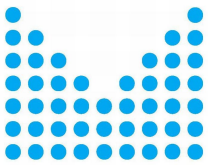
Materiál Ministerstva vnitra



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

Pravidla pro funkční celky architektury jednotlivých úřadů

Tato kapitola popisuje definované funkční celky v celé šíři (v celé architektuře) včetně pravidel, návodů a dobrých praktik k jejich správě a rozvoji. Jde o jiný přístup k popisu požadavků na využívání systémů a služeb eGovernmentu než v části Pravidla tvorby a údržby vlastní čtyřvrstvé architektury jednotlivých úřadů, kde se požadavky popisují skrze jednotlivé vrstvy architektury úřadu.

Skladba této kapitoly odpovídá klíčovým tématickým okruhům z části Architektura a sdílené služby veřejné správy:

- **Univerzální kontaktní místo veřejné správy - CzechPOINT**
- **Portály veřejné správy a soukromoprávních uživatelů údajů - Portál občana, Portál veřejné správy**
- **Systém správy dokumentů - eSSL**
- **Elektornická fakturace - eFaktura**
- **Jednotný identitní prostor veřejné správy – JIP/KAAS**
- **Elektronická identifikace pro klienty veřejné správy – NIA**
- **Úplné elektronické podání - ÚEP**
- **Propojený datový fond - PPDF**
- **Veřejný datový fond ČR - VDF**
- **Elektronické úkony a doručování - Datové schránky**
- **Jednotné obslužné kanály a uživatelská rozhraní úředníků**
- **Národní datová centra**
- **eGovernment Cloud**
- **Sdílená síťová a komunikační infrastruktura - KIVS/CMS**

Dostupné, aktuálně budované a sdílené agendové služby eGovernmentu lze řadit do následujících tematických okruhů, repsektive funkčních celků:

- **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.

Univerzální kontaktní místo veřejné správy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci univerzálního kontaktního místa je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí znát rozdíl mezi samoobslužným a asistovaným kontaktním místem a své služby v těchto kontaktních místech publikovat.</note>

Úřad musí při tvorbě a správě svých služeb zohlednit možnost vyřízení služby jak samoobslužně, tak asistovaně. Primární odpovědnost za toto rozhodnutí nese věcný správce služby, což např. u služeb v přenesené působnosti

není vždy daný úřad. Může však být dána určitá vlastní zodpovědnost za způsob, jakým je umožněno danou službu v přenesené působnosti vyřídit a pokud tuto možnost věcný správce poskytuje, je úřad povinen zohlednit všechny možnosti vyřízení. Nesmí také nastat situace, kdy služba veřejné správy, která je publikována pro samoobsluhu klienta nebude obsahovat všechny možnosti vyřízení, které má k dispozici v asistované formě.

Samoobslužná univerzální kontaktní místa

Aby se plně podporovala samoobsluha služby veřejné správy, musí splnit následující podmínky:

- Poskytování samoobslužných služeb pro klienta pod zaručenou elektronickou identitou
  - Všechny publikované samoobslužné služby jednotlivých úřadů musí mít možnost pracovat s klientem, který se prokazuje svoji zaručenou elektronickou identitou. Technicky to znamená soulad s pravidly a principy Národního identitního prostoru
- Federace pod portal_obcana
  - Služby musí být federovány pod Portál občana / Portál veřejné správy v souladu s Národním identitním prostorem a plnit pravidla portálů veřejné správy a soukromoprávních uživatelů údajů
- Interaktivní uživatelské rozhraní
  - Formuláře a další služby pro klienta veřejné správy používající zaručenou elektronickou identitu a principy úplného elektronického podání.

Asistovaná univerzální kontaktní místa

Při provozování asistovaných univerzálních kontaktních míst je potřeba zajistit přidělení rolí v CzechPOINT pro pracovníky poskytující jeho služby skrze správce, tzv. lokálního administrátora.

V rámci asistovaných univerzálních kontaktních míst je nutné počítat s neustálým rozvojem a přidáváním služeb, které musí v co největší míře odpovídat těm samoobslužným. Žádná samoobslužná služby nesmí být bez své asistované varianty, která však může být řešena i v rámci úřadu, pokud tak vyžaduje její specifická náročnost (například daňové přiznání).

