DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Identifikátory, rodná čísla a jejich vazby

Následující text vychází z článku serveru Lupa.cz jehož autorem je Kamil Zmeškal

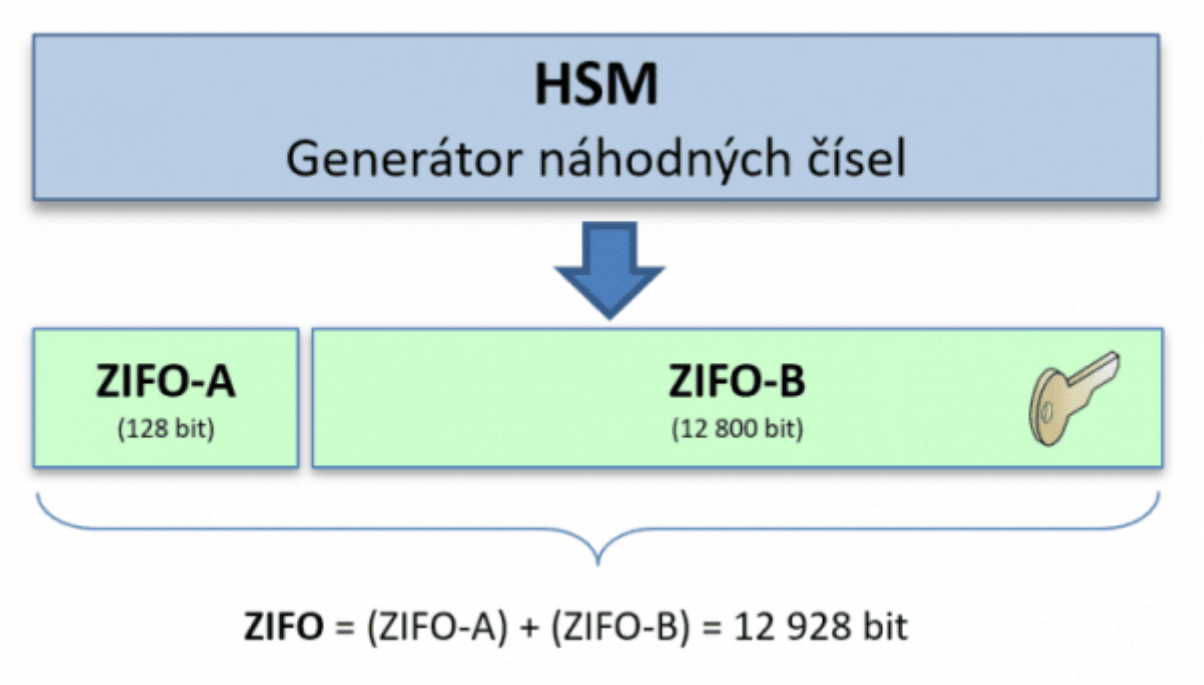
Identifikátory základních registrů – ZIFO a AIFO

Osoby mají v různých agendách rozdílné identifikátory, aby údaje jednotlivých agend nešly bez centrální autority navzájem propojit. Definice těchto identifikátorů jsou zakotveny v § 2 zákona č. 111/2009 Sb. a jedná se o:

- Zdrojový identifikátor fyzické osoby,
- Agendový identifikátor fyzické osoby.

ZIFO – Zdrojový identifikátor fyzické osoby

ZIFO se dá označit za „rodiče“ všech identifikátorů osoby v jednotlivých agendách. Jedná se o bezvýznamový, ze zákona neveřejný identifikátor, tvořený náhodnými čísly. Generuje se v HSM (hardware security module, elektronické zařízení pro provádění kryptografických operací) a skládá se ze dvou částí, ZIFO-A a ZIFO-B. ZIFO-A má délku 128 bitů a ZIFO-B 12 800 bitů, část ZIFO-B je uložena šifrovaně.

