Reg. č. projektu: CZ 1.04/ 4.1.00/A3.00004

Agendové informační systémy a Informační systémy veřejné správy

Příloha č. 1 k pracovnímu sešitu

Materiál vznikl v rámci řešení projektu **„Zajištění vzdělávání v oblasti registrů a v dalších kmenových projektech eGovernmentu“,** registrační číslo projektu: CZ 1.04/ 4.1.00/A3.00004, který je financován z prostředků Evropského sociálního fondu ČR, Operačního programu Lidské zdroje a zaměstnanost

Zpracovatel – Institut pro veřejnou správu Praha

Praha, červen 2014

5. Praktická část a příklady z praxe

Praktická část je rozdělena do tří okruhů. V prvním si prakticky vyjasníme souvislosti s tvorbou a udržováním informační koncepce jako prostředku pro dlouhodobé řízení informačních systémů. Ve druhé se podíváme na životní cyklus informačního systému. Ve třetí si pak prakticky vysvětlíme postup pro připojení agendového informačního systému k základním registrům.

Část 1: Dlouhodobé řízení informačních systémů (informační koncepce)

Pro dlouhodobé řízení informačních systémů a využití informačních technologií slouží úřadům "Informační koncepce". Tu má za povinnost zpracovat a pravidelně aktualizovat každý orgán veřejné správy, a to od roku 2009. Od roku 2010 pak má orgán za povinnost atestovat si dlouhodobé řízení informačních systémů (což zahrnuje především atestaci IK).

Strukturu, náležitosti a podrobnosti související s informační koncepcí a provozní dokumentací informačních systémů stanoví Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy

Platí tyto základní zásady:

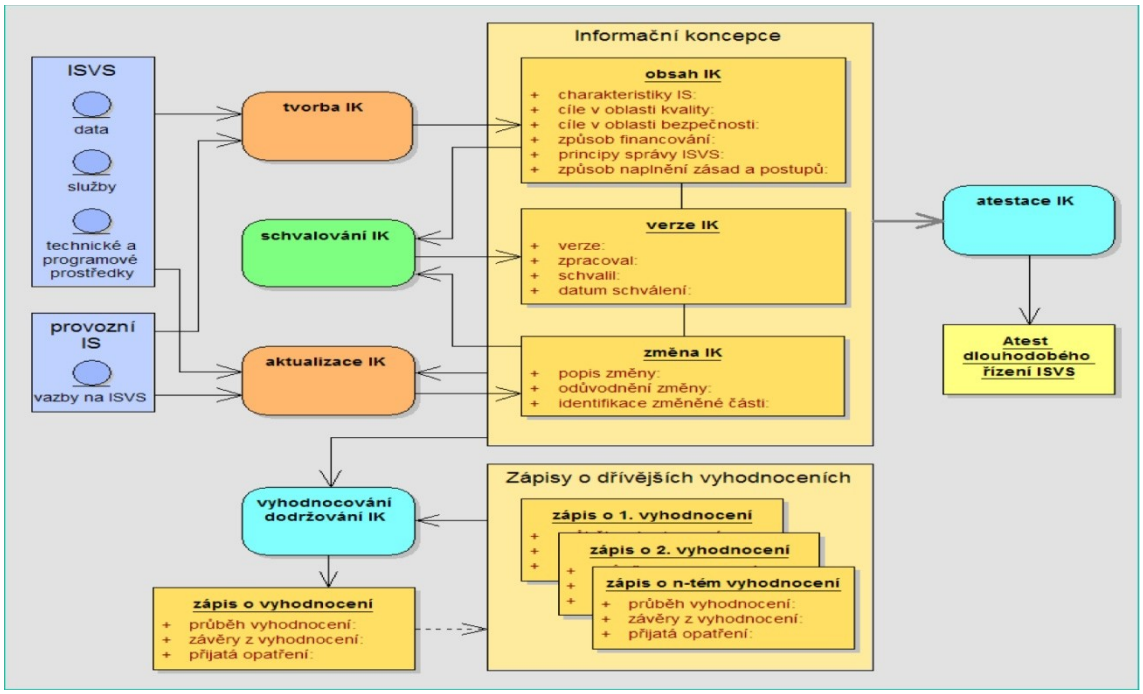
1. V informační koncepci musí orgán veřejné správy uvést, jaké má ISVS, resp. systémy, jejichž je správcem ve smyslu zákona o ISVS. Informace o jednotlivých informačních systémech (charakteristika, analýza současného stavu a předpokládané změny) může být velmi stručná, měla by obsahovat např. údaje o tom, k čemu informační systém slouží, jaké má uživatele, zda poskytuje služby pro jiné informační systémy, kdo jej vytvořil a podle jakého právního předpisu ho orgán veřejné správy měl povinnost vytvořit či pořídit nebo má povinnost ho vést.
2. Součástí informační koncepce jako nástroje dlouhodobého řízení musí být nutně záměry orgánu veřejné správy na pořízení nebo vytvoření nových ISVS.
3. Součástí informační koncepce jsou cíle, požadavky a plán řízení bezpečnosti.
4. Aby mohl orgán veřejné správy realizovat své cíle a spravovat své informační systémy, musí mít popsán způsob, jak bude tyto aktivity financovat. Je možné rovněž stanovit například pravidla a povinnosti při zadávání veřejných zakázek a zakázek malého rozsahu na ISVS, požadavky na akceptační protokoly, na testování informačních systémů před jejich akceptací, požadavky na technickou podporu a aktualizace software, případné požadavky na certifikaci jakosti informačních systémů, případně certifikaci řízení jakosti u dodavatele. Je také možné stanovit a uvést role, jejichž aktéři jsou odpovědní za jednotlivé činnosti v procesu získávání finančních prostředků na realizaci dané aktivity. Z hlediska financování je dále vhodné na základě plánovaných změn v informačních systémech vytvořit plán zdrojů financování takových změn, včetně časového harmonogramu.
5. Aby mohla být informační koncepce úspěšně nasazena do skutečného používání, je nutné stanovit pravidla pro vyhodnocování jejího dodržování a při provádění jejích změn.
6. Orgán veřejné správy stanoví, kdo (v jaké pracovní či jiné pozici) řídí realizaci činností vedoucích k naplňování informační koncepce a k naplňování dalších povinností stanovených zákonem.
7. Před zahájením vytváření informační koncepce je nutné stanovit, po jakou dobu ji orgán veřejné moci bude chtít používat. Doba může být odvozena nejen od doby platnosti atestu (5 let), ale například i od plánů změn v rozsáhlejších informačních systémech, které si vynutí větší zásahy do informační koncepce. Na druhou stranu je možné si vymezit i dlouhodobější trvání informační koncepce, pokud je to z hlediska záměrů orgánů veřejné správy vhodné. Informační koncepce je z hlediska obecnosti na vyšší úrovni a nemusí být měněna zároveň s technologickým vývojem – ke změnám bude docházet především v provozní dokumentaci, která na tento vývoj reagovat musí. Je možné provádět změny i v informační koncepci, aniž by bylo nutné ji měnit zcela (a opětovně atestovat). Záleží tedy na autorovi, do jaké hloubky hodlá popsat v informační koncepci své cíle a v závislosti na tom stanoví dobu, po kterou tato koncepce bude platná.

