samotné IS, technologické dodavatele i celý řetězec.

### Mobilita

Můžeme se prokazovat na dálku, a to i z mobilních zařízení. V tomto směru je důležitou součástí Národní identifikační bod, který umožňuje jak přeshraniční identifikaci

pomocí mezinárodního uzlu, tak identifikaci na území ČR podle zákona č. 250/2017 Sb.

### Kvalifikovaný systém

§2 zákona č. 250/2017 Sb. obsahuje klíčové ustanovení, které má obrovské dopady. Konkrétně je zde napsáno, že „vyžaduje-li právní předpis, nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace“. Tedy elektronickou identifikaci můžeme realizovat prostřednictvím národního bodu, nebo bude-li existovat soukromoprávní subjekt, který bude nabízet tu službu, tak jeho prostřednictvím (Ministerstvo vnitra může akreditovat tzv. kvalifikované poskytovatele elektronické identifikace, kteří když splní konkrétní požadavky, mohou nabízet vlastní prostředky pro identifikaci). Neomezujeme se však pouze na Českou republiku, protože za kvalifikované se též považují systémy propojené přes mezinárodní uzel. Pokud tedy je nutné v rámci výkonu působnosti či jinak prokázat totožnost osoby, tak je to možné buď prezenčně v místě, anebo elektronicky. Pokud elektronicky, tak pouze přes kvalifikovaný systém. Jen pro zajímavost, například zákon o kybernetické bezpečnosti při určitých situacích říká, že správci či administrátoři musí v případě přístupu do konkrétních systémů prokázat svoji totožnost. Bude se tak dít pouze přes kvalifikovaný systém.

Ten je tedy definován v §3 zákona č. 250/2017 Sb. s tím, že musí splňovat alespoň jednu z úrovní záruk. Kvalifikovaný systém umožňuje poskytnutí služby Národního bodu identifikace a autentizace, tedy je propojen s NIA, a musí osobní identifikační údaje jednoznačně identifikovat od okamžiku vydání prostředku identifikace. Tady Robert Píffl upozornil na možnost tzv. řetězení elektronické identifikace. Tedy situaci, kdy konkrétní osoba již má k dispozici nějaký prostředek, například na nejvyšším stupni záruk. V takovém případě si může elektronicky, tedy na dálku, pořídit další identitu, aniž by se někam musela dostavit.

### Elektronická identifikace

Definuje ji článek 3 nařízení eIDAS v odst. 1 – „elektronická identifikace je postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou, či právnickou osobu, nebo fyzickou osobu zastupující právnickou osobu“. Je tedy potřeba,

aby veřejná správa nejpozději do 1. 7. 2020 upravila své systémy, včetně příslušných pracovních postupů.

### Kvalifikovaný správce

Podle definice v §16 zákona č. 250/2017 Sb. je kvalifikovaným správcem v ČR zatím pouze SZR. Může jím být veřejnoprávní orgán i soukromoprávní společnosti. V současné době se zvažuje, že by se takovým kvalifikovaným správcem stalo MojID.

Kvalifikovaný správce vždy ověřuje totožnost prostřednictvím Národního bodu. Platí tedy výše uvedený princip řetězení. Bude-li existovat více kvalifikovaných správců a konkrétní osoba bude mít identitu na nejvyšším stupni od jednoho z nich, pak si může pořídit nejvyšší stupeň záruk od jiného z těchto poskytovatelů prostřednictvím Národního bodu. A vzhledem k tomu, že součástí Národního bodu je i mezinárodní uzel, tak se to týká všech oznámených systémů identifikace v Evropské unii.

