

Materiál Ministerstva vnitra



Export z Národní architektury eGovernmentu ČR

Obsah

Pravidla pro architekturu sdílených služeb, funkčních celků a tématických oblastí jednotlivých

úřadů	3
<i>Pravidla pro Agendový model veřejné správy</i>	<i>3</i>
<i>Pravidla pro Propojený datový fond</i>	<i>6</i>
<i>Pravidla pro Veřejný datový fond</i>	<i>9</i>
<i>Pravidla pro Úplné elektronické podání</i>	<i>13</i>
<i>Pravidla pro Portály veřejné správy a soukromoprávních uživatelů údajů</i>	<i>13</i>
<i>Pravidla pro Přístupnost informací</i>	<i>16</i>
<i>Pravidla pro Elektronickou fakturaci</i>	<i>17</i>
<i>Pravidla pro Elektronickou identifikaci klientů veřejné správy</i>	<i>17</i>
<i>Pravidla pro Univerzální kontaktní místo veřejné správy</i>	<i>20</i>
<i>Pravidla pro Systém správy dokumentů</i>	<i>21</i>
<i>Pravidla pro Elektronické úkony a doručování</i>	<i>21</i>
<i>Pravidla pro Jednotný identitní prostor veřejné správy</i>	<i>22</i>
<i>Pravidla pro Jednotné obslužné kanály a uživatelská rozhraní úředníků</i>	<i>22</i>
<i>Pravidla pro Sdílené agendové IS v přenesené působnosti</i>	<i>22</i>
<i>Pravidla pro Sdílené agendové IS pro samostatnou působnost územních samospráv</i>	<i>22</i>
<i>Pravidla pro Sdílené provozní informační systémy</i>	<i>23</i>
<i>Pravidla pro eGovernment cloud</i>	<i>23</i>
<i>Pravidla pro Národní datová centra</i>	<i>24</i>
<i>Pravidla pro komunikační infrastrukturu veřejné správy</i>	<i>24</i>

~~Title: Pravidla pro architekturu sdílených služeb, funkčních celků a tématických oblastí jednotlivých úřadů~~

Pravidla pro architekturu sdílených služeb, funkčních celků a tématických oblastí jednotlivých úřadů

Tato kapitola popisuje sdílené služby, funkční celky a tématické oblasti v celé šíři (v celé architektuře) včetně pravidel, návodů a dobrých praktik k jejich zanesení do informační koncepce a architektury úřadu. 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 sdíleným službám, funkčním celkům a tématickým oblastem z části [Architektura a sdílené služby veřejné správy](#):

Tématické oblasti

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

Sdílené služby a funkční celky

- **Elektronická identifikace pro klienty veřejné správy - NIA**
- **Univerzální kontaktní místo veřejné správy - CzechPOINT**
- **Elektronické úkony a doručování - Datové schránky**
- **Systém správy dokumentů - eSSL**
- **Jednotný identitní prostor veřejné správy - JIP/KAAS**
- **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**
- **eGovernment Cloud**
- **Národní datová centra**
- **Komunikační infrastruktura veřejné správy - KIVS/CMS**

Pravidla pro Agendový model veřejné správy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci agendového modelu veřejné správy 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>

Na byznysové vrstvě

Na byznys vrstvě architektury veřejné správy se jedná o základní byznysový model fungování veřejné správy. Kombinace agendy, působících OVM, činností, činnostních rolí a oprávnění je jasným modelem fungování OVM celé veřejné správy, alespoň co se týče veřejnoprávních činností.

Při aplikaci principů referenčnosti údajů v registrech tedy platí, že pokud kterýkoliv OVM vykonává veřejnoprávní činnost a není k tomu zmocněn nikoliv pouze zákonem, ale především ohlášením a registrací působnosti v dané agendě, je tento stav v rozporu se zákonem. To se netýká jen využívání údajů, ale každé činnosti ohlášené, resp. neohlášené, v agendě.

Na úrovni byznysové architektury každého úřadu je pak agendový model veřejné správy skládající se zejména z referenčních údajů jednotlivých agend zapsaných v Registru práv a povinností základní byznysovou a motivační vrstvou pro výkon jeho veřejnoprávních činností.

