MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Metodika pro práci s katalogem cloud computingu a katalogem služeb cloud computingu

verze 1.3, 1. 6. 2021

Tento dokument **popisuje postupy a pravidla pro práci s Katalogem cloud computingu a katalogem služeb eGovernment cloudu** (dále také „služby eGC“ nebo „cloudové služby“). Katalog cloud computingu a jeho účel je vymezen ZoISVS v platném znění (dle ustanovení ZoISVS účinných od 1. 8. 2020). Datové položky katalogu cloud computingu definuje vyhláška o údajích vedených v katalogu cloud computingu (vyhláška 433/2020 ze dne 30. 10. 2020 - tzv. „Katalogová vyhláška cloud computingu “).

Ustanovení této metodiky nemají dopad na povinnosti vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a navazujících vyhlášek.

Řídící orgán eGC bude průběžně aktualizovat tuto metodiku tak, aby respektovala, platná znění zákonů, vývoj na trhu s cloudovými technologiemi, vývoj požadavků státu na bezpečnost provozu ISVS a také zkušenosti s provozem eGovernment Cloudu.

Poznámka: *S ohledem na skutečnost, že v PS PČR je v legislativním procesu novela ZoISVS, bude tento stav metodiky platit pouze do doby, kdy vstoupí novela ZoISVS v účinnost.*

Na jaké informační systémy veřejné správy a na jaké služby cloud computingu se metodika nevztahuje

- ZoISVS a tím pádem i tato metodika se nevztahují na ISVS spravované:
  - pro potřeby nakládání s utajovanými informacemi,
  - zpravodajskými službami,
  - Národním bezpečnostním úřadem,
  - Národním úřadem pro kybernetickou a informační bezpečnost.
- ZoISVS a tím pádem i tato metodika se s výjimkou vazeb na jiné informační systémy veřejné správy nevztahují na informační systémy veřejné správy spravované:
  - pro potřeby zajišťování obrany státu,
  - pro potřeby podpory krizového řízení,
  - orgány činnými v trestním řízení pro potřeby trestního řízení; zákon se vztahuje na evidenci Rejstříku trestů,
  - bezpečnostními sbory,
  - ozbrojenými silami České republiky nebo Vojenskou policií,
  - Českou národní bankou,
  - Finančním analytickým úřadem pro potřeby boje proti legalizaci výnosů z trestné činnosti nebo provádění mezinárodních sankcí za účelem udržování mezinárodního míru a bezpečnosti, ochrany základních lidských práv a boje proti terorismu,
  - Ministerstvem vnitra pro potřeby provádění bezpečnostního řízení a vedení evidencí podle zákona upravujícího ochranu utajovaných informací a bezpečnostní způsobilost,
  - Ministerstvem vnitra, Ministerstvem financí nebo Ministerstvem spravedlnosti pro potřeby zpracování osobních údajů příslušníků bezpečnostních sborů.

- ZoISVS a tím pádem i tato metodika se nevztahují na provozní informační systémy (tj. systémy zajišťující pouze informační činnosti pro vnitřní provoz příslušného orgánu) **s výjimkou státními orgány spravovaných**:
  - informační systém pro řízení a rozvoj lidských zdrojů a odměňování,
  - elektronický systém spisové služby,
  - informační systém pro vedení účetnictví nebo řízení finančních zdrojů,
  - systém elektronické pošty.

  Provozními systémy, na které se ZoISVS a tím pádem ani tato metodika nevztahují, jsou také:
  - systémy sloužící k zajištění osobní produktivity, vzdálené obrazové, hlasové a textové komunikace,
  - systémy pro zajištění monitorovacích služeb a služeb reportingu nutných pro rozhodování správce nebo provozovatele informačních systémů veřejné správy při správě a provozu více informačních systémů veřejné správy.
- ZoISVS a tím pádem i tato metodika se nevztahují na vazby provozních informačních systémů; to neplatí, jedná-li se o vazby provozních informačních systémů na jiné informační systémy veřejné správy, které nejsou provozními informačními systémy.

Správci, na jejichž ISVS se ZoISVS ani metodika nevztahují, mohou využívat služby zapsané v katalogu cloud computingu dobrovolně. Výhodou v tomto případě je, že poskytovatelé a služby zapsané v katalogu cloud computingu jsou prověřené, tj. že vyhovují základním bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací.

