Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí jednotlivými úřady 3
Pravidla pro Agendový model veřejné správy 3
Pravidla pro identifikaci klientů veřejné správy 5
Pravidla pro Propojený datový fond 10
Pravidla pro Veřejný datový fond 13
Pravidla pro Evidenci subjektů 24
Pravidla pro Prostorová data a služby nad prostorovými daty 26
Pravidla pro Úplné elektronické podání 28
Pravidla pro Integraci informačních systémů 29
Pravidla pro Portály veřejné správy a soukromoprávních uživatelů údajů 31
Pravidla pro Přístupnost informací 35
Pravidla pro Elektronickou fakturaci 37
Pravidla pro Portál občana a Portál veřejné správy 38
Pravidla pro Národní identitní autoritu 41
Pravidla pro Referenční rozhraní 48
Pravidla pro Univerzální kontaktní místo veřejné správy 53
Pravidla pro Systém správy dokumentů 54
Pravidla pro Systémy a služby spojené s právním řádem a legislativou 63
Pravidla pro Elektronické úkony a doručování 65
Pravidla pro Jednotný identitní prostor veřejné správy 67
Pravidla pro Jednotné obslužné kanály a uživatelská rozhraní úředníků 70
Pravidla pro Sdílené služby INSPIRE 71
Pravidla pro Sdílené agendové IS v přenesené působnosti 72
Pravidla pro Sdílené agendové IS pro samostatnou působnost územních samospráv 73
Pravidla pro Sdílené provozní informační systémy 74
Pravidla pro Sdílené statistické, analytické a výkaznické systémy 74
Pravidla pro eGovernment cloud 75
Pravidla pro Národní datová centra 78
Pravidla pro komunikační infrastrukturu veřejné správy 78

~~Title: Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí jednotlivými úřady~~

Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí jednotlivými úřady

Tato kapitola popisuje způsoby využívání sdílených služeb, funkčních celků a tematických oblastí v celé šíři (v celé architektuře) včetně pravidel, návodů a dobrých praktik k jejich zanesení do informační koncepce a architektury úřadu. Jde o jiný přístup k popisu požadavků na využívání systémů a služeb eGovernmentu než v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury, kde se požadavky popisují skrze jednotlivé vrstvy architektury úřadu.

Skladba této kapitoly odpovídá sdíleným službám, funkčním celkům a tematickým oblastem z části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR:

Tematické oblasti

- **Agendový model veřejné správy**
- **Identifikace klientů veřejné správy**
- **Propojený datový fond - PPDF**
- **Veřejný datový fond ČR - VDF**
- **Evidence subjektů**
- **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

- **Portál občana a portál veřejné správy - PO, PVS**
- **Národní identitní autorita – NIA**
- **Referenční rozhraní veřejné správy - ZR, ISZR, eGSB/ISSS, FAIS**
- **Univerzální kontaktní místo veřejné správy - CzechPOINT**
- **Systém správy dokumentů - eSSL**
- **Systémy a služby spojené s právním řádem a legislativou - eSeL**
- **Elektronické úkony a doručování - Datové schránky**
- **Jednotný identitní prostor veřejné správy – JIP/KAAS**
- **Jednotné obslužné kanály a uživatelská rozhraní úředníků**
- **Sdílené služby INSPIRE**
- **Sdílené agendové IS v přenesené působnosti**
- **Sdílené agendové IS pro samostatnou působnost územních samospráv**
- **Sdílené provozní informační systémy**
- **Sdílené statistické, analytické a výkaznické systémy**
- **eGovernment Cloud**
- **Národní datová centra**
- **Komunikační infrastruktura veřejné správy- KIVS/CMS**

Pravidla pro Agendový model veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci agendového modelu veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k agendovému modelu VS popíše úřad do své informační koncepce.

Základní povinnosti ohlašovatele agendy

Ohlašovatel agendy je podle zákona č. 111/2009 Sb., o základních registrech zodpovědný za řádné ohlášení agendy a za aktualizace agendy, a především za správnost a pravdivost údajů uvedených v agendě. Zjistí-li kdokoliv nesoulad reality s údaji, měl by to jako u dalších referenčních údajů ohlásit ohlašovateli, a ten musí agendu upravit do souladu se skutečností. To se netýká jen základních informací, ale i všech dalších referenčních a nereferenčních údajů, jako jsou činnosti, působnosti OVM, údaje v agendě, agendové informační systémy apod.

Základními povinnostmi ohlašovatele jsou:

- Tam, kde je gestorem legislativy, dodržovat veškeré principy pro legislativu, včetně zásad Digitálně přívětivé legislativy
- Ohlásit agendu
- Ohlásit každou její změnu
- Ohlásit působnost všech OVM a definovat výkon jim svěřených činností
- Zajistit využívání údajů ze základních registrů a související oprávnění pro jejich využívání pro podporu výkonu agendy
- Ohlásit agendové informační systémy, které spravuje a které jsou poskytovány OVM působícím v agendě
- Ohlásit údaje v agendě vedených, čerpaných i poskytovaných
- K centralizovaným agendovým informační systémům vydávat provozní řád
- Metodicky řídit výkon agendy u OVM, který v agendě působí
- Spravovat, tzn. ohlašovat a udržovat aktuální, údaje v rejstříku OVM/SPUU. U SPUU se jedná o všechny subjekty, které jsou povinné dle právních předpisů spadající do agendy, jejichž je OVM ohlašovatel. Ohlašovat může ustanovit jiné OVM, které bude tyto úkony činit.

Základní povinnosti OVM působícího v agendě

V rámci agendy veřejné správy mohou veřejnoprávní činnosti vykonávat pouze ty orgány veřejné moci, které jsou v rámci ohlášení agendy vyznačeny jako orgány veřejné moci vykonávající působnost, a to v rámci konkrétních činností. To znamená, že po aplikaci principu referenčních údajů v Registru práv a povinností lze konstatovat, že pokud v rámci dané agendy vykonává veřejnoprávní činnost orgán veřejné moci, který nemá vyznačenou působnost, jedná se o porušení zákona a ohlašovatel agendy musí neprodleně toto napravit. To se týká nejen samotného seznamu působících orgánů veřejné moci, ale také přiřazení jejich činností. Výkon činnosti je byznysovou vazbou a odborně jej nazýváme "činnostní rolí".

Základními povinnostmi orgánů veřejné moci působících v agendě tedy jsou:

- Vykonávat činnosti dle ohlášení agendy

- Pokud OVM zjistí nesoulad skutečnosti a údajů v ohlášení agendy, je povinen požadovat po ohlašovateli nápravu.
- Pokud sám spravuje agendový informační systém pro výkon agendy (není poskytován centrálně), ohlásit tento systém do RPP jako ISVS.
- Pokud existuje centralizovaný agendový informační systém, tak tento využívat.
- Přistupovat k údajům v základních registrech a dalších ISVS výhradně na základě oprávnění ohlášeného v agendě.
- Spravovat jen ty údaje, které jsou ohlášeny v dané agendě.
- Pokud zjistí nesoulad referenčních údajů v jednotlivých základních registrech se skutečností, zahájit proces reklamace u příslušného editora.

Pravidla pro identifikaci klientů veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci identifikace klientů veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k elektronické identifikaci klientů VS popíše úřad do své informační koncepce.

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.

Samotný občanský průkaz, který může sloužit i k elektronické identifikaci, lze použít k fyzické identifikaci na různé úrovni:

- Střední úroveň
  - Zjištění, zda nejde o padělaný občanský průkaz
    - Strojově čitelné občanské průkazy
    - Ostatní občanské průkazy
  - Zjištění, zda je předložený občanský průkaz platný
    - Seznam platných občanských průkazů
    - Seznam neplatných občanských průkazů
  - Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
- Vysoká úroveň

- Zjištění, zda nejde o padělaný občanský průkaz
  - Strojově čitelné občanské průkazy
  - Ostatní občanské průkazy
- Zjištění, zda je předložený občanský průkaz platný
  - Seznam platných občanských průkazů
  - Seznam neplatných občanských průkazů
- Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
- Vyžádání si aktuálních údajů, včetně fotografie, o klientovi, který jej předložil a jejich kontrola

Fyzická identifikace právnických osob

Pokud jde o právnické osoby v pojetí českého právního řádu, tyto nemohou z jejich povahy nikdy právně jednat samy, musí za ně vždy jednat zástupce, kterým je (byť i nepřímo, např. je-li právnická osoba statutárním orgánem jiné právnické osoby) finálně vždy fyzická osoba (příp. fyzické osoby). Pro použití ve fyzickém prostředí se identifikační prostředky právnických osob v České republice nevydávají. Je tomu tak proto, že právnická osoba není ve fyzickém prostoru přítomna a vždy za ni jedná fyzická osoba, která prokazuje svou vlastní totožnost.

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.

Elektronická identifikace právnických osob

Pokud jde o právnické osoby v pojetí českého právního řádu, tyto nemohou z jejich povahy nikdy právně jednat samy, musí za ně vždy jednat zástupce, kterým je (byť i nepřímo, např. je-li právnická osoba statutárním orgánem jiné právnické osoby) finálně vždy fyzická osoba (příp. fyzické osoby). Z toho plyne, že ustanovení § 2 zákona o elektronické identifikaci, které dopadá na případy fyzických osob, se tak vztahuje i na jednání právnických osob, neboť jsou to vždy fyzické osoby, které fakticky jednají, ať již za sebe, či za jinou fyzickou osobu nebo právnickou osobu.

V elektronickém prostředí, zejména jde-li o automatizovanou komunikaci, jsou nicméně používány mechanismy, které mají charakter identifikačního prostředku právnické osoby. Jde např. o certifikát pro evidenci tržeb podle

zákona č. 112/2016 Sb., o evidenci tržeb, nebo certifikáty vydané Českou národní bankou pro automatizovanou komunikaci mezi ČNB a subjekty podléhající jejímu dozoru, typicky bankami. Platí nicméně, že identifikační prostředky právnických osob s použitím bez ohledu na agendy, ekvivalentní např. občanským průkazům, se v České republice nevydávají.

Zatímco samotná autentizace fyzické osoby není problematická, problematická se jeví otázka určení, zda fyzická osoba jedná v dané situaci za sebe (popř. v jaké roli za sebe) anebo zda jedná za jinou fyzickou osobu nebo za právnickou osobu. Problematika mandátů a oprávnění je řešena níže.

Skutečnost, že daná fyzická osoba, má právo se identifikovat a autentizovat za určitou právnickou osobu (tj. „přihlásit se ke službě jménem právnické osoby“), ještě nezakládá bez dalšího právo na to, že tato fyzická osoba má právo za danou právnickou osobu činit úkony prostřednictvím digitální služby. Autorizaci dané fyzické osoby k poskytnutí digitální služby musí posoudit ten, ke komu se fyzická osoba hlásí na základě jím dostupných údajů (informace z obchodního rejstříku, plná moc opravňující konkrétní osobu jednat jménem právnické osoby,…) ve spojení s příslušnými právními předpisy.

Jako příklad takového přístupu můžeme uvést datové schránky, do nichž se fyzická osoba přihlásí například novým občanským průkazem s aktivovaným čipem. Po úspěšné autentizaci s pomocí prostředku pro elektronickou identifikaci (tj. např. s pomocí „eObčanky)“ a souhlasu s předáním osobních údajů na portálu Národního bodu pro identifikaci a autentizaci, je fyzická osoba pro účely informačního systému datových schránek (ISDS) ztotožněna. Po ztotožnění tak nabídne ISDS fyzické osobě seznam datových schránek, ve vztahu k nimž je přihlášená fyzická osoba oprávněná jednat.

