eGOVERNMENT CLOUD
- cesta k bezpečnému a nákladově přijatelnému informačnímu systému

Prof. Ing. Jiří Voříšek, CSc.
jiri.vorisek@savs.cz, jiri.vorisek@dia.gov.cz

SAVŠ, katedra informatiky
Digitální informační agentura

Agenda

1. Důvody vzniku eGC
2. Historie příprav a realizace eGC
3. Výhody a rizika cloud computingu pro zákazníka
4. Cíle eGC
5. Struktura eGC a jeho služeb
6. Základní pravidla fungování eGC
7. Katalog cloud computingu
8. Metodiky a nástroje podporující využívání služeb eGC
9. Procesy zápisu poptávky, poskytovatele a jeho nabídky do katalogu CC
10. Proces veřejné zakázky pro realizaci IS pomocí eGC
11. Výhody využití eGC pro subjekty, které nejsou OVM
12. Dosavadní zkušenosti z projektu eGC

Důvody vzniku eGC (formulované v r. 2015)

- **Stav datových center (DC) státních institucí -** výsledky průzkumu SPCSS z r. 2015:
  - Žádné DC nesplnilo všechny kritické parametry
  - Jen 10 ze 46 hodnocených DC splnilo alespoň 80 % kritických parametrů

  Stav je nevyhovující a uvedení všech stávajících DC do souladu s požadavky by bylo velmi finančně nákladné. Decentralizace DC způsobuje vysoké nároky na počty IT specialistů.

- **Kontrolní závěr 14/20 NKÚ z r. 2015**
  - *„V současnosti není nastaven systém rozvoje a udržitelnosti sdílených služeb datových center, není stanovena koordinace budování a rozvoje datových center, není stanoveno, kde by měly být současné i nově vzniklé informační systémy provozovány, a neexistují pravidla pro přechod veřejné správy do datových center.“*

- **Nízké sdílení IT technologií a aplikací ve VS**

  Rozsah problému demonstrují následující čísla (dle údajů https://www.sluzby-isvs.cz/ ke dni 25.7.2017):
  - Počet OVS je cca 7500
  - Počet registrovaných informačních systémů VS je celkem 7 408
  - Každá instituce VS buduje a provozuje své IS nezávisle na ostatních

- **Náklady IS - Porovnání systémů ERP, HR, e-mailu a spisové služby** (průzkum MV ČR z 6/2015)
  - Náklady na hodnocené informační systémy (e-mail, spisová služba, ERP a HR) přepočtené na jednoho uživatele se liší mezi resorty řádově
  - Roční výdaje na IT (investiční i provozní) mezi roky 2010 a 2016 postupně rostou od 9 mld. Kč do 15,8 mld. Kč
  - Zkušenosti Velké Británie, Dánska a dalších zemí ukazují úspory při přechodu z nesdílených na sdílené služby formou eGC 10% až 50%. Uvážíme-li konzervativní cílový odhad 20% úspor, pak by roční úspory při využití eGC mohly být v řádu miliard Kč.

Historie příprav a realizace eGC (2015-2023)

- Akční plán k Národní strategii kybernetické bezpečnosti z r. 2015 – první krok k vybudování eGC
  - úkol C.7.01, Vytvořit a vládě předložit Národní strategii cloud computingu
- Strategie rozvoje ICT služeb veřejné správy – schválená vládou **11/2015**
  - O22. Nákup nových ICT služeb směřovat na sdílené služby s využitím tzv. eGovernment Cloudu a Katalogu sdílitelných ICT služeb.
  - O23. Vybudovat síť státních center sdílených služeb propojených bezpečnou datovou komunikační infrastrukturou, která bude poskytovat sdílené ICT služby orgánům veřejné moci s vysokou bezpečnostní úrovní
- 12/2015 Národní strategie cloud computingu – postavena zejména na zkušenostech z eGC VB, množství připomínek v meziresortu – rozhodnutí: přepracovat
- 11/2016 schválila Vláda ČR *Strategický rámec Národního cloud computingu – eGovernment cloud ČR*
- 9.12.2016 byla ustanovena ***Pracovní skupina RVIS pro přípravu vybudování eGovernment cloudu***, složená ze zástupců MV, MF, NBÚ, NÚKIB, zástupců ústředních orgánů státní správy, zástupců zpravodajských služeb a zástupců odborné veřejnosti.
  - Cílem projektu *Příprava vybudování eGovernment cloudu* byla analýza legislativních, technických, ekonomických, organizačních a bezpečnostních podmínek vybudování eGC
  - Výstupem projektu byla **souhrnná analytická zpráva (SAZ)** obsahující kromě analýzy i návrhy opatření a doporučení implementačních kroků a standardů pro využívání cloud computingu ve veřejné správě.
- **Souhrnná analytická zpráva schválena vládou 14/11/2018, č.j.** čj. 891/18 (dostupná na https://www.mvcr.cz/soubor/souhrnna-analyticka-zprava-projektu-egovernment-cloud.aspx) – první komplexní dokument navrhující strukturu eGC, pravidla eGC a věcný záměr legislativy eGC
- **1/8/2020** v účinnosti novela zákona 365/2000 Sb. upravující eGC
  - tato novela (poslanecká iniciativa) obsahovala právně nejasná ustanovení a proto byla nutná další novelizace
- **1/9/2021 v účinnosti další novela zákona 365/2000 Sb. a vyhlášky NUKIBu č. 315/2021** o bezpečnostních úrovních CC a č. 316/2021 o bezpečnostních opatřeních prověřovaných při zápisu poskytovatele a jeho služeb do katalogu CC - kompromis mezi MV, NÚKIB a komerčními poskytovateli, základ legislativy regulující eGC platný dodnes
  - Definice bezpečnostních úrovní CC
  - Oddělení certifikace poskytovatele CC od certifikace jeho služeb
  - Zpřísnění certifikačních pravidel
  - Definice katalogu CC
  - Detailní definice postupu zápisu poskytovatele CC, služeb CC a využívaných služeb CC
- **4/6/2023 v účinnosti Vyhláška NUKIBu 190/2023 Sb. o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.**
  - Stanoví obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu podle § 6 písm. e) zákona, jejichž cílem je zajištění bezpečnosti informací při využívání služeb cloud computingu orgány veřejné moci.

