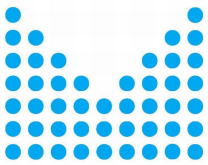
Materiál Ministerstva vnitra



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

~~Title: Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR~~

Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR

Tato kapitola nahlíží na sdílené služby, funkční celky a tematické oblasti veřejné správy ČR tzv. „shora“ a přináší jak definice klíčových pojmů a prvků architektury VS, tak přehled centrálních sdílených služeb eGovernmentu, dostupných pro použití v lokálních architekturách úřadů. Základní pilíře a budoucí směry rozvoje eGovernmentu lze postihnout dále popsanými klíčovými sdílenými službami, funkčními celky či tematickými oblastmi. Jejich prostřednictvím jsou poskytovány centrální sdílené služby eGovernmentu i sdílené agendové služby, které jsou souhrnně zahrnuty do architektonické vize eGovernmentu. V této části popisované sdílené služby, funkční celky a tematické oblasti je povinné zohlednit v informační koncepci úřadu a v architektuře úřadu na základě zákona 365/2000 Sb. a Informační koncepce ČR dle Způsobů využívání sdílených služeb, funkčních celků a tematických oblastí úřady.

Tematické oblasti

- **Agendový model veřejné správy**
- **Identifikace klientů veřejné správy**
- **Propojený datový fond - PPDF**
- **Veřejný datový fond ČR - VDF**
- **Prostorová data**
- **Úplné elektronické podání - ÚEP**
- **Integrace informačních systémů**
- **Portály veřejné správy a soukromoprávních uživatelů údajů**
- **Přístupnost informací**
- **Elektronická fakturace - eFaktura**

Sdílené služby a funkční celky

- **Základní registry a Informační systém sdílené služby - ZR, ISSS**
- **Portál občana a portál veřejné správy - PO, PVS**
- **Národní identitní autorita – NIA**
- **Univerzální kontaktní místo veřejné správy - CzechPOINT**
- **Systém správy dokumentů - eSSL**
- **Systémy a služby spojené s právním řádem a legislativou - eSeL**
- **Elektronické úkony a doručování - ISDS**
- **Jednotný identitní prostor veřejné správy – JIP/KAAS**
- **Jednotné obslužné kanály a uživatelská rozhraní úředníků**
- **Sdílené služby INSPIRE**
- **Sdílené agendové IS v přenesené působnosti**
  - například pro agendy v přenesené působnosti Živnostenský rejstřík, Evidence obyvatel, Evidence řidičů a Registr motorových vozidel, Informační systém technické infrastruktury atd.
- **Sdílené agendové IS pro samostatnou působnost územních samospráv**
- **Sdílené provozní informační systémy**
  - například Informační systém státní služby, Integrovaný informační systém státní pokladny, Národní elektronický nástroj, MS2014+ atd.
- **Sdílené statistické, analytické a výkaznické systémy**
  - například Business Inteligence
- **eGovernment Cloud**
- **Národní datová centra**
- **Komunikační infrastruktura veřejné správy- KIVS/CMS**

Agendový model veřejné správy

Agendový model je základem byznys architektury veřejné správy a základem řízení výkonu digitálních služeb veřejné správy. Všechny agendy veřejné správy jsou zapsány spolu s legislativním ukotvením v Registru práv a povinností včetně definice OVM v agendách působících. V souladu s touto registrací pak OVM musejí vykonávat svoje činnosti a poskytovat svoje služby. Registr práv a povinností dále definuje údaje v agendách vedené a pravidla pro jejich využívání jinými agendami resp. agendovými informačními systémy tyto agendy podporujícími.

Agendový model výkonu veřejné správy

Základ agendového modelu výkonu veřejné správy byl vytvořen při implementaci základních registrů ve veřejné správě. Agendový model definuje působnost a činnosti OVS v jednotlivých agendách – souhrn všech činností ve všech agendách, ve kterých OVS působí, definuje působnost OVS. Orgány veřejné správy mají veškeré své veřejnoprávní činnosti definovány popsáním působnosti v jednotlivých agendách.

Agendy veřejné správy

Agendy veřejné správy jsou nejen právní rámce pro fungování orgánů veřejné moci, ale i základní rámce pro realizaci procesů jako činností a pro evidenci a spravování a využívání údajů v rámci principu propojeného datového fondu.

Existuje následující obecný rozpad toho, co je evidováno k agendě v RPP a co to obecně znamená:

Agenda je soubor činností definovaných zákonem, či zákony (příklad je agenda občanských průkazů, státní sociální podpory, evidence řidičů apod.)

1. Ohlašovatelem je OVM, který je gestorem dané právní úpravy a má tedy povinnost agendu a údaje o ní zapsat do Registru práv a povinností. Součástí ohlášení jsou:
2. Referenční údaje o agendě
    - název agendy a její číselný kód, které jsou součástí číselníku agend,
    - čísla a názvy právních předpisů a označení jejich ustanovení, na jejichž základě orgán veřejné moci vykonává svoji působnost, nebo na jehož základě je soukromoprávní uživatel údajů oprávněn k využívání údajů ze základních registrů nebo agendových informačních systémů,
    - výčet a popis činností, které mají být vykonávány v agendě,
    - výčty činnostních rolí,
    - výčet a popis úkonů orgánů veřejné moci vykonávaných v rámci agendy na žádost subjektu, který není orgánem veřejné moci, identifikátor úkonu, vymezení subjektu, který může podat žádost, a forma úkonu,
    - výčet orgánů veřejné moci a soukromoprávních uživatelů údajů, kteří agendu vykonávají, nebo jejich kategorie,
    - název ohlašovatele agendy a jeho identifikátor orgánu veřejné moci,
    - výčet orgánů veřejné moci, které byly pro výkon agendy zaregistrovány, a jejich identifikátor orgánu veřejné moci,
    - výčet údajů vedených nebo vytvářených podle jiného právního předpisu v rámci agendy; to neplatí pro zpravodajské služby,
    - výčet údajů vedených v základních registrech zpřístupněných prostřednictvím informačního systému základních registrů pro výkon agendy a rozsah oprávnění k přístupu k těmto údajům,
    - výčet údajů vedených v jiných agendových informačních systémech zpřístupněných prostřednictvím referenčního rozhraní pro výkon dané agendy a rozsah oprávnění k přístupu k těmto údajům,
    - číslo a název právního předpisu a označení jeho ustanovení, na jehož základě je orgán veřejné

moci nebo soukromoprávní uživatel údajů oprávněn využívat údaje ze základních registrů nebo z agendových informačních systémů anebo je zapisovat,
    - adresa pracoviště orgánu veřejné moci, které vykonává úkon podle písmene d), vyjádřená referenční vazbou (kódu územního prvku) na referenční údaj v registru územní identifikace, nebo údaj o převedení výkonu úkonu podle písmene d) na jiný orgán veřejné moci.
3. Definice agendových činností a činnostních rolí: V rámci ohlášení ohlašovatel provede dekompozici legislativy a sestaví strom agendových činností (tedy postupu agendy a interakcí zejména z pohledu veřejné správy) a stanoví, jaké činnostní role budou jednotlivé činnosti vykonávat.
4. Působnost v agendě: Je stanovena působnost jednotlivých orgánů veřejné moci (třeba konkrétní ministerstvo, či souhrnné skupiny jako jsou obce, krajské úřady apod.) a u nich jsou stanoveny činnostní role pro výkon jednotlivých činností. Působnost stanovuje/ohlašuje ohlašovatel a daný orgán veřejné moci se přihlašuje k této působnosti a k jejímu rozsahu, vše v rámci agendových informačních systémů v RPP.
5. Adresy pracovišť OVM, kde jsou vykonávány činnosti agendy: Vytváří faktickou mapu výkonu dané agendy v území a každý OVM, který vykonává působnost je povinen ke svým činnostem přiřadit skutečnou adresu výkonu (nikoliv sídlo OVM).
6. Agendové informační systémy: Jsou stanoveny agendové informační systémy, které orgány veřejné moci vykonávající působnost v dané agendě k této působnosti používají, těmto systémům jsou pak stanovena i oprávnění využívat služby základních registrů, a tedy využívat referenční údaje a údaje z jiných agendových informačních systémů prostřednictvím eGon Service Bus / Informačního systému sdílené služby. RPP je metainformačním systémem definujícím datový model veřejné správy, oprávnění a pravidla pro ukládání, využívání a zveřejnování údajů.
7. Výměna (poskytování a využívání údajů) v agendě: Ohlašovatel stanoví, kdo a které údaje smí z agendy využívat anebo je naopak agendě ze svých AIS poskytuje.
8. Údaje v agendě: Jsou ohlášeny všechny propojované a vedené údaje, včetně jejich kontextů a včetně technických údajů o nich.
9. Úkony na žádost: Součástí agendy je i seznam a forma úkonů na žádost a určení toho, kdo smí takovou žádost podat
10. Formuláře: součástí povinností ohlášení agendy je i předání elektronických formulářů či odkazů na ně ministerstvu vnitra.

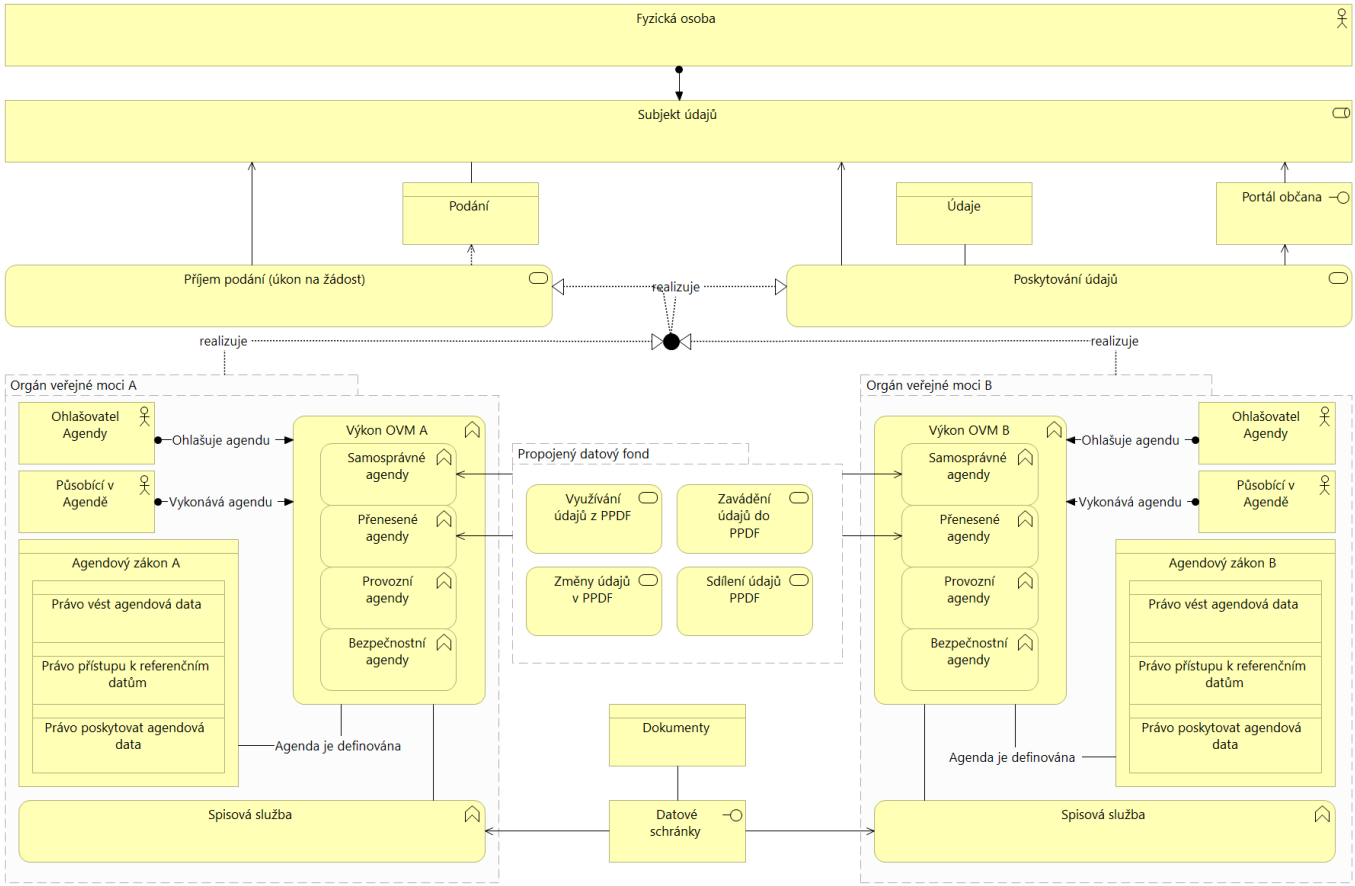
Klíčové role OVS v agendovém modelu

Existují následující klíčové role, o kterých se hovoří i jinde v rámci architektonických dokumentů:

Klíčové role OVS v agendovém modelu veřejné správy	**Role**	**Popis/význam hlavní činnosti**
Ohlašovatel agendy	OVM, který je zodpovědný za legislativní rámec agendy, a tedy určuje i základní parametry jejího výkonu	Je gestorem právních předpisů; koordinuje výkon agendy; metodicky řídí výkon agendy; ohlašuje agendu v RPP a její podrobnosti; stanovuje působnost OVM; poskytuje buď centralizovaný AIS, nebo podmínky a standardy pro decentralizované řešení; ohlašuje a spravuje údaje v RPP, včetně údajů v rejstřících OVM a SPUU; v případě centralizovaného AIS poskytuje údaje přes referenční rozhraní ISVS
Orgán veřejné moci působící v agendě	OVM, který působí v dané agendě. To znamená, že vykonává fakticky nějakou činnost v rámci dané agendy a k tomu využívá buď centrálně poskytnutý AIS, nebo svůj vlastní	Přihlašuje se k působnosti; vykonává jemu svěřené činnosti úředníky v jejich činnostních rolích; zapisuje do RPP údaje o své působnosti; využívá centralizovaný AIS nebo spravuje vlastní; eviduje a spravuje údaje v agendě; vykonává případně funkce editora údajů

Klíčové role OVS v agendovém modelu veřejné správy	Role	Popis/význam hlavní činnosti
Soukromoprávní uživatel údajů	Subjekt, který má na základě zákona oprávnění k přístupu k údajům v základních registrech či AISech a přistupuje k nim prostřednictvím AIS spravovaného k tomu určeným OVM	Využívá údaje podle oprávnění
Správce centralizovaného AIS pro výkon agendy	OVM, který na základě zákona spravuje centralizovaný AIS a poskytuje ho OVM působícím v agendě	Spravuje centralizovaný AIS; zpřístupňuje AIS uživatelům působících OVM; realizuje využívání referenčních údajů ze základních registrů do centralizovaného AIS; poskytuje podporu uživatelům; řeší integrační vazby AIS na další systémy
Správce vlastního AIS, pokud není k dispozici centralizovaný AIS	Jednotlivé OVM, které pro podporu agendy využívají svůj vlastní agendový IS, protože není k dispozici sdílené centralizované řešení	Spravuje svůj vlastní AIS; zapisuje údaje o svém AIS do RPP; řeší vazby na základní registry; řeší vazby na další ISVS; řeší vazby na další svoje informační systémy; spravuje a udržuje datový fond ve svém AISu
Orgán veřejné moci spravující AIS pro přístup soukromoprávních uživatelů	OVM, který na základě zákona vytváří a provozuje AIS, jehož prostřednictvím mohou soukromoprávní uživatelé přistupovat k údajům ze základních registrů či jiných AISů	Spravuje AIS pro SPÚ; zpřístupňuje funkce AISu soukromoprávním uživatelům; realizuje dohled nad oprávněním k využívání údajů; poskytuje soukromoprávním uživatelům údaje; zajišťuje realizaci reklamací údajů od SPÚ k editorům údajů

Pohled na ohlašovatele a vykonavatele agendy



Identifikace klientů veřejné správy

Fyzická identifikace

Fyzickou identifikací je myšlena situace, kdy klient veřejné správy je osobně přítomen v místě, kde je mu služba poskytována nebo je po něm vyžadována součinnost. K fyzickému prokázání totožnosti se používají identifikační doklady, které musí obsahovat:

- Aktuální a platné údaje o jeho držiteli
- Fotografii držitele

Jako identifikační doklad se používá **občanský průkaz** a **cestovní pas**. Identifikačním dokladem **není** řidičský průkaz, protože nesplňuje potřebné parametry při jeho vydávání, ačkoliv obsahuje například fotografii držitele.

Aby mohla fyzická identifikace fungovat jak při aktuální potřebě (člověk se v daný čas dostaví na místo), tak i při historické potřebě (ověření platnosti identifikačního dokladu z historické smlouvy), budou služby eGovernmentu poskytované přes Referenční rozhraní rozšířeny o službu, která na jakékoliv historické číslo a typ identifikačního dokladu vrátí, zda byl v požadované době platný a aktuální údaje držitele tohoto historického identifikačního dokladu.

Fyzická identifikace pro osoby bez identifikačního dokladu

Ačkoliv předcházející text předpokládá identifikaci pouze prostřednictvím identifikačních dokladů, existují situace, kdy osoba nemá možnost se tímto identifikačním dokladem prokázat. Typicky jde o děti pod 15 let či cizince. Základním předpokladem, aby mohla proběhnout identifikace i těchto osob je jejich evidence v informačním systému veřejné správy, napojený na propojený datový fond a následné vydávání potvrzení či úřední/veřejnou listinu, které může zastat roli identifikačního dokladu. Pro osoby do 15 let to může být rodný list vedeny v jednom z editorských agendových informačních systémů nebo povolení o přechodném pobytu pro cizince.

Některé z těchto listin - například povolení k trvalému pobytu, azylový štítek či vízový štítek jsou již dnes vedeny v základním registru obyvatel, avšak jejich použití pro identifikaci není plně dořešeno.

Elektronická identifikace

Elektronickou identifikací je myšlena situace, kdy klient veřejné správy není přítomen v místě poskytování služby. Identifikace tedy probíhá vzdáleně, bez fyzického kontaktu.

Pro jednoznačnou elektronickou identifikaci a autentizaci klientů veřejné správy byl vytvořen technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy tuto činnost vykonávat v souladu s Informační koncepcí ČR a bez nutnosti vytváření vlastních nákladných řešení a zvyšování administrativní zátěže.

Zákon č. 250/2017 Sb., o elektronické identifikaci, zavádí v §2 povinnost provádět prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace. Tento paragraf nabývá účinnosti 1. července 2020. Po tomto datu nebude možné pokračovat v praxi vydávání přístupových údajů klientů veřejné správy mimo systémy kvalifikovaného systému elektronické identifikace, pokud jiný zákon tuto cestu neumožňuje.

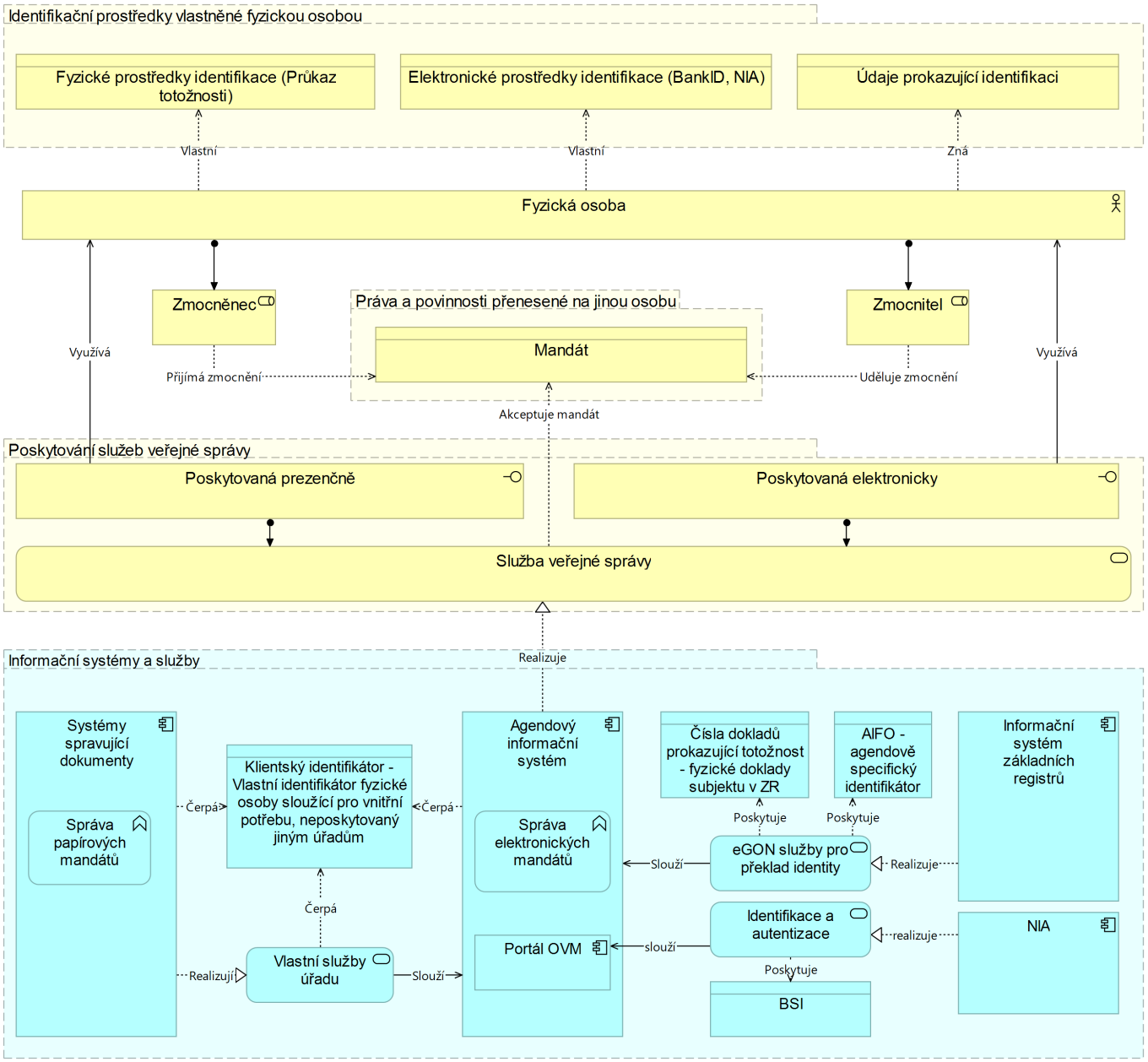
Podporu celého procesu elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace je vytvořena platforma Národní identitní autority (také jako NIA), která vykonává činnosti Národního bodu dle § 20 a následujících a národního uzlu eIDAS pro spolupráci s oznámenými systémy elektronické

identifikace dle nařízení Evropské parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Mandáty, práva a role v elektronické identifikaci pro klienty veřejné správy

Kvalifikovaný poskytovatel elektronických služeb **bude nadále zodpovědný** za řízení oprávnění (autorizaci) fyzické osoby, která prokázala takto svoji totožnost. Nadále tedy musí provádět správu oprávnění na základě údajů o osobě, které získá z Propojeného datového fondu a vlastních údajů vedených v agendě.

Pohled na identifikaci a identifikátory klientů VS



Propojený datový fond

Popis propojeného datového fondu

Zde uvedené informace k propojenému datovému fondu (PPDF) a všech jeho dílčích oblastí (ISZR, eGSB/ISSS, atd.) vycházejí z

Globální architektury propojeného datového fondu

, který je přílohou samotného NAP v rozšiřující znalostní bázi.

Propojený datový fond (také jako PPDF) je tematická oblast tvořená především Informačním systémem základních registrů a eGON Service Bus / Informačním systémem sdílené služby, jejichž služby jsou publikovány prostřednictvím Centrálního místa služeb. PPDF a jeho systémy/služby jsou fyzickou reprezentací referenčního rozhraní veřejné správy. Základní funkcí PPDF je realizace zásad „Once-only“ a „Obíhají data, nikoli lidé“ do běžné praxe veřejné správy ČR. PPDF je primárním zdrojem platných a právně závazných údajů pro subjekty práva i pro všechny OVM a SPUÚ při výkonu jejich působnosti. Tak povede PPDF k náhradě manuálních interakcí mezi úřady pomocí automatizované výměny údajů mezi jednotlivými Agendovými informačními systémy.

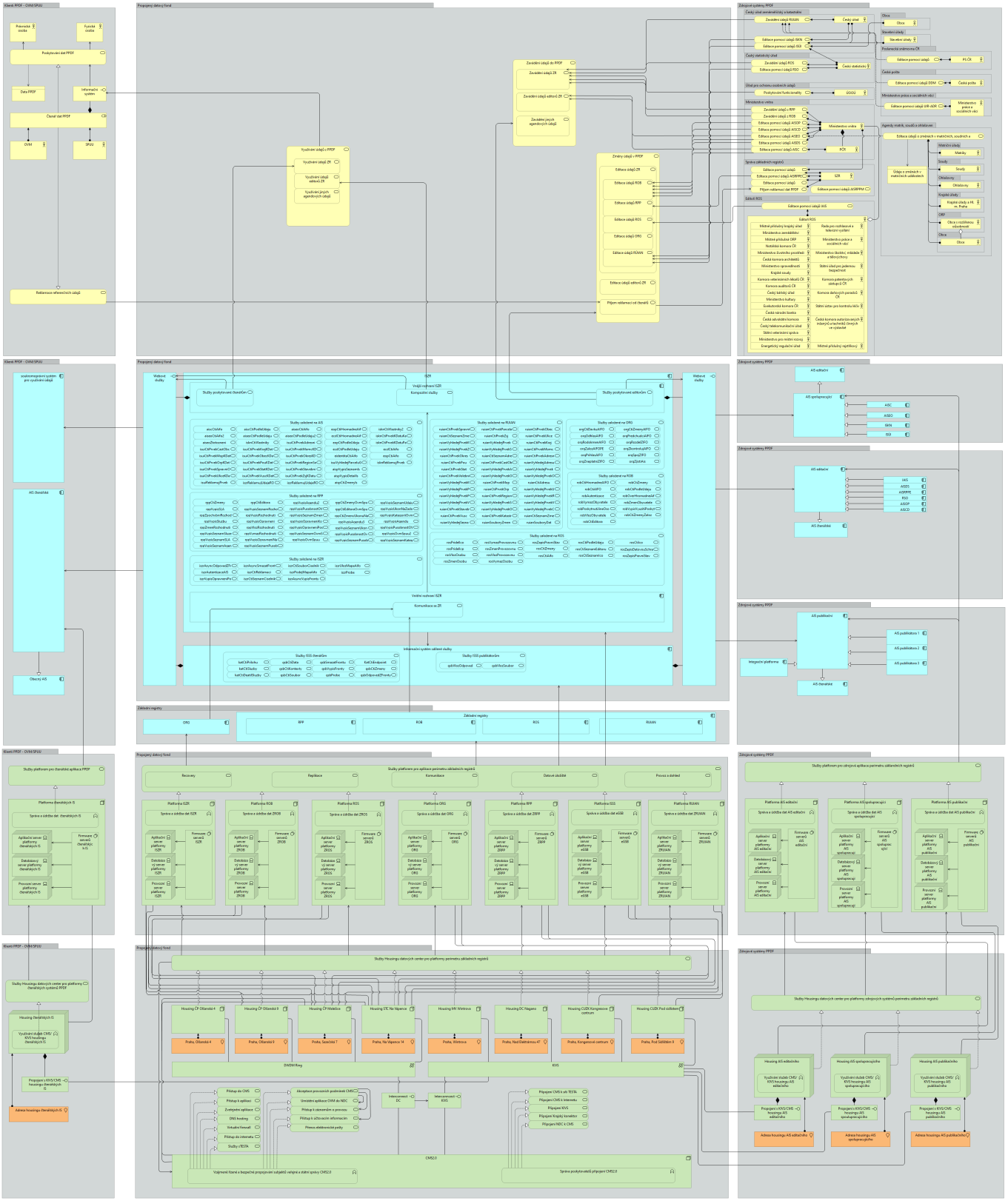
Agendový informační systém je termín ze zákona 111/2009 Sb., a označuje takové Informační systémy veřejné správy, které slouží k výkonu agendy. Texty k PPDF tedy obsahují jak pojmy Informační systém veřejné správy, tak Agendový informační systém. Obsahuje i pojem Soukromoprávní systém pro využívání údajů, který je roven Agendovému informačnímu systému, jen má jiného správce než klasický orgán veřejné moci.

Propojení mezi Agendovými informačními systémy a základními registry zajišťuje Informační systém základních registrů, propojení mezi agendovými informačními systémy navzájem zajišťuje eGON Service Bus / Informační systém sdílené služby. Veškeré vazby činěné v rámci PPDF jsou vždy propojeny se základními registry pomocí referenčních vazeb na referenční údaje o subjektech práva (fyzických osobách, právnických osobách a OVM) a referenční údaje o objektech práva (územní prvky a práva a povinnosti). Pro referenční vazby údajů o fyzických osobách se využívá Agendový identifikátor Fyzické osoby (AIFO), pro referenční vazby právnických osob Identifikační číslo osoby (IČO), pro referenční vazby územních prvků jejich příslušné identifikátory přidělené RUIAN. Kromě rozvoje a podpory navázaných principů správy datového kmene a pseudonymizace, je hlavním cílem PPDF rozvoj o další agendové zdroje neveřejných údajů z klíčových oblastí výkonu veřejné správy (doprava, zdravotnictví, sociální služby…) jasně definovaným garantem a editorem. Mezi členskými státy EU se klade větší důraz na interoperabilitu, PPDF bude připraven poskytovat i služby pro přeshraniční výměnu dat. V reáliích roku 2020 je ke službám PPDF připojeno cca 3 500 informačních systémů z celkového počtu cca 7 000. Základním cílem PPDF je kromě připojení všech informačních systémů veřejné správy také zajištění, aby připojení pro relevantní ISVS nebylo jen čtenářského typu (čerpání údajů), ale i publikátorského typu (poskytují své údaje). Teprve až budou všechny relevantní informační systémy veřejné správy služby PPDF čerpat a poskytovat, může se hovořit o propojeném datovém fondu.

Základními službami PPDF pro oprávněné čtenáře PPDF jsou:

- Ztotožnění (přidělení identifikátoru) subjektu/objektu práva vedeném v AIS a tím i podpora pseudonymizace
- Výdej údajů o subjektu/objektu práva dle požadovaného kontextu v rozsahu oprávnění vedených v RPP pro příslušnou agendu podporovanou AIS
- Notifikace o změnách referenčních a agendových údajů pro údaje v AIS vedené
- Podpora reklamace chybných údajů

Pohled na propojený datový fond



Pravidla propojeného datového fondu

Údaje, dokumenty, výstupy a výpisy

Těžištěm pro správné využívání a pochopení smyslu propojeného datového fondu je porozumění rozdílu mezi **Poskytováním/Využíváním údajů, Poskytováním/Využíváním dokumentů, Výstupům z informačního systému a Výpisem z informačního systému**.

Na business vrstvě orgán veřejné moci, který provádí výkon veřejné správy, působí v agendě, kterou má řádně ohlášenou v RPP, má povinnost využívat pro tyto účely aktuální státem garantovaná data ze ZR a dále publikovat a čerpat agendové údaje přes eGon Service Bus / Informační systém sdílené služby. Soukromoprávní uživatel údajů (také jako SPUU) může také za dodržení zákonného zmocnění pro výkon veřejné správy a působení v určité agendě ohlášené OVM, čerpat údaje ze základních registrů či jiných AIS. Může tak činit přímo prostřednictvím svého soukromoprávního systému pro využívání údajů (také jako SSVU) za splnění zákonných povinností, nebo přes agendový informační systém orgánu veřejné moci, který slouží pro výkon stejné agendy a jsou zajištěny všechny zákonné požadavky. Poslední možností pro SPUU je využívat formuláře Czech POINT. V zákoně č. 111/2009 Sb. - Zákon o základních registrech, je zakotveno globální zmocnění na čerpání údajů OVM ze ZR, přičemž RPP slouží jako zdroj informací pro informační systém ZR při řízení přístupu uživatelů k údajům v jednotlivých registrech a agendových informačních systémech. To znamená, že kdykoliv se daný subjekt pokusí získat určitý údaj, nebo ho dokonce změnit (editovat), systém posuzuje, zda subjektu bude dovolené na základě zákonného zmocnění pracovat s údaji poskytované veřejnou správou. V RPP jakožto metainformačním systému výkonu veřejné správy jsou uvedeny oprávnění v rámci agend pro čerpání údajů ze ZR, ale také veškeré údaje, které stání správa a samospráva publikuje za pomocí eGon Service Bus / Informační systém sdílené služby napříč veřejnou správou. Důležitým faktorem na business vrstvě v rámci čerpání údajů ze ZR a také publikování a čerpání údajů v rámci jednotlivých AIS OVM je mít řádně hlášenou agendu v RPP, což je nezbytnou podmínkou.

Seznam agend vedených v RPP je k dispozici na stránkách: https://rpp-ais.egon.gov.cz/gen/agendy-detail/

Na aplikační vrstvě, prostřednictvím webových služeb jednotlivých referenčních rozhraní, ke kterým patří informační systém správy základních registrů, eGon Service Bus / Informační systém sdílené služby, služby Czech POINT a formulářového agendového informačního systému FAIS, má povinnost instituce čerpat referenční údaje ze ZR svými AIS a dále poskytovat a využívat údaje přes IeGon Service Bus / Informační systém sdílené služby napříč veřejnou správou. Dále je možné čerpat referenční údaje ze ZR i přes datové schránky.

Jedním z pravidel získávání referenčních údajů webovými službami je nejdříve ztotožnit svůj datový kmen vůči ZR a následně se přihlásit pro příjem notifikací o změnách. Další možností, ovšem v krajních případech, pokud datový kmen instituce není příliš rozsáhlý, je možné provádět pravidelnou aktualizaci údajů celého datového kmene pro ztotožnění subjektu práva práva při výkonu veřejné správy.

Dalším pravidlem pro nakládání s osobními údaji je pseudonymizace údajů, což znamená uložení dat technikou oddělení agendových a identifikačních údajů a jejich propojení pomocí agendového identifikátoru fyzických osob (také jako AIFO), aby byly naplněny podmínky bezpečnosti a jednotlivých zákonů a nařízení, které z těchto okolností plynou. Získané AIFO nesmí za žádných okolností opustit AIS, které ho ze služeb ISZR získalo a při jeho předávání (za účelem předávání informací o fyzické osobě) se musí vždy použít služeb ISZR. Více informací o způsobu využití AIFO v rámci pseudonymizace je uvedeno zde.

- Informace ohledně ZR jsou k dispozici na stránkách: http://www.szrcr.cz/vyvojari
- Informace, jakým způsobem připojit svůj AIS nebo komunikační sběrnici do ISZR jsou k dispozici na stránkách: http://www.szrcr.cz/file/170/
- Informace, jakým způsobem využívat notifikace ze ZR je k dispozici na stránkách: http://www.szrcr.cz/spravny-postup-prace-s-notifikacemi-a-udrzovani-datoveho
- Informace k popisu služeb ZR: http://www.szrcr.cz/file/175/display/
- Podrobný popis služeb ZR: http://www.szrcr.cz/vyvojari/podrobny-popis-egon-sluzeb-zakladnich-registru

Z pohledu technologické vrstvy, je čistě na jednotlivé instituci, jakou si zvolí platformu v rámci vnitřního fungování úřadu a připojení se pro využívání služeb propojeného datového fondu, přičemž přistupovat do ZR je možné přes ISZR přímo AISem nebo komunikační sběrnicí.

Na komunikační vrstvě je povinnost instituce při výkonu veřejné správy využívat CMS. CMS je systém, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů veřejné správy ke službám (aplikacím), které poskytují informační systémy jiných subjektů veřejné správy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu. CMS tak můžeme nazvat privátní sítí pro

výkon veřejné správy na území státu. CMS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (také jako OVS) pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do Internetu.

Poskytování / Využívání dokumentů

Dokumenty se přenáší skrze referenční rozhraní ve vazbě na subjekt či objekt práva prostřednictvím eGON Service Bus / Informačního systému sdílené služby, nebo také prostřednictvím informačního systému datových schránek. Dokumenty se tvoří výstupem z informačního systému veřejné správy dle zákona č.365/2000 Sb.

Výpisy z informačního systému veřejné správy

Výpis z informačního systému veřejné správy je dokument, který se vytváří se z veřejných i neveřejných evidencí. Výpis může mít podobu částečného nebo plného výpisu ze všech údajů, které se v informačním systému veřejné správy vedou.

- Výpis z veřejné evidence: Výpis není určen pro konkrétní osobu a všechny obsažené informace jsou veřejné.
- Výpis z neveřejné evidence: Výpis je určen pro konkrétní osobu, která je subjektem práva nebo jinou oprávněnou osobu a obsahuje i neveřejné údaje.

Výpisy se tvoří dle zákona č. 365/2000 Sb.

Výstupy z informačního systému veřejné správy

Výstup z informačního systému veřejné správy je elektronický dokument, který je výpisem z informačního systému veřejné správy, ale je zároveň zabezpečen způsobem zajišťující integritu dat. Tedy je to takový výpis z informačního systému veřejné správy, který je vydávajícím informačním systémem veřejné správy elektronicky opečetěn/podepsán a oražen časovým razítkem.

Existuje i speciální varianta výstupu z informačního systému veřejné správy, tzv. **ověřený výstup**, který vznikne úplným převodem výstupu z informačního systému veřejné správy z elektronické do listinné podoby a obsahuje náležitosti dle zákona č.365/2000 Sb.. Ověřený výstup je tedy vždy v listinné podobě.

Veřejná listina

Veřejná listina je dle občanského zákoníku listina vydaná orgánem veřejné moci v mezích jeho pravomoci nebo listina, kterou za veřejnou listinu prohlásí zákon. Je-li nějaká skutečnost potvrzena ve veřejné listině, zakládá to vůči každému plný důkaz o původu listiny od orgánu nebo osoby, které ji zřídily, o době pořízení listiny, jakož i o skutečnosti, o níž původce veřejné listiny potvrdil, že se za jeho přítomnosti udála nebo byla provedena, dokud není prokázán opak. Zachycuje-li veřejná listina projev vůle osoby při právním jednání a je-li jednajícím podepsána, zakládá to vůči každému plný důkaz o takovém projevu vůle. To platí i v případě, že byl podpis jednajícího nahrazen způsobem, který stanoví zákon.

Veřejnou listinou jsou všechny:

- **listinné** výpisy z informačního systému veřejné správy,
- výstupy z informačního systému veřejné správy,
- ověřené výstupy z informačního systému veřejné správy.

Veřejný datový fond

Popis veřejného datového fondu

Veřejný datový fond (VDF) je definován v Informační koncepci ČR (IKČR) jako dílčí cíl 5.10 a je součástí budovaného eGovernmentu VS ČR.

“Veřejný datový fond tvořený publikovanými veřejnými údaji veřejné správy je základní metodou pro sdílení veřejných informací mezi veřejnoprávními subjekty navzájem i pro sdílení veřejných údajů mezi veřejnoprávní a soukromoprávní sférou v ČR. Veřejný datový fond se od pouhé publikace automatizovaně čitelných otevřených dat posune též k publikaci právně závazných, platných a pravidelně aktualizovaných datových sad s jasně definovanou zodpovědností OVS za takové sady.”

Legislativní ukotvení veřejného datového fondu

VDF není v legislativě jako pojem explicitně zmíněn. Legislativa pouze zavádí pojmy důležité v rámci VDF a pravidla evidence a sdílení údajů ve VDF. VDF je ukotven v zákoně č. 111/2009 Sb., o základních registrech (ZoZR), zákoně č. 106/1999 Sb., o svobodném přístupu k informacím (InfoZ) a zákoně č. 365/2000 Sb. o informačních systémech veřejné správy (ZoISVS).

Základním pojmem je údaj vedený nebo vytvářený v rámci agendy. Podle § 51 odst. 6, písm. k) ZoZR je pro každý údaj vedený nebo vytvářený v rámci agendy v RPP vedena jeho přístupnost veřejnosti a v případě, že údaj není přístupný veřejnosti, číslo a název právního předpisu a označení jeho ustanovení (v budoucnu jako odkaz do eSeL), na jehož základě není údaj přístupný veřejnosti (resp. seznam takových referencí na ustanovení právních předpisů). Pokud tedy neexistují legislativní překážky ke zveřejnění údaje, jedná se o údaj přístupný veřejnosti (dále jen veřejný údaj). Veřejný údaj je speciálním případem údaje.

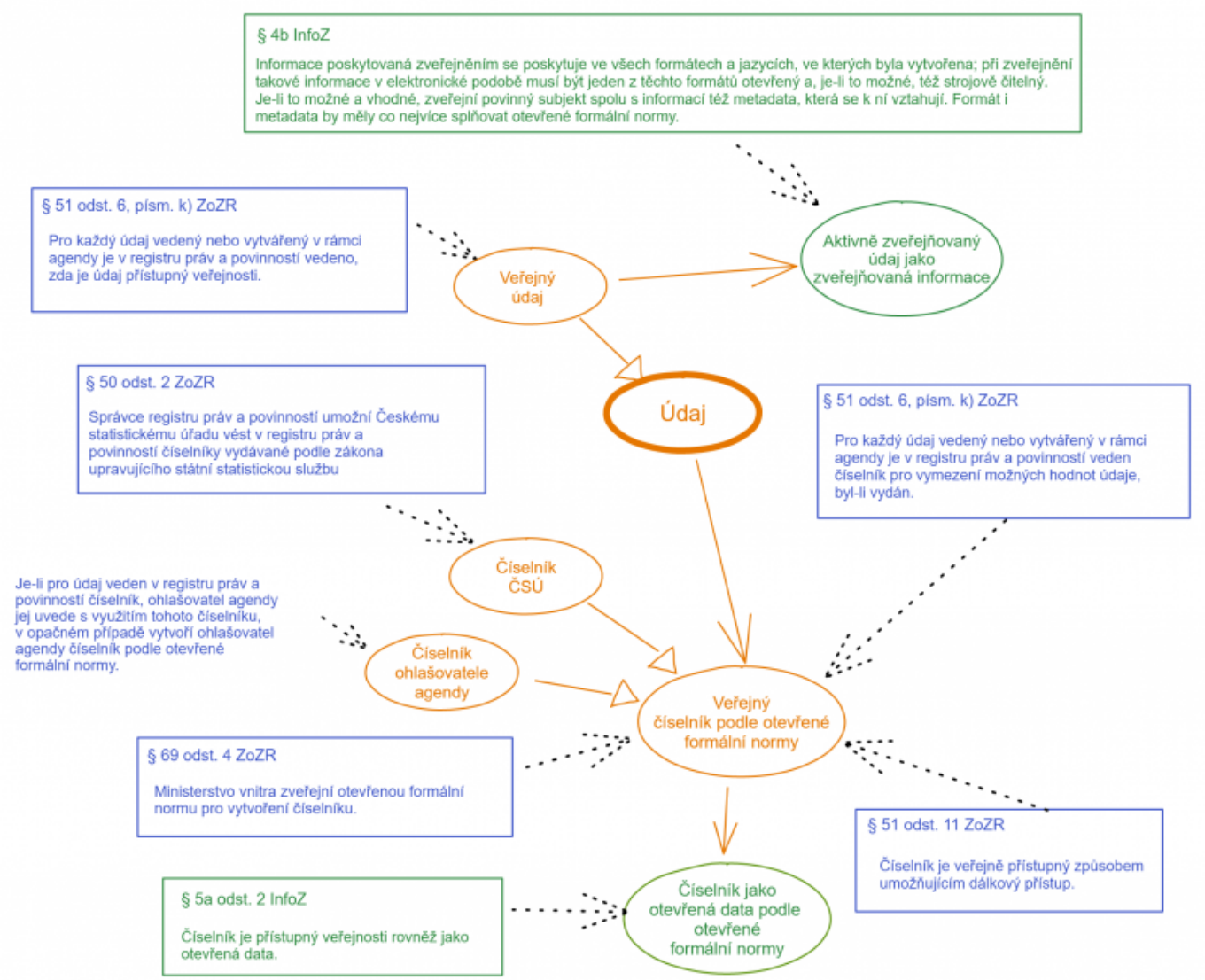
Způsob poskytnutí údaje zveřejněním upravuje § 4b InfoZ, dle kterého se veřejný údaj poskytuje jako informace ve všech formátech a jazycích, ve kterých byla informace vytvořena; při zveřejnění takové informace v elektronické podobě musí být jeden z těchto formátů otevřený a, je-li to možné, též strojově čitelný. Je-li to možné a vhodné, zveřejní povinný subjekt spolu s informací též metadata, která se k ní vztahují. Formát i metadata by měly co nejvíce splňovat otevřené formální normy.

V případě údajů spravovaných v AIS se z principu jedná o informace vedené ve strukturované podobě ve vnitřních databázích informačních systémů, které jsou spravovány databázovými systémy. Databázový systém má rozhraní pro získání obsahu údajů, prostřednictvím kterého lze obsah údajů ve strukturované podobě získat. Jejich zveřejnění v otevřeném a strojově čitelném formátu je tedy technicky možné vždy. Zároveň je možné zveřejnit spolu s informací i metadata a při volbě formátu zveřejněné informace a reprezentaci metadat plně postupovat podle otevřených formálních norem. Z důvodu dosažení interoperability mezi informačními systémy veřejné správy a také z důvodu dosažení přeshraniční interoperability je nutné při zveřejňování údajů postupovat podle otevřených formálních norem vydávaných MV ČR a při zveřejňování metadat je nutné postupovat dle otevřené formální normy rozhraní katalogů otevřených dat. Jinými slovy, veřejné údaje jsou zveřejňovány v otevřeném a strojově čitelném formátu dle otevřených formálních norem vydávaných MV ČR a jsou katalogizovány v Národním katalogu otevřených dat (NKOD).

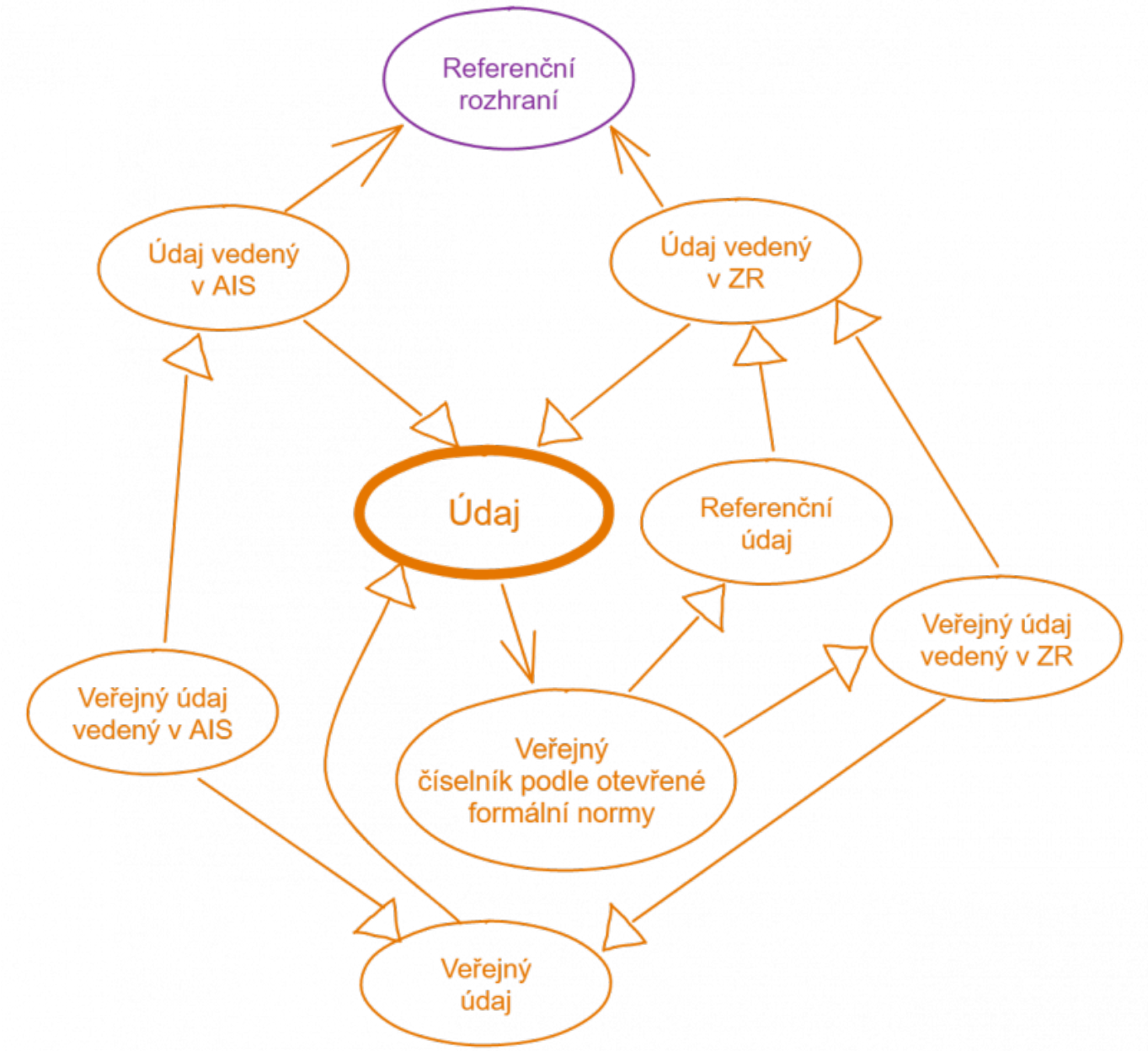
Dále je dle § 51 odst. 6, písm. k) ZoZR pro údaj vedený nebo vytvářený v rámci agendy, jehož možné hodnoty jsou vymezeny číselníkem, tento číselník veden v RPP. Podle § 69 odst. 4 ZoZR MV ČR zveřejní otevřenou formální normu pro vytvoření číselníku a podle § 51 odst. 11 ZoZR jsou tyto číselníky veřejně přístupné způsobem umožňujícím dálkový přístup. Číselník pro vymezení možných hodnot údajů pro účely tohoto dokumentu nazýváme veřejný číselník. Ze spojení s § 5a odst. 2 InfoZ pak vyplývá, že veřejný číselník musí být zveřejněn jako otevřená data podle otevřené formální normy vyplývající z § 69 odst. 4 ZoZR.

Z pohledu ZoZR odlišujeme dva možné typy veřejných číselníků. Dle § 50 odst. 2 ZoZR to jsou číselníky ČSÚ. Dle § 54 odst. 1, písm. a) ZoZR to jsou číselníky ohlašovatelů agend. Jinými slovy, možné hodnoty údaje lze vymezit

buď číselníkem ČSÚ nebo číselníkem ohlašovatele agendy. Z § 54 odst. 1, písm. a) ZoZR vyplývá, že primárně musí být volen číselník, který již je v RPP veden. Pouze pokud žádný vhodný číselník v RPP veden není, uvádí ohlašovatel agendy svůj vlastní číselník, tj. nový číselník ohlašovatele agendy.



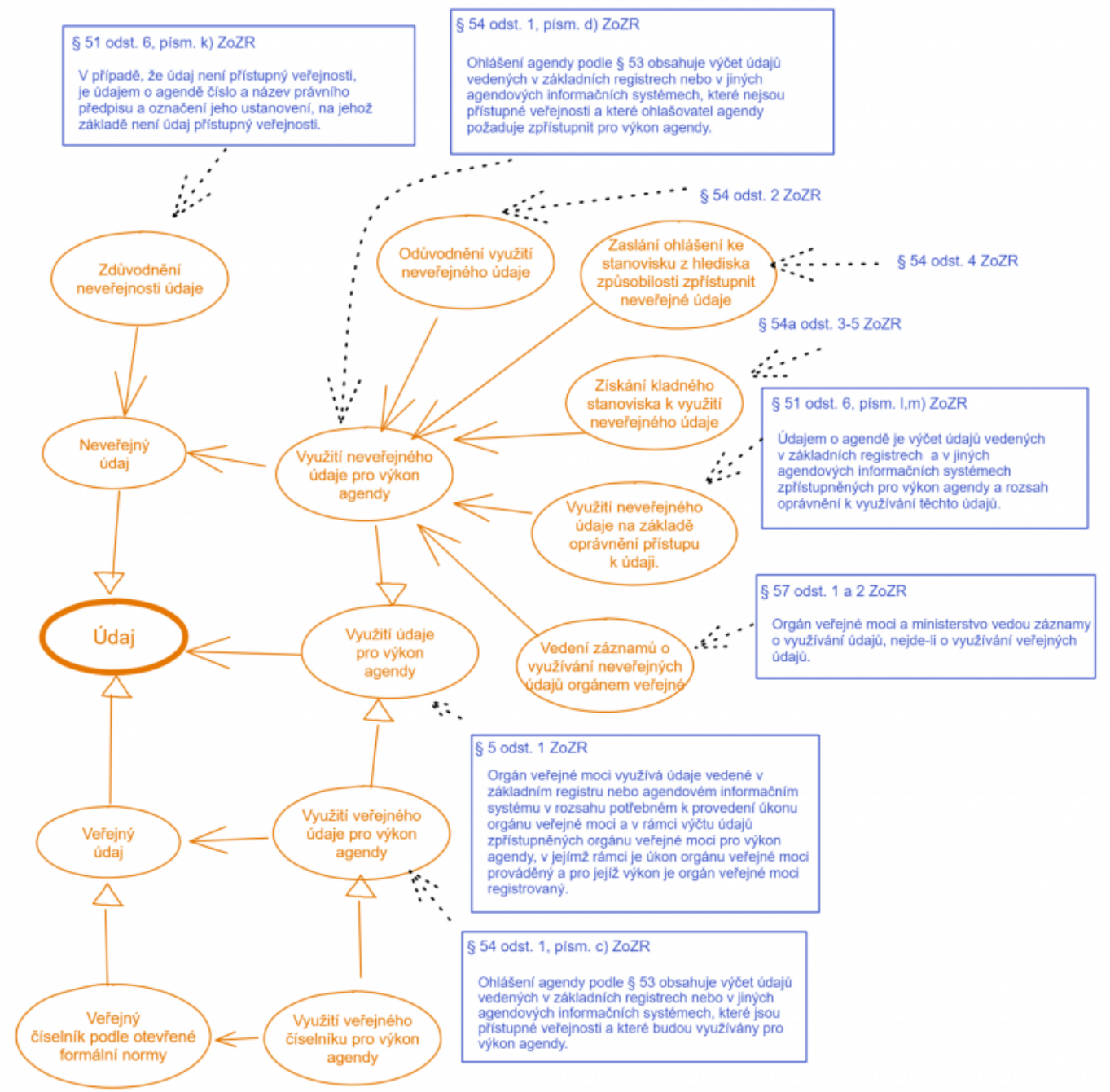
Jak bylo zmíněno na začátku dokumentu, rozlišení údajů na veřejné a neveřejné provádíme z pohledu sdílení údajů. Ať už se jedná o údaje veřejné nebo neveřejné, sdílením se podle § 2 písm. o) ZoISVS rozumí umožnění přístupu k daným datům prostřednictvím referenčního rozhraní.



Podle § 51 odst. 6, písm. k) ZoZR musí ohlašovatel agendy zdůvodnit neveřejnost každého jednotlivého údaje, který není přístupný veřejnosti.

Pro zajištění přístupu k neveřejnému údaji je dle § 54 odst. 1, písm. d) ZoZR nutno projít administrativní procedurou vedoucí k získání kladného stanoviska k využití neveřejného údaje. Je také nutno dle § 51 odst. 6, písm. l,m) ZoZR evidovat údaje zpřístupněné pro výkon agendy a dle § 57 odst. 1 a 2 ZoZR je nutno vést záznamy o využívání neveřejných údajů.

Naproti tomu využívání veřejných údajů je spojeno s nižší administrativní zátěží. Je pouze nutné podle § 54 odst. 1, písm. c) ZoZR při ohlášení agendy uvést, jaké veřejné údaje budou využívány pro výkon agendy.



Principy veřejného datového fondu

Obecným výchozím principem VDF je princip P13 eGovernmentu “Otevřená data jako standard” (Open Data by Default):

“Veřejné údaje evidované orgány veřejné správy ve spravovaných ISVS musí být zveřejňovány jako otevřená data. Pro neveřejné údaje musí být jako otevřená data zveřejňována jejich anonymizovaná podoba, souhrn nebo statistika. V případě, že orgány veřejné správy sdílejí veřejné údaje (včetně anonymizované podoby neveřejných údajů, souhrnů nebo statistik) musí je sdílet jako otevřená data.“

VDF zpřístupňuje veřejné registrované údaje jednotlivým OVM a SPUÚ pro čtení bez omezení přístupu. Navíc jsou všechny údaje přístupné z VDF dostupné ve stejné podobě také prostřednictvím otevřeného přístupu, a to bez výjimky. V obou případech zpřístupnění, tj. prostřednictvím VDF a prostřednictvím otevřeného přístupu, jsou údaje přístupné jako otevřená data dle § 3 odst. 11 InfoZ.

Pro vymezení navazujících pravidel VDF a navržení jeho celkové architektury slouží čtyři základní principy.

- P1 (distribuovanost) - VDF zastřešuje a popisuje skutečné datové zdroje poskytující údaje prostřednictvím referenčního rozhraní a stanovuje pravidla poskytování a čerpání údajů, ale nevynucuje jejich centralizaci na jedno místo.
- P2 (garance) - pro OVM a SPUÚ čerpající údaje z VDF je garantována technická dostupnost a formální správnost (věcná správnost, úplnost, platnost a pravidelná aktualizace) těchto údajů.
- P3 (otevřená data) - údaje přístupné z VDF jsou zpřístupněny jako otevřená data dle § 3 odst. 11 InfoZ bez výjimky.
- P4 (interoperabilita) - údaje jsou z VDF zpřístupněny v podobě, která zajišťuje schopnost různých programových vybavení vzájemně si poskytovat služby a efektivně spolupracovat.