Životní cyklus informační koncepce

V životním cyklu informační koncepce se uplatňují tyto základní procesy:

- Tvorba IK zahrnuje počáteční naplnění obsahu informační koncepce v souladu s vyhláškou č. 529/2006 Sb. § 2. Informační koncepci vydává OVS s definovanou platností, která by měla respektovat stav IT v orgánu veřejné správy a jeho předpokládané zásadní proměny. V běžném ustáleném stavu lze považovat za rozumnou dobu 5 let, která odpovídá zákonem o ISVS stanovené platnosti atestu. Tato doba také odpovídá běžně uvažované životnosti IS (resp. jeho verze mezi dvěma zásadními změnami). Během této doby se uplatňují další níže uvedené procesy až do vzniku nové informační koncepce.
- Schvalování IK probíhá v souladu s vyhláškou č. 529/2006 Sb. § 6. Schvalování se provádí obdobným způsobem pro prvotní verzi IK i pro každou změnu IK.
- Změna IK (též aktualizace IK) se provádí v závislosti na změnách skutečného stavu informačních systémů a v souladu s aktuálními požadavky orgánu VS
- Vyhodnocování dodržování IK vytváří zpětnou vazbu, která podporuje naplnění cílů definovaných v IK. Výsledkem jsou závěry z vyhodnocení a přijatá opatření, která se zaznamenávají do zápisu. Zápisy a především v nich uvedená přijatá opatření se stávají podkladem pro příští vyhodnocování dodržování IK. IK se vyhodnocuje nejméně jednou za 24 měsíců (vyhláška č. 529/2006 Sb. § 7).

Detailní znázornění procesů a životního cyklu informační koncepce je na obrázku.



Povinné náležitosti informační koncepce

Informační koncepce je ve své podstatě obsahově poměrně rozsáhlý dokument. Je vhodné tvořit informační koncepci z více dokumentů dle jednotlivých oblastí (viz příklady níže).

Následuje přehled bodů a témat, která má informační koncepce řešit:

Základní náležitosti v informační koncepci

- charakteristika každého informačního systému veřejné správy, jehož je správcem, stručnou charakteristiku jeho současného stavu a předpokládané změny v tomto systému,

- záměry na pořízení nebo vytvoření nových informačních systémů veřejné správy,
- vazby informačních systémů veřejné správy na povinně využívané informační systémy a principy eGovernmentu (třeba napojení na základní registry, vztah se spisovou službou apod.)
- dlouhodobé cíle v oblasti řízení kvality informačních systémů veřejné správy, požadavky na kvalitu a plán řízení kvality podle § 3,
- dlouhodobé cíle v oblasti řízení bezpečnosti informačních systémů veřejné správy, požadavky na bezpečnost a plán řízení bezpečnosti podle § 4,
- soubor základních pravidel (zásady) pro správu informačních systémů veřejné správy, a to včetně postupů, které vedou k jejich naplňování,
- způsob financování záměrů podle písmene b), dlouhodobých cílů podle písmen c) a d) a správy informačních systémů veřejné správy podle písmene e),
- postupy při vyhodnocování dodržování informační koncepce podle § 7 a při provádění jejích změn podle § 6,
- funkční zařazení zaměstnance nebo určení jiné fyzické osoby nebo název organizačního útvaru, který řídí provádění činností vedoucích k dosažení cílů, naplňování zásad a uplatňování postupů, které jsou v informační koncepci uvedeny, a ke splnění povinností, které orgánu veřejné správy stanoví zákon,
- dobu platnosti informační koncepce.

