Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

<title>NAP: Celky podle vrstev a využití</title>

Základní principy (byznysová vrstva)

Systémy a služby spojené s právním řádem a legislativou

systemy_sluzby_spojene_pravnim_radem_legislativou

Agendový model veřejné správy

Popis Agendového modelu veřejné správy

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

Agendový model výkonu veřejné správy

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

Agendy veřejné správy

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

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

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

1. Ohlašovatelem je OVM, který je gestorem dané právní úpravy a má tedy povinnost agendu a údaje o ní zapsat do Registru práv a povinností. Součástí ohlášení jsou:
2. Referenční údaje o agendě
    - název agendy a její číselný kód, které jsou součástí číselníku agend,
    - čísla a názvy právních předpisů a označení jejich ustanovení, na jejichž základě orgán veřejné moci vykonává svoji působnost, nebo na jehož základě je soukromoprávní uživatel údajů oprávněn k využívání údajů ze základních registrů nebo agendových informačních systémů,
    - výčet a popis činností, které mají být vykonávány v agendě,
    - výčty činnostních rolí,
    - výčet a popis úkonů orgánů veřejné moci vykonávaných v rámci agendy na žádost subjektu, který není orgánem veřejné moci, identifikátor úkonu, vymezení subjektu, který může podat žádost, a

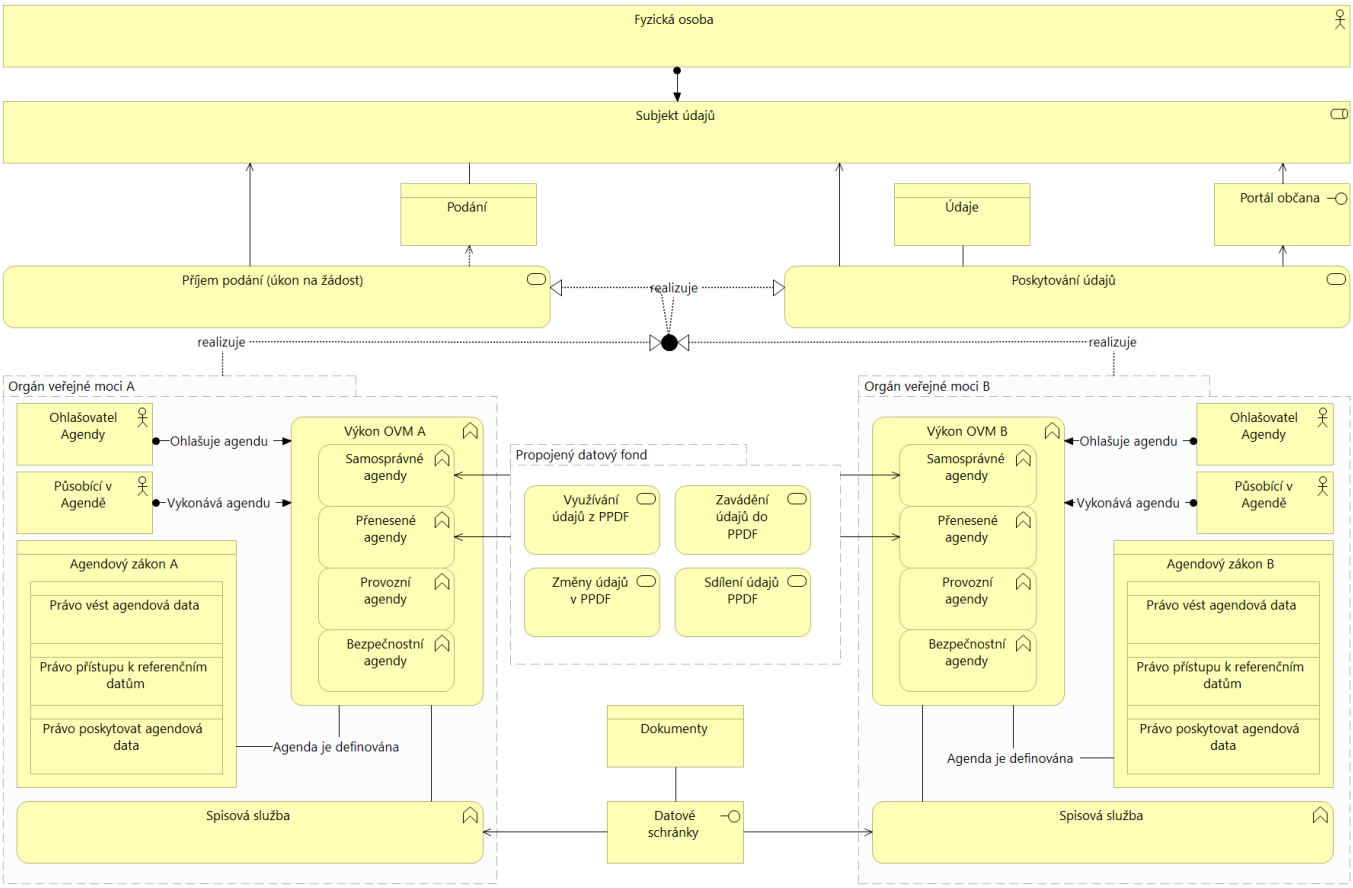
forma úkonu,
    - výčet orgánů veřejné moci a soukromoprávních uživatelů údajů, kteří agendu vykonávají, nebo jejich kategorie,
    - název ohlašovatele agendy a jeho identifikátor orgánu veřejné moci,
    - výčet orgánů veřejné moci, které byly pro výkon agendy zaregistrovány, a jejich identifikátor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