To, co je v Registru práv a povinností označeno jako

- Agenda, ve které vykonává příslušný úřad nějakou působnost a
- agendová činnost, kterou prostřednictvím činnostní role daný úřad vykonává

jsou prvky, na základě kterých vykonává každý konkrétní úřad svoje procesy a činnosti.

To, co je v Registru práv a povinností u agendy zapsáno jako přístup či využívání údajů z příslušných agendových informačních systémů nebo ze základních registrů je potom na byznysové vrstvě každého konkrétního úřadu bráno jako datové objekty a jejich zdroje při využívání a správě údajů v dané agendě.

Agendový model veřejné správy tedy zasahuje jak do byznysové, tak do procesní i datové architektury úřadu. Na byznysové vrstvě se jedná o nejdůležitější architektonický prvek, jehož zdrojem navíc není architektura příslušného úřadu, ale vždy aktuální stav referenčních údajů v ohlášených agendách v Registru práv a povinností.

Zejména na byznysové vrstvě architektury úřadu je pak nutno rozlišovat, jestli je daný OVM jen čtenářem údajů z registrů, nebo jejich editorem. To má pak hluboké konsekvence, jako třeba:

1. Je-li daný OVM editorem údajů v základních registrech
 - Musí zajistit zápis údajů do základních registrů prostřednictvím [ISZR](#)
 - Musí si vytvořit procesy pro správnou editaci údajů, ale také pro vyřizování jejich reklamace, zpochybňování apod.
2. Je-li daný OVM pouze uživatelem údajů ze základních registrů
 - Využívá údaje z registrů prostřednictvím [eGSB](#)
 - Vybuduje si procesy, které zajistí naplnění povinnosti zahájit reklamaci u údaje, u kterého zjistil nesoulad, a to směrem k příslušnému editorovi
 - Nastaví si procesy, které zajistí aktualizaci údajů po jejich reklamaci

Pochopitelně většinou platí, že OVM, který je v určité agendě editorem, je v ostatních agendách čtenářem, takže na byznysové vrstvě je nutno myslet na obě tyto role.

Na aplikační vrstvě

Každý úřad si zpracovává svoji aplikační architekturu. Na vrstvě aplikací nesmí zapomenout na to, že každý jeho agendový informační systém (i ten který sice nespravuje, ale používá) podporuje činnosti v rámci jedné či více agend. Tedy v rámci aplikační architektury.

- Zavede veškeré AISy do své aplikační architektury, a to
 - Ty, které sám spravuje až na úroveň komponent
 - Ty, které využívá na úroveň AIS a jeho integrace
- U každého informačního systému (zejména AIS) má zapsanou vazbu na agendy, které AIS podporuje a takto jej také ohlásí do RPP
- Zná podrobnosti o fungování svých i cizích AISů tak, aby byl schopen na ně reagovat i v architektuře

Ve skutečnosti to opět znamená, že si veškeré základní komponenty svých IS je schopen navázat na agendy a činnosti, které tyto systémy podporují a je tak schopen reagovat na změny v agendách na byznysové vrstvě i úpravou informačních systémů.

Na integrační vrstvě

Při tvorbě architektury v rámci úřadu je na integrační vrstvě počítat s integrací na základní komponenty eGovernmentu, a to podle požadavků, které jsou definovány zákonnými povinnostmi a reprezentovány v jednotlivých agendách veřejné správy. Je tedy vždy, pokud daný úřad vykonává agendovou činnost, nutno počítat s následujícími integracemi:

- Pokud je úřad editorem údajů v základních registrech, tak se integruje prostřednictvím [ISZR](#) a jeho služeb
- Úřad integruje svoje agendové informační systémy na základní registry a další AIS prostřednictvím [eGSB](#) a jeho služeb

Nesmí se zapomínat ani na nutnou vnitřní integraci v rámci úřadu, a to mezi jednotlivými AISy a u agendových informačních systémů směrem k provozním IS. Takovým typickým příkladem je integrace agendového informačního systému na elektronický systém spisové služby pro zajištění procesů a úkonů spojených s evidencí dokumentů a se zpracováním digitálních dokumentů a s vedením jmenného rejstříku o subjektech, nebo integrace na ekonomický systém pro zajištění ekonomických úkol, třeba poplatků, dávek, pohledávek, pokut apod.