### eOP

je prostředek pro nejvyšší stupeň záruk. V současné době probíhá dokončování materiálu, abychom mohli zahájit prenotifikaci našeho systému směrem do zahraničí, tzn. abychom potom mohli donutit, prostřednictvím nařízení eIDAS, ostatní členské státy, aby akceptovaly náš eOP pro



přihlašování do služeb s nejvyšším stupněm záruk. V současné době eOP obsahuje elektronickou identifikaci, která je zařízena přes identifikační certifikát. Tak jako doposud, i nadále je možné na eOP uložit zaručený podpis na kvalifikovaném certifikátu vydaný nějakou certifikační autoritou. Rovněž je možné na něj dávat kryptografické klíče, které slouží k identifikaci. Není ovšem zatím možné do eOP vkládat kvalifikovaný podpis podle eIDAS. Takové státní podpisy se očekávají někdy v průběhu příštího roku

## JAK JSME NA TOM V EVROPĚ

### Německo

Německo bylo v rámci elektronické identifikace první, a tak zavedlo podstatná pravidla - například, že systémy pro elektronickou identifikaci musejí být na principu seamless. Pokud se uživatel v rámci určitého vyřizování přepojuje mezi několika různými institucemi, tak to nezpozoruje a má stále pocit, že vyřizuje jednu záležitost na jednom místě (jednotné grafické prostředí, struktura atp.). To je princip v ČR zatím naprosto nedostížný, přechod mezi jednotlivými úřady v elektronickém světě je stále přehlídkou fontů, grafické pestrosti a různorodosti obsahového uspořádání.

Podstatnější je, že od data účinnosti, tedy 29. 9. 2018 je úřad české veřejné správy, pokud nabízí on-line službu, povinen uznávat německý elektronický občanský či pobytový průkaz a respektovat, že němečtí občané se budou chtít do systému přihlásit. V této souvislosti je důležité, že Němci se rozhodli pro middleware, který zabezpečuje určitou komunikaci. Všechny členské státy tedy musejí implementovat tento middleware do svých uzlů, nebo na své prostředky tak, aby ověřily prostředky identifikace z Německa. Speciálně Německo je rovněž velmi přísné při ochraně osobních údajů. Ústavní soud zde zakázal, aby veřejná správa měla perzistentní - bezvýznamové identifikátory směrem k občanům. V tomto smyslu upozornil Robert Piffel na skutečnost, že v rámci ČR existují nástroje některých projektů nastavovaných jiným směrem, což podle jeho mínění nemůže dopadnout dobře. Základní princip mezinárodního uzlu je, že zde nezůstávají žádná data podle nařízení eIDAS. Jediné, co zde může zůstat, je záznam logu o tom, že určitá data tudy „protekla“.

### Pětice dalších států

Byly prenotifikovány další státy - Itálie, Španělsko, Lucembursko, Chorvatsko a Estonsko a běží prenotifikace Portugalska a Belgie a o prenotifikaci požádala Velká Británie. To znamená, že v letech 2019-2020, podle toho, kdy a jak budou postupně notifikovány, budeme muset umět zacházet s poměrně velkým množstvím identitních prostředků z dalších členských států. V letech 2020-2021 by se dalo očekávat, že naopak členské státy budou muset umět rozpoznat naši eOP.

Některé ty státy mají poměrně hodně identitních prostředků, někteří zajímavá řešení.

### Estonsko

Estonsko například společně s Portugalskem přináší elektronickou identifikaci na vysokém stupni záruk do mobilů, tzn. je opřena o certifikaci SIM karty.

Estonsko přiznalo zásadní dopady objevu Masarykovy univerzity v oblasti zranitelnosti generování RSA klíčů. Náprava stála několik milionů, možná desítek milionů korun. Protože je zde možné volit elektronicky, uvažovalo se dokonce i o odložení voleb. Bylo totiž nutné zneplatnit 600 000-700 000 vydaných certifikátů. Estonsko bylo nuceno udělat řadu změn a nyní nabízí, jako jedno

z prvních, identifikaci přes mobil. Do jisté míry způsobilo poprask s e-residency, tedy elektronickou rezidenční kartou pro cizince. Rozhodně je Estonsko státem, který má širokou paletu elektronických služeb.

### Itálie

Itálie velice dlouho uvažovala o One Time Password (OTP) a videu. Měli představu, že je možné videokomunikací získat nejvyšší stupeň záruk. Nakonec se podařilo dokázat nespolehlivost takového přístupu a stejně jako OTP i videokonference získala úroveň pouze střední záruky. Záruku stupně vysoký získaly pouze italské elektronické karty. Kromě fyzických osob má Itálie i identifikační prostředky pro právnické osoby.