Klíčové role OVS v agendovém modelu

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

Klíčové role OVS v agendovém modelu veřejné správy	Role	Popis/význam hlavní činnosti
Ohlašovatel agendy	OVM, který je zodpovědný za legislativní rámec agendy, a tedy určuje i základní parametry jejího výkonu	Je gestorem právních předpisů; koordinuje výkon agendy; metodicky řídí výkon agendy; ohlašuje agendu v RPP a její podrobnosti; stanovuje působnost OVM; poskytuje buď centralizovaný AIS, nebo podmínky a standardy pro decentralizované řešení; ohlašuje a spravuje údaje v RPP, včetně údajů v rejstřících OVM a SPUU; v případě centralizovaného AIS poskytuje údaje přes referenční rozhraní ISVS
Orgán veřejné moci působící v agendě	OVM, který působí v dané agendě. To znamená, že vykonává fakticky nějakou činnost v rámci dané agendy a k tomu využívá buď centrálně poskytnutý AIS, nebo svůj vlastní	Přihlašuje se k působnosti; vykonává jemu svěřené činnosti úředníky v jejich činnostních rolích; zapisuje do RPP údaje o své působnosti; využívá centralizovaný AIS nebo spravuje vlastní; eviduje a spravuje údaje v agendě; vykonává případně funkce editora údajů
Soukromoprávní uživatel údajů	Subjekt, který má na základě zákona oprávnění k přístupu k údajům v základních registrech či AISech a přistupuje k nim prostřednictvím AIS spravovaného k tomu určeným OVM	Využívá údaje podle oprávnění
Správce centralizovaného AIS pro výkon agendy	OVM, který na základě zákona spravuje centralizovaný AIS a poskytuje ho OVM působícím v agendě	Spravuje centralizovaný AIS; zpřístupňuje AIS uživatelům působících OVM; realizuje využívání referenčních údajů ze základních registrů do centralizovaného AIS; poskytuje podporu uživatelům; řeší integrační vazby AIS na další systémy
Správce vlastního AIS, pokud není k dispozici centralizovaný AIS	Jednotlivé OVM, které pro podporu agendy využívají svůj vlastní agendový IS, protože není k dispozici sdílené centralizované řešení	Spravuje svůj vlastní AIS; zapisuje údaje o svém AIS do RPP; řeší vazby na základní registry; řeší vazby na další ISVS; řeší vazby na další svoje informační systémy; spravuje a udržuje datový fond ve svém AISu
Orgán veřejné moci spravující AIS pro přístup soukromoprávních uživatelů	OVM, který na základě zákona vytváří a provozuje AIS, jehož prostřednictvím mohou soukromoprávní uživatelé přistupovat k údajům ze základních registrů či jiných AISů	Spravuje AIS pro SPÚ; zpřístupňuje funkce AISu soukromoprávním uživatelům; realizuje dohled nad oprávněním k využívání údajů; poskytuje soukromoprávním uživatelům údaje; zajišťuje realizaci reklamací údajů od SPÚ k editorům údajů