Zásady pro správu informačních systémů

V Informační koncepci se uvedou zásady pro správu informačních systémů pro tyto oblasti (které jsou zároveň i články životního cyklu):

- pořizování a vytváření informačních systémů veřejné správy,
- provozování informačních systémů veřejné správy, a to včetně jejich změn a rozvoje.
- doporučeno i popsat vazby na další informační systémy, včetně kmenových projektů eGovernmentu

Dlouhodobé cíle v oblasti řízení kvality

V informační koncepci se stanoví cíle v oblasti řízení kvality informačních systémů. Je třeba v cílech řešit tyto oblasti:

- zajištění kvality dat, která jsou v těchto systémech zpracovávána,
- zajištění kvality technických a programových prostředků podle § 2 písm. a) zákona,
- zajištění kvality služeb, které jsou prostřednictvím těchto systémů poskytovány.

Pro dosažení cílů je třeba v informační koncepci stanovit požadavky na kvalitu. Orgán veřejné správy v informační koncepci také stanoví plán řízení kvality, který obsahuje popis činností, které orgán veřejné správy vykonává pro dosažení stanovených požadavků na kvalitu informačních systémů veřejné správy, včetně časového harmonogramu jejich plnění.

Dlouhodobé cíle v oblasti řízení bezpečnosti

V oblasti bezpečnosti ICT a IS je třeba řešit v informační koncepci zejména tyto oblasti:

- bezpečnost dat, která jsou v těchto systémech zpracovávána,
- bezpečnost technických a programových prostředků podle § 2 písm. a) zákona,
- bezpečnost služeb, které jsou prostřednictvím těchto systémů poskytovány.

Pro dosažení cílů je nutné v informační koncepci stanovit požadavky na bezpečnost informačních systémů veřejné správy, ale zabývat se také fyzickou bezpečností, bezpečností přístupů a bezpečností infrastruktury. Orgán veřejné správy v informační koncepci stanoví plán řízení bezpečnosti, který obsahuje popis činností, které orgán veřejné

správy vykonává pro dosažení stanovených požadavků na bezpečnost informačních systémů veřejné správy, včetně časového harmonogramu jejich plnění.

Zásady a postupy pro pořizování a vytváření informačních systémů veřejné správy

V informační koncepci se uvede, jaké zásady a postupy uplatňuje úřad před pořízením nebo vytvořením informačních systémů veřejné správy podle § 2 odst. 3 písm. a), a to vždy zásady a postupy pro

- definování potřeby informačního systému veřejné správy, který má být pořízen nebo vytvořen, a analýzu zdrojů pro jeho pořízení nebo vytvoření, včetně očekávané finanční náročnosti,
- analýzu výchozího stavu,
- stanovení cílového stavu informačního systému veřejné správy,
- stanovení kvalitativních požadavků a požadavků na zajištění bezpečnosti,
- analýzu důsledků, které pořízení nebo vytvoření informačního systému veřejné správy může vyvolat.

Pokud se jedná o informační systémy dodané dodavatelem, stanoví se tyto zásady:

- jakou dokumentaci a jaká oprávnění nezbytná pro provádění údržby a změn v informačním systému veřejné správy je nutné v rámci dodávek vyžadovat, a to i s ohledem na to, zda správce informačního systému veřejné správy hodlá případné změny v tomto systému nebo odstraňování poruch provádět vlastními silami,
- jaké požadavky na projektové řízení uplatňuje u dodavatele,
- požadavky na testování informačního systému veřejné správy a akceptaci dodávky před jejím převzetím od dodavatele.

Pokud se jedná o informační systémy dodané dodavatelem, stanoví se zásady pro dokumentování procesu vytváření a správy těchto informačních systémů.

Zásady a postupy pro provozování informačních systémů veřejné správy

V informační koncepci se uvede, jaké zásady a postupy uplatňuje úřad při provozování informačních systémů veřejné správy podle § 2 odst. 3 písm. b), a to vždy zásady a postupy pro

- zajištění provozu a údržby informačních systémů veřejné správy, a to včetně vytváření a údržby provozní dokumentace a vyhodnocování jejího dodržování,
- řízení změn v informačních systémech veřejné správy,
- řízené ukončení činnosti informačních systémů veřejné správy.

Součástí zásad a postupů při řízení změn musí být:

- definování potřeby změn v informačním systému veřejné správy,
- analýza výchozího stavu pro rozvoj informačního systému veřejné správy,
- stanovení cílového stavu informačního systému veřejné správy,
- stanovení kvalitativních požadavků a požadavků na zajištění bezpečnosti vztahujících se k cílovému stavu informačního systému veřejné správy,
- návrh transformace z výchozího stavu do cílového stavu informačního systému veřejné správy,
- analýza důsledků, které změna může vyvolat,
- promítnutí změn do provozní dokumentace.

Tvorba informační koncepce a její aktualizace

Zpravidla se informační koncepce tvoří formou zakázky na dodávku informační koncepce (nebo jejích částí) a primární zodpovědnost je tedy na dodavateli. Úřad si ale pochopitelně může informační koncepci tvořit sám.

Ministerstvo vnitra ČR jako metodickou pomůcku vydalo vzorové informační koncepce pro jednotlivé typy orgánů veřejné správy, které jsou asi nejlepším vodítkem pro zpracování informační koncepce jako takové.

