Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

~~Title: Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR~~

Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR

Tato kapitola nahlíží na sdílené služby, funkční celky a tematické oblasti veřejné správy ČR tzv. „shora“ a přináší jak definice klíčových pojmů a prvků architektury VS, tak přehled centrálních sdílených služeb eGovernmentu, dostupných pro použití v lokálních architekturách úřadů. Základní pilíře a budoucí směry rozvoje eGovernmentu lze postihnout dále popsanými klíčovými sdílenými službami, funkčními celky či tematickými oblastmi. Jejich prostřednictvím jsou poskytovány centrální sdílené služby eGovernmentu i sdílené agendové služby, které jsou souhrnně zahrnuty do architektonické vize eGovernmentu. V této části popisované sdílené služby, funkční celky a tematické oblasti je povinné zohlednit v informační koncepci úřadu a v architektuře úřadu na základě zákona 365/2000 Sb. a Informační koncepce ČR dle Způsobů využívání sdílených služeb, funkčních celků a tematických oblastí úřady.

Tematické oblasti

- **Agendový model veřejné správy**
- **Propojený datový fond - PPDF**
- **Veřejný datový fond ČR - VDF**
- **Úplné elektronické podání - ÚEP**
- **Integrace informačních systémů**
- **Portály veřejné správy a soukromoprávních uživatelů údajů**
- **Přístupnost informací**
- **Elektronická fakturace - eFaktura**

Sdílené služby a funkční celky

- **Portál občana a portál veřejné správy - PO, PVS**
- **Elektronická identifikace pro klienty veřejné správy – NIA**
- **Univerzální kontaktní místo veřejné správy - CzechPOINT**
- **Systém správy dokumentů - eSSL**
- **Systémy a služby spojené s právním řádem a legislativou**
- **Elektronické úkony a doručování - Datové schránky**
- **Jednotný identitní prostor veřejné správy – JIP/KAAS**
- **Jednotné obslužné kanály a uživatelská rozhraní úředníků**
- **Sdílené agendové IS v přenesené působnosti**
  - například pro agendy v přenesené působnosti Živnostenský rejstřík, Evidence obyvatel, Evidence řidičů a Registr motorových vozidel, Informační systém technické infrastruktury atd.
- **Sdílené agendové IS pro samostatnou působnost územních samospráv**
- **Sdílené provozní informační systémy**
  - například Informační systém státní služby, Integrovaný informační systém státní pokladny, Národní elektronický nástroj, MS2014+ atd.
- **Sdílené statistické, analytické a výkaznické systémy**
  - například Business Inteligence
- **eGovernment Cloud**
- **Národní datová centra**
- **Komunikační infrastruktura veřejné správy- KIVS/CMS**

Agendový model veřejné správy

Popis Agendového modelu veřejné správy

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

Agendový model výkonu veřejné správy

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

Agendy veřejné správy

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

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

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

1. Ohlašovatelem je OVM, který je gestorem dané právní úpravy a má tedy povinnost agendu a údaje o ní zapsat do Registru práv a povinností. Součástí ohlášení jsou:
2. Referenční údaje o agendě
    - název agendy a její číselný kód, které jsou součástí číselníku agend,
    - čísla a názvy právních předpisů a označení jejich ustanovení, na jejichž základě orgán veřejné moci vykonává svoji působnost, nebo na jehož základě je soukromoprávní uživatel údajů oprávněn k využívání údajů ze základních registrů nebo agendových informačních systémů,
    - výčet a popis činností, které mají být vykonávány v agendě,
    - výčty činnostních rolí,
    - výčet a popis úkonů orgánů veřejné moci vykonávaných v rámci agendy na žádost subjektu, který není orgánem veřejné moci, identifikátor úkonu, vymezení subjektu, který může podat žádost, a forma úkonu,
    - výčet orgánů veřejné moci a soukromoprávních uživatelů údajů, kteří agendu vykonávají, nebo jejich kategorie,
    - název ohlašovatele agendy a jeho identifikátor orgánu veřejné moci,
    - výčet orgánů veřejné moci, které byly pro výkon agendy zaregistrovány, a jejich identifikátor orgánu veřejné moci,
    - výčet údajů vedených nebo vytvářených podle jiného právního předpisu v rámci agendy; to neplatí pro zpravodajské služby,
    - výčet údajů vedených v základních registrech zpřístupněných prostřednictvím informačního systému základních registrů pro výkon agendy a rozsah oprávnění k přístupu k těmto údajům,
    - výčet údajů vedených v jiných agendových informačních systémech zpřístupněných prostřednictvím referenčního rozhraní pro výkon dané agendy a rozsah oprávnění k přístupu k těmto údajům,
    - číslo a název právního předpisu a označení jeho ustanovení, na jehož základě je orgán veřejné moci nebo soukromoprávní uživatel údajů oprávněn využívat údaje ze základních registrů nebo z

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

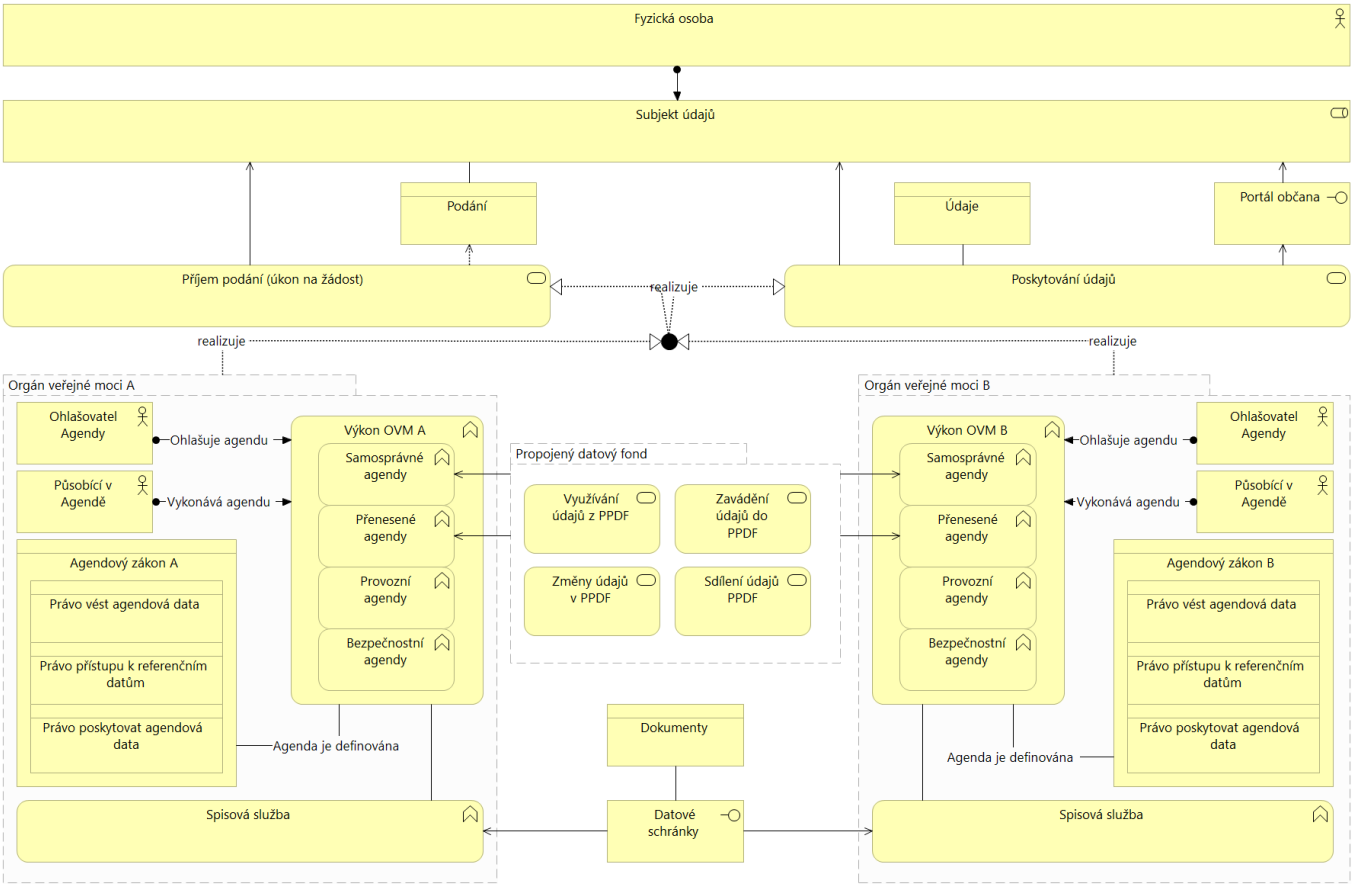
Klíčové role OVS v agendovém modelu

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

Klíčové role OVS v agendovém modelu veřejné správy	**Role**	**Popis/význam hlavní činnosti**
Ohlašovatel agendy	OVM, který je zodpovědný za legislativní rámec agendy, a tedy určuje i základní parametry jejího výkonu	Je gestorem právních předpisů; koordinuje výkon agendy; metodicky řídí výkon agendy; ohlašuje agendu v RPP a její podrobnosti; stanovuje působnost OVM; poskytuje buď centralizovaný AIS, nebo podmínky a standardy pro decentralizované řešení; ohlašuje a spravuje údaje v RPP, včetně údajů v rejstřících OVM a SPUU; v případě centralizovaného AIS poskytuje údaje přes referenční rozhraní ISVS
Orgán veřejné moci působící v agendě	OVM, který působí v dané agendě. To znamená, že vykonává fakticky nějakou činnost v rámci dané agendy a k tomu využívá buď centrálně poskytnutý AIS, nebo svůj vlastní	Přihlašuje se k působnosti; vykonává jemu svěřené činnosti úředníky v jejich činnostních rolích; zapisuje do RPP údaje o své působnosti; využívá centralizovaný AIS nebo spravuje vlastní; eviduje a spravuje údaje v agendě; vykonává případně funkce editora údajů