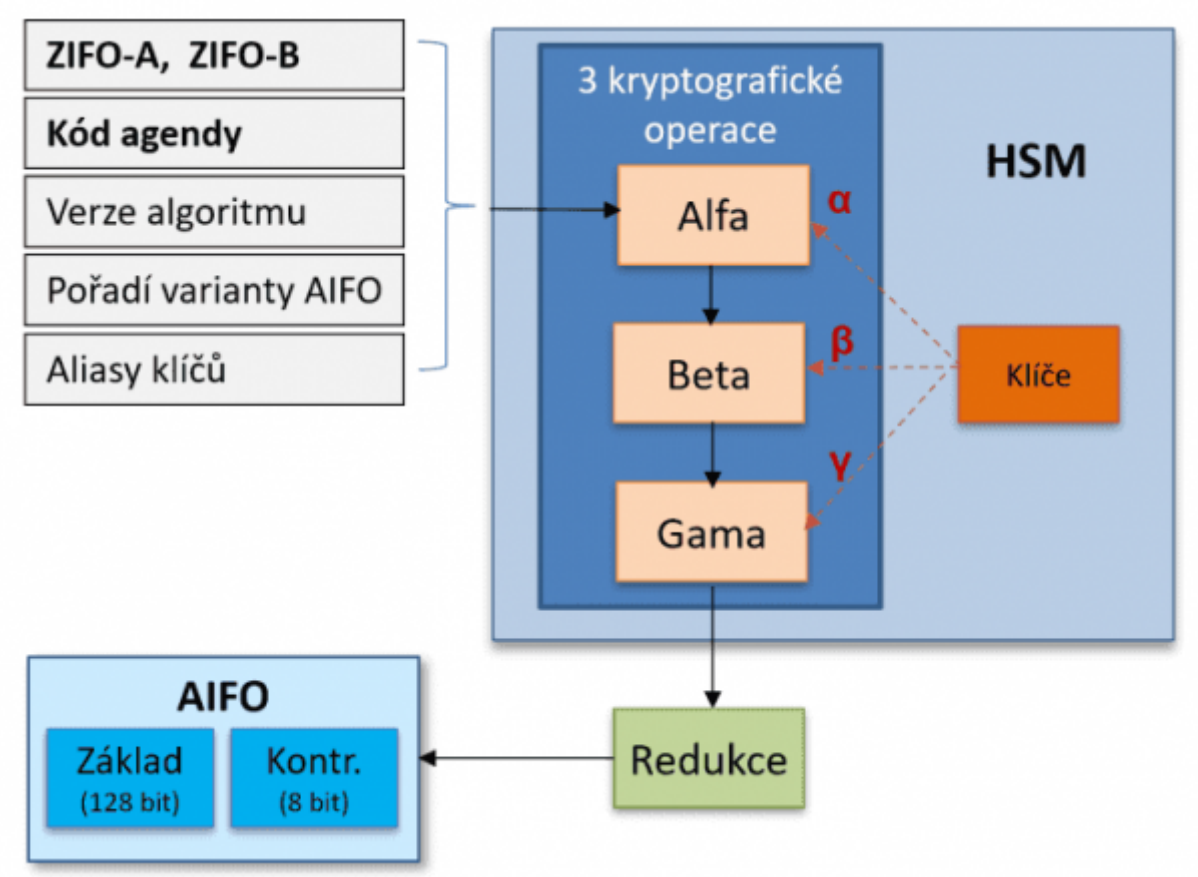


ZIFO se ukládá pouze v informačním systému (IS) ORG, který si popíšeme později. Hlavním účelem ZIFO je jeho využití pro vytváření/odvozování AIFO pro jednotlivé agendy. Se ZIFO se běžné úřady vůbec nesetkají.

AIFO – Agendový identifikátor fyzické osoby

AIFO je stejně jako ZIFO ze zákona neveřejný identifikátor. Vytváří se také v HSM, ale není tvořen náhodnými

čísly, ale jednosměrným odvozením ze ZIFO a dalších údajů, kterými jsou kód agendy, pro kterou se AIFO generuje, pořadí varianty AIFO (čítač verze, např. v případě nutnosti výměny AIFO z důvodu kompromitace), verze algoritmu a odkazy na použité klíče. Odvození probíhá jako posloupnost tří operací, jejichž výsledek se na závěr redukuje na délku 128 bitů + 8 bitů pro kontrolní kód. Ztráta důvěryhodnosti/certifikace jedné z operací tak neznamená nutnost přegenerování všech AIFO.