Princip P1 – distribuovanost

VDF zastřešuje skutečné datové zdroje, které nemusí být centralizovány v jednom jediném úložišti. VDF spravuje a organizuje metadata o datových sadách, ve kterých jsou údaje z datových zdrojů zpřístupněny. Mezi tato metadata zejména patří:

- základní charakteristika datové sady (název, popis apod.),
- dokumentace datové sady,
- popis technického zpřístupnění datové sady.

Metadata o datových sadách jsou evidovány v podobě katalogizačních záznamů v NKOD.

Princip P2 – garance

OVM garantuje zpřístupnění veškerých veřejných registrovaných údajů, jejichž je autoritativním zdrojem, prostřednictvím referenčního rozhraní do VDF a na svůj náklad. Údaje dostupné z VDF musí být navíc pro účely čerpání OVM a SPUÚ dostupné, správné, úplné, platné a pravidelně aktualizované s jasně definovanou odpovědností poskytujícího OVM za poskytnutý obsah.

Pro údaje ve VDF platí:

- OVM může do VDF poskytovat pouze údaje, u kterých je autoritativním zdrojem.
- OVM poskytující údaje do VDF garantuje správnost, úplnost, platnost a aktuálnost pro čerpající OVM a SPUÚ.
- Infrastruktura VDF zajišťuje jejich dostupnost.
- Pokud OVM či SPUÚ čerpá údaje z VDF, považuje je za správné, úplné, platné a aktuální a nemusí tyto jejich vlastnosti ověřovat.
- Pokud OVM či SPUÚ využívá údaje dostupné ve VDF, přičemž je nezískal přímo z VDF, ale nějakým jiným způsobem, nemůže tyto údaje považovat za správné, úplné, platné ani aktuální.
- Při změně údajů dostupných ve VDF jsou notifikovány všechny OVM a SPUÚ, které údaje využívají.

Princip P3 – otevřená data

Údaje dostupné ve VDF jsou v totožné podobě také povinně publikovány jako otevřená data dle § 3 odst. 11 InfoZ. VDF tedy chápeme jako prostředek pro přístup jednotlivých OVM a SPUÚ ke garantovaným otevřeným datům.

Princip P4 – interoperabilita

Dva softwarové systémy jsou interoperabilní, pokud jsou schopné si vyměňovat informace a vzájemně si rozumět. V kontextu VDF, jeho širokého využití a velkého počtu informačních systémů je proto nutné zajistit

interoperabilitu na úrovni dat reprezentujících vyměňované údaje. Datovou interoperabilitu lze charakterizovat jako:

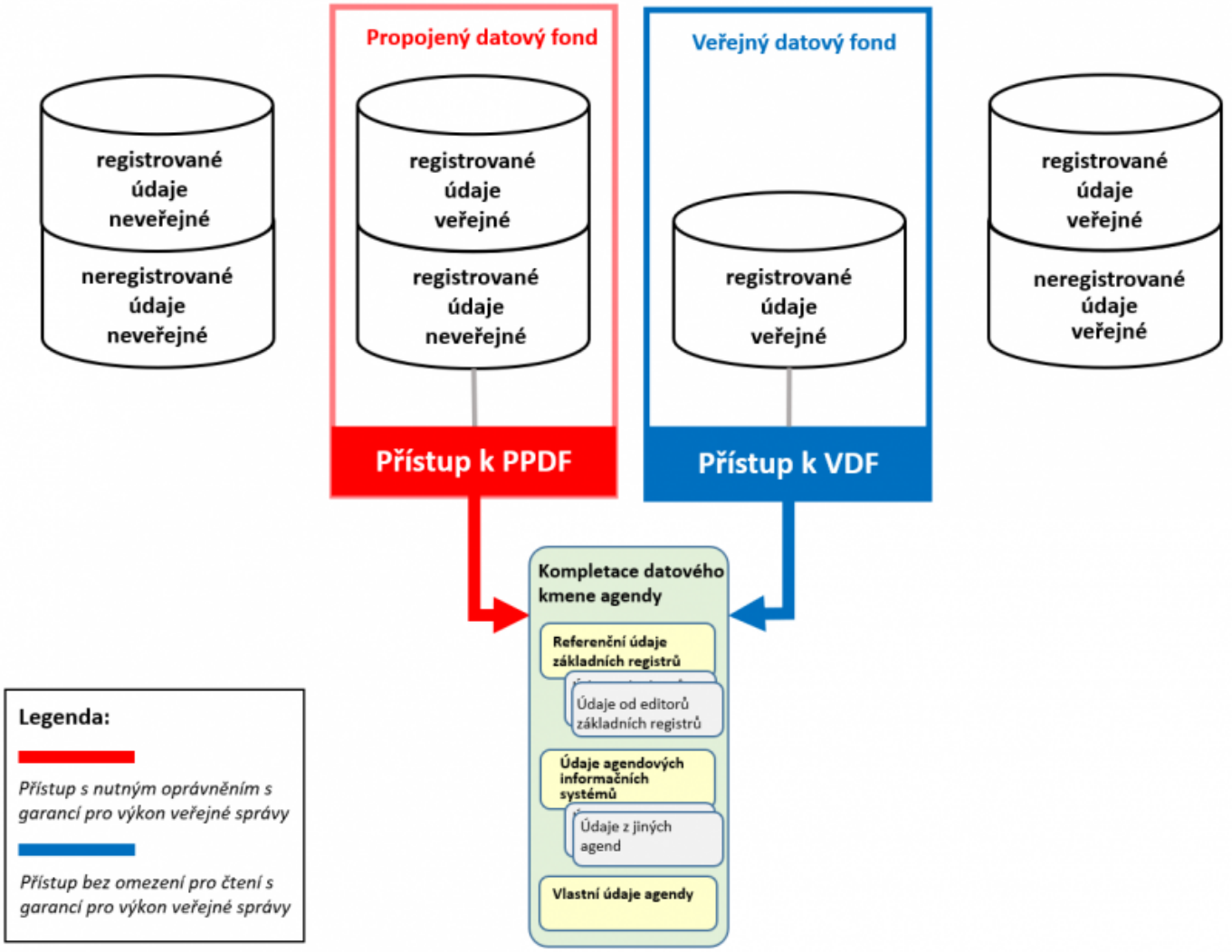
- technickou – použití standardních webových technologií pro perzistentní (tj. trvalou) identifikaci údajů a jejich výměnu,
- syntaktickou – specifikace a dodržování konkrétních formátů dat, komunikačních protokolů a dalších vlastností systémů, které umožňují přistupovat k datům z různých zdrojů standardním způsobem,
- sémantickou – způsob popisu a mapování datových položek, společné slovníky a jednotná klasifikace pojmů.

Ve VDF je technická, syntaktická a sémantická interoperabilita zajištěna prostřednictvím otevřených formálních norem vydávaných MV ČR pro různé typy dat poskytovaných do VDF.

Začlenění veřejného datového fondu do výkonu veřejné správy

Využití veřejného datového fondu pro doplnění datového kmene agendy

Základem pro výkon agendy je její datový kmen. Kompletace datového kmene agendy pro konkrétní výkon je zajišťována prostřednictvím PPDF a VDF. Výměna neveřejných registrovaných údajů je prováděna prostřednictvím PPDF ve vazbě na konkrétní subjekt práva evidovaný v základních registrech na základě oprávnění evidovaných v RPP. Veřejné registrované údaje jsou vyměňovány prostřednictvím VDF. Výměna prostřednictvím VDF je spojena s jednodušším administrativním procesem a oproti výměně prostřednictvím PPDF umožňuje dávkovou výměnu údajů v podobě celého obsahu datových sad s údaji bez vazby na konkrétní subjekt práva. Je-li to nezbytně nutné, lze veřejné registrované údaje sdílet i prostřednictvím PPDF, ale vždy jen na základě oprávnění a ve vazbě na konkrétní subjekt práva.

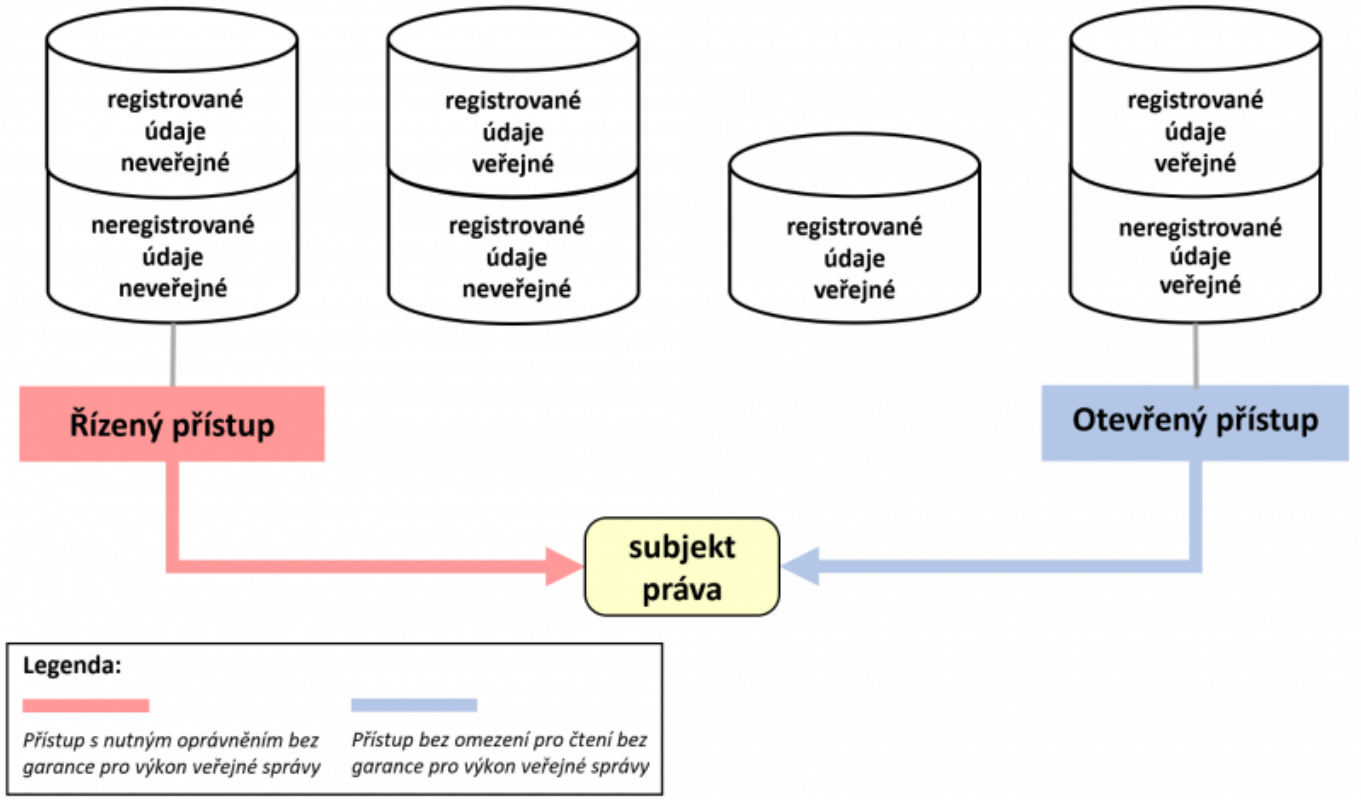


Přístup veřejnosti k údajům

K údajům veřejné správy má možnost přístupu ke čtení i veřejnost.

Přístup veřejnosti k veřejným údajům je zajišťován prostřednictvím otevřeného přístupu. Ten je charakteristický tím, že veřejné údaje jsou pro čtení zpřístupněny anonymním uživatelům z veřejného internetu bez jakéhokoliv omezení.

Přístup veřejnosti k neveřejným údajům je realizován prostřednictvím řízeného přístupu. Pro tento přístup ale platí, že je možný pouze na základě definovaných oprávnění konkrétním subjektům práva. Pravidla řízeného přístupu však budou teprve popsána a zde se jim dále nevěnujeme.



Základní struktura veřejného datového fondu

Vnitřní architektura VDF je kromě samotných veřejných registrovaných údajů datového fondu VS ČR tvořena také dílčími nástroji. Dílčí nástroje jsou primárně určeny pro ukládání obsahu datových sad a práci s metadaty datových sad. Dále je tvořen souborem pravidel, postupů a doporučení, které slouží k zabezpečení vyžadovaných vlastností zpřístupněných údajů, k zajištění jejich správné publikace a vytvoření podmínek pro využití publikovaných údajů při výkonu veřejné správy. Architektura VDF je zcela otevřená a připravená pro její další rozšiřování v závislosti na požadavcích na další funkcionality, a také pro podporu sémantické interoperability.

Přístup k údajům prostřednictvím VDF je technicky zajišťován jako

- přístup k datovým souborům s obsahem datových sad ke stažení (povinně)
- přístup ke konkrétní položce datové sady prostřednictvím REST API (volitelně)
- dotazování nad obsahem datové sady prostřednictvím SPARQL API (volitelně)

Přístup je zajištěn pomocí služeb referenčního rozhraní. Pro účely PPDF jsou služby referenčního rozhraní poskytovány prostřednictvím ISZR a ISSS. Oba ale předpokládají přístup k údajům o konkrétním subjektu práva vedeném v ZR a s potřebnými oprávněními. VDF však zavádí dávkový přístup k obsahu jednoho nebo více údajů bez vazby na konkrétní subjekt práva a to ke kompletnímu obsahu nebo k obsahu vázanému na jednu datovou položku. Za tímto účelem musí být referenční rozhraní rozšířeno o nové služby pro:

- čtení publikovaného datového souboru s obsahem datové sady
- čtení publikované položky datové sady
- dotazování nad obsahem datové sady

Tyto nové služby nemohou být z výše uvedených důvodů poskytovány prostřednictvím ISZR ani ISSS a proto je zavedena nová třetí komponenta referenčního rozhraní *Informační systém garantovaných otevřených dat (ISGOD)*. ISGOD zajišťuje jednotlivým OVM a SPUÚ přístup ke garantovaným otevřeným datům ve VDF prostřednictvím referenčního rozhraní.

Do VDF publikují jednotlivé AIS i ZR. Dále tedy v textu hovoříme o publikujícím ISVS, ale vždy je tím myšleno publikující AIS či ZR.

ISGOD je logickým zastřešením několika aplikačních komponent tvořících prostředí VDF. Komponenty jsou popsány v následujících podkapitolách.

Úložiště datových sad

Úložiště datových sad slouží k ukládání obsahu registrovaných veřejných údajů vedených v daném publikujícím ISVS v podobě distribucí datových sad. Pro každý publikující ISVS je vytvořeno úložiště, jehož správcem je správce ISVS. Úložiště datových sad zajišťuje:

- kontrolu souladu nahrávaného obsahu s otevřenými formálními normami
- transformaci obsahu do všech podob daných otevřenými formálními normami s pomocí transformačních skriptů definovaných otevřenými formálními normami
- zpřístupnění těchto podob jako distribuce datových sad, a to jako
    - datové soubory ke stažení (povinně)
    - API umožňující přistoupit ke každé jednotlivé položce datové sady (nepovinně)
    - API umožňující dotazování nad obsahem uložených datových sad pomocí dotazovacího jazyka SPARQL (nepovinně)
- garantovanou dostupnost distribucí datových sad při přístupu prostřednictvím ISGOD
    - požadovaná úroveň dostupnosti distribucí je stejná jako požadovaná úroveň dostupnosti ostatních služeb ISZR a ISSS
- negarantovanou dostupnost distribucí datových sad při přístupu prostřednictvím veřejného internetu

Úložiště datových sad daného publikujícího ISVS není novým ISVS, ale je součástí publikujícího ISVS.

Softwarový nástroj úložiště datových sad může správce ISVS vyvinout vlastní nebo může využít volně dostupný open-source nástroj nabízený a udržovaný MV ČR.

Národní katalog otevřených dat

V NKOD jsou evidovány katalogizační záznamy o všech datových sadách dostupných ve VDF. Za katalogizaci datových sad je zodpovědný publikující ISVS, který nahrává obsah do svého úložiště datových sad jako distribuce obsahu datové sady. Publikující ISVS poskytuje API dle otevřené formální normy rozhraní katalogů otevřených dat, prostřednictvím kterého poskytuje katalogizační záznamy o svých publikovaných datových sadách. API zaregistruje správce ISVS v NKOD. NKOD si poté pravidelně katalogizační záznamy načítá.

Čtenáři údajů z VDF mohou v NKOD vyhledávat datové sady a získávat tak metadata popisující přístup k jejich distribucím prostřednictvím VDF. Metadata také popisují přístup k distribucím prostřednictvím otevřeného přístupu.

Správcem NKOD je MV ČR.

Registr práv a povinností

V RPP je evidována přístupnost registrovaných údajů veřejnosti (tj. veřejnost údajů) a veřejné číselníky, které kódují jejich možné hodnoty. Ohlašovatel agendy je povinen označit přístupnost údaje veřejnosti. Také je povinen uvést, zda je údaj kódován veřejným číselníkem. Obsah veřejných údajů a veřejných číselníků je pak sdílený v podobě distribucí datových sad dostupných jako otevřená data prostřednictvím otevřeného přístupu a prostřednictvím VDF.

Pro potřeby otevřeného přístupu i VDF je pro každý veřejných číselník evidováno IRI datové sady v NKOD, ve které je obsah číselníku přístupný. To samé platí pro veřejný údaj, pouze může být datových sad více.

Čtenáři údajů z VDF vyhledávají v RPP evidenci údajů potřebné údaje. V případě veřejných údajů získávají IRI

datových sad v NKOD, s pomocí kterých mohou z NKOD získat metadata popisující přístup k obsahu veřejných údajů. Podobně v případě údajů, jejichž hodnoty jsou kódovány veřejnými číselníky, získávají IRI datových sad v NKOD, s pomocí kterých mohou z NKOD získat metadata popisující přístup k obsahu veřejných číselníků.

V RPP je také pro každou agendu evidován výčet veřejných registrovaných údajů, které jsou využívány pro výkon agendy.

Správcem RPP je MV ČR.

Katalog uživatelů dat

Katalog uživatelů dat eviduje, jaké datové sady z VDF čerpají konkrétní OVM a SPUÚ. Registraci čerpání datové sady provádí OVM či SPUÚ za účelem získávání notifikací o změnách v datové sadě. Registrace je předvyplněna z evidence čtení registrovaných veřejných údajů v RPP.

Registrace mj. obsahuje:

- IRI OVM či SPUÚ
- IRI datové sady
- požadovanou maximální frekvenci notifikací (ihned, hodinová, denní, týdenní, …)
- požadovaný způsob a technická specifikace notifikace (datová schránka, WebSub protokol)

Správcem katalogu uživatelů dat je MV ČR.

Notifikační hub

Notifikační hub je nástroj zajišťující s pomocí katalogu uživatelů dat notifikační službu, která informuje subjekty registrované v katalogu uživatelů dat ke čtení datových sad z VDF o změnách v datových sadách. Jedná se o automatickou notifikaci o změnách zjištěných při ohlášení změny ze strany poskytujícího ISVS.

Notifikační hub je implementován na bázi mezinárodního standardu W3C Recommendation WebSub.

Správcem Notifikačního hubu je MV ČR.

Směrovací služba

Distribuce datové sady je v otevřených datech zpřístupněna jako datový soubor ke stažení nebo jako API, které umožňuje získat data každé jednotlivé položky datové sady (entity), o níž jsou v datové sadě reprezentovány údaje. Přístup k údajům je realizován s pomocí tzv. dereference identifikátoru položky. V otevřených datech jsou jako identifikátory použity tzv. IRI (Internationalized resource identifier, více viz Otevřená formální norma pro propojená data). Dereference identifikátoru v podobě IRI znamená přistoupení k IRI prostřednictvím HTTP protokolu podobně jako přistupujeme k webovým stránkám. Výsledkem dereference je strojově nebo lidsky čitelná reprezentace údajů o identifikované položce (v závislosti na HTTP content negotiation).

IRI položky vyplývá z úložiště datových sad, na kterém je datová sada s položkou fyzicky uložena a z pravidel pro tvorbu IRI. To ale činí IRI závislé na konkrétním fyzickém umístění, které se může měnit. Např. může změnit své fyzické umístění celé úložiště tím, že se změní jeho provozovatel nebo je přesunuto do jiného prostředí. Nebo může dojít k rozhodnutí přesunout obsah datové sady do jiného úložiště. Pokud k takové změně dojde, může dojít i ke změně IRI položek. Přes tato IRI ale již mohou být propojeny údaje o prvku či souvisejících prvcích z jiných datových sad ve VDF i v otevřených datech či údajích dostupných přes řízený přístup. Pokud se IRI takto mění, znamená to, že nejsou tzv. perzistentní, tj. trvalé. Pro zajištění perzistentních, tj. trvalých, identifikátorů slouží směrovací a indexační služba.

Pro veřejný údaj je nutné, aby správce ISVS, ze kterého se obsah údaje publikuje, zavedl identifikátory položek datové sady do směrovací služby a určil k nim tzv. referenční identifikátory na doméně gov.cz. Pro položku tak existují dva identifikátory. První je původní identifikátor položky určený správcem ISVS. Vyplývá z úložiště datových sad, ve kterém je obsah datové sady uložen. Jedná se o IRI v doméně úložiště, při jehož dereferenci úložiště poskytne obsah o identifikované položce. Nazýváme jej lokální identifikátor položky nebo zkráceně *lokální IRI položky*. Druhý identifikátor je nový identifikátor, který je nezávislý na úložišti. Nazýváme jej referenční identifikátor položky ve VDF nebo zkráceně *referenční IRI položky*. Referenční IRI používají pro odkazování se na položku všechny datové sady. Dereference referenčního IRI vede na směrovací službu, která provede přesměrování na lokální IRI položky.

Při změně úložiště datových sad nebo obecně při změně lokálních IRI je upraveno směrování ve směrovací službě. Tím je zajištěna perzistence IRI, která umožňuje trvalé a neměnné propojení údajů o stejné položce napříč různými datovými zdroji nezávisle na poskytovatelích těchto údajů.

Správcem směrovací a indexační služby je MV ČR.

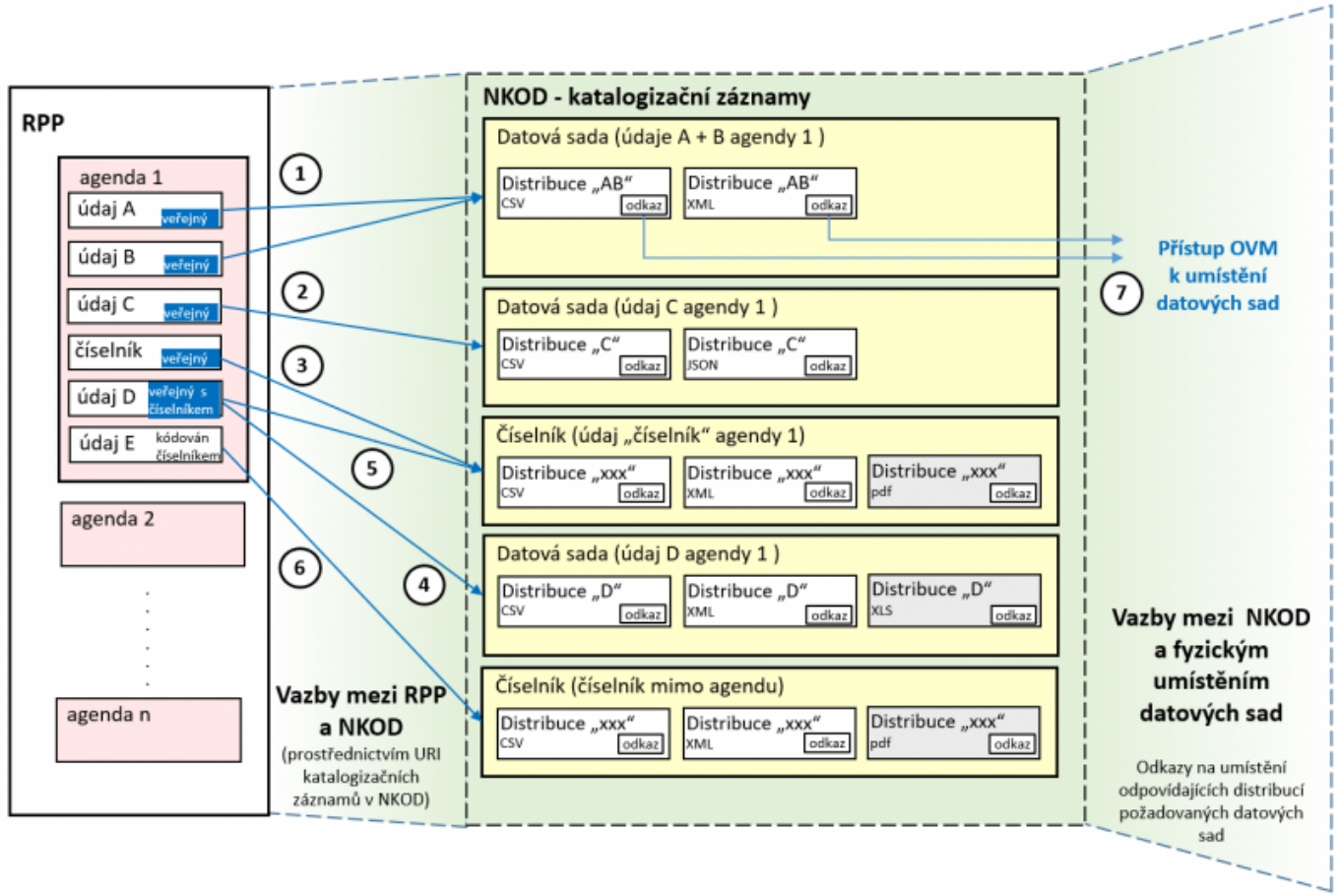
Pravidla veřejného datového fondu

Pravidla pro údaje zpřístupněné veřejným datovým fondem

Ve VDF jsou zpřístupňovány veřejné registrované údaje spravované jednotlivými OVM. Pro údaje zpřístupněné prostřednictvím VDF platí:

- Údaje jsou zpřístupněny v datových sadách prostřednictvím referenčního rozhraní pro potřeby čtenářů údajů - OVM a SPUÚ.
- Datové sady jsou navíc publikovány prostřednictvím otevřeného přístupu (tj. jako otevřená data dle § 3 odst. 11 InfoZ) v totožné podobě (tj. s totožnou strukturou a sémantikou).
- Otevřený přístup i přístup prostřednictvím VDF jsou tedy dva přístupy ke stejnému obsahu v podobě otevřených dat.
    - První je určen pro veřejnost, druhý je určen pro OVM a SPUÚ a je realizován prostřednictvím referenčního rozhraní.
- Datové sady jsou popsány v podobě katalogizačních záznamů (metadat) v NKOD.
- Datové sady jsou fyzicky dostupné v podobě distribucí. Různé distribuce stejné datové sady zpřístupňují její obsah v různých formátech a prostřednictvím různých přístupových mechanismů. Proto je každá distribuce zaznamenána v katalogizačním záznamu datové sady v NKOD. VDF předpokládá tři následující způsoby zpřístupnění obsahu datové sady, z nichž první je povinný a zbylé dva jsou volitelné:
    - v podobě datového souboru s kompletním obsahem datové sady ke stažení,
    - v podobě API, které umožňuje přistupovat ke kompletním údajům o každé jednotlivé entitě či konceptu, o němž jsou v datové sadě reprezentovány údaje, prostřednictvím dereference identifikátoru entity či konceptu, který je stanoven poskytovatelem údajů v podobě IRI (Internationalized Resource Identifier, více viz Otevřená formální norma pro propojená data) a
    - v podobě API, které umožňuje dotazování nad obsahem datové sady s pomocí dotazovacího jazyka SPARQL
- Informace o veřejnosti registrovaného údaje je zachycena v jeho evidenci v RPP označením údaje jako veřejného údaje.
    - Pro veřejný údaj obsahuje RPP v evidenci údaje IRI datové sady (nebo datových sad) v NKOD, v níž je obsah odpovídající údaji zpřístupněn prostřednictvím VDF a publikován jako otevřená data.
    - Pro údaj kódovaný číselníkem obsahuje RPP v evidenci údaje IRI datové sady v NKOD, v níž je číselník zpřístupněn prostřednictvím VDF a publikován jako otevřená data.

Vlastní mechanismus zpřístupnění údajů do VDF přibližuje dále uvedený obrázek na několika příkladech údajů „agendy 1“. Čísla v kroužcích na obrázku označují jednotlivé příklady.

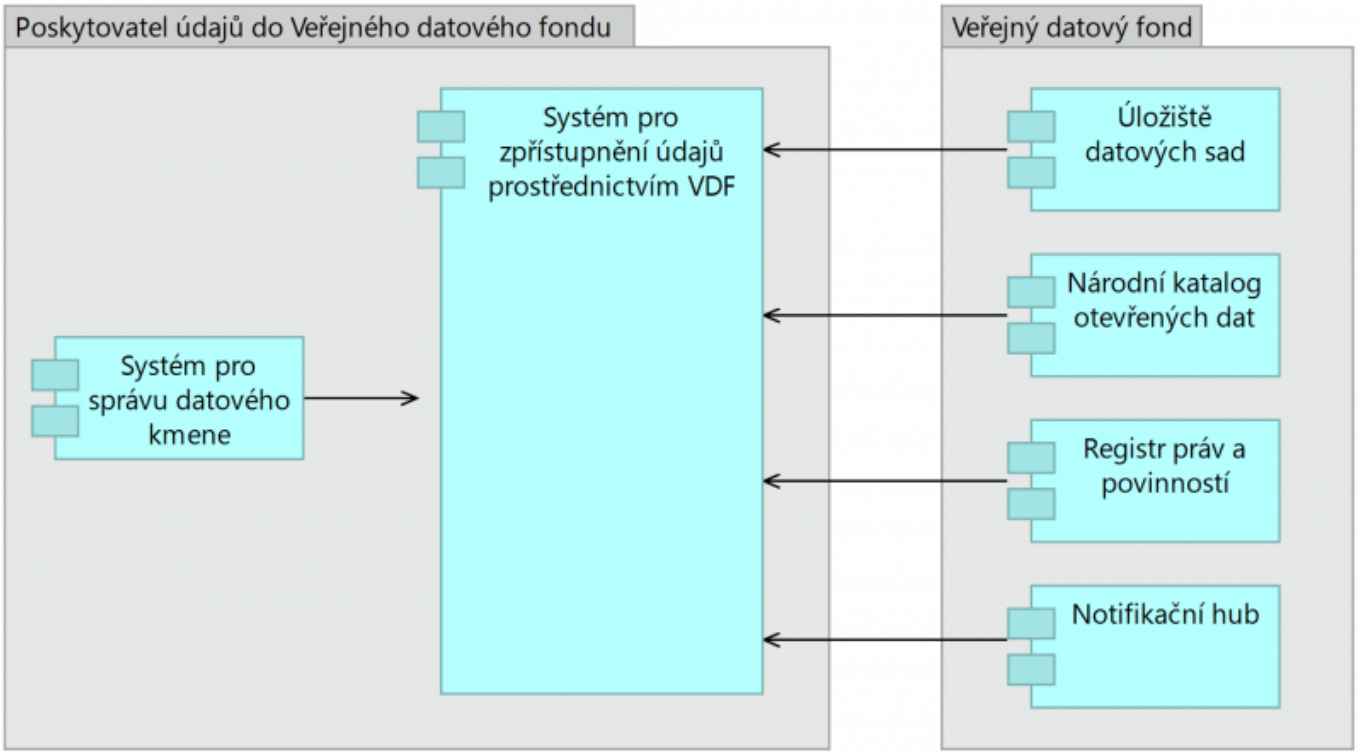


1. V RPP je u agendy 1 evidováno, že údaje A i B jsou veřejné. To znamená, že jsou dostupné jako otevřená data prostřednictvím VDF a otevřeného přístupu.
   - Oba údaje jsou dostupné prostřednictvím stejné datové sady.
   - V RPP je v evidenci těchto údajů uvedeno IRI datové sady v NKOD (datová sada se jmenuje „Údaje A + B agendy 1“).
   - Datová sada je publikovaná a dostupná v několika distribucích, katalogizační záznam obsahuje pro každou distribuci odkaz na její fyzické umístění (tj. její URL).
2. V RPP je u agendy 1 evidováno, že údaj C je veřejný. Jedná se o stejnou situaci jako v příkladu 1, pouze s tím rozdílem, že údaj C je publikován v jiné samostatné datové sadě.
3. Agenda 1 vytváří a udržuje číselník, který je dostupný ve VDF a je publikován jako otevřená data.
4. V RPP je u agendy 1 evidováno, že údaj D je veřejný a je publikován v samostatné datové sadě. Jedná se o stejnou situaci jako v příkladu 1.
5. U údaje D je v RPP evidováno, že je kódován číselníkem (v příkladu je uvedena situace s číselníkem, který agenda přímo vytváří, ale vše uvedené platí, pro jakýkoliv využívaný číselník). Evidence údaje v RPP proto také obsahuje IRI datové sady v NKOD, který obsahuje publikovaný číselník.
6. V RPP je u agendy 1 evidováno, že údaj E je neveřejný a tudíž není možné jej zpřístupnit ve VDF. U údaje E je ale evidováno, že je kódován číselníkem (v tomto případě se pro demonstraci jedná o číselník spravovaný mimo agendu 1). Evidence údaje v RPP obsahuje IRI datové sady v NKOD, který obsahuje publikovaný číselník (stejně jako v příkladu 5).
7. Reprezentuje přístup k distribucím datových sad prostřednictvím VDF.

Pravidla sdílení veřejných údajů prostřednictvím VDF

Pravidla publikace veřejných údajů do VDF

Základní prvky architektury VDF z pohledu poskytovatele údajů zobrazuje následující obrázek.



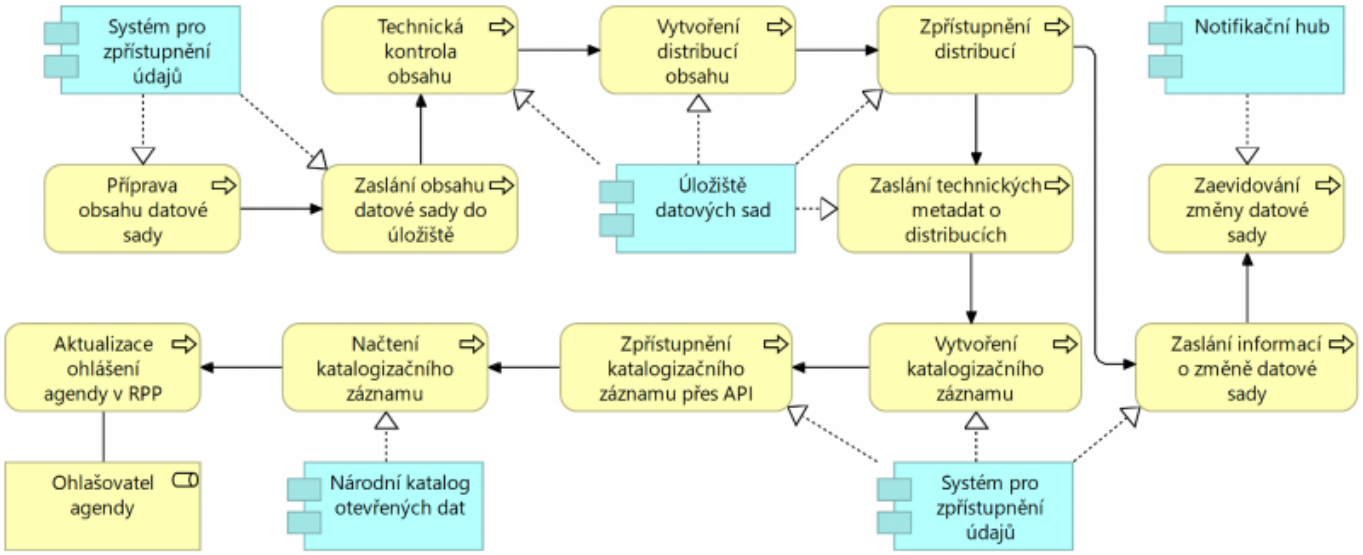
Poskytovatelem údajů do VDF je správce ISVS, ve kterém jsou vedeny registrované veřejné údaje. Tento ISVS je vyznačen na levé straně obrázku jako *systém pro správu datového kmene*, kterým OVM spravuje svůj datový kmen. V praxi se samozřejmě může jednat o více ISVS, zde si pro jednoduchost zobrazujeme jen jeden systém.

Pro potřeby sdílení údajů ve VDF poskytovatel údajů vytvoří *systém pro zpřístupnění údajů prostřednictvím VDF*. Může se jednat o samostatný systém nebo to může být modul v rámci existujícího systému. Zajišťuje získávání obsahu veřejných údajů z datového kmene poskytovatele, rozdělení do vhodných datových sad a převod do podoby definované otevřenými formálními normami a jeho dávkové předání do úložiště datových sad.

Úložiště datových sad zajišťuje kontrolu technické správnosti zaslaných dávek vůči otevřeným formálním normám a zpřístupnění distribucí obsahu ve všech formátech definovaných otevřenými formálními normami. Úložiště dále zajišťuje dostupnost distribucí čtenářům prostřednictvím ISGOD i prostřednictvím veřejného internetu. Dostupnost distribucí prostřednictvím ISGOD navíc garantuje. Úložiště datových sad pro ukládání obsahu datových sad z daného ISVS je vytvořeno pro daný ISVS právě jedno a spravuje jej správce ISVS. V případě, že se jedná o aktualizaci obsahu datové sady, oznamuje úložiště datových sad notifikačnímu hubu, že obsah datové sady byl změněn.

Poté, co jsou distribuce obsahu datových sad uloženy v úložišti a zpřístupněny, jsou datové sady katalogizovány v NKOD prostřednictvím systému pro zpřístupnění údajů. K tomu poskytuje systém pro zpřístupnění údajů API, které splňuje otevřenou formální normu rozhraní katalogů otevřených dat. Katalogizace datových sad v NKOD je tak automatizovaná.

Celý proces publikace údajů sdružených v jedné datové sadě do VDF je znázorněn na následujícím diagramu. Proces předpokládá, že příslušná agenda již byla ohlášena v RPP včetně všech jejích údajů v potřebné úrovni granularity.



V rámci procesu:

- Systém pro zpřístupnění údajů
  - Připraví obsah datové sady v podobě datového souboru v jednom z formátů definovaných otevřenými formálními normami.
    - Specifikaci otevřených formálních norem lze získat z repozitáře otevřených formálních norem.
    - Pokud pro údaje neexistuje otevřená formální norma, musí ji správce systému pro zpřístupnění údajů s podporou MV ČR nejprve vytvořit.
  - Zašle připravený obsah datové sady do úložiště datových sad.
- Úložiště datových sad
  - Provede technickou kontrolu zaslaného obsahu
    - Kontrola správného formátování (např. JSON nebo XML formátování)
    - Kontrola validity datové struktury vůči datovým schématům definovaných otevřenými formálními normami (např. vůči JSON nebo XML schématům)
  - V případě špatné syntaxe zašle zpět systému pro zpřístupnění údajů chybové hlášení a skončí.
  - Vytvoří distribuce obsahu jeho transformací do všech podob definovaných otevřenými formálními normami s využití transformačních skriptů/procedur/mapování, které jsou součástí otevřených formálních norem.
  - Zpřístupní vytvořené distribuce
    - Zpřístupní je jako datové soubory dostupné ke stažení prostřednictvím ISGOD a z veřejného internetu.
      - URL pro stažení datového souboru je stejné pro přístup prostřednictvím ISGOD a veřejného internetu, k čemuž je nutné správně nastavit DNS v prostředí KIVS/CMS a DNS v prostředí veřejného internetu.
    - Volitelně zpřístupní jednotlivé položky obsahu dle otevřené formální normy pro propojená data tak, že má každá položka své referenční a lokální IRI dereferencovatelné prostřednictvím ISGOD a z veřejného internetu.
      - Referenční IRI položky je stejné pro přístup prostřednictvím ISGOD a veřejného internetu, k čemuž je nutné správně nastavit DNS v prostředí KIVS/CMS a DNS v prostředí veřejného internetu.
      - Lokální IRI položky je stejné pro přístup prostřednictvím ISGOD a veřejného internetu, k čemuž je nutné správně nastavit DNS v prostředí KIVS/CMS a DNS v prostředí veřejného internetu.
    - Volitelně zpřístupní jejich obsah v podobě SPARQL endpointu prostřednictvím ISGOD a ve veřejném internetu.
      - URL SPARQL endpointu je stejné pro přístup prostřednictvím ISGOD a veřejného internetu, k čemuž je nutné správně nastavit DNS v prostředí KIVS/CMS a DNS v prostředí veřejného internetu.

    - Zašle zpět systému pro zpřístupnění údajů potvrzení o úspěšném uložení.
        - Jako součást potvrzení zasílá metadata o vytvořených distribucích v podobě definované otevřenou formální normou pro rozhraní katalogů otevřených dat.
- Systém pro zpřístupnění údajů
    - Vytvoří kompletní katalogizační záznam o datové sadě včetně metadat o distribucích vytvořených úložištěm datových sad a zpřístupní jej prostřednictvím API dle otevřené formální normy pro rozhraní katalogů otevřených dat.
    - Zašle notifikačnímu hubu informaci o změně obsahu datové sady.
        - Úroveň detailu informace není v tomto místě řešena.
- Národní katalog otevřených dat
    - Získá katalogizační záznam z API poskytnutého systémem pro zpřístupnění údajů a zaeviduje jej.
- Ohlašovatel agendy
    - Ohlásí do RPP jako součást ohlášení agendy referenční IRI datové sady (datových sad) v NKOD, ve které (kterých) je veřejný údaj zpřístupněn. Ohlášení provede poté, co NKOD datovou sadu na základě zaslaného katalogizačního záznamu zaeviduje (zpravidla do 1 dne).
- Notifikační hub
    - Zaeviduje informaci o změně datové sady zaslanou úložištěm datových sad.

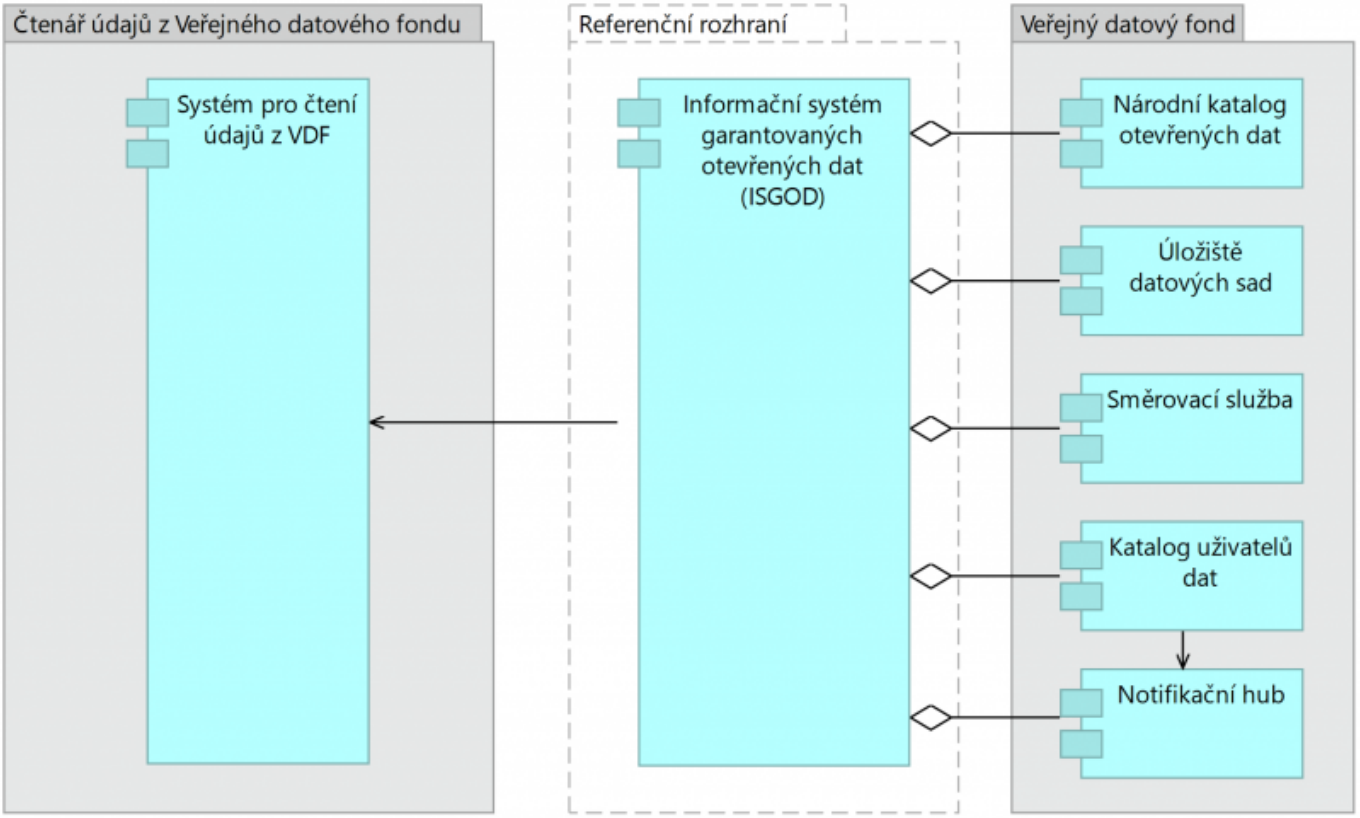
Systém pro zpřístupnění údajů prostřednictvím VDF souvisí s existujícím systémem pro zpřístupnění údajů prostřednictvím PPDF, který zajišťuje poskytování údajů o konkrétním subjektu práva, na který přistupuje čtenářský AIS prostřednictvím PPDF. Systém pro zpřístupnění údajů prostřednictvím VDF (dále jen *systém pro zpřístupnění údajů*) oproti tomu aktivně v pravidelných správcem ISVS definovaných intervalech exportuje obsah veřejných údajů do podoby datových sad a dávkově je předává do *úložiště datových sad*, ze kterého jsou jako otevřená data dostupné prostřednictvím VDF a otevřeného přístupu.

PPDF a VDF jsou tedy dva různé způsoby sdílení datového kmene agendy. Technická podoba dat určená pro sdílení prostřednictvím PPDF je definována v kontextech, tj. XSD schématech popisujících XML struktury, ve kterých je obsah datového kmene agendy sdílen prostřednictvím PPDF. Technická podoba dat určená pro sdílení prostřednictvím VDF je definována otevřenými formálními normami. Otevřené formální normy definují datová schémata. Nejedná se ale nutně jen o XSD schémata, ale také o JSON schémata, CSV schémata nebo ontologie pro popis RDF reprezentace. To z toho důvodu, že totožný obsah, který je dostupný prostřednictvím VDF je dostupný jako otevřená data, kde je nutno z důvodů interoperability a dodržení dobré praxe nabídnout obsah v různých standardních formátech.

Protože ale kontexty pro PPDF a datové struktury v OFN pro VDF jsou dvěma syntaktickými stranami téže sémantické mince (tj. jsou různými syntaktickými reprezentacemi stejné sémantiky), je nutno tuto sémantiku strukturovaně a explicitně vyjádřit. K tomu jsou využívány techniky ontologického konceptuálního modelování, kdy je sémantika všech údajů v dané agendě popsána na konceptuální úrovni v podobě ontologie podle vyhlášky, která nahradí současnou vyhlášku č. 529. Pro tvorbu konceptuálních modelů v podobě ontologie MV ČR spravuje a provozuje sadu volně dostupných modelovacích nástrojů. Ty umožňují také z konceptuálních modelů definice kontextů pro PPDF a datových struktur v OFN pro VDF automatizovaně generovat a zajišťovat tak jejich vzájemnou sémantickou interoperabilitu. Konceptuální model agendy by navíc měl být tvořen konzistentně s modely ostatních agend, a modely agend by měly vycházet ze společné ontologie veřejné správy a ze slovníků definovaných EU (tzv. ISA Core Vocabularies), což podporuje sémantickou interoperabilitu vyměňovaných údajů napříč agendami i v rámci EU.

Čtení veřejných údajů z VDF

Základní stavební kameny architektury VDF z pohledu čtenáře údajů zobrazuje následující obrázek.



Čtenářem údajů z VDF je správce ISVS, který čte veřejné údaje. Tento ISVS je v obecné úrovni vyznačen na levé straně obrázku jako *systém pro čtení údajů z VDF* (dále jen *systém pro čtení údajů*).

Systém pro čtení údajů čte veřejné údaje z VDF jako otevřená data prostřednictvím ISGOD v podobě distribucí datových sad v různých formátech definovaných otevřenými formálními normami. Jsou umožněny 3 základní druhy přístupu prostřednictvím ISGOD:

1. Přístup ke kompletnímu obsahu datové sady v podobě datových souborů voláním
    1. služeb ISGOD umožňujících přistoupit k metadatům o datové sadě a jejích distribucích na základě jejich referenčních IRI a k URL daného souboru a stáhnout jej. (povinné)
2. Přístup k jednotlivým položkám datových sad voláním služeb ISGOD umožňujících přistoupit k datům o dané položce na základě jejího referenčního IRI. (volitelné)
3. Dotazování nad položkami datových sad voláním dotazovacích služeb ISGOD. (volitelné)

Služby ISGOD jsou realizovány jako webové služby postavené na principech REST, které jsou poskytovány jednotlivými komponentami VDF znázorněnými v pravé části obrázku:

- REST služby NKOD umožňují číst metadata o datových sadách a jejich distribucích.
- REST služby úložiště datových sad umožňují číst obsah v nich uložených datových sad v podobě
    - stahování datových souborů s obsahem uložených datových sad (povinné)
    - přístupu k IRI jednotlivých položek obsahu uložených datových sad (volitelné)
    - SPARQL dotazů nad obsahem uložených datových sad (volitelné)

ISGOD je pouhým logickým zastřešením výše uvedených služeb.

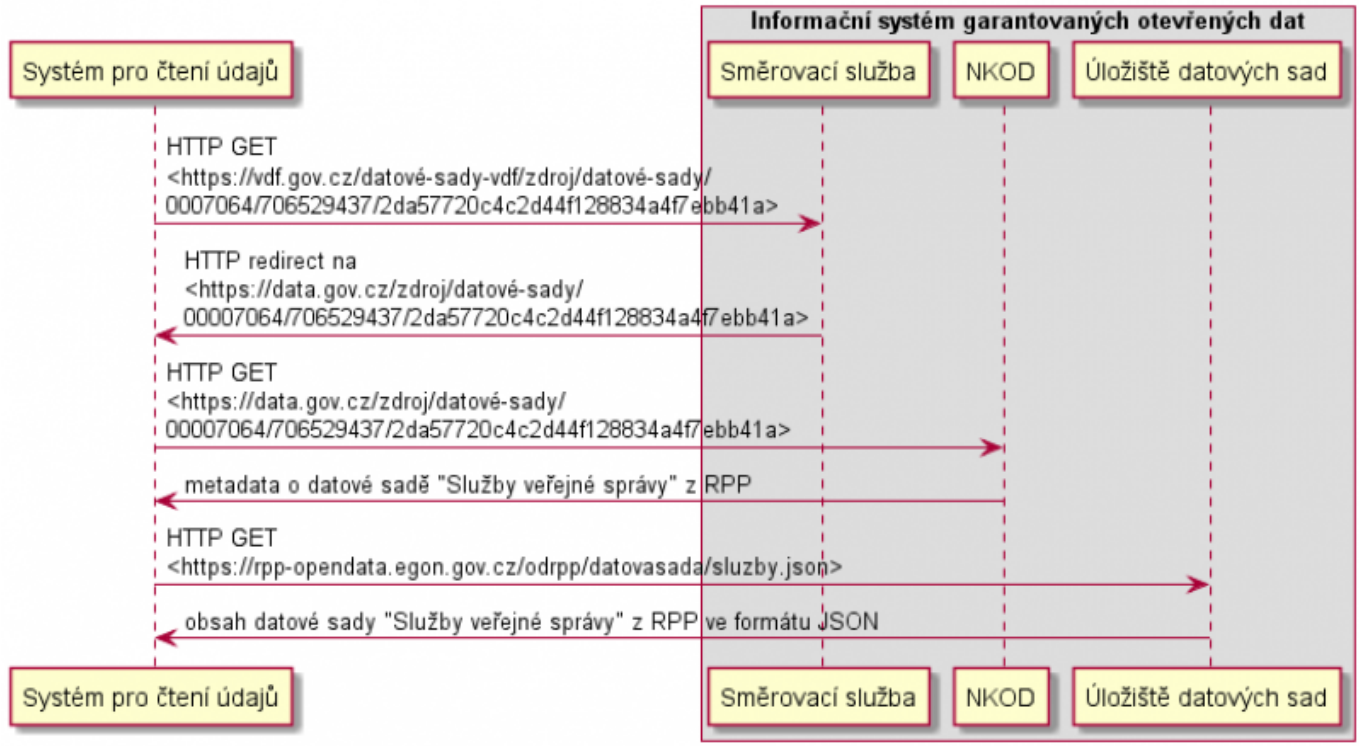
Čtení obsahu datové sady v podobě datového souboru

Čtení obsahu datové sady v podobě datového souboru typicky systém pro čtení údajů provádí za účelem aktualizace vlastní kopie údajů přebíraných z VDF. Aktualizaci typicky provádí v pravidelných intervalech nebo na základě notifikací o změnách zasílaných notifikačním hubem na základě registrace v katalogu uživatelů, ale mimo svůj run-time. Dávkový přístup ke kompletnímu obsahu datové sady v podobě datového souboru

předpokládá, že systém pro čtení údajů zná referenční IRI datové sady. Referenční IRI datové sady je možné zjistit z evidence agendových údajů v RPP nebo vyhledáváním v NKOD. Přístup je pak realizován následujícím postupem:

- Systém pro čtení údajů přistupuje k referenčnímu IRI datové sady.
- Směrovací služba přesměrovává referenční IRI datové sady na lokální IRI datové sady v NKOD.
- Systém pro čtení údajů přistupuje k lokálnímu IRI datové sady v NKOD.
- NKOD vrací metadata o datové sadě.
- Systém pro čtení údajů vybírá distribuci datové sady dle potřebného formátu a přistupuje k URL ke stažení obsahu distribuce.
- Úložiště datových sad zasílá systému pro čtení údajů obsah datového souboru na daném URL.

Následující obrázek postup znázorňuje v podobě sekvenčního UML diagramu na konkrétním příkladu přístupu k datové sadě “Služby veřejné správy”, která je publikována z RPP.



Čtení položky datové sady

Čtení položky datové sady typicky systém pro čtení údajů provádí za účelem zobrazení veřejných údajů o položce v uživatelském rozhraní nebo jiné práce s konkrétní položkou v okamžiku potřeby práce s údaji o položce, tj. v rámci svého run-time. Přístup k položce předpokládá, že systém pro čtení údajů zná referenční IRI položky. Referenční IRI položky je možné získat následujícími způsoby:

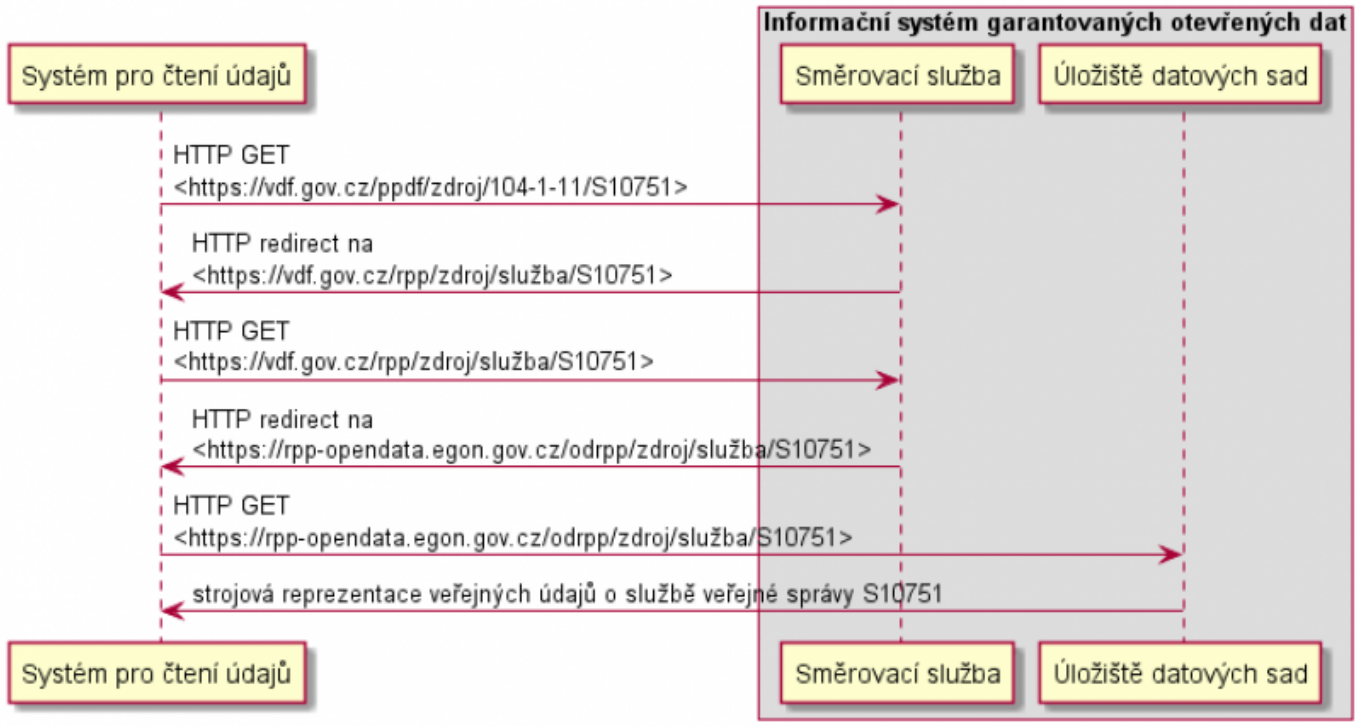
- V předchozích krocích byl přečten z VDF údaj s referenčním IRI jako hodnotou.
- V předchozích krocích byl přečten z PPDF údaj s proprietárním identifikátorem entity jako hodnotou (tj. identifikátor v podobě řetězce, který identifikuje entitu lokálně v rámci ISVS). Referenční IRI položky s veřejnými údaji o entitě získá systém pro čtení údajů voláním směrovací služby s kódem údaje (evidovaným v RPP) a proprietárním identifikátorem.