Klíčové role OVS v agendovém modelu veřejné správy	Role	Popis/význam hlavní činnosti
Soukromoprávní uživatel údajů	Subjekt, který má na základě zákona oprávnění k přístupu k údajům v základních registrech či AISech a přistupuje k nim prostřednictvím AIS spravovaného k tomu určeným OVM	Využívá údaje podle oprávnění
Správce centralizovaného AIS pro výkon agendy	OVM, který na základě zákona spravuje centralizovaný AIS a poskytuje ho OVM působícím v agendě	Spravuje centralizovaný AIS; zpřístupňuje AIS uživatelům působících OVM; realizuje využívání referenčních údajů ze základních registrů do centralizovaného AIS; poskytuje podporu uživatelům; řeší integrační vazby AIS na další systémy
Správce vlastního AIS, pokud není k dispozici centralizovaný AIS	Jednotlivé OVM, které pro podporu agendy využívají svůj vlastní agendový IS, protože není k dispozici sdílené centralizované řešení	Spravuje svůj vlastní AIS; zapisuje údaje o svém AIS do RPP; řeší vazby na základní registry; řeší vazby na další ISVS; řeší vazby na další svoje informační systémy; spravuje a udržuje datový fond ve svém AISu
Orgán veřejné moci spravující AIS pro přístup soukromoprávních uživatelů	OVM, který na základě zákona vytváří a provozuje AIS, jehož prostřednictvím mohou soukromoprávní uživatelé přistupovat k údajům ze základních registrů či jiných AISů	Spravuje AIS pro SPÚ; zpřístupňuje funkce AISu soukromoprávním uživatelům; realizuje dohled nad oprávněním k využívání údajů; poskytuje soukromoprávním uživatelům údaje; zajišťuje realizaci reklamací údajů od SPÚ k editorům údajů

Pohled na ohlašovatele a vykonavatele agendy



Pravidla Agendového modelu veřejné správy

Základní povinnosti ohlašovatele agendy

Ohlašovatel agendy je podle zákona č. 111/2009 Sb., o základních registrech zodpovědný za řádné ohlášení agendy a za aktualizace agendy, a především za správnost a pravdivost údajů uvedených v agendě. Zjistí-li kdokoliv nesoulad reality s údaji, měl by to jako u dalších referenčních údajů ohlásit ohlašovateli, a ten musí agendu upravit do souladu se skutečností. To se netýká jen základních informací, ale i všech dalších referenčních a nereferenčních údajů, jako jsou činnosti, působnosti OVM, údaje v agendě, agendové informační systémy apod.

Základními povinnostmi ohlašovatele jsou:

- Tam, kde je gestorem legislativy, dodržovat veškeré principy pro legislativu, včetně zásad Digitálně přívětivé legislativy
- Ohlásit agendu
- Ohlásit každou její změnu
- Ohlásit působnost všech OVM a definovat výkon jim svěřených činností
- Zajistit využívání údajů ze základních registrů a související oprávnění pro jejich využívání pro podporu výkonu agendy
- Ohlásit agendové informační systémy, které spravuje a které jsou poskytovány OVM působícím v agendě
- Ohlásit údaje v agendě vedených, čerpaných i poskytovaných
- K centralizovaným agendovým informační systémům vydávat provozní řád
- Metodicky řídit výkon agendy u OVM, který v agendě působí
- Spravovat, tzn. ohlašovat a udržovat aktuální, údaje v rejstříku OVM/SPUU. U SPUU se jedná o všechny subjekty, které jsou povinné dle právních předpisů spadající do agendy, jejichž je OVM ohlašovatel. Ohlašovat může ustanovit jiné OVM, které bude tyto úkony činit.

Základní povinnosti OVM působícího v agendě

V rámci agendy veřejné správy mohou veřejnoprávní činnosti vykonávat pouze ty orgány veřejné moci, které jsou v rámci ohlášení agendy vyznačeny jako orgány veřejné moci vykonávající působnost, a to v rámci konkrétních činností. To znamená, že po aplikaci principu referenčních údajů v Registru práv a povinností lze konstatovat, že pokud v rámci dané agendy vykonává veřejnoprávní činnost orgán veřejné moci, který nemá vyznačenou působnost, jedná se o porušení zákona a ohlašovatel agendy musí neprodleně toto napravit. To se týká nejen samotného seznamu působících orgánů veřejné moci, ale také přiřazení jejich činností. Výkon činnosti je byznysovou vazbou a odborně jej nazýváme "činnostní rolí".

Základními povinnostmi orgánů veřejné moci působících v agendě tedy jsou:

- Vykonávat činnosti dle ohlášení agendy
- Pokud OVM zjistí nesoulad skutečnosti a údajů v ohlášení agendy, je povinen požadovat po ohlašovateli nápravu.
- Pokud sám spravuje agendový informační systém pro výkon agendy (není poskytován centrálně), ohlásit tento systém do RPP jako ISVS.
- Pokud existuje centralizovaný agendový informační systém, tak tento využívat.
- Přistupovat k údajům v základních registrech a dalších ISVS výhradně na základě oprávnění ohlášeného v agendě.
- Spravovat jen ty údaje, které jsou ohlášeny v dané agendě.
- Pokud zjistí nesoulad referenčních údajů v jednotlivých základních registrech se skutečností, zahájit proces reklamace u příslušného editora.

Propojený datový fond

Veřejný datový fond

Úplné elektronické podání

Integrace informačních systémů

Portály veřejné správy a soukromoprávních uživatelů údajů

Přístupnost informací

Popis Přístupnosti informací

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

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

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

Obecně o přístupnosti

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

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

Pravidla Přístupnosti informací

Legislativní rámec pro přístupnost

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

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

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

1. OZP musí mít možnost využívat všechny služby veřejné správy jako kdokoliv jiný
2. OZP musí mít možnost plnohodnotně využívat elektronické služby stát i elektronické služby subjektů veřejného sektoru
3. Existuje zde obecná absolutní povinnost přístupnosti výsledků všech veřejných zakázek či zakázek podle legislativy k VZ, pokud jsou jejich výsledky určeny pro jakékoliv užívání fyzickými osobami, to se pochopitelně vztahuje i obecně na veškeré ICT zakázky.
4. Subjekty veřejného sektoru musejí mít svoje informace přístupné a to zejména na internetových stránkách a ve svých aplikacích
5. Přístupnost se vztahuje i na veškeré informační systémy pro zaměstnance, protože ani zaměstnanec s OZP nesmí být diskriminován tím, že není schopen pracovat se svým pracovním systémem

Standardy a metodiky

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

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

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

Architektonická řešení

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

požadavků na dodavatele. Je tedy nutno architektonicky a realizačně zajistit:

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

Elektronická fakturace

Popis elektronické fakturace

Elektronická fakturace (také jako „e-fakturace“ či „efakturace“) je moderní prostředek, jehož primárním cílem je usnadnit a zefektivnit ekonomickým subjektům odesílání, příjem e-faktur a jejich následnou archivaci k dalšímu zpracování v rámci Evropské unie. E-faktura je dokumentem v digitální podobě (elektronickým dokumentem) podle ustanovení § 2 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů a nařízení eIDAS. Může být doručena ve strukturovaném nebo nestrukturovaném datovém formátu. Může být účetním záznamem podle zákona č. 563/1991 Sb., o účetnictví, daňovým dokladem podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, může sloužit i pro jiné účely (např. jako dodací list, záruční list, důkazní prostředek apod.)