Portály veřejné správy a soukromoprávních uživatelů údajů

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci portálů veřejné správy a soukromoprávních uživatelů údaje je uveden zde a popsán v části Architektura sdílených služeb veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad či soukromoprávní uživatel údajů musí provozovat portál jako rozhraní pro poskytnutí služeb elektronicky a respektovat při tom povinnosti dané rozdílnostmi jako např. zda se jedná o přenesenou nebo samosprávnou působnost.</note>

Úřad musí při provozování portálu zavést a změnit současné procesy orientované především na osobní kontakt s klientem. Současné portály již musí disponovat funkcionalitou propojení se zaručenou identitou dle zákona 250/2017 Sb. a musí se umět přizpůsobit situaci, kdy klient veřejné správy bude komunikovat pouze elektronicky. Začíná se tedy samotným uživatelsky přívětivým prostředím, které musí být v souladu s **grafickým manuálem MVČR**. Dále je potřeba formulářový engine, který umožní nejen předvyplnit veškeré státu již známé údaje z propojeného datového fondu a elektronické identity poskytnuté národní identitní autoritou. V neposlední řadě je potřeba zajistit předávání všech podání učiněné v portálu do agendových informačních systémů, ve kterých se dle agendy podání řeší a zároveň do spisové služby úřadu. Při předávání podání z portálu je tak potřeba mít zajištěnou funkcionalitu, která z podání vytvoří "lidsky čitelný" a "strojově čitelný" formát v rámci jedné obálky, která je opečetěná a orazítkovaná portálem. Lidsky čitelný formát, typicky

PDF, jde do spisové služby pro evidenci a strojově čitelný formát jde od agendového systému. Při provozu portálu nezáleží na technologiích, ani infrastruktuře. Není tedy preferované ani On Premise řešení, ani cloudové řešení, vše záleží na potřebách daného úřadu a možnostech, které technologie dokáží nabídnout. Je vždy potřeba myslet na rozložení zátěže, například daňové přiznání z příjmu fyzických osob se podává 1x ročně a není proto nutné klást na infrastrukturu celoroční nepřetržitý provoz. Každé řešení však musí podporovat přístup k centrálním službám eGovernmentu a dalším službám veřejné správy skrze zabezpečenou infrastrukturu **referenčního rozhraní.**

Portál podporuje samoobslužného klienta, který obsahuje jak přenesenou, tak samosprávnou působnost a obsahuje popis životních situací, ve kterých se řeší mandáty v elektronické komunikaci.

Portál občana a portál veřejné správy

Portál občana i portál veřejné správy jsou centrálně poskytované a provozované portály. Integrovat, či federovat služby úřadu lze přes vlastní řešení v podobě agendových portálů, portálů území či soukromoprávních uživatelů údajů. Integrace je celkem na 3 stupních:

1. Proklik na vlastní řešení s využitím Single Sign-On. Obsahuje pouze vlastní prostor na portálu občana, kde úřad zveřejní svou informační dlaždici, skrze kterou se klient dostane, s využitím principu Single Sign-On a zapojení do národního identitního prostoru, na vlastní řešení
2. Poskytování údajů do vlastního prostoru na portálu občana. Kromě možnosti prokliku na vlastní řešení zapojeného do národního identitního prostoru obsahuje i vždy aktuální údaje o klientovi poskytované skrze propojeny_datovy_fond portálu občana
3. Kompletní vyřešení služby veřejné správy na portálu občana pomocí formulářového řešení se všemi integracemi v bodech 1 a 2.

Agendový portál

Agendovým portálem je myšlen portál poskytující služby logicky centralizovaného systému pro jiné orgány veřejné správy. Typicky jde tedy o portál agendy v přenesené působnosti poskytovaný správcem (ohlašovatelem) agendy.