### Belgie

I v době ochrany osobních údajů preferuje Belgie na svých občankách informace o příbuzných – děti, rodiče atd. a jejich identifikaci. Pravda je, že takový přístup umožňuje velmi flexibilní zastupování v řadě životních situací. V Belgii je systém identifikace napojený například na velmi moderní e-health. Je pak snadné i off-line ztotožnit příbuzné s pacienty. Občanky jsou zde vydávány od dvanácti let věku. Spektrum služeb, které je jejich prostřednictvím možné využívat, je omezeno jak dolní, tak horní hranicí věku. Tedy stárnoucím občanům od určité hranice postupně možnosti některých elektronických služeb odpadají. Je to určitá ochrana starších lidí.

### Portugalsko

Podobně jako Estonsko umožňuje i Portugalsko identifikaci pomocí mobilu (SIM) a stejně jako Itálie zavádí identifikační prostředky pro právnické osoby a rovněž profesní identity (např. lékař ...).

### Španělsko

Muselo zneplatňovat 60 milionů vydaných certifikátů – podobně jako v případě Estonska se jednalo o dopady objevu Masarykovy univerzity. V současnosti mají novou kartu, která prochází notifikací na vysoký stupeň záruk.

### Chorvatsko

Rovněž zde mají čipové karty a věkovou hranici 18–65 let s tím, že starší občané nemají certifikáty povinné a mají zúžené právní jednání - rozsah využitelných služeb.

### Lucembursko

Občanské průkazy vydává od 15 let a stejně jako větší na uvedených státech i Lucembursko vydává na eOP svým občanům bezplatně kvalifikované podpisy.

**Pro nás je podstatné, že od okamžiku, kdy to budou mít jednotlivé státy své systémy notifikovány, máme dvanáct měsíců na to, abychom si s nimi poradili.**

## ZÁVĚR

### **Co nám eID přinese?**

Dostupnost 24/7, ztotožnění na dálku a předpokládá se rozvoj nových aplikací.

### **Co nám chybí?**

V rámci ČR nám, v porovnání s jinými státy, chybí především role. Umíme ztotožnit konkrétní fyzickou osobu, ale nedokážeme jí přiřadit roli, například rodič, dítě, zastupující osoba, zmocněnec atp.

### **Globální dopady**

Jedním ze zásadních dopadů, které Robert Piffel prezentoval, je skutečnost, že řada lidí „zmizí ze systému“. Spousta členských států totiž neumí vydat eOP a prostředky identifikace, pokud občan trvale nežije na území toho státu. Tento problém se týká velkého množství starších lidí, kteří se ve vyšším věku stěhují do jiných zemí. Zůstávají ale občany své země a především budou chtít, z uvedeného důvodu, maximálně využívat výhod elektronické identifikace, tedy vyřizování úředních věcí na dálku. Je to problém, který budou muset tyto země řešit.

### **Podstatné**

Závěrem Robert Piffel upozornil, že se stále objevují pokusy používat k identifikaci elektronické podpisy, což není jejich funkcí. Podpis je projev vůle, ale není to identifikace osoby. V řadě řešení je to i v rozporu s certifikačními podmínkami pro vydání elektronického podpisu. Je to zásadní problém, neboť elektronický podpis má v případě nějakých pochybností pouze potvrdit, že certifikační autorita vydala onen podpis někomu konkrétnímu. Není to ale nástroj pro osobní identifikaci.



# Move like your business depends on it.

For 20 years, we've been helping  
companies unleash the power of their  
apps to get where they want to go:  
Faster. Smarter. Safer.



[WeMakeAppsGo.com](http://WeMakeAppsGo.com)

WE MAKE APPS  FASTER.  
SMARTER.  
SAFER.