E-fakturace v kombinaci s řádně vedenou spisovou službou dle zákona č.499/2004 Sb., o archivnictví a spisové službě a s ekonomickým informačním systémem uzpůsobeným pro zpracování elektronických faktur nabízí ekonomickým útvarům orgánů veřejné správy:

- Snížení administrativní a transakční zátěže následováno s výrazným zvýšení produktivity při zacházení s daňovými doklady
- Rychlá a snadná dohledatelnost daňového dokladu
- Bezpečný a spolehlivý prostředek v kombinaci s kvalifikovanými prostředky pro vytváření důvěryhodného podpisu dle nařízení eIDAS č.910/2014
- Zajištění přeshraniční interoperability e-fakturace v rámci Evropské unie

Ekonomické aspekty

Evropská komise předpokládá, že „Masové přijetí elektronické fakturace v EU by vedlo k významným hospodářským přínosům a odhaduje se, že přechodem od papírových faktur k fakturám elektronickým se za období šesti let ušetří přibližně 240 miliard EUR.“1. Na základě tohoto zjištění „Komise chce, aby se elektronická fakturace stala převládající metodou fakturace v Evropě do roku 2020.

Jako prostředek k dosažení tohoto cíle má směrnice 2014/55/EU o elektronické fakturaci při zadávání veřejných zakázek za cíl usnadnit používání elektronických faktur hospodářskými subjekty, které dodávají zboží, práce a služby pro orgány veřejné správy (B2G), jakož i podporovat obchodování mezi samotnými hospodářskými subjekty (B2B). Vymezuje především právní rámec pro zavedení a přijetí evropské normy (EN) pro sémantický datový model vytvořený ze základních prvků elektronické faktury (EN 169311:2017).

Norma EN 169311:2017 a její pomocné normalizační výstupy umožní sémantickou interoperabilitu elektronických faktur a pomohou odstranit bariéry na trhu a překážky v obchodu vyplývající z existence rozdílných vnitrostátních právních předpisů a norem – a přispějí tak k dosažení cílů stanovených Evropskou komisí.

Práce s elektronickými fakturami, ale zejména elektronizace celého nákupního řetězce od sběru požadavků, veřejné výběrové řízení, přes objednávku/smlouvu, potvrzení dodávek, fakturu, po platbu a rozúčtování výdajů/nákladů přinese významné úspory transakční i úspory spojené s lepším rozhodování a mnohem snáze a lépe provedenými řídícími kontrolami (1., 2., 3. a 4.) podle zákona č. 320/2001 Sb. o finanční kontrole a vyhlášky č. 416/2004 Sb., kterou se provádí zákon o finanční kontrole.

Pravidla elektronické fakturace

Povinnost akceptovat elektrickou fakturu (de standardů níže) se dle zákona č. 134/2016, o zadávání veřejných zakázek, ve znění pozdějších předpisů týká všech orgánů veřejné moci, kteří přijímají platbu plnění veřejné zakázky. Tato povinnost platí od 1. 1. 2019 pro ústřední orgány moci a od 1.4.2020 pro uzemní samosprávu §279 (5) b) zákona č. 134/2016, o zadávání veřejných zakázek, ve znění pozdějších předpisů. Všechny povinné orgány veřejné moci musí kromě procesních změn zajistit i příjem a vydávání elektronických faktur dle evropských a českých pravidel.

Technické aspekty

E-fakturaci je možné implementovat a realizovat ve svých organizačních jednotkách za dodržení jednoho z následujících technických standardů, který je v souladu se směrnicí 2014/55/EU:

- Evropská norma pro elektronickou fakturaci EN 16931-1:2017 - otevřená a zdarma dostupná na této stránce
- Syntaxe dle Evropské směrnice 2014/55/EU čl. 3, odst. 2
- XML zprávu meziodvětvové faktury UN/CEFACT podle XML schémat 16B (SCRDM - CII)
- UBL zprávy faktury a dobropisu podle ISO/IEC 19845:2015

Je třeba zmínit, že směrnice 2014/55/EU:

- nepředepisuje, která syntaxe by měla být použita pro elektronickou fakturaci v rámci veřejné zakázky. Pouze uvádí, které syntaxe jsou veřejní zadavatelé povinni akceptovat. Je zcela možné a velmi pravděpodobné, že jiné syntaxe, které nejsou uvedeny na seznamu výše, se budou i nadále používat, a to i pro přeshraniční výměny, zvláště tam, kde již existuje rozšířená národní nebo místní praxe. To je případ českého národního formátu elektronické faktury ISDOC (Information System Document), verze 5.2 a vyšší (který je definován vyhláškou č.194/2009 Sb a který musí být dle Usnesení vlády č. 347/2017 akceptován veřejnoprávními subjekty od 1.1.2019). Tento formát logicky není součástí výše uvedené směrnice, jakkoli je syntaxi UBL 2.1 velmi blízký, jelikož vychází z verze UBL 2.0. V rámci vnitřního trhu České republiky je formát ISDOC velmi široce rozšířen, zejména mezi soukromoprávními subjekty, které ve veřejné zakázce figurují v roli dodavatele, tedy vystavitele faktury.
- neponechává veřejným zadavatelům žádný prostor odmítnout fakturu ve kterékoliv ze syntaxí, které jsou uvedeny na seznamu, jenž bude zveřejněn v Úředním věstníku Evropské unie, v návaznosti na článek 3 směrnice. Článek 7 jasně uvádí, že veřejní zadavatelé a zadavatelé v EU musí přijímat a zpracovávat elektronické faktury, které splňují normu a odpovídají kterékoli ze syntaxí uvedených na zveřejněném seznamu.

Právní aspekty

Implementace e-fakturace do prostředí veřejné správy České republiky je dána směrnicí 2014/55/EU, která nabyla účinnosti 19. 4. 2018. K tomuto datu je také nutné mít ve svých spisových službách v rámci organizace nastavené technickoorganizační opatření, která budou v souladu s výše uvedenou směrnicí a technickými standardy z ní vyplývající. Směrnice byla inkorporována do české legislativy v rámci § 221 [https://www.zakonyprolidi.cz/cs/2016-134|zákona č. 134/2016, o zadávání veřejných zakázek, ve znění pozdějších předpisů]]. Zadavatel nesmí odmítnout elektronickou fakturu vystavenou dodavatelem za plnění

veřejné zakázky z důvodu jejího formátu, který je v souladu s evropským standardem elektronické faktury.

Všechny veřejné zakázky, které jsou nadlimitní mohou být dodavatelem vyžadovány ve formě e-fakturace.

V neposlední řadě bylo schváleno Usnesení vlády č. 347/2017, které dává povinnost od 1. 1. 2019 Ústředním orgánům státní správy a jimi podřízeným organizačním složkám státu přijímat elektronické faktury ve formátech stanovených Evropskou směrnicí 2014/55/EU a dále ve formátu isdoc/isdocx (Information System Document) verze 5.2 a vyšší

Portál občana a portál veřejné správy

Elektronická identifikace pro klienty veřejné správy

Popis identifikace klientů veřejné správy

Fyzická identifikace

Fyzickou identifikací je myšlena situace, kdy klient veřejné správy je osobně přítomen v místě, kde je mu služba poskytována nebo je po něm vyžadována součinnost. K fyzickému prokázání totožnosti se používají identifikační doklady, které musí obsahovat:

- Aktuální a platné údaje o jeho držiteli
- Fotografii držitele

Jako identifikační doklad se používá **občanský průkaz** a **cestovní pas**. Identifikačním dokladem **není** řidičský průkaz, protože nesplňuje potřebné parametry při jeho vydávání, ačkoliv obsahuje například fotografii držitele.

Aby mohla fyzická identifikace fungovat jak při aktuální potřebě (člověk se v daný čas dostaví na místo), tak i při historické potřebě (ověření platnosti identifikačního dokladu z historické smlouvy), budou služby eGovernmentu poskytované přes Referenční rozhraní rozšířeny o službu, která na jakékoliv historické číslo a typ identifikačního dokladu vrátí, zda byl v požadované době platný a aktuální údaje držitele tohoto historického identifikačního dokladu.

Fyzická identifikace pro osoby bez identifikačního dokladu

Ačkoliv předcházející text předpokládá identifikaci pouze prostřednictvím identifikačních dokladů, existují situace, kdy osoba nemá možnost se tímto identifikačním dokladem prokázat. Typicky jde o děti pod 15 let či cizince. Základním předpokladem, aby mohla proběhnout identifikace i těchto osob je jejich evidence v informačním systému veřejné správy, napojený na propojený datový fond a následné vydávání potvrzení či úřední/veřejnou listinu, které může zastat roli identifikačního dokladu. Pro osoby do 15 let to může být rodný list vedeny v jednom z editorských agendových informačních systémů nebo povolení o přechodném pobytu pro cizince.

Některé z těchto listin - například povolení k trvalému pobytu, azylový štítek či vízový štítek jsou již dnes vedeny v základním registru obyvatel, avšak jejich použití pro identifikaci není plně dořešeno.