Pohled na ohlašovatele a vykonavatele agendy



Pravidla Agendového modelu veřejné správy

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.

Propojený datový fond

Úplné elektronické podání

Elektronické úkony a doručování

Univerzální kontaktní místo veřejné správy

Systém správy dokumentů

Přístupnost informací

Popis Přístupnosti informací

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

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

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

Obecně o přístupnosti

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

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

Pravidla Přístupnosti informací

Legislativní rámec pro přístupnost

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

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

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

1. OZP musí mít možnost využívat všechny služby veřejné správy jako kdokoliv jiný
2. OZP musí mít možnost plnohodnotně využívat elektronické služby stát i elektronické služby subjektů veřejného sektoru
3. Existuje zde obecná absolutní povinnost přístupnosti výsledků všech veřejných zakázek či zakázek podle legislativy k VZ, pokud jsou jejich výsledky určeny pro jakékoliv užívání fyzickými osobami, to se pochopitelně vztahuje i obecně na veškeré ICT zakázky.
4. Subjekty veřejného sektoru musejí mít svoje informace přístupné a to zejména na internetových stránkách a ve svých aplikacích

5. Přístupnost se vztahuje i na veškeré informační systémy pro zaměstnance, protože ani zaměstnanec s OZP nesmí být diskriminován tím, že není schopen pracovat se svým pracovním systémem

Standardy a metodiky

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

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

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

Architektonická řešení

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

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

Elektronická fakturace

Sdílené služby (aplikační a integrační vrstva)

Základní registry a referenční údaje

Integrace informačních systémů

Portály veřejné správy a soukromoprávních uživatelů údajů

Elektronická identifikace pro klienty veřejné správy

Jednotný identitní prostor veřejné správy

Jednotné obslužné kanály a uživatelská rozhraní úředníků

Veřejný datový fond

Infrastruktura (infrastrukturní a technologická vrstva)

Komunikační infrastruktura veřejné správy

eGovernment Cloud

Popis eGovernment cloudu

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

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

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

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

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

- definici minimálních standardů pro poskytování IaaS a PaaS služeb pro státní a komerční část eGC,

- sjednocení provozního prostředí informačních systémů a aplikací provozovaných ve státní části eGC na několik vybraných platforem,
- zajištění potřebné bezpečnosti, spolehlivosti, škálovatelnosti a jednotnosti provozu ICT služeb.

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

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

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

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

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

Oblast cloud computingu je od 1. 8. 2020 regulována příslušnými ustanoveními zákona č. 365/2000 Sb., o informačních systémech veřejné správy, kde v Hlavě VI zákona je zaveden mechanismus zápisu poptávek a nabídek cloud computingu do katalogu cloud computingu a zavedena povinnost orgánů veřejné správy využívat pouze takový cloud computing, který byl na základě splnění podmínek uvedených v zákoně zapsán Digitální a informační agenturou do katalogu cloud computingu.

