MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ministerstvo financí
České republiky

NÚKIB

Projekt eGovernment Cloudu

Ing. Miroslav Tůma, Ph.D.

Řídící orgán *eGovernmet Cloudu*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
V4DIS

Agenda

1. Důvody pro vznik eGC
2. Cíle eGC
3. Historie příprav eGC
4. Struktura eGC a jeho služeb
5. Základní pravidla fungování eGC
6. Bezpečnostní úrovně IS v eGC
7. TCO – podklad pro rozhodnutí o využití eGC
8. Dekompozice IS z hlediska využití služeb eGC
9. Katalogy služeb eGC
10. Minimální smluvní podmínky KeGC
11. Řídicí orgán eGC a jeho kompetence
12. Průběh nákupu služby KeGC
13. Řízení a nákup služeb SeGC
14. Harmonogram realizace eGC

eGC

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
V4DIS

Důvody pro vznik eGC

Stav datových center státních institucí

Nízké sdílení IT technologií a aplikací ve VS (*více jak 7.400 ISVS*)

Rostoucí náklady na IS VS (*možné úspory sdílením ICT služeb*)

Nejednotná bezpečnost IS VS

Neexistují pravidla pro přechod veřejné správy do datových center

eGC

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL INFORMATION SOCIETY
V4DIS

Cíle eGC

Zvýšit rozsah sdílení aplikačních služeb VS a tím zefektivnit výdaje na ICT ve veřejné správě

Zrychlit a zefektivnit nákup standardních (komoditních) ICT služeb

Snížit náklady na služby veřejné správy přepočtené na jednu ICT službu a jednoho uživatele

Garance potřebné bezpečnosti a spolehlivosti provozu informačních systémů VS

eGC

Historie příprav eGC

2015:

Akční plán k Národní strategii kybernetické bezpečnosti

Strategie rozvoje ICT služeb veřejné správy

2016:

Strategický rámec Národního cloud computingu – eGC ČR (usnesení Vlády ČR č.1050 z 28.11. 2016)

Ustanovení Pracovní skupiny RVIS pro přípravu vybudování eGovernment cloudu (MV, MF, **NÚKIB, zástupců ústředních orgánů státní správy, zástupců zpravodajských služeb a zástupců odborné veřejnosti)**

- **Cíl: analýza legislativních, technických, ekonomických, organizačních a bezpečnostních podmínek vybudování** eGovernment cloudu
- **Výstup: souhrnná analytická zpráva obsahující kromě analýzy i návrhy opatření** a **doporučení implementačních kroků a standardů pro využívání** cloud computingu ve **veřejné správě**

2018:

Souhrnná analytická zpráva - Projekt Příprava vybudování eGC (usnesení Vlády ČR č.749 z 14.11. 2018)

Pověřen odbor Kybernetické bezpečnosti a koordinace ICT výkonem Řídícího orgánu eGC (ŘOeGC)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
V4DIS

Historie příprav eGC

2019:

Legislativní rozpracování variant eGC (SeGC)

KII a VIS - hodnocení bezpečnostních dopadů a kalkulaci TCO

Zadávací podmínky prvního DNS KeGC

Vypsání prvního kola soutěžních rámců DNS

Vypracování studie proveditelnosti Portálu eGC

eGC

Struktura eGC a jeho služeb

eGovernment Cloud je tvořen:

SeGC – Státní část eGC

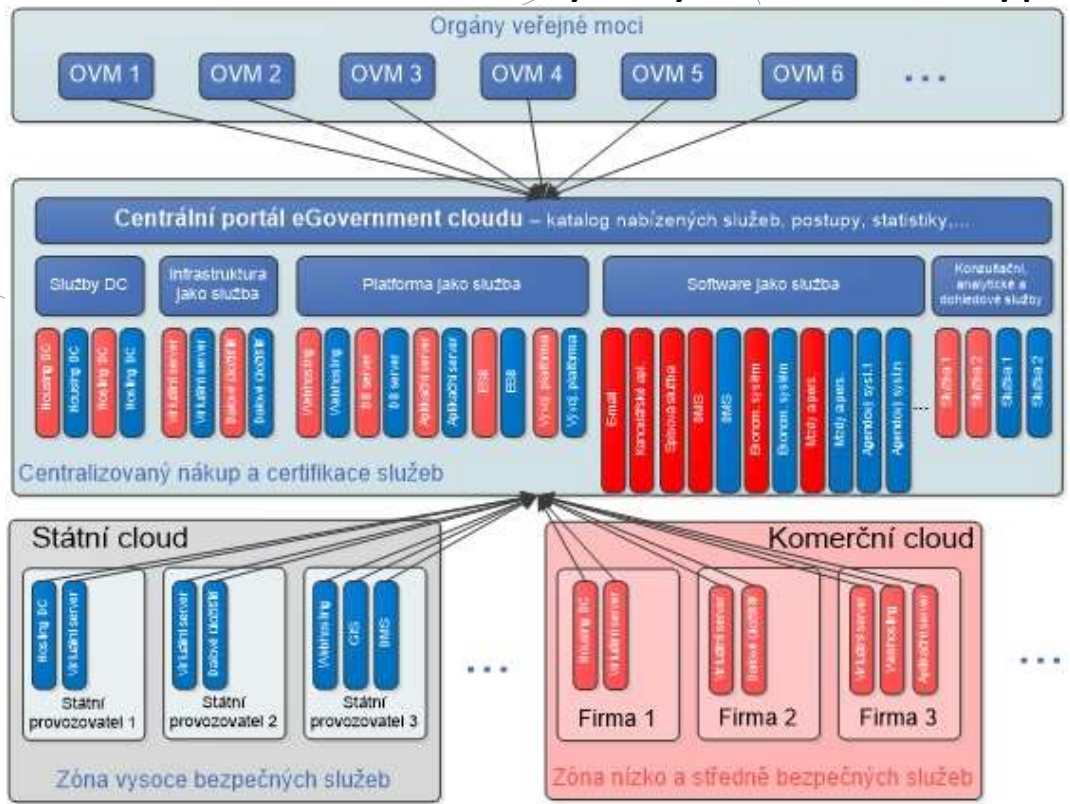
KeGC – Komerční část eGC

Vysoce bezpečnými (*4. bezpečnostní úroveň*) **ICT službami vybraných státních ICT podniků - SeGC**

ICT službami (*1.-3. bezpečnostní úroveň*) **privátních datových center – tzv. komerční cloud (KeGC)**

Hybridní eGC je kombinací služeb KeGC a SeGC, která vychází z principu dekompozice IS na části s různými úrovněmi bezpečnostních dopadů

všechny služby eGC budou nabízeny přes centrální portál eGC



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
V4DIS

Základní pravidla fungování eGC

U každého aktuálně provozovaného IS musí jeho správce určit a sledovat:

- skutečné investiční a provozní náklady
- požadovanou a aktuální bezpečnostní úroveň

Určení služeb eGC – ŘOeGC bude identifikovat identické nebo podobné ICT služby, které budou postupně standardizovány

Provozovatelé SeGC si nebudou konkurovat mezi sebou, ani s provozovateli KeGC

Provozovatelé KeGC si budou mezi sebou konkurovat

SeGC poskytuje služby, které nelze poskytovat v KeGC

Na nákup služeb KeGC jsou aplikována pravidla ZZVZ - DNS

Zákazníci SeGC i KeGC uzavírají s vybraným provozovatelem služeb komerční smlouvu o poskytování služeb včetně SLA

Základní pravidla fungování eGC

Pro organizační složky státu (OSS) a jejich IS bude v **první fázi (cca 2 roky) využití služeb eGC také dobrovolné, po schválení příslušné legislativy bude pro** OSS a jejich IS je **uplatněn princip** cloud first**, tj. jestliže dožije technologická infrastruktura stávajícího informačního systému nebo se staví nový či inovovaný informační systém, pak:**

- **OSS musí využít služby eGC nejvyšší úrovně (prioritně** SaaS, pak PaaS, nakonec IaaS**), které naplňují potřeby části nebo celého IS**
- **umístění do eGC je nepovinné tehdy, když správce IS na základě analýzy TCO prokáže, že jiné řešení je ekonomicky výhodnější**

Umístění IS do eGC je dobrovolné pro

- **kraje, města, obce, ČNB, zpravodajské služby, právnické** osoby, v **nichž má stát podíl alespoň** 50%
- **systémy bezpečnostních sborů, pokud provoz těchto systémů souvisí s plněním zákonem jim stanovených úkolů**
- **systémy orgánů činných v trestním nebo soudním řízení, pokud provoz těchto systémů slouží** pro **trestní nebo soudní řízení**
- **systémy v oblasti národní bezpečnosti**