Kdo a kdy metodiku využívá

Metodiku využívají:

- Řídicí orgán eGC (ŘOeGC) Ministerstva vnitra (MV) – odbor kybernetické bezpečnosti a koordinace ICT (OKB) při:
  - zápisu poptávek do katalogu cloud computingu,
  - certifikaci služeb nabídnutých jednotlivými poskytovateli eGC, tj. při posouzení, zda nabídka služeb poskytovatele splňuje kritéria certifikace (tzv. ex-ante kontrola),
  - zápisu nabídky poskytovatele do katalogu cloud computingu,
- Centrální zadavatel (MV) při:
  - zavedení DNS při vypsání veřejné zakázky na služby eGC,
  - při realizaci veřejné zakázky na dodání služeb eGC,
- Poskytovatelé cloud computingu a služeb eGC při:
  - podání nabídky cloud computingu a služeb eGC pro účel certifikace do katalogu cloud computingu,
  - podání nabídky služeb eGC v rámci veřejné zakázky,
- Orgán veřejné správy (OVS) při:
  - návrhu rozšíření poptávky cloud computingu na služby eGC,
  - realizaci veřejné zakázky na dodání služeb eGC.

1. Používané pojmy

Služby eGC jsou služby cloud computingu využívané orgány veřejné správy pro provoz informačních systémů veřejné správy (ISVS).

Parametrem služby eGC je popisný údaj, který upřesňuje objemové, výkonové, bezpečnostní, cenové a další charakteristiky služby eGC.

Konkrétní služba eGC označuje službu poptávanou v rámci veřejné zakázky, nabízenou v rámci veřejné zakázky a využívanou pro provoz konkrétního ISVS. Konkrétní služba má vždy uvedeny hodnoty všech parametrů. U nabízené služby v rámci veřejné zakázky a u využívaných služeb je vždy uvedena jejich cena.

Typ služby eGC označuje množinu konkrétních služeb eGC, které mají stejný účel a stejné druhy parametrů, které službu charakterizují. Konkrétní hodnoty parametrů se u typu služby neuvádějí.

Např. typ služby „Server bez operačního systému a bez hypervizoru" označuje celou řadu konkrétních virtuálních serverů. Tyto servery se dají charakterizovat těmito parametry: Typ vCPU, Frekvence, RAM, Server storage, Síťové připojení, Instance Sdílená/Dedikovaná/Rezervovaná, s/bez správy poskytovatelem.

Katalog služeb eGC je uspořádanou podmnožinou údajů sestavených z údajů vedených v katalogu cloud computingu. Slouží pro informační systém cloud computingu a jeho procesy (například zápis poptávky, zápis nabídky atd.). Katalog služeb eGC definuje služby eGC, jejich hierarchickou strukturu a parametry těchto služeb. Vzhledem k použitým soutěžním a nákupním mechanismům eGC je katalog služeb eGC tvořen sadou souvisejících katalogů s jednotnou hierarchickou strukturou. Jednotná hierarchická struktura popisu služeb eGC je tato:

- třída služeb – IaaS (infrastruktura jako služba), PaaS (platforma jako služba) a SaaS (softwarová aplikace jako služba). Specifickou třídou jsou konzultační a integrační služby pro využívání služeb Cloud Computingu,
- oblast služeb – skupina obdobných typů služeb v rámci dané třídy služeb, které plní obdobnou základní funkcionalitu cloud computingu *(např. „databáze jako služba" v třídě PaaS)*,
- typ služby – skupina obdobných konkrétních služeb, které mají stejný účel, obdobnou základní funkcionalitu a stejné základní parametry (*např. „relační databáze" v rámci oblasti databáze jako služba),*
- konkrétní služba – konkrétní poptávaná, nabízená nebo využívaná služba.

Bezpečnostní certifikací cloud computingu (v rámci ex-ante kontroly) je potvrzení, že cloud computing (služba cloud computingu) má vlastnosti vyžadované pro zařazení do příslušné bezpečnostní úrovně pro využívání cloud computingu orgány veřejné správy. Bezpečnostní úrovně jsou 1-„Nízká", 2-„Střední", 3-„Vysoká" a 4-„Kritická". Liší se bezpečnostními kritérii, která jsou aplikovaná na provoz ISVS příslušné bezpečnostní úrovně. Kritéria pro bezpečnostní certifikaci a vlastní ex-ante kontrolu specifikuje Ministerstvo vnitra ve spolupráci s NÚKIB.

Poskytovatel cloud computingu (dále jen poskytovatel) je subjekt, který žádá o zápis do katalogu cloud computingu. Poskytovatel má dvě možné formy:

1) **Prodejce** – ten, kdo vstupuje do smluvního vztahu s OVS (zákazníkem). Tento subjekt bude předmětem ex-ante kontroly v určených bodech.
2) **Materiální dodavatel** – ten, kdo přebírá zákaznická data a data generovaná službami do svojí správy (tzn. bezpečnostní politiky), tj. ten, kdo skutečně cloud computingovou službu poskytuje. Tento subjekt bude předmětem ex-ante kontroly v určených bodech.