Elektronická identifikace

Elektronickou identifikací je myšlena situace, kdy klient veřejné správy není přítomen v místě poskytování služby. Identifikace tedy probíhá vzdáleně, bez fyzického kontaktu.

Pro jednoznačnou elektronickou identifikaci a autentizaci klientů veřejné správy byl vytvořen technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy tuto činnost vykonávat v souladu s Informační koncepcí ČR a bez nutnosti vytváření vlastních nákladných řešení a zvyšování administrativní zátěže.

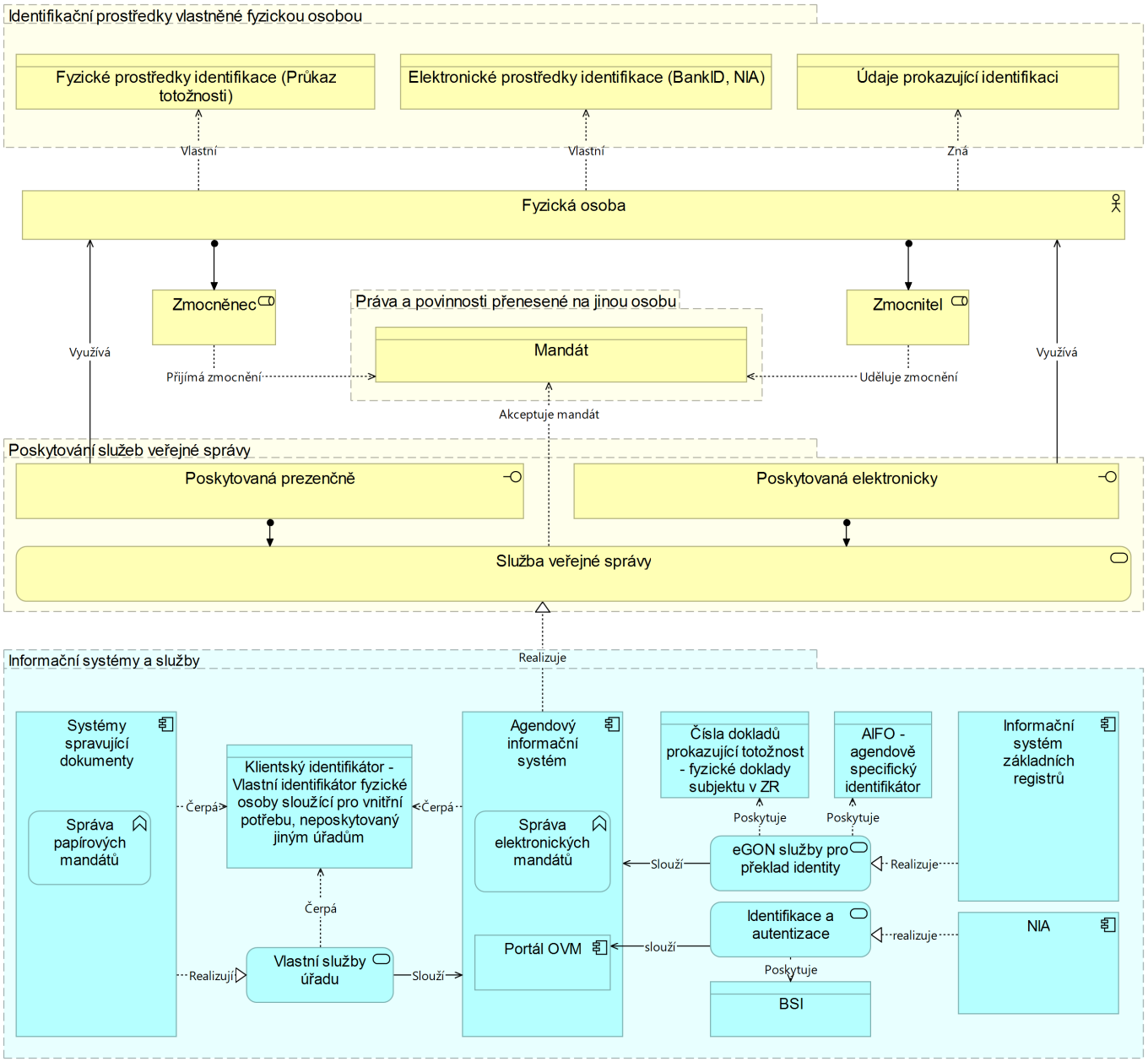
Zákon č. 250/2017 Sb., o elektronické identifikaci, zavádí v §2 povinnost provádět prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace. Tento paragraf nabývá účinnosti 1. července 2020. Po tomto datu nebude možné pokračovat v praxi vydávání přístupových údajů klientů veřejné správy mimo systémy kvalifikovaného systému elektronické identifikace, pokud jiný zákon tuto cestu neumožňuje.

Podporu celého procesu elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace je vytvořena platforma Národní identitní autority (také jako NIA), která vykonává činnosti Národního bodu dle § 20 a následujících a národního uzlu eIDAS pro spolupráci s oznámenými systémy elektronické identifikace dle nařízení Evropské parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Mandáty, práva a role v elektronické identifikaci pro klienty veřejné správy

Kvalifikovaný poskytovatel elektronických služeb **bude nadále zodpovědný** za řízení oprávnění (autorizaci) fyzické osoby, která prokázala takto svoji totožnost. Nadále tedy musí provádět správu oprávnění na základě údajů o osobě, které získá z Propojeného datového fondu a vlastních údajů vedených v agendě.

Pohled na identifikaci a identifikátory klientů VS



Pravidla pro identifikace klientů veřejné správy

Fyzická identifikace

Fyzickou identifikací je myšlena situace, kdy klient veřejné správy je osobně přítomen v místě, kde je mu služba poskytována nebo je po něm vyžadována součinnost. K fyzickému prokázání totožnosti se používají identifikační doklady, které musí obsahovat:

- Aktuální a platné údaje o jeho držiteli
- Fotografii držitele

Jako identifikační doklad se používá **občanský průkaz** a **cestovní pas**. Identifikačním dokladem **není** řidičský průkaz, protože nesplňuje potřebné parametry při jeho vydávání, ačkoliv obsahuje například fotografii držitele.

Samotný občanský průkaz, který může sloužit i k elektronické identifikaci, lze použít k fyzické identifikaci na různé úrovni:

- Střední úroveň
  - Zjištění, zda nejde o padělaný občanský průkaz

        - Strojově čitelné občanské průkazy
        - Ostatní občanské průkazy
    - Zjištění, zda je předložený občanský průkaz platný
        - Seznam platných občanských průkazů
        - Seznam neplatných občanských průkazů
    - Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
- Vysoká úroveň
    - Zjištění, zda nejde o padělaný občanský průkaz
        - Strojově čitelné občanské průkazy
        - Ostatní občanské průkazy
    - Zjištění, zda je předložený občanský průkaz platný
        - Seznam platných občanských průkazů
        - Seznam neplatných občanských průkazů
    - Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
    - Vyžádání si aktuálních údajů, včetně fotografie, o klientovi, který jej předložil a jejich kontrola

Fyzická identifikace právnických osob

Pokud jde o právnické osoby v pojetí českého právního řádu, tyto nemohou z jejich povahy nikdy právně jednat samy, musí za ně vždy jednat zástupce, kterým je (byť i nepřímo, např. je-li právnická osoba statutárním orgánem jiné právnické osoby) finálně vždy fyzická osoba (příp. fyzické osoby). Pro použití ve fyzickém prostředí se identifikační prostředky právnických osob v České republice nevydávají. Je tomu tak proto, že právnická osoba není ve fyzickém prostoru přítomna a vždy za ni jedná fyzická osoba, která prokazuje svou vlastní totožnost.

Elektronická identifikace

Elektronickou identifikací je myšlena situace, kdy klient veřejné správy není přítomen v místě poskytování služby. Identifikace tedy probíhá vzdáleně, bez fyzického kontaktu.

Pro jednoznačnou elektronickou identifikaci a autentizaci klientů veřejné správy byl vytvořen technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy tuto činnost vykonávat v souladu s Informační koncepcí ČR a bez nutnosti vytváření vlastních nákladných řešení a zvyšování administrativní zátěže.

Zákon č. 250/2017 Sb., o elektronické identifikaci, zavádí v §2 povinnost provádět prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace. Tento paragraf nabývá účinnosti 1. července 2020. Po tomto datu nebude možné pokračovat v praxi vydávání přístupových údajů klientů veřejné správy mimo systémy kvalifikovaného systému elektronické identifikace, pokud jiný zákon tuto cestu neumožňuje.