Takový portál musí splnit několik podmínek:

- Musí být registrovaný jako informační systém veřejné správy v systému o informační systémech veřejné správy
- Musí být federovaný do portálu občana
- Musí dle svého agendového zákona být schopný čerpat a poskytovat údaje skrze systém eGON Service Bus
- Musí dle svého agendového zákona být schopný čerpat údaje z informačního systému základních registrů
- Musí být ohlášen jako kvalifikovaný poskytovatel služeb

Portál území

V případě portálů samospráv se předpokládají dva trendy: a) jednak budou lokální portály samospráv obsahovat obrácený směr navigace do Portálu občana, kde bude moci klient vyřídit vše ostatní ze státní správy, co případně nenašel v místním portálu a b) lokální portály budou moci být v dlouhodobé perspektivě nahrazovány místně přizpůsobenými službami centrálního Portálu občana v PVS. Takový portál musí splnit několik podmínek:

- Musí být pro každý úřad jeden - je na něm dostupné vše, v čem má úřad působnost
- Musí být registrovaný jako informační systém veřejné správy v systému o informační systémech veřejné správy
- Musí být federovaný do portálu občana

- Musí dle svého agendového zákona být schopný čerpat a poskytovat údaje skrze systém eGON Service Bus
- Musí dle svého agendového zákona být schopný čerpat údaje z informačního systému základních registrů
- Musí být ohlášen jako kvalifikovaný poskytovatel služeb

Portál soukromoprávního uživatele údajů

V případě portálu soukromoprávního uživatele údajů (také jako SPUÚ) se jedná o situaci, kdy vlastník portálu není orgán veřejné moci, ale dle své povahy je podřízen zákonu 111/2009 Sb . Může se jednat o portály poskytovatelů zdravotních služeb, soukromých pojišťoven, bank, státních podniků, apod. Takový portál a jeho vlastník musí splnit několik podmínek:

- Musí mít zřízenou datovou schránku pro komunikaci s veřejnou správou
  - Právnické osoby mají datovou schránku zřízenou ze zákona
  - Zřídit datovou schránku je možné dle informací na webu České pošty
  - Datová schránka se může obsluhovat skrze webové rozhraní na adrese www.mojedatovaschranka.cz nebo mít funkcionality integrovány do vnitřních systémů organizace. Nejčastěji se jedná o elektronickou spisovou službu.
- Musí být ohlášen v rejstříku SPUÚ v registru práv a povinností. Zde je možnost kontroly https://rpp-ais.egon.gov.cz/AISP/verejne/katalog-spuu.
  - SPUÚ je podnikající fyzická osoba nebo právnická osoba, která není orgánem veřejné moci a je podle jiného právního předpisu oprávněna využívat údaje ze základního registru nebo z agendového informačního systému
  - Ohlášení do rejstříku SPUÚ probíhá pomocí agendového informačního systému působnostního viz https://rpp-ais.egon.gov.cz/AISP/. Do tohoto systému má přistup každý ohlašovatel agendy. Pokud má ohlašovatel agendy zároveň i možnost editace rejstříku OVM a SPUÚ, může SPUÚ přidat.
    - Pokud tedy existuje agenda, v rámci které je SPUÚ oprávněn čerpat údaje ze základních registrů nebo z agendového informačního systému, je třeba kontaktovat správce agendy a požadovat zavedení do rejstříku SPUÚ.
    - Pokud není soukromoprávní uživatel údajů ohlášen v AISP a správce agendy, ani jiné OVM, jej ohlásit nechce, musí SPUÚ kontaktovat správce Registru práv a povinností (pavel.kajml@mvcr.cz) se žádostí o ohlášení do rejstříku SPUÚ s těmito údaji (Název organizace, adresa organizace, IČO, DIČ, zákon a paragraf opravňující k přístupu do základních registrů nebo agendovému informačnímu systému, kontaktní osoba)
- Musí být ohlášen jako kvalifikovaný poskytovatel služeb online služeb (dále též Service Provider). Více také zde https://www.eidentita.cz/Home/Ovm. Ohlášení může proběhnout automatizovaně skrze formulář, pokud to umožňuje typ zřízení datové schránky (typ 10, 14, 15, 16). Pokud nemáte takový typ, je nutné kontaktovat Správu základních registrů skrze datovou schránku napřímo s požadavkem obsahujíc všechny údaje, jako v případě automatizovaného způsobu:
  - Uživatel jako zástupce organizace požaduje po NIA Portálu, který je Service Providerem, službu umožňující registraci dané organizace. Tato registrace umožní fungování dané organizace v NIA a vytváření jednotlivých Service Providerů. NIA Portál kontaktuje Národní identitní autoritu, která ověření zprostředkovává, s požadavkem na ověření dané osoby (uživatele).
  - Pro ověření uživatele pro registraci organizace či konfigurací jednotlivých Service Providerů je jako Identity Provider určen Informační systém datových schránek (ISDS). Národní identitní autorita provede přesměrování na přihlášení prostřednictvím datových schránek.
  - Uživatel provede ověření vlastní osoby přihlášením k datovým schránkám. Aby mohl uživatel registrovat organizaci či provést smazání již vytvořené registrace, musí být přihlášen prostřednictvím ISDS v roli Typ S - Oprávněná osoba se stavem datové schránky Stav schránky 1 - Přístupná a nesmí se jednat o datovou schránku fyzické osoby.
  - V případě, kdy je uživatel úspěšně ověřen, Informační systém datových schránek předá Národní identitní autoritě jako výsledek ověření autentizační token obsahující IČO a název subjektu, roli přihlašovaného uživatele a další atributy.
  - Národní identitní autorita provede sběr atributů v Informačním systému základních registrů (ISZR)