Další dodavatelé cloud computingu jsou další subjekty zapojené do dodavatelského řetězce eGC služby, které ale nemusejí žádat o zápis do katalogu cloud computingu. Mají dvě možné formy:

1) **Systematický zpracovatel –** ten kdo zpracovává data poskytnutá ze strany OVS poskytovateli cloud computingu a data generovaná službami cloud computingu, ale není materiálním dodavatelem. Tento subjekt se řídí bezpečnostní politikou materiálního dodavatele. Jde o

subdodavatele materiálního dodavatele, přičemž vztah mezi materiálním dodavatelem a systematickým zpracovatelem musí být v případě, že služba cloud omputingu využívaná ISVS zpracovává osobní data, ošetřen dle čl. 28 GDPR. Seznam systematických zpracovatelů uvede materiální dodavatel ve své nabídce služeb.

2) **Běžný dodavatel –** ten kdo nijak nezpracovává data poskytnutá ze strany OVS poskytovateli cloud computingu a data generovaná službami cloud computingu

Informační systém cloud computingu je od 1. 8. 2020 do doby zahájení účinnosti připravované novely ZoISVS realizován přes rozhraní webových stránek MV:

(Web eGC - https://www.mvcr.cz/clanek/egovernment-cloud.aspx)

2. Katalog cloud computingu a katalog služeb eGC

2.1 Struktura katalogu cloud computingu a katalogu služeb eGC

Katalog služeb eGC je uspořádanou podmnožinou údajů sestavených z údajů vedených v katalogu cloud computingu. Katalog je součástí informačního systému cloud computingu a obsahuje údaje o poptávkách cloud computingu, údaje o nabídkách cloud computingu a údaje o cloud computngu využívaném orgány veřejné správy.

1. **K1: Katalog poptávek cloud computingu** na služby eGC – obsahuje poptávku veřejné správy na určité typy služeb eGC, které veřejná správa hodlá v daném období využívat pro provoz svých ISVS. Tento katalog neuvádí konkrétní ISVS, ve kterých se budou poptávané služby využívat. Jednotlivé poptávky v katalogu se liší:
   a. třídou, oblastí a/nebo typem poptávaných služeb,
   b. obdobím, ve kterém je poptávka platná.

   Ve stejné době může být platných více poptávek (např. poptávka na IaaS a poptávka na SaaS).

   Katalog poptávek současně obsahuje seznam bezpečnostních a dalších kritérií, které při ex-ante kontrole musí splnit poskytovatel, aby mohl dodávat služby eGC. Seznam kritérií ex-ante kontroly určuje MV ve spolupráci s NÚKIB.
2. **K2: Katalog nabídek** cloud computingu na služby eGC – obsahuje nabídky jednotlivých poskytovatelů služeb eGC, které úspěšně prošly ex-ante kontrolou.

   Nabídka obsahuje názvy a základní parametry konkrétních služeb poskytovatele, které jsou zařazeny pod dané (poptávané) typy služeb, spolu s uvedením bezpečnostní úrovně služeb. Součástí nabídky je i výčet opatření, kterými poskytovatel splňuje bezpečnostní kritéria používaná při ex-ante kontrole.

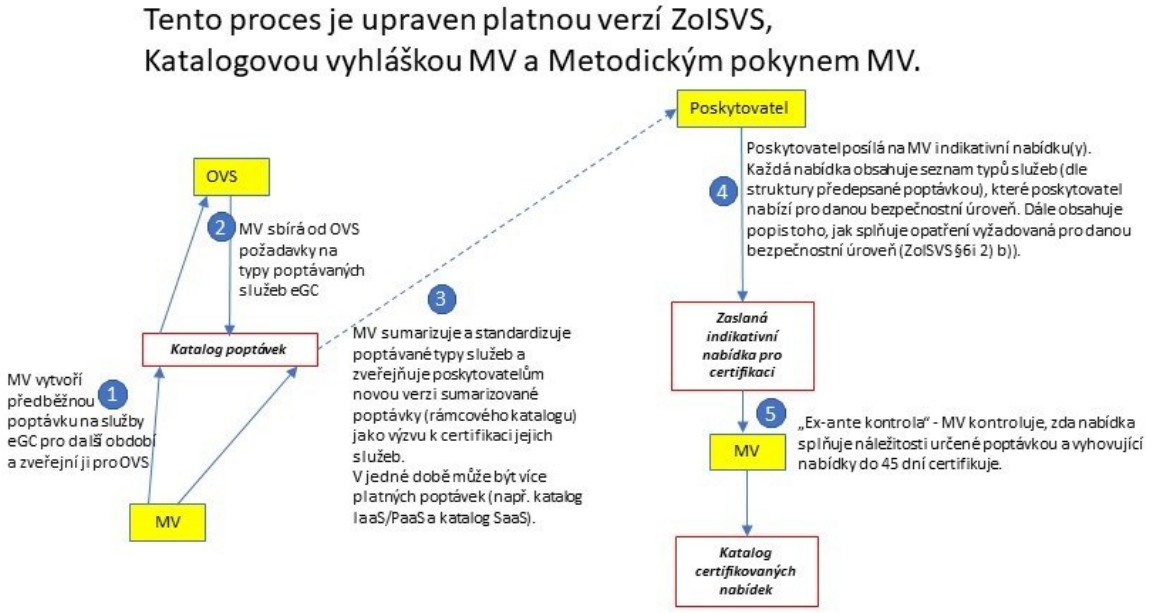
   Nabídka poskytovatele vždy reaguje na určitou poptávku uveřejněnou v katalogu K1, přičemž může obsahovat i nabídku dalších služeb, jestliže poskytovatel nemohl svoje služby cloud computingu zařadit pod standardizované typy služeb.
3. **K3: Katalog využívaných služeb** cloud computingu orgány veřejné správy obsahuje informace o všech službách cloud computingu, které v dané době veřejná správa využívá, a to včetně odkazu na příslušnou obchodní smlouvu do registru smluv. Jedenkrát za rok OVS do tohoto katalogu ukládá i náklady uplynulého roku dle jednotlivých typů služeb cloud computingu (sumarizováno z faktur)[1].