Na procesní vrstvě

Úřad musí u všech svých procesů vědět, jestli a na základě jakých agend veřejné správy je vykonává a jaké mají vazby na společné procesy, které reprezentují společné věci a schopnosti úřadu. Kupříkladu u jednotlivých agendových procesů musí být jasné, že se jedná o proces agendy, ale zároveň v procesech agendy musí být vazba i na společné procesy, jako je například vedení spisové služby, správa dokumentace, přidělování rolí, řešení ekonomických úloh, řešení právních sporů, sledování termínů a další.

Je-li úřad zároveň i gestorem některých agend, musí být schopen je pro sebe i pro všechny v nich působící OVM procesně modelovat podle příslušných standardů PMA v ČR.

Procesní modely jsou pak důležité pro datovou architekturu, pro skladbu a vazby jednotlivých AISů a jejich komponent apod.

Na datové vrstvě

U údajů vedených v informačních systémech platí, že úřad eviduje jen ty údaje, u kterých to má stanoveno legislativou a eviduje sám primárně jen ty údaje, které má jako svoje agendové a ne ty referenční ze základních registrů a ty z jiných agendových informačních systémů. Tedy u každého údaje musí být jasné, na základě kterého zmocnění je eviduje a musí jej mít zapsán v agendě, a to jako:

- Referenční údaje vedené v základních registrech (využívám je)
- Údaje z jiných informačních systémů (využívám je)
- Vlastní agendové údaje (spravuji je)

- Agendové údaje, které poskytují jiným agendám (poskytují je)

Co to znamená pro úřad:

- Základem pro můj byznysový model fungování úřadu jsou údaje z RPP
- Pokud se údaje v RPP liší od skutečnosti, reklamují údaje agend u jejich ohlašovatelů
- Využívám údaje z RPP jako primární zdroj, nestavím si znovu byznys model
- V procesním a byznysovém modelu úřadu jsem schopen u každého elementu udělat vazbu na příslušný element v modelu z RPP
- Zním agendy, ve kterých působím, činnosti, které vykonávám, činnostní role, zodpovědnosti ohlašovatele/editora/uživatelé agend a údajů a mám je zakreslené ve svém byznysovém modelu
- Datové objekty v byznysové vrstvě architektury úřadu mám namapovány na údaje v agendách a jako jejich zdroje znám publikující služby příslušných AISů.

Pravidla pro Propojený datový fond

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci propojeného datového fondu 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>

Povinnost využívat referenční rozhraní

Povinnost využívat referenční rozhraní pro uskutečňování takzvaných "vazeb" mezi jednotlivými informačními systémy veřejné správy ukládá zákon o informačních systémech veřejné správy. Tedy obecně platí, že pro sdílení údajů, výměnu údajů a propojování jednotlivých informačních systémů veřejné správy různých správců, má být primárně využíváno právě referenční rozhraní. U informačních systémů stejného správce toto nemusí platit vždy, pokud se nevyužívá překlad agendových identifikátorů při komunikaci o subjektu údajů vedené v rámci dvou nebo více agend.

Je nutné zdůraznit, že pouze využitím referenčního rozhraní je korektně prováděn překlad AIFO (AIFO jedné osoby v jedné agendě nesmí být poskytnuto jiné agendě). Pouze referenční rozhraní je napojeno na registr ORG a provádí překlad AIFO.

Užívání referenčního rozhraní při výměně údajů v rámci propojeného datového fondu

Výměna/sdílení údajů mezi jednotlivými informačními systémy veřejné správy se realizuje výhradně prostřednictvím referenčního rozhraní, a to konkrétně komponenty [eGSB](#). Jak se upřesňuje v části [propojený datový fond](#), tak výměna údajů se realizuje vždy v rámci kontextu na subjekt práva.