Výhody a rizika cloud computingu (CC) pro zákazníka

1. Výhody

- *Úspora nákladů na provoz IS oproti on-premise provozu (při stejných požadavcích na bezpečnost a spolehlivost) – náklady formou „pay as you go“, úspory z rozsahu, multitenantní provoz SW*
- *Vysoká flexibilita – spotřebovaný objem služeb lze pružně měnit dle potřeb zákazníka*
- *Krátký čas*, který uplyne od identifikace potřeby IT služby k jejímu zprovoznění - *využití Marketplace pro nákup služeb CC*
- *Rychlé technologické inovace*
- *Možnost otestování před zakoupením*
- *Přenos starostí o IT na specializovanou firmu – úspora vlastních zdrojů*

2. Rizika

- *Uživatel částečně ztrácí kontrolu nad svými daty*
- *Možné zneužití dat poskytovatelem (viz např. kauza Schrems II)*
- *Ztráta znalosti, která může být potřebná v budoucnu*
- *Výběr vhodného poskytovatele služby*
- *Úpravy aplikace mimo kontrolu*
- *Omezená customizace aplikace*
- *Nezajištěná integrace s ostatními aplikacemi*
- *Spolehlivost připojení k aplikaci*

Cíle eGC (definovány v SAZ, dosud platné)
– agregovat poptávku a nabídku cloudových služeb a tím:

1. **Garantovat potřebnou bezpečnost a spolehlivost provozu informačních systémů VS**
   - potřebná bezpečnost a spolehlivost je definována
     - NIS2 (Network and Information Security 2, Directive 2022/2555 of the European Parliament)
     - ZKB a související vyhlášky
     - ZoISVS

2. **Zvýšit rozsah sdílení IT zdrojů a tím zefektivnit výdaje na ICT ve veřejné správě**

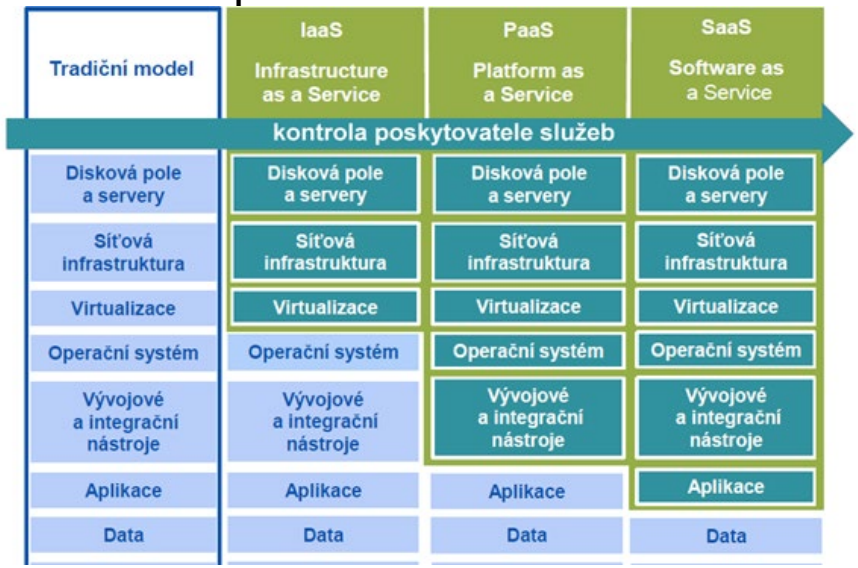
3. **Zrychlit a zefektivnit nákup standardních (komoditních) ICT služeb**
   - viz příklad Velké Británie

4. **Snížit náklady na služby veřejné správy přepočtené na jednu ICT službu a jednoho uživatele**
   - zákazníci, kteří využívají CC dosahují úspor 20-50% oproti on-premise provozu IS

Struktura eGC a jeho služeb

eGovernment Cloud je tvořen:

- Službami CC (bezpečnostní úrovně 1 až 3) privátních datových center – tzv. **komerční cloud (KeGC)**
  – start v 1/8/2020
- Vysoce bezpečnými (bezpečnostní 4. úroveň) službami CC zákonem/vládou určených státních ICT podniků - tzv. **státní cloud (SeGC)** – start až po schválení potřebné legislativy (v r.2024?)
- **Hybridní eGC** je kombinací služeb KeGC a SeGC, která vychází z principu dekompozice IS na komponenty s různými úrovněmi bezpečnostních dopadů