[1] Údaje slouží jednak při ex-post kontrole k ověření, zda OVS využívá pouze certifikované služby uvedené v katalogu služeb eGC a jednak pro analýzu nákladové efektivnosti cloudových služeb

3. Procesy pokryté metodikou

Schémata procesů a aktivity procesů vycházejí z platné verze ZoISVS (účinné od 1. 8. 2020) a z platné verze ZZVZ a ZKB. Schémata jsou v souladu Katalogovou vyhláškou cloud computingu a současně vychází z návrhu Cloudové vyhlášky NUKIB, která po novelizaci ZoISVS stanoví obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, včetně bezpečnostních úrovní pro využívání cloud computingu orgány veřejné moci a určí vstupní kritéria cloud computingu pro nabídky cloud computingu.

V rámci této metodiky jsou popsány procesy „vypsání poptávky“ cloud computingu ze strany OVS, „Vytvoření nabídky poskytovatele“, Ex-ante kontrola nabídky poskytovatele cloud computingu a jeho služeb a „Zápis využívané služby cloud computingu do katalogu cloud computingu“



3.1 Procesy „Vypsání poptávky

3.1.1 Aktivity procesu „Vypsání poptávky“

1) Na základě analýzy trhu cloudových služeb a na základě analýzy potřeb cloudových služeb ve veřejné správě MV vytvoří a na webu MV zveřejní **předběžnou poptávku na služby eGC pro další období** nabídek poskytovatelů a vyzve OVS k doplnění poptávky. Vzor předběžné poptávky služeb je uveden v **Příloze 1**. Při analýze trhu MV analyzuje také došlé nabídky poskytovatelů v minulém období včetně služeb uvedených v typu služby „Ostatní“ a na základě této analýzy vytváří nové standardizované typy služeb pro další období.
2) **Orgány veřejné správy zasílají na MV svoje poptávky na služby eGC včetně těch, které rozšiřují poptávané typy služeb.** Každá poptávaná služba musí být popsána datovými položkami, které určuje **K1: Katalog poptávek** (viz katalogová vyhláška)**.** Poptávka se zasílá dle vzoru uvedeném v **Příloze 1**. Poptávku OVS posílá do datové schránky MV (*předmět zprávy „Poptávka na služby eGC“*), a to do dne určeného na webu MV.
3) **MV analyzuje došlé poptávky od OVS** (viz ZoISVS §6m (3)) a vytváří sumarizovanou poptávku na služby eGC, přičemž služby popisuje dle hierarchie:

   a) třída služeb
   b) oblasti služeb
   c) typy služeb

d) parametry jednotlivých typů služeb (cílem je optimálně vymezit množinu popisných parametrů každého typu služby, která nebude diskriminovat žádného poskytovatele).

4) **MV zveřejní sumarizovanou poptávku na služby eGC**.

Sumarizovanou poptávku MV zveřejňuje na webu eGC s tím, že poptávku identifikuje těmito údaji:

1. údaje identifikující katalog/poptávku
   - druh katalogu („poptávka pro certifikaci“)
   - název poptávky (např: „služby typu IaaS a PaaS verze 1“)
   - účel („požadavek správce katalogů – MV“, nebo název zamýšleného řešení pro dané OVS)
   - doba platnosti poptávky cloud computingu,
   - plánovaná doba využívání poptávaného cloud computingu.