Autentizovaná fyzická osoba si tedy vybírá, za koho a v jaké roli bude prostřednictvím datových schránek jednat. Informaci o tomto oprávnění si ISDS obstarává např. z ROS, z jiných zdrojů (např. údaj o tom, že určitá osoba je advokátem nebo insolvenčním správcem) anebo jej vede na základě sdělení samotného držitele datové schránky (např. údaj o tzv. pověřené osobě). Bez ohledu na zdroj informace o oprávnění k zastupování jiné osoby, resp. na zdroj informace o roli je však na samotném ISDS jakožto poskytovateli služeb, aby oprávnění k zastupování jiné osoby ve svém prostředí řádně implementoval tak, aby osoby mohly toto oprávnění realizovat. Nabídka jednotlivých oprávnění, resp. rolí, tedy spadá do kompetence daného poskytovatele služeb a odvíjí se od údajů a oprávnění, které vede v rámci svého informačního systému nebo od údajů, ke kterým má přístup.

Mandáty, role a práva v elektronické komunikaci

Zajištění správné obsazení do role neboli autorizace, klienta využívajícího elektronické služby je jedním ze základních předpokladů jejího správného fungování. Různé role mají v rámci služby různá oprávnění a povinnosti a poskytovatel služby je povinen nabídnout klientovi veškeré role, do kterých se v rámci služby může pasovat, včetně rolí jako zástupce právnické osoby, zástupce nezletilého, registrující lékař pacienta a další. Tyto role s oprávněními vůči jiným klientům veřejné správy jsou mandáty. Aby proběhlo správné obsazení do role a zjištění mandátu, je pro poskytování elektronických služeb klientům veřejné správy nutné mít zajištěno několik základních náležitostí:

1. Znalost typů mandátů při jednání s veřejnou správou
2. Jednoznačnou identifikaci a autentizaci klienta veřejné správy
3. Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu
4. Vlastní zajištění autorizace klienta veřejné správy

Mandáty pro jednání s veřejnou správou

Při výkonu veřejné správy a to zejména při jakékoliv interakci a komunikaci s klientem veřejné správy je nutné, aby veřejná správa respektovala mandáty k zastupování jedné osoby druhou na základě různých titulů. Zjednodušeně se dá rozdělit forma mandátu zastupování dle následující tabulky.

Typ subjektu	Mandát
Fyzická osoba	Jednající sama svým jménem
	Jednající jménem jiné fyzické osoby ze zákona: - rodič dítěte, - manžel/manželka, - registrovaný partner/partnerka, - opatrovník, osvojitel, poručík, pěstoun - dědic, exekutor, - zastupující osoba pro osoby neschopné jednat nebo nemající zákonného zástupce
	Jednající jménem jiné fyzické osoby ze zmocnění: - plná moc, - advokát, - zastupující FO, - jiný druh zmocnění, - na žádost bez zmocnění
	Plná moc opravňující konkrétní osobu jednat jménem právnické osoby
Fyzická osoba jednající za právnickou osobu	Jednatel právnické osoby
	statutární zástupce právnické osoby (jedna FO)
	Statutární orgán právnické osoby (více FO)
	Insolvenční správce
	Likvidátor
	Jednající jménem zřizovatele právnické osoby
	Pověřen k jednání za právnickou osobu: - Veřejnoprávním titulem, - Soukromoprávním titulem (smlouva, plná moc, společenská smlouva, apod.)
	Pokud agendový předpis povoluje využívání přístupových údajů k systému datových schránek jako identifikačních prostředků je to dále: a) Pro fyzické osoby – statutární zástupce oprávněné k přístupu do datové schránky právnické osoby ověřením oprávnění k datové schránce právnické osoby prostřednictvím Informačního systému datových schránek (ověření přístupových údajů a oprávnění). b) Pro fyzické osoby - oprávněné statutárním zástupcem k přístupu do datové schránky právnické osoby ověřením oprávnění k datové schránce právnické osoby prostřednictvím Informačního systému datových schránek (ověření přístupových údajů a oprávnění). c) Ověřením speciálního agendového oprávnění podle agendového předpisu, na jehož základě jsou poskytovány agendové digitální služby.

Příklady mandátů pro fyzické osoby vyplývající z některých vyhlášek a nařízení měst a obcí:

- Pro přihlášení k platbě poplatku za odvoz komunálního odpadu
- Pro přihlášení k platbě poplatku:
  - ubytovacího,
  - ze psa,
  - za zábor a užívání veřejného prostranství.
- Pro převody, koupě, prodej, nabytí městského majetku, (provozovny v budovách v majetku města)
- Pro užívání, podnájem, zrušení užívání bytového fondu města
- Mandát pro jednání s knihovnou – výpůjčky registrovaného čtenáře

Jak je zdůrazněno níže, při výkonu veřejné správy je nutné, aby příslušný orgán konající nějakou činnost v rámci dané agendy věděl, pro jakou formu zastupování je mandát umožněný nebo dokonce nutný. Zcela jiným způsobem se orgán veřejné moci bude chovat k mandátu plynoucímu z veřejnoprávního titulu rodičovství a jinak k mandátu plynoucímu ze soukromoprávního titulu plné moci.

Je také vhodné rozlišovat účel mandátu, tedy typ úkonů, které prostřednictvím zastupované osoby klient veřejné správy dělá. Ty je možno rozdělit do následujících skupin:

- Nahlížení na údaje subjektů práva bez jakéhokoliv interaktivního využívání či zapisování údajů (informační účel).

- Přístup k údajům subjektů a jejich reklamace, nebo pokud je přímo umožněna editace klientům veřejné správy (transakční účel).
- Zmocnění k přístupu či využívání údajů subjektu práva pro třetí strany, nebo poskytnutí údajů z ISVS třetím stranám (zmocňovací účel).
- Činění podání a úkonů vůči orgánům veřejné správy (účel úkonu).
- Využívání elektronických klientských služeb jako je objednání se k úředníkovi.
- Zápis, úprava a zrušení mandátu.

Jednoznačná identifikace a autentizace klienta veřejné správy

Všechny subjekty povinné dle zákona č. 250/2017 Sb., o elektronické identifikaci mají povinnost dle §2 využívat k prokázání totožnosti při elektronickém kontaktu pouze kvalifikovaný systém, konkrétně:

„Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace.“

Kvalifikovaný systém spravuje kvalifikovaný správce (státní orgán nebo akreditovaná osoba) a splňuje technické normy i specifikace Evropské unie a především je propojen s národním bodem pro identifikaci a autentizaci – tzv. Národní identitní autorita (NIA).

Identifikace a autentizace prostřednictvím NIA zajistí jen a pouze službu ověřené identity fyzické osoby, neboli každý systém čerpající služby NIA, se může spolehnout na to, že přihlášená fyzická osoba je skutečna ta, za kterou se vzdáleně a elektronicky vydává. Již se dále nezajišťují další služby typu autorizace.

Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu

Systém poskytující elektronické služby veřejné správy musí být schopen komunikovat a získávat údaje z propojeného datového fondu. K tomu musí systém odpovídat předpisům:

- Zákon 365/2000 Sb., o informačních systémech veřejné správy. Systém klasifikovaný jako Informační systém veřejné správy (ISVS) využívající referenční rozhraní veřejné správy.
- Zákon 111/2009 Sb., o základních registrech. Systém klasifikovaný jako agendový informační systém (AIS) využívající údaje základních registrů a editorů základních registrů dle svého agendového zákona.
- Zákon 250/2014 Sb., o elektronické identifikaci. Systém, který vyžaduje ověření totožnosti
- Nařízení eIDAS

Více o využívání údajů propojeného datového fondu a infrastruktuře referenčního rozhraní je napsáno v kapitolách:

- eGON Service Bus/Informační systém sdílené služby
- Centrální místo služeb
- Propojenný datový fond

Centrální sdílené služby eGovernmentu dokáží zajistit následující mandáty pro fyzické osoby, které se prokázaly u poskytovatele služeb svou zaručenou elektronickou identitou:

- eGON služba rosCtiPodleUdaju, rosCtiIco, rosCtiAifo (základní registr osob)
  - pro zajištění ověření, zda je fyzická osoba statutárním zástupcem
- eGON služba aiseoCtiPodleUdaju, aiseoCtiAifo (agendový informační systém evidence obyvatel)
  - pro zajištění ověření, zda je fyzická osoba rodič nezletilého, který není svéprávný
  - pro zajištění ověření, zda je fyzická osoba zákonným zástupcem jiné fyzické osoby
  - pro zajištění ověření, zda je fyzická osoba opatrovníkem jiné fyzické osoby
  - pro zajištění ověření, zda je fyzická osoba manžel/manželka
- eGON služba isknCtiVlastniky (informační systém katastru nemovitostí)

    - pro zajištění ověření, zda je fyzická osoba vlastníkem nemovitosti
- Služba ISDS
    - Pro zajištění, zda je fyzická osoba pověřená k činění úkonů v ISDS vlastníkem datové schránky

Žádné další centrální služby ověření oprávnění/mandátů se v současné, ani dohledné době, neplánují. Proto je důležité, aby si každý poskytovatel elektronických služeb zajistit jiné typy mandátů sám.

Vlastní zajištění autorizace klienta veřejné správy

Každá vykonávaná agenda (výkon veřejné správy) může pro svoji potřebu vyžadovat jiné mandáty. Například mandát podání daňového přiznání za jinou fyzickou osobu, mandát nahlížení na zdravotnickou dokumentaci jiné fyzické osoby, nakládání s majetkem právnické osoby, u které nejsem statutární zástupce, či například mandát k zastupování při dědickém řízení.

Všechny tyto mandáty se musí řešit v rámci dané agendy a jako ideální řešení navrhujeme:

- Zřídit buď v jednotlivých agendových informačních systémech, nebo v rámci centralizované správy subjektů mandátní registr.
- V rámci mandátního registru určit předem definované typy mandátů přípustné v dané agendě a způsob zápisu mandátů pro nahlížení a pro transakce ze strany klienta
- Povolit zapisovat všem klientům mandáty dle definovaných typů pod svou zaručenou elektronickou identitou.
- Umožnit klientům přidat mandát i offline, například na přepážce úřadu.
- Při každém přihlášení klienta kontrolovat kromě mandátů z centrálních sdílených služeb eGovernmentu i vlastní mandátní registr a dát vždy při přihlášení vybrat klientovi, v jaké roli a s jakým mandátem chce pracovat.

Je důležité zdůraznit, že veřejná správa nemá rozlišovat formu komunikace a jednání s klientem. Tedy mandát obecně platící pro osobní jednání s úředníkem, nebo pro fyzické prováděné úkony na přepážce, musí mít klient umožněn využívat i při elektronické komunikaci a naopak. Také proto je nutné vést mandáty standardizovanou formou na jednom místě a využívat jich i při elektronické komunikaci klienta.

Mandát plynoucí z veřejnoprávního nebo soukromoprávního titulu a to včetně plných mocí a dohod o zastupování při správním jednání s úřady patří mezi společné rozhodné skutečnosti, tak jak jsou zakotveny v souvisejících ustanoveních Správního řádu (zejména § 6 a § 50 a související). Proto je nanejvýš vhodné, aby příslušný orgán veřejné moci, pokud

- využívá a buduje centrální evidenci subjektů,
- centrální evidenci rozhodných skutečností,
- skutečnosti o zapsaném anebo z něčeho plynoucím mandátu k zastupování,
- je zahrnul do rozhodných skutečností.

Klient se totiž může odvolat na příslušná ustanovení správního řádu a neposkytovat zejména plné moci a další dokumenty, z nichž mandát plyne, úřadu opakovaně.

Pravidla pro Propojený datový fond

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních

celků a tematických oblastí v rámci propojeného datového fondu je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k propojenému datovému fondu popíše úřad do své informační koncepce.

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**.

Poskytování / Využívání údajů

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.

