DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

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.

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. U moderně navržených ISVS pro provoz v cloudu lze provést dekomponování, což vede ke zvýšení efektivnosti využívání prostředků při vývoji a provozování těchto informačních systémů. Dekompozice zároveň umožňuje hybridní provoz s využitím služeb cloud computingu různé bezpečnostní úrovně (dále jen „BÚ“).

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.

Co je a co není cloud dle zákona

Upřesnění definice služeb třídy SaaS aneb jaká aplikační řešení, která orgány veřejné správy využívají/poptávají, lze považovat za cloud computing ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy?

Aplikační řešení, která jsou cloud computing třídy SaaS ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy , musí splňovat současně tyto podmínky:

1. slouží více správcům ISVS (orgány veřejné správy (dále jen „OVS“) v roli tenantů), kteří jej využívají k provozu vlastních ISVS, nebo jiným zákazníkům (mimo OVS) a zároveň
2. jsou provozovány na sdílené platformě cloud computingu třídy IaaS, příp. PaaS

Podmínka 2) může být splněna jedním ze dvou způsobů:

- SaaS je provozován na službách IaaS/PaaS samostatně zapsaných do katalogu CC tímto nebo jiným poskytovatelem CC,
- SaaS je provozován na službách IaaS/PaaS téhož poskytovatele CC, který nabízí SaaS, ale služby IaaS/PaaS využívá pouze pro provoz daného SaaS. V tomto případě služby IaaS/PaaS se do katalogu CC samostatně nezapisují. Existence a účinnost bezpečnostních opatření, která jsou zajišťována jednotlivými vrstvami provozní infrastruktury a která jsou vyžadována pro službu SaaS v dané bezpečnostní úrovni, se ověřují na základě „Podkladů pro ověření SaaS“, které ve své žádosti o zápis služby do katalogu CC uvedl poskytovatel SaaS.

Tyto služby typu SaaS mohou být využívány pouze v souladu s Hlavou VI ZoISVS a mj. musí být celý „stack“ IaaS/PaaS/SaaS zapsán v Katalogu CC. Zároveň musí být zapsáni všichni poskytovatelé CC (ať už materiální poskytovatelé, distributoři nebo koncoví poskytovatelé).

Aplikační řešení, která nejsou CC ve smyslu ZoISVS (a nepovažujeme je za CC třídy SaaS), jsou taková, která

- slouží více správcům ISVS (OVS), ale jsou pro každého správce provozovány na nesdílené (dedikované) výpočetní infrastruktuře;
- slouží pouze pro jednoho správce ISVS (OVS), přičemž může jít o aplikaci umožňující vzdálený přístup přes Internet nebo přes vnitřní síť CMS/KIVS pro mnoho externích uživatelů (např. aplikace pro podání přihlášky na střední školu, nebo aplikace využívané jednotlivými uživateli z řad OVS/OVM, avšak s centrální správou uživatelských účtů a báze dat ze strany toho jednoho správce ISVS), i když je provozována na platformě CC třídy IaaS, příp. PaaS (tato platforma však podléhá povinnosti zápisu do katalogu CC).

Upozorňujeme, že je nutné vždy uvažovat o ISVS v rozsahu ZoISVS, tzn. ve vymezení uvedeném v § 1 ZoISVS (zejména s ohledem na výjimky v odst. (2), (3) a (4) § 1 ZoISVS).