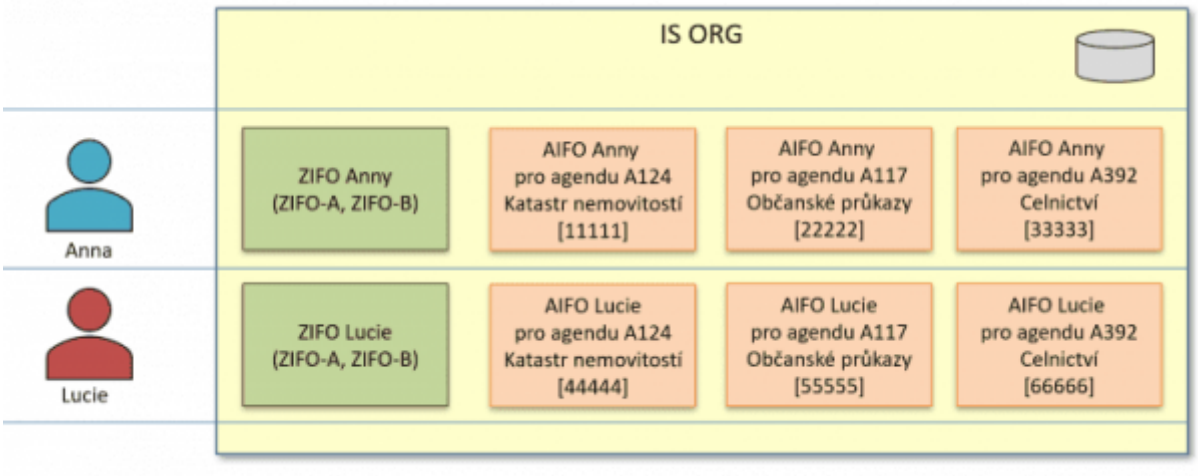
AIFO slouží pro jednoznačnou identifikaci osoby v agendě, pro kterou byl vytvořen, a zabraňuje tak přímému sdružování/propojování dat jednotlivých agend. Formát jeho ukládání v AIS není stanoven, nejčastěji se používá Base64, například AstLse12Q6sduCKMkHZa+g6=.

Protože je AIFO vázáno na agendu, tak v případě, kdy má jeden úřad více agend, se v jejich AISech AIFO stejné osoby liší a ani úřad si nedokáže údaje sám přímo propojit. AIFO ani ZIFO neobsahují žádné osobní údaje a z AIFO nelze zpětně odvodit ZIFO (to je důvod nezvyklé velikosti ZIFO).

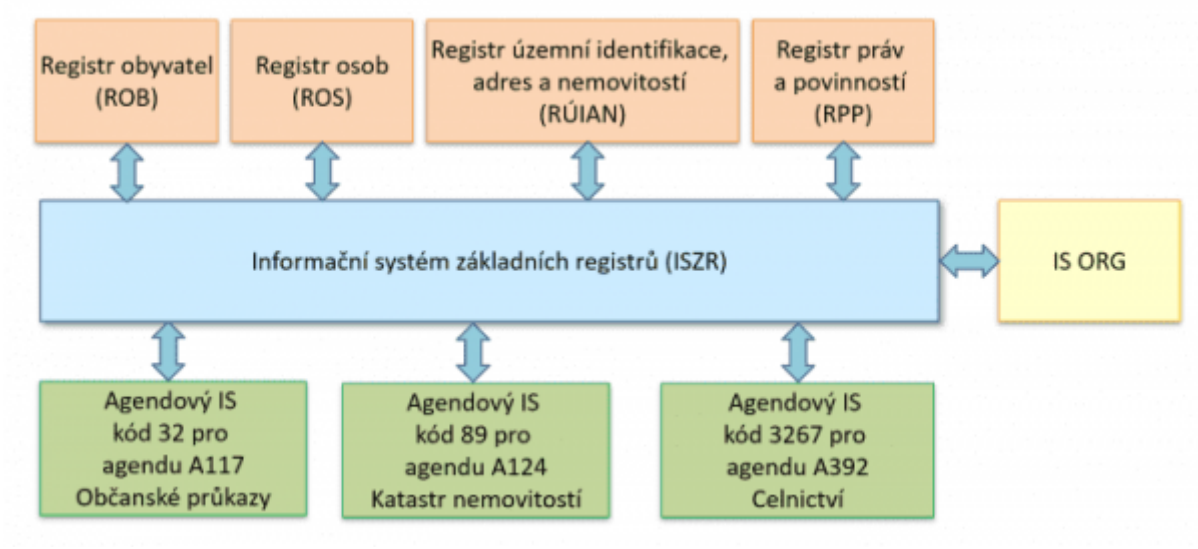
Procesy pamatují i na hraniční situace/chyby, a tak se může stát, že se ZIFO zneplatní a tím se zneplatní i všechny navázané AIFO a musí se vygenerovat nové. Nestává se to často, ale děje se to. Procesy pamatují i na případ kompromitace jednoho AIFO nebo kompromitace celého AIS, kdy se pro danou agendu AIFO přegenerují.