Správci agendových informačních systémů musejí realizovat napojení na referenční rozhraní, a to podle příslušných metodických dokumentů a provozních řádů:

- [Provozní řád ISZR](#)
- [Podmínky pro připojení AIS k ISZR](#)

Užívání referenčního rozhraní pro poskytování sdílených služeb

Správci agendových informačních systémů poskytujících údaje z daných agend realizují napojení svých AISů na **eGSB** v roli publikátora a kontrolu oprávnění k využívání údajů podle oprávnění v **RPP**. Pro výměnu údajů vybudují služby svého AIS tak, aby mohly být volány a zprostředkovány **eGSB**.

Užívání referenčního rozhraní pro využívání sdílených služeb

Správci agendových informačních systémů využívajících údaje poskytované jinou agendou realizují volání služeb **eGSB** (nemusí znát konkrétní AIS, požadují údaje od agendy), a to jen tehdy, pokud k tomu mají příslušné oprávnění zapsané u agendy poskytovatele v **RPP**.

Užívání referenčního rozhraní při zápisu a editaci údajů v základních registrech

Editoři referenčních údajů v základních registrech realizují napojení svých editorských agendových informačních systémů na **ISZR** službami vnějšího rozhraní podle příslušné dokumentace Správy základních registrů. Pro editaci údajů a vyřizování reklamací údajů v základních registrech nevyužívají jiné rozhraní než právě ISZR.

Evidence subjektů

Jako identifikátor fyzické osoby, se v různých agendách používají různé druhy identifikátorů, a to jak pro účely vnitřních procesů a služeb (uvnitř úřadu), , tak i při výměně údajů (ven z úřadu). Toto je nutno změnit, proto je nutno respektovat níže uvedené základní principy pro evidenci subjektů:

1. Identifikátorem pro komunikaci mezi jednotlivými agendovými informačními systémy je vždy AIFO (a překládá se AIFO2AIFO přes služby ORG).
2. Úředním/klientským identifikátorem fyzické osoby může být klientské číslo pro danou agendu, které přidělí správce dané agendy a které se využívá jako prezentovaný identifikátor v AISu a pro úředníka.
3. Při komunikaci s klientem (osobní jednání na přepážce, i zpracování doručených dokumentů a zpráv) se využívají stykové identifikátory, jako jsou typ a číslo dokladů a využije se služba překladu na AIFO.
4. Stykové identifikátory si primárně neevidují, leda by byly zároveň klientským číslem.
5. AIFO osoby se nikdy nesmí přímo poskytnout, vždy se využívá služeb překladu z mého AIFO na AIFO příjemce výměny údajů.
6. Pokud k tomu nejsou specifické závažné důvody, tak při výměně údajů využívám pouze AIFO a nepřidávám k tomu další identifikátory nebo referenční údaje.

Údaje, dokumenty, výstupy a výpisy

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 státní správa a samospráva publikuje za pomoci informačního systému 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 [získávání referenčních údajů](#) 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 sběrnici.

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 nepřenášejí 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 konkrétní 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.](#)

Pravidla pro Veřejný datový fond

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci veřejného datového fondu 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>

VDF je tvořen otevřenými daty poskytovanými jednotlivými OVS za účelem sdílení s dalšími OVS a je podmnožinou všech otevřených dat VS. Je tedy nutné zajistit, aby všechny funkční celky architektury jednotlivých úřadů VS respektovaly a dodržovaly pravidla platná pro:

- otevřená data (legislativně podpořená zákonem č.106/1999 Sb.),
- data VDF - pravidla pro otevřená data navíc doplněná o další specifika odvozená od charakteristik VDF.

Otevřená data

Otevřená data jsou:

- Volně přístupná na webu jako datové soubory ke stažení ve strojově čitelném a otevřeném formátu - CSV, XML, JSON, RDF (JSON-LD, Turtle, ...) a další formáty s otevřenou specifikací.
- Opatřená podmínkami užití neomezuujícími jejich užití.
- Evidovaná v Národním katalogu otevřených dat (NKOD) jako datové sady opatřené přímými odkazy na datové soubory, které je tvoří.
- Opatřená úplnou dokumentací.
- Opatřená kontaktem na kurátora pro zpětnou vazbu (chyby, žádost o rozšíření, apod.).
- Jsou publikovány dle otevřených formálních norem ve smyslu § 4b odst. 1 zákona č. 106/1999 Sb. o svobodném přístupu k informacím.