   Údaj doba platnosti poptávky, specifikuje období, ve kterém mohou poskytovatelé poslat nabídku a požádat o certifikaci nabízených služeb (a zápisu do nabídky do Katalogu eGC).

   Údaj plánovaná doba využívání, specifikuje období, ve kterém veřejná správa plánuje využívat poptávané služby.

2. další údaje poptávky:
   - seznam poptávaných typů služeb - viz **Příloha 1**,
   - formulář pro vyplnění nabídky služeb poskytovatelem – viz **Příloha 2,**
   - požadovaná bezpečnostní kritéria, které musí splnit poskytovatel, chce-li nabídnout své služby v určité bezpečnostní úrovni. Požadovaná kritéria jsou uvedena v **Příloze 3**.

     Součástí bezpečnostních kritérií je ověření, že poskytovatel akceptuje, že ve svých smlouvách na dodávku služeb eGC bude respektovat „Minimální smluvní podmínky“. Tyto minimální smluvní podmínky jsou další součástí poptávky – viz **Příloha 4**.

3.2 Procesy „Vytvoření nabídky a kontrola nabídky

3.2.1 Aktivity procesu „Vytvoření nabídky poskytovatele“

V době platnosti poptávky, mohou **poskytovatelé zasílat své nabídky** s cílem, aby MV provedlo jejich ex-ante kontrolu a ty nabídky, které splňují požadovaná kritéria, zapsalo do katalogu cloud computingu.

Ve své nabídce poskytovatel zasílá Ministerstvu vnitra vyplněné formuláře, jejichž vzory jsou uvedeny v **Příloze 2** a v **Příloze 3**.

1) Příloha 2 obsahuje specifikaci nabízených služeb a Příloha 3 uvádí, jak poskytovatel splňuje bezpečnostní kritéria pro služby uvedené v Příloze 2.
2) **Příloha 2** obsahuje samostatné listy pro:
   - služby IaaS/ PaaS
   - služby SaaS
   - konzultační služby související s výběrem a využíváním služeb eGovernment Cloudu.

Na jednom listu pro služby IaaS/PaaS a na jednom listu pro služby SaaS poskytovatel uvádí množinu služeb, které jsou zajištěny stejnou množinou bezpečnostních opatření doložených stejnou množinou certifikátů, auditů a čestných prohlášení.

V příloze 2 poskytovatel současně uvádí nejvyšší bezpečnostní úroveň (1, 2 nebo 3), pro kterou jsou tyto služby nabízené a pro kterou je lze využívat. Tzn. uvede-li poskytovatel bezpečnostní úroveň 3, mohou zákazníci využívat služby uvedené v Příloze 2 i pro bezpečnostní úroveň 1 a 2.

Upozornění: *Nabízí-li poskytovatel stejný typ služby ve více bezpečnostních úrovních, ale s odlišnou množinou bezpečnostních opatření, pak tuto službu/služby uvádí vždy na samostatném listu Přílohy č. 2 a k tomuto listu přikládá samostatně vyplněnou Přílohu č. 3 s doklady vyžadovanými pro danou*

bezpečnostní úroveň. Tuto Přílohu 3 je třeba jasně identifikovat, aby bylo zřejmé, ke kterému listu Přílohy 2 se vztahuje.

V Příloze 2 může poskytovatel řádek **"Ostatní služby"** uvést vícekrát - separátně pro každý další (dříve neuvedený) typ služby. Tento řádek/řádky poskytovatel využívá k nabídce dalších služeb dané třídy služeb, které nebyly v poptávce explicitně uvedeny. Důvodem této možnosti je fakt, že služby cloud computingu se rychle rozvíjejí a MV nemusí ve své poptávce uvést některé typy služeb, které se na trhu objevily jako nové a které by OVS při provozu svých ISVS mohlo z důvodu nutných technologických vazeb nebo s technologickou výhodou využít.

***Upozornění:** S ohledem na skutečnost, že konzultační a integrační služby nepatří do služeb cloud computingu, nebudou zapisovány do katalogu cloud computingu, ale budou uveřejňovány na portálu MV v sekci pro eGovernment Cloud. Předpokládá se, že tyto služby budou využívat OVS při migraci svých informačních systémů do cloudu.*

3) Splnění požadovaných bezpečnostních kritérií služeb eGC dokladuje poskytovatel vyplněním **Přílohy 3**.

Příloha 3 se vyplňuje pouze pro služby typu IaaS, PaaS a SaaS, nevyplňuje se pro konzultační služby.

