ict unie

# Služby **eGovernmentu** pro privátní sféru

poziční materiál Klubu ICT Unie

# ICT Unie

## SDRUŽENÍ PRO INFORMAČNÍ TECHNOLOGIE A TELEKOMUNIKACE

**ICT Unie** je profesní sdružení firem z oboru informačních technologií a elektronických komunikací, dalších podnikatelských a vzdělávacích subjektů, jehož cílem je zvýšit vnímání důležitosti zavádění a využívání moderních informačních technologií ve společnosti, včetně vytváření optimálních podmínek pro rozvoj veřejných sítí elektronických komunikací v České republice, jako nezbytného předpokladu pro vytváření informační společnosti.

Sdružení bylo založeno v lednu 2010 a navazuje ve své činnosti na cíle Sdružení pro informační společnost (SPIS), a Asociace provozovatelů veřejných telekomunikačních sítí (APVTS).

Sdružení definuje, reprezentuje, podporuje a prosazuje oprávněné a společné zájmy svých členů s cílem vytvářet vhodné podnikatelské prostředí, které při respektování etických zásad podnikání povede k dlouhodobému rozvoji informační společnosti. Vzhledem k tomu, že rozvoj veřejných sítí elektronických komunikací je založen na otevřené soutěži, je specifickým cílem Sdružení podpora a ochrana rovného a otevřeného trhu elektronických komunikací v České republice.

ICTU má za cíl významným způsobem přispět k rozvoji české ekonomiky tak, aby se ČR dostala na špici v konkurenceschopnosti, budování inovativní a znalostní společnosti.

ICTU jako profesní asociace firem z oblasti informačních a telekomunikačních technologií dílem reprezentuje ICT průmysl České republiky a prosazuje efektivní využívání ICT ve všech sférách života v České republice, neboť v tom spatřuje podmínku nutnou pro přechod společnosti ke společnosti založené na znalostech a inovacích.

ICTU je proto spolutvůrcem návrhů zásadních reforem, legislativy a klíčových rozhodnutí zaměřených na rozvoj ICT v České republice. ICTU je partnerem státních regulačních institucí.

ICTU je sdružením pragmatickým a efektivním. To znamená, že chce předkládat návrhy reálné, praktické a samozřejmě prospěšné nejen ICT průmyslu. ICTU v žádném případě nedělá lobby za individuální zájmy svých členů a ovlivňování veřejných zakázek.

Další informace najdete na www.ictu.cz

Vážené čtenářky, vážení čtenáři,
jsem rád, že Vám mohu představit tento unikátní dokument.

Jde o výsledek kolektivního snažení Klubu ICTU (dříve: Klub SPIS), což je výlučný klub tvořený ze zástupců informatiků veřejné správy a ze zástupců komerční sféry – členů ICT Unie. Tento Klub na svých zasedáních odborně posuzoval problematiku eGovernmentu a výsledkem je tento koncepční materiál, který vyjadřuje pozici Klubu a celého sdružení ICT Unie.

V rámci celé nové architektury eGovernmentu - zejména s ohledem na budování systému základních registrů a zavádění elektronických občanských průkazů – tento dokument identifikuje ty oblasti, které je třeba ještě upřesnit či dopracovat, aby se současné změny mohly promítnout i do privátní sféry.

Možná vás napadá, proč tento dokument vznikl a co je jeho cílem. Je to jednoduché: i privátní sféra chce využívat správná, aktuální a garantovaná data, když už budou k dispozici. I privátní sféra chce snižovat své náklady (které by jinak měla se získáváním a udržováním vlastních dat). I privátní sféra chce svým zákazníkům přinášet stejné výhody, jaké ve veřejné sféře přinese moderní eGovernment.

Takže jde o to, aby užitek ze současných změn v eGovernmentu byl maximalizován jak ve veřejné, tak i v privátní sféře. Aby privátní sféra pomohla veřejné sféře propagovat přínosy eGovernmentu, tím že je bude sama využívat. Aby privátní i veřejná sféra vzájemně spolupracovaly, ku prospěchu nás všech – ať již v roli občanů či zákazníků.

Svatoslav Novák
Prezident ICT Unie

Duben 2010

Materiál je také k dispozici na webových stránkách ICT Unie: www.ictu.cz/klub

# 1 Obsah

# 2 Úvod

Rozvoj eGovernmentu v České republice již významně pokročil. Byla navržena a podrobněji rozpracována celá nová architektura eGovernmentu, symbolizovaná motivem eGONa, a postupně se implementují její jednotlivé části.

Již zprovozněn byl „front-office“ nové architektury, v podobě soustavy kontaktních míst veřejné správy (Czech POINT) i v podobě datových schránek, jako nástroje pro doručování mezi subjekty a klienty eGovernmentu. Započat byl také přechod od listinných dokumentů a agend na plně elektronické, včetně mechanismů konverze mezi oběma formami dokumentů.

Další velkou etapou rozvoje eGovernmentu v České republice jsou změny v jeho „back-office“. Tedy změny týkající se uchovávání základních dat pro potřeby agend veřejné správy, spočívající v zavedení celého systému základních registrů a následné úpravě všech agend tak, aby místo s vlastními instancemi základních dat tato data přejímaly od základních registrů jako tzv. referenční údaje.

V současné době jsou tyto změny v „back-office“ v různém stadiu rozpracovanosti: základní zákony jsou již přijaty a v účinnosti tak, aby k 1. 7. 2010 mohlo být zahájeno dvouleté implementační období.

Jinou významnou částí nové architektury eGovernmentu jsou změny v oblasti identifikace a autentizace fyzických osob. Zavedeny budou nové (elektronické) občanské průkazy, které budou logicky dvoudílné, a část údajů na těchto průkazech bude umístěna již pouze v základních registrech.

Všechny tyto změny směřují k výrazně efektivnějšímu, ale také uživatelsky vstřícnějšímu, spolehlivějšímu a bezpečnějšímu eGovernmentu. Nicméně jde o změny, které se netýkají pouze samotného eGovernmentu, ale mají významné dopady na celou společnost, včetně celé privátní sféry.

I privátní sféra tak bude muset reagovat na chystané změny v eGovernmentu. Jednak proto, aby mohla nadále řádně fungovat a plnit povinnosti, které jí ukládají zákony České republiky. Ale i proto, že i privátní sféra sama chce využít změn v eGovernmentu a nových možností, které tyto změny přináší, ke zdokonalení a zefektivnění své vlastní činnosti.

Napomoci takovéto synergii mezi privátní a veřejnou sférou je cílem tohoto dokumentu, který začal vznikat ještě na půdě Sdružení pro informační společnost, nyní již ICT Unie (na platformě Klubu SPIS, resp. Klubu ICT Unie), v rámci vzájemné diskuse představitelů veřejného a privátního sektoru. V rámci celé nové architektury eGovernmentu se snaží identifikovat ty oblasti, které je třeba ještě upřesnit či dopracovat, a navrhuje jejich doplnění a rozšíření tak, aby potenciál nového eGovernmentu mohl být využit co možná nejvíce nejen ve veřejné, ale i v privátní sféře.

# 3 Shrnutí

## Dokument je strukturován do čtyř hlavních částí.

- **První část** rekapituluje podstatu změn, které již jsou připraveny (ať již formou zákona v účinnosti, návrhu novel či zveřejněné koncepce). Popisuje podstatu a princip fungování základních registrů, přínosy nových elektronických občanských průkazů a také nové formy komunikace občanů s veřejnou správnou. Zde **konstatuje, že dosud není dostatečně řešena vazba celého systému základních registrů na komerční informační systémy** (například IS jednotlivých bank, operátorů, utilit apod.), **stejně jako vazba na provozní informační systémy provozované ve veřejné správě** (například IS mzdových agend apod.). Dostatečně rozpracováno není ani poskytování informací a služeb širší občanské veřejnosti.

- **Druhá část** popisuje potenciál, který nová architektura eGovernmentu přináší, a deklaruje zájem privátní sféry podílet se na využití a dalším rozvíjení tohoto potenciálu.

- **Třetí část** shrnuje hlavní úskalí nové architektury eGovernmentu, která autoři identifikovali. Kromě obecného nedostatku v podobě nerozpracované vazby na privátní sféru a směrem k veřejnosti jde konkrétně o:

  - **nedořešenou otázku mandatorního přístupu privátních subjektů k osobním údajům v základních registrech**: některé subjekty, jako například banky, mají zákonem uloženo pracovat s údaji, které budou obsaženy v základních registrech – ale ty na tuto potřebu dosud nepamatují.

  - **chybějící možnost interaktivního přístupu a strukturovaných dat**: dodávání nestrukturovaných dat do datových schránek nelze využít pro vzájemnou interakci informačních systémů v reálném čase.

  - **nepřijatelnost modelu PUSH**: představa, že stát bude z vlastní iniciativy dopravovat změnová data předem určeným příjemcům v privátní sféře („model PUSH“), by znamenala odpovědnost státu za aktuálnost dat, se kterými budou privátní subjekty pracovat.

  - **nedostatečnost dvoufaktorové autentizace**: autentizace fyzických osob pomocí čísla jejich elektronického občanského průkazu (eOP) a bezpečnostního ochranného kódu (BOK-u) je pro řadu transakcí nedostatečná.