Bezpečnostní úrovně IS v eGC

Každý IS bude zařazen do jedné ze 4 bezpečnostních úrovní

Metodika určení úrovně bezpečnostních dopadů IS 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 budou určovat, jaké maximální úrovně dopadu mohou nastat při narušení důvěrnosti, integrity, dostupnosti jejich IS až po ztrátu dat

Dle úrovně dopadu zařadí IS (nebo její komponentu) do jedné ze 4 úrovní bezpečnosti

Metodika definuje vlastnosti a opatření datového centra a jeho služeb, které musí splnit, jestliže chce dodávat služby dané bezpečnostní úrovně

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

isss LOCAL AND REGIONAL INFORMATION SOCIETY

Bezpečnostní úrovně IS v eGC

Úroveň dopadu		Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita)								
		A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Povinnosti ze zákona	D. Trestně-právní jednání	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz OVM	H. Ztráta důvěryhodnosti	I. Finanční ztráty
1	nízká	žádné	Porušení etických							
2	střední	Pravd pove (ohro osobn bezpe svobo zrane nebo osob.								
3	vysoká	Pravd pove (ohro osobn bezpe svobo zrane skupi								
4	kritická	Může ohrož jedné několi								

Stanovení požadavků na bezpečnost	základní požadavky na SLA cloudové služby				Dopady narušení dostupnosti										Ztráta dat						Úrovně důvěrnosti			Úrovně integrity		
	dostupnost	úroveň redundance	přípustná doba výpadku		Nedostupnost 15 min.	Nedostupnost 1h	Nedostupnost 4h	Nedostupnost 8h	Nedostupnost 16 hod.	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (24hod.)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Neúmyslná modifikace (chyba)	Systémová chyba	Úmyslná modifikace
			jedinečný	kumulovaný																						
nízká	99,0%	Podpora a servis pouze v pracovní dny a ve stanovené pracovní době. Smluvní penále při výpadku dostupnosti delší než jednotlivě 48 hod. (nezapočítávají se dny pracovního volna a dny pracovního klidu) nebo celkem 3,65 dní za rok (odpovídá 99,0%)	do 48 hod.	do 87,6 hod.	1							2	2	2	Pro časové intervaly, kde se dopady mění z hodnoty 1 na 2, popř. z hodnoty dopadu 2 na 3 je doporučeno vyjasnit výši nákladů, které mají OVM s dodatečnou rekonstrukcí dat z jiných zdrojů (např. papírové formuláře) oproti nákladům spojeným s vyšší frekvencí vytváření záloh dat.					1	1 Nízké požadavky na důvěrnost dat dle matice dopadů.			1 Nízké požadavky na integritu dat dle matice dopadů.		
střední	99,8%	Smluvní penále při výpadku dostupnosti služby delší než celkem 16 hodin za rok (odpovídá 99,8% s vyhodnocením na roční bázi), a dále v případě jednotlivých výpadků delších než 4 hodiny.	do 4 hod.	do 16 hod.	1		2	2	2	3	3	3	3							2	2 Střední požadavky na důvěrnost dat dle matice dopadů. V případech, kdy je vyžadována ochrana právními předpisy je nutné zvážit úroveň eGC "vysoká".			2 Střední požadavky na integritu dat dle matice dopadů.		
vysoká	99,9%	Fault-tolerantní systém s geo-redundantním uložením dat. Smluvní penále při výpadku dostupnosti služby delším než celkem 8,64 hodin za rok, nebo delším než celkem 43 minut měsíčně. SLA zahrnuje vyhodnocení dostupnosti na měsíční bázi (43 minut odpovídá 99,9% na měsíční bázi), tzn. jakýkoli jeden nebo celkový kumulovaný výpadek delší než 43 minut za měsíc je penalizován.	do 43 min.	do 8,64 hod.	1	3	3	3	3	3	4	4	4							3	3 Vysoké požadavky na důvěrnost dat dle matice dopadů, popř. je ochrana vyžadována právními předpisy.			3 Vysoké požadavky na integritu dat dle matice dopadů.		
kritická	99,99%	Plně fault-tolerantní systém s geo-redundancí a replikací transakčních dat. Smluvní penále při výpadku dostupnosti služby delší než celkem 52 minut za rok (odpovídá 99,99%). Cloudové služby v této úrovni dopadu budou mít smluvně dané max. doby RPO / RTO.	do 15 min.	do 52min.	1-2	3-4														4	4 Kritické požadavky na důvěrnost dat dle matice dopadů.			4 Kritické požadavky na integritu dat dle matice dopadů.		