IS ORG

Nyní musíme vyřešit situaci, kdy si jednotlivé agendy potřebují mezi sebou předat informace o stejné osobě. To je řešeno pomocí IS ORG, který slouží ke generování ZIFO a AIFO a je jediným prvkem, který umí převést AIFO jedné agendy na AIFO agendy jiné. V IS ORG nejsou uloženy žádné osobní údaje, obsahuje pouze ZIFO a AIFO.

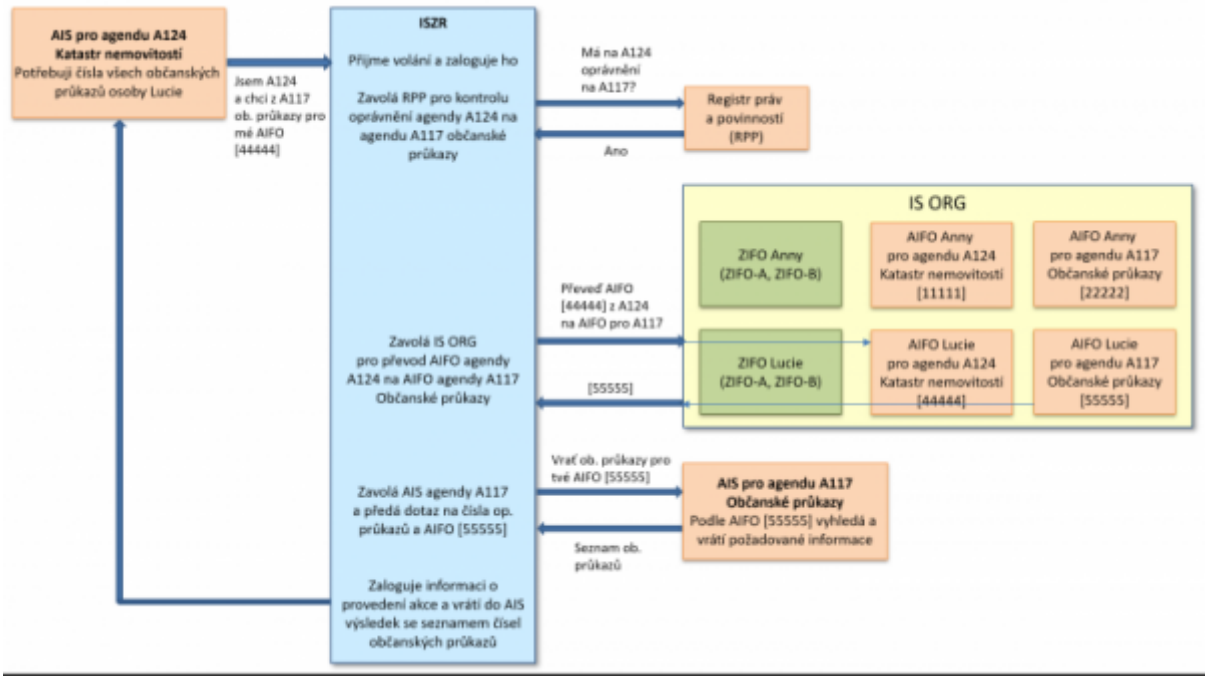


Jednotlivé AIS s IS ORG přímo nekomunikují, komunikace probíhá výhradně pomocí služeb ISZR (Informační systém základních registrů) nebo ISSS (Informační systém sdílené služby).



Pozn.: ISSS není na obrázku pro jednoduchost znázorněn, není pro pochopení funkce IS ORG podstatný.

Pokud bude agenda Katastru nemovitostí potřebovat zjistit k osobě informace z agendy Občanské průkazy, bude komunikace probíhat následovně:



Na obrázku je zmíněn Registr práv a povinností (RPP). Důležitým úkolem toho registru je mimo jiné kontrolovat, zda má agenda oprávnění číst údaje jiné agendy nebo základního registru. Pokud vás zajímá, co se v RPP mimo jiné eviduje, můžete se podívat např. na informace pro agendu A117 Občanské průkazy (XLSX). Seznam agend evidovaných v RPP je dostupný na stránce https:%%//%%rpp-ais.egon.gov.cz/gen/agendy-detail/.