**Miliony studentů  
Deset tisíc akademií  
Jedna vize**

## **Cisco Networking Academy vzdělává studenty přes 20 let**

**Analytická společnost Gartner říká, že do roku 2022 bude 75 % organizací vnímat síť jako klíčový motor pro jejich digitální iniciativy. To je jen jedna z předpovědí, které v budoucnu ovlivní pracovní trh. Jsou na to ale studenti připraveni? A jak je vzdělávat, aby byli? Společnost Cisco podporuje rozvoj globální i lokální pracovní síly již přes 20 let prostřednictvím svého vzdělávacího programu Cisco Networking Academy. V České republice jím prošlo již více než 42 000 studentů, ve světě pak přes 7,8 milionů ve více než 180 zemích. Díky ní získali absolventi praktické dovednosti, které v budoucnu využijí ve svém zaměstnání. „Jsme rádi, že v České republice dlouhodobě nejenom budujeme naše obchodní vztahy, ale zároveň dáváme komunitě i něco unikátního – naše znalosti. Cisco Networking Academy je ideální platformou, díky které zde můžeme udělat něco pro rozvoj celé společnosti,“ říká Jan Elefant, obchodní ředitel společnosti Cisco.**

### **Seznamte se**

Dříve se IT věnovali pouze technicky nadaní studenti, dnes proniká de facto do všech oborů a základní počítačovou gramotnost potřebuje téměř každý. V roce 1997, kdy Networking Academy začínala, proběhlo několik zajímavých technologických milníků. Byla zaregistrována domé-

na Google.com, Microsoft akvíroval Hotmail, byla založena společnost Netflix, byl představen nový standard pro bezdrátové připojení 802.11, tedy základ dnešní podoby Wi-Fi. Vzdělávací program Networking Academy začal jako projekt na 64 akademiích v 7 státech USA. O rok později se kurzy rozšířily do Argentiny, Austrálie,

Kanady, Velké Británie a Irska. V České republice byla první akademie otevřena v roce 2000 na Fakultě elektrotechnické ČVUT v Praze. Dnes v ČR funguje 82 akademií, kde působí 215 lektorů. Za dobu rozvoje programu technologie zcela proměnily náš svět. Vzpomenete si ještě na rok 1997?

## IT specialista v roce 1997 a nyní

Před více než 20 lety se od IT specialistů očekávala pouze hluboká znalost technologií. Síťoví inženýři se tak zaměřovali na propojování jednotlivých zařízení a manuální aktualizaci systémů. Tomu odpovídaly i dovednosti, které po nich zaměstnavatelé vyžadovali. Tehdejší IT specialista musel umět především zajistit plánování sítě, její konfiguraci, řešit nastalé problémy. Nové technologické trendy, jako mobilita, internet věcí, prediktivní analýza, cloud či kybernetická bezpečnost, způsobily, že znalosti i dovednost IT specialistů dnes musí zahrnovat mnohem širší záběr. Rozdíl mezi současnou digitální érou a dobou před dvěma dekádami lze demonstrovat i na statistikách datových přenosů. Už v roce 2020 se do sítě připojí více než 1 milion zařízení za hodinu. A zatímco v roce 1997 protéklo globálně internetem za měsíc 5 petabytů dat, v roce 2018 to podle aktuální studie Cisco Visual Networking Index měsíčně bude asi 151 exabytů, tedy více než 30 000krát více. Tento vývoj se v příštích 10 až 15 letech ještě zrychlí. Dnešní a budoucí IT specialisté tak budou muset umět programovat, zvládnout prototypování, rozumět kontextu v rámci svého oboru a rozumět kyberbezpečnosti, cloudu, automatizaci, internetu věcí či síťovým systémům.

*„Podle Evropské komise dnes 90 % pracovních pozic vyžaduje alespoň částečnou znalost digitálních technologií. Tento údaj se týká všech pozic napříč obory, a to i těch, u kterých to nemusí být na první pohled patrné, jako jsou zemědělství, zdravotnictví či stavebnictví. Proto je nutné zajistit i základní IT vzdělávání dostupné pro všechny tak, aby odráželo potřeby všech sektorů. Světy IT a byznysu se neustále přibližují. Pravděpodobně asi nikdy nesplynou, neboť vždy budou zaměstnanci, od kterých se budou očekávat hlubší technologické znalosti. Tento proces není ničím novým. Přetváří podobu světa a promítá se i do kurzů Cisco Networking Academy. A tak zatímco dříve jsme učili studenty téměř výhradně nastavovat sítě, v současnosti nabízíme kurzy specializované na zařízení internetu věcí či kybernetickou bezpečnost,“ říká Jan Elefant.*

## Spolupráce soukromého a akademického sektoru

Aby společnost Cisco zajistila úspěšné přijetí kurzů, od samého počátku spolupracovala s akademickou sférou a dalšími vzdělávacími organizacemi. To umožnilo přenést nové technologické kurzy na více lidí a spolupracovat na zlepšování technologického vzdělání poskytovaného školami a univerzitami. Postupem času se tento vzdělávací program aktualizoval, aby odpovídal skutečným potřebám. Dnes je rozdělen do tří úrovní dle stupně obtížnosti.