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

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

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

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

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

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

Katalog cloud computingu

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

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

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

Pravidla eGovernment cloudu

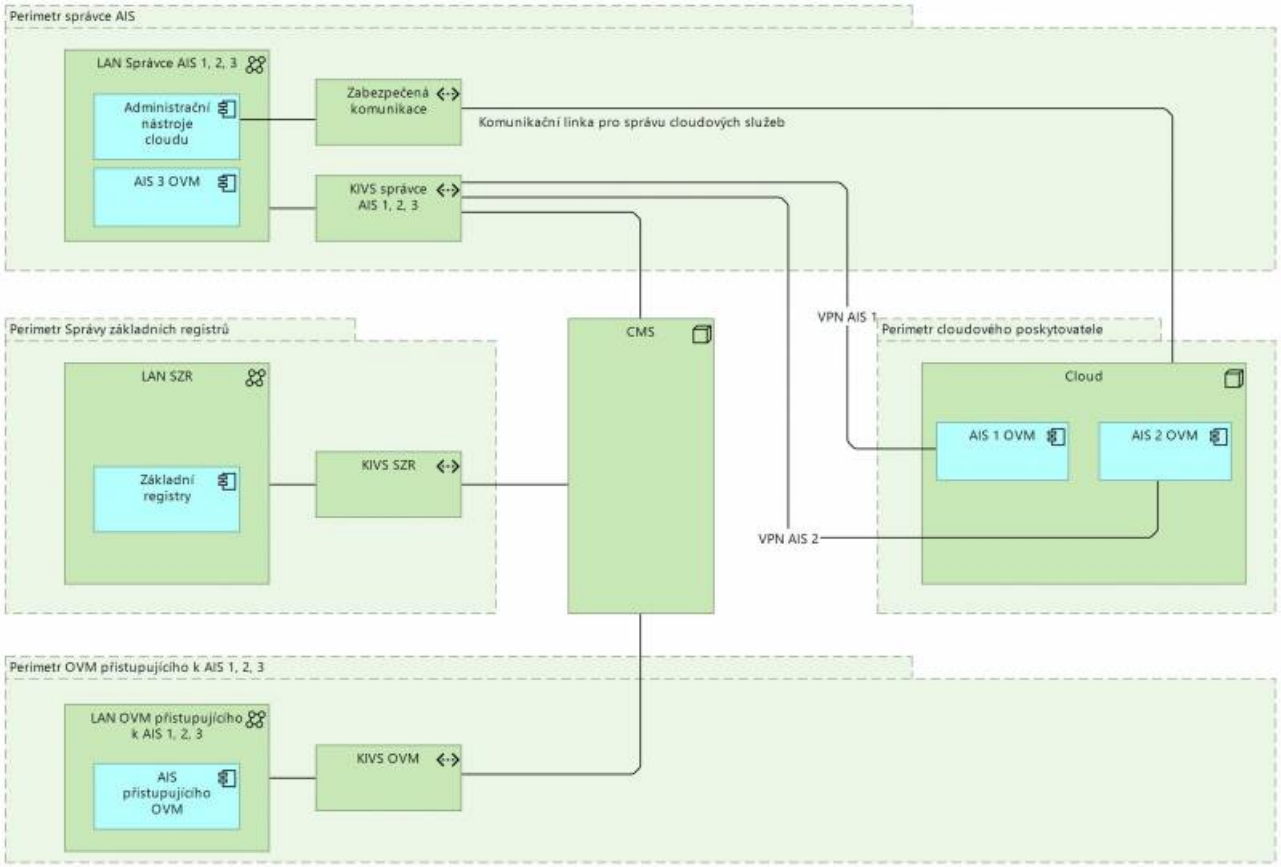
Přístup správců ISVS k eGC