na jehož základě následně provede kontrolu existence IČO.
    - Národní identitní autorita předává NIA Portálu potřebné atributy z Informačního systému základních registrů a atributy přijaté v autentizačním tokenu z Informačního systému datových schránek, které jsou nutné ke zpracování formuláře pro registraci.
    - Na základě úspěšného splnění předchozích kroků umožní NIA Portál uživateli službu registrace organizace (SeP) a zobrazí mu vyplněný formulář pro registraci.
    - Uživatel potvrdí správnost údajů a provedení registrace organizace (SeP).
    - NIA Portál zpracuje přijatý požadavek na registraci a po úspěšném zaregistrování umožní uživateli provést konfiguraci jednotlivých Service Providerů spadající pod danou organizaci.
    - Uživatel provede konfiguraci Service Providera
- Musí umět přijímat a zpracovávat data pomocí standardů SAML2 nebo WS-Federation

Systém správy dokumentů

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí zajistit správné procesy v rámci spisové služby a respektovat povinnosti dle národního standardu</note>

Elektronická fakturace

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí kromě procesních změn zajistit i příjem a vydávání elektronických faktur dle evropských a českých pravidel.</note>

Jednotný identitní prostor veřejné správy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí zajistit propojení svého identitního systému (AD/LDAP/IDM) se systémem JIP/KAAS pro tu část zaměstnanců, kteří se přihlašují k informačním systémům veřejné správy.</note>

Každé OVM musí při správě identit svých zaměstanců zvážit využití systému Jednotného identitiního prostoru (také jako JIP/KAAS). Využití může být provedeno 2 druhy:

- Vytvoření vlastních aplikačníhc rolí pro systémy, jejichž je OVM správce
- Využití existujících rolí v registru práv a povinností

Pro uživatele, kteří nejsou pokrytí centrální licencí provozovatele, lze zakoupit licenci zvlášť. Cena takovéto licence je pro 1 uživatele připbližně 2 000 Kč za první rok a 500 pro další roky.

Elektronická identifikace pro klienty veřejné správy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí zajistit identifikaci a autentizaci klientů veřejné správy prostřednictvím systému NIA tam, kde ověření totožnosti vyžaduje právní předpis nebo výkon působnosti.</note>

Zásadním požadavkem bezpečnosti a transparentnosti pro informační systémy veřejné správy je požadavek na jednotnou elektronickou identifikaci externích uživatelů. Pro každou operaci je nutná znalost osoby, která tuto operaci provádí zvláště z hlediska nepopiratelné zodpovědnosti osoby. Externí uživatelé (klienti) informačních systémů veřejné správy musí být jednoznačně identifikováni zvláště z důvodů ochrany osobních údajů a dále z procesního hlediska, jak předpokládá správní řád (jednoznačné prokázání totožnosti účastníků řízení).