Malá odbočka k NIA a BSI

Vydávání BSI zajišťuje NIA, nikoli IS ORG, jako je to v případě ZIFO/AIFO. Elektronická identifikace je ale agenda jako každá jiná (A3925 Elektronická identifikace a autentizace), což znamená, že NIA po provedení ztotožnění osoby v registru získá pro svou agendu AIFO. Když má následně vydat BSI, tak pokud zatím BSI pro poskytovatele služeb pro dané AIFO nebylo vydáno, vygeneruje nové a uloží si vazbu AIFO-BSI-poskytovatel.

Jedná se o analogii IS ORG se ZIFO, AIFO a agendou, kdy AIFO je v případě NIA v roli ZIFO, BSI je v roli AIFO a poskytovatel je v roli agendy.

Rozhraní stát – soukromoprávní sféra

Dostáváme se k rozhraní mezi úřady a soukromoprávní sférou, kdy úřad potřebuje získané údaje ze soukromoprávní sféry o nějaké osobě přeložit na AIFO své agendy. Je potřebný i opačný postup, aby výstupy úřadů (typicky veřejných rejstříků) obsahovaly jednoznačnou identifikaci osob.

Jednou z možností je na vstupu nebo výstupu použít přirozenou identifikaci pomocí jména, příjmení, adresy a/nebo data narození. Pokud se ztotožnění pomocí těchto údajů jednoznačně povede (tzn. je nalezen pouze jeden záznam), úřad získá AIFO a dále pracuje už s ním. Důvody, proč vyhledávání pomocí zmiňovaných údajů není ideální, jsme si popsali v předchozím článku.

Do úvahy by mohl přijít identifikátor MPSV (IK MPSV), který se používá v oblasti elektronických podpisů. Jeho vložení do certifikátů umožňuje např. I.CA nebo Postsignum a pro úřady byl dlouho jedinou možností, jak si spojit elektronický podpis s konkrétní osobou. Nicméně ministerstvo práce a sociálních věcí (MPSV) nedávno oznámilo záměr ho utlumit, což ho z možností vyřazuje.

Používání rodných čísel se má minimalizovat, takže tudy cesta také nevede a BSI lze používat jen na vstupu. Existují však další dva typy identifikátorů – KIFO a SIFO. Pokud vám tyto názvy nic neříkají, tak věřte, že se s těmito typy identifikátorů běžně setkáváte, jen nevíte, že se tak jmenují.

KIFO – Klientský identifikátor fyzické osoby

KIFO je identifikátor určený pro využití výhradně v rámci jednoho resortu (zdravotnictví, finanční správa atd.). Typickým případem tohoto identifikátoru je Daňové identifikační číslo podnikající osoby (historicky ho sice tvoří rodné číslo, ale už to není nutné a jde změnit). Omezení KIFO na jeden resort je důležitou vlastností, která má zamezit tomu, aby se z něj stal nový plošný identifikátor.

Resort smí KIFO využívat pouze na základě zákona, ve kterém musí být pro jeho vydávání a užívání stanoveny podmínky. Dále musí resort pro své agendy zajistit službu pro převod KIFO na AIFO (a opačně) a platí, že KIFO lze v AISech ukládat. Pro zákonem vyjmenované soukromoprávní použití musí resort zajistit i převod KIFO na identifikační údaje typu jméno, příjmení, datum narození atd.

KIFO je pro jednu osobu trvalý, nemusí existovat mechanismus jeho pravidelné změny. Pro případ jeho zneužití musí být zaveden mechanizmus revokace a vydání nového identifikátoru. Proto musí být i zajištěn překlad historických hodnot identifikátoru na hodnotu aktuální.

KIFO je z principu v rámci resortu veřejný identifikátor a může se uvádět na průkazech/kartičkách, formulářích, listinách, podáních atd. KIFO lze používat i v soukromoprávní sféře (opět pouze v rámci resortu), například soukromými zdravotnickými zařízeními, zařízením sociálních služeb atd.

KIFO tedy slouží ke komunikaci a předávání údajů mezi soukromoprávními informačními systémy a systémy státními **v rámci jednoho resortu**.