Využívání otevřených dat při výkonu veřejné správy

Nejsou stanovené žádné požadavky na způsoby použití publikovaných otevřených dat, data lze libovolně

importovat do vhodných aplikací a informačních systémů. Publikovaná data jsou zpřístupněna prostřednictvím NKOD (POD) a lze je získat jako soubory s datovými sadami. K datům lze také přistupovat s využitím aplikací třetích stran, které příslušné data využívají.

Publikace otevřených dat

Příprava ISVS pro export otevřených dat

Zásadní je zajištění přístupu k datům IS. Provozovaný IS tedy musí:

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

Vhodné otevřené formáty:

- tabulková data - CSV, XML, JSON, RDF (JSON-LD, Turtle, ...),
- hierarchická data - XML, JSON, RDF (JSON-LD, Turtle, ...),
- grafová data - RDF (JSON-LD, Turtle, ...),
- geodata - GeoJSON, ESRI Shapefile, OGC GML, OGC GeoPackage.

Struktura dat musí být zdokumentována lidsky čitelným dokumentem, ale také strojově čitelným schématem. Doporučené jazyky pro definici schémat schémata:

- CSV - schéma CSV on the Web,
- XML - XML Schema,
- JSON - JSON schema,
- RDF - RDFS, OWL, SHACL

Při dodržení výše uvedených bodů 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 v IS provést, využije se stávající export či API, které již systém nabízí (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.

Závěrečná příprava dat k publikaci v podobě otevřených dat

Data získaná z IS jedním z popsanych 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 nenaplnuje 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 POD, včetně vyžadovaných standardů.

Data VDF

Otevřená data ve VDF

Ve VDF jsou poskytována otevřená data, která jsou určena mj. k využití jinými OVS při výkonu veřejné správy i mimo jejich rozsah práv a povinností zachycených v RPP. Nad rámec otevřených dat platí pro otevřená data ve VDF následující:

- Pokud OVS využívá data z VDF, považuje je za správná a nemusí ověřovat jejich správnost.
- Poskytovatel dat do VDF garantuje správnost, kvalitu, aktuálnost a pravidelnou aktualizaci údajů publikovaných ve VDF.
- Poskytovatel dat do VDF zajišťuje automatickou notifikaci všech změn v údajích publikovaných ve VDF zaregistrovaným zájemcům s využitím funkcionality Portálu otevřených dat.

Využívání otevřených dat z VDF při výkonu veřejné správy

Při výkonu veřejné správy může OVS potřebovat údaje jiných OVS, kterým ale nemá přístup v rámci rozsahu stanoveného v RPP. Pokud se jedná o veřejné údaje, přistupuje k nim prostřednictvím VDF. Jsou-li data ve VDF dostupná, není žádný jiný způsob přístupu k datům a sdílení dat povolen. Typicky jsou data z VDF využívána následujícím způsobem:

- ruční vyhledání potřebných datových sad v NKOD a zjištění odkazů ke stažení dat,
- nastavení skriptů k pravidelnému importu nalezených datových sad do vlastního IS ze zjištěných odkazů,
- import datových sad do IS VS,
- registrace v Notifikačním hubu k pravidelnému a strojovému získávání aktualizací,
- nastavení skriptů k importu změn získaných z Notifikačního hubu do IS VS.

Publikace otevřených dat do VDF

Pro publikaci otevřených dat do VDF platí stejná pravidla jako pro publikaci otevřených dat uvedená výše. Navíc musí být dodržena následující pravidla:

- Publikovaná data jsou popsána sémantickým slovníkem pojmů, který je vytvořen na základě údajů v RPP. Popis dat sémantickým slovníkem pojmů je vytvořen a publikován dle otevřené formální normy "Popis dat sémantickým slovníkem pojmů". Sémantický slovník pojmů je tvořen a publikován dle otevřené formální normy "Sémantický slovník pojmů".
- K identifikaci entit, o nichž jsou publikovány údaje ve VDF, jsou použita IRI dle otevřené formální normy "Propojená data".
- V publikovaných datech se nepublikují duplicitní údaje s již publikovanými údaji ve VDF. V případě, že OVS publikuje údaje o entitě, o níž již publikuje ve VDF údaje jiný OVS, publikuje OVS pouze nové doplňující údaje k této entitě. V případě, že zavádí vlastní IRI k identifikaci entity než jiný OVS, propojí vlastní IRI s původním dle otevřené formální normy "Propojená data".
- Souvislosti mezi entitami v datech stejného poskytovatele i různých poskytovatelů jsou reprezentovány dle otevřené formální normy "Propojená data". Poskytovatel údajů ve VDF se snaží maximálně propojit entity, o nichž publikuje údaje, na entity o, nichž publikují údaje jiné OVS.

Společná pravidla pro otevřená data i data VDF

Organizační a procesní zajištění publikace dat

Zapojení VDF do výkonu veřejné správy vyžaduje publikaci skutečně právně závazných, platných a pravidelně aktualizovaných datových sad s jasně definovanou zodpovědností OVS za takové sady. Publikující organizace musí pro splnění uvedených požadavků realizovat vhodná organizační opatření, přiřadit pracovníkům příslušné procesní role a implementovat činnosti publikačních procesů do pracovních náplní pracovníků. Jako minimum je vyžadováno přiřazení těchto klíčových procesních rolí:

- Koordinátor otevírání dat, do jehož kompetencí a povinností spadá:
- zajištění součinnosti a kontroly výstupů všech ostatních rolí, které se na otevírání dat podílejí,
- komunikace se všemi zapojenými pracovníky do publikace dat,
- externí komunikace s uživateli otevřených dat VS,
- komunikace a spolupráce s Národním koordinátorem otevřených dat,
- komunikace s Datovou kanceláří a s příslušným Chief data officer (CDO).

Kurátor dat - klíčová role pro:

- zajištění kvality, správnosti, aktuálnosti a tím i právní závaznosti dat konkrétní agendy,
- publikaci datových sad v souladu s platnými právními předpisy ČR a Standardy publikace a katalogizace otevřených dat VS ČR.

Kompletní doporučení, vhodné vzory interních dokumentů, všechny navržené procesní role a standardní publikační procesy jsou uvedeny na Portále otevřených dat.

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. V těchto případech platí následující doporučení.

1. V případě, že se jedná o veřejnou evidenci či rejstřík a zvláštní právní předpis nařizuje zveřejnění informací, lze zveřejnit osobní údaje v podobě otevřených dat.
2. Ochranu osobních údajů lze zajistit Anonymizací či Pseudonymizací. 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. V závislosti na charakteru dat je ale nutné zkontrolovat, zda data ve své kombinaci neumožňují identifikaci konkrétní osoby i po odstranění zjevných osobních údajů. Může se jednat o kombinace typu město, věk a pohlaví a podobné.
3. Data, která není možné nebo vhodné zveřejnit dle předchozího bodu, lze zveřejnit v agregované podobě. Tedy v podobě statistik. V případě zveřejnění statistik je ale žádoucí použít co nejmenější granularitu dat a časové členění.

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. Podrobnější informace o strategických dokumentech, akčních plánech a souvisejících předpisech ČR i EU jsou k dispozici v aktualizované podobě na stránkách Portálu otevřených dat (POD).

Pravidla pro Úplné elektronické podání

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci úplného elektronického podání 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>

Úřad pro splnění požadavků kladených na úplné elektronické podání musí splnit svými obslužnými kanály (např. portál):