Úloha správy přístupů se pro každý informační systém veřejné správy skládá z následujících kroků:

- **Identifikace –** jednoznačné a nepopiratelné určení fyzické osoby, která přistupuje k informačnímu systému veřejné správy
- **Autentizace** – prokázání, že přistupující osoba je tou osobou, za kterou se vydává. Autentizace probíhá předložením **autentizačních prostředků** (například uživatelské jméno a heslo, autentizační certifikát), které osobě přidělil správce informačního systému
- **Autorizace** – na základě údajů o identifikované a autentizované osobě a dalších údajů o této osobě (například zařazení na pracovní pozici) zařazení osoby do odpovídající role a z toho vyplývající vyhodnocení oprávnění na úkony a data v rámci informačního systému.

NAP v této oblasti vyžaduje naplnění následujících principů pro všechny informační systémy veřejné správy:

1. Každé OVM, které poskytuje své služby elektronicky a potřebuje pro ně ověřeného klienta, musí využít služeb Národní identitní autority
2. Při tvorbě identitního prostoru si prvně udělat analýzu, zda nepostačuje již některý z federovaných identit v rámci NIA
3. Jakýkoliv nový identitní prostor musí být budován tak, aby byl federovaný v rámci NIA
4. Prostředky pro identifikaci a autentizaci jsou vždy vydány bezpečnou a jednoznačnou cestou identifikované osobě tak, aby byla zajištěna minimálně úroveň důvěry značná. O tomto vydání prostředků existuje trvalý záznam spolu s údaji, jak byla ověřena identita osoby
5. Osoba, jíž byly prostředky vydány, nedílně zodpovídá za ochranu těchto prostředků před odcizením a zneužitím
6. Osoba, jíž byly prostředky vydány, nese nedílnou zodpovědnost za všechny úkony, které byly v informačním systému provedeny při použití těchto prostředků
7. Věcný správce agend, které jsou vykonávány v rámci informačního systému, zodpovídá za obsazení osob do rolí (technicky vykonává technický správce informačního systému, vždy však na základě podkladů o věcných správců). Tuto svoji zodpovědnost může delegovat v rámci organizační struktury na více zodpovědných osob.

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

Mandáty pro jednání s veřejnou správou

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.

Mandáty pro jednání s veřejnou správou^ Typ subjektu^ Mandát |

Fyzická osoba	Jednající sama svým jménem
Jednající jménem jiné fyzické osoby ze zákona: * rodič dítěte * manžel/manželka * registrovaný partner/partnerka * opatrovník	
Jednající jménem jiné fyzické osoby ze zmocnění * plná moc * advokát * zastupující FO * jiný druh zmocnění * na žádost bez zmocnění	
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.)	

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 údajů 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 údajů 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.

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

- eGovernment Online Service Bus
- Centrální místo služeb
- propojeny_datovy_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.

Úplné elektronické podání

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí respektovat všechny návazné funkční celky jako např. propojený datový fond, portály veřejné správy či komunikační infrastrukturu veřejné správy a procesně zajistit zpracování podání tak, aby probíhalo elektronicky po celou dobu jeho životního cyklu.</note>

Bude doplněno dle znění zákona o právu na digitální službu.

personalizovaný portál

dostává údaje

předvyplnění údajů

zaručené doručení

zpětné doručení

Propojený datový fond

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí při správě údajů o fyzických a právnických osobách a dalších subjektech využívat služeb propojeného datového fondu, skrze který přebírá referenční údaje základních registrů a agendových údajů agendových informačních systémů.</note>

Těžištěm pro správné využívání a pochopení smyslu propojeného datového fondu je porozumění rozdílu mezi **Poskytováním/Využíváním údajů, Poskytováním/Využíváním dokumentů, Výstupům z informačního systému a Výpisem z informačního systému**.