Pravidla pro Veřejný datový fond

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci veřejného datového fondu je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k veřejnému datovému fondu popíše úřad do své informační koncepce.

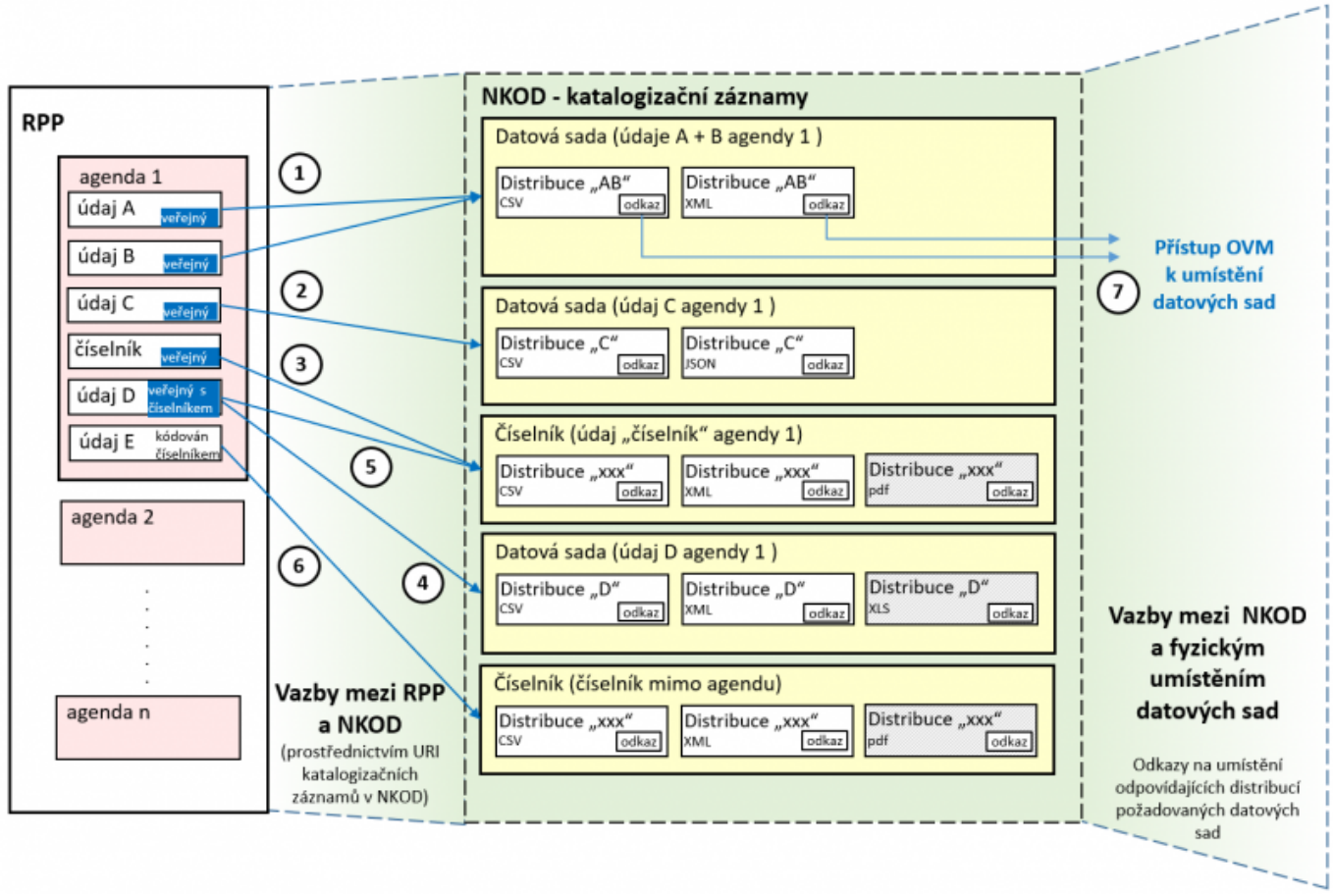
Pravidla pro údaje zpřístupněné veřejným datovým fondem

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

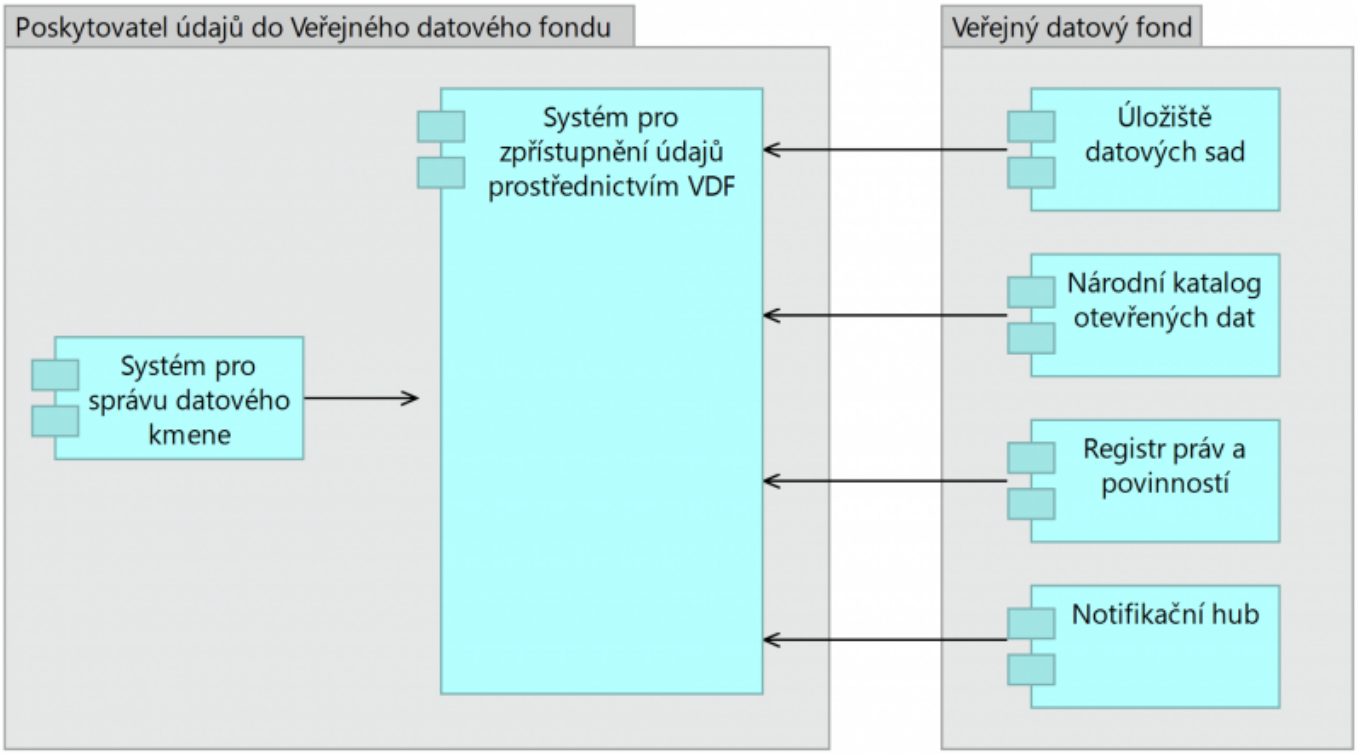
agenda přímo vytváří, ale vše uvedené platí, pro jakýkoliv využívaný číselník). Evidence údaje v RPP proto také obsahuje IRI datové sady v NKOD, který obsahuje publikovaný číselník.

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.

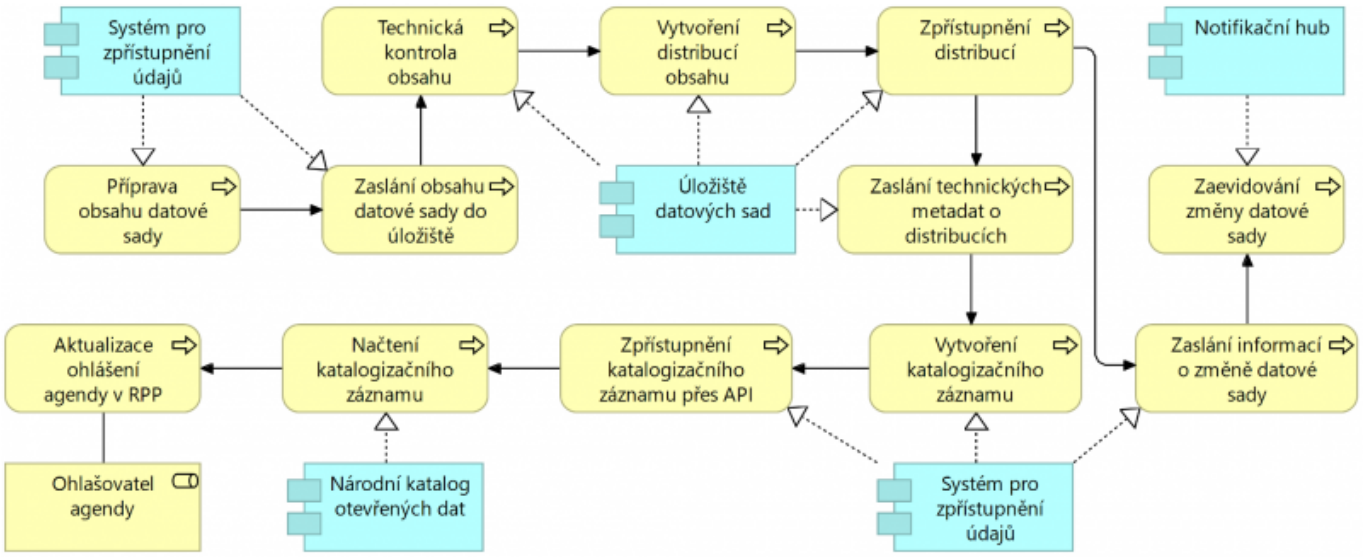
Pro potřeby sdílení údajů ve VDF poskytovatel údajů vytvoří *systém pro zpřístupnění údajů prostřednictvím VDF*. Může se jednat o samostatný systém nebo to může být modul v rámci existujícího systému. Zajišťuje získávání obsahu veřejných údajů z datového kmene poskytovatele, rozdělení do vhodných datových 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.