SIFO – Stykový identifikátor fyzické osoby

SIFO také slouží pro identifikaci osoby v agendě s následným převodem na AIFO (případně KIFO). Typickými příklady SIFO jsou číslo občanského průkazu nebo číslo cestovního pasu.

SIFO je obvykle vydáván centrálním úřadem (např. u čísla občanského průkazu nebo čísla cestovního pasu je jím Ministerstvo vnitra), který jeho vydávání a možnost změny stanovuje v legislativě a současně zajišťuje službu pro jeho převod na AIFO (a opačně) a službu pro převod historických hodnot na hodnotu aktuální.

Stejně jako KIFO je i SIFO v principu veřejný identifikátor, může se uvádět na formulářích, listinách, výstupech/výpisech a může být též využíván v soukromoprávní sféře. **Proti KIFO je ale zásadní rozdíl v tom, že jeho použití není omezeno na jeden resort či agendu, ale lze ho používat plošně, včetně soukromoprávní sféry.** Kvůli možnosti plošného používání jsou na SIFO aplikována přísnější omezení:

- nesmějí se ukládat do AIS (výjimky mohou být stanoveny zákonem), tzn. je nutné na vstupu SIFO převést na AIFO a dále pracovat s ním,
- má omezenou platnost, např. 10 let, a je zajištěna jeho pravidelná obměna,
- musí existovat možnost jednoduchého přidělení nové hodnoty identifikátoru, např. pro případ kompromitace.

Zmíněné omezení ukládání SIFO do AIS se týká ukládání pro další dohledávání osoby v budoucnu s využitím už uloženého SIFO. Pokud ale agenda v oprávněných případech a při legislativním ošetření pro své další fungování, například vydávání údajů na výpisech, SIFO potřebuje, za tímto účelem ho ukládat může.

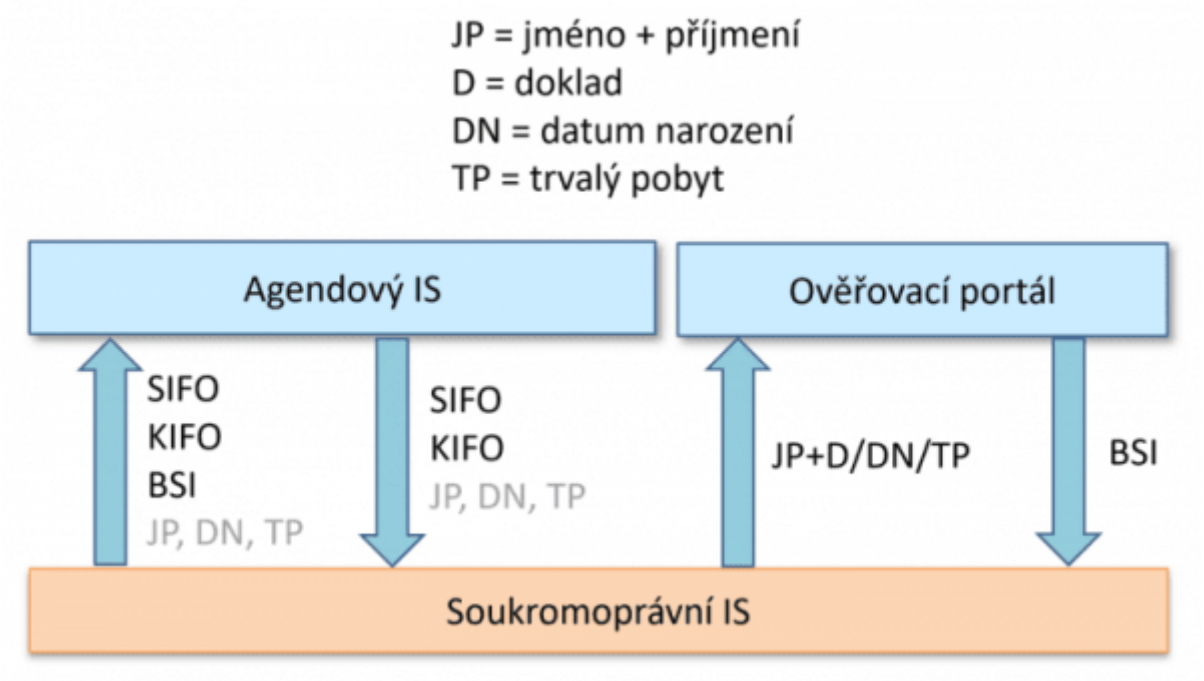
Teoreticky by bylo sice možné SIFO i při vydávání výstupů pokaždé službami základních registrů pomocí AIFO zjistit, ale technicky by to znamenalo obrovskou zátěž jak na AIS, tak na základní registry (např. každý výpis z katastru nemovitostí by znamenal překlad i několika desítek AIFO na SIFO).