# 3 Shrnutí

- **Čtvrtá část** přináší návrhy a doporučení:
  - **upřesnění základních pojmů**:
    - rozlišování mezi **přístupem** (občanů k informacím a službám eGovernmentu) a **propojením** (mezi informačními systémy),
    - mezi **anonymním přístupem** (není známo, kdo je příjemcem služby či informace) a **autentizovaným přístupem** (je známo, kdo je příjemcem),
    - mezi **interaktivním** a **neinteraktivním způsobem komunikace**.
  - **upřesnění terminologie a architektury eGovernmentu**:
    - rozlišování mezi **agendovými IS**, **resp. AIS** (ve smyslu informačních systémů veřejné správy, ISVS), které jako jediné mají možnost přímého napojení na informační systém základních registrů (ISZR), **komerčními IS** (provozovanými v privátní sféře) a **provozními IS** (informačním systémy provozovanými ve veřejné správě, které ale nemají statut ISVS), a nemají možnost napojení na ISZR.
    - zavedení dvou dílčích **variant agendových IS** (AIS):
      - **AISP-I**, které slouží **potřebám přístupu** (anonymního i autentizovaného přístupu občanů ke službám eGovernmentu),
      - **AISP-II**, které slouží potřebám **propojení** (propojení těchto AISP-II s komerčními a provozními IS).
  - **zřízení Univerzální portálové agendy (UPA)**, a to přeměnou stávajícího Portálu veřejné správy, jako jediného AISP-I, pro centrální poskytování všech variant přístupu občanům (tj. společně pro všechny agendy).
  - **zřízení dalších AISP-II**, realizujících propojení s komerčními IS a provozními IS, a to pro:
    - poskytování údajů a služeb n**a základě mandatorních nároků** komerčních či provozních IS,
    - poskytování osobních údajů **na základě uděleného souhlasu** subjektu údajů,
    - poskytování **veřejných údajů**,
    - poskytování **dalších služeb** – zde bude nutná legislativní úprava (pro možnost poskytování takovýchto služeb).
  - **model PULL místo modelu PUSH**: údaje poskytované pomocí původně uvažovaného modelu PUSH mohou mít jen informativní charakter. Pro závazné hodnoty údajů musí být využit model PULL (příjemce si musí sám ověřit platnost dat).
  - **posílení autentizace na třífaktorovou**: dvoufaktorovou autentizaci (jen na základě čísla eOP a kódu BOKu), která pro mnohé agendy není dostatečná, je třeba posílit **zavedením třetího faktoru** v podobě jednorázových autentizačních kódů. A to jednotně a centrálně pro všechny agendy.
  - **poskytování dalších služeb eGovernmentu**: aby i subjekty z privátní sféry mohly autentizovat své zákazníky pomocí nových eOP a s nimi spojenými kódy BOK (a také jednorázovými autentizačními kódy, v rámci třífaktorové autentizace), je nutné zavést v rámci eGovernmentu službu, která by toto umožnila. Další obdobné služby pro privátní sféru by měly být upřesněny ve vzájemné diskusi mezi veřejnou a privátní sférou.

# 4 Vize změn

Tento dokument se zaměřuje především na takové změny v oblasti eGovernmentu, které ještě nebyly plně implementovány, ale nachází se v různých fázích své přípravy a implementace. Konkrétně jde o tyto tři oblasti:

- zavádění základních registrů a přebírání referenčních údajů agendovými informačními systémy veřejné správy,
- zavádění elektronických průkazů,
- nové možnosti komunikace občanů s veřejnou správou.

## 4.1 Koncepce základních registrů

Nejzásadnější změny v celé oblasti eGovernmentu se týkají způsobu, jakým stát hodlá nadále hospodařit se základními daty, která má k dispozici on (resp. státní správa), ale obecně celá veřejná správa. Tedy data, se kterými pracují nejrůznější agendové informační systémy veřejné správy (dále též **agendové IS, AIS**), které mají statut informačních systémů i z pohledu zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

Na správnosti a aktuálnosti těchto dat ale závisí i fungování komerčních informačních systémů (dále též **komerčních IS, KIS**), provozovaných v privátní sféře, stejně jako fungování nejrůznějších provozních informačních systémů provozovaných ve veřejné správě (dále též **provozních IS, PIS**)[1]. Jde přitom o data, která mohou mít charakter osobních údajů (jako například údaje o bydlišti, rodinném stavu konkrétní fyzické osoby), nebo mohou být plně veřejná, případně mohou být kombinací obojího (tj. zahrnovat jak veřejné údaje, tak i osobní údaje).

Až dosud přitom platil obecný princip, že každá jednotlivá agenda si všechna svá data získávala sama, sama si je uchovávala a sama také musela dbát na jejich správnost, úplnost a aktuálnost. Konzistence mezi stejnými údaji v rámci různých agend ale nebyla systematicky řešena a neexistovalo ani sdílení těchto údajů. Za aktualizaci údajů, které se ho týkají, byl obvykle odpovědný subjekt těchto údajů. Především tedy občan, který byl povinen sám a včas hlásit jakoukoli změnu v relevantních údajích – a to obecně všem agendám, které s příslušnými údaji pracovaly.

Řešena dosud nebyla ani obrana proti nežádoucí agregaci osobních údajů v rámci různých agend: jednotlivé osoby byly v různých agendách vedeny nejčastěji pod svým rodným číslem. To významně usnadňovalo možnost zneužití, skrze agregaci osobních údajů o téže osobě z různých agend.

### 4.1.1 Referenční údaje v základních registrech

Podstatou změny, ke které směřuje zavedení základních registrů, je zavedení jiného principu: nejdůležitější a nejčastěji používané údaje budou uchovávány a průběžně aktualizovány jen na jednom centrálním místě, v jednom z tzv. **základních registrů**. Ty agendy, které budou s takovýmito údaji pracovat, je pak již nebudou udržovat a aktualizovat samy, ale pro potřeby svého fungování budou jejich aktuální hodnotu získávat z tohoto centrálního místa (ze základních registrů) jako tzv. **referenční údaje**.

[1] Příkladem takovýchto provozních informačních systémů mohou být například IS pro potřeby mzdové či personální agendy apod. Obecně takové, které nepředstavují výkon veřejné moci, ale slouží interním potřebám samotného orgánu veřejné moci.

# 4 Vize změn

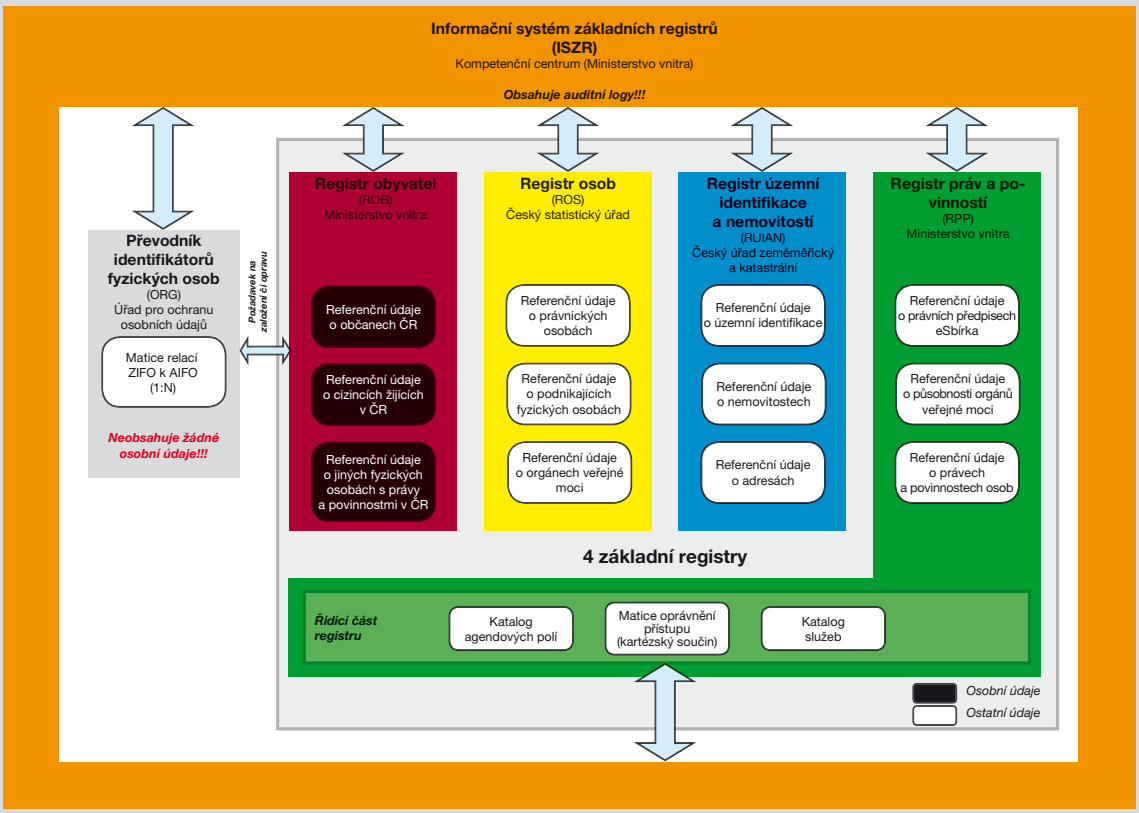
## Architektura základních registrů

Základem celé koncepce nového eGovernmentu je existence čtyř základních registrů:

- **registru obyvatel (ROB)**: tento základní registr bude obsahovat (a poskytovat jako referenční) základní údaje o všech občanech ČR, cizincích s povolením k pobytu v ČR a občanech jiných států vedených v základních registrech. Půjde o osobní údaje, věcným gestorem tohoto základního registru bude Ministerstvo vnitra ČR.
- **registru osob (RO)**: tento základní registr bude obsahovat (a poskytovat jako referenční) údaje o všech ekonomických subjektech v ČR. Tedy o všech právnických osobách, podnikajících fyzických osobách, organizačních složkách státu a organizačních složkách zahraničních právnických osob. Půjde o veřejné údaje, věcným gestorem tohoto základního registru bude Český statistický úřad.
- **registru územní identifikace, adres a nemovitostí (RÚIAN)**: tento základní registr bude obsahovat (a poskytovat jako referenční) základní identifikační lokalizační údaje vztahující se k územním prvkům a územně-evidenčním jednotkám a nemovitostem. Půjde o veřejné údaje, věcným gestorem tohoto základního registru bude Český úřad zeměměřický a katastrální.
- **registru práv a povinností (RPP)**: tento základní registr bude evidovat oprávnění pro přístup do základních registrů, seznam názvů agend a jejich číselných kódů, údaje o právech a povinnostech fyzických a právnických osob (pokud jsou tyto údaje vedeny v základních registrech), údaje o dalších právech a povinnostech osob, pokud to stanoví jiný právní předpis. Věcným gestorem tohoto registru bude Ministerstvo vnitra ČR.

Další nezbytou součástí celé soustavy základních registrů bude **převodník identifikátorů fyzických osob (ORG)**, který bude provozovat Úřad pro ochranu osobních údajů. Bude přidělovat konkrétní hodnoty agendových identifikátorů pro jednotlivé agendy a bude také zajišťovat jejich vzájemný převod (tam, kde je k tomu žadatel oprávněn).