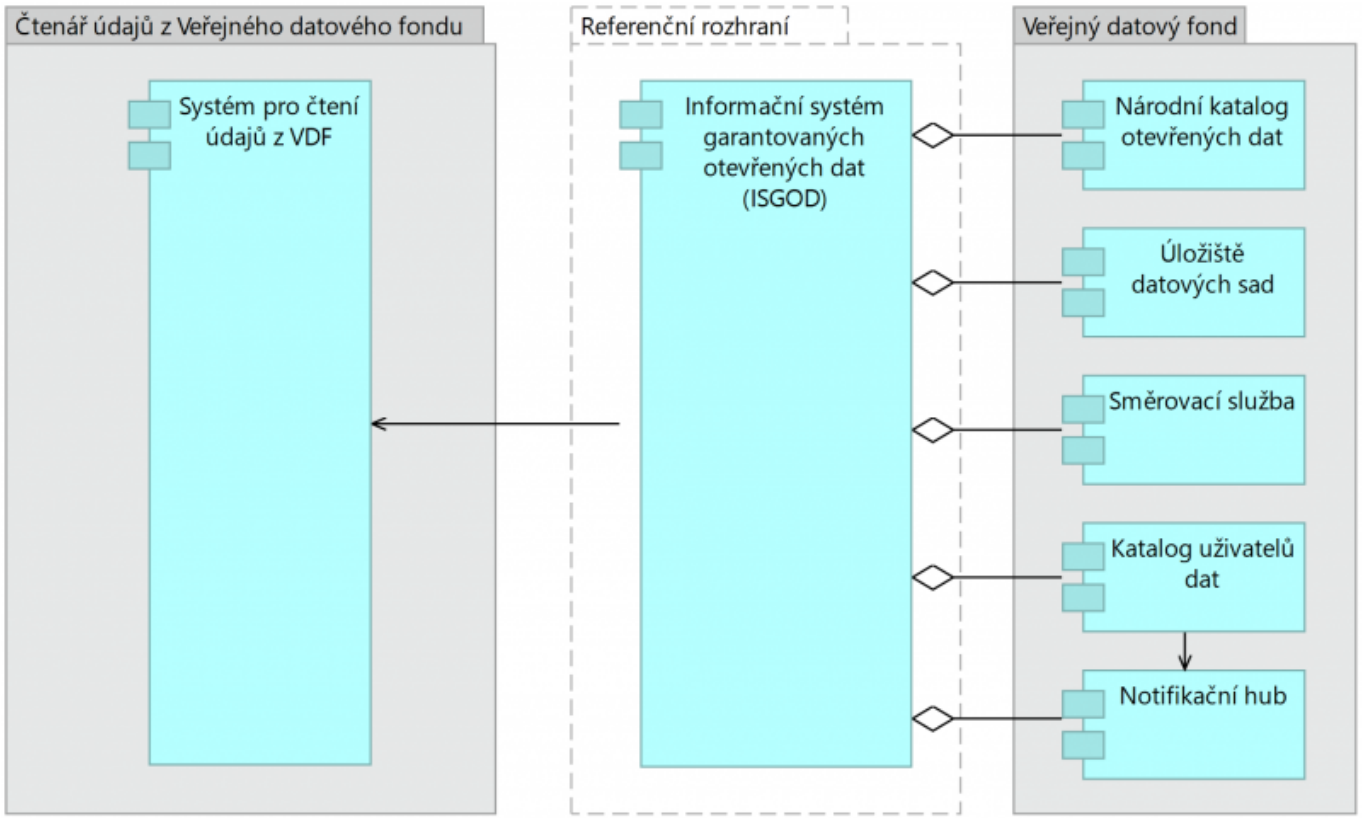
Systém pro zpřístupnění údajů prostřednictvím VDF souvisí s existujícím systémem pro zpřístupnění údajů prostřednictvím PPDF, který zajišťuje poskytování údajů o konkrétním subjektu práva, na který přistupuje čtenářský AIS prostřednictvím PPDF. Systém pro zpřístupnění údajů prostřednictvím VDF (dále 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)

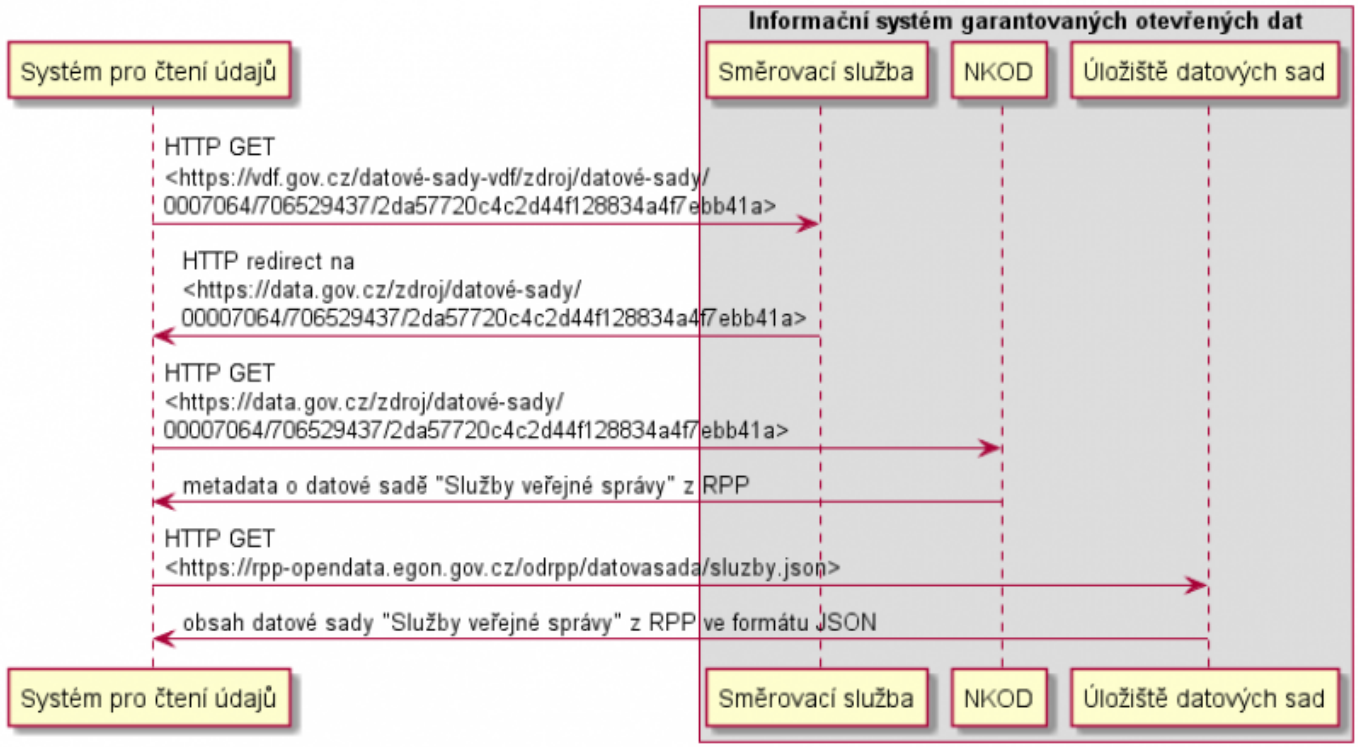
ISGOD je pouhým logickým zastřešením výše uvedených služeb.

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:

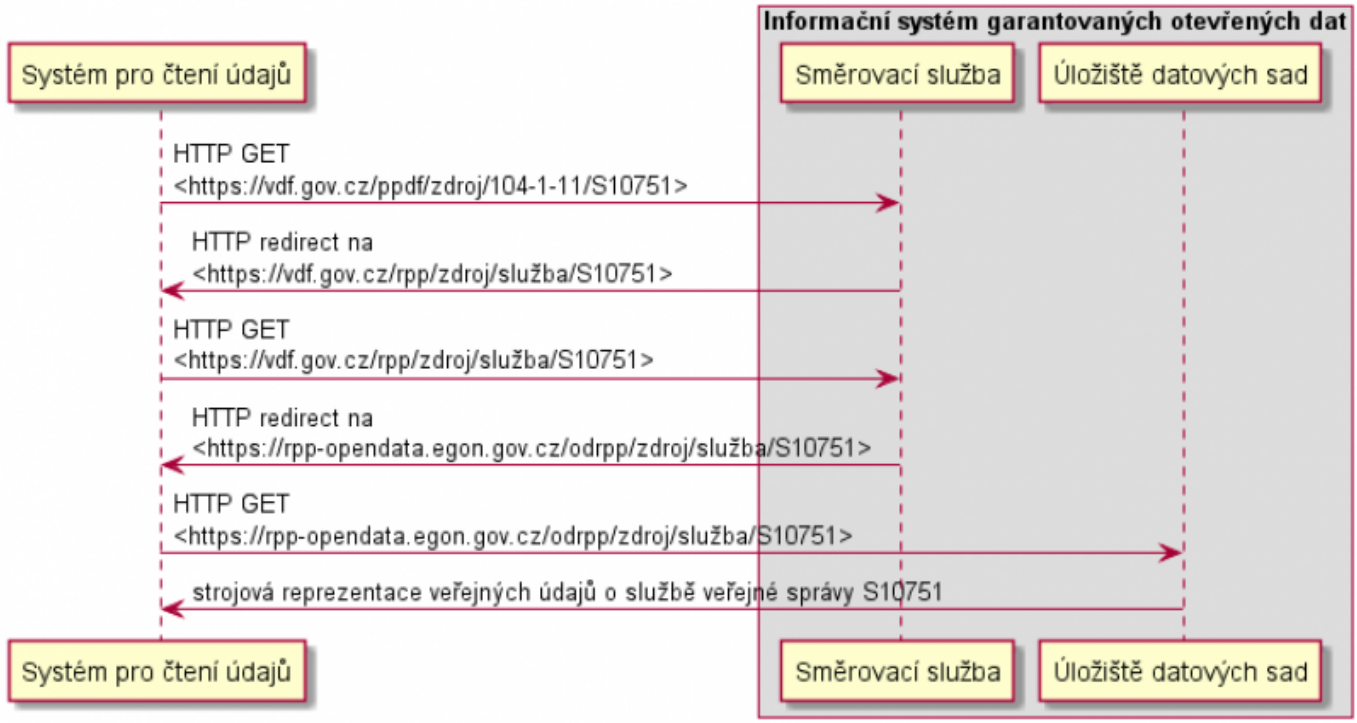
- V předchozích krocích byl přečten z VDF údaj s referenčním IRI jako hodnotou.
- V předchozích krocích byl přečten z PPDF údaj s proprietárním identifikátorem entity jako hodnotou (tj. identifikátor v podobě řetězce, který identifikuje entitu lokálně v rámci ISVS). Referenční IRI položky s veřejnými 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>

Pravidla pro Evidenci subjektů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci agendového modelu veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k agendovému modelu VS popíše úřad do své informační koncepce.

Využívání jednotlivých identifikátorů

Jako identifikátor fyzické osoby (a potažmo i právnické, protože za právnickou osobu vždy jedná fyzická osoba), se v různých agendách používají různé druhy identifikátorů, a to jak pro účely vnitřních procesů a služeb (uvnitř úřadu), tak i při výměně údajů (ven z úřadu). Identifikátory subjektů se využívají při úřední komunikaci a interakci s klientem, při evidenci údajů v příslušných informačních systémech a ve spisové dokumentaci a při výměně údajů s dalšími informačními systémy.

Pravidla pro klientský identifikátor

Klientský identifikátor je možné přidělovat všem subjektům vedeným v evidenci daného úřadu. Není nutné mít legislativní úpravu, přesto je vhodné mít doložitelná pravidla, která klientský identifikátor v úřadu upravují.

- Vydání klientského identifikátoru se musí týkat pouze subjektů ztotožněných proti základním registrům, tedy obdržením AIFO pro fyzické osoby
- Klientský identifikátor lze přidělit i subjektům, které v evidenci ještě nejsou, ale existuje oprávněný zájem na daný subjekt od jiného oprávněného tazatele.
    - Příkladem mohou být evidence, které mají dávat zpětné informace oprávněných tazatelů ve chvíli, kdy se subjekt v evidenci objeví. Tedy oprávněný tazatel chce po evidenci vědět, kdy se v ní subjekt teprve objeví. Aby se nemuselo komunikovat osobními údaji, vydá evidence tazateli klientský identifikátor na subjekt, který dosud v evidenci nemá a bude jej informovat, jakmile se v ní objeví.
- Předchozí bod znamená vedení AIFO na subjekt, který v evidenci neexistuje, a k němu klientský identifikátor. Tento tzv. "klientský kmen" je odlišným od "datového kmene" související s předmětným právem nebo povinností agendy. Klientský kmen je evidencí současných a teprve potenciálních klientů.