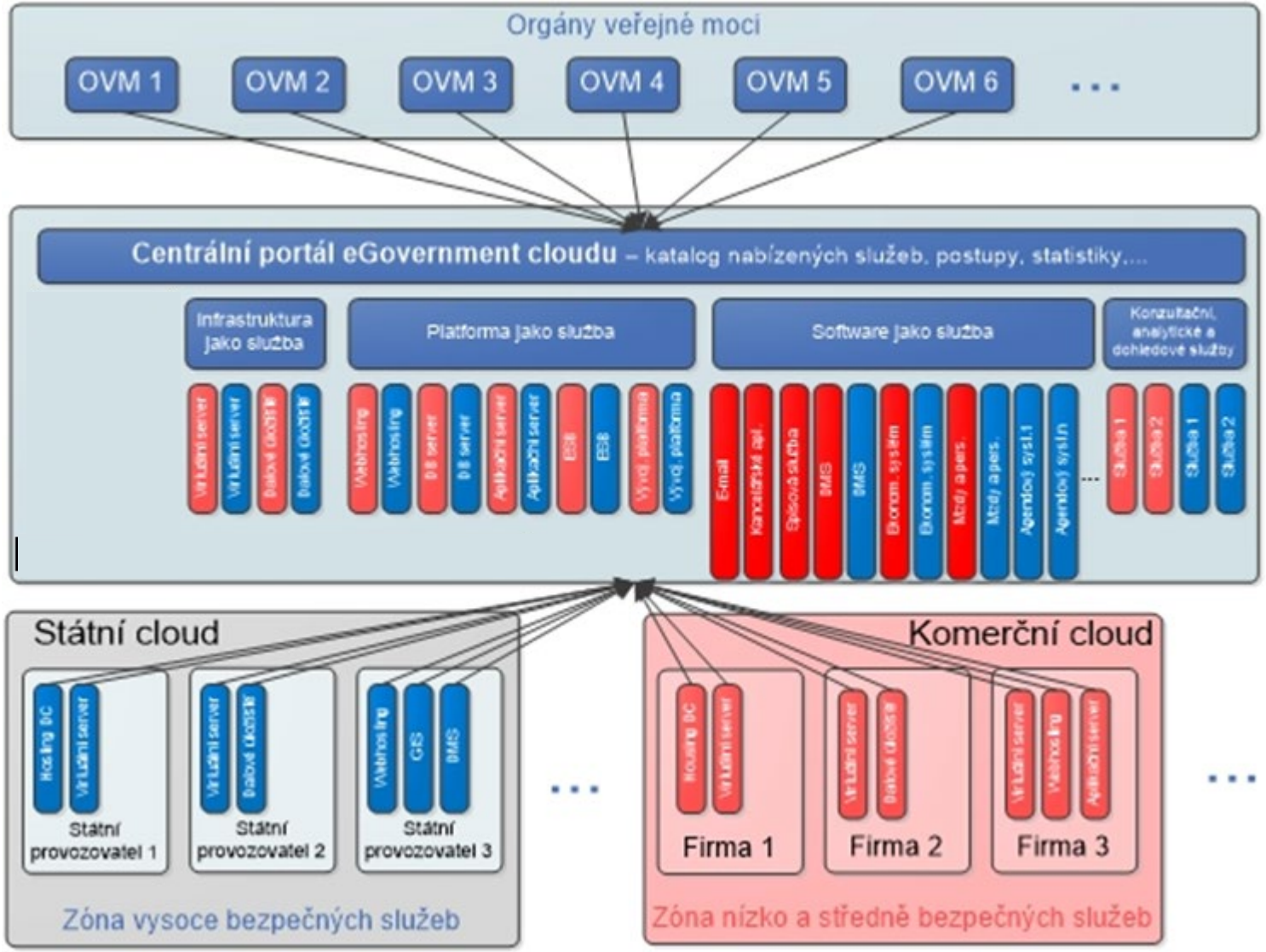


Služby eGC:

- Služby CC
  - IaaS
  - PaaS
  - SaaS
- konzultační služby k nasazení služeb eGC

Struktura eGC a jeho služeb

Všechny služby eGC jsou nabízeny přes portál eGC (https://www.dia.gov.cz/oha/katalog-cloud-computingu/)



Základní pravidla fungování eGC

- **Orgán veřejné správy může využívat pouze CC, který je zapsán v katalogu CC** (ZoISVS, §6l, odst. 1, avšak s řadou výjimek viz např. odst. 4).

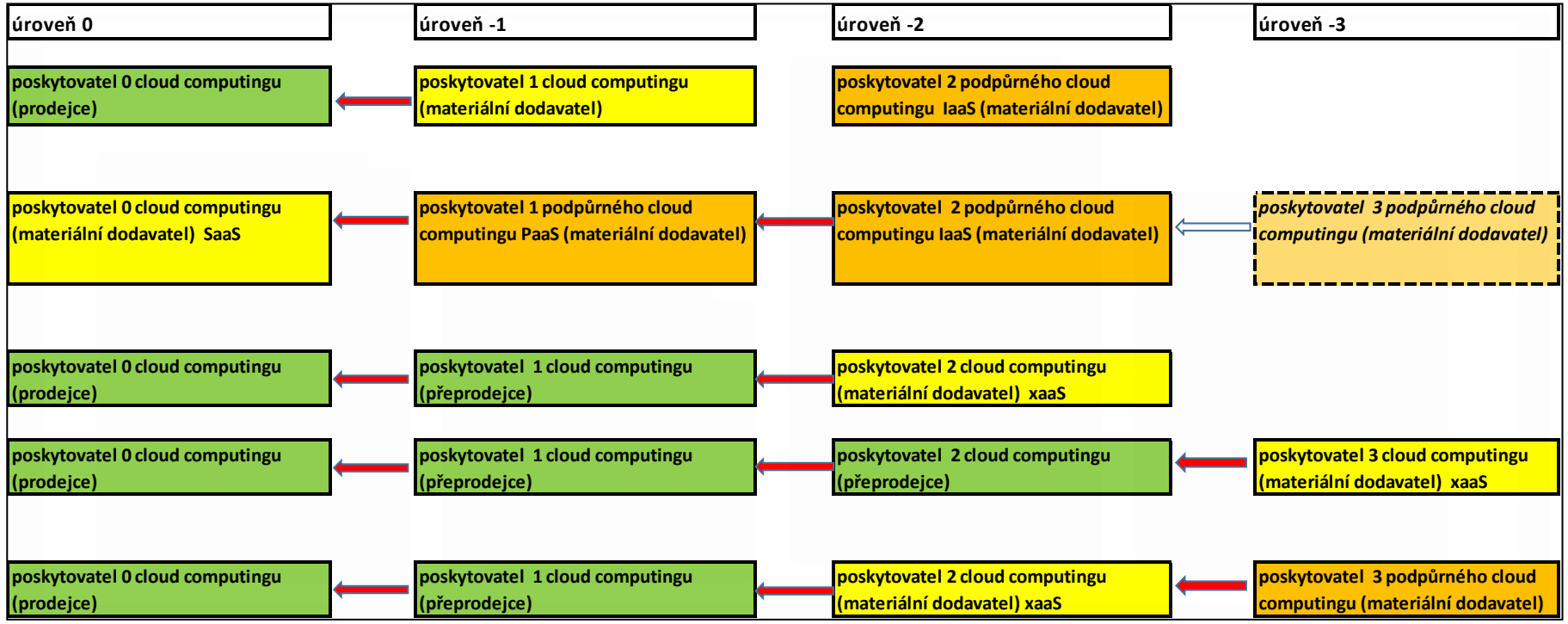
- Všechny služby CC, které orgán veřejné správy využívá pro realizaci svého IS, musí OVS zapsat do **katalogu využívaných služeb CC** (ZoISVS, §6x) a to do 45 dnů ode dne nabytí platnosti smlouvy o poskytnutí cloud computingu.

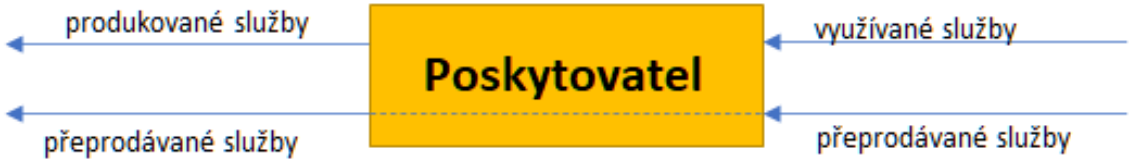
- **O zápis svých nabízených služeb CC do katalogu CC může požádat pouze zapsaný poskytovatel,** tj. ten, který předtím požádal o zápis do katalogu poskytovatelů CC a jeho žádost byla úspěšně ověřena (ZoISVS, §6t, odst. 1).