TCO – podklad pro rozhodnutí o využití eGC

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. Metodika umožňuje porovnat celkové náklady různých variant provozu IS (zejména varianty eGC a varianty in-house provozu).

Metodika TCO řeší:

- **přehledné vymezení (definice) všech relevantních nákladů, které jsou uplatňovány jak při pořízení, tak při provozu ICT služeb v režimu** on-premise
- **popis nákladových položek, který bude plnit roli návodu a umožní správci IS určit hodnoty jako vstupy do kalkulace ekonomické výhodnosti**
- **stanovení hodnot pro ty nákladové položky, které lze obecně uplatnit** pro **každou kalkulaci ICT služby napříč potřebami všech** IS, tyto **údaje mají doporučující charakter a vycházejí** z **příkladů dobré praxe, zkušeností některých správců IS s kalkulací nákladů ICT služeb** v **předešlých letech, nebo legislativního vymezení**
- **porovnání ekonomické výhodnosti ICT služby** v **režimu on**-premise s **pořízením ICT služby** v **prostředí** eGC, a to na **všech požadovaných úrovních (**SaaS, PaaS, IaaS **–** podle povahy ICT **služby)**

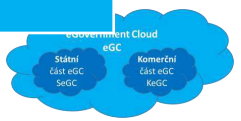
Kalkulace TCO služby v režimu on-premise musí vzít v úvahu náklady na případné uvedení on-premise prostředí do souladu s požadavky bezpečnostní úrovně služeb eGC **určené pro daný IS (bezpečnostní opatření odpovídající bezpečnostním standardům a opatřením)**

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

ISSS V4DIS

TCO – calkulator

Souhrnná položka modelu TCO - nákladová kategorie
A. Předběžné analýzy, tvorba zadání, výběr řešení a dodavatele – náklady nákupního procesu
B. Nákup SW a HW pro projekt (ne v případě SaaS)
C. Analýza, vývoj, implementace a zkušební provoz
D. Provoz a podpora řešení HW a SW (ne v případě SaaS)
E. Hardware/Software údržba a průběžné úpravy (ne v případě SaaS)
F. Projekty postupné inovace a zlepšování (pokud se uskutečnily)
G. Projekty upgrade (pokud se uskutečnily)
H. Zvýšené náklady užívání řešení (pokud se vyskytly)
I. Konzervace a ukončení řešení (u posuzovaných řešení ještě nenastala)
X. Náklady na předplatné ICT služby, plus všechny odpovídající přímé int. náklady (pouze SaaS)
Z. Ostatní, k fázi životního cyklu nepřiřaditelné náklady



Katalog služeb eGC

Katalog služeb eGC je seznam služeb eGC, který definuje strukturu, hierarchii **a parametry služby eGC.**

Katalogový list služby eGC je popis jedné služby, určuje zejména parametry pro definici příslušné služby.

Vzhledem k **použitým soutěžním a nákupním mechanismům** KeGC **je katalog služeb eGC ve skutečnosti tvořen sadou souvisejících katalogů s** jednotnou strukturou:

Rámcový katalog služeb eGC – popisuje strukturu a **hierarchii služeb** eGC**, jejich povinné parametry, minimální smluvní podmínky a další související informace. Slouží zároveň jako primární společná struktura služeb pro všechny ostatní katalogy** KeGC i SeGC**. Je vytvořen a udržován ŘOeGC**.