Podporu celého procesu elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace je vytvořena platforma Národní identitní autority (také jako NIA), která vykonává činnosti Národního bodu dle § 20 a následujících a národního uzlu eIDAS pro spolupráci s oznámenými systémy elektronické identifikace dle nařízení Evropské parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Elektronická identifikace právnických osob

Pokud jde o právnické osoby v pojetí českého právního řádu, tyto nemohou z jejich povahy nikdy právně jednat samy, musí za ně vždy jednat zástupce, kterým je (byť i nepřímo, např. je-li právnická osoba statutárním

orgánem jiné právnické osoby) finálně vždy fyzická osoba (příp. fyzické osoby). Z toho plyne, že ustanovení § 2 zákona o elektronické identifikaci, které dopadá na případy fyzických osob, se tak vztahuje i na jednání právnických osob, neboť jsou to vždy fyzické osoby, které fakticky jednají, ať již za sebe, či za jinou fyzickou osobu nebo právnickou osobu.

V elektronickém prostředí, zejména jde-li o automatizovanou komunikaci, jsou nicméně používány mechanismy, které mají charakter identifikačního prostředku právnické osoby. Jde např. o certifikát pro evidenci tržeb podle zákona č. 112/2016 Sb., o evidenci tržeb, nebo certifikáty vydané Českou národní bankou pro automatizovanou komunikaci mezi ČNB a subjekty podléhající jejímu dozoru, typicky bankami. Platí nicméně, že identifikační prostředky právnických osob s použitím bez ohledu na agendy, ekvivalentní např. občanským průkazům, se v České republice nevydávají.

Zatímco samotná autentizace fyzické osoby není problematická, problematická se jeví otázka určení, zda fyzická osoba jedná v dané situaci za sebe (popř. v jaké roli za sebe) anebo zda jedná za jinou fyzickou osobu nebo za právnickou osobu. Problematika mandátů a oprávnění je řešena níže.

Skutečnost, že daná fyzická osoba, má právo se identifikovat a autentizovat za určitou právnickou osobu (tj. „přihlásit se ke službě jménem právnické osoby“), ještě nezakládá bez dalšího právo na to, že tato fyzická osoba má právo za danou právnickou osobu činit úkony prostřednictvím digitální služby. Autorizaci dané fyzické osoby k poskytnutí digitální služby musí posoudit ten, ke komu se fyzická osoba hlásí na základě jím dostupných údajů (informace z obchodního rejstříku, plná moc opravňující konkrétní osobu jednat jménem právnické osoby,…) ve spojení s příslušnými právními předpisy.

Jako příklad takového přístupu můžeme uvést datové schránky, do nichž se fyzická osoba přihlásí například novým občanským průkazem s aktivovaným čipem. Po úspěšné autentizaci s pomocí prostředku pro elektronickou identifikaci (tj. např. s pomocí „eObčanky)“ a souhlasu s předáním osobních údajů na portálu Národního bodu pro identifikaci a autentizaci, je fyzická osoba pro účely informačního systému datových schránek (ISDS) ztotožněna. Po ztotožnění tak nabídne ISDS fyzické osobě seznam datových schránek, ve vztahu k nimž je přihlášená fyzická osoba oprávněná jednat.

Autentizovaná fyzická osoba si tedy vybírá, za koho a v jaké roli bude prostřednictvím datových schránek jednat. Informaci o tomto oprávnění si ISDS obstarává např. z ROS, z jiných zdrojů (např. údaj o tom, že určitá osoba je advokátem nebo insolvenčním správcem) anebo jej vede na základě sdělení samotného držitele datové schránky (např. údaj o tzv. pověřené osobě). Bez ohledu na zdroj informace o oprávnění k zastupování jiné osoby, resp. na zdroj informace o roli je však na samotném ISDS jakožto poskytovateli služeb, aby oprávnění k zastupování jiné osoby ve svém prostředí řádně implementoval tak, aby osoby mohly toto oprávnění realizovat. Nabídka jednotlivých oprávnění, resp. rolí, tedy spadá do kompetence daného poskytovatele služeb a odvíjí se od údajů a oprávnění, které vede v rámci svého informačního systému nebo od údajů, ke kterým má přístup.

Mandáty, role a práva v elektronické komunikaci

Zajištění správné obsazení do role neboli autorizace, klienta využívajícího elektronické služby je jedním ze základních předpokladů jejího správného fungování. Různé role mají v rámci služby různá oprávnění a povinnosti a poskytovatel služby je povinen nabídnout klientovi veškeré role, do kterých se v rámci služby může pasovat, včetně rolí jako zástupce právnické osoby, zástupce nezletilého, registrující lékař pacienta a další. Tyto role s oprávněními vůči jiným klientům veřejné správy jsou mandáty. Aby proběhlo správné obsazení do role a zjištění mandátu, je pro poskytování elektronických služeb klientům veřejné správy nutné mít zajištěno několik základních náležitostí:

1. Znalost typů mandátů při jednání s veřejnou správou
2. Jednoznačnou identifikaci a autentizaci klienta veřejné správy
3. Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu
4. Vlastní zajištění autorizace klienta veřejné správy

Při výkonu veřejné správy a to zejména při jakékoliv interakci a komunikaci s klientem veřejné správy je nutné, aby veřejná správa respektovala mandáty k zastupování jedné osoby druhou na základě různých titulů. Zjednodušeně se dá rozdělit forma mandátu zastupování dle následující tabulky.

Typ subjektu	Mandát
Fyzická osoba	Jednající sama svým jménem
	Jednající jménem jiné fyzické osoby ze zákona: - rodič dítěte, - manžel/manželka, - registrovaný partner/partnerka, - opatrovník, osvojitel, poručík, pěstoun - dědic, exekutor, - zastupující osoba pro osoby neschopné jednat nebo nemající zákonného zástupce
	Jednající jménem jiné fyzické osoby ze zmocnění: - plná moc, - advokát, - zastupující FO, - jiný druh zmocnění, - na žádost bez zmocnění
	Plná moc opravňující konkrétní osobu jednat jménem právnické osoby
Fyzická osoba jednající za právnickou osobu	Jednatel právnické osoby
	statutární zástupce právnické osoby (jedna FO)
	Statutární orgán právnické osoby (více FO)
	Insolvenční správce
	Likvidátor
	Jednající jménem zřizovatele právnické osoby
	Pověřen k jednání za právnickou osobu: - Veřejnoprávním titulem, - Soukromoprávním titulem (smlouva, plná moc, společenská smlouva, apod.)
	Pokud agendový předpis povoluje využívání přístupových údajů k systému datových schránek jako identifikačních prostředků je to dále: a) Pro fyzické osoby – statutární zástupce oprávněné k přístupu do datové schránky právnické osoby ověřením oprávnění k datové schránce právnické osoby prostřednictvím Informačního systému datových schránek (ověření přístupových údajů a oprávnění). b) Pro fyzické osoby - oprávněné statutárním zástupcem k přístupu do datové schránky právnické osoby ověřením oprávnění k datové schránce právnické osoby prostřednictvím Informačního systému datových schránek (ověření přístupových údajů a oprávnění). c) Ověřením speciálního agendového oprávnění podle agendového předpisu, na jehož základě jsou poskytovány agendové digitální služby.

Příklady mandátů pro fyzické osoby vyplývající z některých vyhlášek a nařízení měst a obcí:

- Pro přihlášení k platbě poplatku za odvoz komunálního odpadu
- Pro přihlášení k platbě poplatku:
  - ubytovacího,
  - ze psa,
  - za zábor a užívání veřejného prostranství.
- Pro převody, koupě, prodej, nabytí městského majetku, (provozovny v budovách v majetku města)
- Pro užívání, podnájem, zrušení užívání bytového fondu města
- Mandát pro jednání s knihovnou – výpůjčky registrovaného čtenáře

Jak je zdůrazněno níže, při výkonu veřejné správy je nutné, aby příslušný orgán konající nějakou činnost v rámci dané agendy věděl, pro jakou formu zastupování je mandát umožněný nebo dokonce nutný. Zcela jiným způsobem se orgán veřejné moci bude chovat k mandátu plynoucímu z veřejnoprávního titulu rodičovství a jinak

k mandátu plynoucímu ze soukromoprávního titulu plné moci.

Je také vhodné rozlišovat účel mandátu, tedy typ úkonů, které prostřednictvím zastupované osoby klient veřejné správy dělá. Ty je možno rozdělit do následujících skupin:

- Nahlížení na údaje subjektů práva bez jakéhokoliv interaktivního využívání či zapisování údajů (informační účel).
- Přístup k údajům subjektů a jejich reklamace, nebo pokud je přímo umožněna editace klientům veřejné správy (transakční účel).
- Zmocnění k přístupu či využívání údajů subjektu práva pro třetí strany, nebo poskytnutí údajů z ISVS třetím stranám (zmocňovací účel).
- Činění podání a úkonů vůči orgánům veřejné správy (účel úkonu).
- Využívání elektronických klientských služeb jako je objednání se k úředníkovi.
- Zápis, úprava a zrušení mandátu.