- Využití [Jednotného identitního prostor veřejné správy](#) pro úřední osoby a [Elektronickou identifikaci pro klienty veřejné správy](#).
- Předvyplnění podání všemi státními známými údaji klientovi po prokázání elektronickou identitou. Zajištění tohoto požadavku se splní čerpáním údajů z [Propojeného datového fondu](#).
- Má služby svých agend v rámci ÚEP a jejich IT aplikace navrženy tak, aby služby bylo možno v obslužných kanálech kombinovat pro efektivní řešení životních událostí.
- Umožňuje klientům učinit podání skrze různá elektronická rozhraní (webová stránka, formulář nebo asistovaná služba) a sledovat průběh vyřizování jejich podání skrze to samé rozhraní, přes které bylo podání realizované nebo jiné klientem určené.
- Postupně všechna existující práva a povinnosti ze vztahu k VS budou doprovázena transakční službou (nejenom popisem návodu) v [Portálu občana](#), a to v těch všech případech, kdy elektronická transakční služba bude proveditelná a bude odpovídat oprávněným zájmům klientů a současně i úřadů.
- Elektronické podání formou ÚEP lze uskutečnit i papírově (off-line), tzn. půjde stáhnout předvyplněný formulář, ručně vyplnit, zaslat datovou schránkou nebo elektronicky podepsané doručit jakkoli jinak (i mailem, vložením do portálu), případně vložit do elektronické aplikace úřadu.
- V případě menší četnosti podání stačí jeden z obou kanálů (on-line nebo off-line), musí však umožňovat dobrou (personalizovanou) navigaci ke službě a k jejímu předvyplnění.
- Stejnou službu lze získat s pomocí služby úředníka na kterémkoli fyzickém kontaktním místě asistovanou formou. Pro typové a jednoduché podání pro řešení typových životních situací to takto bude možné na [Univerzálních asistovaných kontaktních místech](#).
- Zůstanou zachovány tradiční kanály pro příjem listinných podání osobně, diktátem do protokolu nebo poštou – úřední přepážky a podatelny. Jejich úkolem ale bude obdržené vstupy neprodleně plně digitalizovat, aby celé další následné zpracování bylo jednotně plně elektronické.
- Nedílnou součástí řady podání je splnění finanční povinnosti (poplatku, daně). Platební brána tedy musí být součástí obslužného rozhraní. Pro agendy v samostatné působnosti je platební brána plně v zodpovědnosti koncového úřadu, pro agendy v přenesené působnosti musí o způsobu rozhodnout správce agendy.
- Elektronické samoobslužné služby pro klienty/občany i pro právnické osoby musí být doplněny interaktivním podpůrným a poradenským kanálem (service-desk, call-me-back, apod.).
- Podání nemusí vždy činit ta osoba, která je přihlášena [elektronickou identitou](#), ale může se jednat o osobu zastupující jinou osobu. Úřad tedy musí zajistit [správu mandátů](#).
- Pro individuální přizpůsobení uživatelského rozhraní musí úřad využívat tzv. klientské profily. Každý jedinečný a jednoznačně identifikovaný klient má profil jenom jeden. V tomto profilu jsou uchovávány osobní i agendové údaje ve shodě se pravidly správy údajů [Právní aspekty pro pseudonimizaci](#).

Pravidla pro 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 státy 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 veřejné správy](#).

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 [propojený datový fond](#)
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 schopený čerpat a poskytovat údaje skrze systém eGON Service Bus
- Musí dle svého agendového zákona být schopený 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 schopený čerpat a poskytovat údaje skrze systém eGON Service Bus
- Musí dle svého agendového zákona být schopený 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.](#) 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. Může se jednat o portály poskytovatelů zdravotních služeb, soukromých pojišťoven, bank, státních podniků, apod. Takový portál a jeho vlastník musí splnit několik podmínek:

1. 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.
2. 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>.
 - Ohlášení do rejstříku SPUÚ probíhá pomocí agendového informačního systému působnostního viz <https://rpp-ais.egon.gov.cz/AISP/>. Do tohoto systému má přístup každý ohlašovatel agendy.
 - 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, může SPUÚ kontaktovat správce Registru práv a povinností (posta@mvcz.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)
3. 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 žadatel tento typ nemá, je nutné kontaktovat Správu základních registrů skrze datovou schránku napřímo s požadavkem obsahujícím všechny údaje, jako v případě automatizovaného způsobu:

- IČO subjektu
- Název kvalifikovaného poskytovatele (SeP)
- Popis kvalifikovaného poskytovatele
- URL adresa odkazující na úvodní webové stránky
- URL adresa pro odeslání požadavků
- Adresa pro příjem vydaného tokenu (URL)
- URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu
- Načtení certifikátu
- Adresa pro načtení veřejné části šifrovaného certifikátu z metadat (URL). Touto veřejnou částí budou šifrována data v tokenu
- Logo kvalifikovaného poskytovatele

4. Musí umět přijímat a zpracovávat data pomocí standardů SAML2 nebo WS-Federation

Postup ohlášení portálu jako kvalifikovaného poskytovatele služby

- 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 konfiguraci 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 spadajících pod danou organizaci.
- Uživatel provede konfiguraci Service Providera

Pravidla pro Přístupnost informací

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci přístupnosti informací je uveden [zde](#) a popsán v části [Architektura a sdílené služby veřejné správy](#).

Pravidla pro Elektronickou fakturaci

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci elektronické fakturace 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>

Pravidla pro Elektronickou identifikaci klientů veřejné správy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci elektronické identifikace klientů veřejné správy 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 nepopíratelné 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 správný řád (jednoznačné prokázání totožnosti účastníků řízení).

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

- **Identifikace** - jednoznačné a nepopíratelné 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.

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 ověření identity fyzické osoby, neboli každý systém čerpající služby NIA, se může spolehnout na to, že přihlášená fyzická osoba je skutečná 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 infrastruktúře referenčního rozhraní je napsáno v kapitolách:

- [eGovernment Online Service Bus](#)
- [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](#), [rosCtilco](#), [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 zajistil 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 navrhuje:

- 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 provádění úkonů 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.

Pravidla pro 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 [Portál občana](#)
 - 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 služba nesmí být bez své asistované varianty, která však může být řešena i v rámci úřadu, pokud tak vyžaduje její specifická náročnost (například daňové přiznání).

Pravidla pro 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>

Pravidla pro Elektronické úkony a doručování

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci elektronických úkonů a doručování 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.

Využívání oprávněných osob

Integrace do eSSL

Využití identitního prostoru ISDS

Doručování VS Dodávání VS Podání

Pravidla pro Jednotný identitní prostor veřejné správy

Popis centrálně poskytovaných systémů a jejich služeb v rámci jednotného identitního prostoru veřejné správy 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.

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

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

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

Pravidla pro Jednotné obslužné kanály a uživatelská rozhraní úředníků

Popis centrálně poskytovaných systémů a jejich služeb v rámci jednotných obslužných kanálů a uživatelských rozhraní úředníků 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.

Pravidla pro Sdílené agendové IS v přenesené působnosti

Popis centrálně poskytovaných systémů a jejich služeb v rámci sdílených agendových IS v přenesené působnosti 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.

Pravidla pro Sdílené agendové IS pro samostatnou působnost

územních samospráv

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci sdílených agendových IS pro samostatnou působnost 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>

Pravidla pro Sdílené provozní informační systémy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci sdílených provozních IS 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>

Pravidla pro eGovernment cloud

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci eGovernment Cloudu 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 infrastrukturu) 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.

Pravidla pro Národní datová centra

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci národních datových center 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>

Pravidla pro komunikační infrastrukturu veřejné správy

<note important>Popis centrálně poskytovaných systémů a jejich služeb v rámci komunikační infrastruktury veřejné správy 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>

KIVS/CMS je systém, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů státní správy a samosprávy ke službám (aplikacím), které poskytují informační systémy jiných subjektů státní správy a samosprávy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu. KIVS/CMS tak můžeme nazvat privátní sítí pro výkon veřejné správy na území státu. KIVS/CMS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (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.

Komunikace mezi jednotlivými OVS je tak vedena výhradně prostřednictvím KIVS/CMS, Tzn, jednotlivé OVS mají povinnost přistupovat k informačním systémům veřejné správy (ISVS) pouze prostřednictvím KIVS/CMS.

From:
<https://archi.gov.cz/> - Architektura eGovernmentu ČR

Permanent link:
https://archi.gov.cz/nap_dokument:pravidla_pro_funkcni_celky_architektury_jednotlivych_uradu?rev=1566399537

Last update: 2019/08/21 16:58