Poskytování / Využívání údajů

Na business vrstvě orgán veřejné moci, který provádí výkon veřejné správy, působí v agendě, kterou má řádně ohlášenou v RPP, má povinnost využívat pro tyto účely aktuální státem garantovaná data ze ZR a dále publikovat a čerpat agendové údaje přes informační systém sdílení údajů. Soukromoprávní subjekt údajů (také jako SPUU) může také za dodržení zákonného zmocnění pro výkon veřejné správy a působení v určité agendě ohlášené OVM, čerpat údaje ze základních registrů, ovšem výhradně přes AIS OVM nebo formuláře Czech POINT. V zákoně č. 111/2009 Sb. - Zákon o základních registrech, bude nově zakotveno globální zmocnění na čerpání údajů OVM ze ZR, přičemž RPP slouží jako zdroj informací pro informační systém ZR při řízení přístupu uživatelů k údajům v jednotlivých registrech a agendových informačních systémech. To znamená, že kdykoliv se daný subjekt pokusí získat určitý údaj, nebo ho dokonce změnit (editovat), systém posuzuje, zda subjektu bude dovolené na základě zákonného zmocnění pracovat s údaji poskytované veřejnou správou. V RPP jakožto metainformačním systému výkonu veřejné správy jsou uvedeny oprávnění v rámci agend pro čerpání údajů ze ZR, ale také veškeré údaje, které stání správa a samospráva publikuje za pomocí informačního systémů sdílení údajů napříč veřejnou správou. Důležitým faktorem na business vrstvě v rámci čerpání údajů ze ZR a také publikování a čerpání údajů v rámci jednotlivých AIS OVM je mít řádně hlášenou agendu v RPP, což je nezbytnou podmínkou.

Seznam agend vedených v RPP je k dispozici na stránkách: https://rpp-ais.egon.gov.cz/gen/agendy-detail/

Na aplikační vrstvě, prostřednictvím webových služeb jednotlivých referenčních rozhraní, ke kterým patří informační systém správy základních registrů, Informační systém sdílení údajů, služby Czech POINT a formulářového agendového informačního systému FAIS, má povinnost instituce čerpat referenční údaje ze ZR svými AIS a dále poskytovat a využívat údaje přes Informační systém sdílení údajů napříč veřejnou správou. Dále je možné čerpat referenční údaje ze ZR i přes datové schránky.

Jedním z pravidel ziskavani_referencnich_udaju webovými službami je nejdříve ztotožnit svůj datový kmen vůči ZR a následně se přihlásit pro příjem notifikací o změnách. Další možností, ovšem v krajních případech, pokud datový kmen instituce není příliš rozsáhlý, je možné provádět pravidelnou aktualizaci údajů celého datového kmene pro ztotožnění subjektu údajů práva při výkonu veřejné správy.

Dalším pravidlem pro nakládání s osobními údaji je pseudonymizace údajů, což znamená uložení dat technikou oddělení agendových a identifikačních údajů a jejich propojení pomocí agendového identifikátoru fyzických osob (také jako AIFO), aby byly naplněny podmínky bezpečnosti a jednotlivých zákonů a nařízení, které z těchto okolností plynou. Získané AIFO nesmí za žádných okolností opustit AIS, které ho ze služeb ISZR získalo a při jeho předávání (za účelem předávání informací o fyzické osobě) se musí vždy použít služeb ISZR. Více informací o

způsobu využití AIFO v rámci pseudonymizace je uvedeno zde.

- Informace ohledně ZR jsou k dispozici na stránkách: http://www.szrcr.cz/vyvojari
- Informace, jakým způsobem připojit svůj AIS nebo komunikační sběrnici do ISZR jsou k dispozici na stránkách: http://www.szrcr.cz/file/170/
- Informace, jakým způsobem využívat notifikace ze ZR je k dispozici na stránkách: http://www.szrcr.cz/spravny-postup-prace-s-notifikacemi-a-udrzovani-datoveho
- Informace k popisu služeb ZR: http://www.szrcr.cz/file/175/display/
- Podrobný popis služeb ZR: http://www.szrcr.cz/vyvojari/podrobny-popis-egon-sluzeb-zakladnich-registru

Z pohledu technologické vrstvy, je čistě na jednotlivé instituci, jakou si zvolí platformu v rámci vnitřního fungování úřadu a připojení se pro využívání služeb propojeného datového fondu, přičemž přistupovat do ZR je možné přes ISZR přímo AISem nebo komunikační sběrnicí.

Na komunikační vrstvě je povinnost instituce při výkonu veřejné správy využívat CMS. CMS je systém, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů veřejné správy ke službám (aplikacím), které poskytují informační systémy jiných subjektů veřejné správy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu. CMS tak můžeme nazvat privátní sítí pro výkon veřejné správy na území státu. CMS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (také jako OVS) pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do Internetu.