Přístup je pak realizován následujícím postupem:

- Systém pro čtení údajů přistupuje k referenčnímu IRI položky.
- Směrovací služba přesměrovává referenční IRI položky na lokální IRI položky v konkrétním úložišti datových sad, kde jsou údaje o položce uloženy.

- Systém pro čtení údajů přistupuje k lokálnímu IRI položky na daném úložišti datových sad.
- Úložiště datových sad vrací veřejné údaje o položce.
- Systém pro čtení údajů zobrazuje nebo jinak zpracovává získané údaje.

Následující obrázek postup znázorňuje v podobě sekvenčního UML diagramu na konkrétním příkladu přístupu k veřejným údajům o službě evidované v RPP s proprietárním identifikátorem S10751 a s názvem “Pěstitelské pálení”. Jedná se o položku datové sady “Služby veřejné správy”, která je publikována z RPP. Postup zahrnuje i získání referenčního identifikátoru položky z proprietárního identifikátoru na začátku procesu. Systému pro čtení údajů je známo pouze id “S10751” pro údaj agendy 104 s kódem “104-1-11”. Zkonstruuje IRI identifikující položku a přistoupí na něj. Toto IRI vede na směrovací službu, která provede přesměrování na referenční IRI položky.



Pravidla sdílení veřejných číselníků prostřednictvím VDF

Speciálním případem sdílení veřejných údajů prostřednictvím VDF je pak sdílení veřejných číselníků. Vychází z architektury sdílení veřejných údajů popsané v předchozí kapitole. Má však svá specifika, která jsou popsána zde.

Pravidla publikace veřejných číselníků do VDF

Architektura pro publikaci veřejných číselníků do VDF je vystavěna na bázi architektury pro publikaci veřejných údajů do VDF. Aby byl veřejný číselník publikován do VDF, musí být podle § 51 odst. 8 ZoZR zaveden do RPP. Zavedení je provedeno prostřednictvím AIS působnostní a provede jej buď ohlašovatel agendy nebo ČSÚ (dále dohromady jen *poskytovatel číselníku*). ČSÚ zavádí do RPP veřejné číselníky nezávisle na agendách. Ohlašovatel agendy zavádí veřejný číselník jen v případě, že je agendový údaj kódován číselníkem, který ještě není v RPP nikým zaveden.

Všechny veřejné číselníky jsou tedy jako referenční údaje evidovány v RPP prostřednictvím AIS působnostní a z něj jsou také publikovány do VDF. Z AIS působnostní jsou také publikovány do VDF všechny ostatní veřejné údaje evidované v RPP v podobě datových sad. Z pohledu architektury pro publikaci veřejných údajů do VDF je tedy pro potřeby všech veřejných číselníků AIS působnostní systémem pro správu datového kmene a zároveň má jako svoji komponentu systém pro zpřístupnění údajů prostřednictvím VDF, který zajišťuje publikaci obsahu

veřejných číselníků do VDF. Pro ukládání obsahu veřejných číselníků a také obsahu veřejných údajů vedených v RPP je využito stávající úložiště, na kterém je uložen obsah RPP publikovaný jako otevřená data. AIS působnostní zajišťuje také API poskytující katalogizační záznamy o jednotlivých datových sadách s veřejnými číselníky a s obsahem údajů vedených v RPP.

K realizaci výše popsané architektury publikace veřejných číselníků do VDF a jako otevřená data je nutno zajistit následující rozšíření informačního systém AIS působnostní a RPP:

1. označování veřejnosti a neveřejnosti údaje
    1. včetně odkazů na legislativu v případě neveřejnosti údaje
    2. včetně IRI datových sad v NKOD, prostřednictvím kterých je veřejný údaj publikován
2. evidenci veřejných číselníků
    1. pro každý veřejný číselník existuje 1..- verzí, které chápeme jako jednotlivé datové sady
    2. všechny datové sady reprezentující jednotlivé verze číselníku jsou seskupeny do zastřešující datové sady
    3. pro zastřešující datovou sadu a jednotlivé verze jsou evidována metadata datové sady dle otevřené formální normy pro rozhraní katalogů otevřených dat
        1. mimo vlastnosti poskytovatel, protože tato vlastnost reprezentuje poskytovatele datové sady do VDF
            1. kterým je u číselníků vždy MV ČR, nikoliv poskytovatel číselníku
        2. pro zastřešující datovou sadu je navíc evidováno
            1. OVM, který zavádí veřejný číselník do RPP, jako poskytovatele číselníku
                1. což není poskytovatel datové sady s číselníkem do VDF, kterým je v případě veřejných číselníků vždy MV ČR, viz předchozí bod
        3. pro verzi číselníku je navíc evidováno
            1. lokální proprietární identifikátor či kód číselníku
                1. potřebné pro konstrukci lokálních IRI číselníků a jejich položek
                2. může vyplnit poskytovatel číselníku nebo je vygenerováno automaticky, pokud poskytovatel číselníků vlastní identifikátor či kód číselníku neeviduje
    4. pro datové sady reprezentující jednotlivé verze číselníku jsou navíc evidovány následující vazby, které nejsou evidovány pro zastřešující datovou sadu:
        1. Je verzí (reference na zastřešující datovou sadu)
        2. Má předchozí verzi (reference na datovou sadu s předchozí verzí číselníku, existuje-li)
3. zavedení nového veřejného číselníku poskytovatelem číselníku
    1. poskytovatel číselníku specifikuje metadata pro zastřešující datovou sadu číselníku
        1. lze převzít nebo jinak použít existující formulář pro registraci datové sady
    2. poskytovatel číselníku specifikuje metadata pro datovou sadu s první verzí číselníku
        1. může zvolit možnost kopírovat hodnoty zadané pro zastředující datovou sadu
    3. poskytovatel číselníku předá obsah první verze číselníku ručně v uživatelském rozhraní nahráním připraveného souboru s obsahem první verze veřejného číselníku v podobě definované otevřenou formální normou
    4. předchozí tři body lze realizovat také automatizovaně načtením seznamu veřejných číselníků poskytovatele z URL, které zadá
        1. seznam musí být zpřístupněn dle otevřené formální normy pro rozhraní katalogů otevřených dat.
        2. veřejné číselníky ale nemusí být pro účely předání zpřístupněny jejich správcem jako otevřená data.
    5. předaný obsah je zvalidován vůči otevřené formální normě pro číselníky
    6. obsah je uložen v podobě zkontrolovaného předaného datového souboru
        1. obsah veřejného číselníku pouze eviduje, ale nejsou nad ním stavěny žádné aplikační funkce
4. zavedení nové verze již zavedeného veřejného číselníku poskytovatelem číselníku
    1. stejný postup jako při zavádění nového veřejného číselníku, ale je zavedena pouze další verze číselníku zařazená pod zastřešující datovou sadu
    2. původní verze zůstává evidována včetně její publikace do VDF a jako otevřená data
5. funkcionality systému pro zpřístupnění údajů prostřednictvím VDF
    1. veřejné číselníky již jsou evidovány v podobě souborů s jejich jednotlivými verzemi v podobě

definované otevřenými formálními normami, čili je nutno pouze zajistit jejich předání do úložiště veřejných číselníků a datových sad RPP
    2. další veřejné údaje evidované v RPP již jsou získávány z interní databáze RPP a AIS působnostní v podobě definované otevřenými formálními normami a předávány do úložiště veřejných číselníků a datových sad RPP
6. funkcionality úložiště veřejných číselníků a datových sad RPP
    1. bude vytvořeno ze stávajícího úložiště obsahu datových sad publikovaných z RPP jako otevřená data
    2. jako doposud bude zpřístupňovat obsah RPP jako datové sady dle příslušných otevřených formálních norem ve formátech JSON, JSON-LD a prostřednictvím SPARQL endpointu
    3. zajistí také publikaci distribucí datových sad s verzemi veřejných číselníků evidovaných v RPP dle otevřené formální normy pro číselníky (formáty XML, CSV, JSON-LD a SPARQL endpoint)
    4. jelikož se jedná pouze o komponentu v rámci AIS působnostní, resp. RPP, není nutné zajišťovat všechny funkcionality přesně podle obecné architektury publikace veřejných údajů do VDF
    5. je nutné zajistit dostupnost nejen z veřejného internetu jako doposud, ale také prostřednictvím ISGOD (referenční rozhraní) a garantovat dostupnost
7. funkcionality lokálního katalogu otevřených dat pro katalogizaci datových sad publikovaných v úložišti veřejných číselníků a datových sad RPP
    1. zpřístupňuje do NKOD katalogizační záznam pro každou datovou sadu:
        1. datové sady zastřešující verze číselníků a datové sady s verzemi číselníků
            1. metadata o datových sadách jsou získány od poskytovatele
            2. metadata o distribucích jsou doplněny automatizovaně na základě vytvářených distribucí v úložišti
        2. datové sady s obsahem dalších veřejných údajů evidovaných v RPP (tj. ty, které jsou již dnes publikovány jako otevřená data)
            1. metadata jsou fixně předvyplněna
    2. je registrován pod MV ČR
8. označování údaje jako údaje kódovaného verzí veřejného číselníku
    1. včetně zaznamenávání IRI datové sady s touto verzí veřejného číselníku z NKOD
        1. Aby mohlo být IRI zaznamenáno, musí být daná verze veřejného číselníku nejprve do RPP zavedena, publikována do VDF a katalogizována v NKOD.
9. evidence veřejných údajů využívaných ohlášenou agendou

Kromě nových verzí veřejného číselníku existuje možnost, že je číselník kompletně nahrazen zcela novým číselníkem. V tom případě je skutečně zaveden jako zcela nový číselník bez vazby na původní číselník. Původní číselník ale zůstává evidován.

Číselníky kódující údaje evidované v RPP již nebudou publikovány jako otevřená data stávajícím mechanismem. Stanou se veřejnými číselníky, tj. budou evidovány v AIS působnostní a budou z něj publikovány do VDF a jako otevřená data standardním výše popsaným způsobem.

Pravidla čtení veřejných číselníků z VDF

Čtení veřejných číselníků včetně jejich obsahu jako celku v podobě datových souborů ke stažení (VDF), přístupu k jednotlivým položkám datových sad s verzemi číselníků (VDF a otevřená data) a dotazování prostřednictvím SPARQL endpointu (otevřená data) probíhá v rámci architektury pro čtení veřejných údajů popsané výše. Veřejné číselníky jsou dostupné dle otevřené formální normy pro číselníky.

Technická pravidla pro aplikační komponenty veřejného datového fondu

Úložiště datových sad

Úložiště datových sad je složeno ze 3 modulů:

- souborové úložiště distribucí datových sad
  - ukládá distribuce v podobě datových souborů
  - zpřístupňuje datové soubory distribucí prostřednictvím VDF a veřejného internetu
  - každý datový soubor je dostupný na jednom URL, které je stejné pro VDF i veřejný internet
    - nutno správně nastavit DNS pro KIVS/CMS a DNS pro veřejný internet
- modul pro validaci a transformaci distribucí dle příslušných otevřených formálních norem
  - kontroluje správné formátování a validitu
  - provádí transformace mezi jednotlivými formáty s využitím definic transformací v otevřených formálních normách
  - ukládá výsledky transformací do souborového úložiště a v případě RDF distribucí také do triplestore
  - bez definované otevřené formální normy pro daný typ dat není možné údaje prostřednictvím VDF zpřístupňovat
  - příslušnou otevřenou formální normu nebo normy získává modul z repozitáře otevřených formálních norem
- triplestore pro ukládání RDF distribucí
  - ukládá RDF distribuce datové sady dle otevřených formálních norem v triplestore (triplestore = databázový systém pro ukládání RDF dat v podobě trojic)
  - zpřístupňuje SPARQL endpoint pro dotazování nad RDF reprezentací a HTTP dereferenci IRI položek prostřednictvím rozhraní pro čtení distribucí jako otevřená data
    - lokální IRI položky je stejné pro VDF i veřejný internet, URL SPARQL endpointu stejné pro VDF i veřejný internet
      - nutno správně nastavit DNS pro KIVS/CMS a DNS pro veřejný internet

Směrovací služba pro veřejné číselníky a jejich položky

Jak bylo popsáno výše veřejný číselník bude podle otevřené formální normy pro číselníky zpřístupněn jako datový soubor ke stažení a prostřednictvím dereference IRI jednotlivých položek. Je tedy nutno určit tvar referenčních a lokálních IRI položek veřejných číselníků a také samotných číselníků. Ta jsou určena dle pravidel pro tvorbu IRI následovně:

- Referenční IRI číselníku:

https://vdf.gov.cz/číselníky-vdf/zdroj/číselníky/<ID číselníku v RPP>

- Referenční IRI verze číselníku k DDDD-MM-YY

https://vdf.gov.cz/číselníky-vdf/zdroj/číselníky/<ID číselníku v RPP>/<DDDD-MM-YY>

- Lokální IRI číselníku:

https://rpp-opendata.egon.gov.cz/odrpp/zdroj/číselníky/<ID číselníku v RPP>

- Lokální IRI verze číselníku:

https://rpp-opendata.egon.gov.cz/odrpp/zdroj/číselníky/<ID číselníku v RPP>/<DDDD-MM-YY>

- Referenční IRI položky číselníku:

<referenční IRI číselníku>/položky/<lokální kód položky>

- Lokální IRI položky číselníku:

<lokální IRI číselníku>/položky/<lokální kód položky>

Kde

- <ID číselníku v RPP> značí neměnné veřejné ID identifikující číselník v RPP
- <DDDD-MM-YY> značí datum vydání verze číselníku
- <lokální kód položky> značí kód položky číselníku v rámci daného číselníku

Pro potřeby sdílení veřejných číselníků je ve směrovací službě směrování výše uvedených referenčních IRI na lokální IRI přednastaveno a není potřeba, aby správce RPP nebo poskytovatelé jednotlivých číselníků směrování konfigurovali.

Dále je potřeba ve směrovací službě nastavit směrování na referenční IRI pro případy, kdy je znám pouze <lokální kód položky> a RPP identifikátor agendového údaje, jehož je hodnotou. Konfiguraci tohoto směrování provádí RPP. Kdykoliv ohlašovatel agendy uvede pro daný agendový údaj veřejný číselník, má RPP evidováno, kdo je poskytovatelem číselníku. Do směrovací služby tedy zaeviduje pravidlo pro směrování dvojice

(<RPP identifikátor agendového údaje>, <lokální kód položky>)

na referenční IRI

https://vdf.gov.cz/číselníky-vdf/zdroj/číselníky/<ID číselníku v RPP>/položky/<lokální kód položky>

Příloha 1: Metodika poskytování a čerpání údajů prostřednictvím VDF

1. Postupy zpřístupňování údajů prostřednictvím VDF
    - Určení údajů poskytovaných do VDF
    - Návrh podoby datových sad a jejich distribucí
    - Příprava informačního systému pro export dat
    - Export údajů do distribucí datových sad
    - Publikace distribucí datových sad
    - Aktualizace údajů, archivace a notifikace
    - Katalogizace datové sady
    - Registrace lokálního katalogu
    - Evidence odkazů na datové sady v RPP
2. Postupy čerpání údajů prostřednictvím VDF
    - Vyhledávání datových sad s údaji
    - Import údajů z datových sad do informačního systému
    - Příjem notifikací o změnách v datových sadách

Přístupy se liší nejen v tom, jaké údaje zpřístupňují a komu je zpřístupňují, ale také v několika dalších aspektech shrnutých v následující tabulce.

Příloha 2: Srovnání vlastností jednotlivých způsobů přístupu

	Přístup k PPDF	**Řízený přístup**	**Přístup k VDF**	**Otevřený přístup**
úroveň garance kvality obsahu	správnost, úplnost, platnost a aktuálnost	správnost, úplnost, platnost a aktuálnost	správnost, úplnost, platnost a aktuálnost	správnost, úplnost, pravidelné aktualizace pro zajištění maximální možné platnosti a aktuálnosti
úroveň garance zpřístupněných údajů pro výkon agend veřejné správy	vysoká dostupnost, formální správnost	bez garance pro výkon agend	vysoká dostupnost, formální správnost	bez garance pro výkon agend
sjednocený popis zpřístupněných údajů	RPP	bez popisu[1)]	RPP	bez popisu

centrální popis způsobu zpřístupnění údajů	TSÚA	NKOD	NKOD	NKOD
podoba definice datových formátů pro zpřístupnění	TSÚA	OFN	OFN	OFN
systém pro správu oprávnění	RPP	KUD	přístup bez omezení	přístup bez omezení
systém pro vedení evidence přístupu k údajům	RPP	KUD	KUD	bez evidence
identifikace subjektů a objektů práva	IČ a AIFO pro subjekty, proprietární id pro objekty	IRI	IRI	IRI

Prostorová data a služby nad prostorovými daty

Popis Prostorových dat a služeb nad prostorovými daty

Prudký rozvoj ICT umožnil a vyvolává i mnohem větší rozsah prací s informacemi o území a jejich využívání v životě celé společnosti. Tento vývoj klade zásadně nové požadavky na úpravu podmínek pro nakládání s prostorovými daty (data, jejichž nutnou součástí jsou údaje o poloze v prostoru vyjádřená zpravidla ve formě souřadnic a topologie) a prostorovými informacemi (informace získané interpretací prostorových dat a vztahů mezi nimi). Vzhledem k mimořádnému významu prostorových informací především pro ochranu obyvatelstva, předcházení živelním pohromám a zajištění ochrany životního prostředí, navrhla Evropská komise na počátku 21. století zřídit ve spolupráci s jednotlivými členskými státy Infrastrukturu pro prostorové informace (soustava zásad, znalostí, institucionálních opatření, technologií, dat a lidských zdrojů, která umožní sdílení a efektivní využívání prostorových informací a služeb) v Evropském společenství nazvanou INSPIRE. Obecná pravidla pro její zřízení (propojením infrastruktur pro prostorové informace budovanými a rozvíjenými jednotlivými členskými státy) byla stanovena Směrnicí Evropského parlamentu a Rady 2007/2/ES, o zřízení Infrastruktury pro prostorové informace v Evropském společenství (INSPIRE), která byla do českého právního řádu transponována zákonem č. 380/2009 Sb., kterým se mění zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů, a zákon č. 200/1994 Sb., o zeměměřictví a o změně a doplnění některých zákonů souvisejících s jeho zavedením, ve znění pozdějších předpisů. V průběhu implementace principů směrnice INSPIRE do národního prostředí se potvrdilo, že je účelné rozšířit principy INSPIRE nad rámec 34 témat prostorových dat směrnicí INSPIRE řešených a na jejich základě koordinovaně rozvíjet národní infrastrukturu pro prostorové informace (dále jen „NIPI“).

Na budování a využívání NIPI se různým způsobem a různou měrou podílejí veřejná správa (ústřední orgány státní správy, orgány územní samosprávy, bezpečnostní složky státu, složky IZS, …), profesní samospráva, výzkumné a vzdělávací instituce, komerční sféra, neziskové nevládní organizace i občané, přičemž dotčené subjekty vystupují v jedné i více rolích (vlastník, správce, provozovatel, pořizovatel, uživatel apod.). Významnou roli při budování NIPI hraje veřejná správa, neboť velké množství prostorových dat vzniká v procesech agend a informačních systémů veřejné správy. Rozvoj prostorových dat a služeb nad prostorovými daty a jejich využívání v rámci propojeného datového fondu je podmíněn standardizací datových modelů prostorových dat vytvářených jednotlivými agendami a standardizací služeb nad prostorovými daty. Standardizace služeb NIPI musí maximálně vycházet ze stávajících mezinárodních a evropských norem pro oblast prostorových dat a služeb nad prostorovými daty.

Pořízení a aktualizace prostorových dat používaných subjekty veřejné správy představuje soubor dlouhodobých, odborně, technicky, organizačně a finančně náročných úkolů. Do tohoto dlouhodobého procesu vstupují skutečné a nepřetržité změny v území, měnící se požadavky uživatelů, potřeba harmonizace datových sad na různých úrovních rozlišení podrobností, možnosti technologií a další vlivy.

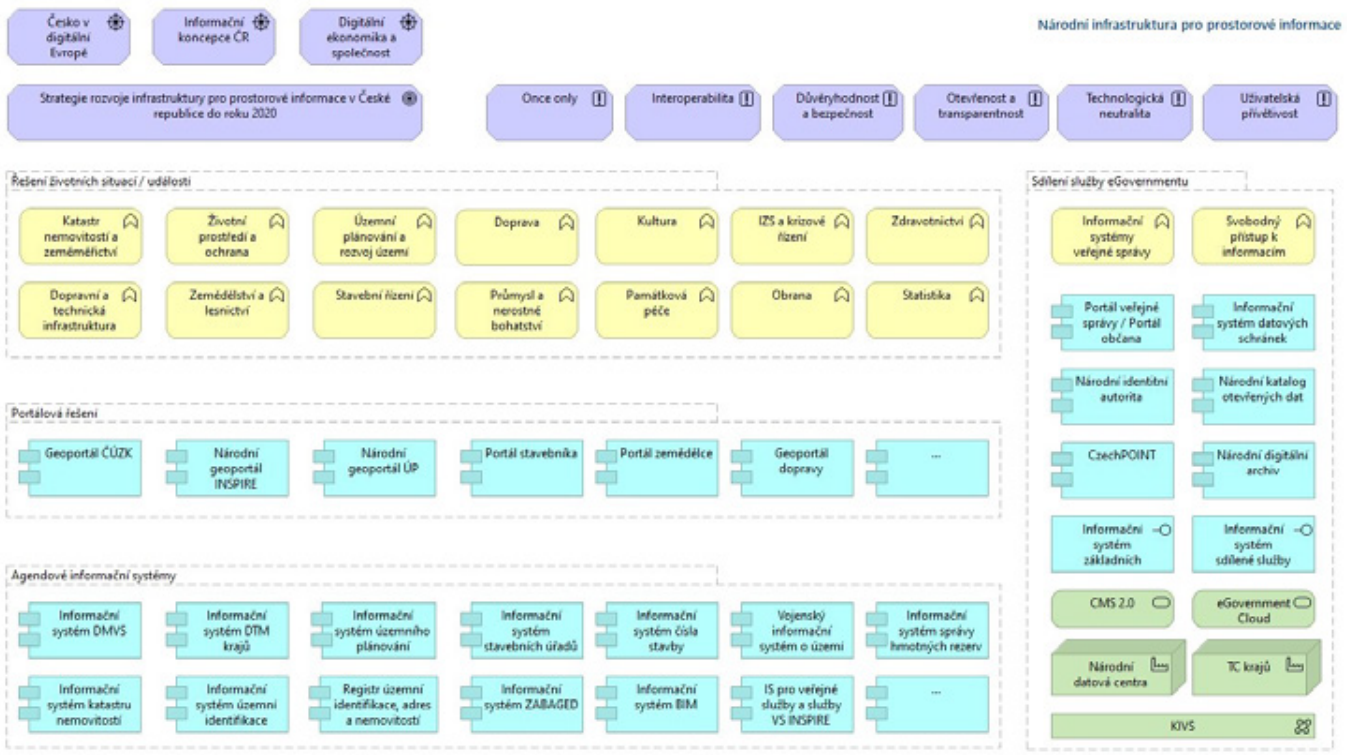
V oblasti poskytování služeb pro zpřístupnění prostorových informací hraje zásadní roli směrnice evropského parlamentu INSPIRE, která v rámci prováděcích předpisů specifikuje požadavky na interoperabilní síťové služby. Specifikace využívá webové služby založené na standardech OGC – Web Map Service (WMS), Web Map Tile

Service, Web Feature Service (WFS), Web Coverage Service apod. Interoperabilitu služeb pro zpřístupnění prostorových informací na národní úrovni je proto možné zajistit relativně snadno oproti časově, kapacitně a finančně náročnější harmonizaci datových sad. Ve výsledku jsou síťové služby požadované INSPIRE používány v rámci národní i evropské infrastruktury pro prostorové informace, zatímco harmonizované datové sady jsou poskytovány paralelně s neharmonizovanými. Existující vyhledávací (katalogové) služby, prohlížecí služby, služby stahování dat a služby transformační odpovídající požadavkům INSPIRE lze považovat za klíčové prvky NIPI, které již plní základní cíle, tj. zpřístupnění a sdílení prostorových informací mezi jinak heterogenními IS. Tyto služby jsou podobně jako soubory prostorových informací opatřeny metadaty (data, která popisují struktury a obsahy sad prostorových dat, prostorové služby a jiné složky IS; umožňují a usnadňují jejich vyhledávání, třídění a používání). Metadata jsou poskytovateli služeb zpřístupněna prostřednictvím katalogové služby podle standardu OGC CSW (Catalogue Service for Web), která umožňuje aplikacím, které ji umí konzumovat, vyhledávání v metadatech, například podle tzv. klíčových slov.

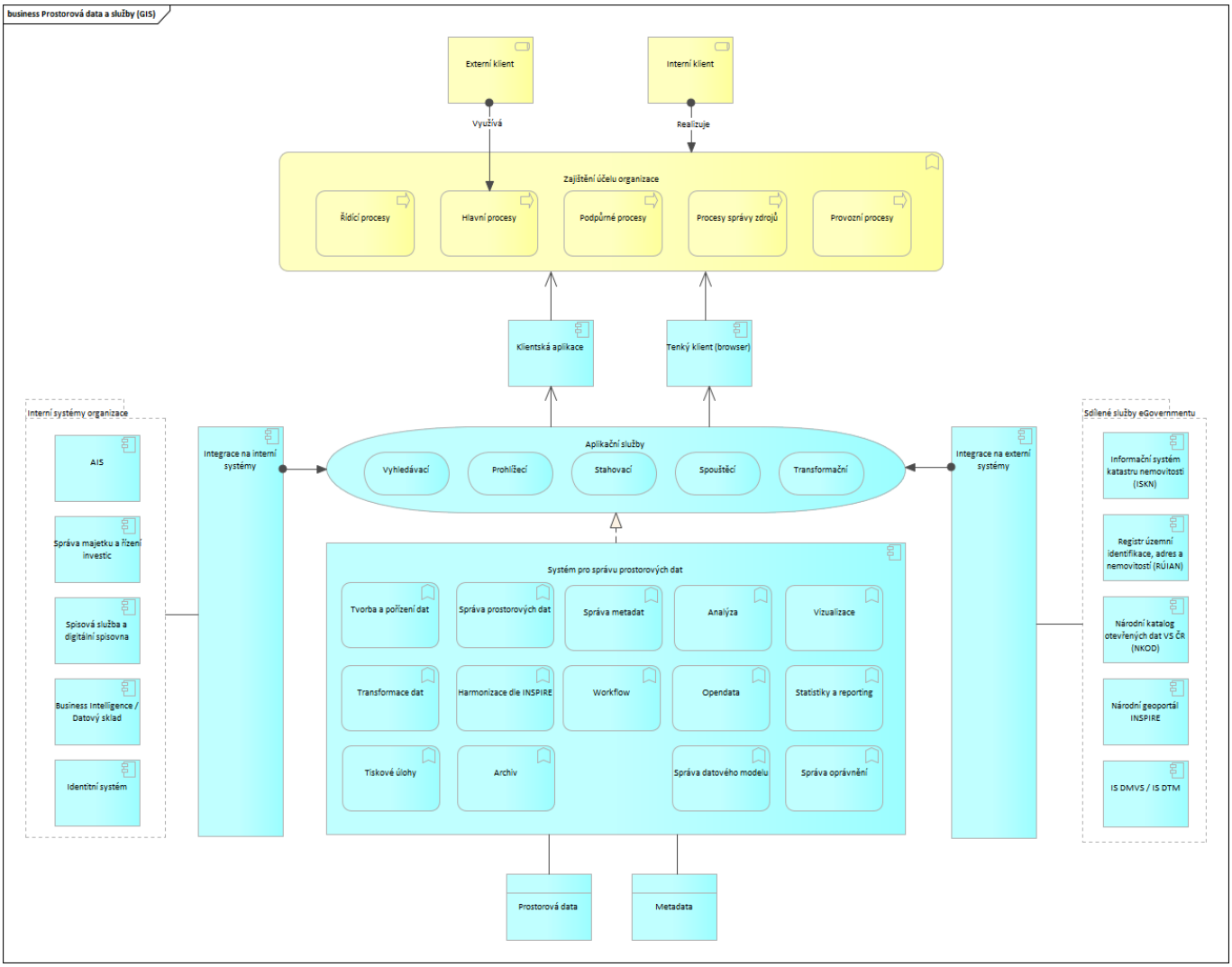
Služby založené na prostorových datech

Národní infrastruktura pro prostorové informace (NIPI): Běžně dostupné služby v rámci NIPI jsou služby, které umožňují vyhledání a zpřístupnění metadat (katalogové služby), zpřístupnění prostorových dat nejčastěji k náhledu (obvykle nazývány zjednodušeně jako služby mapové); v poslední době jsou běžné také služby stahování dat (online nebo formou předpřipravených datových sad). Méně časté, ale stále se rozvíjející, jsou služby analytické. Tvorba, správa a aktualizace prostorových dat a jejich zpřístupnění k náhledu nebo dalšímu užití má v České republice dlouhou tradici, která je podporována trvalým zájmem uživatelů. Tyto služby zpřístupňuje veřejná správa, méně pak soukromé firmy. Stejně jako u prostorových dat stanovení minimálních požadavků na tyto služby případně jejich zakotvení v české legislativě bude koordinováno v rámci plnění Akčního plánu GeoInfoStrategie.

Schéma NIPI



Systémy a služby prostorových dat



Pravidla Prostorových dat a služeb nad prostorovými daty

Veřejná správa využívá prostorová data ve všech agendách (a jsou jejich nedílnou součástí), které zajišťuje, např. se jedná o agendy v oblastech dopravy, regionálním rozvoji, ochraně životního prostředí, územním plánování, stavební činnosti, zemědělství, lesnictví, při řešení daňových potřeb státu, v oblasti evidence a správy majetku, pro ochranu kulturního dědictví. Prostorová data mají mimořádný význam pro bezpečnost státu, ochranu obyvatelstva, pro předcházení haváriím a živelním pohromám a řešení mimořádných situací. Aktuální, jednotná a rychle dostupná prostorová data jsou nezbytná pro kvalitní operační a krizové řízení na všech úrovních.

Pro zajištění sdílení a efektivního využívání prostorových dat a informací je nezbytné vytvořit odpovídající soustavu zásad, znalostí, institucionálních opatření, technologií, dat a lidských zdrojů, která se označuje jako infrastruktura pro prostorové informace. V řadě zemí je národní infrastruktura pro prostorové informace (NIPI) upravena a definována, v České republice doposud ucelené, přehledné, systematické a formálně zakotvené stanovení NIPI schází, proto byla alespoň stanovena strategie rozvoje této infrastruktury, viz Strategie rozvoje infrastruktury pro prostorové informace v České republice do roku 2020.

Aby bylo možné NIPI efektivně budovat, je kromě centrálních prvků infrastruktury a sdílených služeb, vhodné definovat typovou funkcionalitu (na obecné úrovni) pro informační systém spravující prostorová data jako součást informačních systémů veřejné správy příslušného orgánu veřejné moci. Protože prostorová data a služby jsou pouhým nástrojem pro podporu výkonu agend veřejné správy, ať již na úrovni státní správy, tak i na

úrovni samosprávy, je pro stanovení obecného modelu na úrovni business architektury zásadní definovat klíčové konzumenty poskytovaných služeb ve formě agend a činností (dle terminologie základního registru agend orgánů veřejné moci a některých práv a povinností). Je zřejmé, že business vrstva bude odlišná pro jednotlivé segmenty, nicméně vykazuje určité společné rysy, zejména v řídících, podpůrných a provozních činnostech. Z pohledu podpory tzv. hlavních činností je důležitá vazba na Registr práv a povinností zakládající určité kompetence pro výkon konkrétních agend ve smyslu vazby na legislativu a jednotlivé aktéry (účastníky).

Uplatnění prostorových dat a služeb lze tedy fakticky nalézt ve všech oblastech, typicky, bez ohledu na konkrétní segment, při:

- formulování strategických dokumentů souvisejících zejména s rozvojem území, služeb a segmentů (např. zdravotnictví, školství, sociální služby) či správou zdrojů,
- podpoře výkonu agend veřejné správy související např. s územním plánováním, výstavbou, životním prostředím, dopravou, památkami, lesním hospodářstvím či integrovaným záchranným systémem,
- správě majetku, zejména při evidování, údržbě a opravě, investování (např. budovy, pozemky, komunikace, zeleň, infrastruktura),
- plánování kontrolních činností či řízení rizik v kontextu prostorových souvislostí.

Součástí business architektury je rovněž identifikace klíčových aktérů. Mezi externí lze zařadit veřejnost (fyzické osoby, fyzické osoby podnikající, právnické osoby), odbornou veřejnost, partnery a dodavatelé. Mezi interní patří např. politická reprezentace, vedení OVM, zaměstnanci vykonávající konkrétní agendy a činnosti a také zástupci ICT útvaru jako poskytovatelé ICT (GIS) služeb. Při popisu aplikační architektury je kromě vlastní funkcionality týkající se tvorby a správy prostorových dat potřebné se zaměřit také na sdílení dat nejen uvnitř vlastní organizace, ale také vůči ostatním informačním systémům veřejné správy.

Vlastní funkce systému pro správu prostorových dat tvoří na obecné úrovni zejména:

- tvorba a pořízení dat
- správa prostorových dat
- správa metadat
- transformace dat
- vizualizace
- analýzy
- workflow
- statistiky a reporting
- harmonizace dat INSPIRE
- tiskové úlohy
- opendata
- archiv

Pro publikaci a sdílení jsou klíčové služby vyhledávací služby, prohlížecí, stahovací, transformační a spouštěcí. Z pohledu vnitřního propojení s ostatními prvky ICT infrastruktury organizace jsou zásadní integrace na:

- Agendové informační systémy (např. stavební a územní řízení, státní správa lesů, památková péče), kde GIS pomáhá zejména s vizualizací agendových údajů v mapě, vizualizací souvislostí či trendů, s jejich tematizací.
- Elektronický systém spisové služby včetně spisovny; vztah mezi spisovou službu a digitální spisovnou a GIS není zpravidla realizován, přestože množství vstupů a výstupů z GIS má charakter dokumentu v kontextu zákona č. 499/2004 Sb. a národního standardu (NSESSS). GIS se v takových případech chová jako samostatná evidence dokumentů, nicméně nerespektuje příslušné legislativní povinnosti. Jedním z možných řešení je realizace vazby právě na spisovou službu.
- Správa majetku a řízení investic, kdy majetek je primárně evidován a spravován v ERP (zpravidla v provázaných modulech evidence a údržby majetku a řízení investic s vazbou na účetní evidenci a rozpočet). Pro správu majetku jsou klíčová data katastru nemovitostí (vedená v ISKN) obsahující jak popisnou, tak i grafickou složku. Tato data ISKN jsou zpravidla v pravidelných intervalech dávkově aktualizována (lze však rovněž využít webových služeb dálkového přístupu katastru nemovitostí ČÚZK), přičemž dochází k často k duplicitní správě dat (včetně pravidelných aktualizací) rovněž v GIS. Optimální

je zajistit společnou správu referenčních dat, zajistit jejich sdílení a vzájemnou iteraci na úrovni klientů.

Mezi klíčové, z pohledu vnější integrace na sdílené prvky eGovernmentu, patří:

- Registr územní identifikace, adres a nemovitostí
- Informační systém katastru nemovitostí
- Národní geoportál INSPIRE
- Digitální technická mapa ČR (IS DMVS)
- Informační systém identifikačního čísla stavby

Úplné elektronické podání

Popis úplného elektronického podání

Úplné elektronické podání (také jako "ÚEP") je možné popsat tak, že klient/občan, ale i zástupce právnické osoby, má možnost vyřídit všechnu svou potřebnou agendu životní situace, prostřednictvím elektronické interakce samoobslužně kdykoli a odkudkoli či asistovaně z kteréhokoli univerzálního kontaktního místa VS, bez nutnosti osobní návštěvy na příslušných úřadech, a následně možnost mít přehled o stavu a vývoji všech svých řešených životních událostí.

Současně pojem ÚEP představuje pokročilou variantu elektronického podání (elektronické formy úkonu klienta, občana a/nebo organizace vůči veřejné správě ČR), která splňuje sadu požadovaných vlastností, daných primárně tzv. architektonickými principy eGovernmentu a dále vlastnosti předpokládané pro podání vůči veřejné správě právními předpisy, zejm. správním řádem a agendovými zákony.

Elektronické podání klienta vůči veřejné správě je považováno za úplné, pokud splňuje všechny architektonické principy eGovernmentu a další náležitosti, zejména pak:

- Podporuje princip Digital by Default tím, že je navrženo jako vnitřně plně digitální (nikdy se nemusí tisknout nebo osobně řešit), s tím, že ale podporuje asistovanými formami i tzv. elektronicky handicapované.
- Podporuje princip Whole-of-Government tím, že je dostupné rovnocenným způsobem ve všech elektronických kanálech eGovernmentu (samoobslužných i asistovaných), s upřednostněním univerzálních kontaktních míst (CzechPOINT a PO v PVS).
- Podporuje princip Once only tím, že pro předvyplnění formuláře i pro navigaci a volbu služby jsou využity všechny údaje o klientovi, které veřejná správa má a ze zákona je v dané situaci smí použít.
- Podporuje principy Interoperability by Default a Cross-border by default tím, že umožňuje elektronicky obsloužit všechny klienty, rezidenty ČR a EU, pro které je úkon relevantní, a to i vzdáleně ze zahraničí.
- je po podání automatizovaně strojově zpracováno, převedeno do transakčního záznamu agendového informačního systému.
- Podporuje princip Inclusion and Accessibility tím, že podporuje asistovanými formami i tzv. elektronicky (nebo jinak) handicapované.
- Využívá Jednotný identitní prostor veřejné správy a Elektronickou identifikaci pro klienty veřejné správy .
- Umožňuje klientům učinit podání skrze různá elektronická rozhraní (webová stránka, formulář nebo asistovaná služba) a sledovat průběh vyřizování jejich podání skrze to samé rozhraní, přes které bylo podání realizované nebo jiné klientem určené.

Všechny obslužné kanály veřejné správy musí být cílově vzájemně integrovány tak, aby mezi nimi bylo možno libovolně přecházet i v průběhu vyřizování podání a aby všechny informace byly zachovány, přenášely se do nich (mezi nimi).

Pravidla úplného elektronického podání

Úřad musí respektovat všechny návazné funkční celky jako např. propojený datový fond, portály veřejné správy či komunikační infrastrukturu veřejné správy a procesně zajistit zpracování podání tak, aby probíhalo elektronicky po celou dobu jeho životního cyklu.

Úřad pro splnění požadavků kladených na úplné elektronické podání musí splnit svými obslužnými kanály (např. portál):

- Využití Jednotného identitního prostor veřejné správy pro úřední osoby a Elektronickou identifikaci pro klienty veřejné správy.
- Předvyplnění podání všemi státu známými údaji klientovi po prokázání elektronickou identitou. Zajištění tohoto požadavku se splní čerpáním údajů z Propojeného datového fondu.
- Má služby svých agend v rámci ÚEP a jejich IT aplikace navrženy tak, aby služby bylo možno v obslužných kanálech kombinovat pro efektivním řešení životních událostí.
- Umožňuje klientům učinit podání skrze různá elektronická rozhraní (webová stránka, formulář nebo asistovaná služba) a sledovat průběh vyřizování jejich podání skrze to samé rozhraní, přes které bylo podání realizované nebo jiné klientem určené.
- Postupně všechna existující práva a povinnosti ze vztahu k VS budou doprovázena transakční službou (nejenom popisem návodu) v Portálu občana, a to v těch všech případech, kdy elektronická transakční služba bude proveditelná a bude odpovídat oprávněným zájmům klientů a současně i úřadů.
- Elektronické podání formou ÚEP lze uskutečnit i papírově (off-line), tzn. půjde stáhnout předvyplněný formulář, ručně vyplnit, zaslat datovou schránkou nebo elektronicky podepsané doručit jakkoli jinak (i mailem, vložením do portálu), případně vložit do elektronické aplikace úřadu.
- V případě menší četnosti podání stačí jeden z obou kanálů (on-line nebo off-line), musí však umožňovat dobrou (personalizovanou) navigaci ke službě a k jejímu předvyplnění.
- Stejnou službu lze získat s pomocí služby úředníka na kterémkoli fyzickém kontaktním místě asistovanou formou. Pro typové a jednoduché podání pro řešení typových životních situací to takto bude možné na Univerzálních asistovaných kontaktních místech.
- Zůstanou zachovány tradiční kanály pro příjem listinných podání osobně, diktátem do protokolu nebo poštou – úřední přepážky a podatelny. Jejich úkolem ale bude obdržené vstupy neprodleně plně digitalizovat, aby celé další následné zpracování bylo jednotně plně elektronické.
- Nedílnou součástí řady podání je splnění finanční povinnosti (poplatku, daně). Platební brána tedy musí být součástí obslužného rozhraní. Pro agendy v samostatné působnosti je platební brána plně v zodpovědnosti koncového úřadu, pro agendy v přenesené působnosti musí o způsobu rozhodnout správce agendy.
- Elektronické samoobslužné služby pro klienty/občany i pro právnické osoby musí být doplněny interaktivním podpůrným a poradenským kanálem (service-desk, call-me-back, apod.).
- Podání nemusí vždy činit ta osoba, která je přihlášena elektronickou identitou, ale může se jednat o osobu zastupující jinou osobu. Úřad tedy musí zajisti správu mandátů.
- Pro individuální přizpůsobení uživatelského rozhraní musí úřad využívat tzv. klientské profily. Každý jedinečný a jednoznačně identifikovaný klient má profil jenom jeden. V tomto profilu jsou uchovávány osobní i agendové údaje ve shodě se pravidly správy údajů Právní aspekty pro pseudonymizaci.
- Podání zadané či zpracované v rámci řešení pro ÚeP musí být vždy přijímáno na podatelně a evidováno v systému eSSL nebo samostatné evidenci dokumentů v souladu se zákonem o archivnictví a spisové službě. Jejich přijetí musí být potvrzeno příslušnou odpovědní zprávou.

Integrace informačních systémů

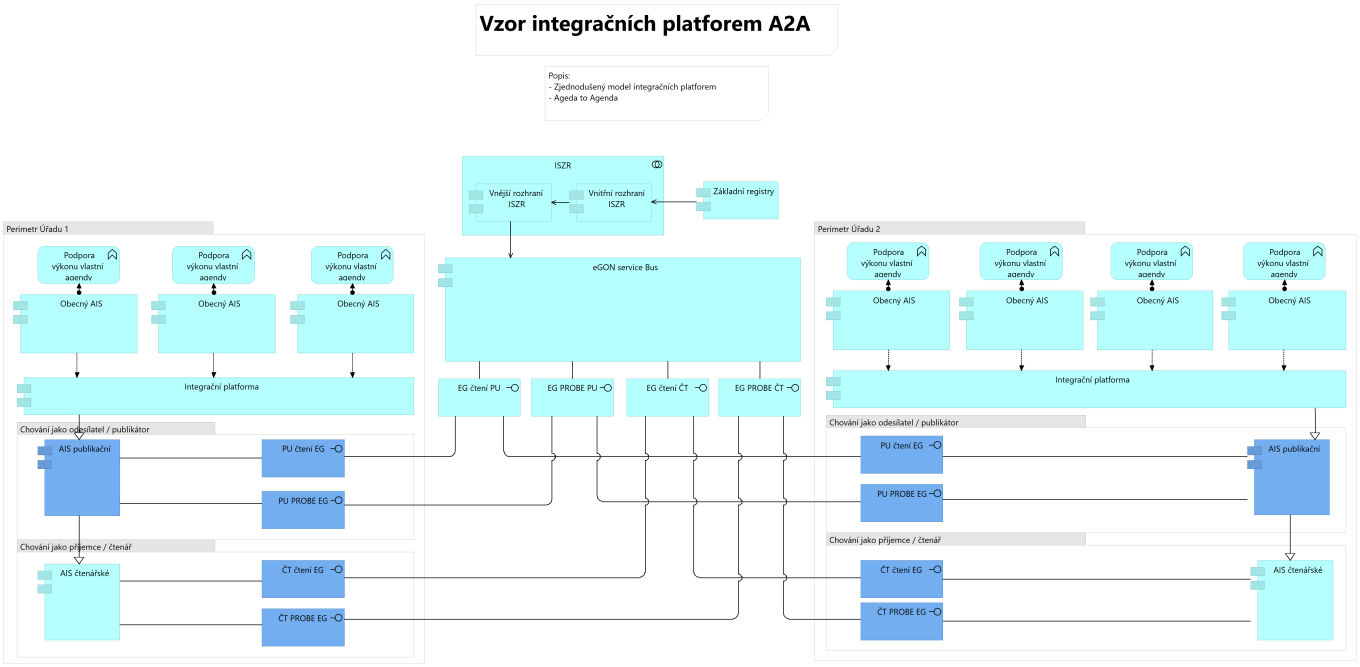
Popis Integrace informačních systémů

Z ostatních částí NAP lze vyvodit určité povinnosti pro integraci mezi jednotlivými informačními systémy. Je nutno rozlišovat, zda se jedná o vnitřní či vnější integraci a také, jaké údaje a za jakým účelem se v integraci vyměňují. Integraci informačních systémů můžeme rozdělit následovně:

1. Integrace uvnitř jednoho ISVS mezi více komponentami

2. Integrace uvnitř systémů jednoho správce (vnitřní integrace)
    - mezi dvěma informačními systémy veřejné správy
    - mezi informačním systémem a systémem spisové služby a mezi informačním systémem a jmenným rejstříkem
    - mezi ISVS a provozním informačním systémem
    - na portál za účelem zveřejnění
3. Integrace na systémy jiného správce (externí integrace)

Integrace na systémy jiného správce s pomocí eGSB / ISSS



Pravidla Integrace informačních systémů

Vnitřní integrace u jednoho správce či v jednom AIS

Integrace mezi informačními systémy jednoho správce je primárně zodpovědností a oblastí onoho správce. To neznamená, že taková integrace nepodléhá splnění EG principů, ale primárně se jí OHA nezabývá, dokud správce ISVS doloží soulad se zde uvedenými principy (jako je evidence subjektů, nebo propojený datový fond).

Technicky je doporučenou optimální metodou vybudovat jednu integrační platformu a integraci mezi jednotlivými informačními systémy zajistit formou služeb volaných a orchestrovaných v této integrační platformě. I při integraci (respektive výměně údajů mezi jednotlivými IS či agendami se musí ale myslet například na řádné logování transakcí a audit zpracování osobních údajů, zejména pokud se jedná o údaje o fyzických či právnických osobách.

Pro vnitřní integraci ale vždy platí následující:

- Jako identifikátor subjektu pro výměnu údajů i ve vnitřní integraci se využije AIFO, pokud se integrace zajišťuje překladem přes eGSB/ISSS.
- Pokud se integrace odehrává jen v perimetru správce, a tedy mimo překlad přes eGSB/ISSS, tak se jako identifikátor využije buď klientské číslo, nebo stykový identifikátor. To platí i v multiagendovém provozu, kdy jsou subjekty integrovány v jedné evidenci jednoho AIS sloužícího pro podporu více agend.
- Identifikátor AIFO se v žádném případě nevyužije při integraci AIS na provozní systémy, pokud tyto systémy nevyužívají AIFO v jejich agendě. V případě integrace subjektů mezi AIS a provozními systémy,

které nemají pro subjekt přidělené AIFO v podporované agendě, se využije klientský identifikátor.
- AIFO se neeviduje a neposkytuje ve společných evidencích a v multiagendových AISech, AIFO se v takovém případě využije jen pro vnější integraci a pochopitelně pro ztotožnění a aktualizaci údajů pro konkrétní agendu. Mezi více agendami v jednom ISVS se pro propojení využije klientský identifikátor a AIFA jsou zapsána jen v komponentách AISu pro jednotlivé agendy, nikdy ve společné evidenci. Při vnější integraci pak volá AIS přes společnou evidenci službu eGSB/ISSS či ISZR prostřednictvím svého AIFO.

Vnitřní výměna údajů o subjektech

Při vnitřní integraci mezi komponentami a systémy jednoho správce se primárně AIFO nevyužívá, protože se využije klientský identifikátor. Pomocí klientského identifikátoru a vazby všech údajů vedených o subjektu ve všech agendách (vždy přes jednotlivý AIS) se dá naplnit povinnost nevyžadovat již jednou vedené údaje a v kombinaci s jednotnou evidencí případů lze snadno zajistit povinnosti poskytnout subjektu práva z ISVS a mít přehled o údajích, které o něm vedeme a o rozhodných skutečnostech, které se ho týkají.

Pokud se jedná o integraci mezi AIS a provozními informačními systémy, tak provozní IS kromě ESSL nevyužívají AIFO ve svých agendách. I proto je nutno využívat klientský identifikátor, nebo si na úřadě zavést jiný klidně i neveřejný identifikátor, kterým provážeme údaje vedené i v provozních systémech. V žádném případě k tomu nevyužíváme některý z AIFO identifikátorů, kterým bychom nahrazovali vlastní identifikátor v úřadu.

Vnější integrace na AIS jiného správce

Při vnější integraci se v maximální míře využívá referenční rozhraní, a to zejména eGSB/ISSS jako technický způsob výměny údajů o subjektech a objektech práva. Technická realizace integrace prostřednictvím eGSB/ISSS se řídí příslušnou provozní dokumentací eGSB/ISSS.

Při vnější integraci se využije:

- při výměně údajů o subjektu (fyzická osoba) překlad AIFO identifikátorů, nikdy se nevyužije přímá výměna prostřednictvím jiného identifikátoru,
- při výměně údajů o objektu (třeba vozidlo) jeho identifikátor (třeba RZ), ale je-li součástí i sada údajů o subjektu, pak se u fyzických osob (třeba vlastník vozidla) využije opět překlad AIFO mezi dvěma agendami.

Vnější výměna údajů o subjektech

Při výměně údajů v rámci propojeného datového fondu se vždy využije mechanismus výměny prostřednictvím překladu agendových identifikátorů (AIFO) přes ORG. Integrace se uskutečňuje prostřednictvím služeb eGSB/ISSS. I v situaci, kdy OVM vede některé další identifikátory o subjektu, vždy postupuje v souladu s § 8, odst. 3, zákona o základních registrech a využije volání služby poskytované agendovým informačním systémem poskytujícím údaje, službu volá přes eGSB/ISSS a volá ji s identifikací subjektu svým AIFO, kdy následně eGSB/ISSS zajistí překlad AIFO, poskytující AIS pak opět přes eGSB/ISSS zašle odpověď, a to zase s přeložených AIFO tazatele. Jiné identifikátory tedy nejsou nutné.

Obě strany integrace pochopitelně všechny transakce logují a samotné eGSB/ISSS uchovává informaci o využití služby.

Chce-li nějaké OVM získat z jiného AISu údaje o subjektu, musí si nejprve daný subjekt ztotožnit a mít k němu přidělené AIFO své agendy. Nezíská-li od poskytovatele údaje třeba proto, že nejsou správně nastavena oprávnění k údajům v RPP, nebo protože poskytovatel nemá řádně ztotožněný subjekt a nemá k němu AIFO, reklamuje to u poskytovatele jako porušení povinností podle zákona o základních registrech. Poskytovatel pak zjedná nápravu.

Pozor: U údajů takto získaných z jiných agend se jedná o údaje, které úřad vede (i když je technicky získal z jiného AIS), a tedy úřad musí postupovat podle paragrafu 6, odst. 2, Správního řádu a po subjektu je nevyžaduje a nepožaduje jejich doložení.

Portály veřejné správy a soukromoprávních uživatelů údajů

Popis Portálů veřejné správy a soukromoprávních uživatelů údajů

Portál je vnímán jako celý funkční celek obsahující Front-end (logika zobrazující chování směrem ke klientovi) i Back-end (logika realizující chování systému a vnitřní i vnější integraci) realizující všechny typy služeb dle Informační koncepce ČR - Informační, Interaktivní a Transakční. Z tohoto mimo jiné vyplývá, že portál je informačním systémem veřejné správy.

- V oblasti informačních služeb poskytuje uživatelům přehled a veřejně dostupné informace z oblasti, kterou portál obsahuje včetně popisu životních situací.
    - V informační části není potřeba řešit identifikaci, autentizaci a autorizaci uživatele.
- V oblasti interakčních služeb poskytuje uživatelům personifikované údaje s využitím vícero informačních kanálů, zpětnou vazbu mezi jeho konáním, a to včetně historie.
    - Interakční služby vyžadují identifikaci, autentizaci a autorizaci uživatele.
- V oblasti transakčních služeb poskytuje uživatelům podání všech typů, včetně provedení platby nebo rezervace termínu pro prezenční jednání, získání potvrzení a doručení rozhodnutí úřadu.
    - Transakční služby vyžadují identifikaci, autentizaci a autorizaci uživatele.

Portály tedy nemohou být samostatné a nepropojené aplikace, ale naopak musí se jednat o prostředek, který je integrován s informačními systémy v úřadu. Především s elektronickou spisovou službou, s agendovými informačními systémy, ale třeba i s ekonomickými systémy tam, kde se jejich prostřednictvím shromažďují údaje o výplatách či o poplatcích podle jednotlivých klientů. V případě poskytování všech 3 typů služeb se jedná o tzv. integrované on-line služby veřejné správy dle Informační koncepce ČR.

Portál má sloužit klientovi k získání informací, jako prostředek pro publikování otevřených dat, statistik a veřejných výstupů, pro elektronická podání a komunikaci klienta s úřadem. Portál musí též sloužit i držitelům zaručené elektronické identifikace jako prostředek pro získání jejich údajů, pro různé notifikace, ale třeba i pro interaktivní podání žádostí, či podání žádostí o výpisy. Klientovi musí poskytnout též tzv. profil neboli personifikovanou část, kde si portál drží základní údaje o klientovi, které zná úřad nebo které klient sdělit sám ze své vůle.

Celkové chování a interakce Portálu vůči občanům i úředníkům se nazývá User Experience (UX). Do UX patří nejen grafická podoba, ale také jazyk (forma, odbornost, …), způsob interakce, komunikační kanály, obdobné způsoby identifikace uživatelů atd. Pro snadné používání občanem je nutné, aby každý portál používal jednotné, centrálně defikované UX. Zjednodušeně řečeno jde o obdobu chování a interakce, jakou má popsaný Portál občana.

Centrální (federující) portály

Centrálními (federujícími) portály jsou myšleny portály, které sdružují informace z dílčích portálů, zprostředkovávají interakci s portály nižší úrovně – federovanými portály (agendové a území). Na rozdíl od portálů nižší úrovně je centrálních (federujících) portálů spočetně méně a slouží především klientům pro snadné vyřízení jeho potřeb na jenom místě. V současné době jsou takovýmito portály pouze Portál veřejné správy a Portál občana (PO a PVS).

Portálem občana je myšlena transakční část Portálu veřejné správy, kde klient/občan může skrze samoobslužné služby pod svou zaručenou elektronickou identitou činit podání vůči veřejné správě a využívat její služby. Více je v samostatném funkčním celku

Agendový portál

Agendovým portálem je myšlen portál poskytující služby logicky centralizovaného systému či systémů pro jiné orgány veřejné správy a klienty veřejné správy. Typicky jde tedy o portál správce agendy, ve kterém lze řešit služby agendy bez ohledu na místní příslušnost. Platí, že služby pro klienta musí být součástí federace a jejich služby přístupné v centrálních (federujících) portálech.

Portál území

Portálem území je myšlen portál poskytující služby, které spadají pod určité území ČR, typicky kraj, obec, město, městská část, souhrnně možno označit za samosprávy. Portál území může obsahovat kromě samosprávních služeb jako např. správa místních poplatků, i služby přenesené, avšak neměla by nastat situace, kdy je služba přenesené působnosti vytvořena jen pro portál území. Je zodpovědnost věcného správce, aby vytvořil centrální prostředí pro vyřizování služeb přenesené působnosti, které portál území využije, ale nevytváří. Platí, že služby pro klienta musí být součástí federace a jejich služby přístupné v centrálních (federujících) portálech.