Zde je příklad minimalistické struktury informační koncepce (seznam hlavních kapitol):

1. Základní informace o informační koncepci
2. Informační systémy ve správě orgánu veřejné správy
3. Záměry na pořízení nebo vytvoření nových informačních systémů
4. Řízení kvality ISVS
5. Řízení bezpečnosti ISVS
6. Zásady a postupy pro správu ISVS
7. Způsob financování ISVS
8. Naplňování informační koncepce
9. Zodpovědnosti organizačních jednotek a útvarů v souvislosti s informační koncepcí a plněním zákonem stanovených úkolů

Oproti tomu může být informační koncepce rozsáhlým strategickým a koncepčním dokumentem, který lze rozdělit do několika samostatných dokumentů, jako například takto:

1. Hlavní dokument informační koncepce
2. Strategie řízení IKT
3. Strategie v oblasti koncových zařízení
4. Strategie v oblasti systémových služeb
5. Strategie v oblasti síťových a hlasových služeb
6. Strategie v oblasti datových center
7. Strategie v oblasti bezpečnosti IKT
8. Strategie v oblasti aplikačních služeb

Schvalování informační koncepce

Informační koncepce musí být schválena orgánem veřejné správy. Pro schvalování informační koncepce platí u úřadu stejné podmínky, jako pro schvalování ostatních strategických a koncepčních dokumentů.

Údaje o schválení informační koncepce nebo jejích jednotlivých verzí se v tomto dokumentu zaznamenávají ve struktuře

- označení verze informační koncepce,
- jméno, popřípadě jména a příjmení zaměstnance nebo jiné fyzické osoby nebo osob, které informační koncepci nebo její verzi zpracovaly,
- jméno, popřípadě jména a příjmení zaměstnance, jiné fyzické osoby nebo orgánu, který informační koncepci nebo její verzi schválil,
  d) datum schválení.

Změny a aktualizace informační koncepce

K aktualizaci informační koncepce lze ze strany úřadu přistoupit dvěma způsoby:

1. Změna informační koncepce
2. Tvorba zcela nové informační koncepce

V obou případech musí být naplněno ustanovení Vyhlášky č. 529/2006 Sb., § 6, tedy splnit požadavky na schválení a změnu informační koncepce.

Pro změnu informační koncepce platí tyto zásady:

1. Pokud orgán veřejné správy provede změnu v informační koncepci v souladu se zásadami a postupy stanovenými v § 2 odst. 1 písm. g) a znění této informační koncepce je schváleno, je vytvořena nová verze informační koncepce. Její změnu lze provést vytvořením nového dokumentu nebo připojením dodatku ke stávajícímu dokumentu.
2. Součástí každé verze informační koncepce, která vznikla provedením změn v předchozí verzi informační koncepce, je vždy popis a odůvodnění změny a identifikace příslušné části dokumentu, která byla změněna.
3. Orgán veřejné správy v průběhu doby, kterou informační koncepce časově pokrývá, provádí změny v informační koncepci tak, aby byl vždy zachován soulad obsahu koncepce se skutečným stavem a aktuálními požadavky orgánu veřejné správy.

Atestace dlouhodobého řízení IS a vazeb IS

Atestací se rozumí prověření shody s požadavky pro tyto dvě oblasti:

1. Atestace způsobilosti k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní, nebo
2. Atestace dlouhodobého řízení informačních systémů veřejné správy

Orgány veřejné správy si zajistí atestaci dlouhodobého řízení informačních systémů veřejné správy a prokáží splnění povinností atestem dlouhodobého řízení informačních systémů veřejné správy.

Dále jsou orgány veřejné správy jako správci ISVS povinny zajistit, aby vazby jimi spravovaného informačního systému na informační systémy jiného správce byly uskutečňovány prostřednictvím referenčního rozhraní s využitím datových prvků vyhlášených ministerstvem a vedených v informačním systému o datových prvcích. Způsobilost informačního systému k realizaci těchto vazeb jsou povinny prokázat atestem.

Atest může vydat pouze akreditované atestační středisko. Atestační středisko provádí atestace na základě smlouvy uzavřené s žadatelem o atestaci za úplatu. Cena se sjednává podle zvláštního právního předpisu. Atestace probíhá podle Podmínek atestačního střediska.

Rámcový postup atestace je následující:

1. Atestační středisko zveřejní podmínky atestace.
2. Orgán veřejné správy osloví atestační středisko s žádostí o uzavření smlouvy o provedení atestace.
3. Atestační středisko navrhne uzavření smlouvy a provedení atestace každému, kdo jej způsobem stanoveným v atestačních podmínkách vyzve k uzavření smlouvy podle zveřejněných atestačních podmínek.
4. Je uzavřena smlouva mezi atestačním střediskem a orgánem veřejné správy, a to s naplněním podmínek atestačního střediska.
5. Atestační středisko provede atestační zkoušku v souladu se Zákonem o ISVS a s jeho prováděcími právními předpisy.
6. Atestační středisko vydá žadateli o atestaci protokol o provedené zkoušce ve lhůtě 7 pracovních dnů ode dne ukončení této zkoušky.
7. Atestační středisko vydá o kladném výsledku atestace žadateli atest. Atest musí obsahovat podmínky platnosti atestu.
8. Atest se vydává na dobu nejvýše 5 let.
9. Atestační středisko, které vystavilo atest, může na základě žádosti držitele atestu před uplynutím platnosti atestu prodloužit jeho platnost o 2 roky, a to i opakovaně. Žadatel i atestační středisko při prodlužování platnosti atestu postupují obdobně jako při provádění atestací.
10. Atestační středisko předá v elektronické podobě prostřednictvím automatizovaného ohlašovacího procesu přístupného dálkovým přístupem na elektronické adrese, kterou ministerstvo uveřejní ve Věstníku,

ministerstvu informace o provedené atestaci ve lhůtě 7 pracovních dnů ode dne jejího provedení. Informaci o vydání atestu ministerstvo uveřejní ve Věstníku.