Jednoznačná identifikace a autentizace klienta veřejné správy

Všechny subjekty povinné dle zákona č. 250/2017 Sb., o elektronické identifikaci mají povinnost dle §2 využívat k prokázání totožnosti při elektronickém kontaktu pouze kvalifikovaný systém, konkrétně:

„Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace.“

Kvalifikovaný systém spravuje kvalifikovaný správce (státní orgán nebo akreditovaná osoba) a splňuje technické normy i specifikace Evropské unie a především je propojen s národním bodem pro identifikaci a autentizaci – tzv. Národní identitní autorita (NIA).

Identifikace a autentizace prostřednictvím NIA zajistí jen a pouze službu ověřené identity fyzické osoby, neboli každý systém čerpající služby NIA, se může spolehnout na to, že přihlášená fyzická osoba je skutečna ta, za kterou se vzdáleně a elektronicky vydává. Již se dále nezajišťují další služby typu autorizace.

Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu

Systém poskytující elektronické služby veřejné správy musí být schopen komunikovat a získávat údaje z propojeného datového fondu. K tomu musí systém odpovídat předpisům:

- Zákon 365/2000 Sb., o informačních systémech veřejné správy. Systém klasifikovaný jako Informační systém veřejné správy (ISVS) využívající referenční rozhraní veřejné správy.
- Zákon 111/2009 Sb., o základních registrech. Systém klasifikovaný jako agendový informační systém (AIS) využívající údaje základních registrů a editorů základních registrů dle svého agendového zákona.
- Zákon 250/2014 Sb., o elektronické identifikaci. Systém, který vyžaduje ověření totožnosti
- Nařízení eIDAS

Více o využívání údajů propojeného datového fondu a infrastruktuře referenčního rozhraní je napsáno v kapitolách:

- eGON Service Bus/Informační systém sdílené služby
- Centrální místo služeb
- Propojenný datový fond

Centrální sdílené služby eGovernmentu dokáží zajistit následující mandáty pro fyzické osoby, které se prokázaly u poskytovatele služeb svou zaručenou elektronickou identitou:

- eGON služba rosCtiPodleUdaju, rosCtiIco, rosCtiAifo (základní registr osob)
    - pro zajištění ověření, zda je fyzická osoba statutárním zástupcem

- eGON služba aiseoCtiPodleUdaju, aiseoCtiAifo (agendový informační systém evidence obyvatel)
  - pro zajištění ověření, zda je fyzická osoba rodič nezletilého, který není svéprávný
  - pro zajištění ověření, zda je fyzická osoba zákonným zástupcem jiné fyzické osoby
  - pro zajištění ověření, zda je fyzická osoba opatrovníkem jiné fyzické osoby
  - pro zajištění ověření, zda je fyzická osoba manžel/manželka
- eGON služba isknCtiVlastniky (informační systém katastru nemovitostí)
  - pro zajištění ověření, zda je fyzická osoba vlastníkem nemovitosti
- Služba ISDS
  - Pro zajištění, zda je fyzická osoba pověřená k činění úkonů v ISDS vlastníkem datové schránky

Žádné další centrální služby ověření oprávnění/mandátů se v současné, ani dohledné době, neplánují. Proto je důležité, aby si každý poskytovatel elektronických služeb zajistit jiné typy mandátů sám.

Vlastní zajištění autorizace klienta veřejné správy

Každá vykonávaná agenda (výkon veřejné správy) může pro svoji potřebu vyžadovat jiné mandáty. Například mandát podání daňového přiznání za jinou fyzickou osobu, mandát nahlížení na zdravotnickou dokumentaci jiné fyzické osoby, nakládání s majetkem právnické osoby, u které nejsem statutární zástupce, či například mandát k zastupování při dědickém řízení.

Všechny tyto mandáty se musí řešit v rámci dané agendy a jako ideální řešení navrhujeme:

- Zřídit buď v jednotlivých agendových informačních systémech, nebo v rámci centralizované správy subjektů mandátní registr.
- V rámci mandátního registru určit předem definované typy mandátů přípustné v dané agendě a způsob zápisu mandátů pro nahlížení a pro transakce ze strany klienta
- Povolit zapisovat všem klientům mandáty dle definovaných typů pod svou zaručenou elektronickou identitou.
- Umožnit klientům přidat mandát i offline, například na přepážce úřadu.
- Při každém přihlášení klienta kontrolovat kromě mandátů z centrálních sdílených služeb eGovernmentu i vlastní mandátní registr a dát vždy při přihlášení vybrat klientovi, v jaké roli a s jakým mandátem chce pracovat.

Je důležité zdůraznit, že veřejná správa nemá rozlišovat formu komunikace a jednání s klientem. Tedy mandát obecně platící pro osobní jednání s úředníkem, nebo pro fyzické prováděné úkony na přepážce, musí mít klient umožněn využívat i při elektronické komunikaci a naopak. Také proto je nutné vést mandáty standardizovanou formou na jednom místě a využívat jich i při elektronické komunikaci klienta.

Mandát plynoucí z veřejnoprávního nebo soukromoprávního titulu a to včetně plných mocí a dohod o zastupování při správním jednání s úřady patří mezi společné rozhodné skutečnosti, tak jak jsou zakotveny v souvisejících ustanoveních Správního řádu (zejména § 6 a § 50 a související). Proto je nanejvýš vhodné, aby příslušný orgán veřejné moci, pokud

- využívá a buduje centrální evidenci subjektů,
- centrální evidenci rozhodných skutečností,
- skutečnosti o zapsaném anebo z něčeho plynoucím mandátu k zastupování,
- je zahrnul do rozhodných skutečností.

Klient se totiž může odvolat na příslušná ustanovení správního řádu a neposkytovat zejména plné moci a další dokumenty, z nichž mandát plyne, úřadu opakovaně.

Univerzální kontaktní místo veřejné správy

Systémy správy dokumentů

Systémy a služby spojené s právním řádem a legislativou

Elektronické úkony a doručování

Popis Informačního systému datových schránek

Pro zajištění důvěryhodné, bezpečné a průkazné elektronické komunikace mezi orgány veřejné moci na straně jedné a fyzickými či právnickými na straně druhé, jakož i mezi orgány veřejné moci navzájem, provozuje Ministerstvo vnitra ČR informační systém datových schránek (také jako "ISDS"). Ministerstvo vnitra ČR a spolupracující subjekty se při provozování ISDS řídí provozním řádem, který je pro ně závazný.

Orgány veřejné moci jsou povinni mezi sebou komunikovat prostřednictvím ISDS, stejně tak s klientem veřejné správy, pokud datovou schránku vlastní.

Typy datové schránky

Způsob, resp. proces zřízení datové schránky se liší podle typu subjektu, pro který má být datová schránka zřízena. Typ subjektu určuje, zda se jedná o datovou schránku zřizovanou ze zákona, tedy automaticky, nebo o datovou schránku zřizovanou na žádost dle následující tabulky

Typ subjektu	Typ datové schránky v ISDS	Zřízena
Orgán veřejné moci	OVM (10)	Ze zákona
Fyzická osoba, která je v roli OVM	OVM_FO (14)	Ze zákona
Podnikající fyzická osoba, která je v roli OVM	OVM_PFO (15)	Ze zákona
Právnická osoba v roli OVM	OVM_PO (16)	Ze zákona
Právnická osoba zapsaná v obchodním rejstříku	PO (20)	Ze zákona
Podnikající fyzická osoba - advokát	PFO_ADVOK (31)	Ze zákona
Podnikající fyzická osoba - daňový poradce	PFO_DANPOR (32)	Ze zákona
Podnikající fyzická osoba - insolvenční správce	PFO_INSSPR (33)	Ze zákona
Podnikající fyzická osoba - statutární auditor (OSVČ nebo zaměstnanec)	PFO_AUDITOR (34)	Ze zákona
Fyzická osoba	FO (40)	Na žádost
Podnikající fyzická osoba	PFO (30)	Na žádost
Právnická osoba - na žádost	PO_REQ (22)	Na žádost
Schránka OVM zřízená na žádost	OVM_REQ (13	Na žádost

Zápis rozhodnutí do Registru práv a povinností

Zákon o základních registrech vyžaduje, aby při každé změně referenčního údaje v základních registrech došlo také k zápisu o příslušném rozhodnutí, na jehož základě byl údaj změněn, do Registru práv a povinností. Ministerstvo vnitra je v agendě datových schránek editorem jediného referenčního údaje – identifikátoru datové schránky. Při každém zápisu i výmazu tohoto údaje do Registru obyvatel nebo Registru osob proto ISDS provádí zároveň zápis do Registru práv a povinností.

Využití údajů základních registrů (ZR)

Ministerstvo vnitra rozsáhle využívá referenční údaje základních registrů pro účely správy datových schránek. Základní registry tak představují nejdůležitější zdroj dat, na základě kterých jsou datové schránky zřizovány i znepřístupňovány a také aktualizovány identifikační údaje datových schránek a jejich uživatelů.