- **Úroveň 1** zahrnuje kurzy pro samouky, které jsou určeny studentům všech typů - a to i těm, kteří nemají žádné IT zkušenosti. Díky těmto kurzům mohou studenti zvážit svoji případnou kariéru v technologických oborech. Do této úrovně patří témata, jako Úvod do kybernetické bezpečnosti či Úvod do internetu věcí.
- **Úroveň 2** nabízí základní vzdělávací kurzy, z nichž mnohé mají úroveň certifikace a připravují studenty na technologickou kariéru. Patří sem témata, jako Základy IT, Základy kyberbezpečnosti či Základy sítí.
- **Úroveň 3** poskytuje kurzy určené pro budování kariéry specialistů. Pokrývá odborné certifikace, jako Cisco Certified Entry Level Technician (CCENT), Cisco Certified Network Associate (CCNA), Cisco Certified Network Associate Security (CCNA Security), Cisco Certified Network Professional (CCNP), CCNA Cyber Ops, NDG Linux I a II.

## Moderní trendy – kyberbezpečnost a internet věcí

Úvod do kybernetické bezpečnosti a Úvod do internetu věcí patří mezi nejmladší kurzy, které se v rámci Cisco Networking Academy vyučují, a jsou příkladem toho, kam se IT posunuje a kam se musí spolu s ním proměnit i vyučované předměty. A právě tyto oblasti dokazují i to, jak se vzájemně různé oblasti propojují. Můžeme si vzít jednoduchý příklad z praxe.

Útočníci dnes využívají bezpečnostní mezery v zařízeních internetu, aby získali kontrolu nad kritickou infrastrukturou organizace. Roste také velikost a síla IoT botnetů (tj. jednotná síť počítačů útočící na zařízení internetu věcí) a již se dostáváme do bodu, kdy bude útok schopný částečně narušit chod celého internetu. I přesto panuje u organizací stále velký nezáměr a podceňování hrozby, kterou IoT

botnety představují. Pouze 13 % organizací podle průzkumu Cisco zařadilo IoT botnety mezi hlavní hrozby, které mohou v roce 2018 ohrozit jejich podnikání. Přitom stále častěji přidávají senzory do svého IT prostředí, ale o bezpečnosti mají jen malý přehled.

Výzkumníci ze společnosti Qualys testovali, jak jsou zabezpečena IP zařízení internetu věcí, jako systémy pro regulaci teploty (HVAC), dveřní zámky, panely požárních panelů a čtečky karet. Na nich zkoušeli odolnost vůči již známým hrozbám. Testováno bylo celkem 7328 zařízení, avšak pouze 1206 z nich mělo instalovanou aktualizaci, která zranitelnost odstranila. To znamená, že 83 % zařízení internetu věcí ze vzorku obsahovalo kritickou zranitelnost. A i když nebylo u žádného testovaného zařízení zjištěno, že by jej útočníci ovládali, přesto se nezdá, že by organizace byly motivovány je zabezpečit.

A právě to jsou příklady z praxe, na které musí být budoucí počítačová experti připravováni. Aktuální kybernetické hrozby shrnuje bezpečnostní expert společnosti Cisco Milan Habrcetl. „Útočníci dnes využívají sofistikované metody, které ještě před pár lety byly spíše v rovině teorie. Rostoucí počet a rozmanitost malwarů dokazuje jejich stále větší snahu o to, být stále o krok napřed proti obráncům. Aktuálně se musíme připravit především na rostoucí nárůst útoků zneužívajících šifrovanou komunikaci, legimitní služby, již zmíněnou zranitelnost zařízení internetu věcí. Velkým tématem současnosti je také kvalitní zabezpečení e-mailu, který stále platí za nejrozšířenější komunikační nástroj. Dnes až 90 % průniků do systému začíná právě u něj. Navíc se mezi útočníky stává oblíbenou platforma Microsoft Office 365.“