Kontrolu atestačních středisek při plnění povinností vyplývajících z tohoto zákona vykonává ministerstvo vnitra, na které se tedy orgány veřejné správy mohou v případě potřeby obrátit.

Přehled atestačních středisek je k dispozici na webových stránkách Ministerstva vnitra.

Návody a vzorové příklady

Obecně platí, že v naprosté většině případů zpracovává informační koncepci dodavatel v rámci dodavatelského díla. Pro oblast dlouhodobého řízení vydalo ministerstvo vnitra sérii metodických a návodných dokumentů:

Jak postupovat při plnění povinností vyplývajících ze zákona č. 365/2000 Sb.

Tento materiál je určen jako pomůcka ministerstvům, jiným správním úřadům a územním samosprávným celkům (dále jen "orgány veřejné správy") – správcům informačních systémů veřejné správy při plnění povinností vyplývajících ze zákona č. 365/2000 Sb. Povinnosti ministerstev, jiných správních úřadů a územních samosprávných celků – správců informačních systémů veřejné správy při plnění povinností vyplývajících ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, v oblasti informačních systémů veřejné správy.

Co je a co není ISVS

Metodický pokyn na konkrétních příkladech, jaký informační systém je podle zákona o ISVS informačním systémem veřejné správy, vysvětluje, jak přistupovat k popisu ISVS v informační koncepci. Zabývá se i vymezením toho, co za ISVS považováno není.

Metodický pokyn má sloužit pracovníkům orgánů veřejné správy i společností, které se zabývají vývojem informačních systémů pro orgány veřejné správy či dodávají služby v této oblasti, aby mohli snáze určit, zda je určitý informační systém informačním systémem veřejné správy ve smyslu zákona o ISVS.

Zákon o ISVS č. 365/2000 Sb. po novelizaci, k níž došlo počátkem roku 2006 (zákon č. 81/2006 Sb.), zakotvuje povinnost orgánů veřejné správy vytvořit a vydat informační koncepci. Tedy dokument, v němž budou uvedeny dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných ISVS, obecné principy pořizování, vytváření a provozování ISVS. Při vytváření informační koncepce jsou orgány veřejné správy postaveny před zásadní úkol identifikovat informační systémy veřejné správy, u kterých vykonávají úlohu správce ve smyslu zákona o ISVS. Tento metodický pokyn jim má v identifikaci ISVS pomoci.

Komentář k vyhlášce č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy

Komentář k vyhlášce vznikl jako pomůcka orgánům veřejné správy při vypracovávání informační koncepce a provozní dokumentace informačních systémů. Novelou zákona č. 365/2000 Sb., o informačních systémech veřejné správy, která byla provedena zákonem č. 81/2006 Sb., se zavádí institut dlouhodobého řízení informačních systémů veřejné správy. Dlouhodobé řízení ISVS se realizuje prostřednictvím informační koncepce orgánu veřejné správy a provozní dokumentace jím provozovaných ISVS. K provedení § 5a odst. 1 až 3 zákona byla vypracována vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy.

Metodický pokyn Řízení kvality informačních systémů veřejné správy

Metodický pokyn má sloužit jako základní návod k řízení kvality informačních systémů veřejné správy podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a vyhlášky č. 529/2006 Sb., o dlouhodobém řízení ISVS. Tyto předpisy stanoví povinnosti orgánů veřejné správy v oblasti dlouhodobého řízení ISVS, které zahrnují i řízení kvality ISVS.

Dlouhodobé cíle v oblasti kvality, požadavky na kvalitu a plán řízení kvality musí být součástí základního dokumentu dlouhodobého řízení ISVS, kterým je informační koncepce každého orgánu veřejné správy. Právní předpisy však blíže nespecifikují, jak konkrétně mají orgány veřejné správy k řízení kvality ISVS přistupovat, existuje pouze obecné doporučení využít mezinárodně uznávané normy a metody.

Záměrem pro vydání tohoto metodického pokynu bylo splnění následujících cílů:

1. zvýšit kvalitu informačních systémů veřejné správy;
2. podpořit zavedení procesů řízení kvality informačních systémů veřejné správy do procesů orgánů veřejné správy;
3. připravit správce informačních systémů veřejné správy na plnění některých povinností, které vyplývají z platné legislativy v oblasti dlouhodobého řízení informačních systémů veřejné správy.

Druhou částí metodického pokynu je praktický příklad řízení kvality ISVS – pro obec s pověřeným obecním úřadem a pro obec s výkonem přenesené působnosti v základním rozsahu.

Metodický pokyn k posuzování způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní

Metodický pokyn osvětluje problematiku atestací ISVS, které realizují vazby prostřednictvím referenčního rozhraní. Je určen atestačním střediskům, která provádějí atestace, a orgánům veřejné správy, které mají ze zákona povinnost zajistit atestaci způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní. Tuto skutečnost jsou orgány veřejné správy povinny prokázat atestem nejpozději do 1. ledna 2009. Tento metodický pokyn vychází ze zákona 365/2000 Sb., ve znění jeho novely č. 81/2006 Sb. a bezprostředně navazuje na vyhlášku č. 53/2007 Sb., o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní (vyhláška o referenčním rozhraní) a na vyhlášku č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní. Nová verze metodického pokynu vznikla na základě zkušeností s využitím předchozí verze.