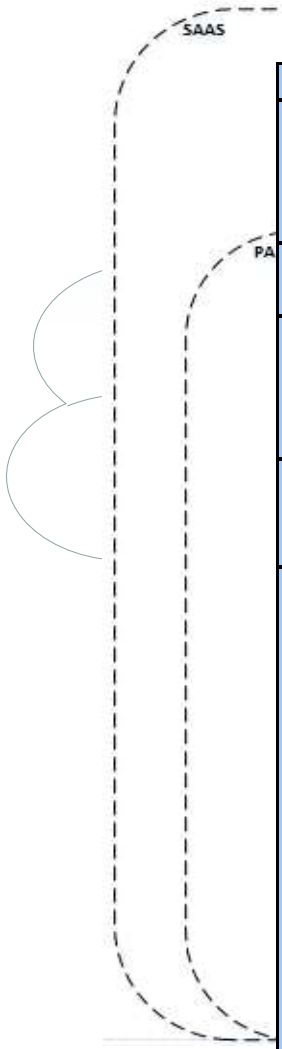
Katalog tržní nabídky služeb KeGC obsahuje obecné nabídky dodavatelů KeGC**, včetně detailních parametrů služby a indikativních cen. Strukturu katalogu a strukturu parametrů služeb určuje ŘOeGC, jeho obsah naplňují potenciální dodavatelé** KeGC.

Katalog poptávek služeb KeGC obsahuje konkrétní zadání minitendrů soutěžního mechanismu KeGC. **Jednotlivá zadání jsou tvořena zákazníky** eGC.

Katalog závazných nabídek služeb KeGC obsahuje závazné nabídky dodavatelů KeGC **včetně cen, odpovědí na poptávky služeb** eGC v **jednotlivých** minitendrech.

Katalog služeb SeGC obsahuje seznam a **popis detailně definovaných, přímo objednatelných služeb** eGC, **vytvořený provozovatelem** SeGC **ve spolupráci a** pod kontrolou **ŘOeGC**.

Katalog služeb eGC



Identifikace SL	Třída služby	Jednotka
Housing	RP v DC Tier III (800x1200)	Rack pozice s včetně racku
	RP v DC TIER III (600x1200)	
	1kWhpm	Příkon v hodnotě 1kW za měsíc
	Instalace zařízení	Jedno zařízení jednorázově
Správa DWDM	Critical	Lambda služba za měsíc
	High	
Správa Firewall a LB	FW - Box	zařízení za měsíc
	FW - Virtual	
	LB - Box	
	LB - Virtual	
Správa LAN	Typ: Low	100Mbps Port za měsíc
	Typ: Middle	1Gbps Port za měsíc
	Typ: High	10Gbps Port za měsíc
Internet access	Internet	10 Mbps za měsíc
	Internet	20 Mbps za měsíc
	Internet	30 Mbps za měsíc
	Internet	50 Mbps za měsíc
	Internet	100 Mbps za měsíc
	Internet	500 Mbps za měsíc
	Internet	1000 Mbps za měsíc
	Veřejné IP adresy**	Plus 16 veřejných IP adres jednorázově
	Doplňkové služby 10 Mbps*	Web proxy a filtr obsahu Služba za měsíc
		E-mail Antivir/Antispam Služba za měsíc
	Doplňkové služby 20 Mbps*	Web proxy a filtr obsahu Služba za měsíc
		E-mail Antivir/Antispam Služba za měsíc
	Doplňkové služby 30 Mbps*	Web proxy a filtr obsahu Služba za měsíc
		E-mail Antivir/Antispam Služba za měsíc
	Doplňkové služby 50 Mbps*	Web proxy a filtr obsahu Služba za měsíc
		E-mail Antivir/Antispam Služba za měsíc
VPN gateway	VPN Gateway	1 concurrent user za měsíc

Minimální smluvní podmínky KeGC

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 ISVS 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. (odpovídá 99,99%)