## Uvažovat v širších souvislostech

Součástí vzdělávání nejenom IT specialistů by mělo být kromě seznámení s aktuálními trendy v dané oblasti také formování správného uvažování o technologiích v tom správném kontextu. Jako příklad lze opět použít oblast kyberbezpečnosti. 72 % bezpečnostních profesionálů v průzkumu Cisco 2018 Security Capabilities Benchmark Study uvedlo, že primárně kupují to nejlepší řešení, které si mohou dovolit. Pouze 28 % bezpečnostních profesionálů pak primárně vybírá řešení tak, aby byla integrována se stávající infrastrukturou. Na první pohled se zdá logické, že organizace chtějí to nejlepší. Avšak tímto způso-

bem uvažují separátně pouze o několika bodech a již si neuvědomují, jaký výsledek to bude mít na úrovni celku.

*„Tímto přístupem si organizace zakládají na několik budoucích problémů. Zaprvé, těžko se jim hledají odborníci, kteří umí pracovat se všemi bezpečnostními nástroji. Zadruhé, ne všechny nástroje dokážete spojit tak, aby se z nich stala skutečně neproniknutelná hradba. Nabízí se jedna paralela. Představte si, že si na závody připravujete sportovní vůz. Nakoupíte nejvýkonnější motor z USA, podvozek z Německa, italskou karoserii a zvolíte japonská kola, protože ve své kategorii se jednalo o nejlepší produkty. Jenže pak zjistíte, že kola vůbec nesedí k ose a motor do zvoleného typu karoserie nemáte šanci vecpat. A tak namísto jistého vítězství v závodech máte garáž plnou prvotřídních autodílů,“ říká Milan Habrcetl.*

## Co bude dál?

Studie Světového ekonomického fóra The Global Competitiveness Report 2017–2018 říká, že konkurence České republiky se bude odvíjet od schopnosti využívat nejsofistikovanější výrobní procesy a inovace. „Pokud chceme být připraveni, potřebujeme podporovat studenty se zájmem o technologie, nesnažit se jim vštípit informace nezáživnou formou, ale skutečně je připravit na budoucí kariéru. Musíme ale být dostatečně flexibilní, abychom je učili skutečně aktuální věci, které hýbou světem. V oblasti technologií totiž více než jinde platí, že to, co před dvaceti lety, deseti, ale i pěti lety fungovalo, je dnes dávno překonané,“ uzavírá Jan Elefant.

# Egovernment

elektronizace veřejné správy



Vše o elektronizaci veřejné správy  
- srozumitelně a zdarma:  
[www.egovernment.cz](http://www.egovernment.cz)



## Jednotný ekonomický systém Královéhradeckého kraje

**Cílem vybudování jednotného ekonomického informačního systému (JEKIS) bylo zefektivnit řízení krajského úřadu a příspěvkových organizací Královéhradeckého kraje a zkvalitnit poskytování služeb veřejné správy na všech jeho úrovních. Projekt měl umožnit krajskému úřadu (KÚ) získávat aktuální a detailní ekonomické informace o jednotlivých příspěvkových organizacích, které lze využít pro plánování i řízení.**

Informační systém požadoval objednatel integrovat do existujícího prostředí technologického centra. Projekt přímo navazoval na stávající e-government strategie Královéhradeckého kraje a byl financován za podpory Evropské unie a Integrovaného operačního programu, specifický cíl 2.1 Zavádění ICT v územní veřejné správě.

### 22 systémů do jednoho

Na základě veřejné zakázky „Jednotný ekonomický informační systém Královéhradeckého kraje“ se dodavatelem stala společnost GORDIC. Celý projekt byl rozdělen do

dvou etap. První byla zahájena v dubnu 2015 a dokončena na konci téhož roku. Etapa zahrnovala důkladnou předimplementační analýzu, která se dotkla samotného KÚ i všech 129 příspěvkových organizací, zřízených Královéhradeckým krajem (působících ve školství, sociálních službách, kultuře, zdravotnictví a dalších oblastech). Zde bylo do té doby využíváno 22 různých informačních systémů.