Při evidenci subjektů v datovém kmenu úřadu

Cílem PPDF a pseudonymizace je zavést jednotnou formu identifikace subjektu při jeho evidenci. Nelze nadále využívat dosud zneužívané persistentní identifikátory, ale je naopak nutné rychle se přizpůsobit povinnostem pseudonymizace. Proto je nutno respektovat níže uvedené základní principy pro evidenci subjektů:

1. Identifikátorem pro komunikaci mezi jednotlivými agendovými informačními systémy je vždy AIFO (AIFO se překládá přes služby ISZR a ISSS).
2. AIFO se nikdy v systému nezobrazí a úředník k němu nesmí mít žádný přístup.
3. Úředním/klientským identifikátorem fyzické osoby nesmí být AIFO, ale vždy klientské číslo pro danou agendu, které přidělí správce dané agendy a které se využívá jako prezentovaný identifikátor v AISu a pro úředníka. Tento identifikátor musí být bezvýznamový, nelze tedy z něj odvodit další osobní údaje fyzické osoby. Agenda přidělující klientský identifikátor musí poskytovat služby pro jeho získání na základě stykového identifikátoru či AIFO a zpět. Současně řídí oprávnění k použití takové služby.
4. Při komunikaci s klientem (osobní jednání na přepážce i zpracování doručených dokumentů a zpráv) se využívají stykové identifikátory, jako jsou typ a číslo dokladu a využije se služba jednorázového překladu na AIFO a služby vydavatele klientského identifikátoru pro získání tohoto identifikátoru.
5. Stykové identifikátory si primárně neeviduji, leda by byly zároveň klientským číslem.
6. AIFO osoby se nikdy nesmí přímo poskytnout, vždy se využívá služeb překladu z mého AIFO na AIFO příjemce výměny údajů.
7. Pokud k tomu nejsou specifické důvody, tak při výměně údajů se vyměňuje pouze AIFO a nepřidávají se další identifikátory nebo údaje.

Služby pro překlad aktuálního stykového identifikátoru musí být poskytovány s úrovní dostupnosti kritická – jedná se o ztotožnění osoby. Vydavatel či správce stykového identifikátoru musí zajistit jeho historickou jednoznačnost a služby zajišťující překlad na AIFO i pro historické hodnoty identifikátoru (pro historické hodnoty je požadovaná úroveň dostupnosti – primární služba).

Při interakci s klientem

1. Při osobním jednání s klientem nebo při jeho prezenčním ztotožnění se využije typ a číslo dokladu, který klient předložil, nebo jinak ověřený stykový identifikátor.
    - Klient předloží doklad s uvedeným identifikátorem, který je stykovým identifikátorem.
    - Prostřednictvím daného AIS se zavolá služba jednorázového ztotožnění osoby přeložením stykového identifikátoru na dané AIFO v jeho agendě.

    - Dále úředník pracuje v AIS podle AIFO subjektu (které sám na obrazovce nevidí), stykový identifikátor si dále neuchovává. Pokud existuje klientský identifikátor, ten při komunikaci uchovat může.
    - Při komunikaci s ostatními AISy a ostatními agendami využije služby svého AISu (kdy AIS prostřednictvím ISSS zajistí výměnu údajů po překladu AIFO).
2. Při osobním jednání s klientem se využije klientský identifikátor vydaný klientovi dříve
    - Dle povahy poskytované služby může stačit pouze identifikace pomocí klientského identifikátoru, pokud nedostačuje, následuje ověření totožnosti či doložení dalších identifikátorů, např. stykových.
    - Klient předloží u poskytovatele zdravotních služeb klientský identifikátor (číslo pojištěnce na kartičce pojištění)
    - Pro potřebu identifikace v čekárně dostačující způsob identifikace
    - Pro potřebu poskytnutí zdravotních služeb klient dokládá stykový identifikátor
    - Při nutnosti obstarat si další údaje z jiných systémů veřejné správy se postupuje obdobně jako výše.

Při zpracování formulářů pak nastávají tyto tři situace a z nich plynoucí postupy:

1. Elektronický formulář: Formulář musí být vytvořen tak, aby umožňoval již přenos identity klienta, a při jeho zpracování provede AIS dohledání aktuálních údajů podle AIFO subjektů.
2. Listinný formulář: Na listinném formuláři se vyžaduje kombinace údajů křestní jméno, příjmení a typ a číslo dokladu, nebo jiný stykový identifikátor. Při zpracování formuláře se opět v AIS provede zavolání příslušné služby pro jednorázový překlad stykového identifikátoru na AIFO, a tím i ztotožnění subjektu pro daný AIS. V tomto případě se všechny údaje (včetně identifikátorů) pamatují z důvodu nutnosti uchovávání samotného formuláře.
3. Asistované podání: Při asistovaném podání na přepážce příslušný pracovník provede prezenční ztotožnění podle dokladu, a pokud na základě jednání na přepážce bude činit něco jménem subjektu, bude k tomu využívat příslušné služby. Pokud bude pak činit úkon jménem OVM, opět při zápisu do AIS tento AIS zavolá službu jednorázového překladu stykového identifikátoru na AIFO.

Pravidla pro Prostorová data a služby nad prostorovými daty

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci úplného elektronického podání je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k prostorovým datům a službami nad prostorovými daty popíše úřad do své informační koncepce.

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

Pravidla pro Úplné elektronické podání

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci úplného elektronického podání je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k úplnému elektronickému podání popíše úřad do své informační koncepce.

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.

Pravidla pro Integraci informačních systémů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci úplného elektronického podání je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k integraci informačních systémů popíše úřad do své informační koncepce.

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.

Pravidla pro Portály veřejné správy a soukromoprávních uživatelů údajů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci portálů veřejné správy a soukromoprávních uživatelů údaje je popsán na samostatné stránce zde nebo v rámci části Architektura sdílených služeb veřejné správy.

Využití a popis k přístupu k portálům VS a SPUU popíše úřad do své informační koncepce.

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!**

Pravidla pro Přístupnost informací

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci přístupnosti informací je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k přístupnosti informací popíše úřad do své informační koncepce.

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.

Pravidla pro Elektronickou fakturaci

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci elektronické fakturace je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k elektronické fakturaci popíše úřad do své informační koncepce.

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

Pravidla pro Portál občana a Portál veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci portálu občana a portálu veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k portálu občana a portálu veřejné správy popíše úřad do své informační koncepce.

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.

Pravidla pro Národní identitní autoritu

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci Národní identitní autority je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k Národní identitní autoritě popíše úřad do své informační koncepce.

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[1)]), 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.

Pravidla pro Referenční rozhraní

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci Národní identitní autority je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k Referenčnímu rozhraní popíše úřad do své informační koncepce.

Detailní průvodce připojení k referenčnímu rozhraní veřejné správy je uveden zde https://pruvodcepripojenim.gov.cz/

Způsob získání referenčních údajů

Webové služby

Prostřednictvím webových služeb může subjekt čerpat referenční údaje ze ZR. Subjekt, který působí v agendě, má tuto agendu řádně ohlášenou v RPP, má zaregistrovaný svůj agendový informační systém (také jako AIS) a vydaný platný certifikát od správy základních registrů (také jako SZR), přičemž na čerpání údajů musí mít vlastní zákonné zmocnění ve svém zákoně a dle zákona č.111/2009 Sb., o základních registrech, je tento subjekt oprávněn čerpat referenční údaje ze ZR prostřednictvím vnějších služeb informačního systému správy základních registrů (také jako ISZR).

Pro získávání referenčních údajů webovými službami je nezbytné nejdříve ztotožnit svůj datový kmen vůči ZR a následně se přihlásit pro příjem notifikací o změnách.

- Informace ohledně ZR jsou na stránkách: http://www.szrcr.cz/vyvojari
- Informace, jakým způsobem připojit svůj AIS do ISZR: http://www.szrcr.cz/file/170/
- Informace, jakým způsobem využívat notifikace ze ZR je k nalezení zde: 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

Czech POINT

Zkratka Czech POINT znamená Český Podací Ověřovací a Informační Národní Terminál. Jde o kontaktní místo veřejné správy, které poskytuje občanům zejména ověřené údaje vedené v centrálních registrech, jako jsou

rejstřík trestů, obchodní rejstřík nebo registr živnostenského podnikání. Kromě standardních služeb, lze využít výpisy ze základních registrů podle zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Občané tak mají možnost ověřit si údaje, které jsou o nich v registrech vedeny, úředníci pak mají prostřednictvím formulářů v části CzechPOINT@office přístup k referenčním údajům ze základních registrů.

Jedním z cílů zavádění je zrychlit, zpřístupnit a zefektivnit služby občanům a dalším subjektům. Czech POINT je tedy kontaktním místem veřejné správy, které umožňuje na jediném místě získávat výpisy nebo činit podání.

- Informace k Czech POINT naleznete na http://www.czechpoint.cz/public/

Informační systém datových schránek

Pomocí datových schránek je možné zasílat dokumenty v elektronické podobě orgánům veřejné moci a také je takto od nich přijímat.

Komunikace prostřednictvím datových schránek nahrazuje klasický způsob doručování v listinné podobě, protože zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, zrovnoprávňuje papírovou a elektronickou verzi zasílaného dokumentu. Orgánům veřejné moci a právnickým osobám jsou datové schránky zřízeny automaticky, všem ostatním na základě jejich žádosti. Požádat o výpisy může každý, kdo má zřízenou datovou schránku a je oprávněnou osobou podle § 8 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

- Informace k datovým schránkám naleznete https://www.datoveschranky.info/

Portál občana a portál veřejné správy

Fyzické osoby (občané) mají možnost žádat o výpisy ze základních registrů prostřednictvím datové schránky na svém personalizovaném účtu portálu občana, pokud mají na portálu občana zřízenou datovou schránku a připojenou do svého profilu. Do portálu občana je možné se přihlásit datovou schránkou, jménem – heslem – SMS nebo elektronickou občankou s čipem, vydávanou od 1. 7. 2018.

- Informace o způsobu přihlášení https://obcan.portal.gov.cz/prihlaseni
- Informace o elektronické identitě https://obcan.portal.gov.cz/prihlaseni
- Dále je možné požádat o výpis ze ZR přes portál veřejné správy.
- Odkaz na jednotlivé formuláře k nalezení zde: https://www.portal.gov.cz/obcan/formulare

Kdo může žádat o referenční údaje ze ZR

Webové služby

Subjekt státní správy svým AIS, který má zákonné zmocnění ve svém zákoně využívat referenční údaje ze ZR, působící v řádně ohlášené agendě v registru práv a povinností a má vydaný platný certifikát od správy základních registrů pro přístup do ZR. Dále soukromoprávní subjekt práva zprostředkovaně přes AIS některého z orgánu veřejné moci, který má opět zákonné zmocnění využívat údaje ze základních registrů v rámci přidělené agendy řádně ohlášené v RPP.

Czechpoint

Na kontaktním místě, dle typu jednotlivých formulářů, které jsou v rámci Czechpoint k dispozici, může žádat fyzická, podnikající fyzická osoba i právnická osoba. Bližší informace, kdo může žádat u jednotlivého typu formuláře je k dispozici v sekci Typy žádostí pro získání referenčních údajů ze ZR.

Informační systém datových schránek

Informační systém datových schránek je prostředek pro získávání referenčních údajů ze základních registrů formou zaslání jednoho z formulářů v sekci Typy žádostí pro získání referenčních údajů ze ZR. Požádat o výpisy může každý, kdo má zřízenou datovou schránku a je oprávněnou osobou podle § 8 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů. Ostatní subjekty si mohou datovou schránku zřídit volitelně.

Portál občana a portál veřejné správy

Žádat o výpis údajů ze základních registrů v rámci portálu občana má možnost podat každá fyzická osoba (občan), která má na svém personalizovaném účtu portálu občana zřízenou datovou schránku připojenou ke svému profilu. V rámci portálu veřejné správy, má možnost podat žádost o získání referenčních údajů ze základních registrů každý subjekt, který je uveden v sekci Typy žádostí pro získání referenčních údajů ze ZR, dle typu žádosti.