- Pro každou službu IaaS/PaaS/SaaS kterou sám produkuje, musí poskytovatel v žádosti doložit, **jak služba splňuje požadavky vyhlášky č. 316/2021 Sb.** „o některých požadavcích pro zápis do katalogu cloud computingu“ (ZoISVS, § 6t odst. 5). **Rozsah těchto dokládaných informací se liší v závislosti na bezpečnostní úrovni, ve které je služba CC nabízena** (viz část „Podklady k ověření“ žádosti o zápis cloud computingu do katalogu CC.)

Základní pravidla fungování eGC

- **Je-li nabízená služba CC dodávána řetězcem poskytovatelů, pak každý poskytovatel tohoto řetězce musí být zapsán v katalogu CC. V katalogu CC musejí být zapsané i všechny služby CC dodavatelského řetězce, které jsou pro tvorbu služby nabízené zákazníkovi veřejné správy využívány.**
- **Zákazník (OVM) zodpovídá za respektování vyhlášky 190/2023 Sb. o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu**





Katalog cloud computingu

Obsahuje *(viz https://www.mvcr.cz/clanek/katalog-cloud-computingu.aspx) :*

- **Katalog poptávek CC**– obsahuje poptávky veřejné správy (společnou poptávku veřejné správy a individuální poptávky jednotlivých OVS) na určité typy služeb CC, které veřejná správa hodlá v daném období využívat pro provoz svých IS. *Poptávky tohoto katalogu nejsou poptávkami ve smyslu Zákona o veřejných zakázkách, ale jsou výzvou poskytovatelům CC, aby si nechali do katalogu CC zapsat svoje služby*, které orgány veřejné správy hodlají využívat.

- **Katalog poskytovatelů CC**, obsahuje poskytovatele CC, kteří požádali o zápis do katalogu poskytovatelů a úspěšně prošli ověřením dle kritérií stanovených zákonem (ZoISVS §6m a §6q).

- **Katalog nabídek CC** – obsahuje nabídky služeb CC jednotlivých zapsaných poskytovatelů CC, které úspěšně prošly ověřením (tzv. ex-ante kontrolou), že splňují požadavky dle zákona (ZoISVS §6n a §6t) a vyhlášky 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

  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 popis opatření, kterými poskytovatel splňuje bezpečnostní kritéria používaná při ex-ante kontrole.

- **Katalog využívaných služeb CC 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 využívaných typů služeb cloud computingu.

Metodiky a nástroje podporující využívání služeb eGC

(https://www.dia.gov.cz/oha/egovernment-cloud/metodiky-navody-formulare/)

- Dekompozice IS na jednotlivé provozní a architektonické komponenty
- Stanovení bezpečnostní úrovně IS a jeho komponent
- Porovnání celkových nákladů vlastnictví (TCO) IS provozovaného různými variantami (on-premise, klasický outsourcing, CC)
- Minimální smluvní podmínky pro smlouvu na poskytování služeb CC
- Katalog cloud computingu (obsahuje poptávky VS po službách CC, poskytovatele CC a nabídky jejich služeb, evidenci využívaných služeb CC veřejnou správou)
- Návod na využívání eGC a formuláře pro zápis poptávek, poskytovatelů služeb CC a využívaných služeb CC do katalogu CC

Dekompozice IS z hlediska využití služeb eGC

Cílem dekompozice IS je využít pro každou komponentu IS co nejméně nákladné služby CC, které splňují požadavky na bezpečnost komponenty.

Každý IS může být dekomponován ze dvou hledisek:

- **Operační (provozně funkční)**
  - Vývojové prostředí
  - Testovací prostředí
  - Školící prostředí
  - Provozní prostředí
  - Sekundární Site Recovery instance IS
  - Záloha dat

- **Architektonické**
  - Front End a Back End
  - Sekundární storage
  - Data a analytické služby
  - Infrastrukturní a aplikační monitoring

- Po dekompozici IS na jednotlivé komponenty dle výše uvedených hledisek **je každá komponenta zařazena samostatně do své úrovně bezpečnosti.**

Bezpečnostní úrovně IS v eGC

(prvotně definovány v SAZ, od r. 2021 vyhláškou NÚKIB č. 315/2021)

- **Každý IS jako celek i jeho jednotlivé komponenty musí být správcem IS zařazeny do jedné ze 4 bezpečnostních úrovní (nízká, střední, vysoká, kritická)**
- **Metodika určení úrovně bezpečnostních dopadů** *(viz též dokument NUKIBu: Průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně)* posuzuje 10 oblastí:
  - bezpečnost a zdraví osob,
  - ochrana osobních údajů,
  - zákonné a smluvní povinnosti,
  - trestně-právní řízení,
  - veřejný pořádek,
  - mezinárodní vztahy,
  - řízení a provoz organizace,
  - ztráta důvěryhodnosti,
  - finanční ztráty,
  - zajišťování nezbytných služeb.
- Správci IS určují, jaké **maximální úrovně dopadu** mohou nastat při narušení důvěrnosti, integrity, dostupnosti jejich IS, až po ztrátu dat (od poslední zálohy, až po totální ztrátu dat).
- Podle ní pak zařadí IS a její komponenty do jedné ze 4 úrovní bezpečnosti (celý IS má přiřazenu bezpečnostní úroveň stejnou jako má jeho komponenta s nejvyšší b.ú.)
- **Z bezpečnostní úrovně pak vyplývají bezpečnostní opatření**, které musí správce IS pro provoz IS (komponenty) zajistit - viz vyhláška NUKIBu č. 190/2023.

Bezpečnostní opatření vyžadovaná pro provoz komponenty s danou BÚ

NÚKIB stanovil ve Vyhlášce 316/2021 Sb. pro jednotlivé bezpečnostní úrovně informačního systému požadavky na bezpečnostní opatření, které musí IS s danou BÚ splňovat. Požadavky na bezpečnostní opatření jsou rozděleny do deseti skupin:

1. Místo zpracování a uložení dat.
2. Žádosti o zpřístupnění a předání dat.
3. Oprávnění k provedení kontroly.
4. Úrovně dostupnosti služby.
5. Připojení do peeringového uzlu.
6. Zajištění poskytování služby cloud computingu.
7. Nakládání s daty.
8. Certifikace služby cloud computingu.
9. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty.
10. Testování služby cloud computingu.