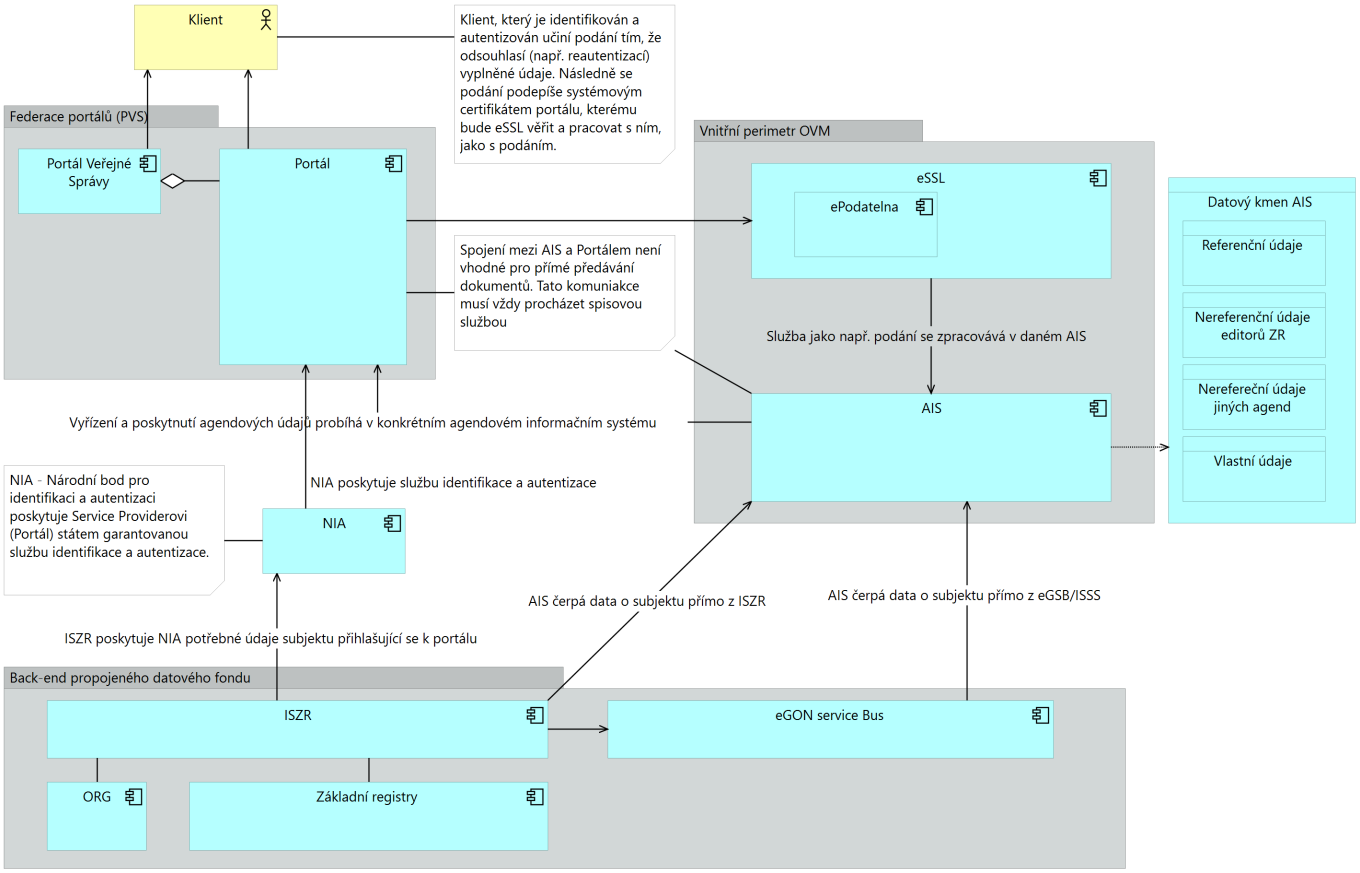
Portál soukromoprávního uživatele údajů

V případě portálu soukromoprávního uživatele údajů (také jako SPUÚ) se jedná o situaci, kdy vlastník portálu není orgán veřejné moci, ale dle své povahy je podřízen zákonu 111/2009 Sb. Může se jednat o portály poskytovatelů zdravotních služeb, soukromých pojišťoven, bank, státních podniků, apod. Takovéto portály poskytují služby, které mohou být federovány do Portálu občana, avšak pouze za předpokladu, že SPUÚ je ohlášen v rejstříku a má povinnost elektronicky ověřovat totožnost klienta.

Pohledy na portály veřejné správy

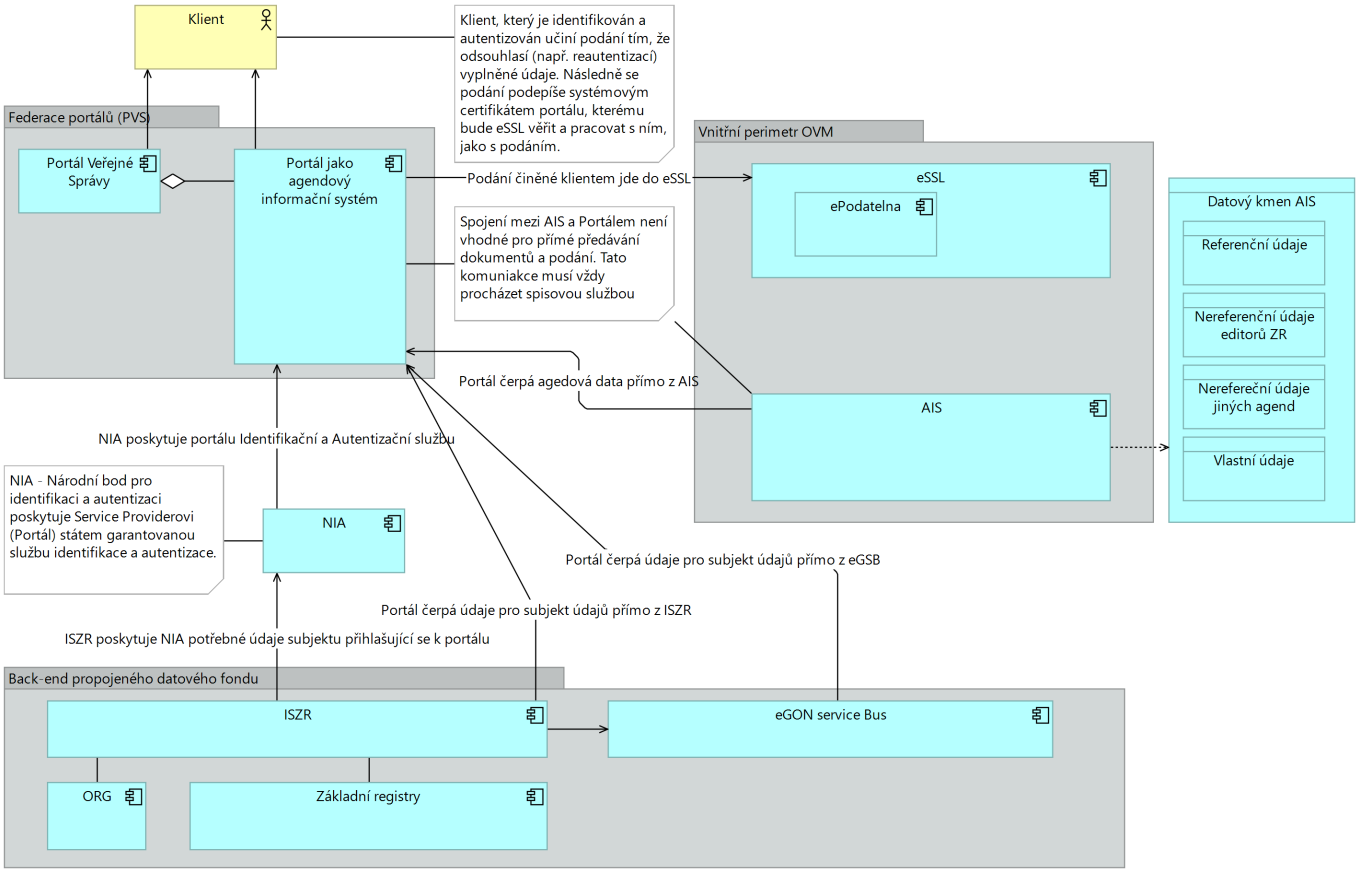
Obyčejný portál

Obyčejným portálem se v tomto smyslu myslí všechny druhy portálů dle jejich zaměření, jak je uvedeno výše, avšak tento diagram zobrazuje práci s daty. Obyčejný portál se chová jako jednotné rozhraní sloužící pro vyřízení služby, avšak její faktické vyřízení probíhá v agendovém informačním systému. Portál si obstarává veškeré údaje a další informace, které klientovi poskytuje, prostřednictvím agendového informačního systému a veškeré dokumenty, které při vyřizování služby vzniknou se musí dostat do spisové služby.



Portál jako Agendový informační systém

Portálem jako Agendovým informačním systémem se v tomto smyslu myslí všechny druhy portálů dle jejich zaměření, jak je uvedeno výše, avšak tento diagram zobrazuje práci s daty. Portál jako Agendový informační systém se chová jako samostatný agendový informační systém, tedy kromě samotného rozhraní pro příjem a vyřízení služby obsahuje i veškerou logiku a podporuje procesy pro její vyřízení. Portál si obstarává veškeré údaje a další informace, které klientovi poskytuje, prostřednictvím přímého napojení na informační systém základních registrů, eGSB/ISSS nebo AIS, které spravuje stejný správce jako portál. Nadále platí, že veškeré dokumenty, které při vyřizování služby vzniknou se musí dostat do spisové služby.



Pravidla Portálů veřejné správy a soukromoprávních uživatelů údajů

Úřad musí při provozování portálu zavést a změnit současné procesy orientované především na osobní kontakt s klientem. Současné portály již musí disponovat funkcionalitou propojení se zaručenou identitou dle zákona 250/2017 Sb. a musí se umět přizpůsobit situaci, kdy klient veřejné správy bude komunikovat pouze elektronicky. Začíná se tedy samotným uživatelsky přívětivým prostředím, které musí být v souladu s grafickým manuálem MVČR. Dále je potřeba formulářový engine, který umožní nejen předvyplnit veškeré státu již známé údaje z propojeného datového fondu a elektronické identity poskytnuté národní identitní autoritou. V neposlední řadě je potřeba zajistit předávání všech podání učiněné v portálu do agendových informačních systémů, ve kterých se dle agendy podání řeší a zároveň do spisové služby úřadu.

Portál podporuje samoobslužného klienta, který obsahuje jak přenesenou, tak samosprávnou působnost a obsahuje popis životních situací, ve kterých se řeší mandáty v elektronické komunikaci. Pokud portál vykonává a podporuje agendu veřejné správy dle registru práv a povinností, musí se chovat jako jakýkoliv jiný agendový informační systém a pracovat dle definice agendy.

Při předávání podání z portálu je tak potřeba mít zajištěnou funkcionalitu, která z podání vytvoří "lidsky čitelné" a "strojově čitelné" informace v rámci jednoho dokumentu, typicky formátu PDF/A3 a vyšší. Tento „kontejnerový“ formát pak slouží jak pro plnění požadavku „čitelnosti“ tak i pro zajištění požadavku na automatizované zpracování dat (vložené XML s údaji pro automatizované zpracování). Dokument musí být dále pak opatřen náležitostmi dle zákona č. 297/2016 Sb., typicky elektronickým podpisem nebo elektronickou pečetí a časovým razítkem. Lidsky čitelný formát, typicky PDF, jde do spisové služby pro evidenci a strojově čitelný formát jde od agendového systému. Při provozu portálu nezáleží na technologiích, ani infrastruktuře. Není tedy preferované ani On Premise řešení, ani cloudové řešení, vše záleží na potřebách daného úřadu a možnostech, které technologie dokáží nabídnout. Je vždy potřeba myslet na rozložení zátěže, například:

1. daňové přiznání z příjmu fyzických osob se podává 1x ročně a ačkoliv se nejedná o jeden rozhodný moment (celková doba je 6 měsíců) a je možné podávat i dodatečná daňová přiznání, není nutné klást na infrastrukturu stejné nároky po dobu celého roku, nebo
2. žádosti o různé dotace (například tzv. "kotlíkové") se podávají do určitého data, dá se předpokládat jisté

vytížení od okamžiku spuštění až do ukončení, kdy budou vysoké nároky na infrastrukturu (se vzrůstajícím trendem) a po uplynutí termínu, kdy budou minimální.

Každé řešení však musí podporovat přístup k centrálním službám eGovernmentu a dalším službám veřejné správy skrze zabezpečenou infrastrukturu Referenčního rozhraní veřejné správy. Níže uvedená pravidla pro centrální, agendové i místní portály jsou výtažkem ze studií zabývajícími se pravidly a federací portálů

Boston Consulting Group - Gov.cz

a

NAKIT + PwC - Zpracování pravidel pro federaci portálů veřejné správy a definování cílového stavu

.

Centrální (federující) portály

- Centrální (federující) portály musí být schopny zpřístupnit informace a služby všech portálů, které splní požadavky kladené federací
- Centrální (federující) portály si kromě uživatelského profilu neuchovávají žádné informace o subjektu práva – identifikovaném a autentizovaném uživateli

Pravidla pro Portál občana a Portál veřejné správy jsou popsána v samostatném funkčním celku.

Agendový portál

Agendovým portálem je myšlen portál poskytující služby logicky centralizovaného systému či systémů pro jiné orgány veřejné správy a klienty veřejné správy. Typicky jde tedy o portál správce agendy, ve kterém lze řešit služby agendy bez ohledu na místní příslušnost.

Takový portál musí splnit několik podmínek:

- Musí být registrovaný jako informační systém veřejné správy v rejstříku informačních systémů veřejné správy
- Spravuje ho orgán veřejné správy, který vykonává jednu nebo více agend dle seznamu agend veřejné správy
- Musí být součástí federace portálů veřejné správy a poskytovat informace a služby do centrálních (federujících) portálů jako je např. Portálu občana
- Musí být součástí federace národního identitního schématu, tedy využívat služby Národní identitní autority a jeho správce musí být ohlášen jako kvalifikovaný poskytovatel služeb
- Musí k identifikovanému a autentizovanému uživateli být schopen propojit údaje své agendy a údaje z propojeného datového fondu a veřejného datového fondu
- Musí využívat datovou základnu katalogu služeb a životních situací, jaká je v RPP
- Musí být v souladu s grafickým manuálem MVČR
- Musí být schopen poskytnout identifikovanému a autentizovanému uživateli možnost udělit mandát/oprávnění k zastupování pro jednotlivé služby, propsat do mandátního registru a nastavené mandáty zobrazovat, přijímat a rušit.
- Musí umožnit učinit podání (učinit úkon) ke službě z katalogu služeb VS pomocí následujících kanálů:
    - Informační systém datových schránek
    - Přímého podání na portále identifikovaným a autentizovaným uživatelem pomocí NIA
    - Elektronicky podepsaným dokumentem ve formě uznávaného podpisu
- Musí být schopen poskytnout náhled na jednotlivá podání vůči úkonům a služeb identifikovanému a autentizovanému uživateli a to jak tomu, který podání učinil, tak tomu, který je k tomu zmocněn
- Musí být schopen poskytnout úhradu poplatku pomocí platební brány
- Veškeré funkcionality, které se vyvinuly na míru, musí být poskytnuty jako otevřený zdrojový kód
- Musí splňovat bezpečnostní požadavky dle minimálního bezpečnostního standardu
- Musí být připraven zvládnout provozní zátěž ve špičkách zájmu o využití jednotlivých služeb (např. pomocí asynchronní architektury, využitím cloud computingu, atd.)

- Pokud portál přímo čerpá nebo poskytuje služby informačním systémům veřejné správy jiných správců, je toto propojení realizováno výhradně prostřednictvím služeb KIVS/CMS.

Postup činností práce s klientem, jeho identifikací a výběrem služeb

- Klienti se identifikují a autentizují s využitím služeb NIA a jsou v portále identifikováni pomocí BSI do doby, než si klient zvolí službu, která je poskytována agendou
- Po zvolení služby klientem, OVS zajistí překlad identity (BSI-AIFO agendy vybrané služby) pomocí eGON služeb ISZR
- OVS se doptá na oprávněné údaje pro potřeby služby dle oprávnění vybrané agendy
- OVS dá klientovi vybrat, do jaké role chce obsadit dle agendy, ve které je služba poskytována (tzv. mandát)
- Po dokončení služby si OVS nepamatuje AIFO ani jiné údaje použité pro službu, pokud to nevyžaduje samotná agenda
- OVS si pamatuje BSI pro klientský profil na portále

Portál území

Portálem území je myšlen portál poskytující služby, které spadají pod určité území ČR, typicky kraj, obec, město, městská část, souhrnně možno označit za samosprávy. Portál území může obsahovat kromě samosprávních služeb jako např. správa místních poplatků, i služby přenesené, avšak neměla by nastat situace, kdy je služba přenesené působnosti vytvořena jen pro portál území. Je zodpovědnost věcného správce, aby vytvořil centrální prostředí pro vyřizování služeb přenesené působnosti, které portál území využije, ale nevytváří.

Takový portál musí splnit několik podmínek:

- Musí být pro každou samosprávu jeden. Je na něm dostupné vše, v čem má samospráva působnost, tedy včetně přenesené působnosti.
- Musí být registrovaný jako informační systém veřejné správy v systému o informačních systémech veřejné správy
- Musí být součástí federace portálů veřejné správy a poskytovat informace a služby do centrálních (federujících) portálů jako je např. Portálu občana
- Musí být součástí federace národního identitního schématu, tedy využívat služby Národní identitní autority a jeho správce musí být ohlášen jako kvalifikovaný poskytovatel služeb
- Musí k identifikovanému a autentizovanému uživateli být schopen propojit údaje své agendy a údaje z propojeného datového fondu a veřejného datového fondu
- Musí využívat datovou základnu katalogu služeb a životních situací, jaká je v RPP
- Musí být v souladu s grafickým manuálem MVČR
- Musí být schopen poskytnout identifikovanému a autentizovanému uživateli možnost udělit mandát/oprávnění k zastupování pro jednotlivé služby, propsat do mandátního registru a nastavené mandáty zobrazovat, přijímat a rušit.
- Musí umožnit učinit podání (učinit úkon) ke službě z katalogu služeb VS pomocí následujících kanálů:
    - Informační systém datových schránek
    - Přímého podání na portále identifikovaným a autentizovaným uživatelem pomocí NIA
    - Elektronicky podepsaným dokumentem ve formě uznávaného podpisu
- Musí být schopen poskytnout náhled na jednotlivá podání vůči úkonům a služeb identifikovanému a autentizovanému uživateli a to jak tomu, který podání učinil, tak tomu, který je k tomu zmocněn
- Musí být schopen poskytnout úhradu poplatku pomocí platební brány
- Veškeré funkcionality, které se vyvinuly na míru, musí být poskytnuty jako otevřený zdrojový kód
- Musí splňovat bezpečnostní požadavky dle minimálního bezpečnostního standardu
- Musí být připraven zvládnout provozní zátěž ve špičkách zájmu o využití jednotlivých služeb (např. pomocí asynchronní architektury, využitím cloud computingu, atd.)
- Pokud portál přímo čerpá nebo poskytuje služby informačním systémům veřejné správy jiných správců, je toto propojení realizováno výhradně prostřednictvím služeb KIVS/CMS.

Příklad postupu činností v portálu území ve vztahu ke klientovi:

- Klienti se identifikují a autentizují s využitím služeb NIA a jsou v portále identifikováni pomocí BSI do doby, než si klient zvolí službu, která je poskytována agendou
- Po zvolení služby klientem, OVS zajistí překlad identity (BSI-AIFO agendy vybrané služby) pomocí eGON služeb ISZR
- OVS se doptá na oprávněné údaje pro potřeby služby
    - OVS rozlišuje mezi samostatnou a přenesenou působností
    - Samostatná působnost je soubor více agend, nelze celou samostatnou působnost konat jako jednu agendu
- OVS dá klientovi vybrat, do jaké role chce obsadit dle agendy, ve které je služba poskytována (tzv. mandát)
- Po dokončení služby si OVS nepamatuje AIFO ani jiné údaje použité pro službu, pokud to nevyžaduje samotná agenda
- OVS si pamatuje BSI pro klientský profil na portále

Portál soukromoprávního uživatele údajů

V případě portálu soukromoprávního uživatele údajů (také jako SPUÚ) se jedná o situaci, kdy vlastník portálu není orgán veřejné moci, ale dle své povahy je podřízen zákonu 111/2009 Sb. SPUÚ je podnikající fyzická osoba nebo právnická osoba, která není orgánem veřejné moci a je podle jiného právního předpisu oprávněna využívat údaje ze základního registru nebo z agendového informačního systému Může se jednat o portály poskytovatelů zdravotních služeb, soukromých pojišťoven, bank, státních podniků, apod. Takový portál a jeho vlastník musí splnit několik podmínek:

1. Musí mít zřízenou datovou schránku pro komunikaci s veřejnou správou
    - Právnické osoby mají datovou schránku zřízenou ze zákona
    - Zřídit datovou schránku je možné dle informací na webu České pošty
    - Datová schránka se může obsluhovat skrze webové rozhraní na adrese www.mojedatovaschranka.cz nebo mít funkcionality integrovány do vnitřních systémů organizace. Nejčastěji se jedná o elektronickou spisovou službu.
2. Musí být ohlášen v rejstříku SPUÚ v registru práv a povinností. Zde je možnost kontroly https://rpp-ais.egon.gov.cz/AISP/verejne/katalog-spuu.
    - Ohlášení do rejstříku SPUÚ probíhá pomocí agendového informačního systému působnostního viz https://rpp-ais.egon.gov.cz/AISP/. Do tohoto systému má přistup každý ohlašovatel agendy.
    - Pokud tedy existuje agenda, v rámci které je SPUÚ oprávněn čerpat údaje ze základních registrů nebo z agendového informačního systému, je třeba kontaktovat správce agendy a požadovat zavedení do rejstříku SPUÚ.
    - Pokud není soukromoprávní uživatel údajů ohlášen v AISP a správce agendy, ani jiné OVM, jej ohlásit nechce, může SPUÚ kontaktovat správce Registru práv a povinností (posta@mvcr.cz) se žádostí o ohlášení do rejstříku SPUÚ s těmito údaji (Název organizace, adresa organizace, IČO, DIČ, zákon a paragraf opravňující k přístupu do základních registrů nebo agendovému informačnímu systému, kontaktní osoba)
3. Musí být ohlášen jako kvalifikovaný poskytovatel služeb online služeb (dále též Service Provider). Více také zde https://www.eidentita.cz/Home/Ovm. Ohlášení může proběhnout automatizovaně skrze formulář, pokud to umožňuje typ zřízení datové schránky (typ 10, 14, 15, 16). Pokud žadatel tento typ nemá, je nutné kontaktovat Správu základních registrů skrze datovou schránku napřímo s požadavkem obsahujíc všechny údaje, jako v případě automatizovaného způsobu:
    - IČO subjektu
    - Název kvalifikovaného poskytovatele (SeP)
    - Popis kvalifikovaného poskytovatele
    - URL adresa odkazující na úvodní webové stránky
    - URL adresa pro odeslání požadavků
    - Adresa pro příjem vydaného tokenu (URL)
    - URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu

    - Načtení certifikátu
    - Adresa pro načtení veřejné části šifrovacího certifikátu z metadat (URL). Touto veřejnou částí budou šifrována data v tokenu
    - Logo kvalifikovaného poskytovatele
4. Musí umět přijímat a zpracovávat data pomocí standardů SAML2 nebo WS-Federation

Postup činností práce s klientem, jeho identifikací a výběrem služeb

- Portál SPUU nemusí být ISVS
- Klienti se připojující přes NIA jsou identifikováni pomocí BSI do doby, než si klient zvolí veřejnoprávní službu
- Pro potřeby doptání se dalších údajů, musí využít ISVS (možno i jiného OVS vykonávající danou agendu), kterému předá BSI uživatele. Předávání údajů mezi SPUU a OVS musí být legislativně podchyceno
- SPUU dá klientovi vybrat, do jaké role chce obsadit
- Po dokončení služby si SPUU nepamatuje údaje použité pro službu, pokud to nevyžaduje specifické zmocnění
- SPUU si pamatuje BSI pro klientský profil na portále
- **Soukromoprávní služby se řídí vlastními specifickými pravidly!**

Přístupnost informací

Popis Přístupnosti informací

Přístupnost informací a služeb ve smyslu “accessibility” je způsob publikování a provozování tak, aby s informacemi a službami mohly na rovnoprávném základě pracovat všichni, včetně uživatelů se specifickými potřebami, zejména osoby se zdravotním postižením (dále také “OZP”). Tyto osoby využívají moderní technologie založené na klasických zařízeních typu počítač, notebook, tablet či mobilní telefon, mají na nich však tzv. “Asistivní software”, který jim umožňuje plnohodnotně pracovat s internetem, pokud jsou příslušné služby, aplikace a informace přístupné.

Přístupnost je v souladu s principy tzv. “Governance accessibility” řešena na třech úrovních:

1. Přístupnost služeb veřejné správy
2. Přístupnost internetových stránek, mobilních aplikací, informačních systémů a informací se kterými pracuje veřejnost včetně OZP
3. Přístupnost informačních systémů využívaných úředníky a zaměstnanci včetně OZP

Obecně o přístupnosti

Přístupnost realizujeme proto, aby také OZP mohly na rovnoprávném základě využívat služby a informace, jako osoby bez jakéhokoliv postižení či specifických potřeb. Přístupnost ve veřejné správě je jednou ze základních společenských povinností, realizuje se jí soubor základních práv a nutnosti zabránit diskriminaci určitých osob.

Přístupnost informací je pak ryze technická disciplína, která říká, jakým způsobem mají být budovány informační systémy a jejich uživatelská rozhraní a jejich funkce tak, aby výstupem byly informace v přístupné podobě (z technického hlediska). Sama přístupnost informací nikterak nezasahuje do samotného vytváření informací, ale do způsobu jejich prezentace a publikace navenek. Jedná se o soubor technik, doporučení, norem a pravidel a postup, jejichž dodržení se zajistí, aby s informacemi a službami v elektronické podobě mohla pracovat co nejširší skupina lidí.

Pravidla Přístupnosti informací

Legislativní rámec pro přístupnost

Legislativní rámec pro povinnosti přístupnosti je poměrně široký. Níže jsou uvedeny pouze klíčové předpisy, které mají přímý vliv na přístupnost informací:

1. Obecná úroveň
    1. Mezinárodní přímo aplikovatelná Úmluva o právech osob se zdravotním postižením
    2. Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací
2. Úroveň základních služeb
    1. Procesně-správní předpisy, jako je Zákon č. 500/2004 Sb., Správní řád, apod.
    2. Zákon č. 155/1998 Sb., o komunikačních systémech neslyšících a hluchoslepých osob
    3. Nařízení EU č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (zejména článek 15)
    4. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
3. Úroveň internetových stránek a mobilních aplikací
    1. Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací subjektů veřejného sektoru
    2. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (zejména § 5, odst. 2, písm. f), § 9, a další)
    3. Částečně legislativa ohledně spisové služby
4. Úroveň realizace veřejných zakázek
    1. Zákon č. 134/2016 Sb., o zadávání veřejných zakázek (zejména § 93)

Vesměs z legislativy plynou pro OZP následující práva a pro veřejnou správu povinnosti:

1. OZP musí mít možnost využívat všechny služby veřejné správy jako kdokoliv jiný
2. OZP musí mít možnost plnohodnotně využívat elektronické služby stát i elektronické služby subjektů veřejného sektoru
3. Existuje zde obecná absolutní povinnost přístupnosti výsledků všech veřejných zakázek či zakázek podle legislativy k VZ, pokud jsou jejich výsledky určeny pro jakékoliv užívání fyzickými osobami, to se pochopitelně vztahuje i obecně na veškeré ICT zakázky.
4. Subjekty veřejného sektoru musejí mít svoje informace přístupné a to zejména na internetových stránkách a ve svých aplikacích
5. Přístupnost se vztahuje i na veškeré informační systémy pro zaměstnance, protože ani zaměstnanec s OZP nesmí být diskriminován tím, že není schopen pracovat se svým pracovním systémem

Standardy a metodiky

K dispozici jsou technické standardy a metodiky, které určují konkrétní technické postupy pro tvorbu a správu přístupného obsahu. Nejdůležitějšími v oblasti informačních systémů jsou následující:

- WCAG - Web content accessibility guidelines - Základní standard pro přístupnost obsahu
- WAI-ARIA: Standard Accessible Rich Internet Applications suite - Standard pro webové aplikace
- MAAP - Mobile accessibility applications principles - Soubor opatření pro přístupnost mobilních aplikací (přičemž pro jednotlivé platformy jsou opět k dispozici podrobné standardy)

Více o standardech a jejich realizaci se můžete dočíst třeba na portálu W3C.

Architektonická řešení

Na obecné úrovni lze konstatovat, že přístupnost A to jak u internetových stránek tak ale třeba i u informačních

systémů, je záležitostí dodavatele. Pokud je daná služba informační systém, aplikace, stránka poptávána jako dodávka v rámci veřejné zakázky, pak zde dopadají jednak obecné povinnosti stanovené v legislativě týkající se veřejných zakázek, jednak technické podrobnosti stanovené v legislativě týkající se přístupnosti internetových stránek a mobilních aplikací. Základním architektonickým řešením tedy je zahrnout potřebu přístupnosti a naplnění konkrétních technických norem jako nepřekročitelný požadavek v rámci architektury a v rámci požadavků na dodavatele. Je tedy nutno architektonicky a realizačně zajistit:

- Aby všechny internetové stránky (ať už veřejné či nikoliv) splňovaly požadavky na přístupnost.
- Aby všechny mobilní aplikace splňovaly požadavky na přístupnost.
- Aby všechny aplikace, systémy a informační systémy dodávané v jakékoliv formě veřejného investování také splňovaly požadavky na přístupnost.
- Aby byl elektronický systém spisové služby, agendové informační systémy a další aplikace a procesy nastaveny tak, aby digitální dokumenty odesílané organizací byly přístupné.
- Aby se požadavky na přístupnost staly nedílnou součástí požadavků na dodávky a veřejné zakázky i požadavků na interní vývoj.

Elektronická fakturace

Popis elektronické fakturace

Elektronická fakturace (také jako „e-fakturace“ či „efakturace“) je moderní prostředek, jehož primárním cílem je usnadnit a zefektivnit ekonomickým subjektům odesílání, příjem e-faktur a jejich následnou archivaci k dalšímu zpracování v rámci Evropské unie. E-faktura je dokumentem v digitální podobě (elektronickým dokumentem) podle ustanovení § 2 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů a nařízení eIDAS. Může být doručena ve strukturovaném nebo nestrukturovaném datovém formátu. Může být účetním záznamem podle zákona č. 563/1991 Sb., o účetnictví, daňovým dokladem podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, může sloužit i pro jiné účely (např. jako dodací list, záruční list, důkazní prostředek apod.)

E-fakturace v kombinaci s řádně vedenou spisovou službou dle zákona č.499/2004 Sb., o archivnictví a spisové službě a s ekonomickým informačním systémem uzpůsobeným pro zpracování elektronických faktur nabízí ekonomickým útvarům orgánů veřejné správy:

- Snížení administrativní a transakční zátěže následováno s výrazným zvýšení produktivity při zacházení s daňovými doklady
- Rychlá a snadná dohledatelnost daňového dokladu
- Bezpečný a spolehlivý prostředek v kombinaci s kvalifikovanými prostředky pro vytváření důvěryhodného podpisu dle nařízení eIDAS č.910/2014
- Zajištění přeshraniční interoperability e-fakturace v rámci Evropské unie

Ekonomické aspekty

Evropská komise předpokládá, že „Masové přijetí elektronické fakturace v EU by vedlo k významným hospodářským přínosům a odhaduje se, že přechodem od papírových faktur k fakturám elektronickým se za období šesti let ušetří přibližně 240 miliard EUR.“1. Na základě tohoto zjištění „Komise chce, aby se elektronická fakturace stala převládající metodou fakturace v Evropě do roku 2020.

Jako prostředek k dosažení tohoto cíle má směrnice 2014/55/EU o elektronické fakturaci při zadávání veřejných zakázek za cíl usnadnit používání elektronických faktur hospodářskými subjekty, které dodávají zboží, práce a služby pro orgány veřejné správy (B2G), jakož i podporovat obchodování mezi samotnými hospodářskými subjekty (B2B). Vymezuje především právní rámec pro zavedení a přijetí evropské normy (EN) pro sémantický datový model vytvořený ze základních prvků elektronické faktury (EN 169311:2017).

Norma EN 169311:2017 a její pomocné normalizační výstupy umožní sémantickou interoperabilitu elektronických faktur a pomohou odstranit bariéry na trhu a překážky v obchodu vyplývající z existence rozdílných vnitrostátních právních předpisů a norem – a přispějí tak k dosažení cílů stanovených Evropskou komisí.

Práce s elektronickými fakturami, ale zejména elektronizace celého nákupního řetězce od sběru požadavků, veřejné výběrové řízení, přes objednávku/smlouvu, potvrzení dodávek, fakturu, po platbu a rozúčtování výdajů/nákladů přinese významné úspory transakční i úspory spojené s lepším rozhodování a mnohem snáze a lépe provedenými řídícími kontrolami (1., 2., 3. a 4.) podle zákona č. 320/2001 Sb. o finanční kontrole a vyhlášky č. 416/2004 Sb., kterou se provádí zákon o finanční kontrole.

Pravidla elektronické fakturace

Povinnost akceptovat elektrickou fakturu (de standardů níže) se dle zákona č. 134/2016, o zadávání veřejných zakázek, ve znění pozdějších předpisů týká všech orgánů veřejné moci, kteří přijímají platbu plnění veřejné zakázky. Tato povinnost platí od 1. 1. 2019 pro ústřední orgány moci a od 1.4.2020 pro uzemní samosprávu §279 (5) b) zákona č. 134/2016, o zadávání veřejných zakázek, ve znění pozdějších předpisů. Všechny povinné orgány veřejné moci musí kromě procesních změn zajistit i příjem a vydávání elektronických faktur dle evropských a českých pravidel.

Technické aspekty

E-fakturaci je možné implementovat a realizovat ve svých organizačních jednotkách za dodržení jednoho z následujících technických standardů, který je v souladu se směrnicí 2014/55/EU:

- Evropská norma pro elektronickou fakturaci EN 16931-1:2017 - otevřená a zdarma dostupná na této stránce
- Syntaxe dle Evropské směrnice 2014/55/EU čl. 3, odst. 2
- XML zprávu meziodvětvové faktury UN/CEFACT podle XML schémat 16B (SCRDM - CII)
- UBL zprávy faktury a dobropisu podle ISO/IEC 19845:2015

Je třeba zmínit, že směrnice 2014/55/EU:

- nepředepisuje, která syntaxe by měla být použita pro elektronickou fakturaci v rámci veřejné zakázky. Pouze uvádí, které syntaxe jsou veřejní zadavatelé povinni akceptovat. Je zcela možné a velmi pravděpodobné, že jiné syntaxe, které nejsou uvedeny na seznamu výše, se budou i nadále používat, a to i pro přeshraniční výměny, zvláště tam, kde již existuje rozšířená národní nebo místní praxe. To je případ českého národního formátu elektronické faktury ISDOC (Information System Document), verze 5.2 a vyšší (který je definován vyhláškou č.194/2009 Sb a který musí být dle Usnesení vlády č. 347/2017 akceptován veřejnoprávními subjekty od 1.1.2019). Tento formát logicky není součástí výše uvedené směrnice, jakkoli je syntaxi UBL 2.1 velmi blízký, jelikož vychází z verze UBL 2.0. V rámci vnitřního trhu České republiky je formát ISDOC velmi široce rozšířen, zejména mezi soukromoprávními subjekty, které ve veřejné zakázce figurují v roli dodavatele, tedy vystavitele faktury.
- neponechává veřejným zadavatelům žádný prostor odmítnout fakturu ve kterékoliv ze syntaxí, které jsou uvedeny na seznamu, jenž bude zveřejněn v Úředním věstníku Evropské unie, v návaznosti na článek 3 směrnice. Článek 7 jasně uvádí, že veřejní zadavatelé a zadavatelé v EU musí přijímat a zpracovávat elektronické faktury, které splňují normu a odpovídají kterékoli ze syntaxí uvedených na zveřejněném seznamu.

Právní aspekty

Implementace e-fakturace do prostředí veřejné správy České republiky je dána směrnicí 2014/55/EU, která nabyla účinnosti 19. 4. 2018. K tomuto datu je také nutné mít ve svých spisových službách v rámci organizace

nastavené technickoorganizační opatření, která budou v souladu s výše uvedenou směrnicí a technickými standardy z ní vyplývající. Směrnice byla inkorporována do české legislativy v rámci § 221 [https://www.zakonyprolidi.cz/cs/2016-134|zákona č. 134/2016, o zadávání veřejných zakázek, ve znění pozdějších předpisů]]. Zadavatel nesmí odmítnout elektronickou fakturu vystavenou dodavatelem za plnění veřejné zakázky z důvodu jejího formátu, který je v souladu s evropským standardem elektronické faktury.

Všechny veřejné zakázky, které jsou nadlimitní mohou být dodavatelem vyžadovány ve formě e-fakturace.

V neposlední řadě bylo schváleno Usnesení vlády č. 347/2017, které dává povinnost od 1. 1. 2019 Ústředním orgánům státní správy a jimi podřízeným organizačním složkám státu přijímat elektronické faktury ve formátech stanovených Evropskou směrnicí 2014/55/EU a dále ve formátu isdoc/isdocx (Information System Document) verze 5.2 a vyšší

Základní registry a Informační systém sdílené služby

Základní registry a Informační systém sdílené služby, jakožto základní kameny sdílení údajů o subjektech a objektech v českém eGovernmentu, jsou popsány v tématické oblasti Propojený datový fond.

Portál občana a portál veřejné správy

Popis Portálu občana a Portálu veřejné správy

Portálem občana je myšlena transakční část Portálu veřejné správy dostupná na adrese https://www.portal.gov.cz/, kde klient/občan může skrze samoobslužné služby pod svou zaručenou elektronickou identitou činit podání vůči veřejné správě a využívat její služby. Služby portálu občana přejímají veškeré služby CzechPOINT@home, který byl určen pro občany, kteří nechtějí pro výpis z rejstříku chodit na kontaktní místo Czech POINT a mají zřízenu vlastní datovou schránku fyzické osoby. Datová schránka žadatele slouží pro odeslání žádosti a pro doručení vystaveného výpisu z rejstříku nebo jiné odpovědi.

V případě Portálu občana, jakožto součásti Portálu veřejné správy, stojí občan jako samoobslužný uživatel „vně" veřejné správy a portál mu poskytuje jedno univerzální vstupní místo dovnitř. Z toho důvodu jsou všechny věcné (agendové) a do budoucna i místní portály se svými službami federalizovány „pod" tímto ústředním portálem. Federace je na různých úrovních, které https://www.portal.gov.cz/Portál občana podporuje:

- Federace Single sing-on
  - Zajištění propojení pomocí jednotné elektronické identity, která je realizována systémem Národní idenitní autority. Na Portálu občana je zveřejněna jen informace (link), na které adrese na nachází federovaný portál.
- Federace s poskytováním údajů
  - Zajištění propojení pomocí jednotné elektronické identity, která je realizována systémem Národní identitní autority. Na Portálu občana je zveřejněna interaktivní část, která aktivně poskytuje údaje ze své působnosti.
- Federace s obsloužením služeb
  - Zajištění propojení pomocí jednotné elektronické identity, která je realizována systémem Národní identitní autority. Na Portálu občana je zveřejněna celá služba, včetně potřebných formulářů a logiky nutné k vyřízení.

Portál občana pro svou funkcionalitu využívá služby propojeného datového fondu, stejně tak služby národní identitní autority. Z pohledu propojeného datového fondu je Portál občana jedním ze čtenářských AIS, který má zmocnění dle agendy A344 zobrazovat subjektu práva jeho informace, které o něm vede veřejná správa. Portál občana v tomto musí zajistit, aby agenda, dle které se řídí byla neustále aktualizovaná dle toho, jak se budou postupně rozšiřovat služby a portály poskytující údaje. Technicky je Portál občana připojený jako čtenářský AIS

na systém eGON Service Bus, skrze který čerpá údaje publikované agendami pomocí tzv. kontextů. V tomto musí Portál občana pouze pravidelně aktualizovat čerpaný seznam kontextů jiných agend. Z pohledu národní identitní autority je Portál občana poskytovatelem služeb čerpající zaručené služby identifikace a autentizace.

Pravidla Portálu občana a Portálu veřejné správy

Portál občana i portál veřejné správy jsou centrálně poskytované a provozované portály. Integrovat, či federovat služby úřadu lze přes vlastní řešení v podobě agendových portálů, portálů území či soukromoprávních uživatelů údajů. Integrace je celkem na 3 stupních:

1. Proklik na vlastní řešení s využitím Single Sign-On. Obsahuje pouze vlastní prostor na portálu občana, kde úřad zveřejní svou informační dlaždici, skrze kterou se klient dostane, s využitím principu Single Sign-On a zapojení do národního identitního prostoru, na vlastní řešení
2. Poskytování údajů do vlastního prostoru na portálu občana. Kromě možnosti prokliku na vlastní řešení zapojeného do národního identitního prostoru obsahuje i vždy aktuální údaje o klientovi poskytované skrze propojený datový fond
3. Kompletní vyřešení služby veřejné správy na portálu občana pomocí formulářového řešení se všemi integracemi v bodech 1 a 2.

Přihlášení k portálu občana

Pro přístup na Portál občana je nutností přihlášení uživatele. Zvolený způsob přihlášení určuje i rozsah služeb, které jsou pro uživatele přístupné. Přihlašovací stránka Portálu občana je dostupná na adrese https://obcan.portal.gov.cz. Přihlášení je možné:

- prostřednictvím kvalifikovaného systému elektronické identifikace (NIA) v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci, a to s využitím občanského průkazu s elektronickou částí (pouze průkazy vydávané od 1. 7. 2018, nevyžadována registrace) nebo s využitím identifikačního prostředku Jméno, heslo a SMS (nutná registrace), příp. s využitím dalších prostředků identifikace.
- prostřednictvím autentizačního rozhraní Informačního systému datových schránek v souladu se zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Přihlášení je umožněno pouze těmto typům subjektů – držitelů datových schránek:
    - fyzická osoba (FO)
    - podnikající fyzická osoba (PFO)

Přitom lze využít pouze datové schránky zřízené na žádost, nikoli ze zákona, tedy nikoli ty zřizované automaticky advokátům, statutárním auditorům, daňovým poradcům nebo insolvenčním správcům. Všechny možnosti přihlášení jsou na sobě nezávislé, ale pro plné využití všech služeb Portálu občana je doporučeno použít elektronický občanský průkaz a dále mít připojenou datovou schránku. V obou případech se jedná o přístup se zaručenou identitou v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, jinými slovy o přístup do informačního systému veřejné správy nebo elektronické aplikace s využitím prostředku pro elektronickou identifikaci, při jehož vydání nebo v souvislosti s ním anebo v souvislosti s umožněním jeho využití byla totožnost osoby ověřena státním orgánem, orgánem územního samosprávného celku nebo orgánem veřejné moci, který není státním orgánem ani orgánem územního samosprávného celku, nebo který byl vydán v rámci kvalifikovaného systému elektronické identifikace.

Evidence údajů

Portál občana uchovává perzistentně typově takovéto informace:

- BSI (bezvýznamové směrové identifikátory) – jde o celou sadu identifikátorů, které slouží ke komunikaci s okolními systémy (např. AIFO – ISZR, SePP – NIA atd.). Tyto identifikátory mají význam cizího klíče. Z

jejich hodnoty (převážně jde o GUID) nelze přímo vyčíst žádné informace o uživateli. Tyto identifikátory neopouštějí perimetr PO jinak, než při komunikaci s dotčeným systémem.
- Nastavení – jde o informace ovlivňující zobrazené informace na Portálu občana (např. zobrazení dlaždic, nastavení notifikací apod.). Z jejich hodnot nelze přímo vyčíst žádné informace o uživateli.
- Dokumenty – jde o celou řadu „souborů“, které se vytvářejí v Portálu občana a nebo které si uživatel do PO nahrál. Jde například o tisknutelnou formu podání, archiv DZ apod. Tyto dokumenty se ukládají do speciální zabezpečené oblasti, která se „odemyká“ až při přihlášení uživatele. Tyto dokumenty mohou obsahovat i zvláštní kategorie osobních údajů (dříve jako citlivé údaje), ale z pohledu PO jsou „neviditelné“ (Portál občana neprovádí parsování těchto dokumentů).
- Komunikační atributy – v současné době jde o e-mail a telefonní číslo. Komunikační atributy neopouštějí přímo perimetr Portálu občana, ale slouží pouze pro navázání komunikace Portálu občana s uživatelem, resp. zasílání notifikací. Portál občana uživatele notifikuje pouze v případě jeho žádosti ve specifických případech (nastavení).

Transientně přes Portál občana prochází mnoho uživatelských informací. Jejich šíře se nedá přesně specifikovat – záleží, s jakým AIS uživatel prostřednictví Portálu občana komunikuje. Nicméně tyto informace se neukládají (jde pouze o on-line náhledy na informace). Co se týče notifikací změn údajů v základních registrech, proces je spouštěn v definovaných časech (konfigurace Portálu občana), Portál občana zjišťuje na základních registrech změnu přihlášených AIFO. Pokud taková změna proběhla a uživatel si nastavil notifikaci, PO vytvoří zprávu (podle nastavení uživatele) a uloží ji do fronty seznamu zpráv.

Komunikace na úrovni frontend

Komunikací na úrovni frontend je míněno především sdílení společného prostoru kvalifikovaného systému elektronické identifikace (NIA). V tomto prostoru má uživatel možnost procházet přes jednotlivá portálová řešení a využívat tzv. principu „single sign-on“, tj. jednotného přihlášení sdíleného mezi všemi portály či aplikacemi. NIA se řídí ustanoveními zákona č. 250/2017 Sb., o elektronické identifikaci. V návaznosti na výše uvedené slouží tzv. statické dlaždice na Portálu občana pro přechod uživatele mezi Portálem občana a dalšími portály či aplikacemi bez potřeby další autentizace. Portál občany tedy z pohledu funkcionality statických dlaždic slouží jako rozcestník. V současné době si uživatel Portálu občana sám vybírá a aktivuje služby (v podání dlaždic) z katalogu. V dalších fázích rozvoje je uvažováno o nabízení relevantních dlaždic dle jejich obsahu a rolí, ve kterých uživatel bude vystupovat. Aktivní služby v podobě dlaždic jsou uživateli zobrazeny na dashboardu Portálu občana.

Komunikace na úrovni backend

Portál občana standardně napřímo komunikuje s jen omezeným množstvím systémů, a to centrálně sdílených služeb. Konkrétně jde o:

- Informační systém základních registrů prostřednictvím svých vlastních nebo kompozitních služeb,
- Informační systém datových schránek.

Pro komunikaci s ostatními systémy Portál občana výhradně využívá eGon Service Bus / Informační systém sdílené služby.

Komunikace prostřednictvím ISZR

- Čtení ze Základních registrů (ROB, ROS):
  - přístup k údajům v základních registrech probíhá v agendové činnosti (RPP), kterou použije čtenář;
  - činnost musí mít oprávnění na přístup k Základním registrům.
- Čtení přes kompozitní služby (AIS EO):
  - čtení přes kompozitní služby probíhá v agendové činnosti (RPP), kterou použije čtenář;

- činnost musí mít oprávnění na čtení z AIS.
- činnost musí mít oprávnění na čtení z ROB podle typu použité služby (ověření AIFO nebo referenčních údajů použitých pro vyhledávání).

Mezi napřímo volané služby patří např. E03 robCtiAifo (čtení referenčních údajů z registru ROB), E22 rosCtiPodleUdaju, E45 orgPrihlasAifo (zaevidování AIFO k notifikaci změn v ROB a ORG pro volající AIS), E98 iszrCtiSouborCiselniku, E106 rppVypisSeznamAgend, E153 iszrZpracujFormular, E181 robVypisSouhlasuPoskytnuti, E199 orgZjistiAis (zjištění kombinací AIFO / Agenda, ve kterých v ORG existuje AIFO odpovídající vstupnímu AIFO) nebo E226 eidentitaCtiAifo (převod bezvýznamového identifikátoru fyzické osoby na odpovídající AIFO AIS).

Komunikace prostřednictvím eGSB/ISSS

Pokud hovoříme o spolupráci přes back-end, je tím míněno napojení Portálu občana na publikační AIS a spolupracovat přes služby, které jsou vystaveny na eGSB/ISSS. Připojení publikačního AIS je z pohledu náročnosti poměrně složité a vyžaduje součinnost ze strany provozovatele eGSB/ISSS. Jeho vstupy jsou nezbytné zejména při definování kontextů (schémat datových zpráv), které jsou sice v kompetenci publikátora, ale pro zachování jednotného formátu přes všechny publikátory, je nutné schválení ze strany provozovatele eGSB/ISSS. Portál občana nekonzumuje veškerá data, která jsou publikována na eGSB/ISSS už i z toho důvodu, že ne vše je určeno pro uživatele – fyzickou osobu. Výběr toho, co a jak zobrazovat na Portálu občana, je tedy výsledkem konkrétní spolupráce gestora publikačního AIS a Portálu občana. Po shodě na rozsahu služeb postupují řešitelé Portálu občana v těchto krocích:

1. vývoj pro čtení dat (čtenářská aplikace),
2. oprávnění pro čtení a získání testovacích dat,
3. testování čtení dat.

Po ověření dostupnosti eGSB/ISSS si Portál občana z katalogu služeb stáhne potřebné WSDL a XSD definice služeb a kontextů pro dostupné publikační AIS. Na základě těchto souborů unikátních pro každý publikační AIS a obecného popisu služeb eGSB/ISSS popsaných v dokumentu „Využití služeb eGSB/ISSS čtenářskými AIS“ si Portál občana vytvoří vlastní klientské rozhraní webových služeb pro čtení dat pomocí eGSB/ISSS.

Národní identitní autorita

Popis Národní identitní autority

Národní identitní autorita vytváří federativní systém zajišťující orgánům veřejné správy státem garantované služby identifikace a autentizace, který se skládá z následujících komponent:

- **Národní bod pro identifikaci a autentizaci** jako centrální bod federativního systému, který zajišťuje komunikaci a registraci účastníků federace. Tato komponenta zajišťuje současně vždy jednoznačné ztotožnění osoby, která prokazuje svoji totožnost s využitím autentizačních prostředků (prostředků pro elektronickou identifikaci). Je definován v zákoně č. 250/2017 Sb. jakožto informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému elektronické identifikace. Zajišťuje orgánům veřejné správy státem garantované služby identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principy Single Sign-On.
- **Kvalifikovaný správce,** který vydává jednoznačně identifikovaným fyzickým osobám prostředky pro vzdálenou autentizaci (prokázání totožnosti) a provádí veškeré činnosti spojené se správou těchto prostředků a prokazováním totožnosti fyzické osoby, tj. spravuje kvalifikovaný systém elektronické identifikace.
- **Kvalifikovaný poskytovatel online služeb,** který připojuje k Národnímu bodu online služby, ke kterým

je vyžadováno přihlášení prostředky vydanými kvalifikovanými správci.
- **Základní registry,** které poskytují jednoznačnou identifikaci osoby a zajištění vazeb této osoby vůči referenčním údajům o osobě.
- **Národní uzel eIDAS,** který je samostatnou součástí Národního bodu a zajišťuje přijímání vzdáleného prokázání totožnosti z ohlášených systémů dle nařízení eIDAS a předávání vzdálené identifikace a autentizace z České republiky ostatním státům EU. Ostatní státy EU musí akceptovat české identity od 13.9.2020, kdy vypršela roční lhůta pro zavedení akceptace ohlášeného prostředku elektronického občanského průkazu.

Pro osoby uvedené v ROB přihlašující se prostředky pro elektronickou identifikaci vydanými v ČR nebo přihlašující se identitou v rámci eIDAS z členských států EU nemusí OVS řešit přihlašovací identity pro své klienty samo.

- V současném stavu ROB (stav As-Is) tedy pouze pro občany ČR a cizince s trvalým/přechodným pobytem (cizinec musí být evidován v ROB).
- V budoucím stavu (stav To-Be) pro občany ČR, cizince s trvalým/přechodným pobytem a jiné fyzické osoby (EjFO), které mají k ČR právní či majetkový vztah (zahraniční vlastník nemovitosti, zahraniční lékař, zahraniční student, apod.).

Ačkoliv nyní poskytuje NIA své služby pouze jako "Front-end" řešení za pomoci SAML tokenů, je plánováno i poskytování služeb jako "Back-end" pro využití překladů identity a identifikátorů za pomoci eGON služeb.