Veškerou komunikaci celé soustavy základních registrů (včetně převodníku ORG) s vnějším okolím bude **zajišťovat informační systém základních registrů (ISZR)**. ISZR bude nabízet sadu služeb (tzv. eGon služeb) a veškerá komunikace všech ostatních informačních systémů se základními registry i s převodníkem ORG bude probíhat pouze přes tyto služby. V tomto smyslu tak bude ISZR „obalovat“ celou soustavu základních registrů (a převodník ORG).

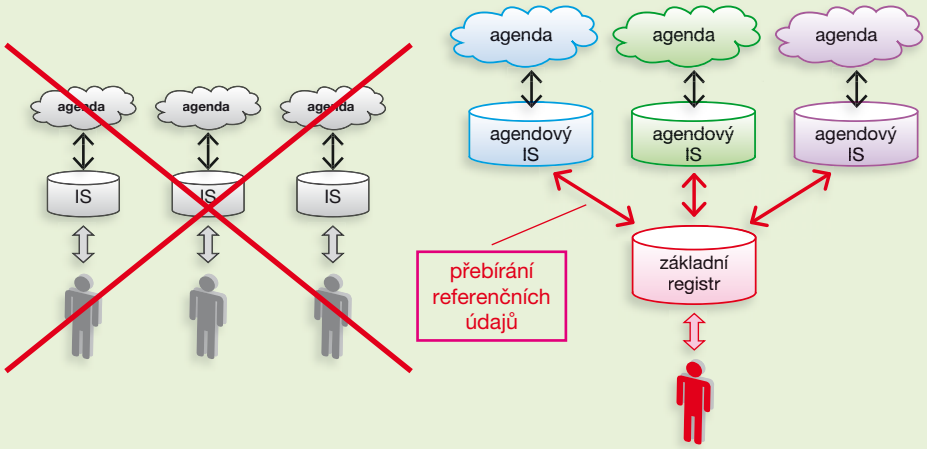


# 4 Vize změn

Významným atributem referenčních údajů bude jejich **důvěryhodnost**: agendy, které budou s těmito údaji pracovat, již nebudou muset ověřovat jejich správnost a platnost (pokud nebude prokázán opak). To je, již samo o sobě, velmi zásadní změnou oproti současnému stavu.

Navíc, vzhledem k charakteru celého řešení (centrálnímu uchovávání a poskytování z jediného centrálního místa), zaniká i nebezpečí nekonzistence dat uchovávaných souběžně na více místech, stejně jako potřeba „přenosu“ těchto dat mezi agendami. Každá agenda, která bude chtít použít nějaký konkrétní referenční údaj, bude vždy povinna použít aktuální hodnotu referenčního údaje.

Dalším důležitým atributem nově zaváděného principu je podmíněnost konkrétním oprávněním: každá agenda, která bude chtít získat jakékoli referenční údaje, k tomu bude muset mít buď oprávnění vycházející ze zákona (v případě osobních i jiných údajů), nebo explicitní souhlas subjektu údajů (v případě osobních údajů).[2]




**Obrázek 1:** Představa využití referenčních údajů

### 4.1.2 Agendové identifikátory a převodník ORG

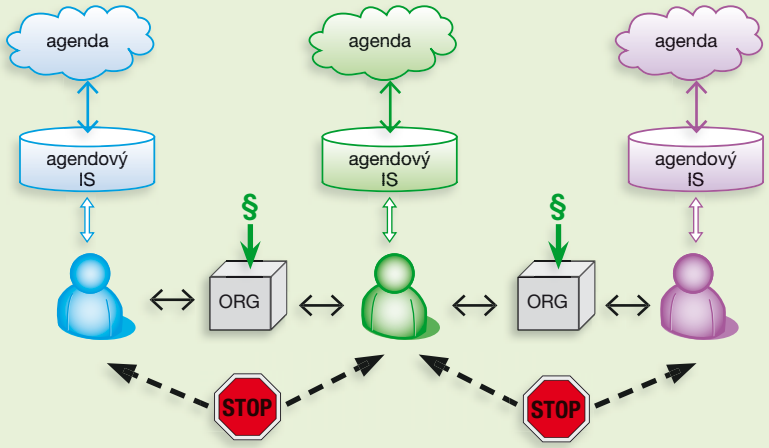
S oprávněními souvisí i další významný atribut nově zaváděného řešení, kterým je omezení nežádoucí agregace osobních údajů. V rámci každé agendy, která pracuje s osobními údaji, budou fyzické osoby identifikovány jiným typem identifikátoru, specifickým pro danou agendu (tzv. **agendovým identifikátorem**). „Jiným typem“ v tom smyslu, že z hodnoty agendového identifikátoru konkrétní osoby v rámci jedné agendy nebude možné odvodit agendový identifikátor téže osoby v rámci jiné agendy.

Jedinou možností, jak „přejít z jedné agendy do druhé“ (na základě konkrétní hodnoty agendového identifikátoru v rámci jedné agendy získat takovou hodnotu agendového identifikátoru, která v jiné agendě identifikuje stejnou fyzickou osobu), je požádat o zprostředkování Úřad pro ochranu osobních údajů, který provozuje **službu ORG** (převodník identifikátorů fyzických osob). ÚOOÚ žádosti vyhoví pouze tehdy, pokud je oprávněná (tj. buď na základě explicitního souhlasu subjektu údajů, nebo na základě zákonného zmocnění).

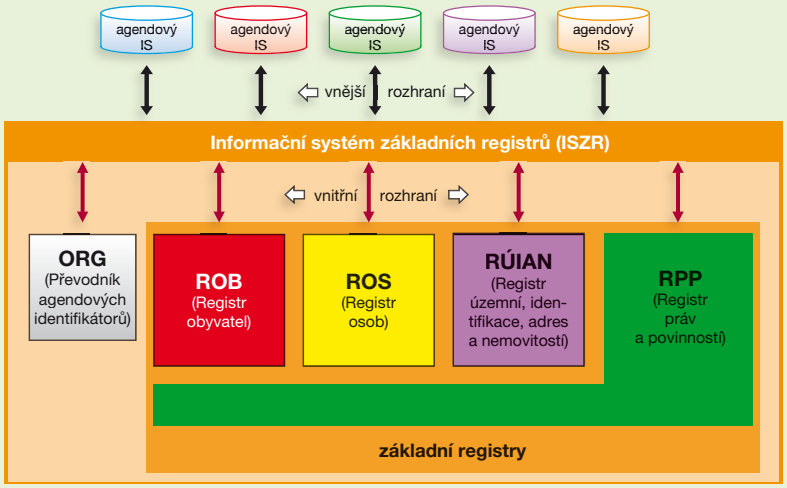
Koncepce základních registrů počítá s tím, že samotné základní registry a jimi poskytované služby nebudou pro agendové IS dostupné přímo, ale jen zprostředkovaně, přes **informační systém základních registrů (ISZR)**. Tento informační systém zprostředkovává vzájemnou komunikaci základních registrů i převod agendových identifikátorů přes službu ORG. Současně „obaluje“ základní registry a službu ORG v tom smyslu, že vytváří potřebná komunikační rozhraní, na která se teprve napojují jednotlivé agendové IS.

[2] Toto oprávnění bude konkrétně zaneseno do jednoho ze základních registrů: registru práv a povinností.

# 4 Vize změn




**Obrázek 2:** Představa fungování převodníku ORG, který převádí agendové identifikátory jen v případě oprávněného nároku




**Obrázek 3:** Představa napojení agendových informačních systémů (AIS) na informační systém základních registrů (ISZR)

Významným důsledkem zavedení celého konceptu základních registrů a přebírání referenčních údajů je nutnost změny všech informačních systémů agend veřejné správy (agendových IS): všechny budou muset být upraveny tak, aby využívaly referenční údaje poskytované základními registry. Teprve tak budou moci být naplněny hlavní přínosy celé změny.

V současné době je zavádění konceptu základních registrů ve stadiu, kdy nezbytné legislativní změny již byly přijaty[3] a nabudou účinnosti k 1. 7. 2010. Tím začne přechodné období, které bylo z původních 12 měsíců prodlouženo na 24 měsíců. Plný provoz celého systému základních registrů a předávání referenčních údajů tak bude zahájen (nejpozději) k 1. 7. 2012.

[3] Konkrétně zákon č. 111/2009 Sb., o základních registrech, zákon č. 227/2009 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o základních registrech.

### 4.1.3 Poskytování údajů třetím stranám

Zákon č. 111/2009 Sb., o základních registrech (dále též „zákon"), zavádí princip, podle kterého se na informační systém základních registrů (ISZR) mohou napojovat (a jeho služby využívat) pouze agendové informační systémy (AIS) zaregistrované u provozovatele ISZR.

**Vazba na ostatní informační systémy (tedy jak komerční IS, tak i provozní IS) ale není v již přijaté koncepci základních registrů – na úrovni zákona (tj. zejména v zákoně č. 111/2009 Sb.) – podrobněji řešena.**

Jedinou výjimkou je ustanovení § 58 odst. 9 zákona o možnosti poskytování osobních údajů třetím stranám. Ale jen na základě explicitního souhlasu údajů a jen do datové schránky:

> *Na žádost subjektu údajů staršího 18 let mohou být z registru obyvatel a registru práv a povinností poskytovány referenční údaje v jím vymezeném rozsahu jiné fyzické nebo právnické osobě do datové schránky této osoby. Subjekt údajů může svůj souhlas s poskytováním referenčních údajů z registru obyvatel a registru práv a povinností jiné fyzické nebo právnické osobě kdykoliv odvolat. Fyzická nebo právnická osoba, které byly údaje podle věty první poskytnuty, nesmí poskytnuté údaje předat dalším osobám bez výslovného souhlasu subjektu údajů.*

Pokud jde o možnost poskytování veřejných údajů, zde je v zákoně č. 111/2009 Sb. pouze jediná zmínka, konkrétně u registru osob (v § 61), o možnosti poskytování údajů přes „k tomu určené agendy":

> *Identifikátory a referenční údaje vedené o osobách, s výjimkou jména, popřípadě jmen, příjmení a místa pobytu v České republice, popřípadě bydliště v zahraničí u fyzické osoby uvedené v § 25 písm. d), jsou veřejně přístupné prostřednictvím k tomu určených agend.*

Zákon již ale neřeší, které konkrétní agendy by to měly být (které jsou k tomu určeny). Stejně tak není řešen princip zpřístupnění veřejných údajů, a to ani na úrovní toho, zda půjde o možnost dálkového přístupu či jen o dodávání do datových schránek či ještě jiné řešení. Rozlišováno není ani to, kdy jde o anonymní veřejný přístup, při kterém není známo, komu jsou údaje poskytovány, a kdy jde o přístup plně identifikované a řádně autentizované osoby (a je tedy známo, komu jsou údaje poskytovány).