Typy žádostí pro získání referenčních údajů ze ZR

Žádost o **výpis údajů z registru obyvatel** – dle § 58 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (fyzická osoba), o kterém jsou údaje vedeny.
- Za subjekt práva podle § 58 odst. 9 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, může žádat jeho zákonný zástupce.
- Za subjekt práva může žádat zmocněnec na základě plné moci s úředně ověřeným podpisem zmocnitele.

Žádost o **veřejný výpis údajů z registru osob** – dle § 61 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat jakákoliv fyzická osoba (nemusí být subjektem práva).
- Žádat lze o poskytnutí údajů o jakékoliv podnikající fyzické osobě, právnické osobě nebo orgánu veřejné moci.
- Ve výpisu se objeví všechny údaje jako v neveřejném výpisu (viz níže) kromě osobních údajů osob, které jsou ve vazbě na registr obyvatel.

Žádost o **výpis (neveřejný) údajů z registru osob** – dle § 61 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (podnikající fyzická osoba nebo statutární orgán právnické osoby), o kterém jsou údaje vedeny v registru osob.

Žádost o **záznam o využívání údajů v registru obyvatel** – dle § 14 zák. č.111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (fyzická osoba), o kterém jsou údaje vedeny v registru obyvatel.
- V žádosti subjekt uvede období, za které má být záznam poskytnut.
- Každá fyzická osoba, která má zřízenu datovou schránku, obdrží vždy za uplynulý kalendářní rok bezplatně *Záznam o využívání údajů v registru obyvatel* automaticky do datové schránky, v souladu s § 14 odst. 4 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.
- Informace, jak číst záznam o využívání údajů naleznete v praktické příručce: viz http://www.szrcr.cz/obcan-a-podnikatel

Žádost o **záznam o využívání údajů v registru osob** – dle § 14 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (podnikající fyzická osoba nebo statutární orgán právnické osoby), o kterém jsou údaje vedeny.
- V žádosti subjekt uvede období, za které má být záznam poskytnut.
- Každá podnikající fyzická a právnická osoba, která má zřízenu datovou schránku, obdrží vždy za uplynulý kalendářní rok bezplatně *Záznam o využívání údajů v registru osob* automaticky do datové schránky, v souladu s § 14 odst. 4 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Žádost o **změnu údajů při zjištění nesouladu v registru obyvatel** – dle § 14 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- O změnu údajů při zjištění nesouladu v registru obyvatel může žádat subjekt práva (fyzická osoba).
- Na základě žádosti dojde k podání **návrhu** na změnu referenčních údajů vedených o subjektu práva v registru obyvatel.
- Dojde-li ke změně referenčního údaje, obdrží fyzická osoba, která má zřízenu datovou schránku, bezplatně *Výpis referenčních údajů* automaticky do datové schránky, v souladu s § 14 odst. 5 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Žádost o **změnu údajů při zjištění nesouladu v registru osob** – dle § 14 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- O změnu údajů při zjištění nesouladu v registru osob může žádat subjekt práva (podnikající fyzická osoba nebo statutární orgán právnické osoby).
- Na základě žádosti podává žadatel **návrh** na změnu referenčních údajů vedených o osobě v registru osob.
- O změnu údajů při zjištění nesouladu v registru osob může žádat podnikající fyzická osoba nebo statutární orgán právnické osoby.
- Dojde-li ke změně referenčního údaje, obdrží každá podnikající fyzická nebo právnická osoba, která má zřízenu datovou schránku, bezplatně *Výpis referenčních údajů* automaticky do datové schránky, v souladu s § 14 odst. 5 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Žádost o **poskytnutí údajů z registru obyvatel třetí osobě** – dle § 58a zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Na základě žádosti poskytne subjekt práva (fyzická osoba) své údaje jiné fyzické nebo právnické osobě.
- Těmto je možné poskytnout všechny nebo vybrané údaje vedené k Vaší osobě v registru obyvatel.
- Orgánu veřejné moci není nutné poskytnout Vaše údaje tímto způsobem, neboť tento má povinnost si referenční údaje zjistit.

Žádost o **odvolání poskytnutí údajů z registru obyvatel třetí osobě** – dle § 58a zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Na základě žádosti přestanou být poskytovány Vaše údaje jiné fyzické nebo právnické osobě. Dojde k odvolání Vámi vybraných předchozích souhlasů s poskytnutím údajů třetí osobě učiněných žádostí výše.

Poplatky spojené s žádostmi o výpisy

- **Portál občana a portál veřejné správy** – podání žádostí datovou schránkou využitím formulářů uveřejněných na Portálu občana a portálu veřejné správy a vydání výpisů je **bezplatné**.
- **Czech POINT** – žádosti podané prostřednictvím kontaktního místa veřejné správy Czech POINT jsou zpoplatněny, avšak podání žádostí o změnu referenčních údajů a poskytnutí/odvolání poskytnutí referenčních údajů třetí osobě jsou **bezplatné**.

Povinnost využívat referenční rozhraní

Povinnost využívat referenční rozhraní pro uskutečňování takzvaných "vazeb" mezi jednotlivými informačními

systémy veřejné správy ukládá zákon o informačních systémech veřejné správy. Tedy obecně platí, že pro sdílení údajů, výměnu údajů a propojování jednotlivých informačních systémů veřejné správy různých správců, má být primárně využíváno právě referenční rozhraní. U informačních systémů stejného správce toto nemusí platit vždy, pokud se nevyužívá překlad agendových identifikátorů při komunikaci o subjektu práva vedené v rámci dvou nebo více agend.

Je nutné zdůraznit, že pouze využitím referenčního rozhraní je korektně prováděn překlad AIFO (AIFO jedné osoby v jedné agendě nesmí být poskytnuto jiné agendě). Pouze referenční rozhraní je napojeno na registr ORG a provádí překlad AIFO.

Možnost využívat referenční rozhraní

Mimo povinnost pro správce informačních systémů veřejné správy, je zde i možnost využití referenčního rozhraní, resp. služeb, které poskytuje, i pro jiné subjekty. Konkrétně jde o subjekty typu SPUÚ (Soukromoprávní uživatel údajů) dle zákona 111/2009 Sb., kteří pro využití služeb referenčního rozhraní potřebují zákonné zmocnění.

Užívání referenčního rozhraní při výměně údajů v rámci propojeného datového fondu

Výměna/sdílení údajů mezi jednotlivými informačními systémy veřejné správy se realizuje výhradně prostřednictvím referenčního rozhraní, a to konkrétně komponenty eGSB/ISSS. Jak se upřesňuje v části propojený datový fond, tak výměna údajů se realizuje vždy v rámci kontextu na subjekt práva.

Přístup ke službám referenčního rozhraní je na síťové úrovni možný pouze prostřednictvím Centrálního místa služeb (CMS), potažmo komunikační infrastruktury veřejné správy (KIVS), které můžeme nazvat privátní sítí pro výkon veřejné správy na území státu.

Správci agendových informačních systémů musejí realizovat napojení na referenční rozhraní, a to podle příslušných metodických dokumentů a provozních řádů:

- Provozní řád ISZR
- Podmínky pro připojení AIS k ISZR

Užívání referenčního rozhraní pro čerpání referenčních údajů

Správci agendových informačních systém se kromě provozních řádů řídí i dalšími postupy a to především legislativními. Současný stav (rok 2020) stále nutí k zákonnému zmocnění pro využívání referenčních údajů. V

Užívání referenčního rozhraní pro poskytování agendových údajů

Správci agendových informačních systémů poskytujících údaje z daných agend realizují napojení svých AISů na eGSB/ISSS v roli publikátora a kontrolu oprávnění k využívání údajů podle oprávnění v RPP. Pro výměnu údajů vybudují služby svého AIS tak, aby mohly být volány a zprostředkovány eGSB/ISSS.

Užívání referenčního rozhraní pro čerpání agendových údajů

Správci agendových informačních systémů využívajících údaje poskytované jinou agendou realizují volání služeb eGSB/ISSS (nemusí znát konkrétní AIS, požadují údaje od agendy), a to jen tehdy, pokud k tomu mají příslušné oprávnění zapsané u agendy poskytovatele v RPP.

Editoři referenčních údajů v základních registrech realizují napojení svých editorských agendových informačních systémů na ISZR službami vnějšího rozhraní podle příslušné dokumentace Správy základních registrů a v případech, kdy agendové informační systémy nejsou též samostatnými evidencemi dokumentů, pak napojení těchto systémů na eSSL v rámci vnitřních vazeb. Pro editaci údajů a vyřizování reklamací údajů v základních registrech nevyužívají jiné rozhraní než právě ISZR.

Pravidla pro Univerzální kontaktní místo veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci univerzálního kontaktního místa je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k univerzálním kontaktním místům popíše úřad do své informační koncepce.

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.

Pravidla pro Systém správy dokumentů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci správy dokumentů je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k systémům správy dokumentů popíše úřad do své informační koncepce.

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

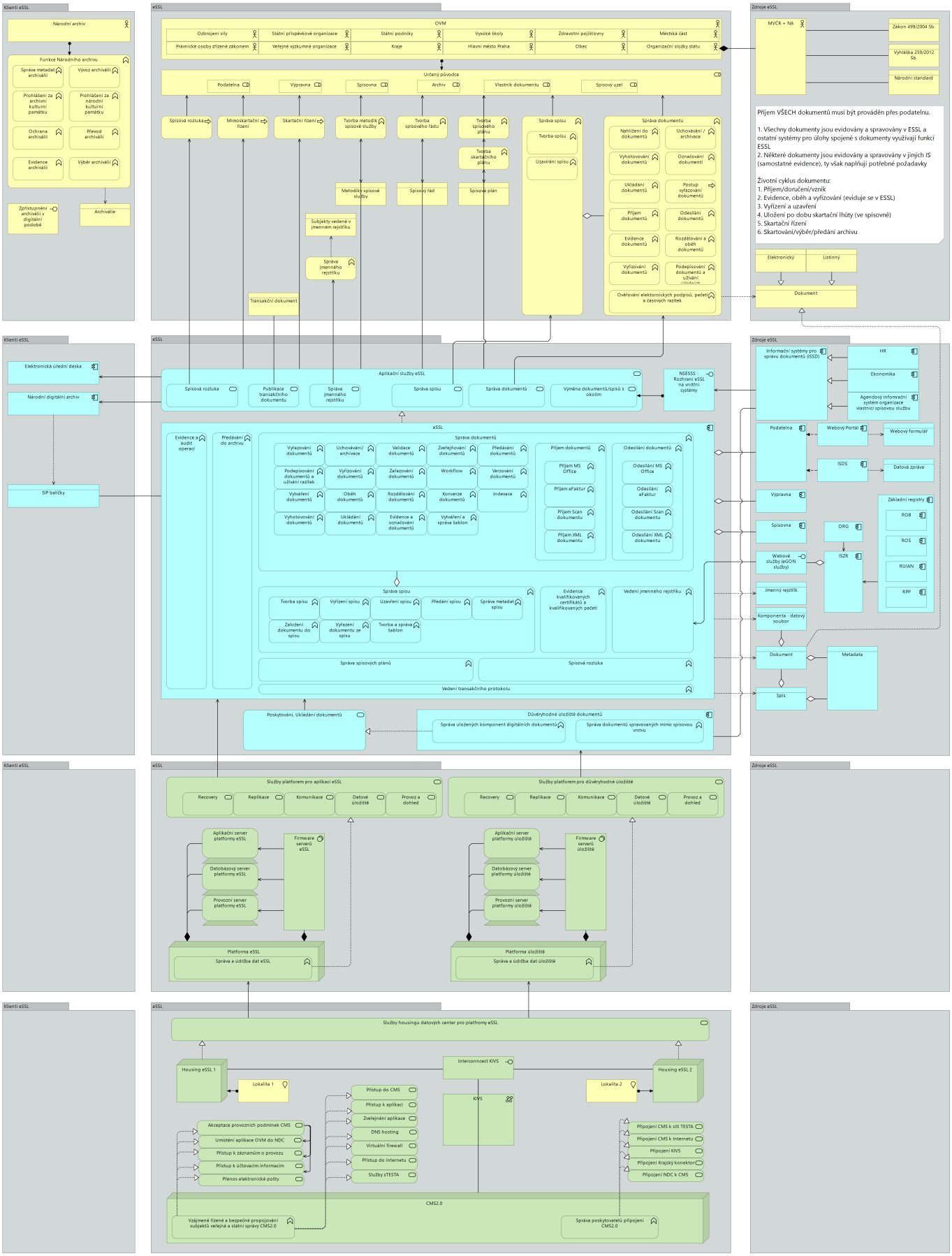
V rámci výkonu spisové služby jsou řídícími dokumenty zejména:

- 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[2)].