Seznam poskytovatelů identity (Identity Provider; IdP)

Název identitního prostředku	Typ prostředku	úroveň záruky prostředku (LoA)	Popis	URL	Použití pro mezinárodní ověření identity v eIDAS
eObčanka	Elektronický občanský průkaz s aktivovanou částí elektronické identifikace	Vysoká (nejvyšší možná dle eIDAS)	Přihlášení prostřednictvím nového občanského průkazu vydaného po 1. 7. 2018, který obsahuje čip a jeho elektronická funkcionalita byla aktivována. Pro přihlášení tímto občanským průkazem je zapotřebí čtečka dokladů a nainstalovaný příslušný software.	https://info.identitaobcana.cz	ANO - eObčanka je zatím jako jediný prostředek ohlášen dle eIDAS pro potřeby mezinárodní identifikace a autentizace. Její použití je pro ostatní státy v rámci eIDAS povinné k použití od září 2020.
Mobilní klíč eGovernmentu	Mobilní aplikace s funkcí ověřování QR kódů	Značná	Mobilní klíč eGovermentu představuje využití přihlašování bez potřeby zadávání dalších ověřovacích kódů. Po jeho instalaci a aktivaci Vám bude umožněno přihlašování ke službám využívajícím elektronickou identifikaci prostřednictvím Národního bodu. Aby vše fungovalo, je nutné mít nainstalovanou aplikaci mobilního klíče na svém mobilním zařízení. Aplikace mobilního klíče je shodná se stávající aplikací mobilního klíče ISDS. Pokud již vlastníte tuto aplikaci pro přihlašování k datovým schránkám, aktualizací této aplikace získáte i možnost využít ji i pro přihlašování ke službám prostřednictvím Národního bodu. Tento prostředek nevyžaduje od uživatele zadávat při jeho použití žádné hodnoty, stačí pouze vyfotit QR kód mobilním zařízením, anebo jej nechat přečíst z obrazovky téhož mobilního zařízení. Mobilní klíč má dále jednu mimořádnou vlastnost, kterou ostatní prostředky nemohou nabídnout. Díky svému propojení s jádrem systému Národního bodu (NIA) dovoluje zapnout notifikaci přihlášení i jakýmkoliv jiným prostředkem téhož uživatele. To je výrazný bezpečnostní prvek, který dovoluje uživateli být v reálném čase informován o tom, že případně někdo jiný nějaký jeho prostředek zneužil a přihlásil se jím.	https://info.identitaobcana.cz/mep/	NE
NIA ID	Jméno + heslo + sms. Klasické přihlašování pomocí druhého faktoru.	Značná	Přihlášení prostřednictvím uživatelského jména a hesla, které jste zadali při založení Vašeho identifikačního prostředku na portálu národního bodu. Přihlášení dokončíte zadáním ověřovacího kódu, který Vám bude zaslán ve formě SMS na Vaše telefonní číslo.	https://info.identitaobcana.cz/ups/	NE
První certifikační autorita, a.s.	Čipová karta Starcos s identifikačním certifikátem	Vysoká (nejvyšší možná dle eIDAS)	Přihlášení prostřednictvím čipové karty Starcos společnosti První certifikační autorita, a.s., která byla použita pro generování a uložení privátního klíče identitního komerčního certifikátu. Pro přihlášení budete potřebovat čtečku čipových karet (pokud není integrována do PC/NTB) a nainstalovaný ovládací software SecureStore (ke stažení z www.ica.cz).	https://www.ica.cz/ica-identity-provider	NE
MojeID - úroveň "značná"	Přihlašovací údaje do účtu MojeID spárovaný s prostředkem FIDO	Značná	Přihlášení prostřednictvím účtu mojeID. Pro přihlášení je potřeba zabezpečit účet bezpečnostním klíčem (tokenem) certifikovaným od FIDO Alliance alespoň na úroveň L1, a to buď fyzickým (USB, NFC, Bluetooth), anebo systémovým (Windows Hello, Android v. 7 a vyšší). Dále je nutné mít účet mojeID aktivován pro přístup ke službám veřejné správy a jednorázově ověřit svou totožnost (již existujícím prostředkem nebo návštěvou Czech POINTu). Službu mojeID provozuje CZ.NIC, správce domény .CZ.	https://www.mojeid.cz/	NE
MojeID - úroveň "vysoká"	Přihlašovací údaje do účtu MojeID spárovaný s prostředkem FIDO	Vysoká	Přihlášení prostřednictvím účtu mojeID. Pro přihlášení je potřeba zabezpečit účet bezpečnostním klíčem (tokenem) certifikovaným od FIDO Alliance alespoň na úroveň L1, a to fyzickým USB, NFC. Dále je nutné mít účet mojeID aktivován pro přístup ke službám veřejné správy a jednorázově ověřit svou totožnost (již existujícím prostředkem nebo návštěvou Czech POINTu). Službu mojeID provozuje CZ.NIC, správce domény .CZ.	https://www.mojeid.cz/	NE
IIG - International ID Gateway	Výběr z možných identitních prostředků, které jsou ohlášené jinými členskými státy EU v rámci eIDAS uzlů	nízká až vysoká dle daného prostředku	Aktuálně je možné v rámci eIDAS uzlů vybírat z prostředků, které jsou zveřejnyny na stránkác eIDAS https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS		NE
Bankovní identita	Identita poskytovaná Československou obchodní bankou, a. s.	Značná		https://www.csob.cz/portal/csob/csob-identita	Ne
	Identita poskytovaná Českou spořitelnou, a. s.	Značná		https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita	Ne
	Identita poskytovaná Bankou CREDITAS a.s	Značná		https://www.creditas.cz/	Ne
	Identita poskytovaná Komerční bankou, a. s.	Značná		https://www.kb.cz/cs/podpora/bankovnictvi-a-nastroje/kb-bankovni-identita	Ne
	Identita poskytovaná Air Bankou, a. s.	Značná		https://www.airbank.cz/produkty/bankovni-identita/	Ne
	Identita poskytovaná Fio Bankou, a. s.	Značná		https://www.fio.cz/bankovni-sluzby/bankovni-identita	Ne
	Identita poskytovaná MONETA Money Bank, a. s.	Značná		https://www.moneta.cz/otevrene-bankovnictvi/bankovni-identita	Ne
	Identita poskytovaná Raiffeisenbank, a.s.	Značná		https://www.rb.cz/informacni-servis/pro-media/tiskove-zpravy/tiskove-zpravy-2021/tiskove-zpravy-202109/01092021-bankovni-identita	Ne
	Identita poskytovaná UniCredit Bank Czech Republic and Slovakia, a.s.	Značná		https://www.unicreditbank.cz/cs/obcane/bankID.html	Ne

Statistiky využití identitních prostředků

Data jsou informativní a platná v konkrétním čase 30.3.2023

Celkem státních ID prostředků	1 518 591
Celkem nestátních ID prostředků	10 565 485
Celkem ID prostředků	12 084 076
Počet profilů alespoň s jedním aktivním prostředkem	6 087 908
Celkový počet unikátních přihlášení	2 432 241
Konverze - procentuální zastoupení těch, kdo se skutečně přihlásili z těch, kdo se přihlásit mohli	39.95% %

Identitní prostředek	Popis počtu	Počet
eOběanka (od 1.7.2018):	Počet aktivovaných prostředků	669 250
	Počet aktivních prostředků	553 811
	Počet aktivních unikátních identit	553 778
	Počet přihlášení	1 960 980
	Unikátních přihlášení	62 446
NIA ID (dříve „Jméno, Heslo, SMS“) (od 1.7.2018):	Počet aktivovaných prostředků	357 741
	Počet aktivních prostředků	347 966
	Počet aktivních unikátních identit	347 965
	Počet přihlášení	8 176 219
	Unikátních přihlášení	333 713
Mobilní klíč eGovernmentu (od 16.11.2020):	Počet aktivovaných prostředků	506 208
	Počet aktivních prostředků	468 963
	Počet aktivních unikátních identit	372 402
	Počet přihlášení	10 011 957
	Unikátních přihlášení	381 271
Technicky IdP pro mobilni aplikace	Počet aktivovaných prostředků	149 314
	Počet aktivních prostředků	147 851
	Počet aktivních unikátních identit	66 006
	Počet přihlášení	501 624
	Unikátních přihlášení	66 354
Bankovní identita Air Bank:	Počet aktivovaných prostředků	1 513 739
	Počet aktivních prostředků	1 274 839
	Počet aktivních unikátních identit	729 574
	Počet přihlášení	2 201 696
	Unikátních přihlášení	214 223
Bankovní identita Banka CREDITAS - Pilot:	Počet aktivovaných prostředků	56
	Počet aktivních prostředků	47
	Počet aktivních unikátních identit	47
	Počet přihlášení	145
	Unikátních přihlášení	26
Bankovní identita Česká spořitelna:	Počet aktivovaných prostředků	3 096 849
	Počet aktivních prostředků	2 322 191
	Počet aktivních unikátních identit	2 320 468
	Počet přihlášení	6 670 709
	Unikátních přihlášení	634 986

Identitní prostředek	Popis počtu	Počet
Bankovní identita ČSOB Identita – plně ověřený přístup	Počet aktivovaných prostředků	2 788 564
	Počet aktivních prostředků	1 650 161
	Počet aktivních unikátních identit	1 556 137
	Počet přihlášení	4 337 035
	Unikátních přihlášení	426 822
Bankovní identita ČSOB Identita – rychlý přístup	Počet aktivovaných prostředků	1 716 823
	Počet aktivních prostředků	1 600 447
	Počet aktivních unikátních identit	1 514 433
	Počet přihlášení	91 618
	Unikátních přihlášení	36 979
Bankovní identita Fio banka:	Počet aktivovaných prostředků	618 021
	Počet aktivních prostředků	612 232
	Počet aktivních unikátních identit	612 221
	Počet přihlášení	393 833
	Unikátních přihlášení	63 247
První certifikační autorita, karta Starcos:	Počet aktivovaných prostředků	2 173
	Počet aktivních prostředků	932
	Počet aktivních unikátních identit	902
	Počet přihlášení	170 349
	Unikátních přihlášení	818
Bankovní identita Komerční banka:	Počet aktivovaných prostředků	1 042 678
	Počet aktivních prostředků	977 404
	Počet aktivních unikátních identit	922 854
	Počet přihlášení	3 681 846
	Unikátních přihlášení	313 741
MojeID - úroveň "značná":	Počet aktivovaných prostředků	111 848
	Počet aktivních prostředků	86 851
	Počet aktivních unikátních identit	72 631
	Počet přihlášení	1 655 765
	Unikátních přihlášení	73 290
MojeID - úroveň "vysoká":	Počet aktivovaných prostředků	4 736
	Počet aktivních prostředků	4 484
	Počet aktivních unikátních identit	4 255
	Počet přihlášení	43 335
	Unikátních přihlášení	3 561
Bankovní identita MONETA Money Bank:	Počet aktivovaných prostředků	1 107 892
	Počet aktivních prostředků	979 848
	Počet aktivních unikátních identit	650 671
	Počet přihlášení	1 400 315
	Unikátních přihlášení	159 679
Bankovní identita Raiffeisenbank:	Počet aktivovaných prostředků	1 319 659
	Počet aktivních prostředků	810 944
	Počet aktivních unikátních identit	807 448
	Počet přihlášení	1 201 408
	Unikátních přihlášení	144 640

Identitní prostředek	Popis počtu	Počet
Bankovní identita UniCredit Bank:	Počet aktivovaných prostředků	252 423
	Počet aktivních prostředků	245 105
	Počet aktivních unikátních identit	243 916
	Počet přihlášení	40 078
	Unikátních přihlášení	10 450

Seznam poskytovatelů služeb (Service Provider; SeP)

Poskytovatelů služeb je již více než 50 a v přípravě jsou další. Konečný počet je v řádu stovek. Aktuální seznam je dostupný zde https://info.identitaobcana.cz/sep/.

Podobně jako jsou jiné státy v rámci eIDAS povinni přijímat české ohlášené prostředky identity (eObčanka), jsou čeští poskytovatelé služeb povinni akceptovat identitu ohlášenou jiným státem v rámci eIDAS. Povinnost umožnit přihlášení pomocí IIG - International Identity Gateway je všem poskytovatelům služeb zapnuta od 30.6.2020. Současné znění nařízení eIDAS, povinuje členské státy, které oznámily systém elektronické identifikace, aby zajistily jedinečnou identifikaci osoby.

Nicméně je vhodné na tomto místě upozornit, že pomocí údajů obdržených na základě využití prostředku pro elektronickou identifikaci vydaného v rámci „zahraničního“ oznámeného systému elektronické identifikace, nemusí být vždy možné udělat jednoznačný „identity matching“ – tj. jednoznačné ztotožnění osoby, která se přihlašuje pomocí „zahraničního“ prostředku pro elektronickou identifikaci s údaji, které vede poskytovatel online služeb. Pro účely „identity matchingu“ by pak mohl posloužit také údaj(či údaje), který by musel zadat sám uživatel. Nejlépe samozřejmě údaj, který by měl být znám ze své podstaty pouze samotnému uživateli. Výše uvedené vychází z předpokladu spolehnutí se na základní osobní údaje obdržené na základě využití prostředku pro elektronickou identifikaci a na údaj (či údaje), které doplní sám uživatel. Seznam dostupných atributů u jednotlivých ohlášených systému elektronické identifikace je k dispozici na: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes.

Atributy vydávané poskytovatelům služeb (Service Providerům; SeP)

Následující atributy jsou NIA vydávány tzv. kvalifikovaným poskytovatelům služby. Problematika je popsána také v části Portály veřejné správy a soukromoprávních uživatelů údajů. Tučně označené atributy odpovídají standardu eIDAS, ostatní atributy sice standardu neodpovídají, kvalifikovaný poskytovatel služby má ale možnost při komunikaci v rámci ČR o jejich vydání zažádat.

Atribut/Element	Název atributu	Popis
Příjmení	**CurrentFamilyName**	Referenční údaj – Příjmení fyzické osoby. Viz eIDAS reference.
Jméno	**CurrentGivenName**	Referenční údaj – Jméno, případně jména fyzické osoby. Viz eIDAS reference.
Datum narození	**DateOfBirth**	Referenční údaj – Datum narození fyzické osoby. Viz eIDAS reference.
Místo narození	**PlaceOfBirth**	Referenční údaj – Místo narození fyzické osoby. Viz eIDAS reference.
Země narození	CountryCodeOfBirth	Referenční údaj – Země narození fyzické osoby, předávána v kódu podle standardu ISO 3166-3.
Adresa pobytu	**CurrentAddress**	Referenční údaj – Adresa pobytu fyzické osoby, je předávána zakódovaná pomocí BASE64. Obsahuje (pokud je uvedeno v ROB) název ulice (Thoroughfare), název pošty (PostName), PSČ (PostCode), název obce, případně doplněnou o část obce (CvaddressArea) a číslo domovní/číslo orientační (LocatorDesignator). Atribut vychází z ISA Core Vocabulary a tam je také uveden podrobnější popis atributu.

Atribut/Element	Název atributu	Popis
Email	Email	Emailová adresa uvedená na Portálu NIA (přihlášení na identitaobcana.cz) v sekci „Vaše údaje“.
Je starší než X	IsAgeOver	Výpočet je starší než X podle referenčního údaje Datum narození.
Věk	Age	Výpočet věku podle referenčního údaje Datum narození.
Telefon	PhoneNumber	Telefonní číslo uvedeno na identitaobcana.cz v sekci „Vaše údaje“.
Adresa pobytu (předávaná v podobě RÚIAN kódů)	TRadresaID	Referenční údaj – Adresa pobytu fyzické osoby je předávána v kódech podle RUIAN. Obsahuje (pokud je uvedeno v ROB) kódy pro okres, obec, část obce, ulici, PSČ, stavební objekt, adresní místo, číslo domovní a orientační.
Level of Assurance (LoA)	LoA	Stupeň (úroveň) jistoty nebo zajištění. Viz eIDAS reference.
Pseudonym	PersonIdentifier	Identifikátor fyzické osoby.
Typ dokladu	IdType	Druh elektronicky čitelného dokladu.
Číslo dokladu	IdNumber	Číslo elektronicky čitelného dokladu.

Při použití prostředku pro elektronickou identifikaci vydaného v rámci „zahraničního“ oznámeného systému elektronické identifikace se množina osobních údajů (v případě fyzických osob) skládá minimálně z následujících údajů:

- příjmení,
- jméno,
- datum narození a
- unikátního identifikátoru (pseudonymu).

Seznam dostupných atributů u jednotlivých ohlášených systému elektronické identifikace je k dispozici na: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes.

Při použití prostředku pro elektronickou identifikaci vydaného v rámci „zahraničního“ oznámeného systému elektronické identifikace nicméně není možné využít služby základních registrů E226 eidentitaCtiAifo pro překlad pseudonymu na AIFO dané agendy.

Pseudonym - bezvýznamový směrový identifikátor

Pseudonym při použití prostředku pro elektronickou identifikaci vydaného v ČR, neboli bezvýznamový identifikátor fyzické osoby, který se od NIA předává je pro každého kvalifikovaného poskytovatele služby, je jedinečný a neměnný. Neslouží jako veřejný identifikátor, ale jako identifikátor technický. Pokud by došlo na situaci, kdy se pseudonym pro fyzickou osobu změní, bude úřad o této skutečnosti informován prostřednictvím informačního systému základních registrů, protože se mu změní i agendový identifikátor fyzické osoby. Soukromoprávní uživatel údajů o této změně nebude notifikován, protože nemůže být napojen na základní registry nepřímo, avšak tuto službu mu může zprostředkovat jeho nadřízený úřad.

Pokud však chce mít kvalifikovaný poskytovatel služby jistotu o aktuálnosti pseudonymu, musí postupovat dle pravidel propojeného datového fondu, tzn. mít ztotožněn svůj datový kmen a odebírat notifikace z informačního systému základních registrů.

Nevizuální přihlašování z mobilních aplikací

Principem tzv. nevizuálního přihlašování je uspořádání, kdy konkrétní instance aplikace daného uživatele byla jednorázově zaregistrována v Národním bodu (NIA), prostřednictvím klasického vizuálního přihlášení. Pro běžné použití této aplikace pak stačí ověření uživatele při vstupu do této mobilní aplikace (typicky otisk prstu,

fotografie obličeje, nebo PIN). Jakmile se uživatel dostane do mobilní aplikace a ta zjistí, že od posledního přihlášení k NIA uběhla více než určitá doba (vývojářům aplikace je doporučeno dodržovat hodnotu 24 hodin), provede aplikace automatické přihlášení daného uživatele k NIA a to způsobem, který nevyžaduje žádnou jeho interakci. Tímto způsobem se mobilní aplikace dozví o možné změně údajů daného uživatele, ke které mezitím v ROB mohlo dojít, například změna příjemní atp. Uživatel má dále možnost vyhledat si v konfiguraci NIA seznam, zobrazující které mobilní aplikace má připojené v režimu nevizuálního přihlašování a z jakého zařízení. V případě potřeby (například ztráty svého mobilního telefonu) je pak možno v tomto seznamu konkrétní aplikaci odpojit. Aby se tento fakt mobilní aplikace dozvěděla a uvedla sama sebe do nezaregistrovaného stavu, je mobilní aplikace povinna v pravidelných intervalech volat příslušnou službu. Doporučená hodnota periodicity tohoto volání je vývojářům mobilní aplikace doporučena v úrovni 60 minut.

NIA poskytuje soubor rozhraní, které mají za cíl umožnit poskytovatelům služeb (SeP) vytvoření takových vlastních mobilních aplikací a vlastních backendových API, které dohromady budou umět ověřit identitu občana prostřednictvím volání webových služeb, tedy nevizuálně bez interakce občana.

Původně generická Mobilní aplikace bude muset být uživatelem nejprve registrována k užívání a následně bude umožňovat opakované přihlašování k NIA nevizuálním způsobem. Mobilní aplikace bude předávat informaci o provedeném přihlášení do API poskytovatele služeb, které následně z NIA získá JSON Web Token s detaily o přihlášeném uživateli. Fakt registrace bude opakovaně kontrolován na NIA prostřednictvím procesů mobilní aplikace a API, aby uživatel mohl např. při ztrátě zařízení možnosti nevizuálního přihlašování zabránit.

Cílem funkcionality není, aby mobilní aplikace poskytovatele služeb byla na úrovni poskytovatele identity (není to Identity provider). Není ji tedy možné používat pro přihlašování k portálům a jiným službám ostatních poskytovatelů služeb.

Více viz popis na stránkách SZR ČR.

Pravidla pro Národní identitní autoritu

Zásadním požadavkem bezpečnosti a transparentnosti pro informační systémy veřejné správy je požadavek na jednotnou elektronickou identifikaci externích uživatelů. Pro každou operaci je nutná znalost osoby, která tuto operaci provádí zvláště z hlediska nepopiratelné zodpovědnosti osoby. Externí uživatelé (klienti) informačních systémů veřejné správy musí být jednoznačně identifikováni zvláště z důvodů ochrany osobních údajů a dále z procesního hlediska, jak předpokládá správní řád (jednoznačné prokázání totožnosti účastníků řízení).

Úloha správy přístupů se pro každý informační systém veřejné správy skládá z následujících kroků:

- **Identifikace –** jednoznačné a nepopiratelné určení fyzické osoby, která přistupuje k informačnímu systému veřejné správy
- **Autentizace** – prokázání, že přistupující osoba je tou osobou, za kterou se vydává. Autentizace probíhá předložením **autentizačních prostředků** (například uživatelské jméno a heslo, autentizační certifikát), které osobě přidělil správce informačního systému
- **Autorizace** – na základě údajů o identifikované a autentizované osobě a dalších údajů o této osobě (například zařazení na pracovní pozici) zařazení osoby do odpovídající role a z toho vyplývající vyhodnocení oprávnění na úkony a data v rámci informačního systému.

NAP v této oblasti vyžaduje naplnění následujících principů pro všechny informační systémy veřejné správy:

1. Každý úřad, který poskytuje své služby elektronicky, potřebuje svého klienta ověřit (ztotožnit) s využitím kvalifikovaného systému elektronické identifikace, jehož služby jsou poskytovány Národní identitní autoritě. Ověření totožnosti vyžaduje právní předpis nebo výkon působnosti.
2. Pro využití Národní identitní autority se musí organizace stát tzv. kvalifikovaným poskytovatelem služeb (Service provider; SeP), dle postupu popsaném níže.
3. Každý úřad musí akceptovat nejen identitu českého občana, ale kteréhokoliv občana Evropské Unie dle eIDAS.
4. Jakýkoliv nový identitní prostor musí být budován tak, aby byl federovaný v rámci Národní identitní

autority.
    1. Před tvorbou nového identitního prostoru je potřeba si prvně udělat analýzu, zda nepostačuje některý z federovaných identitních prostředků v rámci Národní identitní autority.
5. Prostředky pro identifikaci a autentizaci jsou vždy vydány bezpečnou a jednoznačnou cestou identifikované osobě tak, aby byla zajištěna minimální úroveň důvěry. O vydání prostředků existuje trvalý záznam spolu s údaji, jak byla ověřena identita osoby.
6. Osoba, jíž byly prostředky vydány, zachází s prostředkem s náležitou péčí tak , aby nedošlo k jeho zneužití či odcizení.
7. Osoba, jíž byly prostředky vydány, nese nedílnou zodpovědnost za všechny úkony, které byly v informačním systému provedeny při použití těchto prostředků.
8. Věcný správce agend, které jsou vykonávány v rámci informačního systému, zodpovídá za obsazení osob do rolí (technicky vykonává technický správce informačního systému, vždy však na základě podkladů věcných správců). Tuto svoji zodpovědnost může delegovat v rámci organizační struktury na více zodpovědných osob.

Postup ohlášení kvalifikovaného poskytovatele služby (Service provider; SeP)

Následující kroky popisují jednotlivé části procesu, který je naznačen níže, na základě ověření přes ISDS. Aktuálně je registrace organizace prostřednictvím portálu národního bodu přístupná pouze pro orgány veřejné moci, ostatní subjekty musí provést registraci přímo u Správy základních registrů (viz krok 8). Kompletní příručka je dostupná zde.

1. Uživatel jako zástupce organizace požaduje po portálu národního bodu, který je Service Providerem, službu umožňující registraci dané organizace. Tato registrace umožní fungování dané organizace v NIA a vytváření jednotlivých Service Providerů.
2. Portál národního bodu kontaktuje Národní identitní autoritu, která ověření zprostředkovává, s požadavkem na ověření dané osoby (uživatele).
3. Pro ověření uživatele pro registraci organizace či konfigurací jednotlivých Service Providerů je jako Identity Provider určen Informační systém datových schránek (ISDS). Národní identitní autorita provede přesměrování na přihlášení prostřednictvím datových schránek.
4. Uživatel provede ověření vlastní osoby přihlášením k datovým schránkám. Aby mohl uživatel registrovat organizaci na portálu národního bodu, musí být přihlášen prostřednictvím ISDS (v definované roli a typem schránky OVM). V případě, že organizace není OVM, je potřeba provést registraci u Správy základních registrů.
5. V případě, kdy je uživatel úspěšně ověřen, Informační systém datových schránek předá Národní identitní autoritě jako výsledek ověření autentizační token obsahující IČO a název subjektu, roli přihlašovaného uživatele a další atributy.
6. Národní identitní autorita provede sběr atributů v Informačním systému základních registrů (ISZR) na jehož základě následně provede kontrolu existence IČO.
7. Národní identitní autorita předává portálu národního bodu potřebné atributy z Informačního systému základních registrů a atributy přijaté v autentizačním tokenu z Informačního systému datových schránek, které jsou nutné ke zpracování formuláře pro registraci.
8. Na základě úspěšného splnění předchozích kroků umožní portál národního bodu uživateli službu registrace organizace (SeP) a zobrazí mu vyplněný formulář pro registraci. Toto platí pouze pro organizace, které jsou OVM. Není-li organizace OVM, jsou místo registračního formuláře zobrazeny podrobné informace o tom, jakým způsobem provést registraci přímo u Správy základních registrů.
9. Uživatel potvrdí správnost údajů a provedení registrace organizace (SeP).
10. Portál národního bodu zpracuje přijatý požadavek na registraci a po úspěšném zaregistrování umožní uživateli provést konfiguraci jednotlivých Service Providerů spadající pod danou organizaci (seznam konfigurací kvalifikovaných poskytovatelů).
11. Uživatel provede konfiguraci Service Providera zahrnující následující údaje:
    - IČO subjektu
    - Název kvalifikovaného poskytovatele
    - Popis kvalifikovaného poskytovatele
    - URL adresa odkazující na úvodní webové stránky kvalifikovaného poskytovatele

- URL adresa pro odeslání požadavků
- Adresa pro příjem vydaného tokenu
- URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu
- Načtení certifikátu
- Adresa pro načtení veřejné části šifrovacího certifikátu z metadat
- Zpřístupnění autentizace prostřednictvím brány eIDAS
- Logo kvalifikovaného poskytovatele

Příklad pro poskytovatele zdravotních služeb

Poskytovatel zdravotních služeb není orgán veřejné moci, a proto je třeba zajistit kromě výše uvedeného postupu i následující kroky:

1. Požádat Ministerstvo zdravotnictví o zavedení do registru práv a povinností jako SPUÚ dle povinností vyplývající ze zákonů č. 250/2017 Sb. a č. 372/2011 Sb., ideálně pod agendou A1086
2. Na adrese https://www.identitaobcana.cz/Home/Ovm se přihlásit jako oprávněný uživatel datovou schránkou poskytovatele zdravotních služeb
   - Nově by se mělo nabídnout ruční zadání údajů s dalším postupem
   - Pokud se neobjeví, postupovat dle obecných bodů výše – poslání datové zprávy obsahující potřebné údaje (URL, logo….)
3. Upravit si svůj profil na https://www.identitaobcana.cz/Home/Ovm pro přístup jiných osob (IT oddělení např.) a správu svého profilu, konfigurovat pro Portál pacienta poskytovatele zdravotních služeb.

Podmínky pro nevizuální přihlašování

Přihlašování z mobilních aplikací je založeno na následujících předpokladech:

Poskytovatel služby musí

- vytvořit svoji mobilní aplikaci
- vytvořit svoje API
- zabezpečit komunikace mezi svým API a mobilní aplikaci
- provést registraci svého API a mobilní aplikace v NIA
- definovat a zaregistrovat sadu atributů, které budou obsahem JWT (JSON Web Token)
- zajistit komunikaci mezi API a NIA pro vyzvedávání JWT

NIA poskytuje

- rozhraní pro interaktivní přihlášení
- rozhraní pro registraci mobilní aplikace
- rozhraní pro přihlášení mobilní aplikace
- rozhraní pro API, které si z NIA vyzvedne JWT

Uživatel

- musí mít platný a funkční profil NIA a musí mít k dispozici, alespoň jeden platný přihlašovací prostředek, např. mobilní klíč eGovernmentu anebo bankovní identitu,
- nainstaluje si mobilní aplikaci od poskytovatele služby,
- po prvním spuštění aplikace provede interaktivní přihlášení přes NIA, které zajistí registraci aplikace v NIA,
- podle potřeby bude opakovat interaktivní přihlášení z aplikace, pokud z nějakého důvodu bude registrace v NIA zrušena/zneplatněna (změna konfigurace SePa anebo každých 6 měsíců).

Po registraci mobilní aplikace může provést přihlášení k NIA. Výsledkem přihlášení je tzv. access token, který mobilní aplikace předá komponentě (API) poskytovatele služeb. Tato komponenta (API) následně zavolá

definované rozhraní NIA, kde předá access token a své přihlašovací údaje. Na základě tohoto volání NAI provede vydání JWT.

Pravidla určení úrovně záruky pro poskytované služby (LoA)

Každý poskytovatel služby si sám určuje, jakou úroveň záruky (LoA) po uživateli vyžaduje[2)]), pokud neexistuje právní předpis, který by výslovně stanovoval úroveň záruky. Ideální stav je, že toto určení je provedeno pro každou jednotlivou službu, která se na portále poskytuje. Protože se však typicky uživatel předem nehlásí k jedné jednotlivé službě, ale k portálu jakožto agregaci více služeb, má poskytovatel služeb následující možnost:

1. Nastaví úroveň záruky podle nejčastěji využívaných služeb nebo dle nejčetnější úrovně záruky u nabízených služeb. Tato možnost zajistí, že uživateli bude po autentizaci dostupná většina služeb a zároveň se po uživateli nepožaduje prostředek s vysokou úrovní záruky. Pokud však uživatel chce využít služby s vyšší úrovní záruky, než použil při původní autentizaci, měl by být uživatel vyzván k autentizaci prostředkem s vyšší úrovní záruky.
2. Nenastaví žádnou vstupní úroveň záruky. Tato možnost zajistí, že se uživatel autentizuje na daný portál jakýmkoliv identitním prostředkem NIA a až následně se při výběru služby uživatelem kontroluje, zda je pro ni splněna minimální úroveň záruky. Pokud není, měl by být uživatel vyzván k autentizaci prostředkem s vyšší úrovní záruky.
3. Potřebnou úroveň záruky nastaví podle nejpřísnější služby. Tato možnost zajistí, že uživatel bude moci vždy využít všechny služby, které jsou na portále dostupné k vyřízení. Nevýhodou je, že se po uživateli může vyžadovat zbytečně vysoká úroveň záruky, kterou nemusí disponovat prostředky, které vlastní.

Pro jakoukoliv zvolenou variantu z pohledu poskytovatele služeb však platí několik povinností:

1. Požadovaná úroveň záruky u jednotlivých služeb odpovídá informacím uvedených v katalogu služeb a v případném právním předpise, který výslovně stanovuje úroveň záruky.
2. Uživateli autentizovaném s nižší úrovní záruky se neskrývá nabídka služeb vyžadující vyšší úroveň záruky.

Podstatné otázky a odpovědi na využívání NIA

Otázky týkající se Centrálního registru životního prostředí

Otázky týkající se přihlašování uživatelů do systémů Centrální registr životního prostředí, potažmo Integrovaného systému ohlašovacích povinností. Předání proběhlo přípisy Ministerstva životního prostředí:

1. ze dne 19. ledna 2024, sp. zn. ZN/MZP/2024/280/6, odpověď DIA byla poskytnuta pod sp. zn. DIA-2188-2/OPL-2024
2. ze dne 21. listopadu 2023, sp. zn. MZP/2023/110/787, odpověď DIA byla poskytnuta pod sp. zn. DIA-16244-2/OHA-2023

Žádám o doložení právního předpisu nebo o doložení faktu, že výkon působnosti vyžaduje prokázání totožnosti fyzické osoby. Zákon č. 250/2017 Sb., §2 říká, že pokud je nutné prokázání totožnosti, lze to pouze prostřednictvím kvalifikovaného systému. Neříká však, že ISPOP má právo vyžadovat identifikaci fyzické osoby. Roční hlášení je prováděno za právnickou osobu, nikoli za fyzickou.

Jak je vysvětleno výše, pokud agendový zákon neomezí způsob činit podání, je nutné se řídit obecnou úpravou podání uvedenou ve správním řádu, která je pro elektronické podání upravena zejména v ZoPDS a dalších speciálních předpisech. Informační systém veřejné správy je pouze jednou z možností, jak činit podání vůči orgánu veřejné správy. Pokud je agendovým zákonem stanoveno, že se podání vůči orgánu veřejné správy činí prostřednictvím informačního systému veřejné správy dle § 4 odst. (1) písm. d) ZoPDS, je nutné, aby se fyzická osoba, která za povinný subjekt jedná, přihlásila do informačního systému veřejné správy prostřednictvím

identity občana, jak ostatně vyplývá také z § 2 ZoEI. V takovém případě pak není nutné podání ani podepisovat, jelikož se uplatní fikce podpisu dle § 8 zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

Identitu občana nemám a nebudu si ji zřizovat, takovou povinnost jako občan nemám, jak se mám nadále přihlašovat?

V případě, kdy agendový zákon omezí způsob činit podání vůči orgánu veřejné správy pouze na elektronickou podobu (a agendový zákona nijak blíže neurčuje závaznou podobu úkonu a jeho podání), je možné úkon činit nejen za použití informačního systému, ale dále též např. prostřednictvím datové schránky či sítě elektronických komunikací za použití uznávaného elektronického podpisu dle §4 odst. (1) ZoPDS. Fyzická osoba jednající jménem PO není povinna si pořizovat identitu občana. Identita občana, resp. elektronická identifikace, je obecně pouze jednou z možností, jak učinit podání vůči orgánům veřejné moci.

Nebudu identitu občana využívat v rámci plnění pracovních povinností. Z jakého důvodu by řadoví zaměstnanci měli používat svoji Identitu občana pro plnění zákonných povinností svého zaměstnavatele? Proč není dostačující současný způsob přihlašování do systémů CRŽP? Proč je zásadní znát totožnost ohlašovatele/zaměstnance právnické osoby při takových úkonech jako je ohlášení produkce odpadů?

Využití identity občana je pouze jednou z možností, jak činit úkony vůči orgánům veřejné správy. Zajištění potřebných nástrojů pro plnění povinností povinného subjektu vyplývajících z agendových zákonů by mělo být primárně povinností konkrétního subjektu, na který plnění zákonných povinností dopadá. Pokud zaměstnanci povinného subjektu odmítají využívat či si pořídit identitu občana, měl by jim subjekt, za který mají jednat, umožnit užití datové schránky či zprostředkovat vydání certifikátu pro uznávaný elektronický podpis.

Pokud si propojím Identitu občana ke svému účtu v ISPOP, jak to pak funguje ohledně pokut atp.? Nemůže se stát, že firma bude po mě vymáhat zaplacení pokuty nebo nějakého poplatku, kterou obdrží, na základě podaného hlášení, když tam teď bude moje identita? Předtím to byl účet firemní a bral jsem to jako hlášení za firmu, teď to bude hlášení s mojí identitou.

Odpovědnost fyzické osoby (FO) za digitální úkony činěné v zastoupení právnické osoby (PO) je shodná, jako v případě úkonů činěných v listinné, nedigitální formě. Pokud FO činí úkon vůči orgánu veřejné moci svým jménem, ale v zastoupení a při plnění povinnosti stanovené PO, tak její odpovědnost za toto právní jednání není neomezená, ale odvíjí se od právního titulu, kterým je FO oprávněna za PO jednat. Ať už se jedná například o jednatele uvedeného v Obchodním rejstříku, zaměstnance pověřeného k určitým úkolům nebo zmocněnce na základě plné moci, odvíjí se odpovědnost této FO od konkrétního právního titulu a způsobené škody.

Do SEPNO ohlašuji automatizovaně ze SW přes účet, který jsme si zřídili jako systémový (tzn. pro komunikaci systém-systém), vztahuje se povinnost i na tyto účty? Lze i nadále využívat přihlašování přes Jméno + Heslo + 2. faktor?

Není-li nutné prokazovat totožnost, tak není povinnost využívat identitu občana. Komunikace mezi systémy nevyžaduje prokazování totožnosti, ovšem když je potřeba například zřídit danou komunikaci (vystavení či evidence systémového certifikátu) je nutné tuto službu obsloužit s prokázanou totožností, a tedy i využitím identity občana.

Jakým způsobem je zajištěna bezpečnost úniku dat z identity občana, může zaměstnavatel přikázat zaměstnancům, ať poskytnou svoje osobní údaje? Nedojde tím k porušení zákona GDPR?

Při přihlášení do informačního systému veřejné správy za použití identity občana uživatele přesměruje na Národní bod pro identifikaci a autentizaci (NIA), kde jsou popsány předávané osobní údaje, způsob jejich předání, důvod jejich zpracování, a osoba je vyzvána k udělení trvalého nebo jednorázového souhlasu s jejich zpracováním. Toto řešení je v souladu s právními předpisy upravujícími zpracování osobních údajů. Více

informací k této věci konec konců uvádí i MŽP v dokumentu k CRŽP dostupném na tomto odkazu.

Dle jakého konkrétního ustanovení právního předpisu je dovozována povinnost užívat Identity občana, popř. Bankovní identitu k přihlašování do systému ISPOP?

Pokud jde o předmětné ustanovení § 2 zákona č. 250/2017 Sb., o elektronické identifikaci, platí, že „Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace *pouze* prostřednictvím kvalifikovaného systému elektronické identifikace (dále jen „kvalifikovaný systém“).“ Elektronickou identifikací se podle čl. 3 odst. 1 Nařízení Evropského parlamentu a Rady č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (nařízen eIDAS) rozumí mj. postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují fyzickou osobu zastupující právnickou osobu.

Ministerstvo životního prostředí, jak sám uvádíte, je správcem obou zmíněných informačních systémů veřejné správy, správa zmíněných informačních systémů je tedy součástí výkonu jeho působnosti. Ke správě informačních systémů veřejné správy nepochybně patří též řízení přístupu k informačním systémům, které probíhá mj. požadavkem na prokázání totožnosti osob, které k těmto informačním systémům přistupují. Prokázání totožnosti je tedy vyžadováno v rámci výkonu působnosti Ministerstva životního prostředí jakožto orgánu veřejné moci a není nutné, aby bylo uvedeno v právním předpisu explicitně. Postup zjišťování totožnosti v rámci přístupu ke zmíněným informačním systémům odpovídá výše uvedené definici elektronické identifikace uvedené v nařízen eIDAS, toto nařízení zároveň počítá s tím, že svou totožnost prokazuje fyzická osoba mj. při zastupování právnické osoby.

Shrnuji, že pokud požadavek na prokázání totožnosti vyplývá z výkonu působnosti a je činěn s využitím elektronické identifikace, lze jej umožnit pouze prostřednictvím kvalifikovaného systému elektronické identifikace (označovaný též jako NIA, identita občana, atd.), nikoliv jiným způsobem, jak uvádí závěrečná část výše zmíněného zákonného ustanovení.

S ohledem na uvedené považuje Digitální a informační agentura postup Ministerstva životního prostředí za souladný s právní předpisy upravujícími elektronickou identifikaci.

Z jakého důvodu není při přihlašování zaměstnance postupováno stejně jako v případě přihlašování úřední osoby, když se vždy rovněž jedná de facto o zaměstnance?

Pokud jde o jednání při zastupování právnické osoby, je vhodné zmínit, že pokud jde fyzické prokazování totožnosti při jednání za právnickou osobu, je používání fyzických dokladů, které nepochybně nejsou vydány jen pro jednání za právnickou osobu, naprosto běžné. Např. pokud jednatel společnosti s ručením omezeným nebo jiný její zástupce jedná vůči orgánu veřejné moci za tuto společnost osobně nebo činí za tuto společnost písemné právní jednání vyžadující úředně ověřený podpis, prokáže vůči orgánu veřejné moci svou totožnost občanským průkazem nebo např. cestovním pasem, nikoliv dokladem vydaným jen pro kontext zastupování právnické osoby. Digitální a informační agentura neshledává používání kvalifikovaných prostředků elektronické identifikace v těchto situacích od používání fyzických dokladů totožnosti zásadně odlišným. V této souvislosti lze pro úplnost poukázat na to, že je rovněž běžné, že osoby, které nejsou statutárními orgány právnické osoby, ale jde o zmocněné zaměstnance či jiné zmocněné osoby, sdělují v rámci svého zastupování právnické osoby řadu osobních údajů, které se následně objevují např. ve sbírce listin obchodního rejstříku, např. datum narození nebo adresu trvalého pobytu takového zmocněnce.

Pokud jde o autentizaci, tedy o spojení totožnosti určité fyzické osoby s jejím oprávněním jednat za právnickou osobu, a s rozsahem tohoto oprávnění, je toto záležitostí nastavení předmětných informačních systémů a legislativy je upravující. Lze v tomto směru odkázat na analogii např. s nastavením přihlašování k informačnímu systému datových schránek, kdy relevantní právní úprava odlišuje osoby mající primární oprávnění přihlašovat se do datové schránky, tj. v případě právnické osoby její statutární orgán nebo členy statutárního orgánu (srov. § 8 odst. 3 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů) od osob

majících odvozené oprávnění přihlašovat se do datové schránky, tj. tzv. pověřených osob (srov. § 8 odst. 6 písm. b) zákona o elektronických úkonech a autorizované konverzi dokumentů). Rovněž právní úprava přihlašování k informačním systémům v působnosti orgánů Finanční správy rozlišuje mezi primárně oprávněnými přihlašujícími se osobami a odvozeně oprávněnými přihlašujícími se osobami (zde např. daňový poradce). Používání kvalifikovaných prostředků elektronické identifikace tedy nebrání společnosti ORLEN Unipetrol RPA s.r.o., aby oprávnění k přístupu k předmětným informačním systémům udělovala a odnímala sama.

Pokud jde o vyjádření pověřence pro ochranu osobních údajů Ministerstva životního prostředí, k tomu uvádíme, že přechod z tzv. proprietární (tj. jen pro konkrétní informační systém vytvořené) elektronické identifikace je procesem postupným a nelze tedy vyloučit, že proprietární identifikace je k přístupu k některým informačním systémům stále využívána do doby zavedení přístupu výlučně prostřednictvím kvalifikovaného systému elektronické identifikace. Vyjádření pověřence pro ochranu osobních údajů Ministerstva životního prostředí je tedy vyjádřením popisu praktické implementace již účinné právní úpravy, nikoliv popis právní úpravy účinné v budoucnu.

Pokud jde o důvody, proč není postupováno stejně jako v případě úřední osoby, platí, že autentizační informační systém (JIP/KAAS) podle § 56a zákona č. 111/2009 Sb., o základních registrech, je zřízen pro ztotožnění fyzických osob, které vykonávají činnosti v agendách jako tzv. nositelé rolí. Cílem je nejen řádná autentizace těchto fyzických osob, ale též vedení řádných záznamů o využívání údajů obsažených v informačních systémech veřejné správy, a to až na úroveň konkrétní fyzické osoby, která údaje využila. Na rozdíl od elektronické identifikace určuje konkrétní fyzické osoby jakožto nositelé rolí přímo orgán veřejné moci, tyto údaje se zapisují do základního registru práv a povinností. S ohledem na výše uvedené je JIP/KAAS určen pro ztotožnění úředníků, kteří jménem orgánu veřejné moci jednají, tj. pro státní zaměstnance, zaměstnance nebo jiné osoby v podobném vztahu k orgánu. Pro úplnost dodávám, že právnická osoba nemůže být nositelem role.

Jakým způsobem se bude postupovat, pokud nastane technická porucha na straně provozovatele systému Identity občana popř. Bankovní identity a systém bude nedostupný a proto nebude možno ověřit ohlašovatele a přihlásit se zejména do systému SEPNO, kde je nutno v krátkých časových intervalech provádět ohlášení? Zákon o odpadech řeší v §79 odst. 3 pouze náhradní postup ohlašování přepravy nebezpečných odpadů při přerušení provozu ISPOP. Nedostupnost systému Identity občana popř. Bankovní identity není nikde řešena, Toto ve svém důsledku znemožní odvoz nebezpečných odpadů a způsobí provozovatelům zvýšenou administrativní i finanční zátěž.

Právní úprava postupu pro případy technických poruch není ve vztahu k elektronické identifikaci zavedena, je nicméně vhodné doplnit, že právní úprava postupu pro případy technických poruch není zavedena ve valné většině případů ani např. ve vztahu např. k technické poruše informačních systémů veřejné správy nebo datových schránek a není mi známo, že by úprava postupu pro případy technických poruch byla zavedena ve vztahu k technické poruše dosud používaných identifikačních nástrojů vůči informačním systémům zmíněným v přípisu. Právní úprava počítá s tím, že tyto nástroje budou dostupné. V případě potřeby je možné využít zmírňujících institutů podle příslušných právních předpisů, v tomto doporučujeme konzultaci s Ministerstvem životního prostředí. Upozorňuje, že v případě využití prostředku elektronické identifikace, jejichž vydavatelem je banka (tzv. bankovní identita nebo bankID), může nastat technická porucha též na straně konkrétní vydávající banky.

Jak bude řešeno neohlášení ve smyslu odmítání požadovaného přihlášení za právnickou osobu prostřednictvím individuálních možností fyzické osoby dle výše uvedených argumentací?

V tomto doporučujeme konzultaci s Ministerstvem životního prostředí.

Univerzální kontaktní místo veřejné správy

Popis Univerzálního kontaktního místa

Univerzální kontaktní místa představují obslužné kanály, tj. místa a prostředky, kterými klienti veřejné správy mohou realizovat služby veřejné správy, bez ohledu na věcnou a místní příslušnost služby a služebního úřadu, a to jak samoobslužné (Portál občana jako součást Portálu veřejné správy), tak asistované. Asistovaná kontaktní místa se dále dělí na specializovaná a univerzální, a to především z důvodu komplexity a náročnosti některých služeb, které vyžadují vysoce kvalifikovaný personál, který není možné zaručit pro univerzální kontaktní místa.

Při rostoucí elektronizaci služeb klientům bude nezbytným dalším univerzálním kontaktním místem také multikanálové (hlas, mail, chat, SMS, ...) kontaktní centrum / Call-centrum, primárně určené na podporu uživatelů samoobslužných elektronických kanálů.

Kromě univerzální kontaktních míst existují i specializovaná kontaktní místa, opět v rozlišení na samoobslužná a asistovaná. Jejich úkolem je poskytnout služby VS přesahující rozsahem nebo složitostí možnosti univerzálních kontaktních míst.

Samoobslužná univerzální kontaktní místa

Samoobslužná kontaktní místa mají za svůj cíl omezit přímý kontakt klienta veřejné správy s úřady veřejné správy. Pro splnění tohoto cíle musí splnit podmínky uživatelské přívětivosti a zajistit, že samoobslužná alternativa služby je rovnocenná asistované verzi. Ministerstvo vnitra ČR vybudovalo a provozuje důležité systémy a služby, bez kterých by samoobslužná kontaktní místa nemohla fungovat či by jejich potenciál nemohl být naplněn jako např. Portál občana, Národní identitní autoritu nebo Centrální místo služeb. Samooblužné univerzální kontaktní místo může narozdíl od asistovaného univerzálního kontaktního místa obsahovat i služby, které jsou vysoce specializované, protože jde o vůli klienta využít službu a je si vědom všech na něj kladených požadavků. Samoobslužné univerzální kontaktní místo vždy klientovi poskytne dostatek informací a návodů, jak danou službu správně využít. V rámci všech poskytovaných služeb se plánuje rozvoj, který se zaměřuje na rozšíření dostupných služeb či zajištění bezodstávkového režimu 24x7.

Samoobslužná specializovaná kontaktní místa

Specializovaná samoobslužná kontaktní místa slouží pro případy, kdy je vyřešení služeb na univerzálním samooblužném místě nepřiměřeně náročné pro jeho správu a údržbu. Klienti však stále musí mít možnost využít služeb samoobslužných kontaktních míst. Jedná se ve většině případů o specializovaný agendový portál.

Asistovaná univerzální kontaktní místa

Ministerstvo vnitra ČR vybudovalo Czech POINT (zkratka pro Český Podací Ověřovací Informační Národní Terminál), jakožto součást Asistovaného univerzálního kontaktního místa s cílem vytvořit univerzální podatelnu, ověřovací místo a informační centrum, kde by bylo možné na jednom místě získat veškeré údaje, opisy a výpisy, které jsou vedeny v centrálních veřejných evidencích a registrech, jakož i v centrálních neveřejných evidencích a registrech ke své osobě, věcem a právům. Místo, kde je dále možné ověřit dokumenty, listiny, podpisy a také elektronickou podobu dokumentů a učinit podání ke kterémukoli úřadu veřejné správy. Hlavní služby tedy jsou:

- Služba autorizovaného výpisu z informačního systému veřejné správy
- Služba autorizovaného podání do informačního systému veřejné správy
- Služba autorizované konverze dokumentů

Aktuálně lze na pracovištích Czech POINT získat například výpis z katastru nemovitostí, obchodního rejstříku či rejstříku trestů. Kompletní seznam služeb je zveřejněn zde https://www.czechpoint.cz/public/verejnost/sluzby/.

Asistovaná kontaktní místa Czech POINT budou rozvíjena v následujících letech do té míry, že jejich

prostřednictvím bude možné učinit podobný rozsah podání, získat podobný rozsah údajů a informace o průběhu řízení ve všech věcech, které stát k jeho osobě vede, jaká budou nabízet samoobslužná kontaktní místa. Není však reálné, že by asistované univerzální kontaktní místo někdy obsáhlo veškeré služby a informace, které lze získat samoobslužně či na specializovaném kontaktním místě. Důvodem je vysoká míra specializace některých služeb (např. daňové přiznání), které zabraňují tomu, aby všechny služby dokázal asistovaně zprostředkovat člověk na univerzálním kontaktním místě.

V plánu je rovněž využití kontaktních míst Czech POINT pro podání žádosti o vydání různých typů dokladů, přičemž nepravděpodobněji půjde v první fázi o tzv. profesní průkaz.

Služby CzechPOINT

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Výpisy z informačních systémů veřejné správy	Vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů	Ministerstvo pro místní rozvoj	Seznam kvalifikovaných dodavatelů je veden Ministerstvem místního rozvoje jako součást Informačního systému o veřejných zakázkách. Ministerstvo místního rozvoje do seznamu zapisuje dodavatele, kteří splnili kvalifikaci podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, splnění kvalifikace doložili ministerstvu příslušnými doklady a zaplatili správní poplatek.	Tato služba je především určena firmám a dodavatelům, kteří mají zájem se ucházet o veřejné zakázky. Výpisem ze Seznamu kvalifikovaných dodavatelů tak může dodavatel v zadávacím řízení nahradit doklady prokazující splnění základních a profesních kvalifikačních kritérií. Zadavatel je povinen výpis ze seznamu uznat, není-li starší více než 3 měsíce. Jde o veřejný rejstřík, požádat o výstup může kdokoliv.	Pro získání výstupu ze Seznamu kvalifikovaných dodavatelů je nutné znát pouze identifikační číslo organizace.	Vydání první strany výpisu je zpoplatněno částkou, jejíž maximální výše je zákonem omezena na 100,- Kč; každá další strana výpisu je zpoplatněna částkou, jejíž maximální výše je zákonem omezena na 50,- Kč.	zákon č. 37/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů
Výpisy z informačních systémů veřejné správy	Výpis z bodového hodnocení řidiče	Ministerstvo dopravy	Tato služba umožňuje občanům zjistit na kontaktním místě veřejné správy stav trestných bodů (bez bodů ve správním řízení). Výpis je poskytován z Centrálního registru řidičů vedeného Ministerstvem dopravy, jehož součástí je právě i evidence bodového hodnocení. Tento výpis má pouze informativní charakter pro občany, nenahrazuje výpis z karty řidiče pro styk s úřady. Vydávání výpisů o trestných bodech řidičů kontaktními místy veřejné správy je upraveno zákonem č. 480/2008 Sb.	O výpis může zažádat pouze žadatel sám, nebo jím určený zmocněnec. Výpis lze vydat i cizincům, kteří mají například trvalé bydliště v České republice.	Osoba, která na pracovišti Czech POINT o výpis žádá, musí mít platný doklad totožnosti (občanský průkaz, cestovní pas) a musí mít přiděleno rodné číslo. Pro dohledání řidiče v registru je možné nepovinně zadat i číslo řidičského průkazu.	Správní poplatek, který žadatel zaplatí na samosprávních úřadech je za první stránku max. 100,-Kč a za každou další max. 50,-Kč. U ostatních provozovatelů kontaktních míst (Česká pošta, Hospodářská komora, notáři) se poplatek řídí vnitřními sazebníky jednotlivých organizací.	zákon č. 480/2008 Sb., kterým se mění zákon č. 274/2008 Sb., kterým se mění některé zákony, v souvislosti s přijetím zákona o Policii České republiky, zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů
Výpisy z informačních systémů veřejné správy	Výpis z insolvenčního rejstříku	Ministerstvo spravedlnosti	Insolvenční rejstřík je informační systém veřejné správy, který je spravován Ministerstvem spravedlnosti ČR. Jeho základní úlohou je zajistit maximální míru publicity o insolvenčních řízeních a umožnit sledování jejich průběhu. Prostřednictvím insolvenčního rejstříku jsou zveřejňovány veškeré relevantní informace týkající se insolvenčních správců, dokumenty z insolvenčních spisů i zákonem stanovené informace týkající se dlužníků.	Pro veřejnost	Jedná se o veřejně přístupný rejstřík, není tedy nutné ověřovat totožnost žadatele. V rejstříku je možné vyhledávat na základě dvou parametrů – identifikačního čísla organizace (hledání příslušné organizace) a podle osobních údajů (hledání konkrétní osoby).	Poplatek za ověřený výpis se řídí zákonem o správních poplatcích, tzn. 100 Kč za první stranu a 50 Kč za každou následující stranu.	zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Výpisy z informačních systémů veřejné správy	Výpis z Katastru nemovitostí	Český úřad zeměměřičský a katastrální	O výpis z Katastru nemovitostí České republiky může požádat anonymní žadatel. Výpis lze požadovat na základě • listu vlastnictví, • seznamu nemovitostí, • seznamu jednotek. Na kontaktních místech lze žádat o • úplný výpis z Katastru nemovitostí, • částečný výpis z Katastru nemovitostí, kdy lze vydat výpis např. pouze s některými nemovitostmi, uvedenými na listu vlastnictví. • výpis snímku z katastrální mapy.	Pro veřejnost. O výpis z Katastru nemovitostí České republiky může požádat anonymní žadatel. Výpis lze požadovat na základě listu vlastnictví nebo podle seznamu nemovitostí.	• Pokud žadatel žádá výpis podle listu vlastnictví, musí znát katastrální území a číslo listu vlastnictví. • Pokud žadatel žádá o výpis podle seznamu nemovitostí, měl by znát katastrální území a dále buď parcelní číslo požadované nemovitosti, jedná-li se o pozemek, nebo stavební parcelu případně číslo popisné, jedná-li se o stavbu. • O výpis lze zažádat i podle seznamu jednotek, v případě, že budova je dělena na jednotky, což je typické u větších staveb, dělících se na jednotlivé byty, garáže atd. V tomto případě pochopitelně musí žadatel znát nejen popisné číslo domu, ale i přesné číslo bytu v domě. • Pokud žadatel žádá o výpis snímku z katastrální mapy, musí žadatel znát v případě pozemku údaje o parcele (kmenové číslo a poddělení čísla), nebo v případě stavby typ a číslo stavby.	Pokud žadatel žádá výpis podle listu vlastnictví nebo podle seznamu nemovitostí: V obou případech, vydání první strany výpisu je zpoplatněno částkou, jejíž maximální výše je zákonem omezena na 100,- Kč; každá další strana výpisu je zpoplatněna částkou, jejíž maximální výše je zákonem omezena na 50,- Kč.	zákon č. 256/2013 Sb., o katastru nemovitostí, ve znění pozdějších předpisů
Výpisy z informačních systémů veřejné správy	Výpis z Rejstříku trestů	Rejstřík trestů – Ministerstvo spravedlnosti	Žadatel může požádat, aby do výpisu byly zahrnuty také údaje z Rejstříku trestů z jiného členského státu EU, v němž žadatel pobýval. Na základě podepsané písemné žádosti odešle pracovník Czech POINT elektronickou žádost na Rejstřík trestů, který odpoví buď předáním výpisu, nebo informací o zařazení žádosti do tzv. manuálního zpracování. V případě, že Rejstřík trestů odpoví předáním elektronického výpisu, se tento výpis vytiskne, doplní ověřovací doložkou a zkompletuje. V případě tzv. manuálního zpracování je žadateli pouze vytištěn tzv. šatní lístek, který obsahuje lhůtu, do kdy by měl být výpis připraven. Žadatel v daném termínu dorazí libovolné kontaktní místo a na základě šatního lístku a dokladu totožnosti si nechá vydat výpis z Rejstříku trestů.	Pro veřejnost. Podle §11a odst. 1 zákona č. 269/1994 Sb., o Rejstříku trestů, v platném znění lze vydat výpis z evidence Rejstříku trestů osobě, které se výpis týká, pouze na základě písemné žádosti. Tuto žádost není třeba ručně vyplňovat, klient ji obdrží vyplněnou k podpisu předtím, než mu je výpis z Rejstříku trestů vydán. Tato žádost se archivuje dle zákona.	Žadatel o výpis z Rejstříku trestů musí mít platný doklad totožnosti a musí mít přiděleno rodné číslo. To znamená, že výpis lze vydat i cizincům, kteří mají například trvalé bydliště v České republice. Na pracovištích Czech POINT lze vydávat výpisy i zplnomocněncům, kteří žádají o výpis z Rejstříku trestů na základě úředně ověřené plné moci. V dalším kroku se vytiskne žádost o vydání výpisu, kterou žadatel podepíše. V případě elektronického výpisu žadatel převezme na místě výpis a zaplatí správní poplatek. V případě tzv. manuálního zpracování žadatel v daném termínu dorazí libovolné kontaktní místo a na základě šatního lístku a dokladu totožnosti si nechá vydat výpis z Rejstříku trestů. A zaplatí správní poplatek.	1. V případě elektronického výpisu: Žadatel převezme výpis a zaplatí správní poplatek ve výši 100 Kč (bez ohledu na počet stran, v souladu se zákonem č. 634/2004 Sb., o správních poplatcích ve znění pozdějších předpisů). Správní poplatek je příjmem ověřující obce. Na poskytnutý výpis se nevylepuje žádný kolek. 2. V případě tzv. manuálního zpracování: Žadatel uhradí správní poplatek ve výši 100 Kč bez ohledu na počet stran.	zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů
Výpisy z informačních systémů veřejné správy	Výpis z Rejstříku trestů právnické osoby	Rejstřík trestů – Ministerstvo spravedlnosti	V souvislosti s přijetím zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, a zákona č. 420/2011 Sb., o změně některých zákonů v souvislosti s přijetím zákona o trestní odpovědnosti právnických osob a řízení proti nim, vznikla na Ministerstvu spravedlnosti evidence Rejstříku trestů právnické osoby. Z této evidence je vydáván výpis z Rejstříku trestů právnické osoby. Údaje z evidence Rejstříku trestů právnických osob, které se uvádějí ve výpisu, jsou veřejně přístupné, žadatelem může být kterákoliv fyzická osoba. Z tohoto důvodu se při podání žádosti o výpis týkající se právnické osoby neověřuje totožnost osoby, která žádost podává. Žádost se netiskne, ani nearchivuje.	Pro veřejnost, žadatelem může být fyzická osoba	Identifikační číslo osoby. V případě, že subjekt nemá v České republice přiděleno identifikační číslo osoby, nelze vydat výpis na počkání. Žadatel se může obrátit přímo na Rejstřík trestů, Soudní 140 66, Praha 4. Vzor žádosti o výpis lze nalézt zde.	Správní poplatek za vydání výpisu je ve výši max. 100 Kč za první stranu a za každou následující max. 50 Kč.	zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, zákona č. 420/2011 Sb., o změně některých zákonů v souvislosti s přijetím zákona o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Výpisy z informačních systémů veřejné správy	Výpis z Veřejných rejstříků	Ministerstvo spravedlnosti	O výpis z Veřejných rejstříků (viz zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob) může požádat anonymní žadatel. Veřejnými rejstříky právnických a fyzických osob se rozumí: • spolkový rejstřík • nadační rejstřík • rejstřík ústavů • rejstřík společenství vlastníků jednotek • obchodní rejstřík • rejstřík obecně prospěšných společností Pracovník kontaktního místa Czech POINT může vydat: • Úplný výpis – jsou v něm obsaženy všechny informace, které byly zapsány v obchodním rejstříku po dobu existence firmy. • Výpis platných – obsahuje souhrn informací o firmě k aktuálnímu datu.	Pro veřejnost. Může požádat anonymní žadatel.	IČO. Výpis lze požadovat na základě znalosti identifikačního čísla osoby (IČO) zapsané v jednom z veřejných rejstříků.	Vydání první strany výpisu je zpoplatněno částkou, jejíž maximální výše je zákonem omezena na 100 Kč; každá další strana výpisu je zpoplatněna částkou, jejíž maximální výše je zákonem omezena na 50 Kč.	zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob, ve znění pozdějších předpisů
Výpisy z informačních systémů veřejné správy	Výpis z Živnostenského rejstříku	Ministerstvo průmyslu a obchodu	O výpis z Živnostenského rejstříku České republiky může požádat anonymní žadatel.	Pro veřejnost. O výpis z Živnostenského rejstříku České republiky může požádat anonymní žadatel.	IČO. Výpis lze požadovat na základě znalosti identifikačního čísla (IČO) organizace.	Vydání první strany výpisu je zpoplatněno částkou, jejíž maximální výše je zákonem omezena na 100,- Kč; každá další strana výpisu je zpoplatněna částkou, jejíž maximální výše je zákonem omezena na 50,- Kč.	zákon č. 455/1991 Sb., o živnostenském podnikání, ve znění pozdějších předpisů
Výpisy z informačních systémů veřejné správy	Výpis elektronických receptů pacienta	Státní ústav pro kontrolu léčiv	Výpis elektronických receptů pacienta. Lékový záznam poskytne žadateli přesný přehled o tom, jaké léky mu byly předepsány a vydány, kdy, kým a v jakém množství. Nová služba tak napomůže zkvalitnit zdravotní péči a vyloučit případná pochybení při ordinaci další medikace, když si třeba nejsme jisti, jaké léky jsme užívali.	O výpis si může žádat fyzická osoba na sebe, případně i rodič, jakožto zákonný zástupce dítěte do 18 let věku, i zmocněná osoba. Zastoupení i zmocnění je nutné doložit příslušnými doklady.	O výpis si může žádat fyzická osoba na sebe, případně i rodič, jakožto zákonný zástupce dítěte do 18 let věku, i zmocněná osoba. Zastoupení i zmocnění je nutné doložit příslušnými doklady.	Za výpis se hradí správní poplatek 100 Kč za první stranu a 50 Kč za každou další.	zákon č. 378/2007 Sb., o léčivech, ve znění pozdějších předpisů
Podání vůči veřejné správě	Podání do registru účastníků provozu modulu autovraků ISOH	Ministerstvo životního prostředí	Vyhláška č. 352/2008 Sb., o podrobnostech nakládání s autovraky, definuje informační systém sledování toků vybraných autovraků pro evidenci přijatých autovraků. Pro evidenci autovraků je nutné, aby se provozovatelé autovrakovišť zaregistrovali na MA ISOH, což je jim právě umožněno přes Czech POINT. Provozovatelé autovrakovišť potřebují získat přístupové údaje do systému evidence autovraků. Přístupové údaje obsahují přihlašovací jméno a heslo, které jednoznačně identifikují provozovatele a provozovnu zařízení ke sběru vybraných autovraků. Přístup do systému může získat pouze podnikatelský subjekt, který k provozování činnosti sběru vybraných autovraků získal povolení od příslušného krajského úřadu. Podrobnější informace o problematice autovraků jsou k dispozici na //autovraky.cenia.cz/ v sekci Odpadové hospodářství. Kontaktní místa Czech POINT mohou provést následující činnosti související s MA ISOH: • registrace a vydání přístupových údajů, • změna v přiřazení provozoven k uživatelským účtům, • vygenerování jednorázového hesla k existujícím účtům. Pracovník kontaktního místa provádí kontrolu totožnosti žadatele pouze za účelem ověření, zda je daný žadatel oprávněn jednat za příslušnou instituci.	Pro podnikatelský subjekt: provozovatelé autovrakovišť	Pro vydání přístupových údajů do MA ISOH musí žadatel předložit: • identifikaci provozovatele (identifikační číslo organizace), • platný dokladu totožnosti, • plnou moc k převzetí oprávnění k přístupu do MA ISOH v případě, že se nejedná o statutární orgán provozovatele.	Vydání první strany výpisu je zpoplatněno částkou, jejíž maximální výše je zákonem stanovena na 100 Kč; každá další strana výpisu je zpoplatněna částkou, jejíž maximální výše je zákonem stanovena na 50 Kč.	vyhláška č. 352/2008 Sb., o podrobnostech nakládání s autovraky, ve znění pozdějších předpisů