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

Řídicí orgán eGC

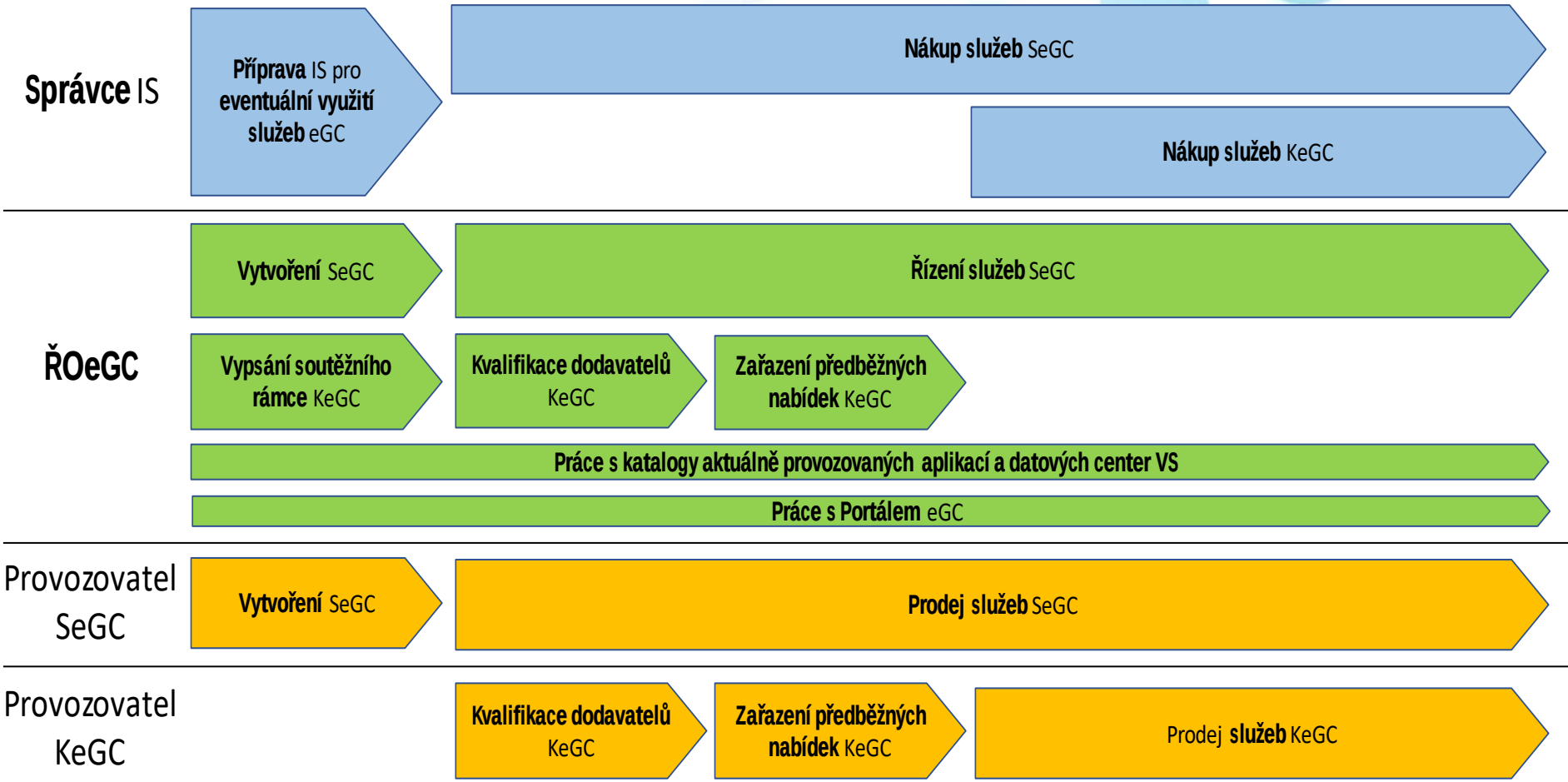
Řídící orgán eGC - ŘOeGC (*obdoba Government Digital Service ve Velké Británii nebo Úradu podpredsedu vlády SR pre investície a informatizáciu na Slovensku*)

ŘOeGC řídí rozvoj a provoz státní i komerční částí eGC

ŘOeGC zřídí ministr vnitra jako nový útvar v rámci MV ČR

ŘOeGC bude **využívat meziresortní poradní** sbor **složený ze zástupců Ministerstva vnitra, Ministerstva financí a NÚKIB, zástupců zpravodajských služeb, zástupců ústředních orgánů státní správy, zástupců orgánů veřejné správy a zástupců odborné veřejnosti**