***Upozornění:** Konkrétní způsob pokrytí daného bezpečnostního opatření se pro konkrétní služby eGC, deklarované na jednom listu IaaS/PaaS nebo SaaS, mohou lišit vzhledem k vlastnostem konkrétní služby. Tak např. konkrétně použité šifrovací algoritmy a délky jejich klíčů se u služeb deklarovaných na jednom listu mohou lišit v rámci souladu s „Minimálními požadavky na šifrovací algoritmy NÚKIB…". V takovém případě musí být v rámci daného ex-ante kritéria přiložen přehled, který detailně popisuje odlišnosti splnění daného kritéria pro konkrétní služby eGC, a to nejlépe výčtem nebo tabulkou.*

Poskytovatelem, který musí doložit splnění požadovaných bezpečnostních kritérií, je jednak **„prodejce"** (reseller nebo integrátor při nepřímém obchodním modelu) a jednak každý „**materiální dodavatel"**.

Za všechny své materiální dodavatele v dodavatelském řetězci formulář vyplňuje prodejce.

Za materiálního dodavatele může splnění kritérií dokládat společnost, která je k tomu zmocněna materiálním dodavatelem.

V případě, že je splnění některého z kritérií doloženo čestným prohlášením, musí z něho být patrné, kdo a kdy jej činí, a co se jím dokladuje.

Pokud splnění některého z kritérií spadá do rozsahu odpovědnosti materiálního dodavatele, tak takové čestné prohlášení musí být vydáno materiálním dodavatelem nebo společností (např. prodejcem, dceřinou společností apod.), která je k tomu materiálním dodavatelem zmocněna.

Doklady, které přikládá poskytovatel k žádosti o zápis nabídky, musí v případě, že se týkají materiálního dodavatele, obsahovat stejnou identifikaci materiálního dodavatele, jakou poskytovatel uvádí v této příloze.

Jestliže se popis splnění bezpečnostního **kritéria odvolává na jiný dokument poskytovatele**, předá poskytovatel relevantní část tohoto dokumentu v **pdf formátu** v samostatné příloze nabídky poskytovatele s vyznačením přesné části obsahu dokumentu, která dokládá splnění bezpečnostního kritéria.

4) Způsob podání a identifikace dokumentů

Jedno podání může obsahovat řadu podkladů (dokumentů, výpisů, prohlášení). Do datové zprávy systému datových schránek však nelze z bezpečnostních důvodů kvůli kontrole malwaru vložit přílohu typu ZIP. Dokumenty je tedy nutné vložit jednotlivě. Omezte počet příloh do max. 50 MB objemu v jedné datové zprávě. Jedno podání je možné rozdělit do několika následných datových zpráv.

Vyžadované dokumenty budou předávány v rámci datové zprávy/datových zpráv jako samostatné soubory, jejichž název je definován takto:

Identifikace ex-ante kontroly_ Pořadové číslo dokumentu_RRMMDD_Volitelná část

kde jednotlivé části identifikace mají následující význam:

Identifikace ex-ante kontroly je identifikátor kritéria, ke kterému poskytovatel přikládá dokument/dokumenty dle seznamu kritérií uvedeném v **Příloze č. 3** (například *Sm1, ID1*),

Pořadové číslo dokumentu je pořadové číslo dokumentu v rámci dokumentů, které se vztahují k témuž kritériu (např. *01, 02*)**,**

RRMMDD je datum vytvoření dokumentu,

Volitelná část je část identifikace dle volby poskytovatele. Může se např. jednat o iniciálu zpracovatele dokumentu, stručný název dokumentu apod.

Oddělovačem jednotlivých částí identifikace dokumentu je znak „_".

V případě, že je poskytování služby materiálního dodavatele závislé na využití služeb dalších materiálních dodavatelů nebo služeb systematických zpracovatelů, uvede jejich seznam v nabídce a deklaruje, že vztah s každým systematickým zpracovatelem je ošetřen dle čl. 28 GDPR.

Svoji nabídku může poskytovatel kdykoliv v průběhu platnosti poptávky aktualizovat. Aktualizovaná nabídka musí projít opětovnou certifikací.

5) Nabídku poskytovatel zašle do datové schránky zřízené speciálně pro účel přijímání žádostí o zápis do katalogu cloud computingu s kapacitou přenášené datové zprávy 50 MB (aditivní datová schránka).

   Předmět zprávy bude vyplněn takto: „**Nabídka cloud computingu-*Identifikace poskytovatele-Název nabídky nabízeného cloud computingu"***

   kde

   Identifikace poskytovatele je identifikace poskytovatele shodná s údajem identifikujícím poskytovatele cloud computingu, který cloud computing nabízí uvedeným na záložce „identifikační údaje" ve formuláři nabídky dle **Přílohy č. 2** (např. *1. poskytovatel cloud computingu s.r.o*.)