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Podání vůči veřejné správě	Přijetí podání podle živnostenského zákona (§ 72):	Ministerstvo průmyslu a obchodu	Podle § 72 zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenského zákona), lze veškerá podání obecním živnostenským úřadům předat prostřednictvím kontaktního místa veřejné správy. Jde o: • ohlášení živnosti • ohlášení údajů, vedených v živnostenském rejstříku, nebo jejich změn • žádost o udělení koncese • žádost o změnu rozhodnutí o udělení koncese.	Pro veřejnost	Vyplnit formulář: Žadatel při podání předkládá vyplněný jednotný registrační formulář, který získá na Ministerstvu průmyslu a obchodu. Listinnou formu podání pracovník Czech POINTu převezme a odešle na zvolený živnostenský úřad.	Správní poplatek vybíraný pracovištěm Czech POINT činí v případě samosprávních úřadů 50 Kč za přijetí podání, na ostatních kontaktních místech Czech POINT podle ceníku. Další poplatek se vybírá dle druhu podání. Tento druhý poplatek je určen pro Živnostenský úřad, na který je poté kontaktním místem Czech POINT zasílán. Změna v RŽP je aktivní do 5 pracovních dní.	zákon č. 455/1991 Sb., o živnostenském podnikání, ve znění pozdějších předpisů
Zprostředkovaná identifikace osoby	Vydání veřejné listiny o identifikaci osoby	Finanční analytický úřad - Ministerstvo financí	Vydání veřejné listiny o identifikaci osoby podle § 10 zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Zprostředkovaná identifikace spočívá v ověření totožnosti žadatele, zjištění potřebných informací a převzetí podkladů od žadatele a vystavení veřejné listiny o identifikaci. Přílohou veřejné listiny jsou kopie dokumentů, které byly použity pro identifikaci daného subjektu. O provedení identifikace se učiní záznam do interní evidence.	Pro veřejnost – FO, PO (zastoupená jednajícími osobami) nebo jejich zmocněnci	Žadatel se musí v případě fyzické osoby prokázat průkazem totožnosti, v případě zmocněnce také úředně ověřenou plnou mocí. Žadatel žádající jako právnická osoba se musí prokázat průkazem totožnosti, dokladem o existenci právnické osoby a předložit doklady o oprávnění jednat za právnickou osobu, v případě zmocněnce též úředně ověřenou plnou mocí. Výběr potřebných dokladů může být v jednotlivých případech i širší (např. rozhodnutí soudu).	Správní poplatek za vydání veřejné listiny je stanoven na 200,- Kč.	zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování, ve znění pozdějších předpisů
Základní registry	Výpis údajů z registru obyvatel (ROB) – neveřejný	Ministerstvo vnitra Odbor správních činností	Žadatel může v této agendě požádat o výpis referenčních údajů, které jsou o jeho osobě vedeny v registru obyvatel (ROB).	Pro veřejnost	Provádí se ověření totožnosti žadatele nebo zmocnitele.	Cena za výpis je standardně dle Sazebníku správních poplatků, tedy max. 100 Kč za první stranu za každou další max. 50 Kč	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
Základní registry	Výpis údajů z registru osob (ROS) – neveřejný	Český statistický úřad	V této agendě lze požádat o výpis referenčních údajů podnikající fyzické osoby, evidované v registru osob (ROS).	Pro veřejnost.	Neprovádí se ověření totožnosti žadatele	Cena za výpis je standardně dle Sazebníku správních poplatků, tedy max. 100 Kč za první stranu za každou další max. 50 Kč.	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
Základní registry	Veřejný výpis údajů z registrů osob (ROS)	Český statistický úřad	Žadatel může požádat o výpis referenčních údajů libovolné podnikající fyzické osoby či organizace, evidované v registru osob (ROS).	Pro veřejnost	Neprovádí se ověření totožnosti žadatele	Cena za výpis je standardně dle Sazebníku správních poplatků, tedy max. 100 Kč za první stranu za každou další max. 50 Kč	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
Základní registry	Výpis o využití údajů z registru obyvatel (ROB)	Ministerstvo vnitra Odbor správních činností	Žadatel může požádat o výpis využívání referenčních údajů o jeho osobě v ROB orgány veřejné moci („kdo se na mě, kdy a za jakým účelem díval“). Volí se období, za které se výpis požaduje	Pro veřejnost	Průkaz totožnosti. Provádí se ověření totožnosti žadatele nebo zmocnitele	Cena za výpis je standardně dle Sazebníku správních poplatků, tedy max. 100 Kč za první stranu za každou další max. 50 Kč.	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
Základní registry	Výpis o využití údajů z registru osob (ROS)	Český statistický úřad	Žadatel může požádat o výpis využívání referenčních údajů podnikající fyzické osoby či organizace v ROS orgány veřejné moci („kdo se na mě, kdy a za jakým účelem díval“). Volí se období, za které se výpis požaduje.	Pro veřejnost	Průkaz totožnosti. Provádí se ověření totožnosti žadatele. Žadatel musí být osobou oprávněnou jednat za danou organizaci či přímo danou podnikající fyzickou osobou	Cena za výpis je standardně dle Sazebníku správních poplatků, tedy max. 100 Kč za první stranu za každou další max. 50 Kč.	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Základní registry	Žádost o změnu údajů v registru obyvatel	Ministerstvo vnitra Odbor správních činností	Žadatel může požádat o změnu nesprávných referenčních údajů, které jsou o něm vedeny v registru obyvatel (ROB). Žadatel může žádat o změnu svých údajů osobně, nebo prostřednictvím zmocněnce či zákonného zástupce.	Pro veřejnost	Průkaz totožnosti. Provádí se ověření totožnosti žadatele	Zdarma	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
Základní registry	Žádost o změnu v registru osob	Český statistický úřad	Žadatel může požádat o změnu nesprávných referenčních údajů, které jsou o podnikající fyzické osobě či organizaci vedeny v registru osob (ROS).	Osobě oprávněné jednat za danou organizaci či přímo daná podnikající fyzická osoba.	Průkaz totožnosti. Provádí se ověření totožnosti žadatele. Žadatel musí být osobou oprávněnou jednat za danou organizaci či přímo danou podnikající fyzickou osobou	Zdarma	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
Základní registry	Žádost o poskytování údajů jiné osobě	Ministerstvo vnitra Odbor správních činností	Žadatel může požádat (nebo odvolat) poskytování svých referenčních údajů z registru obyvatel (ROB) a jejich změn třetí osobě. Referenční údaje jsou následně zasílány do datové schránky třetí osoby v rozsahu, který si určí žadatel	Pro veřejnost	Žadatel může podat žádost osobně, nebo prostřednictvím zmocněnce či zákonného zástupce	Zdarma	zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
Konverze na žádost a související služby	Centrální úložiště ověřovacích doložek	Ministerstvo vnitra, odbor eGovernmentu	Na základě zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, vede systém Czech POINT centrální evidenci všech doložek o provedení konverze. Prostřednictvím webového rozhraní je možné ověřit výstup konverze na adrese //www.czechpoint.cz/overovacidolozky/. Pro kontrolu je nutné zadat do pole Identifikační číslo ověřovací doložky – číslo provedené konverze, které je umístěno na dokumentu pod 2D kódem. Systém pak zobrazí původní doložku o provedení konverze z centrálního úložiště ověřovacích doložek tak, jak byla vytvořena při samotné konverzi. V případě, že nedojde ke shodě čísla v centrálním úložišti ověřovacích doložek s číslem doložky zadaným ke kontrole, tak se jedná o dokument, který v žádném případě nevznikl provedením konverze dokumentů. V takovém případě nelze považovat kontrolovaný dokument za výstup z konverze dokumentů.	Pro veřejnost	Identifikační číslo ověřovací doložky – číslo provedené konverze, které je umístěno na dokumentu pod 2D kódem	Zdarma	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, zavádí termín (autorizovaná) konverze dokumentů. Technické parametry ke konverzi specifikuje vyhláška č. 193/2009, o stanovení podrobností provádění autorizované konverze dokumentů
Konverze na žádost a související služby	Úschovna systému CzechPoint	Ministerstvo vnitra, odbor eGovernmentu	Úschovna dokumentů je podpůrný systém pro konverzi dokumentů. Využívá se pro dočasné uložení dokumentů v rámci konverze. Při konverzi dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru na kontaktním místě Czech POINT lze zkonvertovaný dokument pro další použití uložit do úschovny. Zkonvertovaný dokument bude v úschovně uložen po dobu 3 dnů. Při konverzi dokumentu obsaženého v datové zprávě nebo datovém souboru do dokumentu v listinné podobě může být vstupní dokument uložen do úschovny prostřednictvím tohoto portálu, nebo odesláním z datové schránky. Následně může být na kontaktním místě Czech POINT konvertován do listinné podoby. Dokument určený pro konverzi může být uložen v úschovně až 30 dnů. Dokument uložený pro potřeby konverze musí být ve formátu PDF verze 1.3 a vyšší. Dále musí být dokument v případě provedení konverze na žádost opatřen uznávaným elektronickým podpisem, značkou či pečetí. Nevyzvednuté či nezkonvertované dokumenty po uplynutí stanovené doby budou automaticky smazány. //www.czechpoint.cz/uschovna/	Pro veřejnost	/	Zdarma	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, zavádí termín (autorizovaná) konverze dokumentů. Technické parametry ke konverzi specifikuje vyhláška č. 193/2009, o stanovení podrobností provádění autorizované konverze dokumentů

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Konverze na žádost a související služby	Autorizovaná konverze na žádost	Ministerstvo vnitra, odbor eGovernmentu	Konverze dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru – zákazník přinese listinu, kterou chce konvertovat, a zvolí si formu výstupu – CD/DVD nebo možnost zaslání do tzv. Úschovny, tedy do úložiště konvertovaných dokumentů, kde si jej nejpozději do 7 dnů vyzvedne. Úhrada nosiče CD/DVD je provedena v rámci úhrady poplatku za konverzi. Výstupem konverze bude dokument ve formátu PDF verze 1.7 a vyšší. Konverze dokumentu obsaženého v datové zprávě nebo datovém souboru do dokumentu v listinné podobě – dokument, který chce zákazník konvertovat, je možné přinést na CD/DVD nebo vložit do Úschovny (datového úložiště) ručně či posláním z datové schránky zákazníka. V tomto případě s sebou zákazník přinese potvrzení o vložení dokumentu do datového úložiště pro potřeby konverze, které obsahuje jeho jednoznačnou identifikaci. Vstupní dokument musí být ve formátu PDF verze 1.3 a vyšší. Orgány veřejné moci mohou využívat konverzi z moci úřední pro výkon své působnosti.	Pro veřejnost	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, zavádí termín konverze dokumentů. Technické parametry ke konverzi specifikuje vyhláška č. 193/2009, o stanovení podrobností provádění autorizované konverze dokumentů Konverze je: 1. úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru způsobem zajišťujícím shodu obsahu těchto dokumentů a připojení doložky o provedení konverze, nebo 2. úplné převedení dokumentu obsaženého v datové zprávě či datovém souboru do dokumentu v listinné podobě způsobem zajišťujícím shodu obsahu těchto dokumentů a připojení doložky o provedení konverze. 3. dokument, který provedením konverze vznikne, má stejné právní účinky jako dokument, jehož převedením výstup vznikl. Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy. Doložka o provedení konverze se ukládá do Centrálního úložiště ověřovacích doložek. Pro veřejnost je určena tzv. konverze na žádost, která funguje následujícím způsobem.	Poplatek za nosič (CD/DVD) a konverzi	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, zavádí termín (autorizovaná) konverze dokumentů. Technické parametry ke konverzi specifikuje vyhláška č. 193/2009, o stanovení podrobností provádění autorizované konverze dokumentů
Datové schránky	Žádost o zřízení datové schránky	Ministerstvo vnitra, odbor eGovernmentu	Na kontaktních místech veřejné správy Czech POINT je možné podat žádost o zřízení datové schránky. Žadatel předloží doklad totožnosti. Žádost vyplní pracovník přepážky elektronicky, následně jí vytiskne a předloží zákazníkovi ke kontrole a k podpisu. Datová schránka bude zřízena do tří dnů. Poté obdrží zákazník přístupové údaje poštovní zásilkou do vlastních rukou	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Datové schránky	Žádost o znepřístupnění datové schránky	Ministerstvo vnitra, odbor eGovernmentu	Použije se v případě, kdy žadatel potřebuje znepřístupnit datovou schránku podle § 11 odst. 4 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.
Datové schránky	Žádost o opětovné zpřístupnění datové schránky	Ministerstvo vnitra, odbor eGovernmentu	Použije se k obnovení dříve znepřístupněné datové schránky	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.

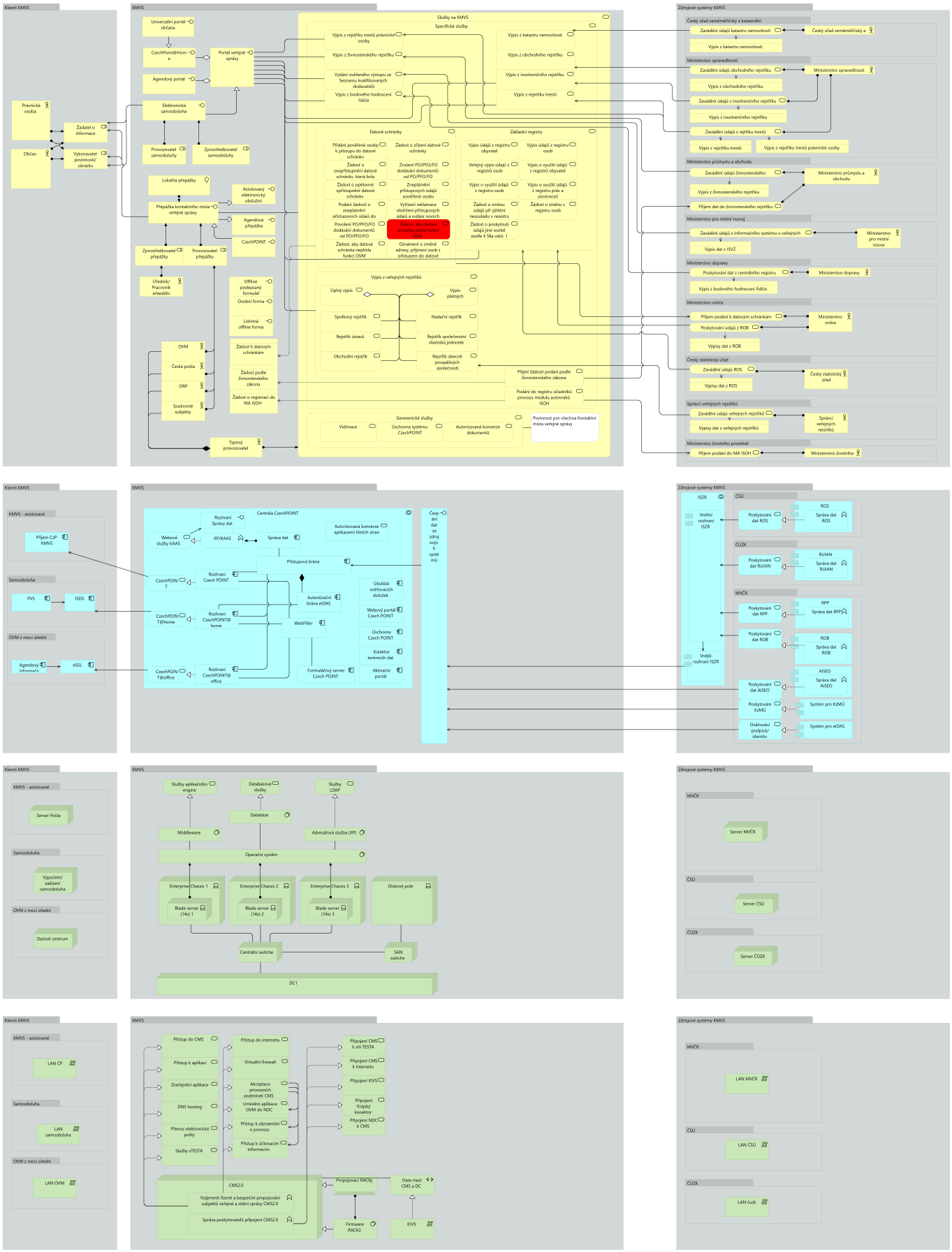
Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Datové schránky	Podání žádosti o zneplatnění přístupových údajů do datové schránky a vydání nových	Ministerstvo vnitra, odbor eGovernmentu	V případě ztráty, nebo odcizení přístupových údajů do datové schránky může oprávněná osoba k datové schránce požádat o zneplatnění přístupových údajů a vystavení nových. Žadatel předloží doklad totožnosti. Žádost vyplní pracovník přepážky elektronicky, následně jí vytiskne a předloží zákazníkovi ke kontrole a k podpisu. Ke zneplatnění stávajících přístupových údajů dojde okamžitě, poté bude automaticky odeslán e-mail s odkazem na aktivační portál, kde si žadatel vyzvedne nové přístupové údaje	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.
Datové schránky	Vyřízení reklamace obdržení přístupových údajů a vydání nových	Ministerstvo vnitra, odbor eGovernmentu	Tímto způsobem lze zjistit stav žádosti o zaslání nových přístupových údajů k datové schránce. Využít jej mohou žadatelé, kteří požadovali zaslání přístupových údajů prostřednictvím emailové adresy, a z nějakého důvodu jim přístupové údaje nebyly doručeny. Pracovník kontaktního místa nalezne pomocí formuláře chybu, vyřeší ji a dokončí doručení nových přístupových údajů k datové schránce.	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Datové schránky	Přidání pověřené osoby k přístupu do datové schránky	Ministerstvo vnitra, odbor eGovernmentu	Dojde k přidání pověřené osoby k přístupu do datové schránky. V oznámení je nutné zvolit typ oprávnění (pověřená osoba, administrátor). Dále je potřeba nastavit práva pro přístup pověřené osoby.	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.
Datové schránky	Zneplatnění přístupových údajů pověřené osoby (zrušení osoby)	Ministerstvo vnitra, odbor eGovernmentu	Dojde ke smazání pověřené osoby, která má přístup k datové schránce. Smazáním pověřené osoby dojde ke zneplatnění jejich přístupových údajů.	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Datové schránky	Povolení PO/PFO/FO dodávání dokumentů od PO/PFO/FO	Ministerstvo vnitra, odbor eGovernmentu	Datová schránka se nastaví do speciálního režimu, kdy je možné doručovat komerční datové zprávy do dané datové schránky. Tato služba je na straně ISDS zpoplatněna.	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.
Datové schránky	Zrušení PO/PFO/FO dodávání dokumentů od PO/PFO/FO	Ministerstvo vnitra, odbor eGovernmentu	Zruší se doručování komerčních zpráv do datové schránky. Je možné pouze komunikovat s orgány veřejné moci.	Pro veřejnost	1. platný doklad totožnosti. Zastupuje-li žadatel jinou osobu, musí být touto osobou zplnomocněn na základě plné moci, která je sepsána za tímto účelem a je notářsky ověřená. 2. V případě, že je zřizována datová schránka pro právnickou osobu na žádost, je nutné navíc k žádosti doložit jmenovací dekret, usnesení valné hromady, či jakýkoliv jiný dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. I tento dokument musí být úředně ověřen. Všechny přiložené dokumenty k žádosti jsou konvertovány do elektronické podoby. Žádosti pak vždy spadají do správního řízení. Konverze je v těchto případech provedena zdarma.	Činnosti v rámci informačního systému datových schránek jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč).	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů zavádí termín (autorizovaná) konverze dokumentů, ve znění pozdějších přístupů.

Kategorie služby	Název služby	Věcný gestor služby	Obsah služby	Cílová skupina služby	Co je potřeba k využití služby	Poplatky	Legislativa
Aktivace identifikačního prostředku na kontaktním místě Czech POINT	Aktivace identifikačního prostředku na kontaktním místě Czech POINT	Ministerstvo vnitra, odbor eGovernmentu	Pokud jste se rozhodli aktivovat svůj uživatelský účet (identifikační prostředek Jméno, heslo a SMS) poskytnutím referenčních údajů z registru obyvatel jiné osobě na pobočce Czech POINT, postupujte dle následujícího návodu, který jsme pro Vás připravili. Jako první krok je nutné podat Žádost o poskytnutí referenčních údajů z registru obyvatel jiné osobě, kterou je v tomto případě Správa základních registrů. Podání žádosti můžete provést bezplatně na jakémkoli kontaktním místě Czech POINT. V žádosti vyplňované na kontaktním místě je nutné vložit do zprávy pro příjemce Váš identifikační kód pro připojení souhlasu, který je zasílán po dokončení registrace uživatelského účtu na Vámi vyplněnou e-mailovou adresu. Stejný kód je zároveň zaslán i na vyplněné telefonní číslo.	Pro veřejnost	• Váš doklad totožnosti • Váš identifikační kód Následně si vyberte kteroukoliv z poboček Czech POINT. Kontaktní místa se nacházejí na pobočkách České pošty nebo na obecních či městských úřadech. Pokud si nejste jistí adresou kontaktního místa, můžete najít polohu nejbližšího kontaktního místa na stránkách Czech POINT. 1. U přepážky sdělte úředníkovi, že byste rádi poskytli „Žádost o poskytnutí referenčních údajů z registru obyvatel jiné osobě“. 2. Předložte svůj průkaz totožnosti. 3. Sdělte, že chcete poskytnout své osobní údaje právnické osobě s IČO 72054506. Jedná se o IČO Správy základních registrů. 4. Při dotazu na rozsah poskytnutých údajů volte položky „Datum narození“ a „Čísla elektronicky čitelných dokladů“. 5. Následně do zprávy pro příjemce nahlaste Váš identifikační kód. 6. Nakonec zvolte variantu jednorázového poskytnutí. Obsluha Vám vytiskne ke kontrole a podepsání vyplněný formulář žádosti. Na tomto formuláři zkontrolujte zejména Vaše osobní údaje, správné IČO identifikující Správu základních registrů, rozsah poskytnutých údajů (datum narození a čísla dokladů) a zkontrolujte si ve zprávě pro příjemce Váš identifikační kód. V případě, že jsou všechny údaje v pořádku, dokument podepište a vraťte zpět obsluze na přepážce. Ta provede odeslání Vaší žádosti a vytiskne Vám potvrzení. Aktivace Vašeho účtu jako identifikačního prostředku pro přihlašování mimo portál národního bodu proběhne obvykle do několika minut a tento prostředek je možné plnohodnotně využívat pro přístup k online službám.	Zdarma	

Pohled na univerzální kontaktní místo



Asistovaná specializovaná kontaktní místa

Specializovaná asistovaná kontaktní místa slouží pro klienty, kteří z jakéhokoliv důvodu nemohou využít služeb samoobslužných kontaktních míst, a zároveň není služba kvůli své specializaci dostupná v univerzálním

asistovaném kontaktním místě. Jedná se ve většině případů o přepážky úřadů, na kterých služby vyřizuje personál proškolený pro danou specializaci. Příkladem může být finanční úřad (daňové povinnosti), Katastrální úřad (vlastnictví nemovitostí) nebo Ministerstvo zemědělství (zemědělské dotace). Jakkoliv je služba specializovaná, nemělo by to bránit v zavedení její samoobslužné varianty v univerzálním kontaktním místě.

Pravidla pro Univerzální kontaktní místo

Úřad musí při tvorbě a správě svých služeb zohlednit možnost vyřízení služby jak samoobslužně, tak asistovaně. Primární odpovědnost za toto rozhodnutí nese věcný správce služby, což např. u služeb v přenesené působnosti není vždy daný úřad. Může však být dána určitá vlastní zodpovědnost za způsob, jakým je umožněno danou službu v přenesené působnosti vyřídit a pokud tuto možnost věcný správce poskytuje, je úřad povinen zohlednit všechny možnosti vyřízení. Nesmí také nastat situace, kdy služba veřejné správy, která je publikována pro samoobsluhu klienta nebude obsahovat všechny možnosti vyřízení, které má k dispozici v asistované formě.

Samoobslužná univerzální kontaktní místa

Aby se plně podporovala samoobsluha služby veřejné správy, musí splnit následující podmínky:

- Poskytování samoobslužných služeb pro klienta pod zaručenou elektronickou identitou
  - Všechny publikované samoobslužné služby jednotlivých úřadů musí mít možnost pracovat s klientem, který se prokazuje svoji zaručenou elektronickou identitou. Technicky to znamená soulad s pravidly a principy Národního identitního prostoru
- Federace pod Portál občana
  - Služby musí být federovány pod Portál občana / Portál veřejné správy v souladu s Národním identitním prostorem a plnit pravidla portálů veřejné správy a soukromoprávních uživatelů údajů
- Interaktivní uživatelské rozhraní
  - Formuláře a další služby pro klienta veřejné správy používající zaručenou elektronickou identitu a principy úplného elektronického podání.

Asistovaná univerzální kontaktní místa

Při provozování asistovaných univerzálních kontaktních míst je potřeba zajistit přidělení rolí v CzechPOINT pro pracovníky poskytující jeho služby skrze správce, tzv. lokálního administrátora.

V rámci asistovaných univerzálních kontaktních míst je nutné počítat s neustálým rozvojem a přidáváním služeb, které musí v co největší míře odpovídat těm samoobslužným. Žádná samoobslužná služby nesmí být bez své asistované varianty, která však může být řešena i v rámci úřadu, pokud tak vyžaduje její specifická náročnost (například podání nároku v insolvenčním řízení). V Czech POINT mají být především takové služby, u kterých:

- převažuje listinný vstup nebo výstup či vidimace listin a legalizace podpisu (mělo by se minimalizovat na nejnižší možnou míru),
- je skutečně nezbytná prezenční kontrola identity,
- je účelný přesun výkonu služby co nejblíže klientovi a existuje poptávka po asistované podobě takové služby.
- Je vhodné, aby kompletní odbavení klienta na KMVS pro daný úkon nepřekročilo deset minut.“

Při využívání systému CzechPOINT jako asistovaného univerzálního kontaktního místa je zakázáno požadovat a udržovat editační (zapisovací) formuláře pro informační systémy veřejné správy, které poskytují své služby pomocí tenkého klienta. Není tedy možné například požadovat editační formulář v systému CzechPOINT pro systém řidičských oprávnění, protože systém řidičských oprávnění poskytuje své vlastní rozhraní dostupné ve formě tenkého klienta.

Systém správy dokumentů

Popis Systému správy dokumentů

Obecně o spisové službě

Podle zákona č. 499/2004 Sb. vykonávají spisovou službu tzv. určení původci, přičemž zákon rovněž stanoví, pro které subjekty je povinnost výkonu spisové služby v elektronické podobě v informačních systémech spravujících dokumenty (dále jen „ISSD“), tedy v systémech elektronické spisové služby (eSSL) a v samostatných evidencích dokumentů. Výkonem spisové služby se rozumí „zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností“. Zákon o archivnictví a spisové službě definuje pojem „dokument“ jako každou písemnou, obrazovou, zvukovou nebo jinou zaznamenanou informaci, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena. Zákon o archivnictví a spisové službě definuje též pojem „metadata“ jako data popisující souvislosti, obsah a strukturu dokumentů a jejich správu v průběhu času.

Nařízení (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „eIDAS“) definuje pojem „elektronický dokument" jako jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvukovou, vizuální nebo audiovizuální nahrávku.

Legislativní rámec pro výkon spisové služby určuje zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů (dále též „Zákon“) a prováděcí vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby. Národní standard pro eSSL (dále též „NSESSS“) vydaný Ministerstvem vnitra a publikovaný ve Věstníku Ministerstva vnitra pak stanovuje podrobné technické požadavky na aplikační a byznysové funkce eSSL a samostatných evidencí dokumentů. Novelizací Zákona z roku 2021 byla zavedena povinnost atestací pro eSSL (blíže v podkapitole týkající se atestací), ovšem platnost této novely byla několikrát odložena, resp. došlo k odsunu termínů, kdy tato povinnost začne platit. Aktuálně (březen 2024) je ve sněmovně před schválením další novela, která stanovuje tyto termíny:

- Od 1. ledna 2025 již nebude možné nabízet a dodávat veřejnoprávním původcům neatestované eSSL
- Od 1. ledna 2027 již bude muset většina veřejnoprávních původců využívat výlučně atestované eSSL

Z hlediska „nosiče“ můžeme pak dokumenty rozdělit na skupinu analogových (typicky dokument vyhotovený na papíru) a na skupinu elektronických dokumentů (viz nařízení eIDAS). Pojem elektronický dokument je v tomto kontextu shodný s pojmem digitální dokument.

Zákon zavádí pojem „výstupní datové formáty dokumentů“, tj. formáty, ve kterých musí původce ukládat příslušné typy digitálních dokumentů. Definice výstupních datových formátů je uvedena v § 23 vyhlášky č. 259/2012 Sb. Výstupní datové formáty jsou aktuálně definovány pro nejčastější typy digitálních dokumentů.

Zákon ě v § 3, odst. 5) stanoví podmínky pro dokumenty v digitální podobě, kde se jejich uchováváním rozumí rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a čitelnosti, tvorba a správa metadat náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase. Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.

Zákon též stanoví specifické podmínky pro práci s dokumenty v digitální podobě jako je například převod mezi analogovou a digitální podobou nebo změna datového formátu.

Zákon též pamatuje na situace, kdy mohou veřejnoprávní původci plnit své povinnosti evidencí dokumentů i mimo systémy spisových služeb v tzv. samostatných evidencích dokumentů, kdy tyto evidence obdobně jako systémy elektronické spisové služby musí splňovat požadavky Národního standardu.

Shrneme-li základní požadavky, pak povinné subjekty musí:

1. Vykonávat spisovou službu tak, že eviduje dokumenty v eSSL nebo v samostatné evidenci dokumentů.
2. Zajistit soulad eSSL a všech samostatných evidencí dokumentů vedených v elektronické podobě s požadavky NSESSS.
3. Mít alespoň jeden eSSL.
4. Zajistit integraci mezi ISSD dle požadavků NSESSS.
5. Vést jmenný rejstřík, přiřazovat subjektům bezvýznamové identifikátory a vytvářet a spravovat vazby všech dokumentů obsahujících osobní údaje na osoby ve jmenném rejstříku.
6. Řádně uchovávat a spravovat digitální dokumenty a jejich komponenty v eSSL nebo samostatné evidenci dokumentů.
7. Provádět evidenci metadat o spisech, dokumentech a dalších entitách a zajistit evidenci všech transakcí a definovaných operací v eSSL či v samostatné evidenci dokumentů v souladu s požadavky NSESSS.
8. Zajistit příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování dokumentů ve skartačním řízení v souladu se Zákonem, vyhláškou č. 259/2012 Sb, a NSESSS
9. Zajistit řádné ověření autenticity a integrity doručených dokumentů v digitální podobě v souladu s nařízením eIDAS a zákonem č. 297/2016 Sb. a zajistit v souladu s uvedenými předpisy řádné připojení autentizačních a autorizačních prvků na dokumenty v digitální podobě vyhotovené původcem
10. Uchovávat dokumenty a umožnit výběr archiválií, vybrané archiválie v analogové podobě předávat k uložení příslušnému archivu a archiválie v digitální podobě předávat k uložení příslušnému digitálnímu archivu.

Digitální kontinuita

Digitální kontinuita je soubor procesů, opatření a prostředků nutných k tomu, aby byl původce schopen zajistit dlouhodobou důvěryhodnost informací a dokumentů. S ohledem na odlišný charakter činnosti soukromoprávních původců dokumentů a veřejnoprávních původců je u veřejnoprávních původců situace jednodušší. Pro obě skupiny původců lze však vycházet ze základních principů obsažených v ISO normách, zejména pak v ČSN ISO 30300 Systémy správy dokumentů, ČSN ISO 15489 Správa dokumentů, ČSN ISO 16363 Audit a certifikace důvěryhodných digitálních úložišť. Výše uvedené normy upravují vazby podnikových procesů a dokumentů, zajištění vypovídací hodnoty, koncepty a principy správy dokumentů od zrodu až k uložení a zajištění dlouhodobé důvěryhodnosti.

Autenticitou dokumentů se rozumí otázka, zda jde o původní dokument: dokument je autentický, pokud nedošlo k žádné jeho změně. V případě elektronických dokumentů dokáží jejich neměnnost (označovanou též jako integritu) zajistit všechny druhy kryptografických elektronických podpisů, pečetí a časových razítek. Tedy zaručený elektronický podpis, stejně jako všechny vyšší druhy elektronických podpisů (zaručený elektronický podpis, založený na kvalifikovaném certifikátu, i kvalifikovaný elektronický podpis), zaručená elektronická pečeť, stejně jako všechny vyšší druhy elektronických pečetí, a také elektronické časové razítko.

Pravostí dokumentu se rozumí otázka, zda dokument pochází od toho, koho považujeme za jeho původce, a obecně se dovozuje z autentizačních prvků, kterými je dokument opatřen. V případě elektronických dokumentů jde o elektronické podpisy, elektronické pečeti a elektronická časová razítka. U nich se nejprve zkoumá (ověřuje) jejich platnost, která je technickým pojmem a je závislá na splnění určitých technických podmínek (podrobněji popsaných v článku 32, resp. 40 nařízení eIDAS). Teprve v případě prokázání jejich platnosti je možné, v závislosti na druhu elektronického podpisu či pečeti, z technické platnosti dovozovat i právní pravost příslušných autentizačních prvků (podpisů a pečetí), a z ní následně i pravost elektronického dokumentu jako takového.

V souvislosti s tím je nutné zdůraznit, že možnost ověřit (technickou) platnost elektronických podpisů a pečetí, stejně jako časových razítek, se s postupem času ztrácí. Jde o základní vlastnost, jakousi časovou pojistku, charakteristickou pro všechny zaručené (a vyšší) druhy elektronických podpisů, pečetí a razítek. Jejím účelem je chránit již vytvořené elektronické dokumenty před zastaráváním a oslabováním kryptografických postupů a algoritmů, použitých u jejich podpisů (ale i pečetí a časových razítek). Bez této časovém pojistky by po uplynutí určité doby již nebylo možné z technické platnosti dovozovat právní pravost podpisů, a tím ani celých dokumentů: vzhledem k oslabení kryptografických algoritmů, použitých u původně podepsaného dokumentu, by již bylo možné reálně najít (vypočítat) jiný dokument, který je tzv. kolizní vůči původně podepsanému

dokumentu. Tedy takový dokument, který má jiný obsah, ale stejný elektronický podpis. Pak by bylo možné přenést elektronický podpis z původně podepsaného dokumentu na onen později vytvořený kolizní dokument, a v obou případech by byl takovýto podpis ověřen jako (technicky) platný – a nebylo by tak již možné spolehlivě prokázat, který dokument je pravý (který byl původně podepsán).

Problematika digitální kontinuity elektronických dokumentů naopak nezahrnuje otázku jejich pravdivosti neboli správnosti obsahu těchto elektronických dokumentů. Požadavek na dlouhodobě zajištění, resp. dlouhodobé udržování digitální kontinuity elektronických dokumentů se v praxi týká jen těch elektronických dokumentů, u kterých je nějaký důvod pro zachování možnosti prokázat jejich autenticitu a pravost.

Výběr a dlouhodobá archivace digitálních dat

Výběr a dlouhodobá archivace digitálních dat (dokumentů) probíhá dle zákona o archivnictví č. 499/2004 Sb., kde je dokument definován v § 2 písm. e) jako „každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, která byla původcem vytvořena nebo byla původci doručena“.

Povinnost uchovávat dokumenty a umožnit výběr archiválií má naprostá většina právnických osob působících v ČR. Tyto subjekty označuje archivní zákon jako původce dokumentů (viz § 3 Zákona). Chystaná novela Zákona z roku 2024 zavádí navíc § 3a, dle kterého by veřejnoprávní původci měli evidovat dokumenty a umožnit jejich výběr (export dle standardu stanoveným Národním archivem) nejen ze systémů eSSL, ale i z dalších informačních systémů, které využívají. De facto se tedy jedná o zavedení standardu Archiving by Design.

Archivně relevantní informace se vyskytují také řadě dalších prostředí, ať jsou to **databáze, specializované IS** (např. GIS, CAD, BIM), **webové stránky či sociální sítě, ze kterých se také provádí výběr a jsou trvale ukládány v prostředí digitálního archivu**.

Problematiku výběru dokumentů (informací) trvalé hodnoty, tedy archiválií, a jejich exportu do digitálního archivu řeší také připravovaná **vyhláška o dlouhodobém řízení ISVS**. Již při vzniku systémů je třeba pamatovat na možnost exportu dat z nich a to jak pro účely migrace dat do jiného systému nebo pro archivní účely. Archiváři by měli mít možnost již při vzniku systému definovat archivně cenné informace, podobu jejich výstupu a proces přenosu do digitálního archivu (***Archiving by Design***).

Řídící dokumenty

V rámci výkonu spisové služby jsou řídícími dokumenty zejména:

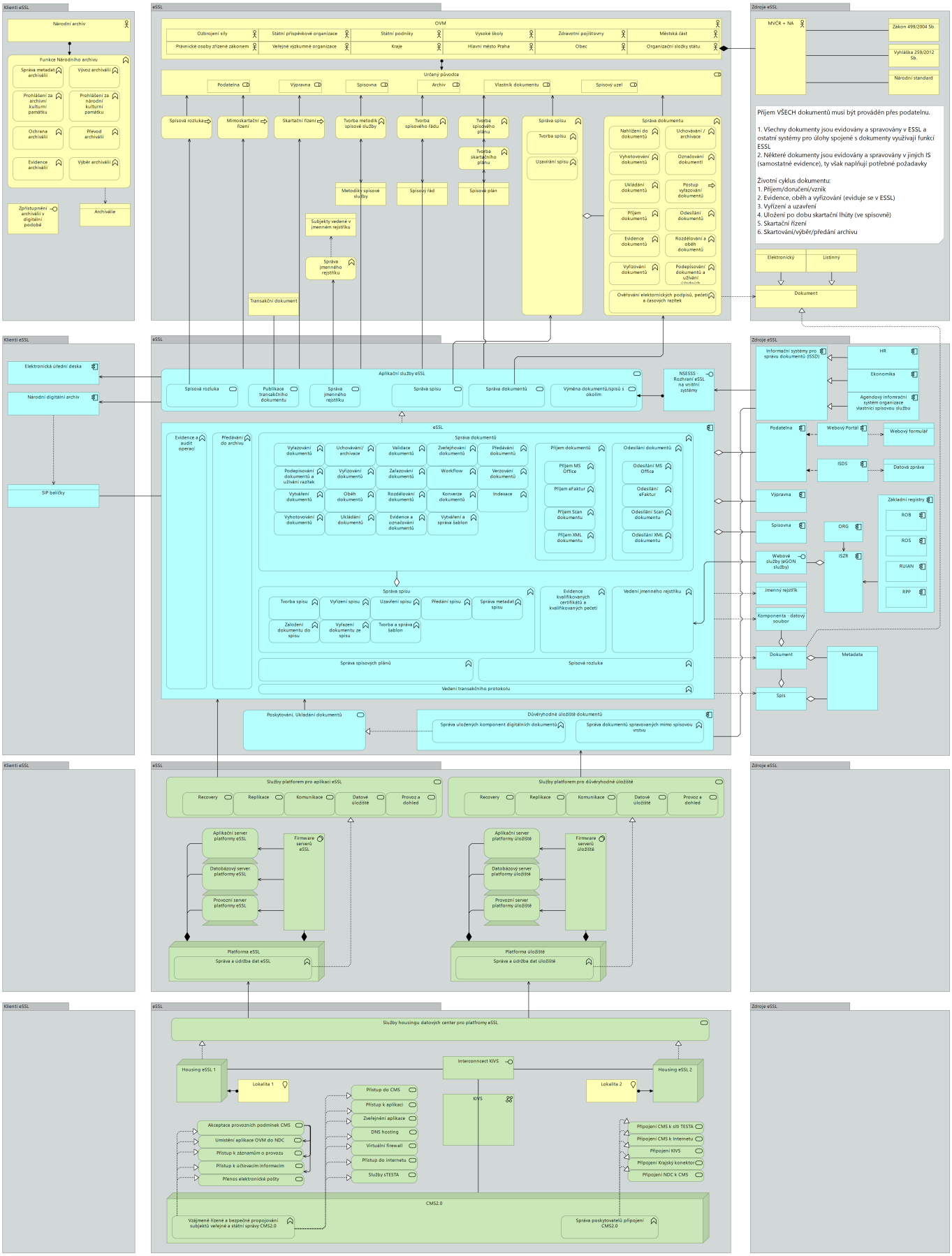
- Legislativa
    1. Zákon č. 499/2004 Sb., o archivnictví a spisové službě
    2. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
    3. Národní standard pro elektronické systémy spisové služby
- Technické a architektonické požadavky
    1. Národní architektonický plán
- Vnitřní řídící dokumenty úřadu
    1. Spisový řád (jehož součástí je spisový a skartační plán a podpisový řád)
    2. Informační koncepce úřadu
- Dokumentace k elektronickému systému spisové služby
    1. Dokumentace k ISSD
    2. Dokumentace k integracím ESSL a jiných ISSD, popř. integracím mezi ISSD
    3. Dokumentace související s výkonem spisové služby

Další zdroje

V souvislosti s výkonem spisové služby existuje celá řada dalších zdrojů informací a metodických dokumentů

publikovaných zejména Odborem archivnictví a spisové služby (OAS) Ministerstva vnitra a Národním archivem (např. INFORMAČNÍ LIST pro otázky elektronické spisové služby a dokumentů v digitální podobě).

Pohled na systém správy dokumentů



Pravidla pro Informační systémy spravující dokumenty

Spisovou službu považujeme za společnou schopnost na úrovni úřadu (capability), kde většina principů je shodných napříč celým úřadem (motivační vrstva, aplikační vrstva eSSL a integrace, byznysová vrstva procesů

a funkcí a interakcí) a na úrovni jednotlivých agend se odlišuje dle výkonu dané agendy minimálně. Architekturu výkonu spisové služby tedy je třeba zahrnout do mapy schopností úřadu.

Při zpracování Enterprise architektury úřadu i při zpracování a realizaci jednotlivých architektur, týkajících se ať už agend nebo schopností, nebo jejich řešení, je nutno zahrnout spisovou službu jako obecnou schopnost a správným způsobem řešit její realizaci. Je přitom nutno zvážit, do jaké míry je faktický i technický výkon spisové služby společný v rámci celé organizace a jestli a jakým způsobem se bude lišit v rámci jednotlivých agend či řešení. Jednoznačným doporučením je mít jeden eSSL a u ostatních informačních systémů, včetně samostatných evidencí dokumentů (informačních systémů veřejné správy i provozních informačních systémů), zajistit úkony spojené se správou dokumentů (příloh k transakcím) a s výkonem spisové služby formou integrace na eSSL rozhraním.

Součástí architektury úřadu by tedy z pohledu spisové služby měly být vždy alespoň následující elementy:

- Elektronický systém spisové služby (splňující požadavky NSESSS) včetně modulů podatelny a výpravny umožňující příjem a odesílání i digitálních dokumentů správnými komunikačními kanály
- Jmenný rejstřík (může být i samostatnou komponentou), nejlépe integrovaný na rejstřík kmenových dat klientů úřadu, notifikovaný ze základních registrů.
- Spisovna pro uchování uzavřených spisů a vyřízených digitálních dokumentů po dobu skartační lhůty (eSSL je spisovnou pro dokumenty v digitální podobě)
- Rozhraní eSSL zajišťující úkony spojené s dokumenty a procesy evidence dokumentů a správy jejich metadat v eSSL formou aplikačních služeb pro další informační systémy úřadu (samostatné evidence dokumentů i systémy, které dokumenty nespravují)
- Samostatné evidence dokumentů integrované na rozhraní eSSL

Jelikož legislativa obecně počítá s tím, že v rámci úřadu je vždy provozován jeden eSSL a ostatní ISSD jsou na něj integrovány a úkony spojené s dokumenty se realizují formou rozhraní eSSL, měla by v úřadu být implementována integrace všech samostatných evidencí dokumentů (pokud samy nezajišťují minimální požadavky stanovené NSESSS pro samostatné evidence dokumentů) s eSSL a samotný eSSL navázán na úložiště pro uchovávání komponent digitálních dokumentů. Na obrázku níže je znázorněn obecný stav pochopení integrace eSSL za využití jednoho centrálního úložiště pro digitální dokumenty.

Hovoříme-li o integraci samostatné evidence dokumentů s eSSL a o správě úkonů spojených s dokumentem, může tato integrace být na úrovni byznysových objektů a jejich metadat řešena v souladu s následujícími pravidly:

1. Digitální dokument, respektive jeho komponenty a datové soubory, jsou uloženy v úložišti digitálních dokumentů, které zajišťuje péči o digitální soubory
2. Metadata o dokumentu jsou spravována evidenčním nástrojem, tedy:
    - eSSL, nebo
    - informačním systémem, který plní funkci samostatné evidence
3. Se soubory v úložišti jsou oprávněny pracovat:
    - eSSL, nebo
    - samostatná evidence dokumentů, nebo
    - samostatná evidence dokumentů integrovaná na eSSL prostřednictvím rozhraní eSSL
4. Ve Jmenném rejstříku se vede evidence údajů o subjektech, jejichž se týkají dokumenty evidované ve spisové službě

Atestace eSSL

Novelou Zákona z roku 2021 (§ 69b-d) bylo stanoveno, že veřejnoprávní původci budou postupně muset přejít a využívat výhradně systémy eSSL, které jsou atestované. Atestace budou prováděny atestačním střediskem, které určí Ministerstvo vnitra (v současnosti je určena agentura ČAS), případně pokud není určeno, tak samotným ministerstvem. Proces atestace není pouze formální, ale spočívá v tom, že atestační středisko provede funkční testy dle stanovených atestačních scénářů . Atestační scénáře jsou veřejně dostupné na stránkách agentury ČAS . V případě, že eSSL splňuje podmínky stanovené Zákonem, vyhláškou a NSESSS, tak

středisko vydá vystaví žadateli písemný atest (platný 2 roky), který je následně zveřejněn, jak na stránkách střediska, tak i ve Věstníku MV. Chystaná novelizace z roku 2024 přináší několik zásadních změn:

- Posun lhůt
  - Od 1. ledna 2025 zákaz nabídky a dodávky neatestovaných eSSL veřejnoprávním původcům
  - Od 1. ledna 2027 bude muset většina veřejnoprávních původců již využívat výhradně atestovaný eSSL
- Vyjmutí malých obcí a škol z povinnosti mít atestovaný eSSL
- Vyjmutí a úprava povinností IS bezpečnostních složek v oblasti atestace eSSL
- Veřejnoprávní původci, resp. jejich IS (nejenom eSSL), budou muset umět dokumenty opatřovat strojově čitelnými metadaty
- Reatestace zůstává 1x za 2 roky a pokud se v tomto období změní legislativa či technické podmínky (např. uvolnění nového releasu, ovšem bez zásadních změn), tak je možné daný eSSL využívat až do konce platnosti původního atestu a reatestovat ho až v další dvouroční lhůtě
  - MV může v případě pochybností (např. na základě kontroly) zažádat středisko o reatest

Vazby na architekturu informačního systému veřejné správy

V rámci architektury každého informačního systému veřejné správy sloužícího pro podporu výkonu činností agendy veřejné správy je nutno myslet také na oblast výkonu spisové služby. Vzhledem k tomu, že prakticky v každé agendě veřejné správy se buď vytváří, nebo zpracovávají, nebo odesílají, nebo evidují dokumenty, anebo u ní dochází k zápisu záznamu do spisu (z pohledu legislativy týkající se spisové služby), je nutno zajistit úkony spojené se spisem a dokumentem. Vesměs existují dvě formy, jak zajistit povinnosti výkonu spisové služby v souvislosti s daným ISSD, a to následující:

1. Integrovat samostatnou evidenci dokumentů na eSSL prostřednictvím předepsaného rozhraní a zajistit, aby úkony spojené s dokumentem vykonávala samostatná evidence dokumentů prostřednictvím tohoto rozhraní.
2. Zajistit, aby daný ISSD splňoval požadavky NSESSS kladené na samostatnou evidenci dokumentů a vykonávat úkony spojené s dokumenty a všechny procesy týkající se výkonu spisové služby v samostatné evidenci tímto systémem.

Vazby na architekturu provozních systémů

Velice často se zapomíná na to, že výkon spisové služby se týká všech dokumentů, a tedy nejen úředních dokumentů typu podání a rozhodnutí v rámci výkonu agend veřejné správy. U veřejnoprávních původců se jedná o evidenci a správu veškerých dokumentů (s výjimkou těch, které si daný původce odůvodněně vyňal z evidence ve svém spisovém řádu), a tedy je nutno zajistit výkon spisové služby v elektronické podobě také pro pracovní a provozní dokumenty. To se týká jak dokumentů pracovního charakteru (zápisy z porad, organizační a řídící dokumenty, řídící akty, interní sdělení), tak ale také všech dokumentů ekonomického a provozního charakteru (faktury, objednávky, smlouvy ekonomické doklady, personální dokumentace, žádanky, závěrky a výkazy apod.).

V případě provozních informačních systémů jednoznačně doporučujeme jejich integraci na eSSL. Zejména u ekonomických informačních systémů, systému pro řízení personalistiky a mezd a zdrojů a dalších manažerských informačních systémů týkajících se různých žádanek, evidencí, a workflow procesů, se dost často na výkon spisové služby zapomíná. Zde je vhodná integrace na eSSL, neboť zajištění splnění všech požadavků NSESSS na samostatné evidence pro tyto systémy by s sebou přineslo neúměrné finanční náklady spojené s pořízením a rozvojem těchto provozních IS. Integrací na eSSL se také zajistí řádné realizování skartačních řízení u těchto druhů dokumentů.

Souvislosti s architekturou údajů o subjektech

Určení původci, kteří vykonávají spisovou službu v elektronické podobě, musejí podle § 64, odst. 4 až 8, Zákona č. 499/2004 Sb., o archivnictví a spisové službě provozovat jako samostatnou komponentu takzvaný "Jmenný rejstřík", kam zapisují určené minimální údaje o všech subjektech, kterých se týkají jimi evidované dokumenty.

Realizace propojení jmenného rejstříku a ostatních komponent, respektive realizace procesů evidence subjektů je následující:

- V úřadu je u každého eSSL jako logická komponenta i Jmenný rejstřík. Funkce Jmenného rejstříku může za splnění všech dalších podmínek zastávat i zdroj evidence subjektů.
- Do jmenného rejstříku se evidují údaje o všech subjektech, kterých se týkají evidované dokumenty a to s využitím AIFO fyzických osob v agendě spisové služby, nikoliv v agendách, ve kterých se o osobách úřaduje. Pro vazby jmenného rejstříku na eSSL a další evidence dokumentů je třeba využívat interní identifikátor, nikoliv AIFO.
- Evidence subjektů ve Jmenném rejstříku a evidence subjektů za účelem úřadování v agendě jsou dvě oddělené věci, proto je nutno dbát na správné postupy, viz související kapitoly k evidenci subjektů a identifikátorům.

Výběr a dlouhodobá archivace digitálních dat

Výběr archiválií z dokumentů provádí příslušný archiv podle své působnosti a to nejpozději po uplynutí uschovacích (skartačních) lhůt s tím, že ideální je označit podstatná data za archiválie mnohem dříve. Kritériem výběru je trvalá hodnota dokumentu daná mj. jeho hospodářským, právním, politickým, informačním, historickým, kulturním nebo vědeckým významem. Veškeré archiválie jsou **evidovány** jako součást národního archivního dědictví. Úkolem archivů je dále trvalé **uložení** archiválií a jejich **ochrana**, archivní **zpracování a zpřístupnění**.

Digitální archiválie lze uchovávat pouze v akreditovaném digitálním archivu metodika. Od roku 2015 je zatím jedinou infrastrukturou tohoto typu **Národní digitální archiv (NDA)** provozovaný Národním archivem. Ten na Národním archivním portále (NArP) mj. nabízí nástroje pro skartační řízení a přejímku digitálních archiválií.

Výstupní formáty dle pravidel stanovených vyhláškou č. 259/2012 Sb. pokrývají nejběžnější typy dokumentů . U původců se však mohou vyskytovat i jiné typy dokumentů, u kterých není výstupní formát vyhláškou určen. Mimo jiné i proto, že na jeho stanovení není všeobecná shoda. Z hlediska dlouhodobé archivace i potřeb veřejné správy by však bylo přínosné, kdyby existoval registr formátů shrnující vhodnost používání určitého formátu. Proto také vznikl Národní standard formátů pro archivaci, který určuje, jaký formát je pro různé typy dokumentů (dokument tak, jak jej definuje zákon o archivnictví) vhodný k archivaci.

Důležitým zdrojem pro výběr archiválií jsou dokumenty spravované v eSSL. Archivy provádějí dohled nad vedením eSSL a následně dokumenty vybírají ve skartačním řízení k trvalému uložení. Dalšími zdroji dokumentů pro výběr archiválií jsou **samostatné evidence dokumentů**, na něž se také vztahuje NSESSS.

Možné způsoby zajištění digitální kontinuity dokumentů

Je velmi důležité pamatovat na problematiku digitální kontinuity a o své elektronické dokumenty se aktivně starat. Veřejnoprávní původci musí zajistit evidenci dokumentů a to buď v systému spisové služby, nebo v samostatných evidencích dokumentů. Oba výše uvedené způsoby pak musí splňovat požadavky Národního standardu pro elektronické systémy spisové služby v souladu se zákonem č. 499/2004 Sb. Zaměříme-li se na elektronické dokumenty ve smyslu nařízení eIDAS, pak budeme hovořit o elektronickém systému spisové služby a elektronických evidencích dokumentů. Jedním z klíčových požadavků Národního standardu je existence tzv. transakčního protokolu – zápisu provedených operací uskutečněných v rámci elektronického systému spisové

služby nebo v rámci samostatné evidence dokumentů v elektronické podobě. Transakční protokol v případě elektronických dokumentů zajišťuje, že od okamžiku zaevidování dokumentu až do okamžiku jeho předání do archivu nebo okamžiku vyřazení a zničení je systematicky evidována jakákoliv operace týkající se evidovaného dokumentu. Tímto je zcela jednoznačně po dobu životního cyklu dokumentu zajištěno, že lze v rámci evidenčního systému garantovat určité vlastnosti elektronického dokumentu, zejména pak věrohodnost původu a neporušenost obsahu. U každého elektronického dokumentu musí být rovněž zajištěna po celou dobu životního cyklu jeho čitelnost, a to jak v technickém slova smyslu, tak z pohledu jeho uživatelsky vnímatelné podoby.