Metodika tvorby XML schémat v oblasti informačních systémů veřejné správy

Tento metodický materiál se podrobněji věnuje implementaci XML schémat v prostředí informačních systémů veřejné správy. Je souhrnem pravidel a doporučení ("Best Practices") pro design schémat. Cílovou skupinou uživatelů tohoto dokumentu jsou především vývojáři XML řešení v rámci ISVS. Měli by zde nalézt odpovědi na otázky návrhu struktury, vytvoření vhodného designu a návrhu spolehlivého modelu údržby XML schémat ISVS včetně objasnění životního cyklu schémat. Předpokládá se, že čtenáři tohoto dokumentu mají znalosti XML technologií, a to zvláště XML Schema, přinejmenším na mírně pokročilé úrovni.

Metodický pokyn pro popis datových prvků

Metodický pokyn pro popis datových prvků v Informačním systému o datových prvcích (ISDP) vstoupil v platnost od 1.1.2007 v souvislosti se zahájením rutinního provozu této nové webové aplikace. Metodický pokyn formalizuje a realizuje doporučení stanovená prováděcím právním předpisem k formě a technickým náležitostem předávání údajů do ISDP a o postupech Ministerstva informatiky a jiných orgánů veřejné správy při vedení, zápisu a vyhlašování

datových prvků v ISDP (vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích. Dodržování tohoto metodického pokynu je na základě uvedené vyhlášky pro orgány veřejné správy závazné.

Vzorové informační koncepce orgánů veřejné správy

Ministerstvo vnitra vydalo jako metodickou pomůcku sadu vzorových informačních koncepcí, které mohou sloužit jako obsahové a věcné návody k tvorbě a aktualizaci informačních koncepcí. K dispozici jsou tyto materiály:

- Vzorová úplná struktura informační koncepce
- Vzorová informační koncepce pro ústřední správní úřad
- Vzorová informační koncepce pro obec s rozšířenou působností
- Vzorová informační koncepce pro obec s pověřeným obecním úřadem
- Vzorová informační koncepce pro obec základního typu

Procesní model dlouhodobého řízení informačních systémů

Ministerstvo vnitra vydalo jako metodickou pomůcku popis procesů v oblasti dlouhodobého řízení informačních systémů veřejné správy.

Část 2: Životní cyklus informačních systémů v úřadu

Každý informační systém v úřadu s sebou nese určité povinnosti dané buď legislativou, nebo samotnou logikou věci. Při správě jakýchkoliv IS (ať už informačních systémů veřejné správy jako agendových informačních systémů, či provozních informačních systémů) platí pro úřad tyto základní aspekty:

1. Má platnou informační koncepci, v níž má popsány všechny svoje IS se všemi podrobnými aspekty
2. Má jasně danou strukturu zodpovědnosti za fungování IT a související procesy, včetně stanovení zodpovědných organizačních jednotek a pracovníků
3. Zná povinnosti využívat informační systémy (třeba centrální AIS) a ví jak je naplňovat
4. Má popsány zásady pro životní cyklus informačního systému, a to včetně podmínek financování a souvislosti s využíváním jiných IS
5. Ví, jak IS vznikl, kdo jej vytvořil či dodal, na základě čeho je tvořen a provozován, kdo je správcem a provozovatelem, jaké procesy souvisí v jeho úřadu s daným IS apod.

Procesy životního cyklu ISVS

Všechny procesy lze rozdělit do tří základních sekcí:

- Pořizování a vytváření ISVS
  zahrnuje postupy uplatňované při pořizování ISVS od dodavatele nebo při vytváření ISVS prostřednictvím svých zaměstnanců (vyhláška č. 529/2006 Sb. § 8). Proces přímo ovlivňují pravidla pro tvorbu ISVS, která stanoví řadu omezení a povinností v této oblasti. Správci ISVS vznikají povinnosti předávat některé údaje o vytvořených ISVS Ministerstvu vnitra do ISoISVS a vznikají další povinnosti, pokud se ISVS jako agendový informační systém připojuje k základním registrům.
- Správa a provozování ISVS
  zahrnuje postupy uplatňované při zajišťování provozu a údržby IS, řízení změn v IS a řízeném ukončení jeho činnosti (vyhláška č. 529/2006 Sb. § 9).
- Financování pořizování, vytváření, rozvoje a provozu ISVS
  zahrnuje všechny činnosti související se zajištěním potřebných finančních prostředků pro realizaci dlouhodobého řízení ISVS a fungování samotných informačních systémů.

Pořizování informačních systémů

Informační systémy lze pořizovat výhradně na základě stanovených zásad pro pořizování ISVS a příslušné dokumentace. Zásady stanoví úřad ve své informační koncepci. (vyhláška 529/2006 Sb., § 8)

Pořídit ISVS lze dvěma způsoby:

1. Dodavatelsky (ISVS dodá dodavatel)
2. Vlastní tvorbou (ISVS vytvoří zaměstnanci úřadu)

Před pořízením ISVS musí být zpracován dokumentační podklad pro jeho pořízení, který obsahuje minimálně:

- definování potřeby informačního systému veřejné správy, který má být pořízen nebo vytvořen,
- analýzu zdrojů pro jeho pořízení nebo vytvoření, včetně očekávané finanční náročnosti,
- analýzu výchozího stavu,
- stanovení cílového stavu informačního systému veřejné správy,
- stanovení kvalitativních požadavků,
- stanovení požadavků na zajištění bezpečnosti,
- analýzu důsledků, které pořízení nebo vytvoření informačního systému veřejné správy může vyvolat.