Procesy eGC

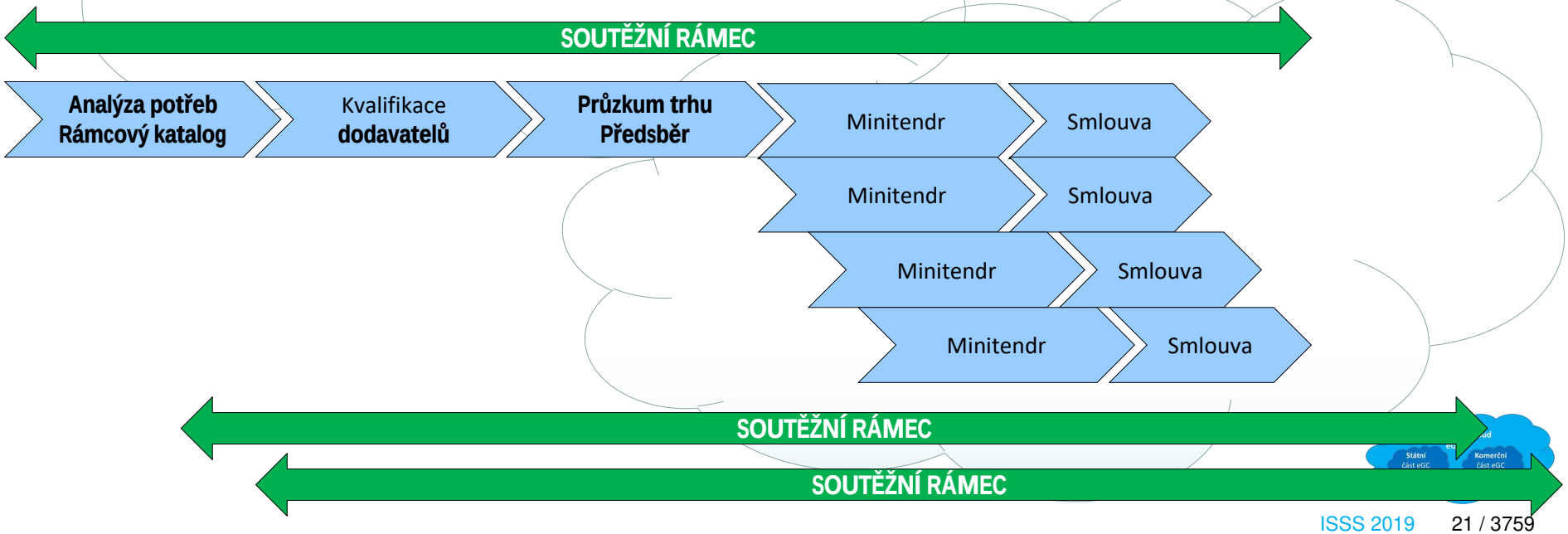

Správce IS
Příprava IS pro eventuální využití služeb eGC
Nákup služeb SeGC
Nákup služeb KeGC
ŘOeGC
Vytvoření SeGC
Řízení služeb SeGC
Vypsání soutěžního rámce KeGC
Kvalifikace dodavatelů KeGC
Zařazení předběžných nabídek KeGC
Práce s katalogy aktuálně provozovaných aplikací a datových center VS
Práce s Portálem eGC
Provozovatel SeGC
Vytvoření SeGC
Prodej služeb SeGC
Provozovatel KeGC
Kvalifikace dodavatelů KeGC
Zařazení předběžných nabídek KeGC
Prodej služeb KeGC

Průběh nákupu služby KeGC

Pro nákup služeb z KeGC se využívá dvoustupňový soutěžní mechanismus DNS s centrálním zadáváním. Mechanismus umožňuje průběžné zapojování dalších zadavatelů (zákazníků KeGC) a dodavatelů/provozovatelů služeb eGC

Soutěžní mechanismus KeGC je organizován v pevně daných, obsahově a časově vymezených **soutěžních rámcích** - soutěžní rámce se mohou časově překrývat a mohou v nich platit různá pravidla

Katalog služeb eGC bude realizován rozdělením do několika paralelních soutěžních rámců podle typu služby (např. oddělení IaaS/PaaS a SaaS) nebo podle bezpečnostních úrovní