Shrnutí identifikátorů

ZIFO a AIFO jsou čistě interní, neveřejné identifikátory, s využitím pouze v rámci AIS. Každá agenda má pro stejnou osobu přiděleno jiné AIFO, takže nelze údaje agend napřímo kombinovat, k tomu je potřeba centrální autorita (IS ORG), která vše loguje a hlídá oprávnění, přičemž v ORG nejsou uloženy žádné osobní údaje.

BSI stojí někde na pomezí. V rámci soukromoprávní sféry se nesmí předávat (výjimka je předání BSI formou vygenerování nových identifikátorů nástupnické organizaci). Stát si může BSI obdržené od soukromoprávní sféry převést na AIFO, ale naopak nesmí BSI uvádět na výstupy atd., což by stejně nemělo z principu žádný smysl. Využití BSI je spíše v soukromoprávní sféře a v rozhraní mezi ní a státem, kde může velmi účelně sloužit jako

identifikátor osoby na vstupu do AIS (např. vyhledání osoby v katastru nemovitostí nebo insolvenčním rejstříku).



Univerzálním identifikátorem je **SIFO**, nejčastěji zastupován číslem občanského průkazu, který může mít každý občan. Jedná se o identifikátor veřejný, jehož hodnota se pravidelně obměňuje a mimořádná výměna je v případě zneužití rychlá. Může sloužit jak na vstupu, tak výstupu státních AIS (např. jako identifikátor ve výpisu z katastru nemovitostí).

KIFO má výhodu, že se na rozdíl od SIFO nemusí v čase pravidelně obměňovat, ale je omezen pouze na jeden typ používání/resort. Využití KIFO je spíše ve scénářích, kdy resort KIFO vydá soukromé sféře a ta pak pomocí něj se státem dále komunikuje, než v jeho používání jako identifikátoru na výstupech veřejných rejstříků. Pro tento účel je vhodnější SIFO, nicméně i použití KIFO vyloučeno není.

Jméno, příjmení, adresa trvalého pobytu a/nebo datum narození mohou sloužit pro identifikaci na vstupu, ale jednoznačnou identifikaci nezaručují (v registru obyvatel je více než 30 tisíc osob, které nejsou podle jména, příjmení a data narození určeny jednoznačně), mohou se měnit a jsou „dlouhé“. Jejich uvádění do výstupů moc vhodné není, adresa a datum narození jsou z mého pohledu osobní údaje citlivější než bezvýznamový KIFO nebo SIFO, a proto by se jejich používání mělo omezovat jen na nejnutnější opodstatněné případy.

Quo vadis, rodná čísla?

Minule jsem v závěru uvedl, že na straně státu i soukromých firem bude ještě potřeba odvést hodně práce, hlavně na rozhraní mezi veřejnou a soukromoprávní sférou. Pokud se podíváme do legislativy, kde všude se rodná čísla vyskytují, narazíme na případy, jako je nutnost rodné číslo uvádět např. při ohlašování živnosti (§ 45 zákona č. 455/1991):

§ 45 Fyzická osoba v ohlášení uvede
*a) jméno a příjmení, popřípadě obchodní firmu, státní občanství, adresu bydliště, **rodné číslo**, bylo-li přiděleno, datum narození, místo narození (obec, okres, stát) a rodné příjmení,*

nebo v žádosti o kvalifikační zkoušku daňového poradce, v návrhu na vklad, ve většině formulářů souvisejících s dávkami a příspěvky, ale i na místech, kde byste to čekali méně, jako např. v žádosti o zpřístupnění svazků STB.