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

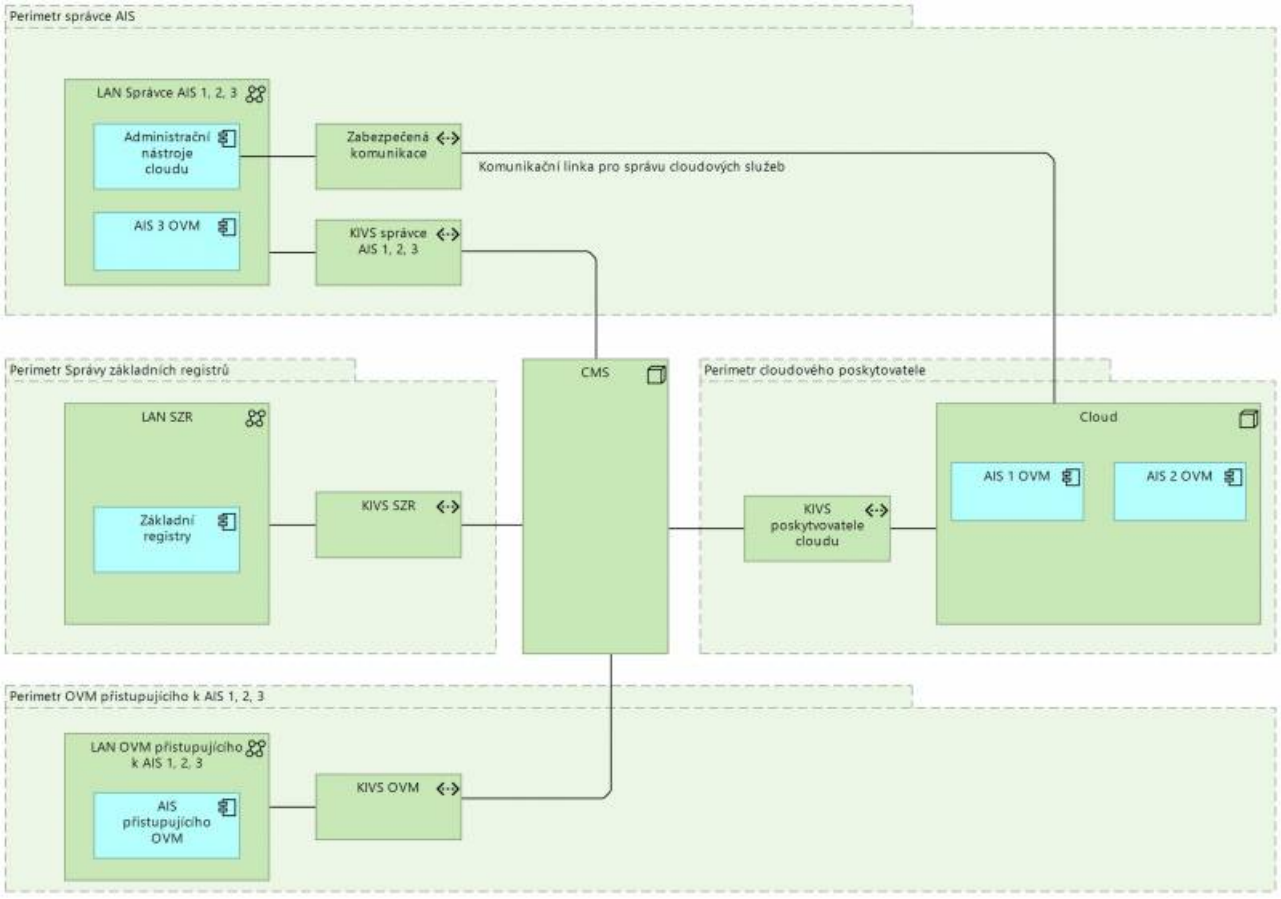
Provozování AIS OVM v eGC v souvislosti s komunikací pomocí CMS/KIVS

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

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



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



Publikování portálu OVM

Publikování portálu OVM je specifický případ publikování AIS OVM, kdy se v rámci provozu portálu v eGC

umožňuje, aby byly služby portálu dostupné pro klienty, kteří nejsou OVM, prostřednictvím internetu přímo od poskytovatele eGC.