Stejně tak není v zákoně řešeno, jakým konkrétním způsobem budou moci fyzické osoby (občané) vykonávat některá práva, která jim zákon nově přináší. Například udělovat svůj souhlas s poskytováním vlastních osobních údajů třetím stranám (viz výše).

### 4.1.4 Agendové informační systémy pro veřejný přístup

Teprve v zadávací dokumentaci pro výběrové řízení na implementaci ISZR[4] se objevuje zmínka o **agendových informačních systémech pro veřejný přístup (AISVP)**, které by zřejmě měly zprostředkovávat přístup dalších informačních systémů (zřejmě i provozních IS a komerčních IS) k vybraným službám ISZR. A také nabízet možnost přístupu pro koncové uživatele z řad fyzických osob.

Zmínka o agendových informačních systémech pro veřejný přístup se pak objevuje i v některých prezentacích autorů současných změn v eGovernmentu, ale stále bez dalšího upřesnění.

## 4.2 Zavádění elektronických průkazů

Další velkou oblastí, kde dochází k významným změnám, je agenda občanských průkazů. Podstatou změn je přechod od stávajících (neelektronických) občanských průkazů **k elektronickým občanským průkazům (eOP)**.

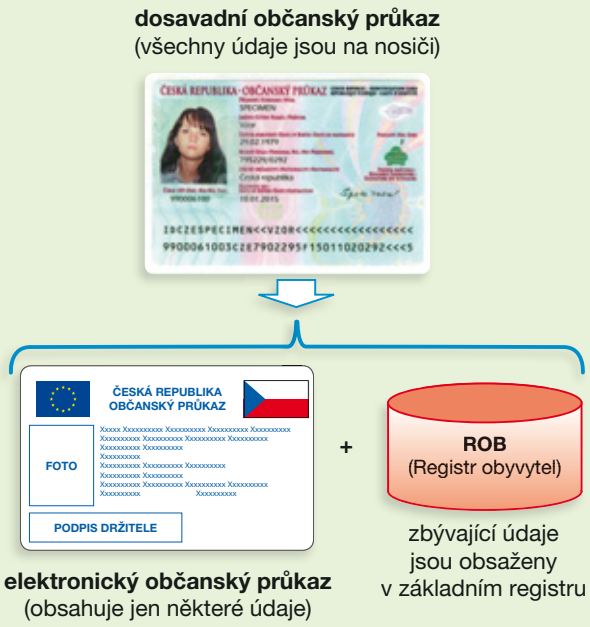
Až dosud přitom platilo, že občanský průkaz je sám o sobě nosičem řady osobních údajů. Včetně těch, které se mohou měnit relativně často – jako například bydliště či rodinný stav. Nově se zavádí princip, podle kterého se část osobních údajů (zejména

[4] Konkrétně v dokumentu ZD_ISZR_Příloha 1a.pdf, s názvem „Globální architektura základních registrů"

# 4 Vize změn

těch, které se mohou měnit častěji) odstraňuje z fyzického nosiče (občanského průkazu) a přesouvá se do základních registrů. Konkrétně do základního registru obyvatel. Právě tímto krokem (resp. v tomto smyslu) se občanský průkaz stává elektronickým (eOP). Současně s tím se stává fakticky dvoudílným:

- jedním dílem elektronického občanského průkazu je samotný fyzický nosič (realizovaný jako plastová kartička se strojově čitelnými údaji), na kterém jsou uvedeny jen nejzákladnější údaje (včetně fotografie fyzické osoby). Podle původních předpokladů se ve viditelné podobě mělo jednat pouze o jméno, příjmení, datum a místo narození, státní příslušnost a sériové číslo dokladu.
- druhým dílem elektronického občanského průkazu je datový záznam, umístěný v základním registru obyvatel a obsahující ostatní údaje o subjektu (fyzické osobě).




**Obrázek 4:** Představa dvoudílného elektronického občanského průkazu

Původním záměrem bylo to, aby se do druhého dílu (a tedy z nosiče do registru) přesunul i údaj o bydlišti a rodinném stavu a rodné číslo se přestalo používat úplně. Poslanecká sněmovna však při projednávání příslušné právní úpravy (zákona č. 227/2009 Sb.) rozhodla toto neučinit a na prvním dílu (fyzickém nosiči) ponechat jak údaj o bydlišti, tak i o rodinném stavu, a dokonce i rodné číslo. Toto opatření lze ale považovat jen za přechodné, resp. pouze dočasné, s tím, že záměrem je tyto údaje z prvního dílu (fyzického nosiče) znovu – a tentokráte již definitivně – odstranit.

Podle původního záměru (zákona č. 227/2009 Sb.) mělo vydávání nových elektronických průkazů začít 1. 7. 2010. Skrze novelu zákona o elektronickém podpisu ale bude tento termín zřejmě posunut na 1. ledna 2012.

### 4.2.1 Agendový identifikátor a sériové číslo eOP

Dalším údajem, o kterém se původně předpokládalo, že bude umístěn na prvním dílu (fyzickém nosiči), měl být agendový identifikátor osoby (subjektu údajů). Od tohoto záměru se ale také upouští, jednak kvůli neveřejnému charakteru tohoto údaje, ale i kvůli tomu, že jeho umístění na fyzický nosič (první díl eOP) by bylo zbytečné (nepřineslo by nic, co by bez tohoto údaje nebylo možné).

# 4 Vize změn

**Identifikaci** je nejsnáze si představit jako odpověď na otázku: *„o koho jde?“*, resp. *„kým jsem?“*. Například má-li nějaký poskytovatel služby určitý okruh zákazníků, jde mu při identifikaci o zjištění, který z již existujících zákazníků ho oslovuje, nebo zda jde o zcela nového zákazníka. Za poskytovatele služby lze považovat i stát, s tím že jeho „zákazníky“ jsou všichni občané. Údajem, který se v praxi používá pro identifikaci, může být jméno a příjmení, číslo občanského průkazu apod.

**Autentizace** je pak odpověď na otázku, zda *„jde skutečně o toho, za koho se vydává?“*. Při identifikaci není až tak těžké vydávat se za někoho jiného – a v rámci autentizace dochází k ověření, zda tomu tak je, či není. Například v počítačových systémech se jako autentizační údaj používá heslo (a identifikačním údajem je uživatelské jméno). V případě vyšších nároků na spolehlivost autentizace bývají využívány kryptografické postupy a metody, například s využitím osobních certifikátů.

**Rozdíl mez identifikací a autentizací** je dobře vidět například při zastupování (na základě plné moci): zde musí být spolehlivě identifikována osoba, která je zastupována, ale nedochází k její autentizaci. Místo toho se identifikuje a autentizuje zastupující osoba, která následně prokazuje svou plnou moc k zastupování.

Vzhledem k tomu (zřejmě) nebude elektronický občanský průkaz vybavován tzv. 2D kódem, tudíž nebude práce s ním vyžadovat čtečku pro tento typ kódů.

Každý elektronický občanský průkaz (eOP) tak bude jednoznačně identifikován jen svým 9místným sériovým číslem (číslem občanského průkazu ve smyslu výrobního čísla fyzického nosiče). Tedy stejně jako dosavadní (neelektronické) občanské průkazy. Převod tohoto sériového čísla eOP na odpovídající agendový identifikátor příslušného držitele občanského průkazu již zajistí systém základních registrů.

To znamená, že i držitel elektronického občanského průkazu se bude identifikovat (vůči informačním systémům veřejné správy i na kontaktních místech) primárně tímto 9místným číslem svého občanského průkazu. A tedy stejně jako držitel stávajícího (neelektronického) občanského průkazu.

Vynechání agendového identifikátoru na elektronickém občanském průkazu (resp. na jeho prvním dílu) má i jednu významnou přednost, která je i jedním z cílů zavádění nových elektronických občanských průkazů: možnost revokace neboli předčasného zneplatnění. V případě ztráty či jiné kompromitace občanského průkazu je možné tento průkaz (i s jeho sériovým číslem) snadno a ihned zneplatnit a fyzické osobě vydat nový občanský průkaz s novým sériovým číslem. Naproti tomu agendový identifikátor (který by se měnil mnohem obtížněji, podobně jako třeba rodné číslo) díky tomu může zůstat stále stejný.

### 4.2.2 Kontaktní elektronický čip na eOP

Elektronický občanský průkaz může být dále obohacen o kontaktní elektronický čip. S tím se ale počítá jen u části vydávaných eOP (a jen na žádost fyzické osoby, která si za vydání takovéhoto eOP bude muset připlatit). Způsob využití tohoto elektronického čipu není v současné době definován – a tudíž se s ním ani nepočítá pro potřeby identifikace a autentizace držitele eOP.

Příkladem možného využití kontaktního elektronického čipu je uložení osobního podpisového certifikátu držitele elektronického občanského průkazu.

### 4.2.3 Bezpečnostní osobní kód

Pro potřeby autentizace se počítá s využitím tzv. **bezpečnostního osobního kódu** (BOKu), představujícího analogii PINu u bankovních karet. Půjde o číselný údaj, který bude logicky sdružen s konkrétním eOP a bude uložen v jednom ze základních registrů (konkrétně v registru obyvatel). Takovýto BOK tak bude moci být vydáván i držitelům stávajících občanských průkazů (ještě neelektronických).

Předpokládaný princip využití bezpečnostního osobního kódu (BOKu) – a to jak u elektronických občanských průkazů, tak i u těch neelektronických – je následující: konkrétní fyzická osoba se identifikuje 9místným sériovým číslem svého eOP (resp. číslem svého neelektronického občanského průkazu). Následně se autentizuje zadáním svého BOKu.[6]

### 4.2.4 Získávání údajů z druhého dílu elektronického občanského průkazu

Hlavním rozdílem mezi elektronickým a neelektronickým občanským průkazem tak bude umístění

[6] Viz § 18 odst. 2 zákona č. 111/2009 Sb.