Katalog cloud computingu

Pravidla eGovernment cloudu

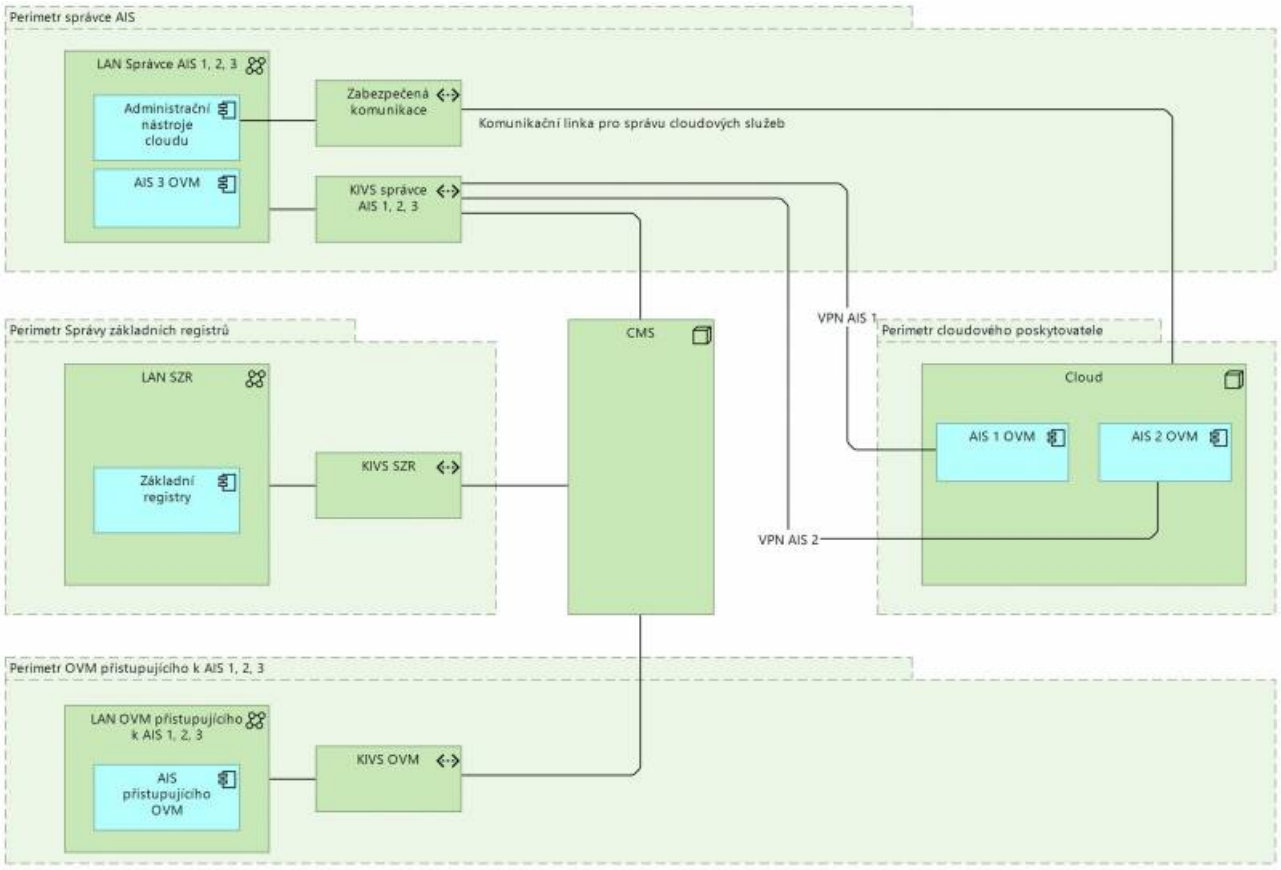
Přístup správců ISVS k eGC

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.

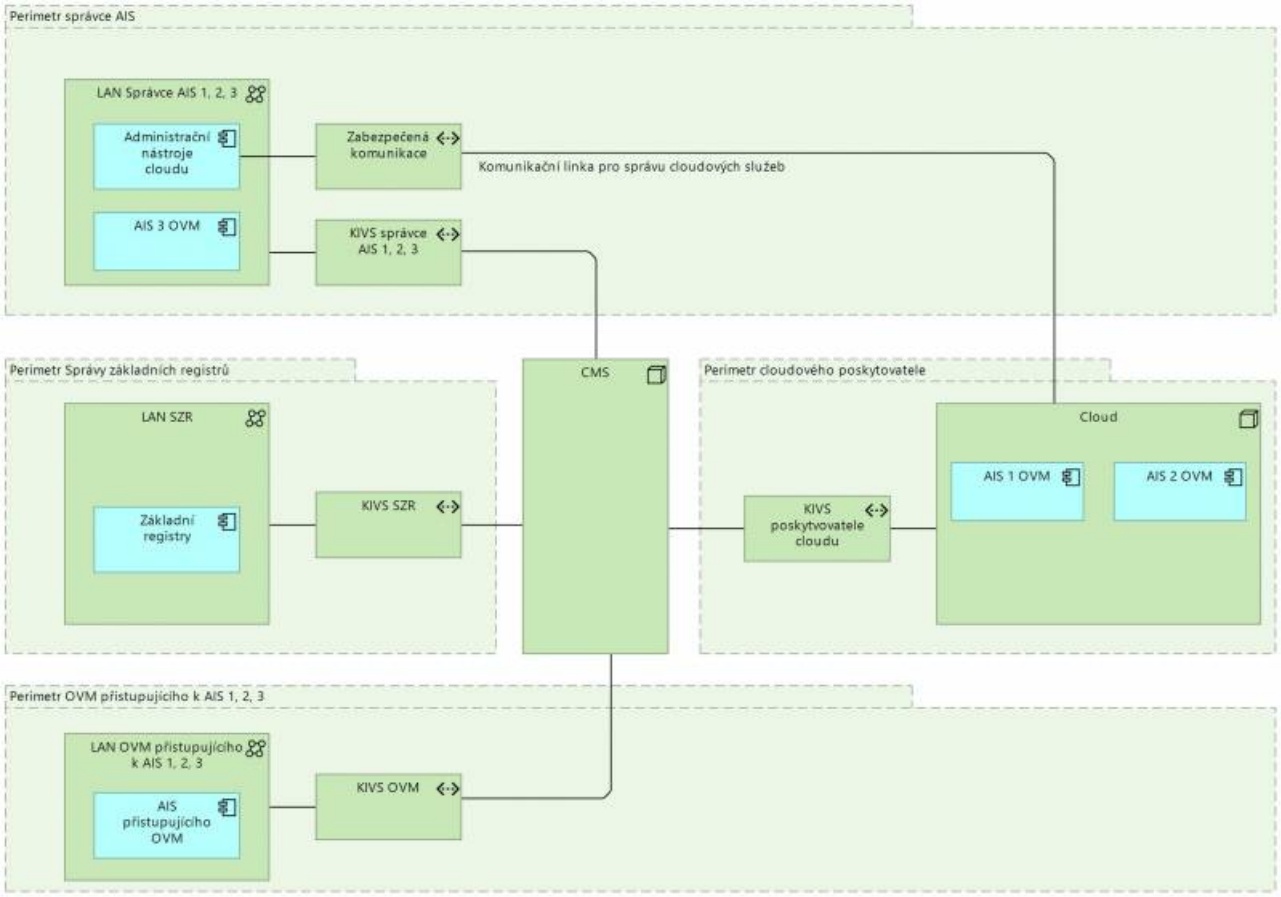
Provozování AIS OVM v eGC v souvislosti s komunikací pomocí CMS/KIVS