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.

Pravidla pro Systémy a služby spojené s právním řádem a legislativou

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci systémů a služeb spojených s právním řádem a legislativou je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k systémům a službám spojených s právním řádem a legislativou popíše úřad do své informační koncepce.

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.

Pravidla pro Elektronické úkony a doručování

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci elektronických úkonů a doručování je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k elektronickým úkonům a doručování popíše úřad do své informační koncepce.

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

Typ subjektu	Typ datové schránky v ISDS	Zřízena
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.

Pravidla pro Jednotný identitní prostor veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci jednotného identitního prostoru veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k jednotnému identitnímu prostoru popíše úřad do své informační koncepce.

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:

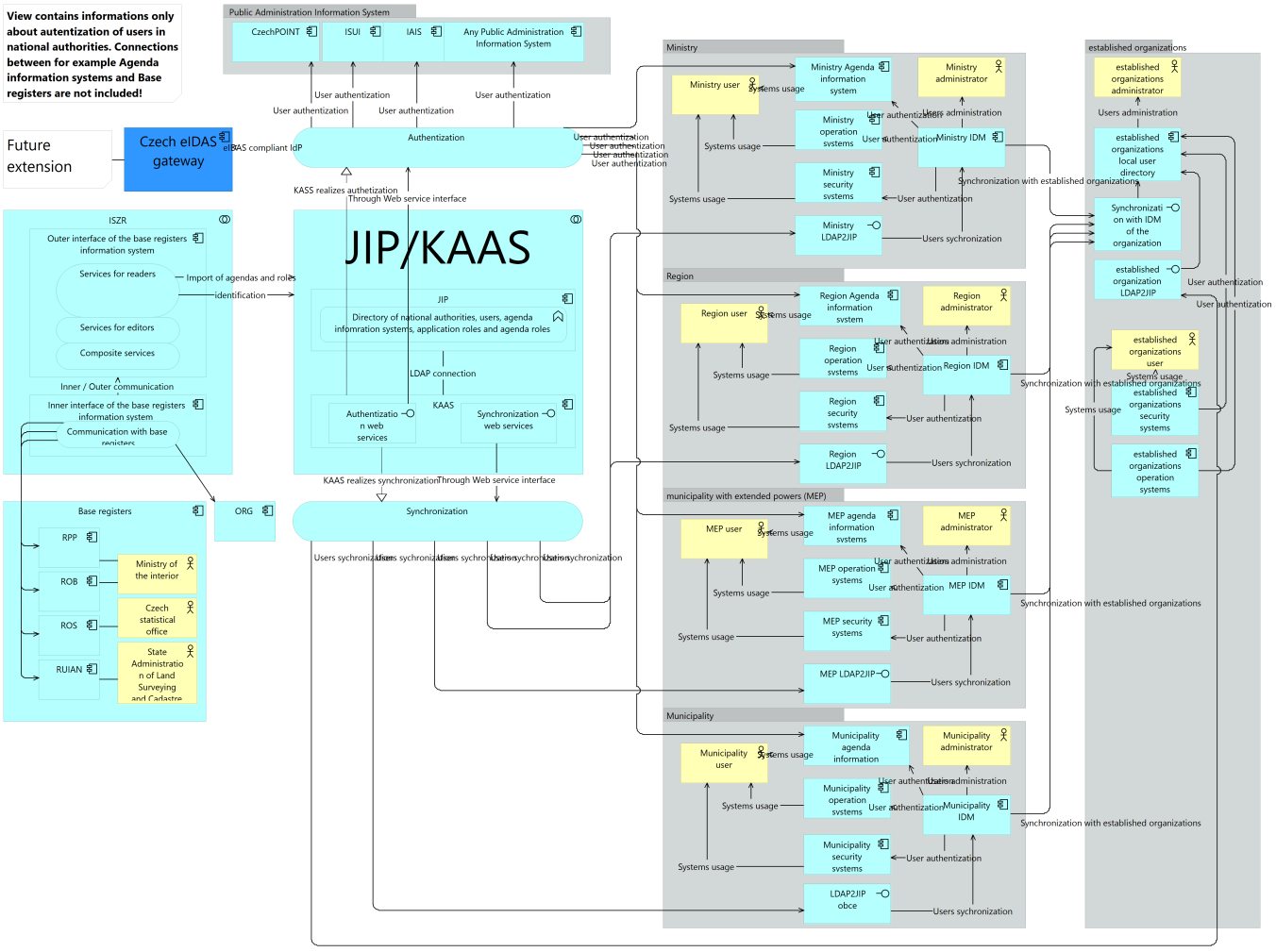
- Aktivní identita a identifikace - opravňuje zaměstnance k přístupu k informacím a informačním systémům, (+ k prostorám a zařízením) - zaměstnanec jako subjekt
- Pasivní identita a identifikace - jednoznačně označuje předmětného (většinou zodpovědného) zaměstnance v rámci centrálních nástrojů řízení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

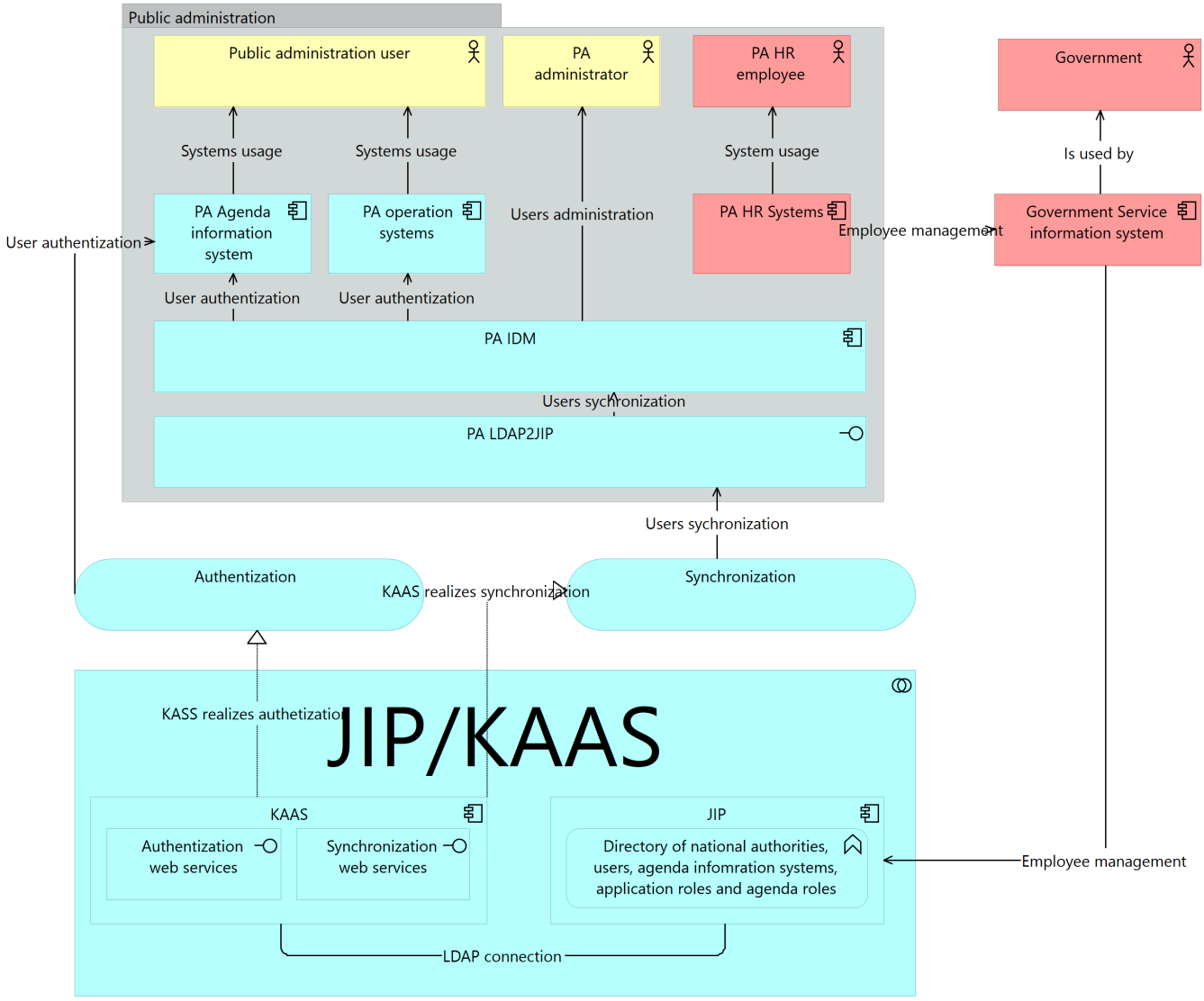
Stávající řešení JIP/KAAS nebylo určeno pro takto široké účely a koncepčně ani fyzicky nevyhovuje změněným nárokům. Jeho budoucí rozvoj musí vycházet z diskuse o reálných potřebách všech zainteresovaných. Předpokladem budoucího efektivního využívání jednotného identitního prostoru veřejné správy a naplnění 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
eIDAS compliant IdP
Public Administration Information System
CzechPOINT
ISUI
IAIS
Any Public Administration Information System
User authentization
Authentization
KASS realizes autetization
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
Ministry security systems
Ministry LDAP2JIP
User authentication
Users administration
Users sychronization
Synchronization with established organizations
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



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.

Pravidla pro Jednotné obslužné kanály a uživatelská rozhraní úředníků

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci jednotných obslužných kanálů a uživatelských rozhraní úředníků je popsán na samostatné stránce

zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k jednotným obslužným kanálům a UI úředníků popíše úřad do své informační koncepce.

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

Pravidla pro Sdílené služby INSPIRE

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených agendových IS v přenesené působnosti je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným službám INSPIRE popíše úřad do své informační koncepce.

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*

Pravidla pro Sdílené agendové IS v přenesené působnosti

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených agendových IS v

přenesené působnosti je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným agendovým IS pro přenesenou působnost popíše úřad do své informační koncepce.

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

Pravidla pro Sdílené agendové IS pro samostatnou působnost územních samospráv

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených agendových IS pro samostatnou působnost je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu sdíleným agendovým IS pro samostatnou působnost popíše úřad do své informační koncepce.

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.

Pravidla pro Sdílené provozní informační systémy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených provozních IS je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným provozním IS popíše úřad do své informační koncepce.

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

Pravidla pro Sdílené statistické, analytické a výkaznické systémy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci Sdílených statistických, analytických a výkaznických systémů je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným statistickým, analytickým a výkaznickým systémům popíše úřad do své informační koncepce.

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

Pravidla pro eGovernment cloud

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci eGovernment Cloudu je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k eGovernment Cloudu popíše úřad do své informační koncepce.