Pokud je ISVS dodáván dodavatelem, je třeba jak v informační koncepci, tak při pořízení konkrétního ISVS řešit i tyto aspekty:

- jakou dokumentaci a jaká oprávnění nezbytná pro provádění údržby a změn v informačním systému veřejné správy je nutné v rámci dodávek vyžadovat, a to i s ohledem na to, zda správce informačního systému veřejné správy hodlá případné změny v tomto systému nebo odstraňování poruch provádět vlastními silami,
- jaké požadavky na projektové řízení uplatňuje u dodavatele,
- požadavky na testování informačního systému veřejné správy a akceptaci dodávky před jejím převzetím od dodavatele,
- Vztah k datům v informačním systému vedeným,

Správa a provozování informačních systémů

V informační koncepci se stanoví a v praxi se uplatňují zejména tyto procesy:

- zajištění provozu a údržby informačních systémů veřejné správy, a to včetně vytváření a údržby provozní dokumentace a vyhodnocování jejího dodržování,
- řízení změn v informačních systémech veřejné správy,
- řízené ukončení činnosti informačních systémů veřejné správy.

Součástí postupů v souvislosti s řízením změn v jakémkoliv ISVS je vždy

- definování potřeby změn v informačním systému veřejné správy,
- analýza výchozího stavu pro rozvoj informačního systému veřejné správy,
- stanovení cílového stavu informačního systému veřejné správy,
- stanovení kvalitativních požadavků a požadavků na zajištění bezpečnosti vztahujících se k cílovému stavu informačního systému veřejné správy,
- návrh transformace z výchozího stavu do cílového stavu informačního systému veřejné správy,
- analýza důsledků, které změna může vyvolat,
- promítnutí změn do provozní dokumentace.

Při samotné správě informačního systému jsou klíčové dvě role:

1. Správce ISVS:
   Je zodpovědný za celý ISVS včetně provozní dokumentace a určuje pravidla jeho fungování a vazeb
2. Provozovatel ISVS:
   na základě smlouvy či zákona provozuje ISVS dle stanovených pravidel správce a spolu se správcem aktualizuje provozní dokumentaci

Pro každý ISVS musí být jasně vymezeny role fyzických osob:

1. správce systému, kterým je zaměstnanec nebo jiná fyzická osoba, která zajišťuje řízení provozu informačního systému veřejné správy,
2. bezpečnostního správce systému, kterým je zaměstnanec nebo jiná fyzická osoba, která zajišťuje kontrolu bezpečnosti informačního systému veřejné správy;

Tyto role jsou jednoznačně stanoveny i v provozní dokumenty ke každému ISVS.

Orgány veřejné správy jsou v souvislosti se správou a provozem a využíváním ISVS povinny (dle Zákona 365/2000 Sb., § 2):

- předložit ministerstvu vnitra k vyjádření návrhy dokumentací programů obsahující pořízení, obnovu a provozování informačních a komunikačních technologií vypracovaných podle zvláštního právního předpisu a investiční záměry akcí pořízení, obnovy a provozování informačních a komunikačních technologií, jejichž registrace v Informačním systému financování reprodukce majetku, zadání jejich realizace a změna jejich závazně stanovených parametrů se provádí pouze se souhlasem Ministerstva financí podle zvláštního právního předpisu. Náležitosti dokumentací programů a investičních záměrů stanoví zvláštní právní předpis
- zpřístupňovat ministerstvu v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem, bez zbytečného odkladu informace o jimi spravovaném informačním systému a jím poskytovaných službách a používaných datových prvcích, a to za účelem uveřejnění v informačním systému podle § 4 odst. 1 písm. h) a i), pokud zvláštní zákon nestanoví jinak; zpřístupňovanými datovými prvky jsou rovněž provozní údaje, pokud jsou využity pro realizaci vazby podle písmene d)
- uveřejňovat číselníky, pokud jsou správci těchto číselníků a není zákonem stanoveno jinak, a to i způsobem umožňujícím dálkový přístup a předávat ministerstvu údaje do informačního systému o datových prvcích v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem
- zajistit, aby vazby jimi spravovaného informačního systému na informační systémy jiného správce byly uskutečňovány prostřednictvím referenčního rozhraní s využitím datových prvků vyhlášených ministerstvem a vedených v informačním systému o datových prvcích. Způsobilost informačního systému k realizaci těchto vazeb jsou povinny prokázat atestem. Toto ustanovení se nevztahuje na vazby mezi jimi spravovanými informačními systémy a informačními systémy vedenými zpravodajskými službami

To znamená v běžné správě zejména povinnosti:

1. Předávat do informačního systému o informačních systémech veřejné správy (ISoISVS) informace o jejich informačních systémech veřejné správy (podrobnosti stanoví Vyhláška č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy)
2. Zapisovat a využívat datové prvky a jejich číselníky pro zejména zajištění v informačních systémech veřejné správy (podrobnosti stanoví Vyhláška č. 469/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému o datových prvcích a o postupech Ministerstva informatiky a jiných orgánů veřejné správy při vedení, zápisu a vyhlašování datových prvků v informačním systému o datových prvcích)
3. Vést a spravovat provozní dokumentaci informačních systémů veřejné správy (podrobnosti stanoví Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy)

Pokud daný ISVS poskytuje dalším ISVS služby, správci informačních systémů veřejné správy poskytují služby informačních systémů veřejné správy prostřednictvím centrálního místa služeb.