Zřizování datových schránek ze zákona

Na základě informací z Registru osob jsou zřizovány datové schránky subjektům, kterým se datová schránka zřizuje ze zákona. Výjimku představuje malá množina subjektů, které v Registru osob nejsou vedeny, protože nemají přiděleno své unikátní IČO (orgány veřejné moci bez právní subjektivity).

Znepřístupňování datových schránek

Na základě informací z Registru osob jsou znepřístupňovány datové schránky subjektů, u kterých bylo v Registru osob vyplněno datum zániku. Obdobně, jakmile je u fyzické osoby v Registru obyvatel vyplněno datum úmrtí, datová schránka je k tomuto datu znepřístupněna.

Aktualizace údajů datových schránek

Pro datové schránky všech typů platí, že pokud je subjekt veden v základních registrech, identifikační údaje datové schránky jsou automatizovaně přebírány ze Základních registrů. Tzn. změny názvu subjektu nebo adresy sídla není nutné Ministerstvu hlásit – změny jsou promítnuty automaticky.

Přidání / odebrání Oprávněné osoby

Oprávněné osoby u datových schránek těch subjektů, které jsou zapsány v Registru osob, jsou aktualizovány podle změn ve výčtu statutárních zástupců vedených u daného subjektu v Registru osob. Tzn. je-li do registru zapsán nový statutární zástupce, automatizovaně mu je zřízen účet Oprávněné osoby u datové schránky subjektu a naopak, je-li statutární zástupce z registru odebrán, jeho účet Oprávněné osoby u datové schránky je zrušen.

Aktualizace osobních údajů uživatelů datových schránek

U všech uživatelů datových schránek se Ministerstvo vnitra pokouší o jejich automatizované ztotožnění vůči příslušnému záznamu v Registru obyvatel. U těch uživatelů, kde se ztotožnění zdařilo, jsou automatizovaně přebírány aktuální referenční údaje z Registru obyvatel. Tzn. např. v případě změny příjmení nebo adresy pobytu nemusí držitel datové schránky Ministerstvu vnitra nic hlásit – změna je promítnuta automaticky.

Pravidla Informačního systému datových schránek

Úřadu je doporučeno využívat systém ISDS jako integrální součást své elektronické spisové služby. Úřady musí mezi sebou komunikovat prostřednictvím systému ISDS a svých datových schránek, pokud se jedná o výměnu dokumentů a jejich zaručeného doručení. Pokud se jedná o výměnu údajů mezi úřady, nevyužívají se datové schránky, ale propojený datový fond a jeho referenční rozhraní. Je nutné brát v potaz, že veškeré úkony činěné skrze datovou zprávu směrem do úřadu od klienta VS se pokládají za elektronicky podepsané a není potřeba po klientovi vyžadovat žádné další formy autorizace.

ISDS umožňují na vyžádání u věcného správce (Ministerstva vnitra) využívat identitní prostor datových schránek k přihlašování do vlastních řešení - typicky portálů. **Tento způsob identifikace a autentizace klienta VS bude umožněn pouze do 1.7.2020**, kdy vyprší přechodné ustanovení zákona 250/2017 Sb., které zavádí povinnost využívat systém Národní identitní autority .

Pro zajištění digitální kontinuity datové zprávy, podobně jako v části Systém správy dokumentů, je z pohledu uživatele (příjemce) nutné si vždy uložit nejen přijatý dokument, ale celou datovou zprávu (obálka + dokument). Tato celá datová zpráva lze kdykoliv zpětně věřit proti samotnému informačnímu systému datových schránek, samotný dokument však ne.

Jednotný identitní prostor veřejné správy

Jednotné obslužné kanály a uživatelská rozhraní úředníků

Sdílené agendové IS v přenesené působnosti

Sdílené agendové IS pro samostatnou působnost územních samospráv

Sdílené provozní informační systémy

Sdílené statistické, analytické a výkaznické systémy

eGovernment Cloud

Popis eGovernment cloudu

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

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

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

Služby eGC jsou poskytovány komerční částí eGC (KeGC - služby provozované komerčními subjekty s využitím jejich vlastních datových center a komunikační infrastruktury) a státní částí (SeGC – služby provozované v

datových centrech a na HW a SW platformách v majetku státu a provozované organizacemi řízenými státem – poskytovatelem státního cloud computingu).

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

- definici minimálních standardů pro poskytování IaaS a PaaS služeb pro státní a komerční část eGC,
- sjednocení provozního prostředí informačních systémů a aplikací provozovaných ve státní části eGC na několik vybraných platforem,
- zajištění potřebné bezpečnosti, spolehlivosti, škálovatelnosti a jednotnosti provozu ICT služeb.

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

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

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

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

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

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

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

Poskytovatelé služeb eGC musí splňovat zákonem určené podmínky, které zahrnují zejména oblast bezpečnosti poskytovaných služeb a jejich provozních parametrů, ale také důvěryhodnosti poskytovatele. Splnění podmínek ověřuje Digitální a informační agentura ve spolupráci s Národním úřadem pro kybernetickou a informační

bezpečnost a dalšími složkami státu. Požadavky, které musí splnit poskytovatel cloud computingu, aby byla jeho nabídka zapsána do katalogu cloud computingu, stanovuje vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