Řízení a nákup služeb SeGC

ŘOeGC:

prověřuje a schvaluje **požadavky věcných správců IS na využití služeb** SeGC

prověřuje naplnění bezpečnostních a provozních požadavků provozovatelem SeGC

určuje potřebnou kapacitu služeb SeGC v **jednotlivých časových obdobích**

nastavuje s provozovatelem SeGC **nabídkové parametry služeb** SeGC (*zejména vzorová SLA a jednotkové nabídkové ceny*)

zveřejní na **portálu eGC katalog služeb** SeGC **ve stejné struktuře** jako katalog **služeb** KeGC

spolupracuje na migraci IS do SeGC

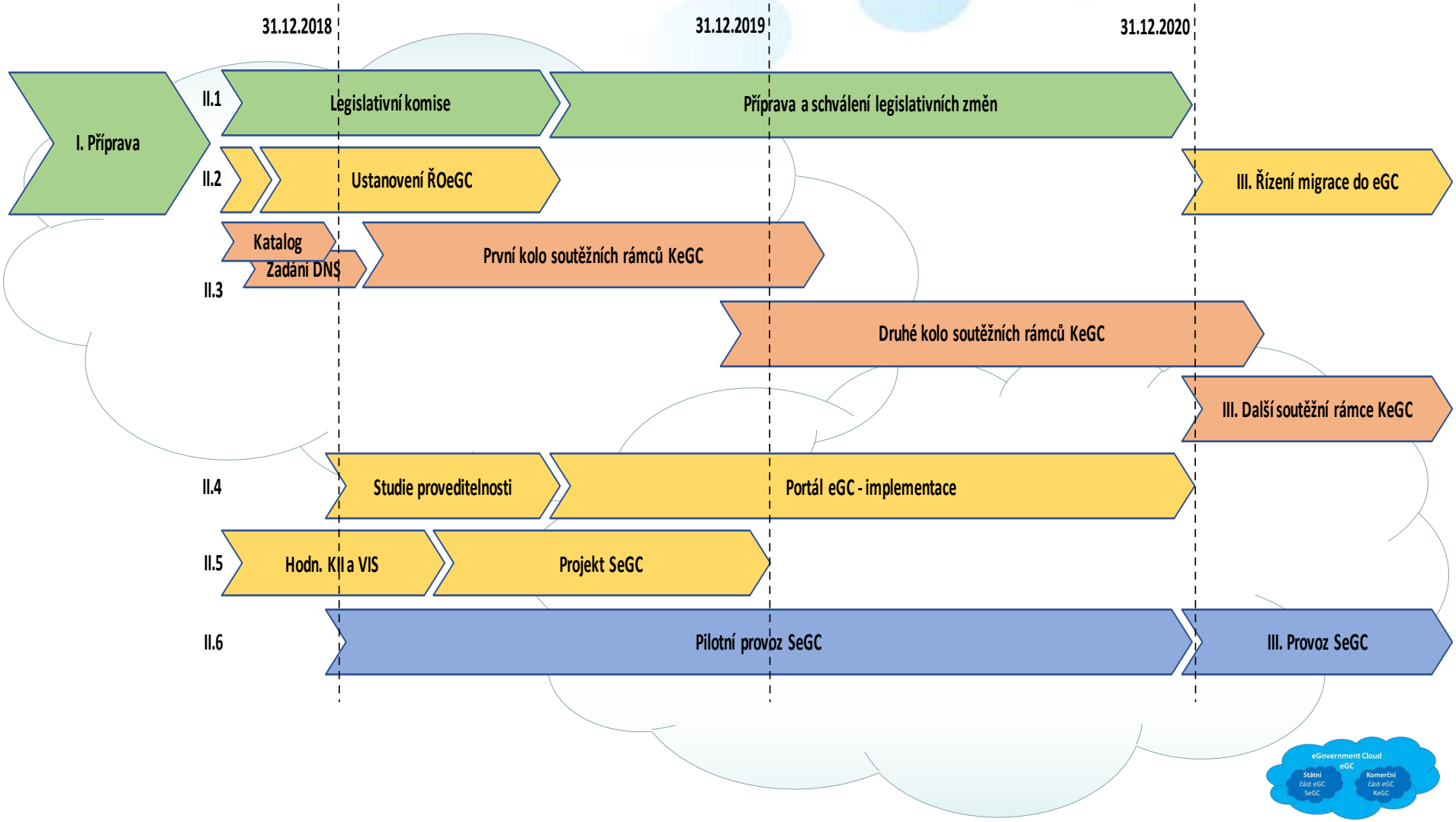
monitoruje migraci IS do SeGC

monitoruje **provoz služeb** SeGC

Věcný správce IS:

Na základě katalogu služeb SeGC dohodne s provozovatelem SeGC **poskytované služby** a **uzavře** smlouvu

Harmonogram realizace eGC



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ministerstvo financí
České republiky

NÚKIB

… děkuji za pozornost a Váš čas.