Detailně jsou požadavky na bezpečnostní opatření uvedeny ve formulářích žádosti na zápis služby do katalogu CC - *https://www.dia.gov.cz/oha/egovernment-cloud/metodiky-navody-formulare/*

TCO – podklad pro rozhodnutí o využití CC

(viz https://www.dia.gov.cz/oha/egovernment-cloud/metodiky-navody-formulare/metodika-tco-metodika-pro-vypocet-celkovych-nakladu-vlastnictvi-isvs/)

- Metodika TCO (tj. **určení celkových investičních a provozních nákladů IS za 5 let provozu**) je nástrojem eGC, který podporuje činnost správce IS, aby se mohl chovat jako správný hospodář.
- Metodiku a její kalkulátor lze využít zejména v těchto případech:
  - při kalkulaci celkových nákladů informačního systému (IS) za určité období;
  - jako přílohu k žádosti o realizaci ICT projektu informačního systému veřejné správy zasílanou na Odbor hlavního architekta eGovermentu;
  - při porovnávání nákladů různých variant řešení IS (on-premise, klasický outsourcing, cloud, hybridní řešení);
  - při modelování ekonomické výhodnosti různých cloud scénářů řešení IS;
  - při porovnávání nákladů realizace a provozu IS při různých bezpečnostních úrovních daného IS (tj. např. lze zjistit o kolik se zvednou náklady IS, jestliže bude přeřazen z bezpečnostní úrovně „vysoká“ do bezpečnostní úrovně „kritická“);
  - při detailní analýze vlivu jednotlivých nákladových položek na náklady IS;
  - při porovnání různých nabídek na realizaci a provoz IS v rámci výběrového řízení.

Minimální smluvní podmínky KeGC (výběr)

(viz prvotně SAZ, dnes aktuální znění zákona o kybernetické bezpečnosti 181/2014 Sb., vyhlášky č. 315/2021, č. 316/2021 a č. 190/2023

Minimální dostupnosti IS – viz též vyhl. č. 316/2021 (ID 4.1, 4.2)

Bezp. Úroveň	Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků, s měsíčním vyhodnocováním
Nízká KeGC	96,16%	Provozní doba pod SLA: minimálně určených 10 hodin v pracovní dny. Nezapočítávají se dny pracovního volna a dny pracovního klidu stanovené pro ČR. Např. r. 2018 má 250 pracovní dní, na bázi 10 hod. pod SLA denně, což dává max. měsíční výpadek 8,3 hod. při dostupnosti 96% (vztaženo na dobu pod SLA). Tato dostupnost může být např. vhodná pro některé back office systémy obcí a měst.	Max. 8 hod., avšak pouze v rámci definované pracovní doby
Střední KeGC	99,45%	Provozní doba pod SLA: 24x7 (připravenost pro služby související s úplným el. podáním). Avšak určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu. To znamená, že el. podání bude obvykle fungovat nepřetržitě, ale reakce poskytovatele na nahlášené incidenty je omezena.	Max. 4 hod. na bázi 24x7
Vysoká KeGC	99,9%	Provozní doba pod SLA: 24x7 (připravenost pro služby úplného el. podání, a pro IS pod ZoKB). Určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu.	Max. 43 min. na bázi 24x7
Kritická SeGC	99,99%	Provozní doba pod SLA: 24x7 (připravenost pro systémy kritické informační infrastruktury pod ZoKB). Vyhodnocování je zde z praktických důvodů na roční bázi, avšak jednotlivé výpadky bez penalizace jsou omezeny na max. 15 minut. Cloudové služby SaaS v této úrovni dopadu budou mít rovněž smluvně dané max. doby RPO / RTO.	Jednotlivý výpadek max. 15 min. Max. kumulovaný roční výpadek 52 min.

Minimální smluvní podmínky KeGC

Minimální doba podpory služby pro jednotlivé bezpečnostní úrovně:

Bezp. úroveň	Doba podpory služby
Nízká	Podpora a servis pouze v pracovní dny a v určené pracovní době.
Střední	Podpora a servis 24x7 (Pro SaaS může být variantně určená Pracovní doba)
Vysoká	Podpora a servis 24x7 (Pro SaaS může být variantně určená Pracovní doba)
Kritická	Podpora a servis 24x7

Úrovně podpory služby a prioritizace hlášených incidentů ze strany zákazníka:

Úroveň podpory	Priority incidentu a očekávaná doba reakce		
	Nízký business impact	Střední business impact	Kritický business impact
Úroveň 1.	Max. 8 hodin, pouze v pracovní dny	Max 4 hod., 24x7, případně pouze po vymezenou pracovní dobu	Max. X hod,. 24x7
Úroveň 2.	Max. X hod., pouze v pracovní dny	Max. X hod., 24x7	Max. X hod,. 24x7
Úroveň 3.	Max. X hod., pouze v pracovní dny	Max. X hod., 24x7	Max. X hod,. 24x7