Současně existuje i spousta míst, kde legislativa vyžaduje vést rodná čísla v různých soukromoprávních rejstřících, seznamech, evidencích atd., např. ve mzdových listech (§ 38j zákona č. 586/1992 Sb.):

(2) Mzdový list musí pro účely daně obsahovat
*b) **rodné číslo**, a u daňového nerezidenta datum narození, číslo a typ dokladu prokazujícího jeho totožnost a kód státu, který tento doklad vydal, identifikaci pro daňové účely ve státu daňové rezidence a kód státu, jehož je daňovým rezidentem,*
*d) jméno a **rodné číslo** osoby, na kterou poplatník uplatňuje slevu na dani podle § 35ba a daňové zvýhodnění.*

nebo v evidenci, kterou vede zaměstnavatel pro účely důchodového pojištění, v evidenci rizikových prací a najdou se i méně obvyklá místa, jako např. evidence pěstitelského pálení. Vyskytuje se ve zdravotnictví, finančním sektoru, školství (školství je myslím dobrým příkladem pro implementaci KIFO) a v dalších odvětvích.

Ve většině případů se spolu s rodným číslem nepředávají jiné jednoznačné identifikátory, což může znamenat, že se rodná čísla používají pro identifikaci osob a jejich výměna za jiný identifikátor bude znamenat úpravy dotčených systémů.

Usnesení vlády č. 28 ze dne 13. ledna 2020, k věcnému řešení minimalizace využívání rodného čísla při ověřování totožnosti fyzických osob, stanovilo členům vlády a vedoucím ostatních ústředních správních úřadů zpracovat přehled právních předpisů, na které bude mít dopad zavedení nových elektronických identifikátorů fyzických osob, které nahradí používání rodných čísel. Seznam obsahuje k březnu 2020 celkem 137 položek. Některé jsou od roku 2020 už vyřešeny, některé zatím ne.

Odhady na náklady v soukromé sféře (v médiích hojně citovaná analýza Grant Thornton uvádí přes 40 miliard Kč) si komentovat netroufám, nicméně myslím, že alespoň základní vhled do fungování státních systémů a procesů mám a částka 14 miliard Kč uvedená ve zmiňované analýze na straně státu mi přijde značně nadsazená i přes spoustu míst, která bude ještě třeba vyřešit.

Naopak značně podhodnocená mi přijde částka nákladů státu v pouhých stovkách tisíc Kč, o které hovoří náměstek ministra pro legislativu Ondřej Profant (Události, komentáře; čas 05:20). Za stovky tisíc se možná při běžných cenách 10 000 Kč/MD pořídí analýza nutných úprav jednoho informačního systému a cena za implementaci, testování atd. se může pohybovat o jeden až dva řády výše, přičemž se nejedná pouze o jeden systém. S názorem, že je stát připraven a jediný problém je insolvenční rejstřík, se také z výše uvedených důvodů ztotožnit nemohu.

Útlum rodných čísel započal v letech 2009/2010 a termín 31. prosince 2024 by měl být po 15 letech jeho vyvrcholením a zakončením, nikoli tím, že se jen přestane uvádět rodné číslo v občanských průkazech, jak se nyní snaží vláda prezentovat.

Pokud požadavky na uvádění rodných čísel v legislativě zůstanou, bude stát rodná čísla ve svých rozhraních stále vyžadovat za účelem identifikace osob (s následným překladem na AIFO) a bude vyžadovat i jejich vedení v různých soukromých i státních rejstřících, evidencích apod. a občané je pořád budou muset dokládat jak státu, tak např. zaměstnavatelům (a ti zase státu) nebo jiným soukromým společnostem. Prakticky žádná z problematických věcí vyřešena nebude.

V architektuře eGovermentu je uvedeno: Základním požadavek je, aby občan nemusel rodné číslo nijak dokládat. Pouhým odstraněním rodného čísla z občanského průkazu tohoto cíle nedosáhneme.

Přestat uvádět rodná čísla v občanských průkazech má smysl nejdříve poté, co na tento okamžik bude připraven stát na své straně a přestane je vyžadovat a současně přestane jejich vedení požadovat po soukromoprávním sektoru, jinak by se jednalo spíše komplikaci v běžném životě obyvatel.

Lze cíl 31. prosince 2024 zvládnout? Pokud stát včas zapracuje na legislativě, provede změny ve svých systémech, zpřístupní soukromé sféře s předstihem změny v rozhraní elektronické výměny dat a ideálně po nějakou dobu umožní paralelní provoz původního a nového řešení, zvládnout by se měl. Pokud se termín už počtvrté posune, v dalším volebním období budeme pravděpodobně ve stejné situaci, jako jsme nyní, a bude to

spíše signál „tak to nedělejte, stejně to zase odložíme“