Poskytování / Využívání dokumentů

Dokumenty se nepřenáší skrze referenční rozhraní, ale skrze informační systém datových schránek. Dokumenty se tvoří výstupem z informačního systému veřejné správy dle zákona č.365/2000 Sb.

Výpisy z informačního systému

Výpis z informačního systému je informace, která má elektronickou podobu a vytváří se z veřejných evidencí. To znamená, výpis není personifikován pro konkrtění osobu a všechny obsažené informace jsou veřejné. Výpisy se tvoří dle zákona č. 365/2000 Sb.

Výstupy z informačního systému

Výstup z informačního systému je dokument, ať už v elektronické nebo listinné podobě, tvořený pro konkrétní osobu, přičemž obsahuje veřejné i neveřejné informace. Existuje i varianta ověřeného výstupu, která vznikla úplným převodem výstupu z informačního systému veřejné správy z elektronické do listinné podoby a obsahuje náležitosti dle zákona č.365/2000 Sb.

Veřejný datový fond

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.

Úřad musí zajistit, že svá data, u kterých je to relevantní, zveřejní jako otevřená data včetně všech náležitostí.</note>

Možnosti přípravy IS pro otevřená data

Zásadní je mít přístup k datům IS. Provozovaný IS tedy musí:

1. umožňovat přístup k databázi nebo
2. mít možnost stahovat volitelně strukturovaná data (tabulky) z reportingového modulu systému nebo
3. nabídnout API, ze kterého se dají pravidelně získávat kompletní data v podobě datových souborů

Export dat nebo API v otevřeném formátu - preferované řešení

IS má rozhraní pro pravidelný export dat nebo neomezené API, které organizace může vytěžit a získat kompletní data v jednom z otevřených formátů.

- Pro tabulková data je to CSV
- Pro hierarchická data je to XML nebo JSON
- Pro grafová data je to RDF
- Pro geodata je to jeden z otevřených formátů pro geodata - GeoJSON, ESRI Shapefile, OGC GML, OGC GeoPackage.

Struktura dat je zdokumentována jednak lidsky čitelným dokumentem a jednak strojově čitelným schématem.

- Pro CSV je to schéma CSV on the Web
- Pro XML je to XML Schema
- Pro JSON je to JSON schema
- Pokud je použit vlastní slovník pro RDF, je popsán pomocí RDFS nebo OWL

V takovém případě jsou získaná kompletní data z IS připravena k publikaci formou otevřených dat.

Export dat nebo API v proprietárním formátu

Pokud se jedná o rozšíření existujícího IS, který neumožňuje export dat nebo nenabízí API ve strojově čitelném a otevřeném formátu a takovou úpravu nelze ve Vašem IS provést, využije se stávající export či API, které váš IS již umí (např. do MS Excel), a tento výstup se dále zpracuje do otevřeného formátu pomocí dalších nástrojů tak, aby bylo dosaženo stavu jako v případě přímého exportu do otevřeného formátu.

Následná příprava dat k publikaci v podobě otevřených dat

Data získaná z IS jedním z popsaných způsobů je následně třeba publikovat jako otevřená data. To znamená minimálně:

1. V případě API zajistit jeho vytěžení pro získání kompletních dat k publikaci (tj. případná přímá publikace API nenaplňuje podmínky otevřených dat)
2. Zajistit pravidelnou aktualizaci získaných dat (dle charakteru dat to může být ve frekvenci např. denně, měsíčně nebo ročně)
3. Publikovat získaná data na web ke stažení a následně publikovat každou jejich aktualizaci
4. Opatřit je dokumentací, podmínkami užití a kontaktem na kurátora
5. Katalogizovat je v Národním katalogu otevřených dat (NKOD)

K tomu lze využít nástrojů pro přípravu, publikaci a katalogizaci otevřených dat, jako je třeba LinkedPipes ETL.

Publikace otevřených dat by měla být zajištěna koncepčně na úrovni celé organizace. Kompletní postupy jsou k dispozici na Portálu otevřených dat, naleznete zde rovněž informace o školeních a workshopech, které Ministerstvo vnitra k této problematice poskytuje.

Pro příklad vhodného způsobu zveřejnění datové sady v lokálním katalogu se lze podívat na katalog České správy sociálního zabezpečení (ČSSZ).