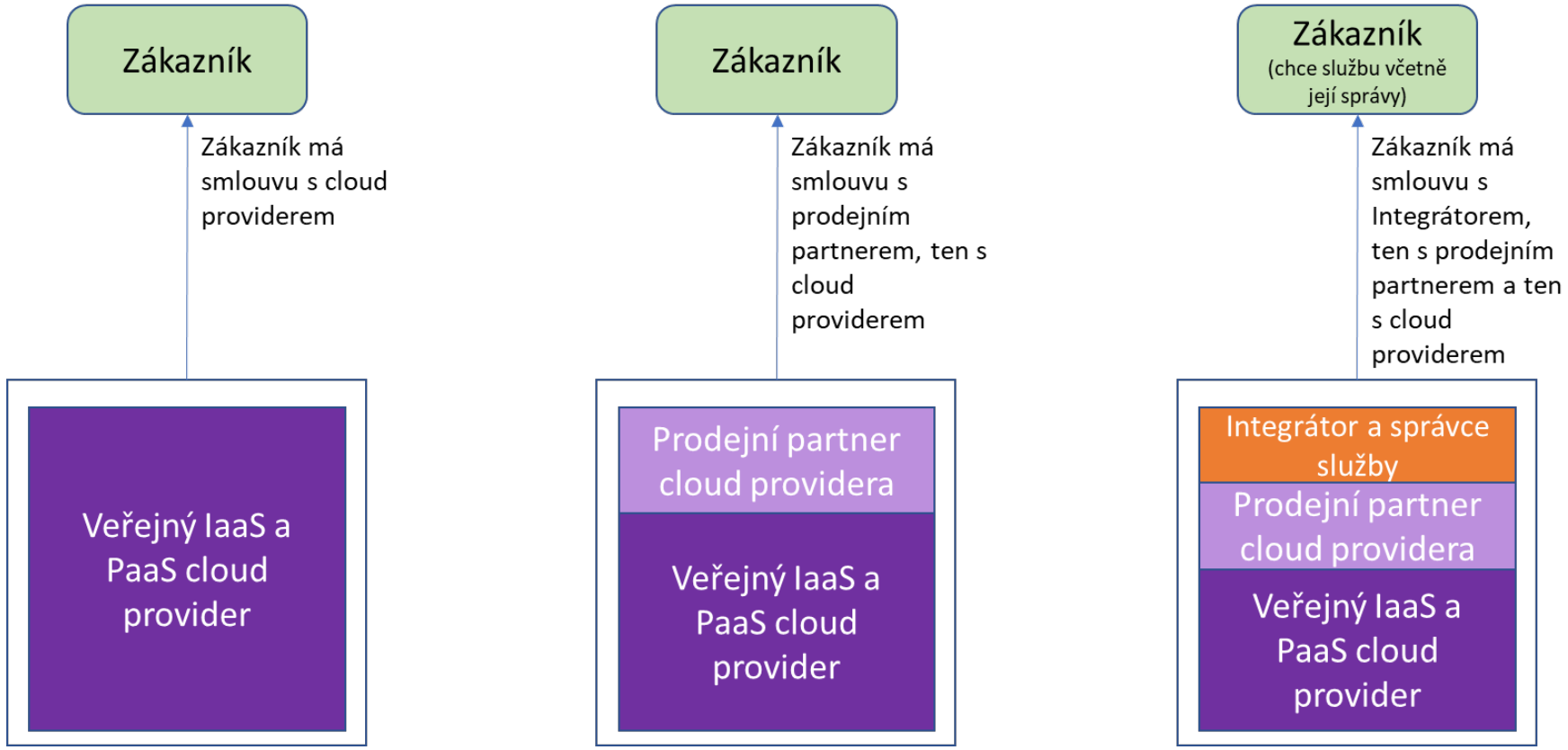
Minimální smluvní podmínky KeGC – ukončení smlouvy a sankce

- Koncept **„hrubého porušení SLA**“, musí být zakotven ve smlouvě. Za hrubé porušení SLA se rozumí situace, kdy v kterémkoli měsíci kumulovaná dostupnost služby dle její definice v SLA (s ohledem na definovanou „provozní dobu služby“) klesne pod **hraniční hodnotu 66%.**

- V takovém případě bude mít zadavatel možnost smlouvu okamžitě ukončit a nastartovat změnový proces k jinému poskytovateli nebo do prostředí on-premise.

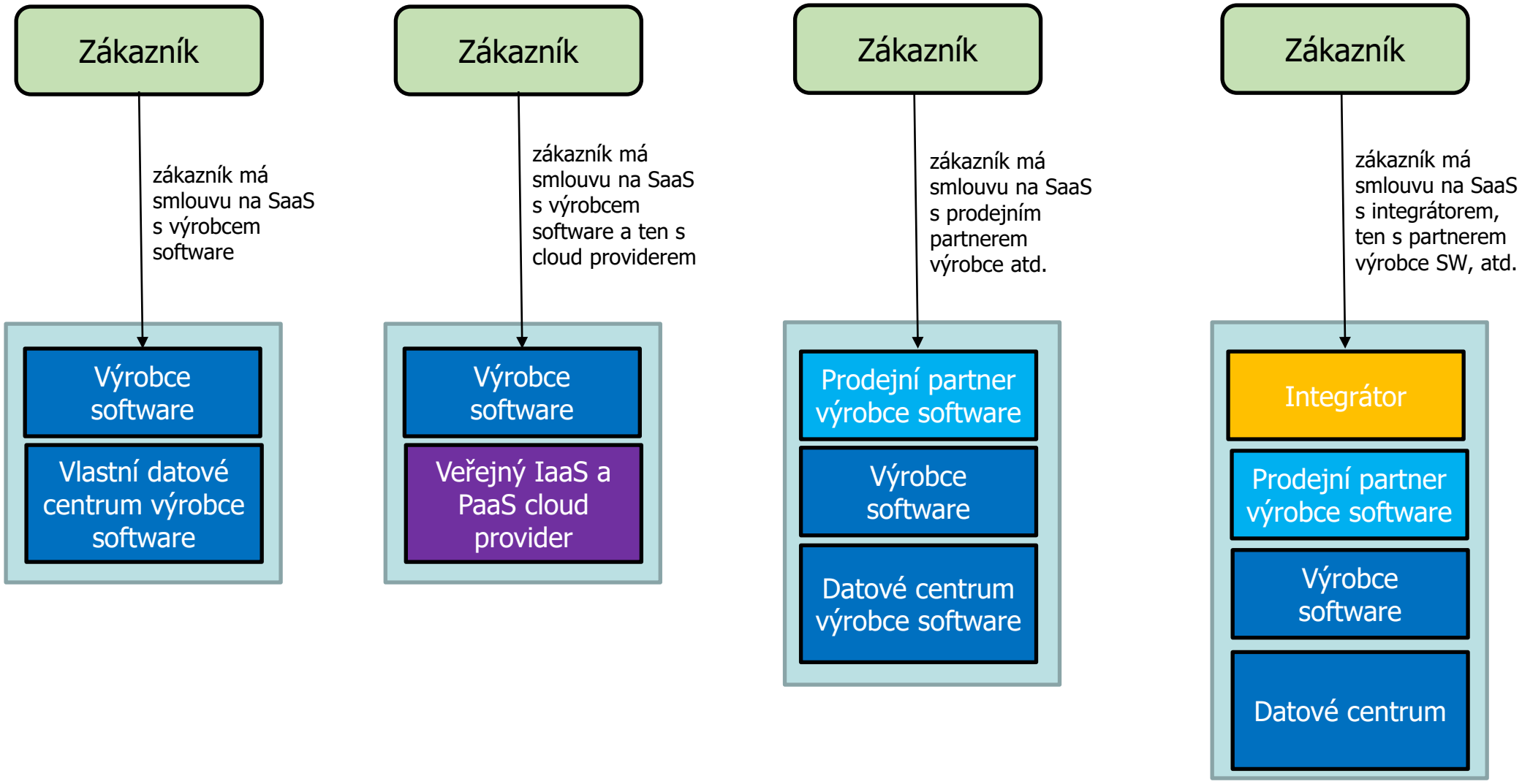
- Toto hrubé porušení SLA bude doprovázeno **odškodněním**, kterým poskytovatel služby KeGC uhradí předem sjednanou výši odhadovaných migračních nákladů zadavatele k jinému poskytovateli KeGC. Tato částka bude jako možná výše odškodnění uvedena každým zadavatelem v rámci zadání veřejné zakázky.