údajů o držiteli průkazu: u neelektronických průkazů budou všechny tyto údaje umístěny na samotném („jednodílném“) občanském průkazu, zatímco u elektronických občanských průkazů bude část údajů přímo na průkazu (na jeho prvním dílu neboli na nosiči), přičemž zbývající část údajů bude umístěna v základním registru obyvatel. Lze předpokládat, že výhledově bude v registru umístěn i údaj o adrese pro doručování a o rodinném stavu.

Důsledkem bude nový způsob práce s elektronickými občanskými průkazy: kdykoli bude třeba zjistit či ověřit některý z údajů, který se nenachází na samotném nosiči (na prvním dílu občanského průkazu), bude nutné o tyto údaje požádat základní registry skrze některou ze služeb poskytovaných informačním systémem základních registrů (ISZR). Takovouto možnost ale bude mít jen ten, komu budou takovéto služby poskytovány.

## 4.3 Nové možnosti komunikace občana s veřejnou správou

Součástí již připravených či teprve chystaných změn v eGovernmentu jsou i změny toho, jak budou občané (jako klienti eGovernmentu) moci komunikovat s veřejnou správou. Tyto možnosti navazují na úpravu občanských průkazů a existenci bezpečnostního osobního kódu (BOKu), které umožňují elektronickou identifikaci a autentizaci.

Možnosti komunikace občana s veřejnou správou bude nově možné rozdělit do dvou variant:

- **neinteraktivní varianta**: občan jednorázově zformuluje a podá svou žádost (jakýmkoli způsobem, který je k tomu využitelný) a následně získá odpověď. Tato mu je doručena buďto do jeho datové schránky na elektronickou adresu[7], nebo v listinné podobě (obecně dle pravidel pro doručování).

- **interaktivní varianta**: u této varianty občan může klást své dotazy opakovaně a odpovědi na ně získává průběžně (interaktivně). Lze předpokládat, že tato varianta komunikace bude vždy probíhat on-line způsobem (způsobem umožňujícím dálkový přístup).

Interaktivní varianta vyplývá mj. z ustanovení § 5 odst. 4 zákona č. 111/2009 Sb., o základních registrech, který říká, že:

> *Fyzická osoba získává údaje, které jsou o ní vedeny v základních registrech, po ověření její totožnosti občanským průkazem umožňujícím elektronickou identifikaci; fyzická osoba může po ověření její totožnosti umožnit přístup k údajům, které jsou o ní vedeny, též třetí osobě.*

Tato možnost byla v návrhu zákona č. 111/2009 Sb. (konkrétně v předkládací zprávě) detailněji popsána takto:

> *Aby mohly osobní údaje ze základních registrů využívat i samy osoby, o nichž jsou tyto údaje v základních registrech vedeny, případně i další subjekty, pokud s tímto přístupem dané fyzické osoby souhlasí, je jim přístup do základních registrů umožněn, s využitím občanských průkazů umožňujících elektronickou identifikaci. Pokud se fyzická osoba rozhodne, že umožní přístup ke svým údajům např. bance, při návštěvě banky použije svůj občanský průkaz (musí se jednat o průkaz vydaný podle navrhované novely zákona o občanských průkazech), který vloží do čtečky, zadá následně v agendovém informačním systému elektronických občanských průkazů svůj bezpečnostní osobní kód a zobrazí se údaje, které jsou o něm vedeny v základním registru obyvatel. Tyto údaje pak může poskytnout bance. Banka nemůže údaje získat, pokud daná fyzická osoba není fyzicky přítomna. Pokud vlastní fyzická osoba čtečku, může tento způsob identifikace použít pro získání referenčních údajů ze základních registrů s využitím agendového informačního systému elektronických občanských průkazů (webové aplikace) i z domova.*

Z výše uvedeného lze dovodit, že u komunikace občanů s veřejnou správu bude nutné dále rozlišovat, zda jde o anonymní komunikaci, nebo o komunikaci s plně identifikovanou a řádně autentizovanou osobou.

[7] KDle § 19 odst. 8 správního řádu.

V zákoně ale není řešeno, jaký bude statut poskytovaných odpovědí (resp. informací a údajů obsažených v odpovědích). V případě neinteraktivní varianty lze z podstaty věci uvažovat právně platné (závazné) výstupy, díky možnosti opatřit výstup elektronickým podpisem (značkou) či klasickým podpisem a razítkem (u listinných výstupů). U výstupů poskytovaných v rámci interaktivní varianty komunikace (typicky: zobrazovaných na displeji) by ale zajištění právní relevance bylo velmi obtížné.

Z výše uvedeného (i v souladu s odstavcem 4.1.4.) lze také dovodit, že musí existovat možnost výše uvedené interaktivní i neinteraktivní komunikace. Konkrétně, že občané budou mít kde a kam zadávat své dotazy a žádosti a získávat na ně odpovědi. Pro možnost interakce je proto nezbytně nutné, aby alespoň některé agendové informační systémy (AIS) nabízely či alespoň zprostředkovávaly obě varianty komunikace.

Toto ale není řešeno. Stejně jako to, zda k tomuto účelu bude sloužit jeden konkrétní agendový informační systém, nebo více agendových informačních systémů.

### 4.3.1 Univerzální portálová agenda

V některých podkladech k nové koncepci eGovernmentu lze přesto nalézt určitý náznak toho, jak by interaktivní část komunikace s koncovými uživateli (občany) mohla být řešena, byť jen pro veřejné údaje a anonymní přístup.

Jde o zmínku o **univerzální portálové agendě (UPA)**, která by poskytovala veřejné údaje na základě anonymního přístupu. Její existence je explicitně zmiňována například v předkládací zprávě k návrhu zákona č. 111/2009 Sb., v komentáři k § 5 odst. 3:

> *Protože zdaleka ne všechny agendové informační systémy budou moci ihned používat rozhraní ve formě webové služby (některé budou ještě po určitou dobu fungovat off-line), vznikne tzv. univerzální portálová agenda dostupná přes webové grafické uživatelské rozhraní, kterou budou moci k přímému přístupu k údajům v základních registrech orgány veřejné moci používat. Veřejné údaje budou v této univerzální portálové agendě dostupné na základě anonymního přístupu všem občanům.*

Další zmínku o univerzální portálové agendě (UPA) a nutnosti její implementace lze nalézt v dodatečné informaci k zadávací dokumentaci[8] na implementaci informačního systému základních registrů.

[8] Konkrétně dokument 100111_ISZRdodatečné_informace_19.pdf konstatuje, že „Dodavatel navíc musí zajistit výstavbu portálu pro poskytování veřejných dat veřejnosti dálkovým přístupem, jak je požadováno v zadávací dokumentaci.“

# 5 Další potenciál

Výše popsané změny, ať již v oblasti základních registrů, či v oblasti identifikace a autentizace, se svými dopady týkají celé společnosti. Tedy nejen veřejné správy (státní správy a samosprávy), ale i celé občanské veřejnosti i celé privátní sféry, jako klientů eGovernmentu. Bezprostředně se týkají všech vztahů, kde alespoň jedna jednající či komunikující strana je subjektem z veřejné správy.

Přinejmenším nepřímo se ale tyto změny – a nové možnosti, které se jimi otevírají – budou týkat i ostatních vztahů. Tedy i takových, do kterých nemusí být zapojen žádný subjekt z veřejné správy. Zejména vztahů mezi firmami a jejich zákazníky z řad fyzických osob (občanů), ale obecně všech soukromoprávních vztahů, do kterých mohou vstupovat i orgány veřejné moci.

Části z těchto soukromoprávních vztahů se popisované změny budou týkat přímo a povinně. Konkrétně těch, které jsou alespoň z části vymezeny zákonem, jako například vztahy mezi finančními institucemi a jejich klienty. Zde pro banky a další instituce z finančního sektoru vyplývají konkrétní povinnosti vedoucí k povinnosti jednoznačně a spolehlivě identifikovat zákazníka. Proto budou tyto subjekty muset reflektovat i výše popisované změny v této oblasti související se zaváděním nových elektronických průkazů.

Lze ovšem oprávněně předpokládat, že na popisované změny v identifikaci a autentizaci fyzických osob budou chtít reagovat i další subjekty z privátní sféry (firmy), a to i když jim takováto povinnost přímo nevyplývá ze zákona. I ony budou – ve vlastním zájmu – potřebovat vědět, kdo je jejich zákazníkem (tj. identifikovat a autentizovat svého zákazníka). A to co možná nejspolehlivěji.

Pro využití nových možností identifikace a autentizace, které přinesou nové elektronické občanské průkazy, ale budou i privátní subjekty potřebovat vyhodnotit, zda jejich zákazníkem zadaný BOK (bezpečnostní osobní kód) je správný. Vzhledem k umístění BOKu (v základním registru obyvatel) to bude vyžadovat dostupnost služby, která takovéto ověření umožní. Podobně budou potřebovat možnost ověřit vůči registru obyvatel, zda je předložený občanský průkaz stále platný (zda nebyl revokován, tj. zařazen mezi již neplatné) atd.

Stejně tak lze očekávat, že obecně všechny privátní subjekty budou mít zájem využít veškerou „novou kvalitu“, kterou popisované změny přinesou. A to nejen pokud jde o přesnější možnosti identifikace a spolehlivější metody autentizace fyzických osob. Stejně tak to platí i pro přínosy ze zavedení základních registrů a z poskytování referenčních údajů.

Jestliže jedním z hlavních přínosů změn v eGovernmentu má být to, že občan nebude muset oznamovat každou změnu ve svých osobních údajích (například novou adresu svého bydliště) každé jednotlivé agendě – ale že každá agenda se o změně dozví sama skrze poskytnuté referenční údaje – pak lze předpokládat, že o stejnou možnost budou mít velký zájem i privátní subjekty (firmy). Aby i ony mohly pracovat s aktuálními a důvěryhodnými údaji o svých zákaznících a byly informovány i o jejich změnách a nemusely požadovat jejich oznamování a prokazování po samotných zákaznících.

Ostatně, takováto možnost byla veřejnosti opakovaně předkládána při prezentaci důvodů pro zavádění základních registrů jako jeden z hlavním benefitů: že občan bude moci zadat „trvalý příkaz“, na jehož základě budou změny v jeho osobních údajích propagovány těm subjektům (například právě bankám, utilitám apod.), které si občan sám zvolí. Prakticky je tato možnost zakotvena v již zmiňovaném § 58 odst. 9 zákona č. 111/2009 Sb.

# 6 Úskalí

Naplnění výše naznačeného potenciálu (subjekty z privátní sféry) však stojí v cestě určitá úskalí.