U veřejnoprávních původců je s ohledem na výše zmíněný požadavek prokázání věrohodnosti původu a neporušitelnosti obsahu dokumentu stanovena zákonná povinnost ověřování elektronických podpisů, elektronických pečetí a elektronických časových razítek, pokud je příchozí elektronický dokument obsahuje. Uvedení původci jsou ze zákona povinni výsledky ověření zaznamenat ve svých evidenčních systémech, které jak bylo uvedeno výše, musí splňovat zákonem stanovené požadavky, včetně požadavku na vedení transakčního protokolu. Proto není nutné po prvotním ověření u veřejnoprávních původců používat takové metody, jaké se používají běžně pro zajištění „věrohodnosti původu“ u soukromoprávních původců - například není nutné opětovně opatřovat elektronické dokumenty časovými razítky před jejich expirací a podobně - věrohodnost původu elektronických dokumentů je u veřejnoprávních původců zajištěna řádnou systematickou evidencí dokumentů v určených systémech, kde je navíc pomocí transakčního protokolu možné po celou dobu životního cyklu dokumentu prokázat veškeré operace, které se s evidovaným dokumentem uskutečnily - tj. pro prokázání věrohodnosti původu je zcela dostačující systematická evidence a transakční protokol[3)].

Výše uvedené lze u veřejnoprávních původců i snadno ověřit – audit systémů zajišťujících vedení spisové služby je možné realizovat v průběhu času a každý veřejnoprávní původce má zákonem stanovenou povinnost kontroly těchto činností. Elektronické systémy spisové služby, ale i některé významné samostatné evidence dokumentů (typicky informační systémy veřejné správy), splňují z pohledu zákona o kybernetické bezpečnosti charakteristiku tzv. významného informačního systému, neboť v případě jejich výpadku nebo nesprávného fungování by veřejnoprávní původci nemohli plnit řádně a souvisle svůj výkon. S ohledem na to by tyto měly být jako významné informační systémy identifikovány a oznámeny Národnímu úřadu pro kybernetickou a informační společnost procedurou dle kybernetického zákona. Tím se tyto systémy dostanou rovněž pod pravidelný dohled útvarů zajišťujících kybernetickou bezpečnost.

Elektronické systémy spisové služby a samostatné evidence dokumentů též zpracovávají osobní údaje fyzických osob, proto veřejnoprávní původci nad těmito systémy mají s ohledem na povinnosti vyplývající z obecného nařízení na ochranu osobních údajů a ze zákona o zpracování osobních údajů řadu povinností, které též zvyšují celkovou důvěryhodnost systémů, ve kterých veřejnoprávní původci evidují své dokumenty.

Výše uvedenými opatřeními lze u veřejnoprávních původců zcela spolehlivě prokázat věrohodnost původu a to i u přijatých dokumentů obsahující elektronické podpisy, elektronické pečetě a elektronická časová razítka a to bez nutnosti jejich opětovného opatřování časovými razítky nebo jinými autentizačními či autorizačními prvky.

Možné problémy

Možným rizikem zajištění digitální kontinuity založeného na základě transakčních protokolů eSSL je problematika kolizních dokumentů. Jedná se o situaci, kdy je do transakčního protokolu v souladu s NSESSS poznamenán otisk (tzv. hash) dokumentu spolu s označení použitého hashovacího algoritmu, ovšem stejný hash může odpovídat i jiným dokumentům. Následně není možné, především u přijatých dokumentů, dovodit o jakém dokumentu (skrze jeho hash) transakční protokol pojednává, což výrazně komplikuje případné dosvědčení právní validity.

Pro eliminaci tohoto rizika, lze využít postupy, kterými se prodlužuje ověřitelnost podle standardu ETSI (The European Telecommunications Standards Institute) a který odpovídá předpisům eIDAS. Jde tedy o opakovaného přidávání kvalifikovaných elektronických časových razítek a validačních informací sloužící k prodlužování možnosti ověření platnosti podpisů a pečetí na elektronických dokumentech. Zjednodušeně lze říci, že tato opatření mají charakter nového elektronického podepsání, nového zapečetění či nového opatření kvalifikovaným

elektronickým časovým razítkem. Tyto možnosti totiž znamenají, že se na autentizaci původního dokumentu použijí aktuálně dostatečně silné kryptografické postupy a algoritmy (konkrétně dostatečně robustní hashovací funkce a dostatečně velké klíče), a tím je – opět na určitou dobu – dostatečně ztíženo hledání kolizních dokumentů. Vzhledem k různým právním účinkům elektronických podpisů (představujících projev vůle), elektronických pečetí (představujících vyjádření původu) a časových razítek (představujících „fixaci v čase“) se v praxi, k prodloužení možnosti ověření platnosti původních podpisů a pečetí, využívají právě kvalifikovaná elektronická časová razítka. Důležité je, aby každý jednotlivý krok tohoto dlouhodobého procesu byl proveden včas. Tedy aby další časové razítko bylo přidáno ještě dříve, než zaúčinkuje tzv. časová pojistka (než skončí v čase omezená možnost ověření původního podpisu či pečeti). Případně promeškání nejzazšího okamžiku způsobí, že pozdě přidané časové razítko již nemá prodlužující účinek.

V praxi přitom není nutné (včas) přidávat časová razítka k jednotlivým dokumentům. Vhodnými postupy je možné minimalizovat spotřebu časových razítek, například společným umístěním více dokumentů (či pouze jejich otisků) do vhodného kontejneru (ASiC), a časovými razítky opatřovat pouze kontejner jako takový. Sdružování do kontejnerů je vhodné dle logického spojení dokumentů, například do úrovně spisů. Stejně tak není podstatné, kdo podniká výše naznačená opatření, nutná pro zajištění digitální kontinuity dokumentů.

Je však nutné konstatovat, že ač riziko kolizních dokumentů existuje, současné legislativní prostředí nedává veřejnoprávním původcům dostatečný prostor k rozhodnutí a vlastnímu zvážení rizik a dodatečné připojování elektronických pečetí či časových razítek by mohlo být v rozporu s péčí řádného hospodáře, neboť u nákladů na zajištění takového postupu by se mohlo jednat o neúčelně vynaložené prostředky veřejného rozpočtu.

Dalším možným řešení je předávání transakčních protokolů do archivu v krátké lhůtě.

Systémy a služby spojené s právním řádem a legislativou

Popis Systémů a služeb spojených s právním řádem a legislativou

Veřejná správa se řídí primárně legislativou. Proto je nesmírně důležité jednak právnímu řádu dobře rozumět a jednak zahrnout legislativu jako motivační a kontraktační rámec do architektur.

Základní komponenty právních systémů státu

Základní informační systémy a služby státu týkající se práva a legislativy

Systém	Správce	Popis	Příklady užití
eSbírka	Ministerstvo vnitra	Elektronická sbírka právních předpisů s jejich konsolidovaným časovým zněním	Pomocí služeb rozhraní ESEL bude možné automatizovaně přebírat dekomponované právní předpisy a mít je tak jako vazbové zdroje pro motivační a procesní a byznysovou architekturu. eSbírka bude představovat výchozí referenční zdroj znění a změn právních předpisů
eLegislativa	Ministerstvo vnitra	Informační systém pro podporu tvorby a projednávání návrhů legislativních změn a pro elektronizaci procesu přijímání legislativy	V rámci služeb ESEL bude k dispozici sledování stavu přípravy a projednávání změn a návrhů, ale také prostředí a nástroje pro tvorbu návrhů na legislativní úpravy (může pocházet z výsledků návrhů optimalizace dle architektury)

Systém	Správce	Popis	Příklady užití
ODOK	Úřad vlády	IS pro oběh dokumentů určených pro vládní agendu a pro jednání vlády a jejich orgánů	V tomto informačním systému jsou dokumenty a informace v rámci vládní agendy, podklady pro jednání vlády, ale jeho prostřednictvím se sledují i vládní a legislativní úkoly
EKLEP	Úřad vlády	Elektronická knihovna legislativního procesu slouží jako IS pro podporu celého procesu projednáván´, připomínkování a schvalování legislativních návrhů	
VEKLEP	Úřad vlády	Veřejná část knihovny EKLEP	Je publikováno i schematicky podle XML schémat metadat a jako opendata, takže se dá využít v řadě případů jako informační zdroj
RPP	Ministerstvo vnitra	V Registru práv a povinností jsou také referenční a závazné údaje o jednotlivých agendách, vazbách na legislativu, působnostech OVM a úkonech a činnostech v těchto agendách	Slouží jako autoritativní a referenční zdroj o výkonu veřejné správy

Každý z těchto IS může a má být využíván jednak jako zdroj informací pro úřady a jednak jako jeden z komponent při optimalizaci činností úřadu. Kupříkladu, chceme-li v úřadu optimalizovat agendu, měli bychom mít její architekturu. Jedním ze vstupů pro tuto architekturu je legislativa (zdroj ESEL) a agendový model dané agendy (zdroj RPP). Po návrhu procesní optimalizace bude pravděpodobně nutné novelizovat i legislativu, k čemuž zase poslouží i výše zmíněné informační systémy.

Pravidla Systémů a služeb spojených s právním řádem a legislativou

Míra možnosti a dokonce povinnosti využívat výše zmíněné informační systémy a jejich sdílené služby závisí na tom, v jakém postavení vůči konkrétní legislativě je příslušný úřad.

V tomto případě tedy můžeme rozdělit úřady do třech následujících kategorií:

- Gestor legislativy: Je zodpovědný za přípravu, provádění procesu připomínkování a projednání a následnou realizaci schválené legislativy. Gestor by také měl pravidelně provádět zhodnocení platné legislativy a na základě toho navrhovat její úpravy.
- Spolupracující subjekt: Jedná se o subjekt, který se aktivně podílí na spolutvorbě legislativy a je aktivně zapojen do procesu připomínkování a vyhodnocování daných návrhů
- Uživatel legislativy: Jedná se o subjekt, který se Danou legislativou řídí ať už v rámci veřejnoprávní činnosti jako výkon působnosti v dané agendě, nebo je pro něj příslušná legislativa jinou formou nějak závazná a ovlivňuje jeho činnost

V Každé z těchto třech základních rolí mohou být výše zmíněné informační systémy aktivně používány.

Nesmí se zapomínat ani na povinnosti výkonu spisové služby, ty se pochopitelně vztahují i na procesy návrhu a projednávání legislativy. Jsem-li tedy gestor za legislativu, především si zajistím integraci svých autorských systémů na ESSL a následně i integraci na závazně používané informační systémy (eLegislativa, ODOK, EKLEP, apod.).

Při vyhodnocování a následné přípravě návrhů na změnu jsou dvěma klíčovými zdroji platná legislativa (aktuální znění právních předpisů a jejich vazeb) a dopad na faktický výkon (zdrojem je RPP a agendový model a seznam úkonů v agendě). Pomocí vazeb s ostatními právními předpisy si také úřad zmapuje souvislosti na další schopnosti. Třeba u agendového zákona je třeba zohlednit i povinnosti spisové služby, povinnost nevyžadovat údaje, které již mám, apod. I s ohledem na to je vhodné jako zdroj mít vždy aktuální či očekávaná znění právních

předpisů.

Při tvorbě architektury je pak nanejvýš vhodné mít prvky architektury s vazbou na příslušnou legislativu. Například pokud spravuji informační systém, tak ten slouží pro podporu procesu v zákoně. Tedy vím, že systém provozuji na základě zákona o ISVS a na základě příslušných agendových zákonů a požadavky na funkce musi zajistit realizaci příslušných procesů v jednotlivých zákonech.

Zdroje informací o právních předpisech a jejich promítnutí do agend veřejné správy se hodí i pro tvorbu a aktualizaci vnitřních směrnic a předpisů v organizaci. Kupříkladu, změní-li se legislativa k základním registrům či ke spisové službě, vím, že to bude mít dopad na moje procesy a tedy i na předpisy a směrnice jež procesy určují. Dojde tedy jistě ke změnám agendových procesních metodik, ke změně Spisového řádu, apod. K tomu také mám využívat výše zmíněné zdroje a zajistit jejich integraci na komponenty, které využívám k udržování dokumentace.

Pokud daný úřad není gestorem za příslušnou legislativu, ale přesto je pro něj legislativa závazná, pak by měl také splnit některé z výše uvedených základních principů. Aktuální údaje o stavu právních předpisů včetně vazby mezi jednotlivými ustanoveními a jednotlivými právními předpisy musí sloužit jako základ pro byznysovou architekturu. Druhým zdrojem jsou pak údaje v registru práv a povinností.

Je vhodné tedy:

- Vybudovat a udržovat mechanismus, jak pokud možno automatizovaně zpracovávat dekomponované právní předpisy
  - Lze realizovat s využitím služeb eSbírky, či obdobného systému
  - Zajistit si notifikace o aktualizacích právních předpisů, jež mě zajímají a o aktualizacích vazeb z jiných právních předpisů na ně
- Vytvořit procesy a podporu pro sledování návrhů změn a stavu jejich projednávání
- Být schopen přiřadit klíčové elementy architektury ke konkrétním ustanovením či alespoň ke konkrétním právním předpisům
- Udržovat povědomost o všech právních předpisech, kterými se řídím

Z hlediska architektury se očekávají následující změny na centrální i lokální úrovni

- Po uvedení systému e-Sbírka do ostrého provozu (předpoklad k 1. 1. 2022) přehodnotí úřady politiku pořizování komerčních právních informačních systémů, zejména objem a rozsah potřebných licencí pro výkon své působnosti s přihlédnutím k individuální povaze pracovní činnosti konkrétních zaměstnanců, kteří vyžívají tyto systémy ke své práci. Případný poptávaný rozsah licencí komerčních právních informačních systémů pak při přihlédnutí k smluvním podmínkám dodávek kontrahovaných v této oblasti a potřebám konkrétních pracovníků následně omezí na uspokojení pouze těch potřeb podmiňujících výkon své působnosti, které nelze využitím systému e-Sbírka pokrýt.
- Informační systém eSbírka a eLegislativa a ODoK musí být funkčně propojeny tak, aby byly naplněny předpoklady fungování elektronického legislativního procesu podle zákona č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv (zákon o Sbírce zákonů a mezinárodních smluv), ve znění pozdějších předpisů.
- Od okamžiku spuštění informačního systému e-Sbírka a e-Legislativa budou všechny úřady povinny ve svých systémech a nově vytvářených materiálech obohacovat právní citace právních předpisů obsažených v e-Sbírce typu "§1 zákona č. 100/2000 Sb." technicky o odkazy do systému e-Sbírka, které budou vytvářet pomocí funkcionality pro tvorbu citací obsažené v e-Sbírce.

Elektronické úkony a doručování

Popis Informačního systému datových schránek

Pro zajištění důvěryhodné, bezpečné a průkazné elektronické komunikace mezi orgány veřejné moci na straně jedné a fyzickými či právnickými na straně druhé, jakož i mezi orgány veřejné moci navzájem, provozuje Ministerstvo vnitra ČR informační systém datových schránek (také jako "ISDS"). Ministerstvo vnitra ČR a spolupracující subjekty se při provozování ISDS řídí provozním řádem, který je pro ně závazný.

Orgány veřejné moci jsou povinni mezi sebou komunikovat prostřednictvím ISDS, stejně tak s klientem veřejné správy, pokud datovou schránku vlastní.

Typy datové schránky

Způsob, resp. proces zřízení datové schránky se liší podle typu subjektu, pro který má být datová schránka zřízena. Typ subjektu určuje, zda se jedná o datovou schránku zřizovanou ze zákona, tedy automaticky, nebo o datovou schránku zřizovanou na žádost dle následující tabulky

Typ subjektu	Typ datové schránky v ISDS	Zřízena
Orgán veřejné moci	OVM (10)	Ze zákona
Fyzická osoba, která je v roli OVM	OVM_FO (14)	Ze zákona
Podnikající fyzická osoba, která je v roli OVM	OVM_PFO (15)	Ze zákona
Právnická osoba v roli OVM	OVM_PO (16)	Ze zákona
Právnická osoba zapsaná v obchodním rejstříku	PO (20)	Ze zákona
Podnikající fyzická osoba - advokát	PFO_ADVOK (31)	Ze zákona
Podnikající fyzická osoba - daňový poradce	PFO_DANPOR (32)	Ze zákona
Podnikající fyzická osoba - insolvenční správce	PFO_INSSPR (33)	Ze zákona
Podnikající fyzická osoba - statutární auditor (OSVČ nebo zaměstnanec)	PFO_AUDITOR (34)	Ze zákona
Fyzická osoba	FO (40)	Na žádost
Podnikající fyzická osoba	PFO (30)	Na žádost
Právnická osoba - na žádost	PO_REQ (22)	Na žádost
Schránka OVM zřízená na žádost	OVM_REQ (13	Na žádost

Zápis rozhodnutí do Registru práv a povinností

Zákon o základních registrech vyžaduje, aby při každé změně referenčního údaje v základních registrech došlo také k zápisu o příslušném rozhodnutí, na jehož základě byl údaj změněn, do Registru práv a povinností. Ministerstvo vnitra je v agendě datových schránek editorem jediného referenčního údaje – identifikátoru datové schránky. Při každém zápisu i výmazu tohoto údaje do Registru obyvatel nebo Registru osob proto ISDS provádí zároveň zápis do Registru práv a povinností.

Využití údajů základních registrů (ZR)

Ministerstvo vnitra rozsáhle využívá referenční údaje základních registrů pro účely správy datových schránek. Základní registry tak představují nejdůležitější zdroj dat, na základě kterých jsou datové schránky zřizovány i znepřístupňovány a také aktualizovány identifikační údaje datových schránek a jejich uživatelů.

Zřizování datových schránek ze zákona

Na základě informací z Registru osob jsou zřizovány datové schránky subjektům, kterým se datová schránka zřizuje ze zákona. Výjimku představuje malá množina subjektů, které v Registru osob nejsou vedeny, protože nemají přiděleno své unikátní IČO (orgány veřejné moci bez právní subjektivity).

Znepřístupňování datových schránek

Na základě informací z Registru osob jsou znepřístupňovány datové schránky subjektů, u kterých bylo v Registru osob vyplněno datum zániku. Obdobně, jakmile je u fyzické osoby v Registru obyvatel vyplněno datum úmrtí, datová schránka je k tomuto datu znepřístupněna.

Aktualizace údajů datových schránek

Pro datové schránky všech typů platí, že pokud je subjekt veden v základních registrech, identifikační údaje datové schránky jsou automatizovaně přebírány ze Základních registrů. Tzn. změny názvu subjektu nebo adresy sídla není nutné Ministerstvu hlásit – změny jsou promítnuty automaticky.

Přidání / odebrání Oprávněné osoby

Oprávněné osoby u datových schránek těch subjektů, které jsou zapsány v Registru osob, jsou aktualizovány podle změn ve výčtu statutárních zástupců vedených u daného subjektu v Registru osob. Tzn. je-li do registru zapsán nový statutární zástupce, automatizovaně mu je zřízen účet Oprávněné osoby u datové schránky subjektu a naopak, je-li statutární zástupce z registru odebrán, jeho účet Oprávněné osoby u datové schránky je zrušen.

Aktualizace osobních údajů uživatelů datových schránek

U všech uživatelů datových schránek se Ministerstvo vnitra pokouší o jejich automatizované ztotožnění vůči příslušnému záznamu v Registru obyvatel. U těch uživatelů, kde se ztotožnění zdařilo, jsou automatizovaně přebírány aktuální referenční údaje z Registru obyvatel. Tzn. např. v případě změny příjmení nebo adresy pobytu nemusí držitel datové schránky Ministerstvu vnitra nic hlásit – změna je promítnuta automaticky.

Pravidla Informačního systému datových schránek

Úřadu je doporučeno využívat systém ISDS jako integrální součást své elektronické spisové služby. Úřady musí mezi sebou komunikovat prostřednictvím systému ISDS a svých datových schránek, pokud se jedná o výměnu dokumentů a jejich zaručeného doručení. Pokud se jedná o výměnu údajů mezi úřady, nevyužívají se datové schránky, ale propojený datový fond a jeho referenční rozhraní. Je nutné brát v potaz, že veškeré úkony činěné skrze datovou zprávu směrem do úřadu od klienta VS se pokládají za elektronicky podepsané a není potřeba po klientovi vyžadovat žádné další formy autorizace.

ISDS umožňují na vyžádání u věcného správce (Ministerstva vnitra) využívat identitní prostor datových schránek k přihlašování do vlastních řešení - typicky portálů. **Tento způsob identifikace a autentizace klienta VS bude umožněn pouze do 1.7.2020**, kdy vyprší přechodné ustanovení zákona 250/2017 Sb., které zavádí povinnost využívat systém Národní identitní autority .

Pro zajištění digitální kontinuity datové zprávy, podobně jako v části Systém správy dokumentů, je z pohledu uživatele (příjemce) nutné si vždy uložit nejen přijatý dokument, ale celou datovou zprávu (obálka + dokument). Tato celá datová zpráva lze kdykoliv zpětně věřit proti samotnému informačnímu systému datových schránek, samotný dokument však ne.

Jednotný identitní prostor veřejné správy

Popis Jednotného identitního prostoru veřejné správy

Jednotný identitní prostor (JIP) informačních systémů veřejné správy a Katalog autentizačních a autorizačních služeb (KAAS) je autentizační informační systém podle § 56a zákona o základních registrech a jeho správcem je Ministerstvo vnitra. Na základě znění zákona zavedení jakékoli osoby do tohoto autentizačního informačního systému vyžaduje její jednoznačné ztotožnění oproti základnímu registru obyvatel. Ministerstvo dále spravuje prostředky pro autentizaci, které vydává.

V rámci současného stavu (As-Is 2018) předpokládá co nejširší používání autentizačního informačního systému JIP/KAAS pro splnění zásadních podmínek pro identifikaci a autentizaci interních uživatelů informačních systémů veřejné správy. **Pro ty informační systémy, kde interní uživatelé informačního systému jsou zaváděni úřady, které nejsou správci tohoto informačního systému, je použití autentizačního informačního systému JIP/KAAS povinností.**

Využití systému JIP/KAAS je možné i s pomocí prostředků národního identitního prostoru. Aby přihlašování do JIP/KAAS bylo umožněno i jinými prostředky národního identitního prostoru, než je např. občanský průkaz nebo jméno+heslo+sms, je potřeba zajistit úředníkům jiný prostředek jedním z následujících způsobů:

- Sekce pro státní službu na MV zajistí jednotný prostředek identity úředníka v rámci národního identitního prostoru.
- Jiný orgán veřejné moci zajistí vydávání profesních identit v rámci národního identitního prostoru z nichž požadavky na úřední identitu (včetně zajištění finančních prostředků) sdělí Sekce pro státní službu na MV.

Unikátní a jednotná identita zaměstnance v rámci veřejné správy jako celku je nutná ve dvou rovinách, jako:

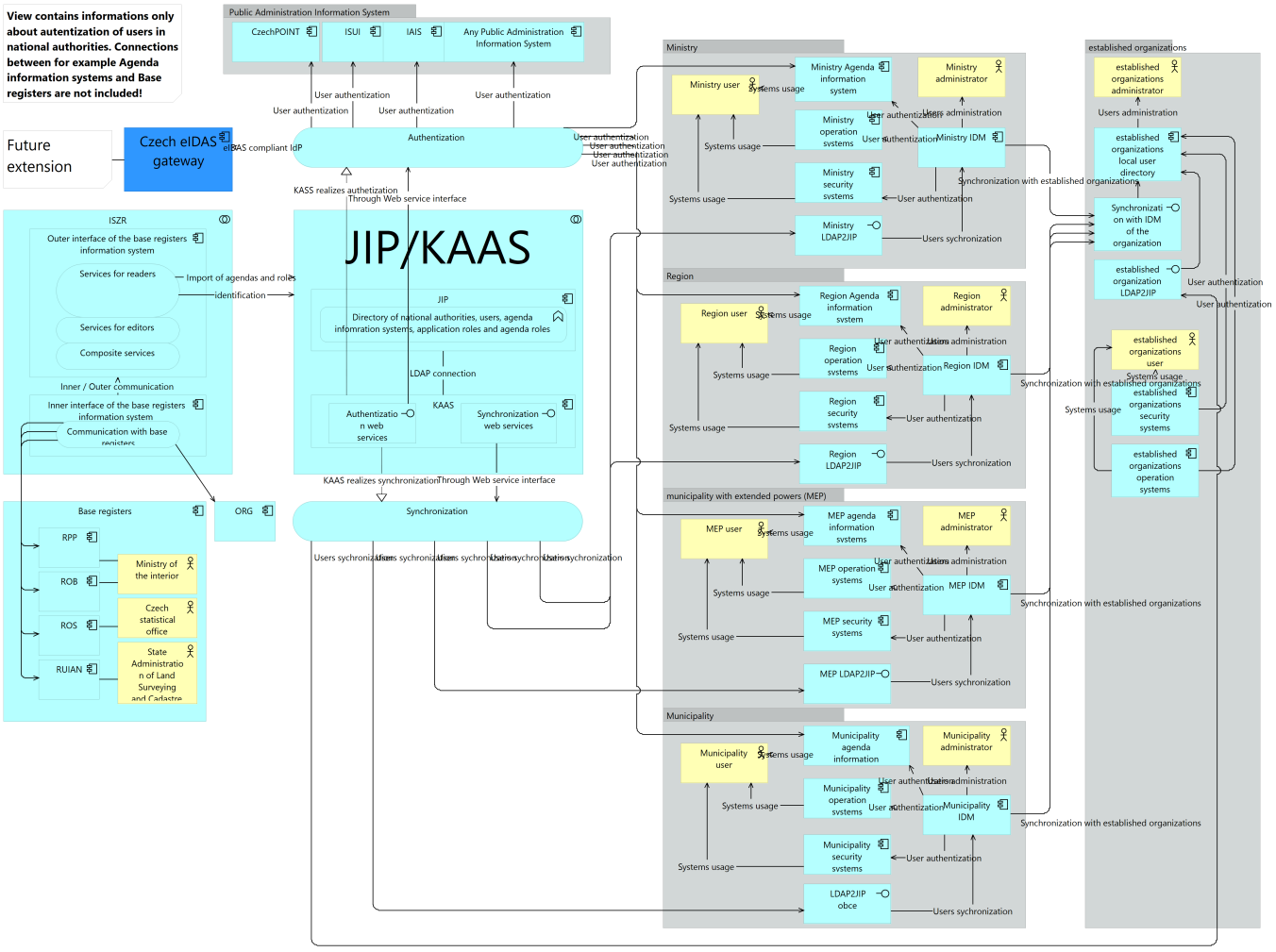
- Aktivní identita a identifikace - opravňuje zaměstnance k přístupu k informacím a informačním systémům, (+ k prostorám a zařízením) - zaměstnanec jako subjekt
- Pasivní identita a identifikace - jednoznačně označuje předmětného (většinou zodpovědného) zaměstnance v rámci centrálních nástrojů řízení a koordinace veřejné správy - zaměstnanec jako objekt evidence (totéž pro pozici - služební místo a vzájemný vztah k zaměstnanci).

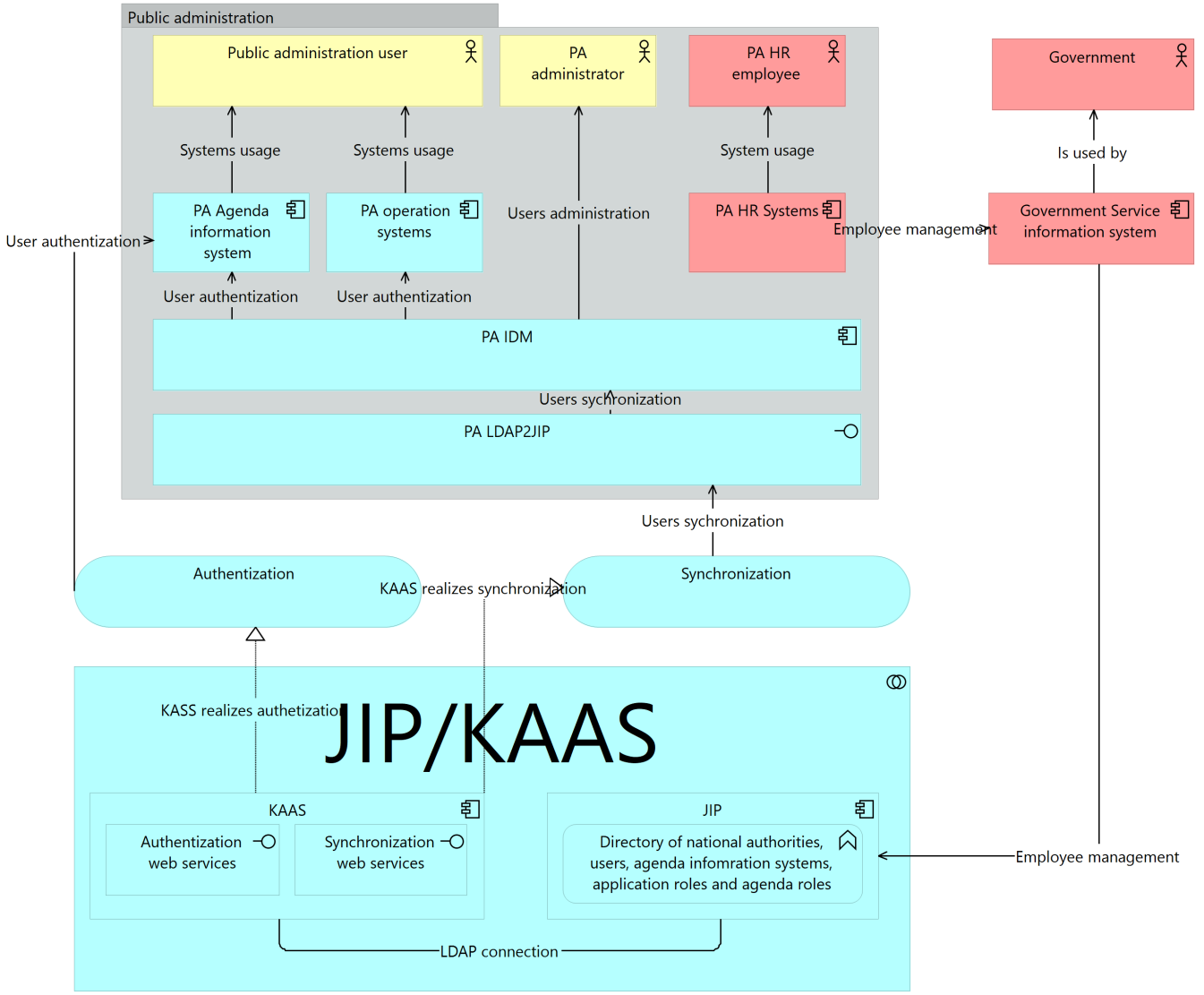
Stávající řešení JIP/KAAS nebylo určeno pro takto široké účely a koncepčně ani fyzicky nevyhovuje změněným nárokům. Jeho budoucí rozvoj musí vycházet z diskuse o reálných potřebách všech zainteresovaných. Předpokladem budoucího efektivního využívání jednotného identitního prostoru veřejné správy a naplnění některých konceptů architektonické vize eGovernmentu, jako je například transakční Portál úředníka, poskytující kromě jiného i společné personální, vzdělávací, nákupní a další funkce, musí dojít ke sjednocení identit a identifikací pracovníků veřejné správy bez ohledu na typ zaměstnaneckého/ služebního poměru, tj. společně pro:

- státní službu, dle zák. č. 234/2014 Sb., o státní službě,
- služební poměr, dle zák. č. 361/2003 Sb. o služebním poměru příslušníků bezpečnostních sborů,
- poměr dle zák. č. 312/2002 Sb. Zákon o úřednících územních samosprávných celků,
- zaměstnanecký poměr, dle zák. č. 262/2006 Sb. Zákoník práce.

Důležité je, že vznik a zejména zánik identifikace a oprávnění k roli musí v JIP vznikat na základě jeho integrace s lokálními personálními systémy, resp. s centrálními služebními a zaměstnaneckými registry na jedné straně a v integraci na lokální IDM/IAM systémy na druhé straně. Tyto základní požadavky a potřeby budou formovat budoucí architekturu JIP a nezbytných spolupracujících systémů.

Pohledy na jednotný identitní prostor


View contains informations only about autentization of users in national authorities. Connections between for example Agenda information systems and Base registers are not included!
Future extension
Czech eIDAS gateway
Public Administration Information System
CzechPOINT
ISUI
IAIS
Any Public Administration Information System
User authentization
eIDAS compliant IdP
Authentization
KASS realizes authetization
Through Web service interface
ISZR
Outer interface of the base registers information system
Services for readers
Services for editors
Composite services
Import of agendas and roles
identification
Inner / Outer communication
Inner interface of the base registers information system
Communication with base registers
JIP/KAAS
JIP
Directory of national authorities, users, agenda information systems, application roles and agenda roles
LDAP connection
KAAS
Authentication web services
Synchronization web services
KAAS realizes synchronization
Through Web service interface
Base registers
RPP
ROB
ROS
RUIAN
Ministry of the interior
Czech statistical office
State Administration of Land Surveying and Cadastre
ORG
Synchronization
Users sychronization
Ministry
Ministry user
Systems usage
Ministry Agenda information system
Ministry administrator
Ministry operation systems
Ministry IDM
Users administration
Ministry security systems
Ministry LDAP2JIP
Region
Region user
Region Agenda information system
Region administrator
Region operation systems
Region IDM
Region security systems
Region LDAP2JIP
municipality with extended powers (MEP)
MEP user
MEP agenda information systems
MEP administrator
MEP operation systems
MEP IDM
MEP security systems
MEP LDAP2JIP
Municipality
Municipality user
Municipality agenda information
Municipality administrator
Municipality operation systems
Municipality IDM
Municipality security systems
LDAP2JIP obce
established organizations
established organizations administrator
established organizations local user directory
Synchronization with IDM of the organization
established organization LDAP2JIP
established organizations user
established organizations security systems
established organizations operation systems
Synchronization with established organizations



Pravidla Jednotného identitního prostoru veřejné správy

Úřad musí zajistit propojení svého identitního systému (AD/LDAP/IDM) se systémem Jednotného identitního prostoru (také jako JIP/KAAS) pro tu část zaměstnanců, kteří se přihlašují k informačním systémům veřejné správy. Využití může být provedeno 2 druhy:

- Vytvoření vlastních aplikačních rolí pro systémy, jejichž je OVM správce
- Využití existujících rolí v registru práv a povinností

Pro uživatele, kteří nejsou pokrytí centrální licencí provozovatele, lze zakoupit licenci zvlášť. Cena takovéto licence je pro 1 uživatele přibližně 2 000 Kč za první rok a 500 pro další roky.

Jednotné obslužné kanály a uživatelská rozhraní úředníků

Popis Jednotných obslužných kanálů úředníků

Ve shodě s cílem a s principy poskytnout úředníkům efektivní navigační a uživatelské prostředí pro elektronické úřadování, pro elektronickou správu zdrojů úřadu a pro zaměstnaneckou samoobsluhu je potřeba výrazně posílit a rozvinou, případně nahradit dosavadní možnosti sdílených služeb Portál úředníka a CzechPOINT@Office.

Portál úředníka

Aktuálně částečně plní tuto roli pouze portál IS o Státní službě (ISoSS), který má dvě části - veřejnou část a část pro služební úřady, s přístupem přes JIP/KAAS.

Veřejná část poskytuje 3 funkce:

- Přihlašování na úřednickou zkoušku
- Evidence obsazovaných služebních míst
- Evidence provedených úřednických zkoušek

Portál ISoSS v sekci pro služební úřady umožňuje:

- Vkládání návrhů na systemizaci pracovních míst (a dále také Vlastní kontrola návrhů, Úprava návrhů, Odesílání návrhů do schvalovacího procesu, Možnost vkládání odůvodnění k návrhu, Prohlížení postupu schvalovacího procesu návrhu)

Podle architektonické vize eGovernmentu pro každého úředníka bude v jeho „kmenovém“ úřadě poskytnuto jednotné univerzální vnitřní navigační prostředí a webové uživatelské pracovní prostředí, umožňující mu přístup do všech místních a do všech centrálních informačních systémů, k nimž je z titulu svých rolí v OVS oprávněn.

Portál úředníka (PÚ) bude federativní (federalizovaný) obráceným způsobem než PVS. Tj. budou existovat jednotlivé centrální portálové služby (HR, vzdělávání, NEN, IISSP, ...), které budou připojovány do lokálního transakčního PÚ, do něhož by se měl postupně transformovat každý tzv. Intranet úřadu. Vedlo toho se jeden z centrálních portálů VS, IKČR navrhuje, aby to byl buď personální portál ISoSS, případně portál odvozený od Portálu občana, rozšíří tak, aby pro úřední osoby a zaměstnance úřadů, pro něž je nehospodárné spravovat svůj vlastní PÚ, poskytl službu zprostředkování všech centrálních interních portálů na jednom místě.

Vedlo toho se jeden z centrálních portálů VS, IKČR navrhuje, aby to byl personální portál ISoSS, rozšíří tak, aby pro úřední osoby a zaměstnance úřadů, pro něž je nehospodárné spravovat svůj vlastní PÚ, poskytl službu zprostředkování všech centrálních interních portálů na jednom místě.

Všechny funkce portálu úředníka, přesahující hranice „domovského“ OVS budou dostupné výhradně s využitím JIP/KAAS. Proto musí být i lokální IS dostupné se stejnou identitou nebo musí mít úřad pro Portál úředníka a do něj zařazené IS vybudovaný lokální Single-Sign-On řešení, integrované s JIP/KAAS.

CzechPOINT@Office

Jde o neveřejné pracoviště úřadu, kde úředník samostatně čerpá informace, ověřuje a předkládá podání v rámci k eGovernmentu. Je určeno pro úředníky orgánů veřejné moci, kteří ze zákona přistupují k rejstříkům nebo provádějí autorizovanou konverzi dokumentů z moci úřední. (Např. místo toho, aby občan nebo podnikatel dokládal Výpis z rejstříku trestů, úředník si pořídí nutný doklad pomocí Czech POINT@Office).

Jedná se o pracoviště na libovolném úřadě, s technickým vybavením stejným jako v případě veřejnosti přístupných pracovišť Czech POINT, tzn. standardní počítač s přístupem na internet, webový, formulářový a dokumentový prohlížeč, účet pro používání Czech POINT@Office (přístup pomocí dvojice certifikátů pro autentizaci a podpis žádostí).

Systém Czech POINT poskytuje rozhraní CzechPOINT@office, které je určeno pro orgány veřejné moci. Pomocí formulářů, dostupných v rozhraní CzechPOINT@office, mohou úředníci využívat pro výkon své působnosti. Jedná se zejména o:

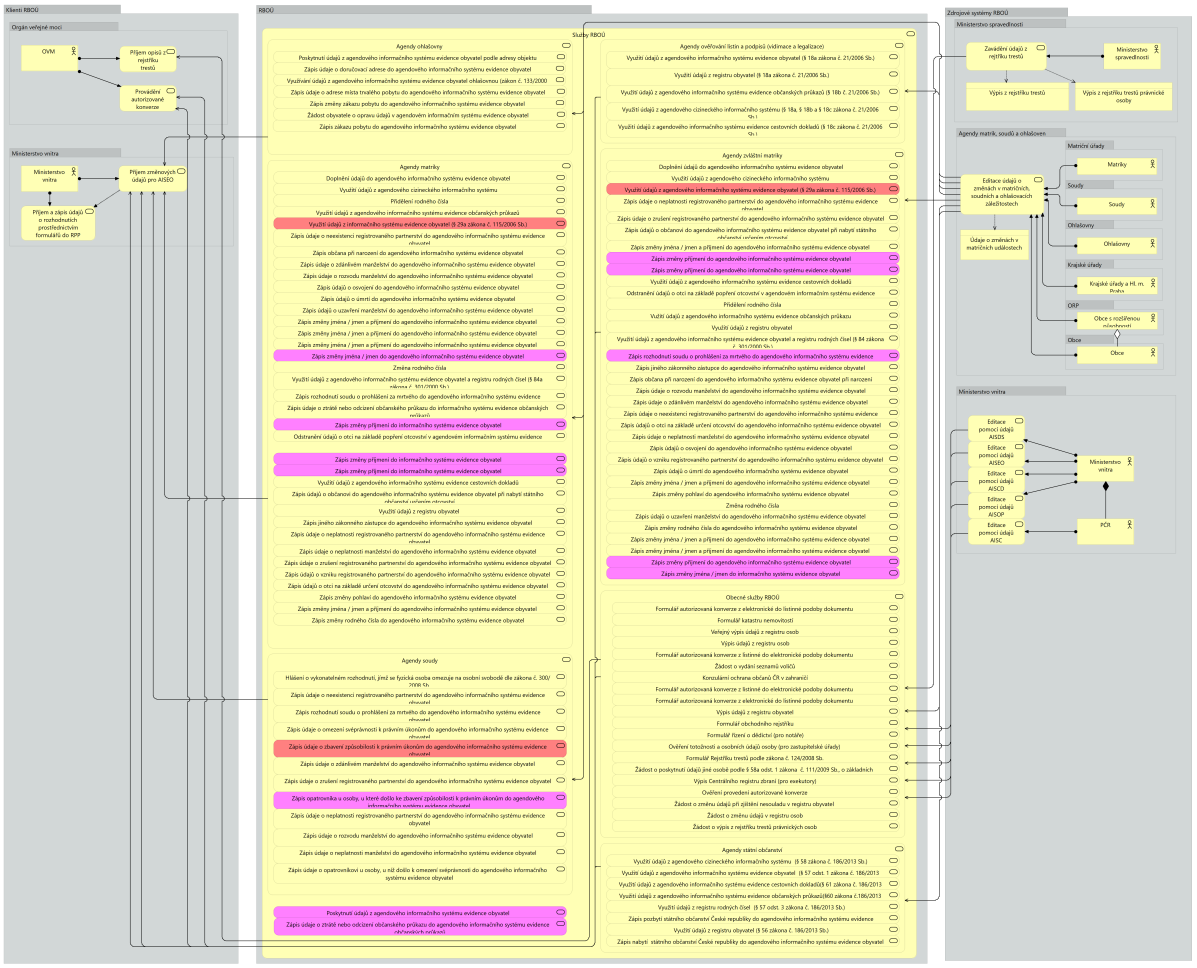
- výpis a opis z Rejstříku trestů
- výpisy ze základních registrů
- autorizovanou konverzi z moci úřední

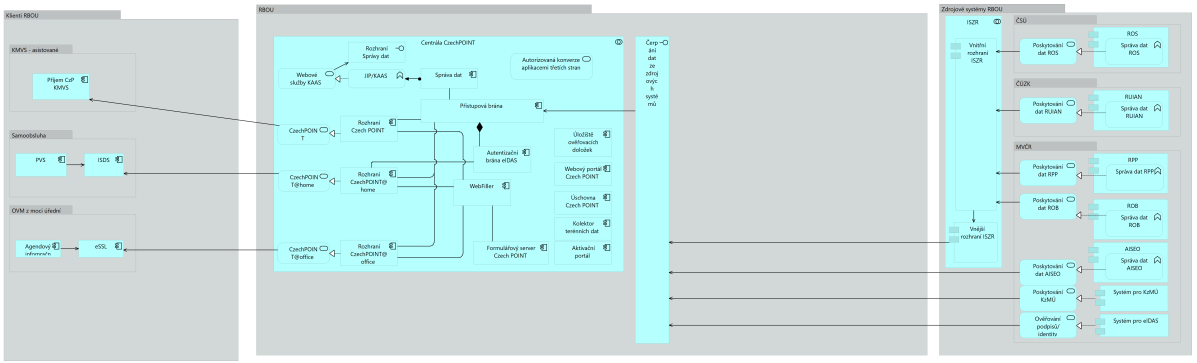
- agendy matrik
- agendy ohlašoven
- agendy soudů

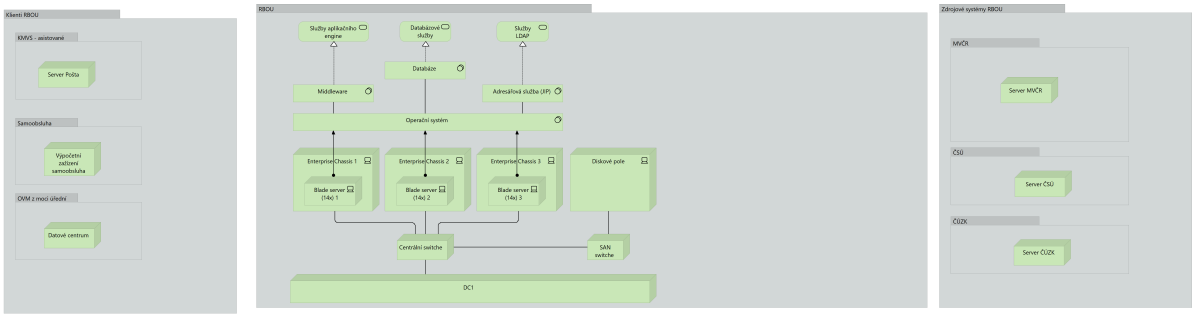
Do oblasti nástrojů pro úředníky patří také podpora provádění autorizované konverze z moci úřední (také jako KzMU). K dispozici jsou dvě API rozhraní systému CzechPOINT pro tuto úlohu.

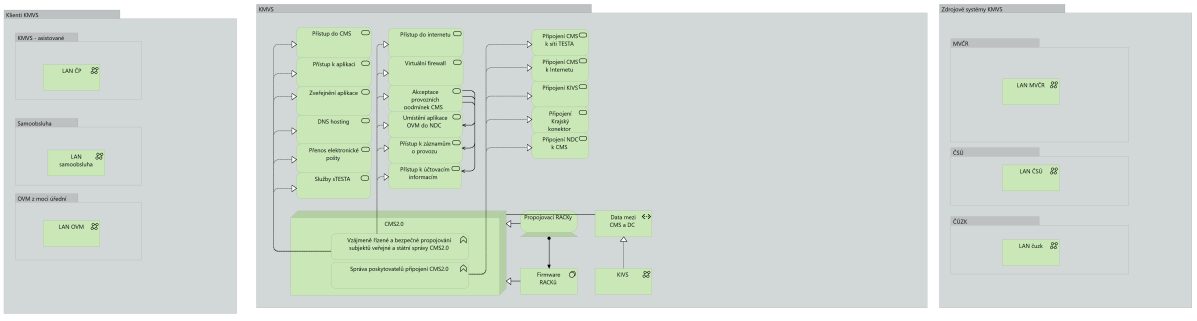
Služby CzechPOINT@Office budou představovat jedny z prvních centrálních sdílených služeb pro Portály úředníka, CzechPOINT@Office bude postupně konvergovat k Portálu úředníka, splyne s ním nebo bude nahrazen a společně vytvoří jedno efektivní interní obslužné rozhraní.

Pohled na jednotné obslužné kanály úředníků









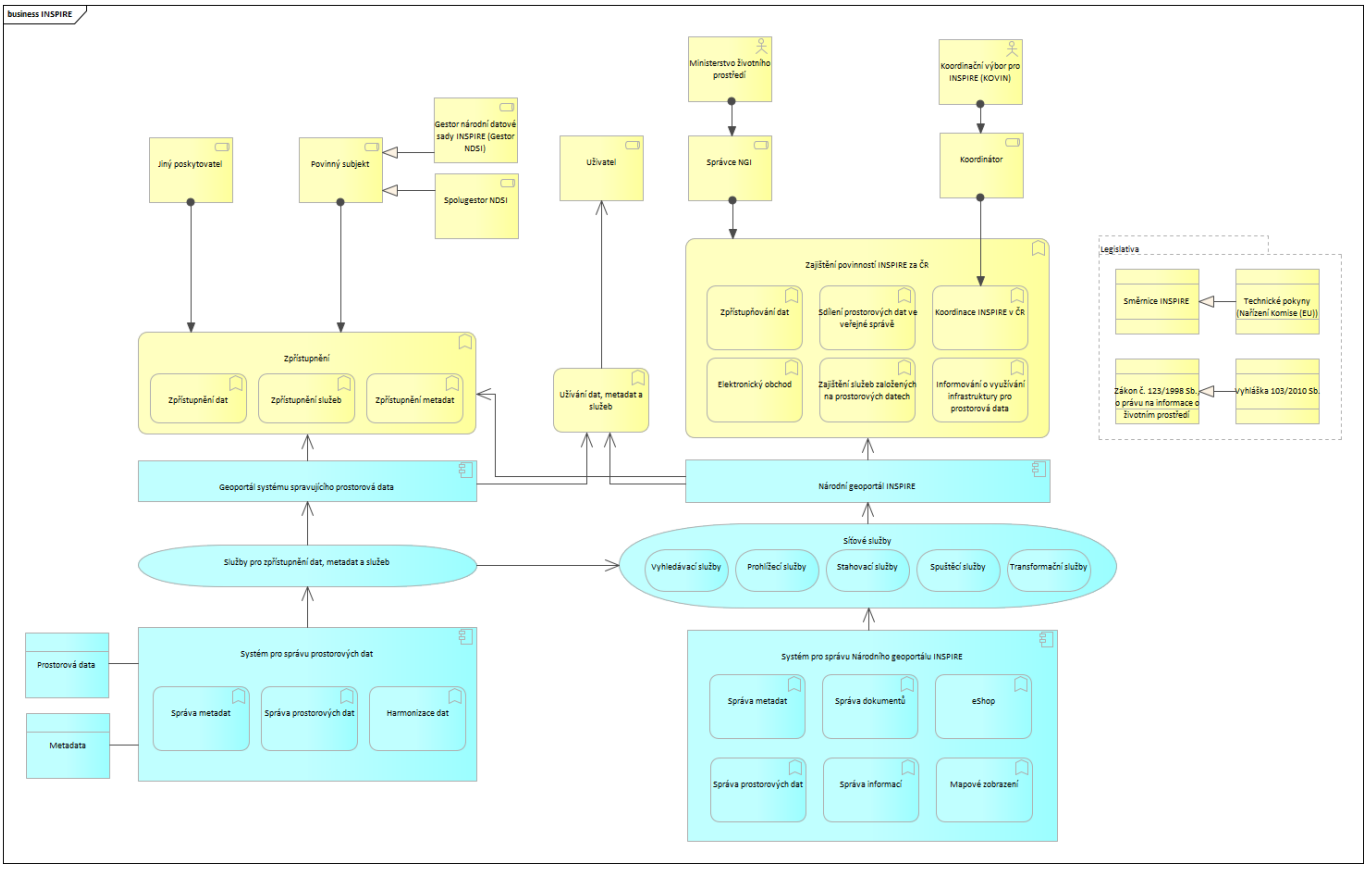
Pravidla Jednotných obslužných kanálů úředníků

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Sdílené služby INSPIRE

Popis Sdílených služeb INSPIRE

Evropská směrnice INSPIRE ukládá členským státům povinnost zajistit zpřístupnění prostorových dat a souvisejících síťových služeb, které náleží k 34 tématům 3 příloh Směrnice INSPIRE. V České republice se tak děje prostřednictvím Národního geoportálu INSPIRE (gesce Ministerstva životního prostředí), jehož součástí je centrální metadatový katalog, který obsahuje metadata prostorových dat, síťových služeb a z nich vytvořených mapových kompozic. Národní geoportál INSPIRE zpřístupňuje prostorová data a služby nad prostorovými daty i pro národní účely, pro potřeby veřejné správy a ostatních subjektů (veřejnost, soukromé firmy) České republiky.



Směrnice INSPIRE zavádí jednotné závazné standardy formou nařízení a doporučujících i technických prováděcích pokynů, které jednotlivá nařízení doplňují. Východiskem pro nařízení a pokyny jsou celosvětově platné ISO normy řady 19 1XX nebo dokumenty známé jako standardy OGC (Open Geospatial Consorcium), INSPIRE však zavádí některé další specifikace. Technické prováděcí pokyny týkající se služeb nad prostorovými daty jsou publikovány na http://inspire.ec.europa.eu/index.cfm/pageid/761. Infrastruktura INSPIRE disponuje obdobným výčtem typů služeb jako infrastruktura národní, v rámci INSPIRE jsou však služby nad prostorovými daty přesně pojmenovány a specifikovány. Jedná se o služby vyhledávácí (služby, které umožňují vyhledání a zpřístupnění metadat), prohlížecí, stahovací (online nebo formou předpřipravených datových sad), transformační služby a služby umožňující spuštění služeb nad prostorovými daty. Tyto služby jsou pak v rámci infrastruktury INSPIRE rozděleny na harmonizované (nad INSPIRE datovými sadami), interoperabilní (zpřístupňující data v geodetickém referenčním systému ETRS89) a vyhledatelné (popsané metadaty). Uvedené služby nemusí zajišťovat každý poskytovatel sám, pro zajištění povinnosti vůči Směrnici INSPIRE lze využít i

nástrojů Národního geoportálu INSPIRE. Vzhledem k rozdílným termínům pro soulad služeb a interoperabilitu prostorových dat zobrazují, s výjimkou ČÚZK, všechny přístupné prohlížecí služby data neharmonizovaná (nekonformní). ČÚZK, jako ústřední správní úřad zeměměřictví a katastru nemovitostí České republiky odpovídající za geodetické systémy závazné na území státu, provozuje i službu transformační umožňující transformaci souřadnic ze systému S-JTSK do ETRS89 s využitím zpřesněných transformačních klíčů.

Zákon 123/1998 Sb. povinuje poskytovatele zpřístupňováním prostorových dat na základě licenčních smluv. Související nařízení Komise (EUS) č. 268/2010 pak určuje termín pro doručení dat a služeb vyžádaných orgány a institucemi EU (20 dní od podání žádosti). Prováděcí pokyny k tomuto nařízení doporučují pro zrychlení komunikace využít pro INSPIRE data a služby dva typy licenčních smluv a to smlouvu základní (pro data bezplatná s účelem užití, ke kterému byl primárně vytvořen i INSPIRE) a specifickou (kde již může být požadována úhrada, účely užití mohou být rozšířeny atd.)

Pravidla pro Sdílené služby INSPIRE

Stručný přehled povinností pro naplnění technických požadavků INSPIRE (detailně viz Strategie implementace INSIRE):

1. vytvořit, zpřístupňovat a aktualizovat metadata dat a služeb INSPIRE (v souladu s nařízením (ES) č. 1205/2008); Metadata musí být zpřístupněna na Národní geoportál INSPIRE buď pomocí služby vytvořené nad katalogem každého poskytovatele nebo uložením metadat do katalogu geoportálu. Metadaty je možné popsat i aplikace využívající prostorová data.
2. zpřístupňovat vyhledávací a prohlížecí síťové služby (v souladu s nařízením (ES) č. 976/2009); Požaduje se vytvořit vyhledávací službu, která umožní vyhledat služby na základě specifikovaných vyhledávacích kritérií, a prohlížecí službu, která umožní datové sady zobrazit.
3. vytvořit a aktualizovat nově vytvořené nebo rozsáhle rekonstruované datové sady; Požaduje se publikovat prostorová data ve formátu GML dle datových specifikací maximálně do 6 měsíců od počátku jejich platnosti v produkčních databázích, sledovat jejich kvalitu a informace o ní zpřístupnit v metadatech.
4. zpřístupňovat stahovací a transformační síťové služby (mít je v souladu s nařízením (ES) č. 976/2009); Požaduje se umožnit stahování INSPIRE datových sad on-line (WFS) nebo tzv. předpřipravených datových sad off-line způsobem. Transformační služby musí umožňovat transformovat datové sady neharmonizovaných dat ve formátu GML do požadovaného geodetického referenčního systému. Je požadováno zajistit kvalitu služby a popsat ji v metadatech;
5. poskytovat přístup k datovým sadám a službám orgánům a subjektům Evropské unie (v souladu s nařízením (EU) č. 268/2010); Požaduje se poskytovat datové sady nebo služby orgánům a subjektům Evropské unie do 20 dnů od doručení žádosti s možností využití standardizované licence.
6. mít interoperabilní a harmonizované služby prostorových dat v souladu s nařízením (EU) č. 1089/2010; mít v souladu s novelizovaným nařízením (ES) č. 976/2009 služby umožňující spuštění služeb založených na prostorových datech; Požaduje zpřístupnit informace o kvalitě služeb a doplnit ke službám další operace zajišťující interoperabilitu (do října 2020).