Základní varianty poskytování IaaS a PaaS služeb v KeGC
(dodavatelské řetězce)

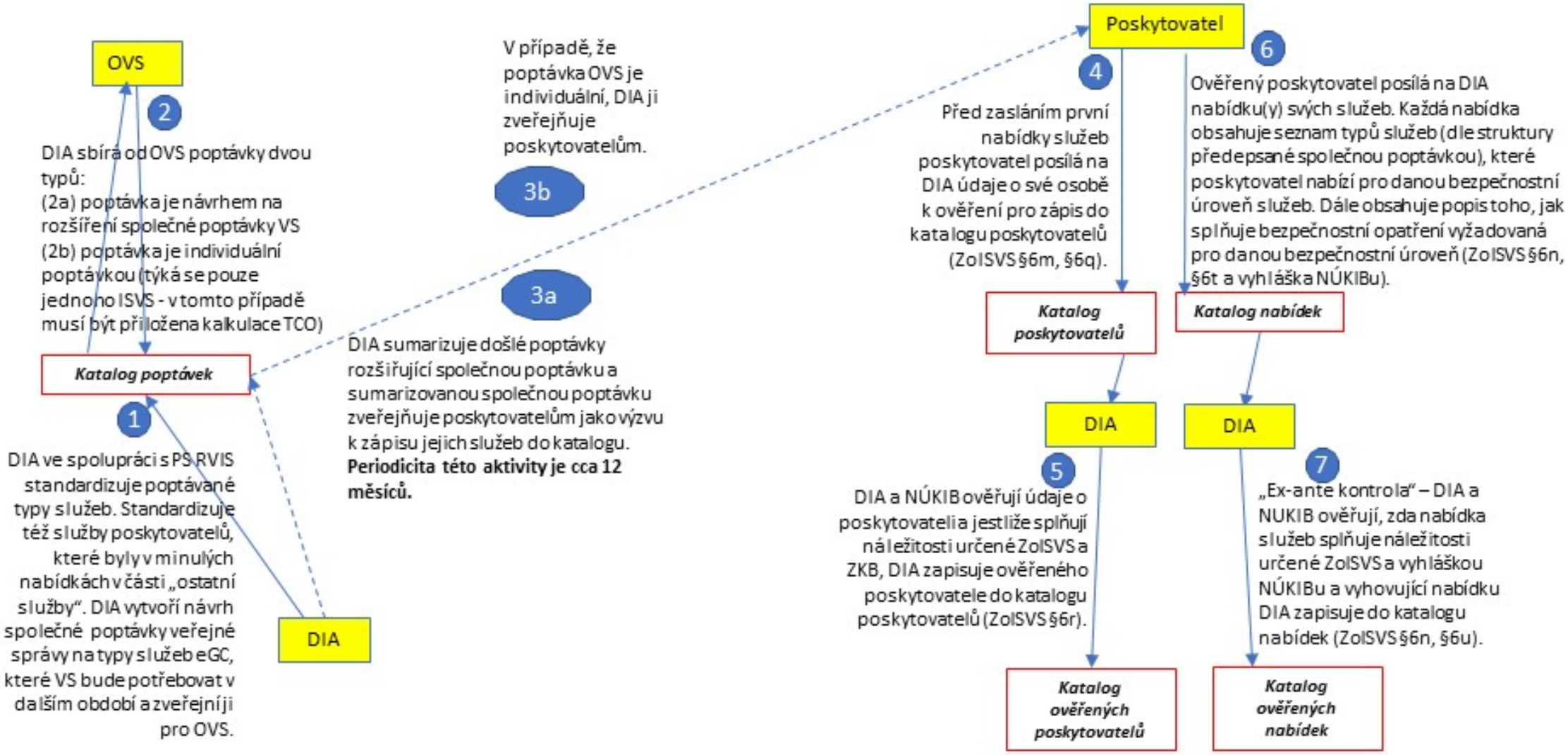


cloud provider = materiální dodavatel CC (vlastník datového centra)

Základní varianty poskytování SaaS služeb v KEGC
(dodavatelské řetězce)