Ochrana osobních údajů

Pokud jsou předmětem evidence informačního systému osobní údaje ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů a nařízení (EU) č. 2016/679, Obecné nařízení o ochraně osobních údajů (GDPR), neznamená to, že nelze ze systému publikovat otevřená data. Ve formátu otevřených dat lze zveřejnit následující:

1. Pakliže se jedná o veřejnou evidenci či rejstřík a zvláštní právní předpis nařizuje zveřejnění informací, lze zveřejnit osobní údaje v podobě otevřených dat.
2. Anonymizace či Pseudonymizace. Z dat se odstraní osobní údaje a případně se nahradí bezvýznamovým umělým identifikátorem. Data bez osobních údajů se pak mohou zveřejnit v podobě otevřených dat. Ovšem pozor, v závislosti na charakteru dat je třeba zkontrolovat, zda data ve své kombinaci neumožňují identifikaci konkrétní osoby i po odstranění zjevných osobních údajů. Zejména se může jednat o kombinace jako město, věk a pohlaví nebo podobné.
3. Agregace. Data, která není možné nebo vhodné zveřejnit dle předchozího bodu, lze zveřejnit v agregované podobě. Tedy v podobě statistik. V případě zveřejnění statistik je žádoucí použít co nejjemnější možné členění.Tedy například počet přijatých podání uvádět raději po měsících namísto jen po letech.

Právní aspekty

Legislativní rámec otevřených dat v České republice tvoří jejich úprava obsažená v Zákoně č. 106/1999 Sb., o svobodném přístupu k informacím a v Nařízení vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data, které stanovuje vybraným orgánům veřejné správy povinnost zveřejňovat data z konkrétních jimi spravovaných informačních systémů ve formě otevřených dat.

Více informací o strategických dokumentech, akčních plánech a souvisejících předpisech ČR i EU naleznete na stránce věnované legislativnímu prostředí otevřených dat.

Elektronické úkony a doručování

Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>

Využívání oprávněných osob

Integrace do eSSL

Využití identitního prostoru ISDS

Doručování VS Dodávání VS Podání

Jednotné obslužné kanály a uživatelská rozhraní úředníků

Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v

části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>

Národní datová centra

Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>

eGovernment cloud

Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy. Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>

Rozhodnutí o vstupu do eGC

Jedním ze dvou hlavních kritérií pro využití služeb Státní část eGovernment Cloudu (také jako SeGC) nebo Komerční část eGovernment cloudu (také jako KeGC) je úroveň bezpečnostních dopadů daného IS. SeGC zajistí maximální úroveň bezpečnosti a je určen pro provoz služeb eGC bezpečnostní úrovně 4 (Kritická). KeGC je určen pro provoz služeb eGC bezpečnostních úrovní 1-3 (Nízká, Střední, Vysoká) 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. K oběma způsobům stanovení bezpečnosti a ekonomické náročnosti vznikly metodické pomůcky dostupné na:

- Stanovení ekonomické náročnosti
  - Metodika
  - Pomocný excel
- Stanovení požadavků na bezpečnost
  - Metodika
  - Pomocný excel

Správce eGC do konce října 2019 zveřejní dynamický nákupní systém (také jako DNS) pro nákup eGC služeb vedených v jeho katalogu. Portál pro objednávání a správu služeb nebude spuštěn spolu s DNS, ale jeho spuštění se dá očekávat v první polovině roku 2020.

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 infrastrukturu od samotné technologické 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.

V následující fázi budování eGC, dlouhé zhruba dva roky, bude umísťování IS do eGC (využívání služeb eGC) dobrovolné. Dlouhodobě bude uplatněn princip cloud-first – povinné umístění IS do eGC, pokud kalkulace TCO neprokáže nákladově efektivnější provoz onpremise.

Sdílená síťová a komunikační infrastruktura

Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>

Sdílené agendové IS v přenesené působnosti

Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>

Sdílené agendové IS pro samostatnou působnost územních samospráv

Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>

Sdílené provozní informační systémy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci správy dokumentů je uveden zde a popsán v části Architektura a sdílené služby veřejné správy.

Využití a popis k přístupu kontaktních míst a obslužných kanálů pro klienty VS popíše úřad do své informační koncepce v části XXX.</note>