V průběhu analýzy došlo ke zmapování současného prostředí, procesů i způsobů řešení zpracování, oběhu a vyřizování ekonomických dokladů a dokumentů v organizacích. Zjištěné skutečnosti sloužily jako podklad pro

optimalizaci celého řešení. Analýza se konkrétně týkala základních i ekonomických informací, personálního zabezpečení v oblasti ekonomických agend, používaných bankovních účtů, účetního deníku, pokladen i HW a SW vybavení.

Jako základ řešení využil GORDIC svoji softwarovou platformu GINIS. Pro JEKIS, implementovaný v technologickém centru, je využíváno jádro GINIS a dále subsystémy Ekonomika a interface. Systém zajišťuje komplexně správu ekonomických procesů pro zmiňovaných 129 příspěvkových organizací, dislokovaných na 181 pracovištích, i pro samotný krajský úřad. Kromě analýzy, rozšíření HW technologického centra, dodávky licencí a instalace samotných softwarových produktů zahrnovala první etapa projektu i migraci dat, implementaci a spuštění produkčního provozu pro pilotní skupinu 20 organizací.

Druhá etapa projektu byla realizována v roce 2016. Byla při ní dokončena implementace a ke spuštění produkčního provozu již došlo i ve všech zbývajících organizacích, KÚ nevyjímaje. Po proškolení administrátorů a uživatelů proběhly zátěžové, akceptační a bezpečnostní testy.

### Masivní integrace i jednotná metodika

K 1. 1. 2017 se již datuje zahájení produktivního provozu ve všech organizacích. Nahrazení široké škály původních systémů zjednodušilo řadu procesů. Přispěla k tomu i vytvořená vazba na aplikace třetích stran, konkrétně na oblasti majetku, datového skladu a speciální evidence. S využitím integrační platformy bylo dosaženo propojení JEKIS také s celostátními systémy, jako jsou ISZR, ISIR, registr nespolehlivých plátců DPH, IISP, ARES, ISDS, ISRS atd.

Došlo k zefektivnění práce například v agendách účetnictví, rozpočet, výkaznictví, objednávky, kniha došlých faktur, evidence smluv, sklady, pohledávky a v celé řadě dalších. K nim byla zároveň zpracována jednotná metodika použití systému, vycházející ze základní implementační metodiky s přihlédnutím ke specifickým jednotlivých organizací. Nastaveny byly konkrétní a přesné postupy, procesy, činnosti odborů, oddělení i jednotlivých pracovníků.

### Kontrolní procesy nastaveny

Pro příspěvkové organizace byla vypracována ve spolupráci s KÚ jednotná účetní analytika. Díky tomu je možné sledovat a porovnávat hospodaření jednotlivých organizací. Dále došlo ke sjednocení výstupních sestav a zavedení elektronického oběhu dokumentů krajského úřadu, včetně schvalovacích procesů pro řídicí kontrolu.

Součástí projektu byla i série odborných workshopů, při kterých bylo proškoleno více než 500 uživatelů. Samostatně pak probíhalo školení administrátorů JEKIS. V této souvislosti je třeba poděkovat celému vedení projektu na straně KÚ za kvalitní součinnost nutnou pro úspěšnou realizaci projektu i všem zainteresovaným pracovníkům, kteří si museli osvojit práci v prostředí nových aplikací.

I jejich zásluhou se podařilo uvést do provozu jednotný systém, který splňuje veškeré vymezené požadavky napříč organizacemi kraje a agregovat jejich jednotně strukturovaná data díky funkčnímu procesu kontrol a hlášení. Taková data se mohou stát cenným podkladem pro plány dalšího rozvoje a zvyšování efektivity fungování kraje.

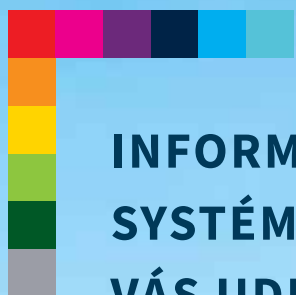
Ing. Michal Tausch,  
marketingový specialista



GORDIC®



**ICZ**



**INFORMAČNÍ  
SYSTÉMY ICZ  
VÁS UDRŽÍ  
NA ŠPICI**

[www.iczgroup.com](http://www.iczgroup.com)