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.

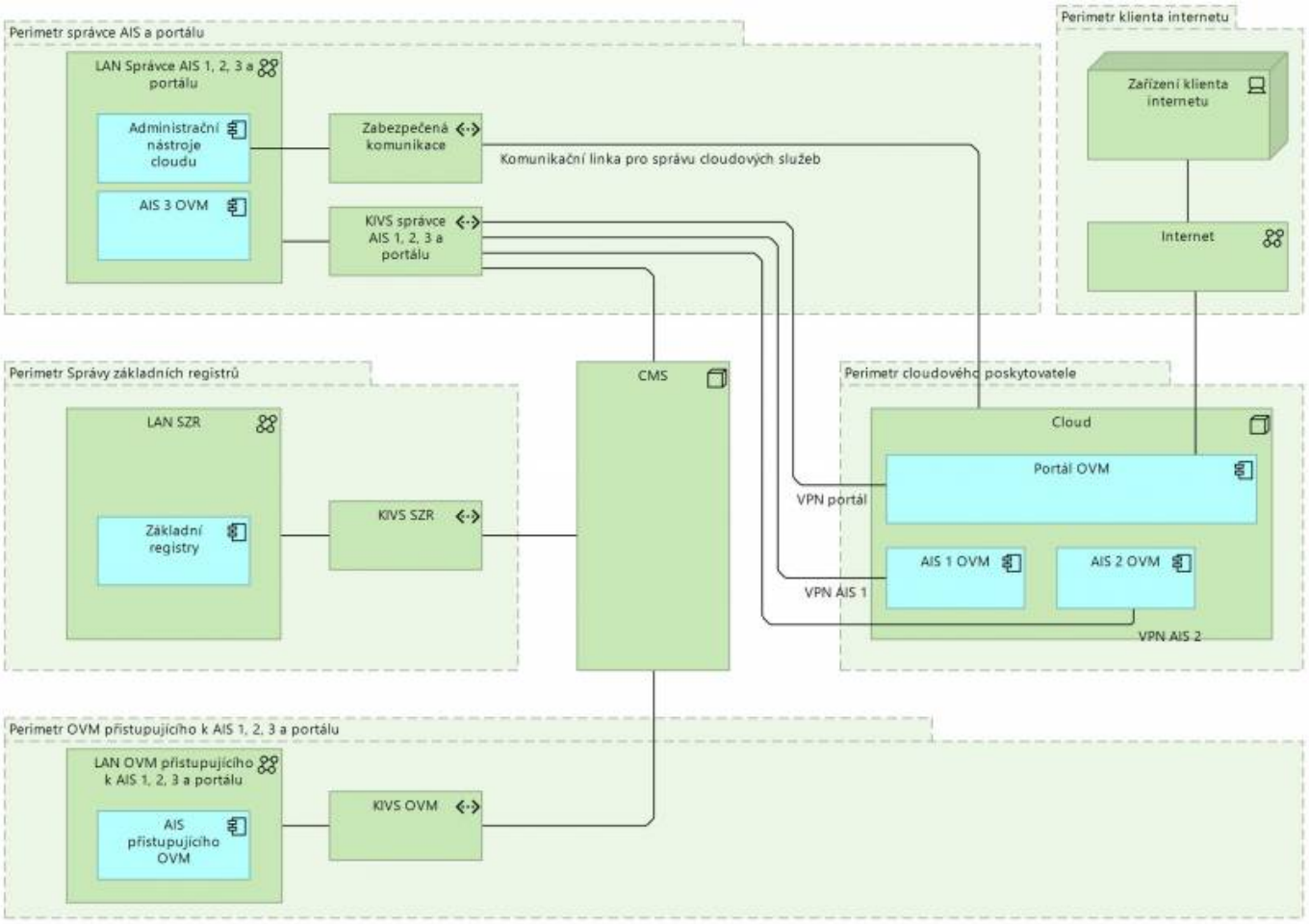
Portál je v případě provozu na vlastní infrastruktuře publikován výhradně prostřednictvím CMS službou CMS2-02 Zveřejnění aplikace a to do:

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

Určování nástrojů osobní produktivity jako ISVS

Orgány veřejné správy se musí při poskytování interaktivních nástrojů osobní produktivity úředníka využívající cloud computing rozhodnout, zda jde o informační systém veřejné správy (ISVS) nebo jeho část ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS), a mohou tak podléhat regulaci cloud computingu podle Hlavy VI tohoto zákona.

Dle § 2 odst. 1 písm. b) ZoISVS je: „informačním systémem veřejné správy funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy nebo plnění jiných funkcí státu anebo dalších veřejnoprávních korporací …“

Informační činností dle § 2 odst. 1 písm. a) se myslí: „získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na nosičích. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů veřejné správy prostřednictvím technických a programových prostředků“.

Z definice ISVS vyplývá, že cílevědomá, avšak ne-systematická, informační činnost pro účely výkonu veřejné správy nemusí spadat pod rozsah definice. Scénáře interaktivního využívání nástrojů s podporou cloud

computingu (jako jsou např. interaktivní nástroje umělé inteligence, volně dostupné on-line mapy nebo jazykové překladače) nesplní podmínku systematické informační činnosti výkonu veřejné správy, pokud využívání určitého konkrétního nástroje k určitému informačnímu účelu není interně v rámci orgánu veřejné správy ustanoveno jako závazné. Jestliže se tedy úředník sám rozhoduje ad-hoc, který a jestli vůbec nějaký on-line nástroj pro daný účel využije, nenaplní se tento atribut definice ISVS.

Naopak se lze domnívat, že systematické využití např. tabulkového kalkulátoru (např. MS Excel) v malé obci pro evidenci poplatků za psy nebo za hrobová místa naplní znaky „cílevědomé a systematické informační činnosti pro účely výkonu veřejné správy“, a tento informační systém by tedy měl být označen a spravován jako ISVS. Za rozlišující kritérium výkladu pojmu „systematická informační činnost pro účely výkonu veřejné správy“ tedy považujeme jakýkoli interní předpis OVS, který zavazuje úředníky využívat vždy určitý konkrétní nástroj (informační systém nebo jeho část) pro zabezpečení určitého účelu výkonu veřejné správy.

Ač tedy nástroje osobní produktivity jednoznačně spadají do definice informační činnosti, je potřeba vždy vážit hledisko systematičnosti pro účel výkonu veřejné správy.

Dále ještě zohledníme metodické vodítko Co je a co není ISVS. V kapitole „Pomůcka pro určování ISVS“ jsou uvedeny dvě pomocné otázky k rozhodování OVS, zda se v konkrétním případě nějakého informačního systému má jednat o ISVS:

- Bylo by nefunkčností informačního systému bezprostředně narušeno nebo ohroženo plnění povinnosti vyplývající z kompetencí daného orgánu veřejné správy?
- Jsou v informačním systému uloženy údaje o vykonávané správní činnosti nebo údaje pro podporu výkonu u této činnosti?

Pokud jsou odpovědi na tyto otázky ANO, s největší pravděpodobností se v případě posuzovaného informačního systému jedná o ISVS.

Toto vodítko může potvrdit výše vyslovený názor, že tabulkový kalkulátor instalovaný byť jen na jednom notebooku v rámci malé obce, který je však jediným zavedeným nástrojem pro správu určitých agend (viz výše), splní obě podmínky a měl by být tedy spravován jako ISVS.

Naopak, ad-hoc využití interaktivních nástrojů dle shora uvedených příkladů (interaktivní nástroje umělé inteligence, volně dostupné on-line mapy, on-line jazykové překladače apod.) zpravidla nedá odpověď “ano” na tyto dvě otázky metodického vodítka, a v takovém případě se nekvalifikuje jako ISVS.

eGC, Cloud, Funkční celek, gcloud, Government cloud, eGovernment cloud