   Název nabídky nabízeného cloud computingu je název nabídky nabízeného cloud computingu shodný s údajem uvedeným v záložce „Identifikační údaje" ve formuláři nabídky dle Přílohy č. 2 (např. Best cloud computing*)*

   Tato datová schránka má název „**Katalog cloud computingu (Ministerstvo vnitra)**" a ID této schránky je: **ap2hwi6**

3.2.2 Aktivity procesu „Ex-ante kontrola poskytovatele a jeho služeb a zápis nabídky do katalogu cloud computingu"

1) **MV došlou nabídku v termínu 45 dní zkontroluje a nabídku certifikuje a zapíše do katalogu nabídek nebo odmítne**.

   Tato kontrola se nazývá „ex-ante kontrolou". Tato ex-ante kontrola a certifikace nabídky probíhá formou posouzení žádosti poskytovatele o zápis nabídky cloud computingu do katalogu cloud computingu podle zákona 500/2004 Sb. správní řád v rámci správního řízení. Ve správním řízení správní orgán ověřuje, zda nabídka cloud computingu obsahuje všechny požadované údaje a náležitosti a zda služby nabízené jednotlivými poskytovateli splňují bezpečnostní kritéria, která MV obecně vyžaduje pro služby cloud computingu určité bezpečnostní úrovně (viz ZoISVS § 6o bod 3.). Ex-ante kontrola se tedy nezabývá ověřením či posuzováním, zda nabízené služby jsou vhodné pro konkrétní ISVS.

   Poznámka: *To, zda jsou nabízené služby a jejich bezpečnostní opatření vhodné pro specifické*

podmínky konkrétního ISVS se rozhoduje:

a) v průběhu veřejné zakázky, ve které orgán veřejné správy vybírá z katalogu certifikovaných služeb služby eGC, které hodlá použít pro realizaci svého ISVS. Při této kontrole již OVS nemusí prověřovat ta bezpečnostní kritéria, která byla prověřena ex-ante kontrolou, ale musí prověřit ta kritéria, která jdou nad rozsah ex-ante kontroly a která OVS dle ZKB a jeho vyhlášek vyžaduje pro zajištění bezpečnosti svého ISVS.

b) v tzv. „ex-post kontrole", kterou může provést NÚKIB při kontrole bezpečnosti provozu daného ISVS dle ZKB, resp. MV při kontrole ISVS dle ZoISVS.

Bezpečnostní kritéria prověřovaná MV při ex-ante kontrole jsou uvedena v **Příloze 3.** Prověřovaná bezpečnostní kritéria byla definována MV ve spolupráci s NÚKIB a jsou odstupňována podle bezpečnostních úrovní. Z důvodu zjednodušení náročnosti ověřování podkladů v ex-ante kontrole a z důvodu dodržení krátkého termínu této kontroly, byla z kritérií obsažených v SAZ kap. 6.2.2 pro účely ex-ante kontroly použita pouze ta kritéria, která lze jasně doložit z certifikátů a citacemi z auditních zpráv dle uvedených standardů – to jsou kritéria označená jako ID1 až ID 18.

Množiny služeb nabízené na odlišných listech Přílohy 2 mohou mít odlišný výsledek kontroly. Vyplývá to z faktu, že ke každé množině služeb uvedené na jednom listu Přílohy 2 se dokládá samostatná Příloha 3, která dokládá, jak poskytovatel naplňuje požadovaná bezpečnostní kritéria.

V případě, že výsledek kontroly je pozitivní (služby jsou zapsány do katalogu cloud computingu), poskytovatel může tyto služby nabízet orgánům veřejné správy. Může je ale nabízet nejvýše s tou bezpečnostní úrovní, pro kterou byly ověřeny. To např. znamená, že když množina služeb uvedená na jednom listu Přílohy 2 byla ověřena pro bezpečnostní úroveň „2", může je poskytovatel nabízet orgánům veřejné správy jak pro bezpečnostní úroveň „2", tak bezpečnostní úroveň „1".

2) O výsledku kontroly MV poskytovatele informuje přes datovou schránku poskytovatele.

Po uzavření kontroly MV zapíše nabídku, která úspěšně prošla ex-ante kontrolou do katalogu eGC a uveřejní ji v informačním systému cloud computingu (ISCC).

3.3 Zápis využívané služby do katalogu eGC

V katalogu **K3: Katalog využívaných služeb** musí být zapsány údaje o všech službách cloud computingu, které aktuálně využívají orgány veřejné správy. Údaje do katalogu zapisuje správce ISVS, a to v této struktuře:

a) údaje identifikující cloud computing, jimiž jsou

1. název využívaného cloud computingu,
2. datum zahájení využívání cloud computingu,
3. předpokládané datum ukončení využívání cloud computingu (nejlépe datum expirace v dané chvíli platné smlouvy s poskytovatelem)

b) údaje identifikující orgán veřejné správy, který cloud computing využívá, jimiž jsou