Jedno z nich již bylo zmíněno výše, a to absence možnosti zkontrolovat správně zadaný bezpečnostní osobní kód (BOK) při použití elektronického občanského průkazu.

## 6.1 Nerozpracovaná vazba na privátní sféru

Zřejmě nejzávažnějším úskalím je skutečnost, že celá koncepce zavádění základních registrů a elektronických občanských průkazů je relativně podrobně rozpracovaná z pohledu agendových informačních systémů veřejné správy a jejich potřeb. Mnohem méně se ale zabývá (či spíše: vůbec se nezabývá) potřebami provozních informačních systémů provozovaných ve veřejné správě, potřebami komerčních informačních systémů a také potřebami nejširší občanské veřejnosti. A to jak z pohledu jejich napojení na celý systém základních registrů, tak i z pohledu fungování jejich vzájemné vazby: poskytování veřejných údajů, údajů charakteru osobních údajů a dalších služeb.

**Celkově je nutné konstatovat, že celá vazba (eko)systému základních registrů na jeho okolí – mimo veřejnou správu – není řešena prakticky vůbec.**

Konkrétním příkladem může být již výše popisovaný způsob, jakým zákon řeší poskytování služeb základních registrů (včetně poskytování veřejných i osobních údajů) směrem do privátní sféry: na úrovni zákona je jedinou zmínkou možnost poskytování osobních údajů (na žádost subjektu údajů) do datových schránek příjemců. V případě veřejných údajů (ze základního registru osob) pak zmínka o tom, že by měly být dostupné „prostřednictvím k tomu určených agend“.

Detailněji ošetřeno ale není například ani to, jakým konkrétním způsobem budou subjekty údajů udělovat svůj souhlas s poskytnutím jejich osobních údajů třetím stranám, jaké budou při udělování souhlasu požadavky na jejich identifikaci a autentizaci či kde se bude takovýto souhlas zaznamenávat (zda v registru práv a povinností či jinde) atd.

## 6.2 Chybějící možnost mandatorního přístupu

Koncepce základních registrů, tak jak je vymezena (zejména v zákoně č. 111/2009 Sb.), tedy sice počítá s možností poskytování osobních údajů třetím stranám (a tím i privátním subjektům a jejich komerčním IS), a to dokonce i průběžně – ale jen na principu dobrovolnosti, tj. se souhlasem subjektu údajů a s možností jeho pozdějšího odvolání, viz předchozí odstavec.

To je princip, který vychází z obecného předpokladu, že privátní subjekty samy nemají zákonem dané právo na získávání osobních údajů (tj. aniž by k tomu potřebovaly souhlas subjektu údajů). Z tohoto obecného předpokladu ale existují výjimky, například u finančních institucí, kterým zákon ukládá určité povinnosti v oblasti práce s osobními údaji (například finančním institucím v boji proti praní špinavých peněz), a proto jim zákon také dává i právo získávat určité osobní údaje.

Možnost takovéhoto „mandatorního“ přístupu privátních subjektů k osobním údajům – na základě explicitního zmocnění zákonem – ale není v koncepci základních registrů podrobněji ošetřena. Není ale vyloučena, alespoň následující zmínkou (v § 14 odst. 3 zákona č. 111/2009 Sb.):

*Není-li zákonem stanoveno jinak, správce základního registru poskytne údaje ze základního registru pouze osobě, o které jsou tyto údaje vedeny.*

## 6.3 Chybějící možnost interaktivního přístupu a strukturovaných dat

Pokud platí premisa, že se provozní a komerční informační systémy mohou napojovat na některé z agendových informačních systémů, pak v rámci celé koncepce základních registrů není nijak rozpracován princip jejich interakce. A to ani pokud jde o základní režim jejich vzájemné komunikace: zda má jít o interaktivní komunikaci (například skrze rozhraní webových služeb), či zda by se mělo jednat o neinteraktivní (dávkovou) komunikaci, například prostřednictvím datových schránek.

V případě osobních údajů je nepřímo předjímána pouze neinteraktivní komunikace s doručováním do datových schránek (viz již zmiňovaný § 58 odst. 9 zákona č. 111/2009 Sb., který umožňuje zasílání osobních údajů do datových schránek na základě souhlasu subjektu údajů). Ani zde ale není řešeno to, zda vůbec půjde o data strukturovaná, tak aby se dala přímo využít jiným informačním systémem, nebo zda půjde jen o data nestrukturovaná (elektronickou podobou listinného dokumentu), která by před svým dalším využitím musela být dále zpracována (data přepsána či rozpoznána pomocí technik OCR).

Z pohledu fungování služeb v privátní sféře (například v oblasti bankovnictví, ale i jinde) je ale nezbytné, aby komunikace mezi informačními systémy probíhala v reálném čase. Tak aby zákazník nemusel čekat předem neodhadnutelnou dobu (třeba i dlouhé desítky minut) na doručení datové zprávy do datové schránky banky, na jejíž přepážce právě stojí. Nehledě již na zásadní komplikaci, kterou přináší absence možnosti strojového třídění došlých datových zpráv (a je nutné zapojení člověka, které přináší další zpoždění).

Stejně tak je nezbytné, aby v rámci interakce mezi informačními systémy byla předávána data ve strukturované podobě, tak aby byla na straně příjemce přímo využitelná a nemusela být ručně přepisována či rozpoznávána na principu OCR.

## 6.4 Nepřijatelnost modelu PUSH

Již několikrát zmiňovaná možnost poskytování osobních údajů třetím stranám (na základě § 58 odst. 9 zákona č. 111/2009 Sb.) je v zadávací dokumentaci k implementaci ISZR rozvedena tak, že pokud subjekt údajů jednorázově udělí svůj souhlas, jsou třetí straně poskytovány informace o změnách jeho osobních údajů, kdykoli k nim dojde, do její datové schránky.

Konkrétně v dokumentu „Globální architektura základních registrů“ je na tuto možnost pamatováno skrze tzv. push služby:

> *Push služby – Iniciátorem jsou základní registry. Tento typ služeb bude poskytován pouze směrem k datovým schránkám registrovaných subjektů (zasílání informací o změnách, na které má registrovaný subjekt právní nárok).*

Takovýto „PUSH“ princip (tj. poskytování údajů z iniciativy zdroje, a nikoli z iniciativy příjemce) ale nemůže být použit pro referenční údaje. Tedy pro takové údaje, na které by se jejich příjemce mohl chtít spoléhat (a následně jednat podle nich). Důvodem je skutečnost, že u tohoto modelu leží odpovědnost za včasné dodání aktuálních dat (ale i za korektní realizaci a dokončení samotné datové transakce) na zdroji dat, a tedy na státu jako zřizovateli základních registrů a jejich informačního systému (ISZR), resp. na tom orgánu státu, který je jejich provozovatelem.

Pokud by například nedošlo k včasné a korektní propagaci aktuálních dat, příjemce by mohl jednat ještě na základě původních dat, v dobré víře v jejich platnost – a eventuální škodu, která by mu přitom mohla vzniknout, by pak mohl vymáhat na zřizovateli či provozovateli systému základních registrů.

Proto je nutné, aby data poskytovaná na PUSH principu měla pouze nezávazný (informativní) status – a příjemce měl povinnost sám (tj. z vlastní iniciativy) ověřit si jejich aktuálnost a platnost. Současně to ale znamená, že musí mít takovouto možnost (fungující již na principu PULL neboli z iniciativy příjemce).

## 6.5 Příliš slabá dvoufaktorová autentizace

Pokud jde o identifikaci a autentizaci občanů (resp. fyzických osob) vůči agendám veřejné správy a jejich informačním systémům, zde koncepce základních registrů předpokládá již popisované využití dvou prvků:

- 9místného sériového čísla občanského průkazu, jako identifikačního údaje,
- bezpečnostního osobního kódu (BOKu), jako autentizačního údaje.

Zákon č. 111/2009 Sb. požaduje právě takovouto identifikaci fyzických osob vůči všem informačním systémům veřejné správy (viz § 18 odst. 2 zákona) i na kontaktních místech veřejné správy (viz § 58 odst. 5 zákona). O autentizaci pomocí bezpečnostního osobního kódu pak hovoří v souvislosti s registrem obyvatel a s kontaktními místy veřejné správy.

Z toho lze odvodit, že zákon považuje takovouto dvoufaktorovou autentizaci[9] za dostatečnou, alespoň pro oba výše zmiňované účely. Zákon naopak neklade žádné požadavky na správu bezpečnostního osobního kódu (například na jeho pravidelnou změnu).

Z hlediska bezpečnosti lze přinejmenším polemizovat s dostatečností takovéto dvoufaktorové autentizace. Pro některé agendy může být ještě postačující, ale pro jiné již nikoli. Například i u bankovních karet je podobná dvoufaktorová autentizace (na bázi čísla karty a PINu) již považována za nedostatečnou a je povyšována na vícefaktorovou[10] a kombinována s dalšími bezpečnostními prvky (omezením životnosti karty, nastavováním limitů, zamykáním karty apod.).

Pro praktické využití nejen v rámci „citlivějších“ agend veřejné správy – ale třeba i pro identifikaci a autentizaci v on-line prostředí – by bylo více než vhodné místo dvoufaktorové autentizace zavést autentizaci třífaktorovou, zahrnující ještě jednorázové (jednorázově použitelné) autentizační údaje.

Navíc je vhodné znovu připomenout skutečnost popisovanou již v odst. 4.2.3, že pro subjekty privátní sféry chybí dostupnost služby, která by umožňovala ověřit správnost zadaného kódu BOK. Tyto subjekty by tak pro své informační systémy nemohly využít možnosti autentizace, které elektronické občanské průkazy přinesou.

[9] O dvoufaktorovou autentizaci jde díky tomu, že znalost sériového čísla občanského průkazu plní současně i autentizační funkci.

[10] Zavedením údajů Card Verification Value (CVV) či Card Verification Code (CVC).

# 7 Návrhy a doporučení

Autoři tohoto materiálu na základě zhodnocení popisovaných změn předkládají dále uvedené návrhy a doporučení. Jejich cílem je napravit výše popisovaná úskalí a realizovat co možná nejvíce z potenciálu, který již připravené změny v oblasti eGovernmentu otevírají.