Při implementaci technických požadavků Směrnice INSPIRE je nutné náročnosti jednotlivých činností poskytovatelů dat dále rozlišit podle role ve vztahu k tvorbě, správě a rozvoji infrastruktury INSPIRE. Zapojení všech dotčených subjektů do infrastruktury INSPIRE předpokládá jejich rozdělení do různých rolí ve vztahu k prostorovým datům, službám založených na prostorových datech, anebo aplikacím, které jsou nad daty nebo službami vytvořeny. Je samozřejmostí, že jeden poskytovatel může vystupovat ve více rolích:

- Povinný subjekt (definován v § 2 písm. b) zákona č. 123/1998 Sb.)
- Jiný poskytovatel (definován v § 11a odst. 3 zákona č. 123/1998 Sb.)
- Gestor národní datové sady INSPIRE – povinný subjekt odpovědný za konsolidaci a publikaci výsledné národní datové sady INSPIRE, pokud je jediným poskytovatelem pro dané téma příloh Směrnice INSPIRE. V opačném případě koordinuje spolugestory přispívající svými prostorovými daty do obsahu národní datové sady INSPIRE (přesně a úplně definován ve Strategii implementace INSPIRE)
- Spolugestor národní datové sady INSPIRE - Jeden či více povinných subjektů k danému tématu příloh

Směrnice INSPIRE, který odpovídá za harmonizaci příslušné části NDSI (přesně a úplně definován ve Strategii implementace INSPIRE)

Tabulka uvádí základní přehled oblastí, které jsou pro jednotlivé role závazné:

Součást infrastruktury *(v závorce uvedeno číslo legislativního dokumentu, který povinnost ustanovuje)*	Povinný subjekt	Jiný poskytovatel	Gestor NDSI	Spolugestor NDSI	Zajištěné centrálně
Metadata (1205/2008/ES) *)	■	■	■	■	
Metadata kvality (1089/2010/ES)			■	■	
Datová sada v souladu (1089/2010/ES, 1253/2013/ES)			■	■	
Vyhledávací služby (976/2009/ES)					■
Prohlížecí služby (976/2009/ES)	■	■	■		
Stahovací služby (976/2009/ES)		■	■		
Transformační služby – souřadnice (976/2009/ES)					■
Transformační služby – datové formáty (1089/2010ES) **)			■		
Spouštěcí služby (noveliz. 1089/2010/EU a 976/2009/ES) ***)	■	■	■		
Sdílení (268/2010/ES)	■	■	■		
Monitoring a reporting (vyhláška č.103/2010 Sb.)	■	■	■		■
Koordinace (zákon 123/1998 Sb.)		■	■		■

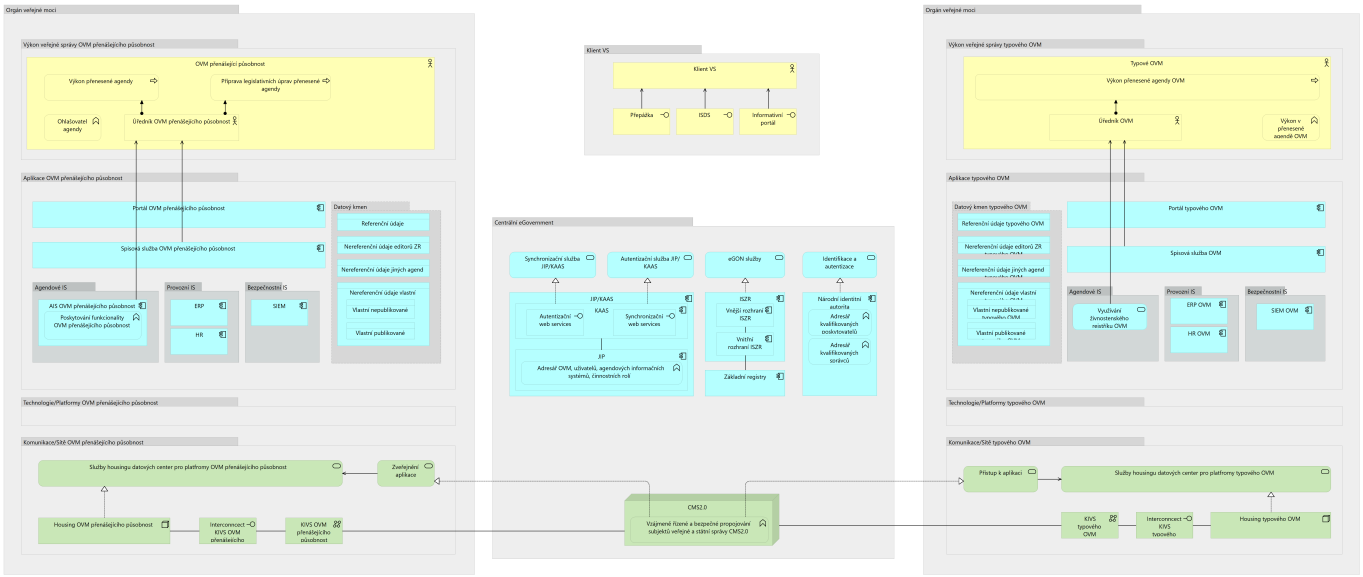
**) zpřístupnění metadat lze zajistit uložením dat na Národní geoportál INSPIRE nebo vytvořením a registrací katalogové služby nad vlastním metadatovým katalogem taktéž na Národním geoportálu INSPIRE. Toto zajišťuje každý poskytovatel dat.*
***) transformace datových formátů není třeba provádět, pokud gestor národní datové sady INSPIRE zvolí cestu zpřístupnění datové sady v souladu s INSPIRE, tedy v souladu s 1089/2010/ES, 1253/2013/ES*
****) soulad s tzv. službami umožňujícími spouštění služeb založených na prostorových datech je povinný, pokud tyto služby poskytovatel provozuje*

Sdílené agendové IS v přenesené působnosti

Popis Sdílených agendových IS v přenesené působnosti

Sdílené agendové informační systémy pro agendy v přenesené působnosti, jako jsou např. Živnostenský rejstřík, Evidence obyvatel, Evidence řidičů a Registr motorových vozidel, budou rozšířeny i na další agendy jejich ohlašovatele tak, že pokud je někdo ohlašovatelem agendy s výkonem v přenesené působnosti, musí zajistit i centrální agendový informační systém (jeho Middle-Office a agendový portál) s možností integrace na lokální systémy úřadů v území.

Pohled na sdílené agendové IS v přenesené působnosti



Pravidla Sdílených agendových IS v přenesené působnosti

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Sdílené agendové IS pro samostatnou působnost územních samospráv

Popis Sdílených agendových IS pro samostatnou působnost

Specifická role samosprávy, kdy každý samosprávný celek je autonomní v oblasti samosprávných činností má rozhodující vliv na jakékoliv sdílení v IT. Rozmanitost velikosti municipalit (od krajů po nejmenší obce) má vliv na velikost jejich útvarů, které se zabývají ICT. Nejmenší municipality, které disponují ICT útvary, jsou obce s rozšířenou působností (ORP). Ve správním obvodě ORP je počet subjektů, kterým jsou poskytovány sdílené služby nebo data dostatečně velký, aby sdílení bylo efektivní, a současně počet umožňuje efektivní řízení. Existence útvaru ICT je rozhodující pro poskytování jakéhokoliv sdílení (služby, data). V současné době již řada ORP ve svém správním obvodě tyto služby poskytuje.

Pravidla Sdílených agendových IS pro samostatnou působnost

OVS, které musí vybudovat IT podporu pro samosprávné agendy a mají pro to k dispozici potřebné zázemí (infrastrukturu, kapacity, znalosti), typicky ORP (zejména statutární města a bývalá okresní města) nebo kraje, mohou poskytnout podporu v malým obcím (1. a 2. typu) ve svém správním území. A to za podmínek daných změnami legislativy, ke kterým bude muset pro plnou realizaci tohoto konceptu dojít. Stejná forma sdílení je možná mezi těmito úrovněmi samosprávy i v případě spisové služby a provozních systémů, pokud malé obce nevyužijí možnosti sdílení centrálních služeb, budou-li k dispozici.

NAP doporučuje municipalitám pro určitou dílčí sadu sdílených služeb použít jako základní prvek správní obvody ORP a vychází z následujících předpokladů:

- ORP jsou nejmenšími subjekty, které zpracovávají architektonický plán.
- Správní obvod ORP je jednoznačně dán a všechny subjekty, kterých se bude sdílení ve správním obvodě týkat, jsou známy.
- Poskytování služeb a dat je určeno standardy (např. u spisové služby).
- Tento model již v řadě ORP funguje.

Pro jiné sdílené služby (například dlouhodobé ukládání dokumentů v elektronických digitálních spisovnách) se mohou využít technologická centra krajů, neboť:

- Mají vybudovanou infrastrukturu
- Disponují IT kapacitami a kompetencemi

Pro další sdílené služby, například pro aplikační služby ekonomických systémů nebo spisových služeb, bude možné v dohledné době 3 let (2022) využít SaaS služby eGovernment Cloudu, protože:

- Procesy a o IT potřeby v těchto oblastech fungování samospráv jsou vysoce standardizované a opakovatelné, proto jsou velmi vhodné pro řešení v cloudu
- Tyto funkce a jejich podpora zůstávají v plné zodpovědnosti obcí, a proto tyto potřebují multi-tenantní řešení

Sdílené aplikační služby kraje

Doporučujeme, aby kraje pro obce zřídily a poskytovaly služby například informačního systému spisové služby.

Krajské sítě

Publikace služeb krajských center do krajské sítě a dále přes krajský konektor do CMS.

Sdílené aplikační, technologické a síťové služby ORP

Malé obce, typicky všechny obce prvního a druhého typu, provozující méně než 10 přístupových zařízení, jsou zproštěny povinnosti zajišťovat informatizaci svých služeb veřejné správy a svůj podíl na eGovernmentu vlastními silami.

Sdílené provozní informační systémy

Popis Sdílených provozních informačních systémů

Další provozní systémy (existující i plánované) budou zahrnuty po zpracování podkladů od věcných správců.

Centrální finanční plánovací a rozpočetnické IS (ERP)

Integrovaný informační systém Státní pokladny (také jako "IISSP") je účinný, transparentní, efektivní a centralizovaný nástroj pro řízení veřejných financí, centralizaci účetních informací státu, konsolidaci vybraných ekonomických ukazatelů za veřejnou správu a komplexní přesné a včasné výkaznictví za celý veřejný sektor v souladu s mezinárodními standardy.

Implementovaný informační systém integruje základní funkční bloky Státní pokladny zaměřené na řízení specifických procesů řízení a kontroly veřejných financí, kterými jsou:

- Rozpočtový informační systém (RISPR a RISRE)
- Centrální účetní systém (CSÚIS)
- Řízení státního dluhu (ŘSD)
- Platební styk (PS)

- Prezentační vrstva - Monitor Státní pokladny (Státní monitor, Krajský monitor a Obecní monitor)

Státní pokladna má před sebou několik možných směrů rozvoje, například integraci na nákupní řešení, na Registr smluv nebo podporu controllingu (nákladové, manažerské účetnictví) veřejné správy.

Monitor Státní pokladny je specializovaný informační portál Ministerstva financí, který umožňuje veřejnosti volný přístup k rozpočtovým a účetním informacím ze všech úrovní státní správy a samosprávy. Prezentované informace pocházejí ze systému Státní pokladny a Centrálního systému účetních informací státu a jsou čtvrtletně aktualizovány. Monitor zahrnuje grafickou webovou část, analytickou část a strojově čitelná zdrojová data.

Centrální registr administrativních budov (CRAB) má vyřešit dosavadní absenci aktuálního celostátního přehledu o administrativních objektech v majetku státu, o jejich obsazenosti a dislokaci státních zaměstnanců. Registr na základě získaných informací umožní maximální využití státních objektů. Ve své činnosti se opírá o Usnesení vlády České republiky ze dne 20. prosince 2012 č. 954 o Centrálním registru administrativních budov.

Informační systém CEDR jako celek je nástrojem zejména pro poskytování, evidenci a kontrolu dotací a pro výkon řady s tím souvisejících agend. Systém se skládá z řady vzájemně provázaných subsystémů, které jsou provozovány na MF- GFŘ, resortech, agenturách a územních orgánech finanční správy.

V informačním systému CEDR jsou shromažďovány údaje o všech dotacích a návratných finančních výpomocích ze státního rozpočtu, státních fondů, státních finančních aktiv a Národního fondu a jejich příjemcích na základě Usnesení vlády č. 584/1997Sb. (subsystém CEDRIII).

- **CEDR - resorty**: Údaje jsou do IS CEDR zaznamenávány buď pomocí subsystému CEDR - **resorty,** který mohou využívat všichni poskytovatelé dotací, nebo prostřednictvím jiných informačních systémů, ve kterých jsou všechny požadované údaje také shromažďovány (např. EDS/SMVS, MSC2007). Předávání údajů do IS CEDR ukládá zákon č. 218/2000 Sb., o rozpočtových pravidlech, §75. Lhůty pro předávání dat a povinné položky stanoví vyhláška č. 296/2005 Sb., o centrální evidenci dotací.
- **CEDR II - Kontrolní útvary FÚ** - Všechny údaje, shromážděné v **IS CEDR III,** jsou předávány do subsystému **CEDR II,** který využívají kontrolní útvary finančních úřadů. CEDR II proto obsahuje i moduly pro podporu evidence kontrol a vymáhání nedoplatků nebo částek, které mají být vráceny v případě zjištění porušení rozpočtové kázně. Informace o výsledcích provedených kontrol jsou na vyžádání zpřístupněny příslušným poskytovatelům dotací.
- **CEDR III - Veřejnost: Veřejné údaje z databáze CEDR** jsou zpřístupněny prostřednictvím subsystému CEDR – web na Internetu MF, který umožňuje i tvorby sestav a výběrů.

ISPROFIN-EDS/SMVS - Informační Systém PROgramového FINancování (ISPROFIN) je manažerský systém pro řízení a kontrolu čerpání položek státního rozpočtu. Dělí se na:

- EDS - Evidenční Dotační Systém eviduje a řídí poskytování návratných finančních výpomocí a dotací ze státního rozpočtu na pořízení nebo technické zhodnocení dlouhodobého hmotného a nehmotného majetku
- SMVS - Správa Majetku ve Vlastnictví Státu řídí poskytování prostředků ze státního rozpočtu na pořízení nebo technické zhodnocení hmotného a nehmotného dlouhodobého majetku státu.

MS2014+ - Informační systém MS2014+, oficiální monitorovací systém evropských strukturálních a investičních fondů (ESIF) pro programové období 2014 -2020. Je určen k procesnímu i datovému zabezpečení kompletního řízení a administrativních procesů nad projekty dotačních programů ze strukturálních fondů EU v České republice v programovém období 2014 - 2020.

Funkcionalita systému Monit2014+ pokrývá veškeré základní procesy životního cyklu dotačních programů i v rámci nich realizovaných konkrétních projektů.

Monit2014+ je napojen řadou rozhraní na desítky informačních systémů státní správy České republiky i Evropské unie podílejících se na implementaci dotačních programů EU.

Centrální systém nákupu a veřejných zakázek

Národní elektronický nástroj (NEN), jako klíčový prvek soustavy Národní infrastruktury pro elektronické zadávání veřejných zakázek (NIPEZ), je komplexní elektronický nástroj pro administraci a zadávání veřejných zakázek a koncesí pro všechny kategorie veřejných zakázek a všechny kategorie zadavatelů, vč. sektorových. NEN podporuje všechny rozsahy elektronizace od evidence zadávacích řízení po plně elektronické postupy.

NEN umožní provázání (elektronickou procesní integraci) na interní systémy zadavatelů i dodavatelů či systémy eGovernmentu v ČR. Plně podpoří plánovací aktivity, neboť často bude využíván pro veřejné zakázky realizované v rámci dlouhodobých investičních projektů.

Pro operace relevantní pro Státní rozpočet musí být NEN integrován jak na lokální rozpočetnictví úřadů, tak zejména na RIS-PR a RIS-RE z IISSP.

Uživatelské rozhraní NEN musí být zařazeno do centrálního Portálu úředníka (PÚ), dostupného pro ty OVS, pro něž by bylo nehospodárné budovat svůj lokání PÚ. Dále musí být uzpůsobeno tak, aby jej ostatní OVS jako jednu z mnoha centrálních služeb mohly řady zařadit do svých lokálních Portálů úředníka (Intranet).

Uživatelé NEN se k němu musí přihlašovat pomocí JIP. To znamená klienti VS (dodavatelé) pomocí NIA a úředníci pomocí JIP/KAAS.

Pravidla Sdílených provozních informačních systémů

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Sdílené statistické, analytické a výkaznické systémy

Popis Sdílených statistických, analytických a výkaznických systémů

Statistické, analytické a výkaznické systémy systémy (existující i plánované) budou zahrnuty po zpracování podkladů od věcných správců.

Pravidla Sdílených statistických, analytických a výkaznických systémů

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

eGovernment Cloud

Popis eGovernment cloudu

Základním cílem projektu eGovernment Cloud (dále také jako "eGC"), je zvýšení efektivity, rozsahu poskytovaných služeb, kvality a bezpečnosti a zároveň snížení nákladů provozu informačních systémů a aplikací veřejné správy, a to využíváním sdílených ICT služeb na úrovni infrastruktury, výpočetních platforem a standardizovatelných aplikací. Tím dochází k naplnění strategie 3E při současném zvýšení kvality a bezpečnosti při pořizování a provozu informačních systémů veřejné správy využíváním sdílených cloudových služeb eGC. Dalším cílem projektu eGC je v maximální míře usnadnit jednotlivým správcům ISVS architektonické, bezpečnostní, nákupní a projektové procesy využíváním služeb eGC.

Informační koncepce ČR zohledňuje základní cíle a koncepty eGC, stanovené usnesením Vlády ČR ve Strategickém rámci Národního cloud computingu (UV 1050/2016) a rozpracovávané v rámci projektu Příprava vybudování eGovernment cloudu, jehož výstupy byly schváleny v listopadu 2018 vládou ČR (UV 749/2018).

Služby eGC zahrnují tři hlavní kategorie cloudových služeb: IaaS (Infrastructure as a Service – služby na úrovni datových center, sítí a HW), PaaS (Platform as a Service – služby na úrovni standardních SW platforem, jako jsou databáze, webové servery) a SaaS (Software as a Service – kompletní funkcionalita standardních nebo standardizovatelných aplikací poskytovaná jako služba, např. e-mail, ekonomický systém, spisová služba apod.).

Služby eGC jsou poskytovány komerční částí eGC (KeGC - služby provozované komerčními subjekty s využitím jejich vlastních datových center a komunikační infrastruktury) a státní částí (SeGC – služby provozované v datových centrech a na HW a SW platformách v majetku státu a provozované organizacemi řízenými státem – poskytovatelem státního cloud computingu).

Součástí vybudování eGC je i konsolidace datových center a HW platforem, čímž se rozumí postupný přesun provozu většiny informačních systémů a aplikací veřejné správy z datových center jednotlivých institucí do vybraných datových center státu (státní část eGC), resp. do datových center ověřených komerčních subjektů (komerční část eGC). Konsolidovaná infrastruktura a HW/SW platformy budou poskytovány formou IaaS a PaaS služeb eGC. Vybudování těchto služeb zahrnuje mj.:

- definici minimálních standardů pro poskytování IaaS a PaaS služeb pro státní a komerční část eGC,
- sjednocení provozního prostředí informačních systémů a aplikací provozovaných ve státní části eGC na několik vybraných platforem,
- zajištění potřebné bezpečnosti, spolehlivosti, škálovatelnosti a jednotnosti provozu ICT služeb.

Součástí vybudování eGC je dále postupná definice standardů pro vybrané softwarové aplikace podporující stejnou agendu či podpůrný a administrativní proces. Standardizované aplikační služby budou poskytovány formou SaaS služeb eGC. Využití standardizovaných aplikací přispěje ke standardizaci pracovních postupů (byznys procesů) ve veřejné správě.

Vybudování eGC umožní organizacím veřejné správy, aby se více soustředily na svoje klíčové procesy místo podpůrných procesů typu zajištění provozu informačních systémů a aplikací. Organizace však musí i nadále být schopny definovat svoje požadavky na ICT služby a integrovat je do svých klíčových procesů.

Jedním ze základních pravidel pro využití služeb SeGC nebo KeGC je zajištění požadované úrovně bezpečnosti eGC služeb v závislost na bezpečnostní úrovni informačního systému veřejné správy, pro který jsou služby eGC využívány. Tato bezpečnostní úroveň se odvozuje od bezpečnostních dopadů daného IS. Zařazení poptávaného cloud computingu do bezpečnostní úrovně provádí orgán veřejné moci podle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci. SeGC zajistí nejvyšší kritickou úroveň bezpečnosti a je určen pro provoz služeb eGC nejvyšší bezpečnostní úrovně (automaticky to jsou informační nebo komunikační systémy, které jsou kritickou informační infrastrukturou podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti). KeGC je určen pro provoz služeb eGC ostatních bezpečnostních úrovní a v maximální míře umožňuje využití tržních mechanismů pro zajištění optimálních cen.

Druhým rozhodujícím kritériem pro využití služeb eGC je kalkulace a porovnání nákladů vlastnictví (TCO) jednotlivých IS v modelu provozu on-premise (na vlastní infrastruktuře) a s využitím služeb eGC. Ke stanovení ekonomické náročnosti je dostupný Kalkulátor nákladů ISVS provozovaného v cloud; včetně uživatelské příručky.

Každý úřad si také musí být vědom toho, že financování cloudových služeb se liší od provozu vlastního řešení. Při provozu a nákupu vlastních technologií jde o tzv. CAPEX, tedy kapitálové výdaje, a pořízené věci zůstávají v majetku úřadu. Naopak nákup cloudových služeb je tzv. OPEX, tedy provozní výdaje, kdy úřadu v majetku nic nezůstává a platí si pouze službu. S tímto odlišným způsobem financování je třeba počítat při tvorbě rozpočtu a jeho čerpání, protože při využívání cloudových služeb pro celou infrastrukturu úřadu se razantně zvýší provozní výdaje a sníží investiční.

Oblast cloud computingu je od 1. 8. 2020 regulována příslušnými ustanoveními zákona č. 365/2000 Sb., o

informačních systémech veřejné správy, kde v Hlavě VI zákona je zaveden mechanismus zápisu poptávek a nabídek cloud computingu do katalogu cloud computingu a zavedena povinnost orgánů veřejné správy využívat pouze takový cloud computing, který byl na základě splnění podmínek uvedených v zákoně zapsán Digitální a informační agenturou do katalogu cloud computingu.

Na webových stránkách Digitální a informační agentury je dostupný Metodický návod pro zápis poptávky a nabídky cloud computingu do katalogu cloud computingu.

Poskytovatelé služeb eGC musí splňovat zákonem určené podmínky, které zahrnují zejména oblast bezpečnosti poskytovaných služeb a jejich provozních parametrů, ale také důvěryhodnosti poskytovatele. Splnění podmínek ověřuje Digitální a informační agentura ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost a dalšími složkami státu. Požadavky, které musí splnit poskytovatel cloud computingu, aby byla jeho nabídka zapsána do katalogu cloud computingu, stanovuje vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

Rozsah údajů vedených v katalogu cloud computingu o poptávkách, nabídkách a využívaném cloud computingu specifikuje vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.

Řídící orgán eGovernment Cloudu (také jako ŘOeGC) koordinuje budování a rozvoj eGC, rozvíjí a udržuje metodické postupy pro eGC, kontroluje a řídí soutěžní mechanismus KeGC a nabídku služeb SeGC.

V současné době je umísťování IS orgánů veřejné správy do eGC (využívání služeb eGC) zcela dobrovolné, přičemž se uplatňuje princip mandatory-compare. Podle § 5 odst. 2 písm. j) a k) zákona č. 365/2000 Sb., o informačních systémech veřejné správy, resp. vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy mají orgány veřejné správy povinnost zajistit si ekonomické zhodnocení výhodnosti provozu ISVS. Orgán veřejné správy musí provést kalkulaci TCO, takže umístění on-premise pro nově pořizované systémy nebo v rámci technického zhodnocení anebo rozvoje spravovaného informačního systému veřejné správy bude nadále možné pouze tehdy, pokud kalkulace TCO neprokáže, že je nákladově efektivnější než umístění do eGC.

Bezpečnostní pravidla pro orgány veřejné správy, která musí nastavit, pokud využívá cloud computingu jsou dána vyhláškou č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.

Katalog cloud computingu

Katalog cloud computingu dle zákona o informačních systémech veřejné správy naleznete na webu Digitální a informační agentury.

Nástroj pro vyhledávání v katalogu cloud computingu není momentálně k dispozici z důvodu probíhajících prací na jeho aktualizaci. Děkujeme za pochopení.

{{url>https://app.powerbi.com/view?r=eyJrIjoiOTNiOGM3NzUtMzRhOC00NjUzLWI4MGYtZmZjMTY4MzQ2NjM0IiwidCI6IjFkYjQxZDZmLTFmMzctNDZkYi1iZDNlLWM0ODNhYmI4MTA1ZCIsImMiOjh9 100%,1000}}

Pravidla eGovernment cloudu

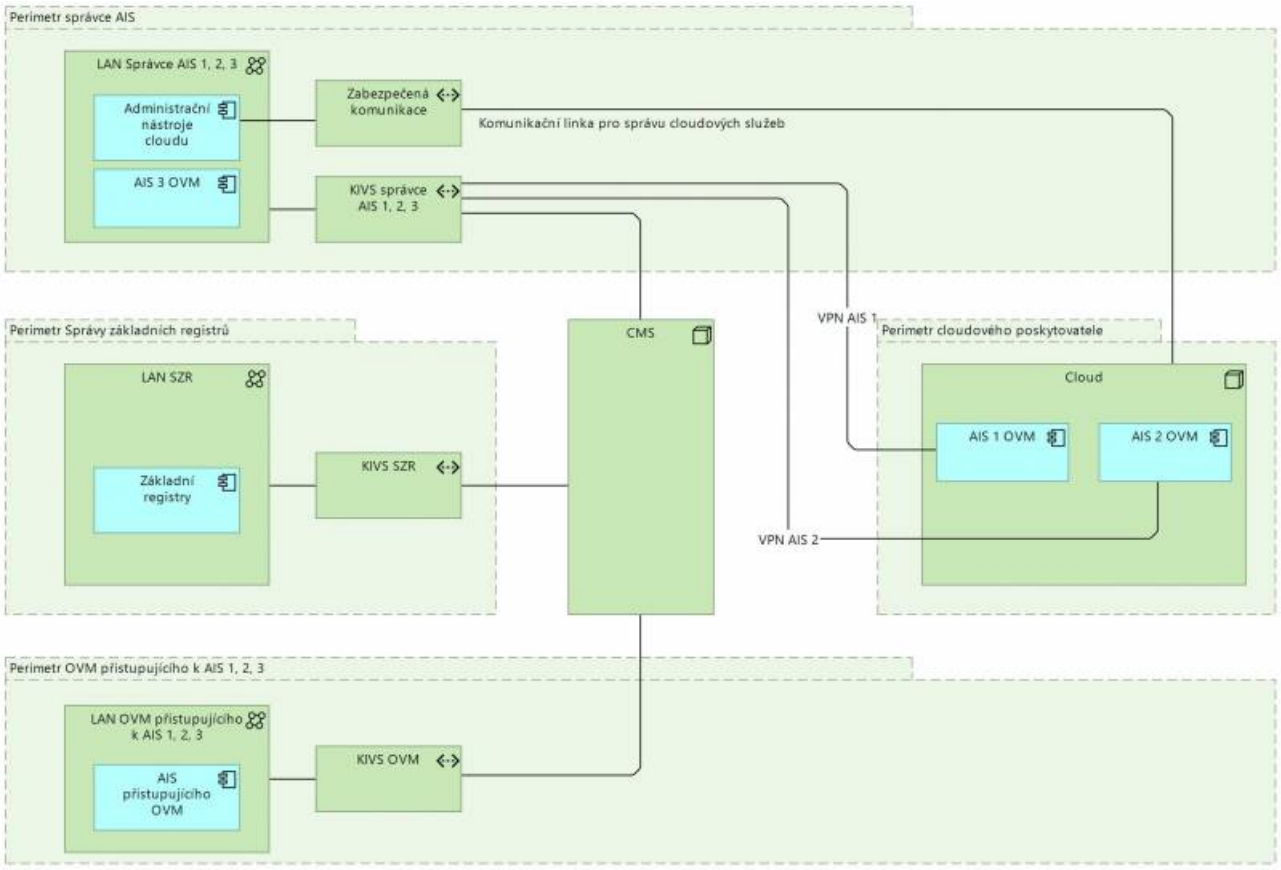
Přístup správců ISVS k eGC

Každý správce centralizovaného poskytovaného agendového informačního systému by měl postupně činit při správě a rozvoji svých informačních systémů takové kroky, aby oddělil vrstvu platformy a technologií od vrstvy komunikační a aplikační vrstvy příslušných informačních systémů. To znamená, že by se svými postupnými kroky měl připravit na to, že od určité doby bude provozovat svoje centralizované agendové informační systémy v cloudu a měl by postupně omezovat svoji závislost na vlastních datových centrech a pouze jím provozovaných technologických platformách.

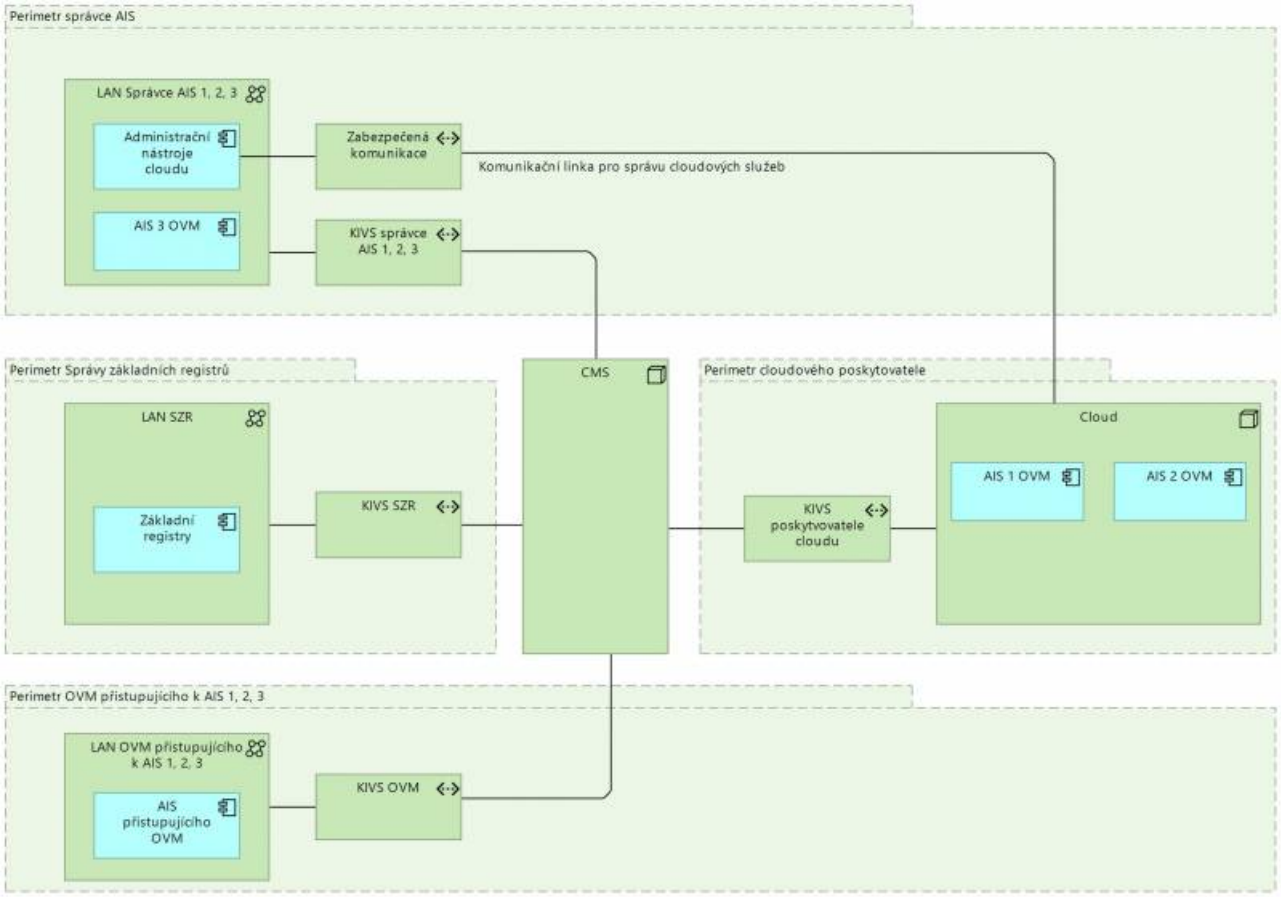
Provozování AIS OVM v eGC v souvislosti s komunikací pomocí CMS/KIVS

Umístění AIS OVM v eGC znamená, že eGC je jen jiná adresa daného OVM. Zde jsou dvě možnosti přístupu do CMS:

1. Připojené do CMS/KIVS je OVM a AIS v eGC je přesměrován do CMS/KIVS přes OVM (př. Portál občana). Pro tento scénář je AIS v eGC brán jako interní AIS OVM, který se připojuje do CMS/KIVS přes připojení daného OVM



2. Poskytovatel eGC má zřízenou KIVS linku do CMS. Skrze tuto KIVS linku si jednotlivá OVM mající ASIy v cloudu vytváří svá VPN do CMS. (př. (AISy Městských policií si sahají na Základní registry)



Publikování portálu OVM

Publikování portálu OVM je specifický případ publikování AIS OVM, kdy se v rámci provozu portálu v eGC umožňuje, aby byly služby portálu dostupné pro klienty, kteří nejsou OVM, prostřednictvím internetu přímo od poskytovatele eGC.

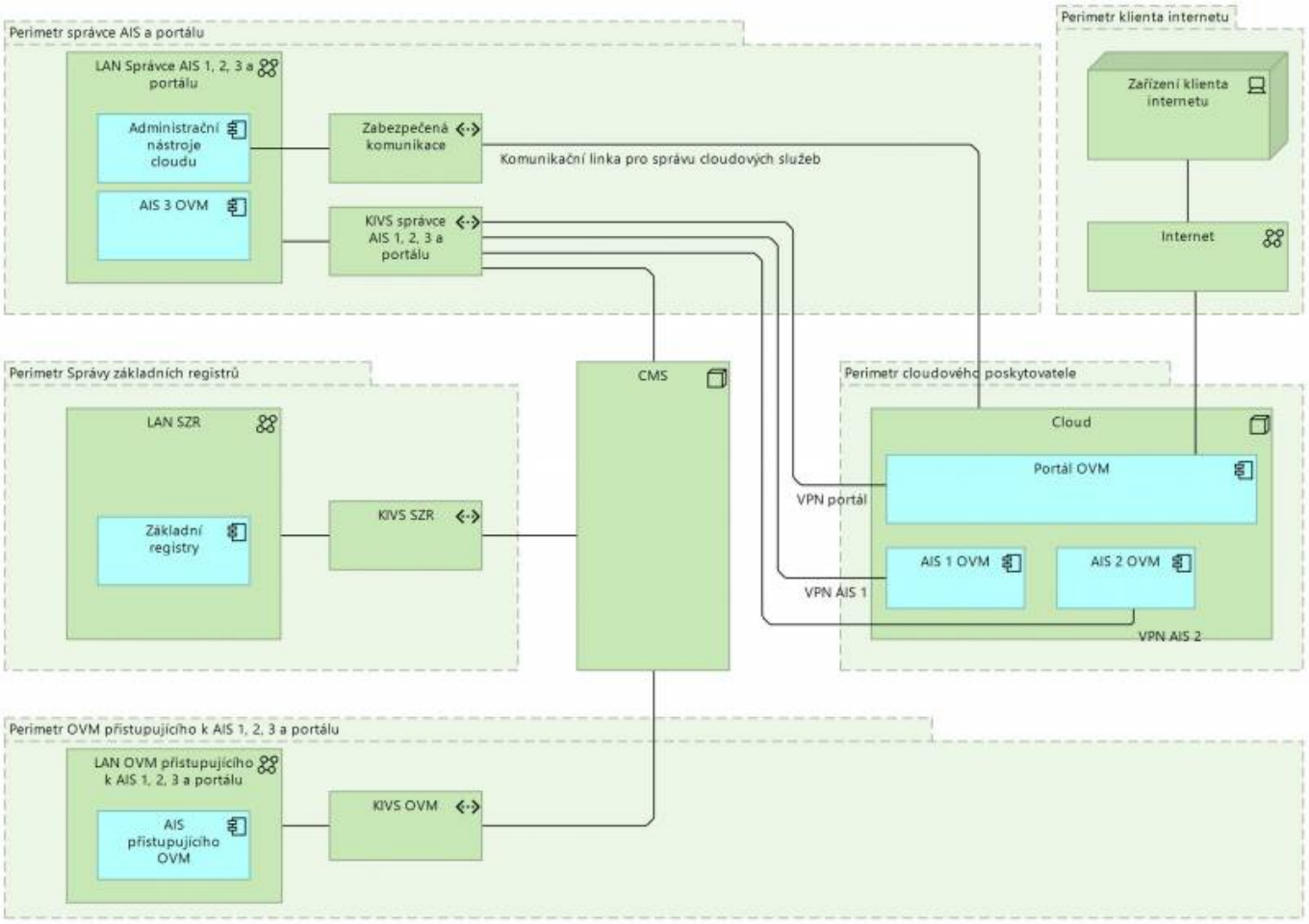
Portál je v případě provozu na vlastní infrastruktuře publikován výhradně prostřednictvím CMS službou CMS2-02 Zveřejnění aplikace a to do:

1. Do sítě CMS/KIVS, služba CMS2-02-1 a/nebo
2. Do sítě Internet, služba CMS2-02-2

V případě umístění portálu v eGC, je umožněna publikace portálu z eGC, kdy:

1. eGC je rozšířeným IP prostorem CMS/KIVS a
2. CMS/KIVS a eGC jsou propojeny standardním způsobem dle podmínek připojení se k CMS/KIVS.
3. AIS OVM všech subjektů, kteří přispívají do portálu OVM v eGC, čerpají údaje o subjektu práva prostřednictvím referenčního rozhraní.

Klienti, kteří nejsou OVM, přistupují k portálu v otevřeném internetu přes HTTPS publikovaném přímo z eGC.



Povinnosti komerčních poskytovatelů služeb eGC

Konkrétní povinnosti stanoví zákon o informačních systémech veřejné správy a na základě tohoto zákona pak vydané vyhlášky ministerstva a NÚKIB. Řídící orgán eGovernment Cloudu pak na základě zákona a vyhlášek připravuje a vydává metodické pokyny. Již nyní však platí pravidla pro nutnost připojení skrze infrastrukturu CMS/KIVS a tím i respektování katalogového listu služby připojení přes IPSec

Národní datová centra

Popis Národních datových center

Cílově jsou i NDC nadále nedílnou součástí IKČR, budou se rozvíjet vedle eGC a často dokonce ve stejných prostorách a se stejnými kvalitativními parametry, například bezpečnosti. Jejich role je pro řadu centrálních systémů eGovernmentu nezastupitelná.

Lze předpokládat, že bude společně s požadavky na parametry eGC definován povinný minimální standard pro NDC a že ještě několik resortních DC bude „povýšeno“ na NDC. Současně lze předpokládat, že části některých NDC se zapojí jako významné součásti státní části eGC a budou své služby nabízet vedle přímé dodávky „kmenovým klientům“ - organizacím svého zřizovatele, také volně, komukoli za podmínek eGovernment Cloudu. Národní Datové Centrum jako sdílená služba IT poskytuje:

- Služby bezpečného prostředí výpočetního centra
- Služby virtuální výpočetní kapacity
- Služby databázových serverů
- Služby datového zálohování

- Služby vystavení publikovaných služeb v DMZ1 a DMZ2 v CMS KIVS

Pravidla Národních datových center

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Komunikační infrastruktura veřejné správy

Popis Komunikační infrastruktury veřejné správy

KIVS/CMS je centrální funkční celek, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů státní správy a samosprávy ke službám (aplikacím), které poskytují informační systémy jiných subjektů státní správy a samosprávy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu. Skládá ze ze 2 hlavních složek, jednak **Centrálního místa služeb (CMS)** a následně sítí, které jsou s ním propojeny (KIVS). Pro účely tohoto popisu se bere CMS/KIVS jako jeden celek, tedy samostatná a oddělená infrastruktura sloužící pro síťové a bezpečné propojení eGovernmentu.

KIVS jako samostatný pojem je také používán jako specifická možnost připojení do CMS. Při používání CMS/KIVS se myslí celek, který obsahuje obecně jakýkoliv způsob připojení, viz dále.

KIVS/CMS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (OVS) pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do Internetu.

OVS přistupuje ke službám CMS pomocí portálu CMS na adrese https://www.cms2.cz/. Adresa portálu je dostupná pouze z vnitřní sítě KIVS/CMS, tedy až poté, kdy je OVS připojeno jednou z možných variant níže. Pokud se na adresu přistupuje mimo vnitřní síť KIVS/CMS, dostane se uživatel pouze na stránku MVČR.

OVS a SPUÚ se připojují ke službám CMS výhradně jedním ze čtyř možných způsobů:

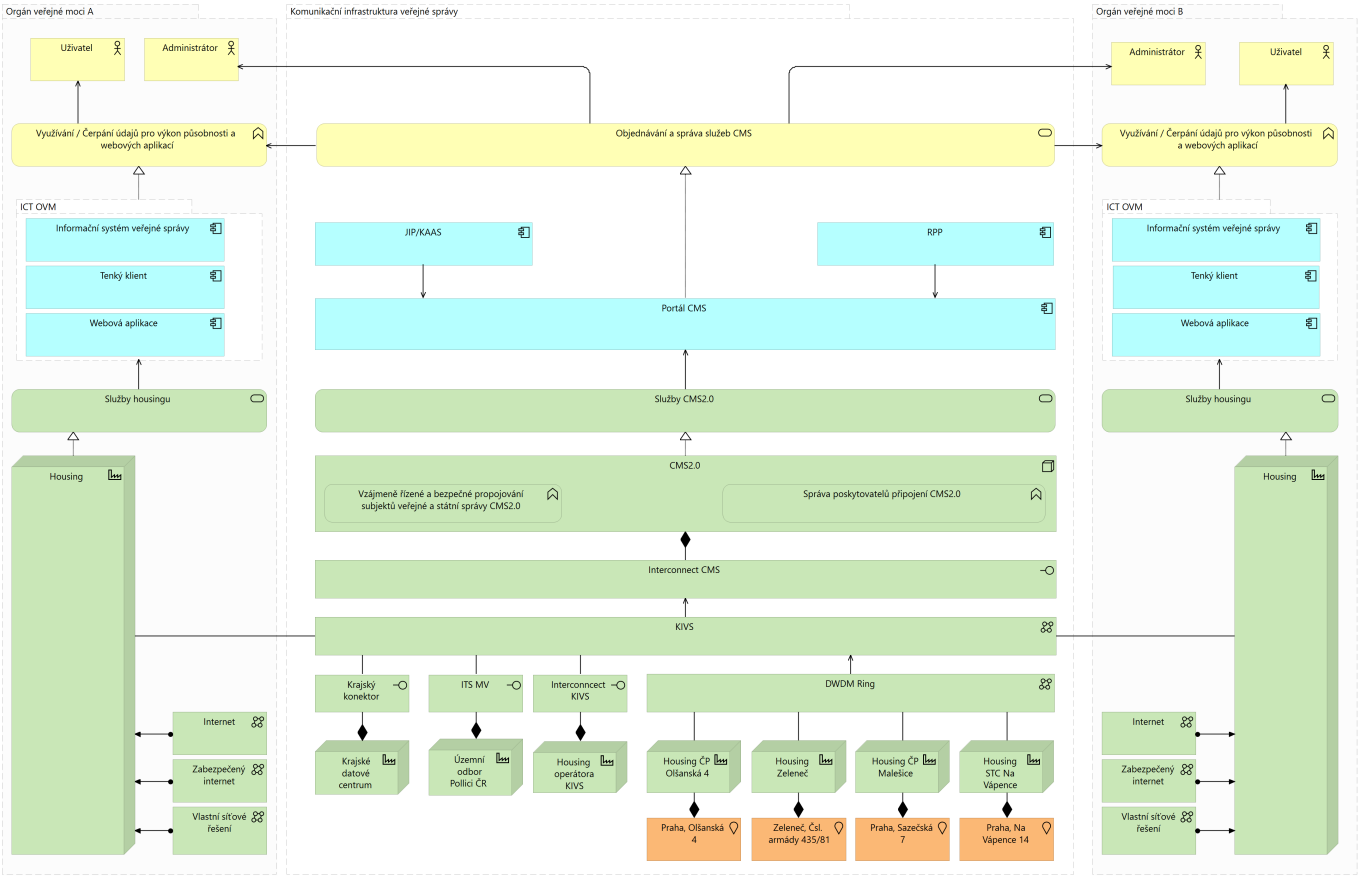
1. Prostřednictvím Krajských sítí (aktuálně v krajích Vysočina, Plzeňském, Karlovarském, Zlínském a částečně Pardubickém + další budou-li vybudovány).
2. Prostřednictvím metropolitních sítí připojených např. na Integrovanou telekomunikační síť (ITS) MVČR.
3. Prostřednictvím Komunikační infrastruktury veřejné správy (KIVS) s využitím komerčních nabídek soutěžených prostřednictvím Ministerstva vnitra.
4. Prostřednictvím veřejného internetu, a to přes zabezpečený tunel VPN SSL nebo VPN IPSec.

OVS čerpají služby eGovernmentu, jako např. propojený datový fond, výhradně přes CMS. Pro čerpání služeb z CMS jsou pro OVS, **s výjimkou obcí I. typu**, přípustné pouze varianty 1 až 3 výše. Komunikace mezi jednotlivými OVS je vedena výhradně prostřednictvím KIVS/CMS, tzn. jednotlivé OVS mají povinnost přistupovat k informačním systémům veřejné správy (ISVS) pouze prostřednictvím KIVS/CMS.

Obce I. typu mají povolený způsob čerpání služeb CMS, a tedy i publikovaných služeb eGovernmentu (jako například CzechPOINT, služby základních registrů, atd.), prostřednictvím veřejného internetu, pokud jsou tyto služby publikovány do veřejného internetu s využitím služeb CMS.

Pokud chce úřad využít KIVS, tj. soutěž přes centrálního zadavatele Ministerstvo vnitra, je nutné definovat požadavky dle katalogových listů a následně zrealizovat nákup v dynamickém nákupním systému. Služby CMS lze čerpat také prostřednictvím Národních datových center.

Pohled na CMS/KIVS



Pravidla Komunikační infrastruktury veřejné správy

Zákon 365/2000 sb. v aktuálním znění, zavedl povinnost publikovat služby ISVS jednotlivým uživatelům prostřednictvím Centrálního místa služeb (také jako CMS). V kombinaci s komunikační infrastrukturou veřejné správy (také jako KIVS) zavádí pro jednotlivé orgány veřejné správy bezpečnou, od internetu oddělenou, komunikační infrastrukturu poskytující pro jednotlivé orgány veřejné správy:

- Bezpečný a spolehlivý přístup k aplikačním službám jednotlivých ISVS
- Bezpečnou a spolehlivou publikaci aplikačních služeb jednotlivých ISVS
- Bezpečný přístup do internetu
- Bezpečný přístup k poštovním službám v internetu
- Zabezpečuje bezpečné síťové prostředí pro zajištění interoperability v rámci EU
- Umožňuje bezpečný přístup k aplikačním službám ISVS určeným pro koncové klienty VS ze sítě internet

Cílem je:

- Publikovat bezpečným způsobem přes CMS/KIVS všechny aplikační služby centralizovaných ISVS se současným zajištěním bezpečného přístupu jednotlivých OVS k těmto službám při výkonu jejich působnosti.
- Umožnit bezpečný přístup k aplikačním službám ISVS určeným pro koncové klienty VS ze sítě internet
- Zabezpečit bezpečné síťové prostředí pro zajištění interoperability v rámci EU

OVS přistupuje ke službám CMS pomocí portálu CMS na adrese https://www.cms2.cz/. Adresa portálu je dostupná pouze z vnitřní sítě KIVS/ CMS, tedy až poté, kdy je OVS připojeno jednou z možných variant níže. Pokud se na adresu přistupuje mimo vnitřní síť KIVS/CMS, dostane se uživatel pouze na stránku MVČR. Centrální místo služeb, jakožto součást komunikační infrastruktury veřejné správy, je systém, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů státní správy ke službám

(aplikacím), které poskytují informační systémy jiných subjektů státní správy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu.

CMS tak můžeme nazvat privátní sítí pro výkon veřejné správy na území státu.

Připojení k CMS

CMS/KIVS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (OVS) pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do Internetu.

OVS a SPUÚ se připojují ke službám CMS výhradně jedním ze čtyř možných způsobů:

1. Prostřednictvím Krajských sítí (aktuálně v krajích Vysočina, Plzeňském, Karlovarském, Zlínském a částečně Pardubickém + další budou-li vybudovány).
2. Prostřednictvím metropolitních sítí připojených např. na Integrovanou telekomunikační síť (ITS) MVČR.
3. Prostřednictvím Komunikační infrastruktury veřejné správy (KIVS) s využitím komerčních nabídek soutěžených prostřednictvím Ministerstva vnitra.
4. Prostřednictvím veřejného internetu, a to přes zabezpečený tunel VPN SSL nebo VPN IPSec.

OVS čerpají služby eGovernmentu, jako např. propojený datový fond, výhradně přes CMS. Pro čerpání služeb z CMS jsou pro OVS, **s výjimkou obcí I. typu**, přípustné pouze varianty 1 až 3 výše. Komunikace mezi jednotlivými OVS je vedena výhradně prostřednictvím KIVS/CMS, tzn. jednotlivé OVS mají povinnost přistupovat k informačním systémům veřejné správy (ISVS) pouze prostřednictvím KIVS/CMS.

Obce I. typu mají povolený způsob čerpání služeb CMS, a tedy i publikovaných služeb eGovernmentu (jako například CzechPOINT, služby základních registrů, atd.), prostřednictvím veřejného internetu, pokud jsou tyto služby publikovány do veřejného internetu s využitím služeb CMS.

Pokud chce úřad využít KIVS, tj. soutěž přes centrálního zadavatele Ministerstvo vnitra, je nutné definovat požadavky dle katalogových listů a následně zrealizovat nákup v dynamickém nákupním systému. Služby CMS lze čerpat také prostřednictvím Národních datových center.

IPsec a jeho úskalí

Ačkoliv jsou pro OVS přípustná jen připojení pomocí KIVS, existují úřady využívající připojení IPsec, který se ovšem nehodí pro kritické služby a funkce úřadování. Nevhodné je toto připojení např. pro systém CDBP (systém sběru žádostí o vydání občanského průkazu nebo cestovního dokladu občana České republiky), kdy mohou nastat následující rizika:

1. Spojení realizovaná prostřednictvím kryptografických prostředků přes veřejný internet nejsou vhodná jako primární způsob čerpání služeb, které mají mít garantovanou funkčnost a dostupnost. Systém CDBP je koncepčně založen na předpokladu provozu na vyhrazené síti, která je zcela oddělena od běžného internetového provozu a tomu odpovídá i úroveň jeho zabezpečení.
2. V rámci spojení realizovaných prostřednictvím veřejného internetu není možné dostatečným způsobem garantovat následující:
    - požadavek na dostupnost, protože internet není zaručeně garantované přenosové prostředí s definovanými SLA,
    - požadavek na propustnost, protože systém CDBP využívá na ORP "těžkého" klienta se vzdálenou správou; nezbytná je tedy komunikace oběma směry (centrum systému CDBP – ORP a ORP – centrum systému CDBP) pro instalací nových verzí aplikace pomocí "balíčků" o velikosti cca 500 MB/PC a pro stahováním logů z PC o velikosti cca 100 MB/PC,
    - požadavek na fungování protokolu WoL, který umožňuje dálkové „probouzení“ jednotlivých

pracovních stanic systému CDBP bez zásahu obsluhy, je nezbytný z důvodů distribuce nových verzí SW, stahování logů či jiných činností souvisejících s provozem Systému CDBP.

3. Na základě výše uvedeného reálně hrozí, v případě využití IPsec, riziko výpadků spojení při pořizování žádostí o občanské průkazy a cestovní pasy, což může vést ke zpomalení nebo úplné nedostupnosti pracovišť systému CDBP. V případě, že by v důsledku užívání IPsec, nebylo možné dálkově nainstalovat na koncová pracoviště systému CDBP aktualizace, bude nezbytné, aby instalaci provedl technik při výjezdu, který by úřad musel uhradit.

CMS, popis zahrnutých služeb

Odbor Hlavního architekta eGovernmentu a Ministerstvo vnitra v rámci svých kompetencí požaduje od jednotlivých správců ISVS, aby služby ISVS publikovaly v rámci Centrálního místa služeb – CMS (služba CMS2 -02, CMS2 -04).

Jednotliví uživatelé ISVS na úrovní státní správy a samosprávy služby těchto systémů konzumují, resp. k ISVS přistupují výhradně prostřednictvím CMS (služba CMS2 -03).

Služba CMS2 – 02 – Zveřejnění aplikace

Název parametru	Vysvětlení
Kód služby	CMS2-02
Název služby	Zveřejnění aplikace
Popis služby	Služba vytvoří prostředí pro publikaci aplikační služby informačního systému OVM. Varianty služby se liší podle cílového prostředí. Možné varianty jsou: 1. do sítě Internet 2. do sítě CMS 3. do sítě TESTA-ng 4. do Extranetu

Aplikační služba může být umístěna v infrastruktuře orgánu nebo v infrastruktuře Národního datového centra (NDC). Aplikační služba může být zveřejněna do více prostředí současně. Aplikační služba je zveřejněna na definovaných protokolech a portech.

Při zveřejnění aplikace do sítě Internet jsou aplikaci přiděleny veřejné IP adresy z prostoru CMS. Přístup ke zveřejněné službě může být omezen na definované zdrojové IP adresy.

Při zveřejnění aplikace do sítě CMS jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Službu je možné zveřejnit pro všechny ostatní subjekty připojené do sítě CMS (Veřejná služba) nebo pro definované subjekty a skupiny subjektů (Schvalovaná služba). O přístup ke Schvalované službě musí přistupující subjekty žádat prostřednictvím služby CMS203-1.

Při zveřejnění aplikace do sítě TESTA-ng (síť EU)[4)] jsou aplikaci přiděleny IP adresy z prostoru pro ČR v síti TESTA-ng. Přístup ke zveřejněné službě je omezen na definované zdrojové IP adresy. Zveřejnění aplikace musí být provozováno v souladu s provozními a bezpečnostními požadavky EU pro síť TESTA-ng.

Při zveřejnění aplikace do Extranetu jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Aplikační služba je zveřejněna do existujícího extranetu (extranet vytváří Správce CMS). Přístup k aplikaci v extranetu je umožněn všem uživatelům, kteří mají do daného extranetu přístup.

Služba CMS2 – 03 – Přístup k aplikaci

Název parametru	Vysvětlení
Kód služby	CMS2-03
Název služby	Přístup k aplikaci
Popis služby	Služba umožňuje zřizovat a rušit přístupy k aplikačním službám. Varianty služby se liší podle cílového prostředí. Možné varianty představují přístup: 1. k aplikaci v síti CMS 2. k aplikaci v síti TESTA-ng 3. k aplikaci v síti Internet

Služba umožňuje zřizovat, měnit a rušit přístupy subjektu k nabízené aplikační službě. Jednou žádostí lze zřídit přístup právě k jedné aplikační službě. Připojení je povoleno z definovaných IP adres v síti subjektu.

Přístup k aplikaci v síti CMS umožní subjektu připojení k aplikační službě zveřejněné jiným subjektem prostřednictvím služby CMS2-02-1 v síti CMS. Zřízení přístupu je podmíněno souhlasem vlastníka zveřejněné aplikační služby, které probíhá prostřednictvím portálu CMS.

Přístup k aplikaci v síti TESTA-ng umožní subjektu připojení k aplikační službě zveřejněné jiným státem Evropské unie v síti TESTA-ng. Připojení je povoleno na definovaných protokolech a portech. Přístup k aplikaci musí být provozován v souladu s provozními a bezpečnostními požadavky EU pro síť TESTA-ng.

Přístup k aplikaci v síti Internet umožní subjektu připojení k aplikační službě zveřejněné v síti Internet na definovaných protokolech a portech. Cílovou aplikační službu v síti Internet je nutné definovat konkrétními IP adresami, protokoly a porty.

Služba CMS2 – 04 – Publikace AIS na eGSB/ISSS

Název parametru	Vysvětlení
Kód služby	CMS2-04
Název služby	Publikace AIS na eGSB/ISSS
Popis služby	Služba zajišťuje zpřístupnění publikačního agendového informačního systému (AIS) v rámci CMS a povolení síťové komunikace s rozhraním eGon Service Bus / Informační systém sdílené služby

Služba zajistí provozovateli publikačního agendového informačního systému (AIS) síťovou konektivitu mezi eGSB/ISSS (eGON Service Bus / Informační systém sdílené služby, tj. sdílená služba obecného rozhraní) a publikačním AIS na definovaných protokolech a portech. V rámci publikace jsou přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy).

Ve výchozím stavu je komunikace mezi eGSB/ISSS a publikačním AIS synchronní, volitelně lze zprovoznit komunikaci asynchronní.

Právní aspekty

S výjimkou tzv. provozních informačních systémů, které jsou uvedeny v § 1 odst. 4 písm. a) až d) zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS), je § 6g odst. 3 tohoto zákona správcům ISVS uložena povinnost poskytovat služby informačních systémů veřejné správy prostřednictvím CMS. Organům veřejné správy je prostřednictvím § 6g odst. 4 ZoISVS uložena povinnost využívat sítě elektronických komunikací CMS.¨

Protože skrze CMS se publikují služby tzv. referenčního rozhraní, definovaného v § 2 písm. j) ZoISVS, má vztah k CMS i povinnost uložená v § 5 odst. písm. d) ZoISVS, tj. povinnost správců ISVS zajistit, aby vazby jimi spravovaného ISVS na ISVS jiného správce byly uskutečňovány prostřednictvím CMS.

S ohledem na výše popsané vlastnosti CMS, jakož i s ohledem na výše popsané právní aspekty, lze také dodat, že využívání, popř. nevyužívání CMS je relevantním faktorem pro posuzování plnění souvisejících právních povinností, a to zejména povinností v oblasti kybernetické bezpečnosti nebo ochrany osobních údajů, jakož i povinnosti řádného a hospodárného nakládání s veřejnými finančními prostředky a povinnosti k předcházení vzniku škod.

[1)]

Pro definici oprávnění a řízení přístupu je popis nutný. V současné době ale žádný systematický nástroj popisu neexistuje a bude nutné jej vytvořit. Tímto nástrojem bude sémantický slovník pojmů vyjádřený v podobě ontologických modelů právních předpisů a agend. Ten bude navíc sloužit jako zastřešující model a popis všech dat v datových fondech OVM.

2)

Přehled prostředků s jejich úrovní záruky seznam_poskytovatelu_identity_identity_provideridp

3)

Může být v rozporu eIDAS ver 2.0, recitál 33 a 33a a článek 45 g a článek 45ga (jde o draft) https:%%//%%data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/cs/pdf

4)

Interaktivní mapa TESTA-ng https://ec.europa.eu/isa2/solutions/testa_map_en/