1. název orgánu veřejné správy,
2. identifikátor orgánu veřejné moci přidělený orgánu veřejné správy,

c) údaje identifikující prodejce cloud computingu, který cloud computing poskytuje, jimiž jsou

1. u právnické osoby obchodní firma nebo název a identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,
2. u podnikající fyzické osoby obchodní firma nebo jméno, popřípadě jména, a příjmení, včetně

odlišujícího dodatku nebo dalšího označení, a identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,

d) údaje o základních parametrech cloud computingu, jimiž jsou

1. třída cloud computingu,
2. oblast cloud computingu,
3. typy cloud computingu, do nichž skutečně využívané služby spadají
4. bezpečnostní úroveň cloud computingu,
5. identifikační číslo smlouvy o poskytování cloud computingu uzavřené mezi orgánem veřejné správy a poskytovatelem cloud computingu přidělené správcem registru smluv, eviduje-li se smlouva v registru smluv,
6. identifikátor informačního systému veřejné správy, pro který cloud computing slouží
7. finanční objem zaplacený za dodávané služby cloud computingu pro daný ISVS v uplynulém kalendářním roce.

Zápis využívané služby do katalogu OVS realizuje přes datovou schránku zřízenou speciálně pro účel přijímání žádostí o zápis do katalogu cloud computingu s kapacitou přenášené datové zprávy 50 MB (aditivní datová schránka). Předmět zprávy: **Zápis využívaných služeb eGC do katalogu-*OVS*** (kde „***OVS***“ je název orgánu veřejné správy shodný s údajem identifikujícím orgán veřejné správy, který cloud computing využívá uvedený v záložce „Základní údaje“ formuláře v **Příloze č. 5**.
Tato datová schránka má název „**Katalog cloud computingu (Ministerstvo vnitra)**“ a ID této schránky je: **ap2hwi6**

Formulář pro zápis využívané služby cloud computingu je **v příloze č. 5** této metodiky.

3.3.1 Termíny zápisu využívané služby do katalogu eGC

Orgán veřejné správy musí zapsat výše uvedené údaje do katalogu v těchto termínech:

a) u nově pořízených služeb: zapíše cloud computing, který využívá (položky 1 až 6 výše), do katalogu cloud computingu do 45 dnů ode dne nabytí platnosti smlouvy o poskytnutí cloud computingu. Náklady cloud computingu (položka 7 výše) zapíše po uplynutí kalendářního roku nejpozději do 31. ledna následujícího kalendářního roku.

b) u již využívaných služeb: zapíše cloud computing, který využívá nejpozději do **1. 11. 2020**. Náklady cloud computingu (položka 7 výše) zapíše po uplynutí kalendářního roku nejpozději do 31. ledna následujícího kalendářního roku.

3.3.2 Výmaz služby z katalogu využívaných služeb

Orgán veřejné správy musí vymazat cloud computing, jehož využívání ukončil do 45 dnů ode dne pozbytí platnosti smlouvy o poskytnutí cloud computingu.

4. Poznámka: Proces Veřejné zakázky

Orgány veřejné správy mohou nakupovat služby cloud computingu buď individuálně (tj. přes samostatně organizované výběrové řízení) nebo přes centrálního zadavatele, kterým je MV. V obou případech je podmínkou využívání služby cloud computingu, že nabídka této služby (těchto služeb) je

součástí nabídky služeb poskytovatele zapsané (certifikované) v Katalogu nabídek (K2) – viz ZoISVS §6l (1).

Aktivity procesu veřejné zakázky definuje Zákon o zadávání veřejných zakázek. Proto je tato metodika nepopisuje.

5. Význam zkratek

eGC	eGovernment Cloud
ISVS	informační systém veřejné správy
ISeGC	informační systém cloud computingu
KeGC	komerční část eGC
DNS	dynamický nákupní systém (pojem ZZVZ)
ŘOeGC	řídicí orgán eGC
SAZ	souhrnná analytická zpráva projektu Příprava vybudování eGovernment cloudu schválená usnesením vlády ČR č. 749 ze dne 17. listopadu 2018
SeGC	státní část eGC
ZKB	zákon o kybernetické bezpečnosti 181/2014 Sb.
ZoISVS	zákon o informačních systémech veřejné správy 365/2000 Sb.

6. Přílohy

6.1 Příloha 1 - Vzor poptávky OVS na služby eGC pro zápis poptávky cloud computingu do katalogu cloud computingu

6.2 Příloha 2 - Formulář nabídky poskytovatele na služby eGC pro zápis nabídky poskytovatele do katalogu cloud computingu

6.3 Příloha 3 - Bezpečnostní kritéria používaná při ex-ante kontrole

6.4 Příloha 4 – Minimální smluvní podmínky

6.5 Příloha 5 – Formulář pro zápis využívané služby cloud computingu do katalogu cloud computingu orgánem veřejné správy