Samozřejmě se zachováním všech hlavních koncepčních rysů a principů nové architektury eGovernmentu. Včetně respektování základního principu, že na systém základních registrů (skrze informační systém základních registrů a jeho vnější rozhraní) mohou být napojeny pouze agendové informační systémy (AIS).

## 7.1 Upřesnění základních pojmů a termínů

Prvním návrhem je upřesnění některých základních pojmů. Pokud se v tomto materiálu řeší napojení celého systému základních registrů na jeho vnější okolí, směrem do privátní sféry a ke koncovým uživatelům (občanům), tak zde nelze používat všeobjímající pojem „veřejnost“ a „veřejný přístup“. Místo toho je nutné rozlišovat:

- **anonymní přístup**, při kterém protistrana není identifikována (tj. není známo, o koho jde a komu je informace či služba poskytována);
- **plně autentizovaný přístup**, při kterém je protistrana plně identifikována a úspěšně autentizována (tzn. je přesně známo, komu je informace či služba poskytována).

Dále je třeba rozlišovat způsob komunikace zmiňovaný již v kapitole 4:

- **interaktivní komunikace**, kdy dotazy či požadavky mohou být vznášeny průběžně a průběžně jsou také poskytovány odpovědi, typicky on-line způsobem (způsobem umožňující dálkový přístup);
- **neinteraktivní komunikace**, kdy je jednorázově vznesen dotaz či požadavek a následuje poskytnutí odpovědi – ať již do datové schránky, do emailové schránky, k vyzvednutí na kontaktním místě veřejné správy atd.

V neposlední řadě je vhodné rozlišovat mezi:

- **přístupem** jako možností apriorně neomezeného počtu subjektů (typicky: koncových uživatelů, tj. občanů) komunikovat s jedním subjektem v roli zdroje (informací, údajů) či poskytovatele (služeb);
- **propojením** jako symetrickým vztahem mezi dvěma subjekty, které spolu vzájemně komunikují.

Typickým příkladem přístupu může být využití portálu koncovými uživateli (občany): portál může být i jen jeden, zatímco počet uživatelů nemusí být apriorně omezen (a fakticky bude omezen jen kapacitními možnostmi portálu). Může přitom jít jak o anonymní přístup k portálu (uživatel se nemusí nijak přihlašovat), tak i o plně autentizovaný přístup (uživatel se musí úspěšně přihlásit).

Typickým příkladem propojení může být vazba mezi dvěma informačními systémy. Například mezi agendovými informačním systémem (AIS) a komerčním informačním systémem. Jde tedy o vazbu typu 1:1, která bude vždy interaktivní a nikdy nebude anonymní.

# 7 Návrhy a doporučení

## 7.2 Upřesnění architektury eGovernmentu

Dalším návrhem je upřesnění celkové architektury základních registrů, zejména pokud jde o vazbu na vnější okolí, směrem do privátní sféry a ke koncovým uživatelům (fyzickým osobám) a sjednocení zde používané terminologie.

Pokud jde o terminologii, dnes používané informační systémy je možné rozdělit na:

- **agendové informační systémy (AIS)**: jde o takové IS, které jsou provozovány ve veřejné správě nebo jsou alespoň spravovány subjektem z veřejné správy a mají statut informačních systémů podle zákona č. 365/2000 Sb. Pouze takovéto informační systémy mohou být napojeny na informační systém základních registrů (ISZR) a skrze jeho služby (tzv. eGon služby) komunikovat se základními registry.

- **provozní informační systémy (PIS)**: jde o takové IS, které sice jsou provozovány ve veřejné správě, ale nemají statut informačních systémů dle zákona č. 365/2000 Sb., a tudíž nemohou být napojeny na ISZR, využívat jeho služby a skrze ně komunikovat se základními registry.

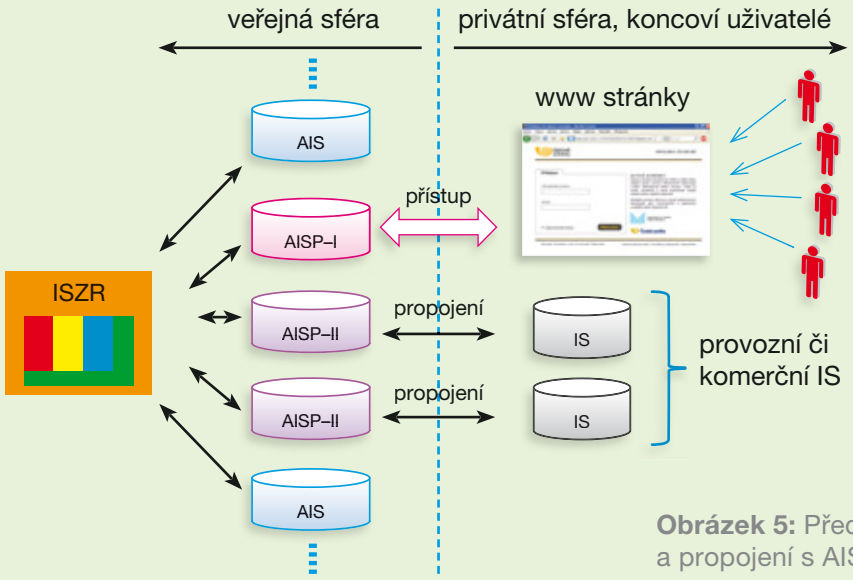
- **komerční informační systémy (KIS)**: jde o takové IS, které jsou provozovány v privátní sféře, nemají statut informačních systémů dle zákona č. 365/2000 Sb., a tudíž nemohou být napojeny na ISZR, využívat jeho služby a skrze ně komunikovat se základními registry.

Dále se navrhuje řádně vymezit nový pojem pro ty agendové informační systémy (AIS), které budou zprostředkovávat vazbu do privátní sféry a ke koncovým uživatelům, ať již na bázi přístupu či na bázi propojení. Jelikož ale nejde o propojení s veřejností, resp. o veřejný přístup, navrhuje se nepoužívat pojem „agendový informační systém (AIS) pro veřejný přístup“.

Místo toho se navrhuje zavést dva příbuzné pojmy:

- **AISP-I** jako zvláštní případ agendového informačního systému (AIS), který slouží potřebám přístupu ve výše uvedeném smyslu. Tedy ke komunikaci s koncovými uživateli (občany) a jejich aplikacemi tak, aby ti (jeho prostřednictvím) mohli využívat nové služby a nové možnosti eGovernmentu.

- **AISP-II** jako zvláštní případ agendového informačního systému (AIS), který slouží potřebám propojení ve výše uvedeném smyslu. Tedy k napojení jednotlivých informačních systémů z privátní sféry (komerčních IS), případně provozních IS, tak, aby i tyto informační systémy mohly využívat nové služby a možnosti eGovernmentu.




**Obrázek 5:** Představa přístupu a propojení s AISP-I a AISP-II

# 7 Návrhy a doporučení

## 7.3 Univerzální portálová agenda jako AISP-I

Dále je nutné přesněji vymezit a ošetřit pojem **univerzální portálová agenda (UPA)**, který je v dostupných materiálech pouze zmíněn, ale také není podrobněji definován. Lze ale dovodit už podle názvu, že půjde o agendu veřejné správy ve smyslu zákona č. 365/2000 Sb. Její informační systém by tudíž byl agendovým informačním systémem (AIS), a měl by tedy možnost přímého napojení na ISZR a využívání jeho služeb.

Dále lze předpokládat, že tato konkrétní agenda bude určena koncovým uživatelům (občanům), bude jim zprostředkovávat nové služby a další funkce eGovernmentu a bude fungovat na bázi přístupu. Její agendový IS tedy bude agendovým informačním systémem typu AISP-I ve smyslu předchozí definice (v části 7.2).

Z pohledu výše uvedených skutečností se jeví jako účelné – a doporučuje se – svěřit univerzální portálové agendě (UPA) všechny funkce a služby, které jsou určeny koncovým uživatelům a fungují na bázi přístupu. A to jak služby dostupné anonymně (na bázi anonymního přístupu, tj. bez přihlašování), tak i adresně (na bázi plně autentizovaného přístupu, tj. po řádném přihlášení).

> **Navrhuje se tedy řešit možnost veřejného přístupu pro koncové uživatele na jednom centrálním místě, skrze jeden AISP-I, pro všechny agendy, které takovýto přístup budou umožňovat – a nikoli na více místech, pro každou jednotlivou agendu samostatně (tj. více AISP-I).**

Univerzální portálová agenda by přitom sloužila jak pro služby, které již dnes vyplývají z platných právních předpisů (jako například udělování a odnímání souhlasu s poskytnutím osobních údajů třetí straně, viz § 58 zákona č. 111/2009 Sb.), tak i pro další funkce a služby, které bude český eGovernment chtít poskytovat přímo širší veřejnosti.

Po praktické stránce lze předpokládat, že univerzální portálová agenda (UPA) bude realizována dnešním Portálem veřejné správy. K jeho využití v roli UPA ale bude zapotřebí přijmout novou právní úpravu, která by dále vymezila a specifikovala jeho novou roli.[11]

Zejména bude nutné ošetřit:

- rozsah poskytovaných služeb, včetně vymezení služeb poskytovaných anonymně (bez přihlášení) a služeb poskytovaných adresně (v rámci plně autentizovaného přístupu),
- způsob uchovávání již udělených souhlasů s poskytováním osobních údajů (zda se budou uchovávat v rámci RPP či jinde).

## 7.4 Další AISP – II

I když bude varianta přístupu svěřena Univerzální portálové agendě (UPA) v roli AISP-I, stále ještě zbývá potřeba umožnit variantu propojení mezi agendovými informačními systémy (AIS) a komerčními IS či provozními IS. A to jak pro potřeby poskytování veřejných informací, tak i informací charakteru osobních údajů, a pro poskytování dalších služeb.

Tuto roli by podle předchozích definic měly plnit agendové informační systémy typu AISP-II. Z hlediska „oprávněnosti“ jejich zřízení je třeba je rozdělit do čtyř skupin, na:

- **AISP-II, které budou poskytovat jiným informačním systémům údaje a služby na základě jejich mandatorního nároku** popisovaného v části 6.2. Jejich zřízení tedy nevyžaduje žádnou změnu současné právní úpravy, protože práva (i povinnosti) příslušných komerčních a provozních IS, které by tyto údaje a služby využívaly, jsou již dnes zakotveny v legislativě.
- **AISP-II, které poskytují jiným IS osobní údaje a další služby na základě souhlasu subjektu údajů**. Pro jejich zřízení také není zapotřebí nová legislativní úprava.