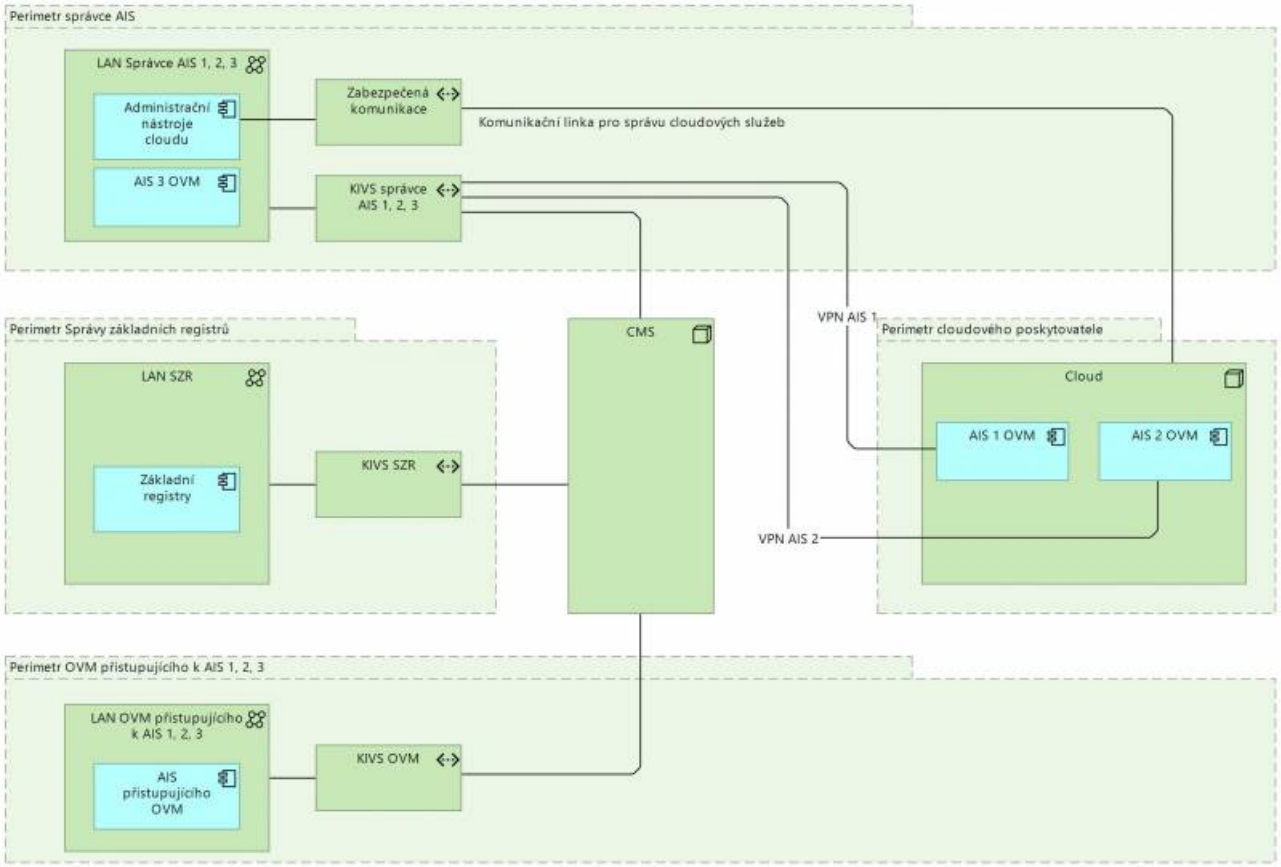
Přístup správců ISVS k eGC

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.

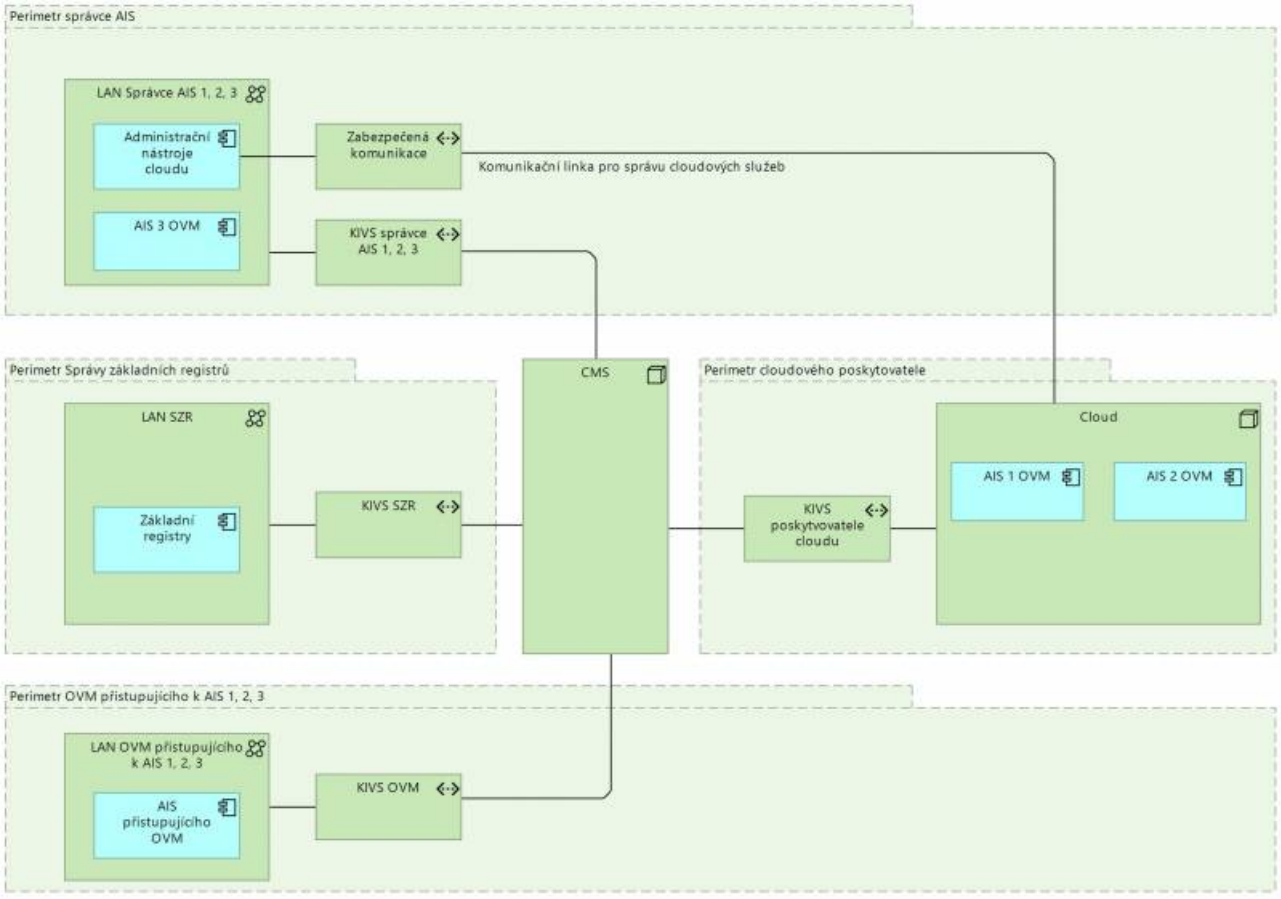
Provozování AIS OVM v eGC v souvislosti s komunikací pomocí CMS/KIVS

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.

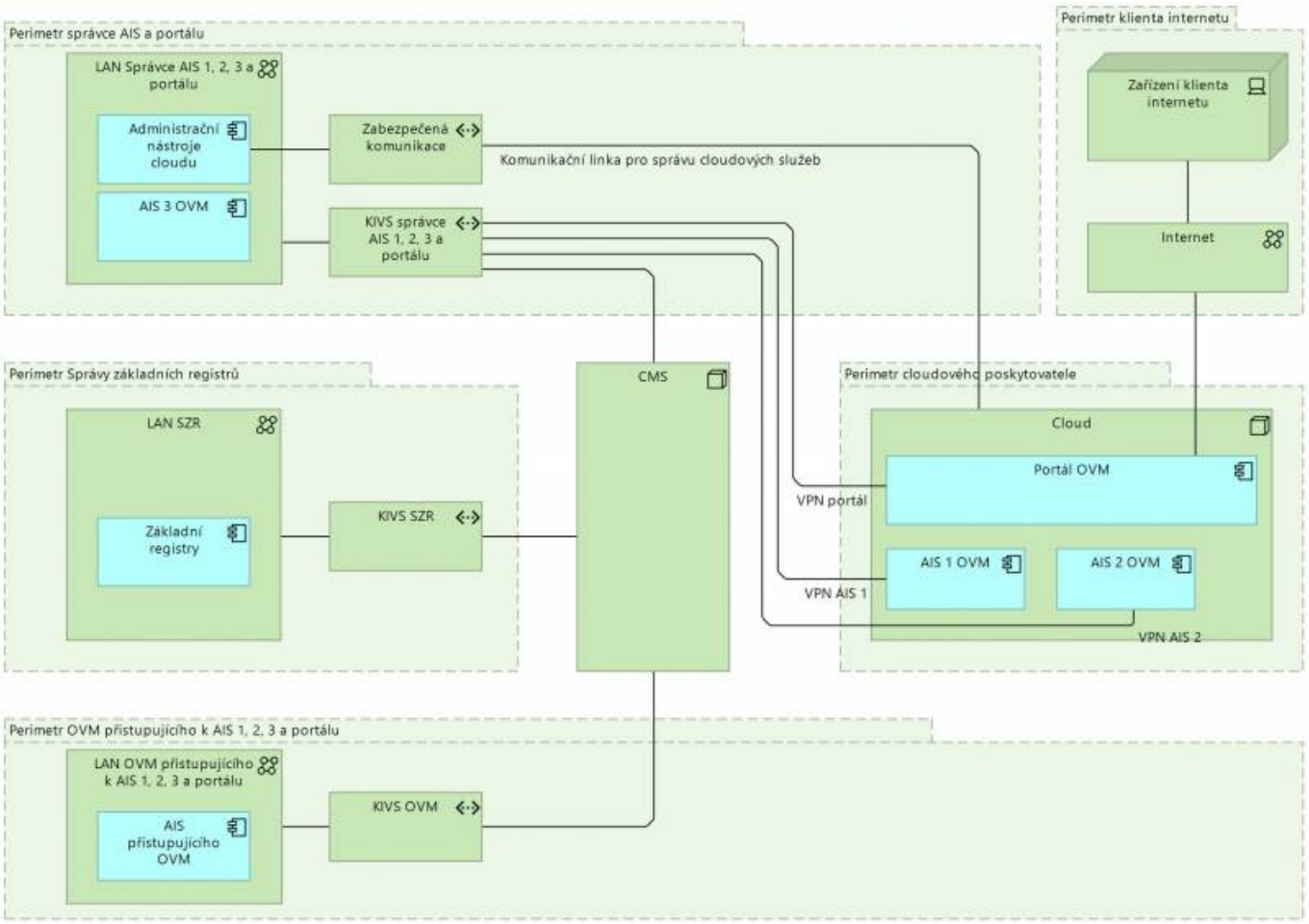
Portál je v případě provozu na vlastní infrastruktuře publikován výhradně prostřednictvím CMS službou CMS2-02 Zveřejnění aplikace a to do:

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

Pravidla pro Národní datová centra

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci národních datových center je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k národním datovým centrům popíše úřad do své informační koncepce.

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

Pravidla pro komunikační infrastrukturu veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci komunikační infrastruktury veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke komunikační infrastruktuře veřejné správy popíše úřad do své informační koncepce.

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)[3)] 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)

Přehled prostředků s jejich úrovní záruky seznam_poskytovatelu_identity_identity_provideridp

2)

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

3)

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