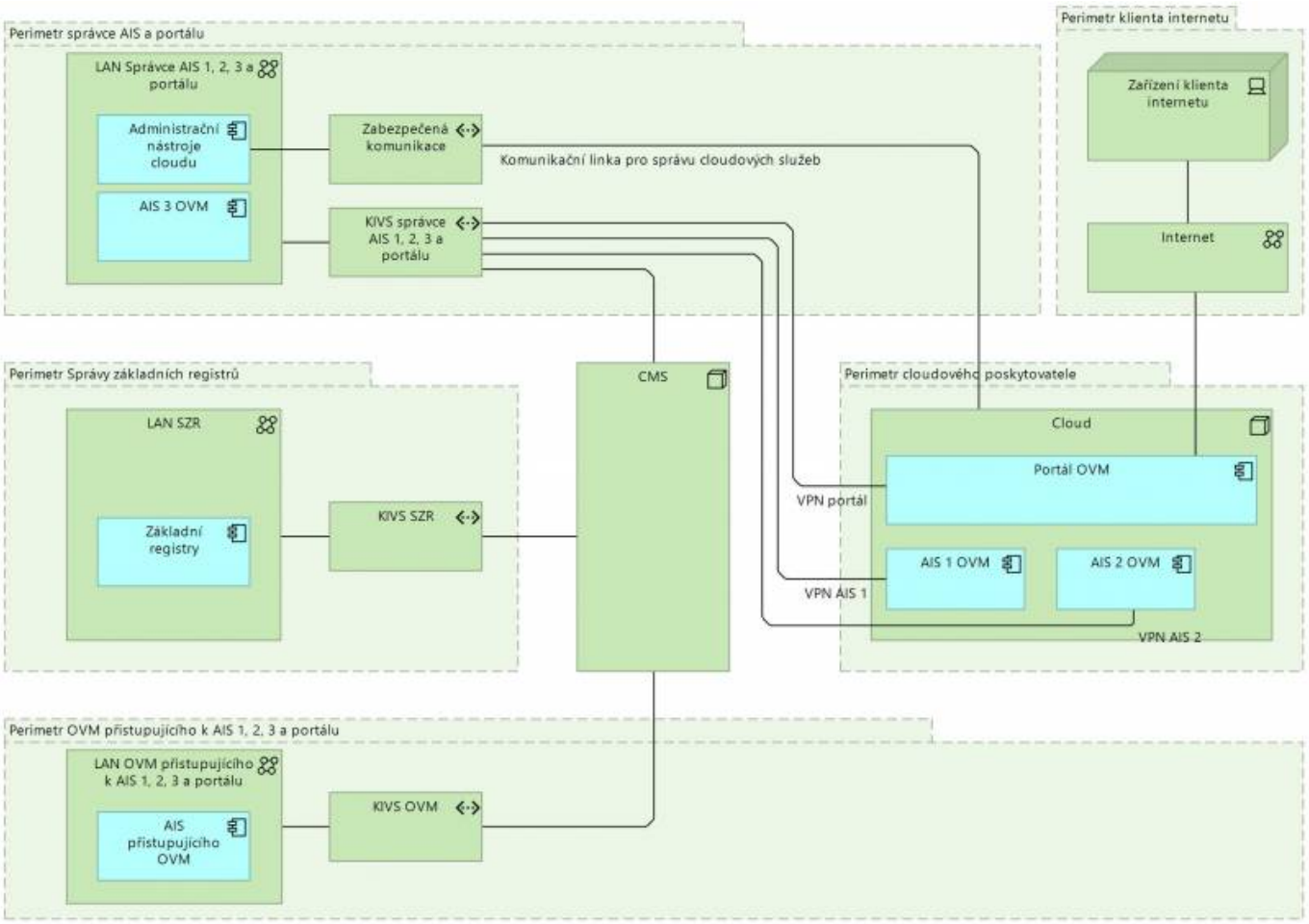
Portál je v případě provozu na vlastní infrastruktuře publikován výhradně prostřednictvím CMS službou CMS2-02 Zveřejnění aplikace a to do:

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

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

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

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



Povinnosti komerčních poskytovatelů služeb eGC

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

Národní datová centra

Popis Národních datových center

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

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

- Služby bezpečného prostředí výpočetního centra
- Služby virtuální výpočetní kapacity
- Služby databázových serverů
- Služby datového zálohování
- Služby vystavení publikovaných služeb v DMZ1 a DMZ2 v CMS KIVS

Pravidla Národních datových center

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