Procesy zápisu poptávky, poskytovatele a jeho nabídky do katalogu CC



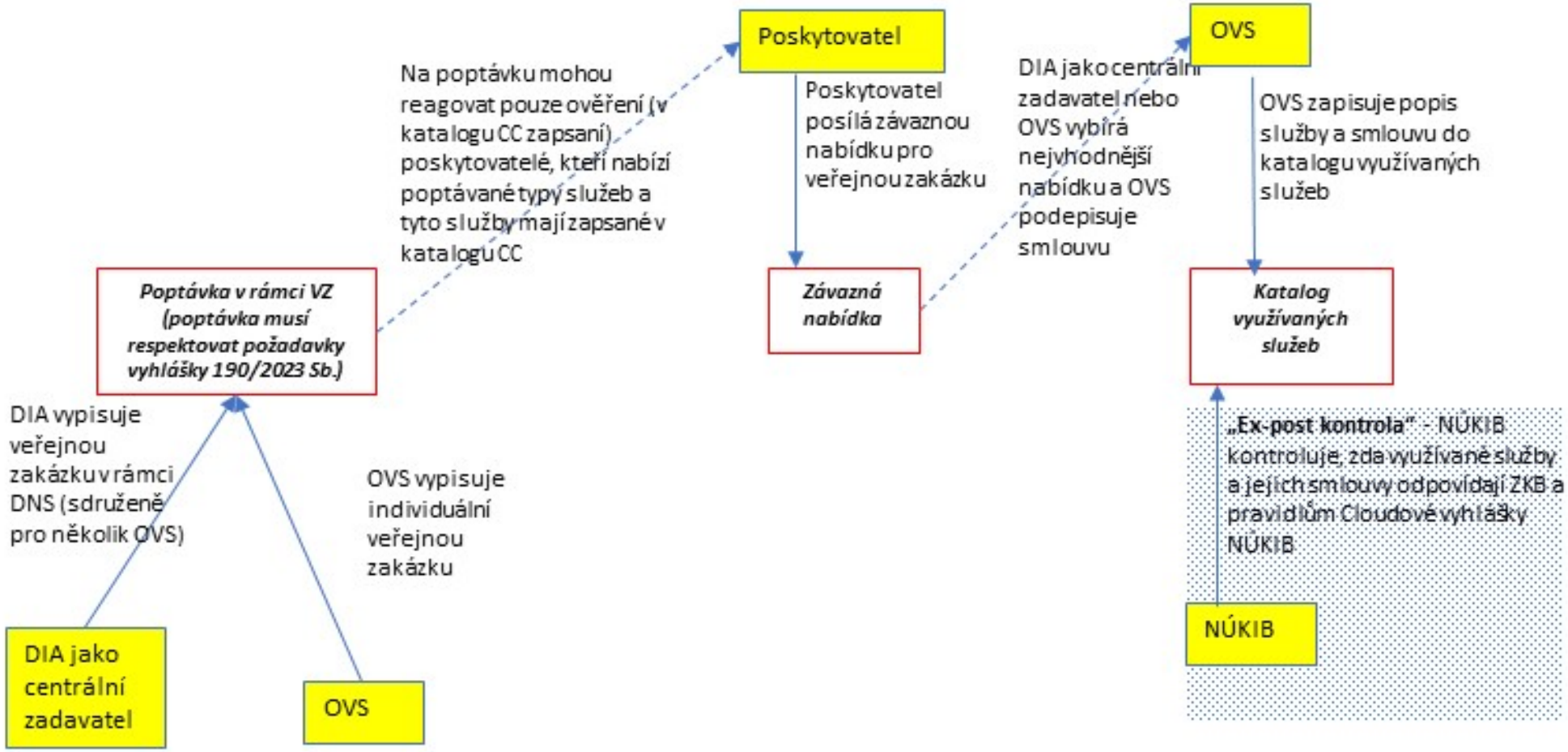
Formuláře pro zápis poptávky, poskytovatele a jeho nabídky do katalogu CC

- **Formulář pro zápis poptávky OVS na služby CC**

- **Formulář pro zápis poskytovatele CC**

- **Formulář pro zápis služeb CC (pro bezpečnostní úroveň 3)**

Proces veřejné zakázky pro realizaci IS pomocí eGC



Výhody využití eGC pro subjekty, které nejsou povinny využívat pouze služby zapsané v katalogu CC

- Poskytovatelé CC a jejich služby, které jsou zapsány v katalogu CC, jsou prověřeny NÚKIBem a Digitální informační agenturou. Tím se zákazníkovi zjednodušuje komplikované hodnocení, zda poskytovatel a jeho služby jsou vhodné pro jeho IS (hodnocení poskytovatele a jeho služeb v průměru trvá 6 měsíců).

- Metodiky, které jsou součástí eGC jsou využitelné obecně pro jakýkoliv subjekt.

- Využitím katalogu CC a souvisejících metodik lze výrazně zkrátit výběrové řízení na poskytovatele CC a snížit náklady na provoz IS.

Dosavadní zkušenosti z projektu eGC

- Dle zákona 365/2000 Sb. **účinného do 31/8/2021** bylo do katalogu cloud computingu úspěšně zapsáno **701 služeb od 76 poskytovatelů**. Schvalovací proces trval v průměru 5 měsíců.
  - Lze považovat za úspěch
- Dle zákona 365/2000 Sb. **účinného od 1/9/2021** bylo do katalogu CC do 20/9/2023 úspěšně zapsáno **68 poskytovatelů a 53 služeb**.
  - Průměrná doba zápisu poskytovatele je 4 měsíce
  - Zápis služeb pouze od 2 poskytovatelů
- SeGC nebylo dosud ustaveno, což představuje základní **bariéru pro využívání eGC pro IS zařazené do kritické infrastruktury státu** – hlavní problém legislativa

Dosavadní zkušenosti z projektu eGC

- **Pozitiva:**
  - Spolupráce různých odborníků (MV, NUKIB, OVS, poskytovatelé, vysoké školy) při tvorbě zákona, metodik a nástrojů
  - Usnadnění výběru služeb CC pro OVS – nemusejí pracně ověřovat důvěryhodnost poskytovatelů a spolehlivost služeb CC
  - V Evropě patříme mezi země, které mají eGC nejdetailněji legislativně a metodicky zajištěné – viz zkušenosti z konce r. 2022, kdy ČR předsedala Member States Cloud Coordination Group. Současně ale detailní legislativní požadavky vedou k vysoké administrativní náročnosti zápisu poskytovatele CC a jeho služeb do katalogu CC.

- **Negativa / výzvy:**
  - Vysoká admin. náročnost pro poskytovatele, MV, NUKIB i správce IS
  - Náročná kritéria bezpečnosti zatím aplikována jen na CC, nikoliv na ostatní formy provozu (klasický outsourcing, in-house). Důsledkem je preferování in-house provozu
  - Obtížné balancování různých dimenzí eGC – **legislativa, bezpečnost, náklady, čas, administrativní náročnost** – dosažení cílů eGC není vždy hlavním kritériem
  - Dosud neexistuje informační systém CC (je ale hotova zadávací dokumentace)
  - OHA by mělo při schvalování investic do IS přísněji vyžadovat kvalitní kalkulaci TCO pro různé varianty provozu IS
  - Dosud se nezačaly systematicky sledovat náklady eGC
    - Náklady MV a NUKIBu na eGC zatím tvořeny jen náklady na zaměstnance (MV cca 5, NUKIB cca 3 až 4)
    - Na r. 2023 naplánován investiční výdaj 30 mil. Kč na realizaci ISCC
  - Tím, že OVS zatím nezapisují využívaný cloud computing do katalogu CC, nelze sledovat nárůst využívání služeb CC ani četnost využívání různých typů služeb CC

Děkuji za pozornost