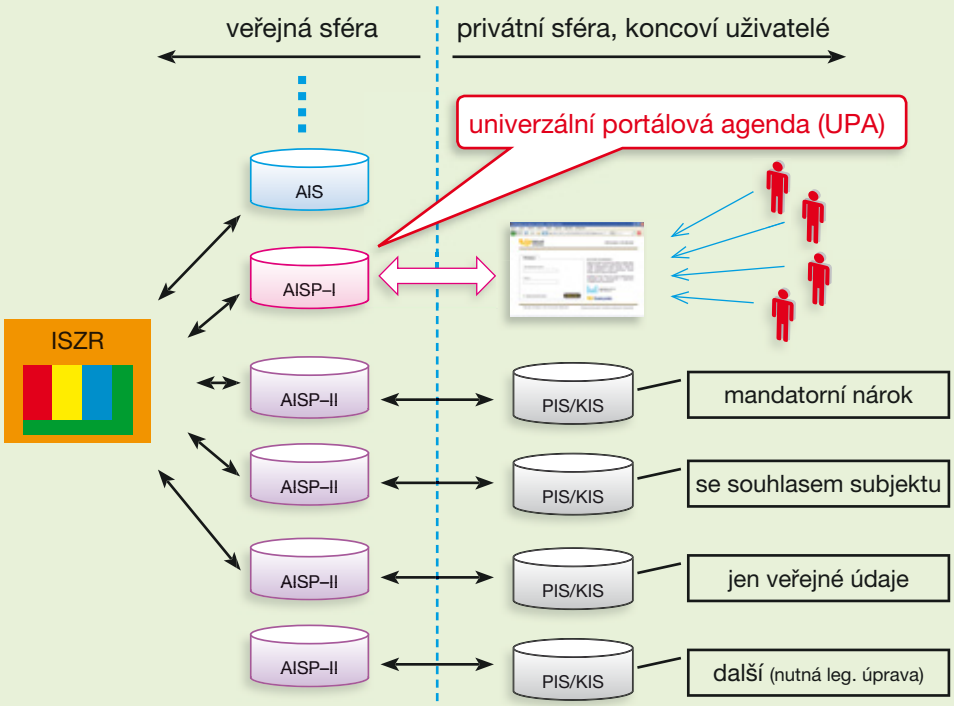
[11] Takováto právní úprava již je zvažována jako „změnový zákon o PVS“, který by novelizoval zákon č. 365/2000 Sb., zejména v § 2/q, 4/1/j, 6f, 6g, 6h, 6i a dalších.

# 7 Návrhy a doporučení

- **AISP-II, které poskytují jiným IS veřejné údaje.** Ani zde, vzhledem k charakteru poskytovaných údajů, není třeba žádných legislativních úprav.

- **AISP-II, které budou poskytovat jiným IS další služby** – například v oblasti identifikace a autentizace, kontroly stavu osobních dokladů a dalších. Zřízení těchto AISP-II již bude vyžadovat přijetí nové legislativní úpravy. Okruh služeb, které by tyto AISP-II měly poskytovat, bude zapotřebí ještě blíže konkretizovat.

Výše uvedenou klasifikaci je vhodné chápat ve smyslu logických rolí. Z pohledu praktické implementace samozřejmě již nemusí jít o samostatné informační systémy. Jeden konkrétní informační systém může plnit více rolí současně.




**Obrázek 6:** Představa dalších AISVP umožňujících propojení

## 7.5 Režim komunikace a poskytování údajů ostatním informačním systémům

Vzhledem ke skutečnostem uvedeným v části 6.4 (o nepřijatelnosti modelu PUSH) je nutné postavit model komunikace mezi informačními systémy pro veřejný přístup (ISVP) a komerčními či provozními IS – pro potřeby poskytování osobních údajů a za předpokladu předchozího explicitního souhlasu subjektu údajů – na jiném principu, a to na principu PULL. A to zejména z pohledu důvěryhodnosti a závaznosti poskytovaných údajů: systém základních registrů (skrze ISZR) sice bude poskytovat informace o změně údajů (či přímo nové hodnoty údajů) na principu PUSH, a tedy z vlastní iniciativy při jakékoli změně – ale tyto informace (údaje) by měly mít pouze informativní statut a neměly by být právně závazné. Místo toho by měla být zavedena povinnost příjemce (komerčního či provozního IS), aby si sám a ze své iniciativy získal či ověřil aktuální a platné údaje a za toto ověření také nesl odpovědnost.

# 7 Návrhy a doporučení

Pro uskutečnění tohoto principu je ale nezbytně nutné, aby příjemce (komerční či provozní IS) vůbec měl možnost z vlastní iniciativy získat aktuální a platné hodnoty těch údajů, k jejichž získávání mu jejich držitel (subjekt údajů) udělil souhlas. To znamená, že způsob komunikace mezi ním a příslušným AISP-II musí podporovat režim PULL (tj. přenos dat z iniciativy příjemce). Poskytování informací na principu PUSH však může mít i přesto svůj smysl, a to pro optimalizaci vzájemné komunikace obou stran.

Komunikace mezi informačními systémy pro veřejný přístup a komerčními či provozními IS navíc musí být založena na předávání strukturovaných dat tak, aby je obě strany dokázaly dále strojově zpracovávat. Práce s nestrukturovanými daty (například s dokumenty v podobě PDF) je z tohoto důvodu nepoužitelná. Viz část 6.3.

Stejně tak je klíčové, aby charakter komunikace mezi informačními systémy pro veřejný přístup a komerčními či provozními IS byl interaktivní a mohl probíhat v reálném čase – a nikoli aby byl neinteraktivní (dávkový, resp. na principu messagingu), jako by tomu bylo například při využití datových schránek. Ty navíc nepodporují možnost automatizovaného třídění došlých zpráv v reálném čase, takže by místo toho vyžadovaly zapojení lidského faktoru pro jejich třídění, a tím zaváděly do celé komunikace (která musí probíhat v reálném čase) zpoždění v předem neodhadnutelných časech (například i desítek minut).

## 7.6 Posílení identifikace a autentizace

Již v kapitole 4 bylo konstatováno, že umístění bezpečnostního osobního kódu (BOKu) do základního registru obyvatel sice umožňuje jeho využití pro potřeby autentizace, ale jen tam, kde je možnost přístupu k obsahu registru obyvatel a kontroly zadaného BOKu s hodnotou uloženou v registru.

Aby takováto možnost autentizace byla využitelná i v privátní sféře, je nutné zřídit službu, která umožní ověření správně zadané hodnoty BOKu. Takováto služba by měla být nabízena na bázi propojení (mezi informačním systémem pro veřejný přístup a komerčním či provozním IS), a to jen těm komerčním či provozním IS, které se úspěšně zaregistrují u provozovatele příslušného agendového IS pro veřejný přístup. Jelikož takováto možnost zatím není v koncepci základních registrů obsažena a nelze ji odvodit z již přijatých zákonů, musela by být podpořena novou právní úpravou.

Další doporučení vychází z konstatování v odstavci 6.5 o tom, že pouze dvoufaktorová autentizace je dnes již příliš slabá. Tedy alespoň pro takové agendy, u kterých by důsledky eventuální chybné identifikace a autentizace byly závažnější. Zde by bylo více než vhodné zavést vícefaktorovou autentizaci. Optimálně prostřednictvím jednorázově použitelného kódu. Technických možností realizace připadá v úvahu více, od autentizačních SMS, přes autentizační kalkulačky v mobilu, až třeba po tištěný seznam jednorázově použitelných kódů.

Z hlediska praktické využitelnosti a celkového posílení bezpečnosti lze jednoznačně doporučit společnou implementaci těchto jednorázových kódů – pro všechny agendy, které budou k identifikaci a autentizaci využívat sériové číslo elektronického občanského průkazu a bezpečnostní osobní kód (BOK). Tedy již na úrovni celého systému základních registrů a takovým způsobem, aby celá třífaktorová autentizace byla využitelná jak ve veřejné sféře, tak i ve sféře privátní.

Stejně tak lze doporučit maximální propagování varianty elektronického občanského průkazu se zabudovaným kontaktním čipem. Díky němu by bylo možné dále zvýšit spolehlivost a bezpečnost identifikace a autentizace použitím nejmodernějších metod kryptografie využívajících techniky elektronického podpisu.

# 7 Návrhy a doporučení

## 7.7 Ověření platnosti občanského průkazu

Jednou z nejpopulárnějších služeb dosavadního eGovernmentu je služba umožňující dálkovým přístupem (on-line) zjistit, zda konkrétní osobní doklad (občanský průkaz, řidičský průkaz) je platný a nebyl například odcizen. Tuto službu využívá řada subjektů z privátní sféry a pomohla jim předejít řadě škod a jiných komplikací.

U nových elektronických občanských průkazů by bylo více než vhodné takovouto službu přinejmenším zachovat, nebo ještě lépe dále rozvinout (a spojit se službou zajišťující ověření správně zadaného kódu BOK). Samotné zjištění toho, zda občanský průkaz je, či není platný, by nadále mělo zůstat dostupné jako anonymní služba. Realizována by mohla být skrze Univerzální portálovou agendu.

O kontrolu platnosti občanského průkazu by ale měla být obohacena i (již neanonymní) služba umožňující ověřit správnost zadaného kódu BOK (popisovaná v předchozí části). Ta by měla vracet, vedle výsledku ověření, i údaj o tom, zda občanský průkaz je nadále platný.

ICT UNIE o.s.
K Červenému dvoru 25a/3269
130 00, Praha 3
tel.: +420 222 582 880
fax: +420 222 585 278
e-mail: ictu@ictu.cz
www.ictu.cz



Na zpracování dokumentu se podíleli členové Klubu ICTU, zastupující jak veřejnou správu, tak komerční firmy – členy ICTU (seřazeno abecedně):

Cvrček Vít, Filip Miroslav, Fridrich Jiří, Holenda Tomáš, Kaucký Richard, Kolář Jindřich, Kolář Pavel, Konečný František, Kučera Aleš, Kučera Roman, Marčan Miloslav, Martaus Jaroslav, Pejčoch Jaroslav, Polák Jiří, Renčín Tomáš, Rutrle Tomáš, Suchánek Vít, Štochel Jiří

Redakci provedl Jiří Peterka.