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

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

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

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

Katalog cloud computingu

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

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

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

Pravidla eGovernment cloudu

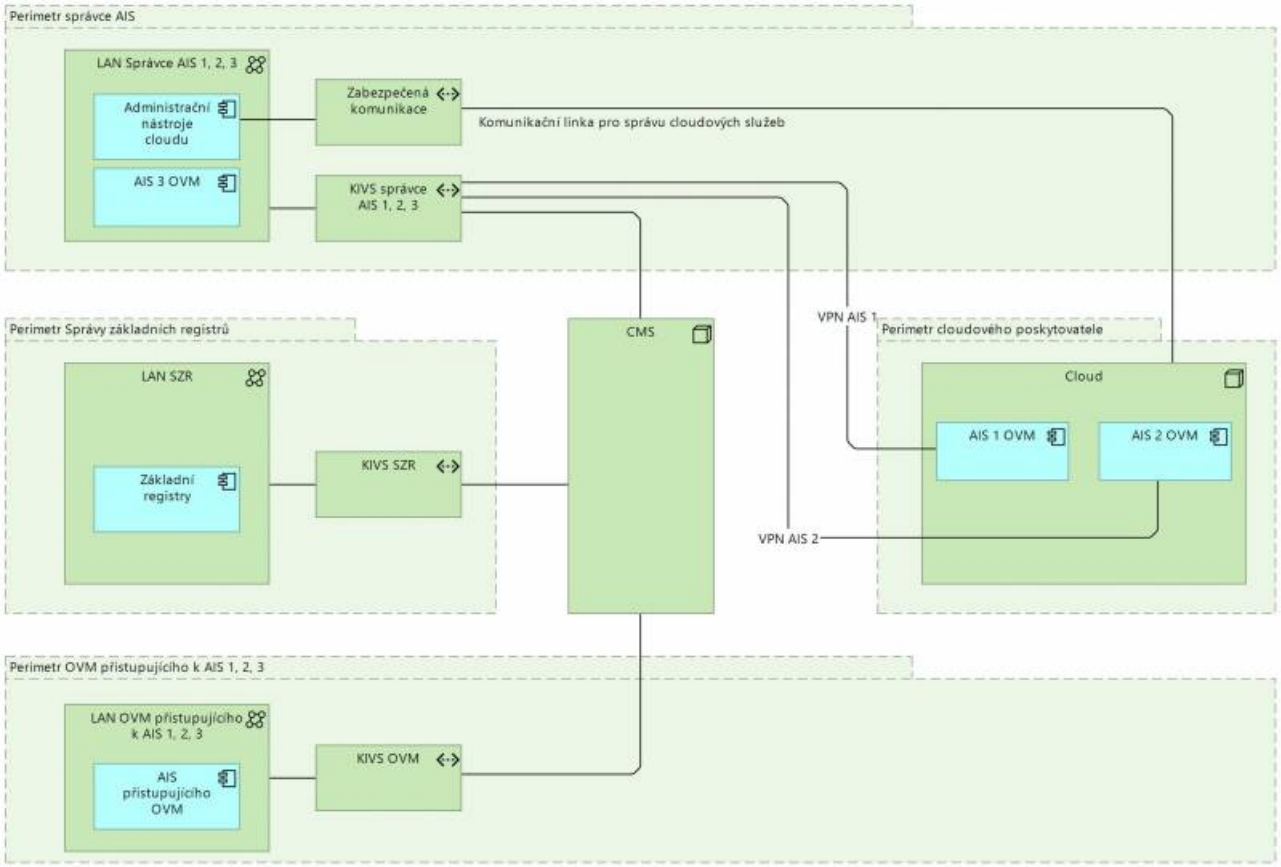
Přístup správců ISVS k eGC

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

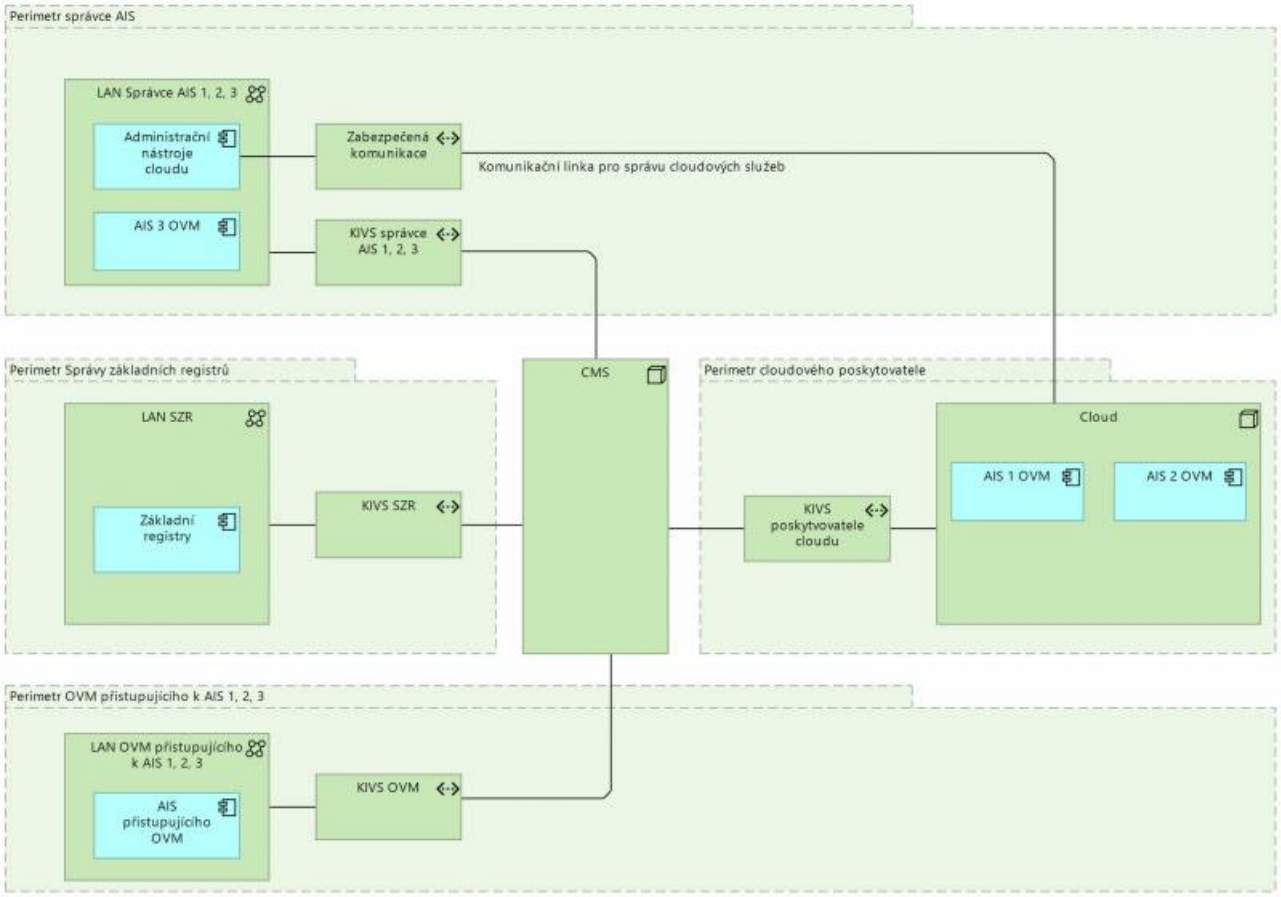
Provozování AIS OVM v eGC v souvislosti s komunikací pomocí CMS/KIVS

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

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



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



Publikování portálu OVM

Publikování portálu OVM je specifický případ publikování AIS OVM, kdy se v rámci provozu portálu v eGC umožňuje, aby byly služby portálu dostupné pro klienty, kteří nejsou OVM, prostřednictvím internetu přímo od poskytovatele eGC.

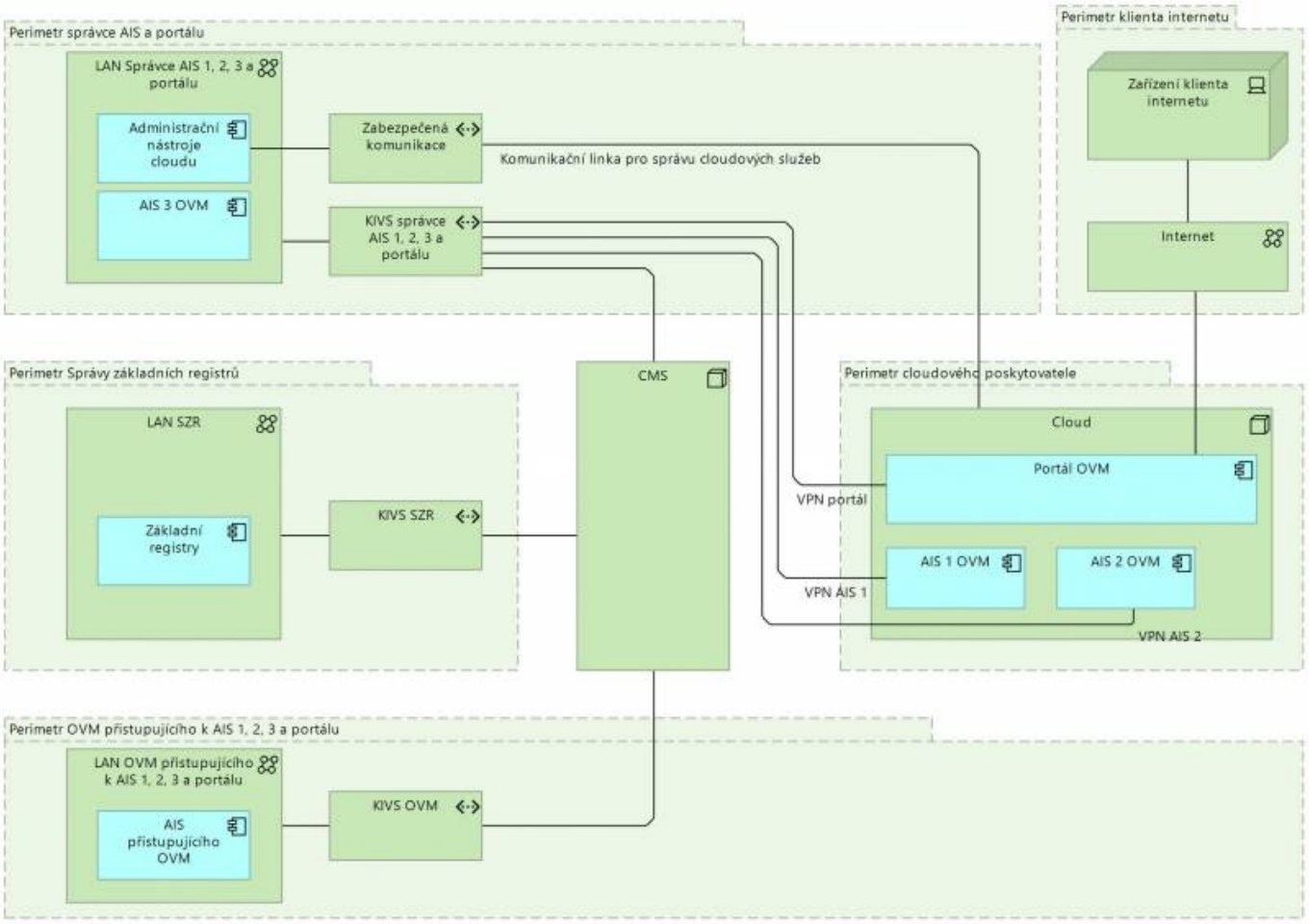
Portál je v případě provozu na vlastní infrastruktuře publikován výhradně prostřednictvím CMS službou CMS2-02 Zveřejnění aplikace a to do:

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

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

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

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



Povinnosti komerčních poskytovatelů služeb eGC

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

Národní datová centra

Popis Národních datových center

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

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

- Služby bezpečného prostředí výpočetního centra
- Služby virtuální výpočetní kapacity
- Služby databázových serverů
- Služby datového zálohování

- Služby vystavení publikovaných služeb v DMZ1 a DMZ2 v CMS KIVS

Pravidla Národních datových center

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

Komunikační infrastruktura veřejné správy