Provozní dokumentace k ISVS

Provozní dokumentace ISVS je základní dokumentací systému. Požadavky na provozní dokumentaci stanovuje zejména Vyhláška 529/2006 Sb., a to § 10 a § 11. Další požadavky na provozní dokumentaci, její tvorbu, udržování, změny a využití stanoví úřad ve své informační koncepci.

Provozní dokumentaci informačního systému veřejné správy tvoří tyto dokumenty:

1. bezpečnostní dokumentace informačního systému veřejné správy,
2. systémová příručka,
3. uživatelská příručka.

V provozní dokumentaci orgán veřejné správy uvádí aktuální stav informačního systému veřejné správy popisem funkčních a technických vlastností každého informačního systému veřejné správy, jehož je správcem, a to včetně organizačně technických opatření, která zajišťují zachování těchto vlastností. Provozní dokumentace k informačnímu systému veřejné správy musí být zpracována tak, aby odpovídala zásadám a postupům stanoveným v informační koncepci.

Bezpečnostní dokumentace ISVS

Bezpečnostní dokumentaci informačního systému veřejné správy tvoří:

- bezpečnostní politika informačního systému veřejné správy, a to vždy pokud systém má vazby s informačním systémem veřejné správy jiného správce nebo pokud orgán veřejné správy není provozovatelem tohoto systému,
- bezpečnostní směrnice pro činnost bezpečnostního správce systému.

Bezpečnostní politika informačního systému veřejné správy obsahuje popis bezpečnostních opatření, která orgán veřejné správy uplatňuje při zajišťování bezpečnosti tohoto systému a která odpovídají požadavkům na bezpečnost stanoveným v informační koncepci.

Bezpečnostní směrnice pro činnost bezpečnostního správce systému obsahuje podrobný popis bezpečnostních funkcí, které bezpečnostní správce systému používá pro provádění určených činností v informačním systému veřejné správy, a návod na použití těchto funkcí.

Bezpečnostní atestace

Orgán veřejné správy předkládá při atestaci bezpečnostní politiku informačního systému veřejné správy, pokud je povinen ji zpracovat podle Vyhlášky 529/2006 Sb., § 10, odst. 2, písm. a). To znamená, že každá bezpečnostní politika ISVS musí být řádně atestována.

Systémová příručka ISVS

Systémová příručka ISVS je primárně určena správci ISVS a provozovateli ISVS.

Systémová příručka informačního systému veřejné správy vždy obsahuje:

- popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v informačním systému veřejné správy, a návod na použití těchto funkcí,

- parametry kvality, které vycházejí z požadavků na kvalitu podle § 3 odst. 2,
- podrobný popis informačního systému veřejné správy nebo odkaz na dokument, ve kterém je popis uveden a který je správci systému dostupný,
- popis jednotlivých činností vykonávaných při správě informačního systému veřejné správy, včetně činností definovaných pro role podle § 12, určení fyzických osob, které tyto činnosti vykonávají, a oprávnění nezbytných pro výkon těchto činností,
- definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání informačního systému veřejné správy.

Uživatelská příručka ISVS

Uživatelská příručka ISVS je primárně určena pro jeho uživatele, ať už jsou jimi konkrétní fyzické osoby, anonymní uživatelé, či orgány veřejné správy, které daný ISVS používají.

Uživatelská příručka informačního systému veřejné správy vždy obsahuje:

- popis funkcí, včetně bezpečnostních, které používá uživatel pro svou činnost v informačním systému veřejné správy, a návod na použití těchto funkcí,
- vymezení oprávnění a povinností uživatelů ve vztahu k informačnímu systému veřejné správy.

Provozní dokumentaci informačního systému veřejné správy tvoří či mohou tvořit také i jiné dokumenty, pokud je jejich zpracování a využívání nezbytné pro efektivní správu informačního systému veřejné správy; to platí vždy pro informační systémy veřejné správy, které zpracovávají velké objemy dat nebo které jsou vytvářeny a provozovány, včetně provádění změn v těchto systémech, v souladu s českými technickými normami, které zpracování jiných dokumentů předpokládají.

Část 3: Agendové informační systémy a jejich napojení na základní registry

Orgán veřejné moci přistupuje k údajům v základních registrech také prostřednictvím svých agendových informačních systémů, které spravuje. Jeden AIS může přitom využívat více OVM, ovšem každý AIS musí mít svého konkrétního jediného správce.

Agendový informační systém využívá sadu webových služeb Informačního systému základních registrů, přičemž veškeré aspekty týkající se připojení a využívání ISZR a webových služeb (včetně podpory pro OVM) řeší Správa základních registrů.

Orgány veřejné moci přistupují k základním registrům ve dvou hlavních rolích:

Role	Popis	Využití AIS
EDITOR	OVM v dané agendě je editorem údajů v registrech	centrální editační AIS
ČTENÁŘ	OVM v dané agendě využívá údaje z registrů	Centrální či lokální AIS

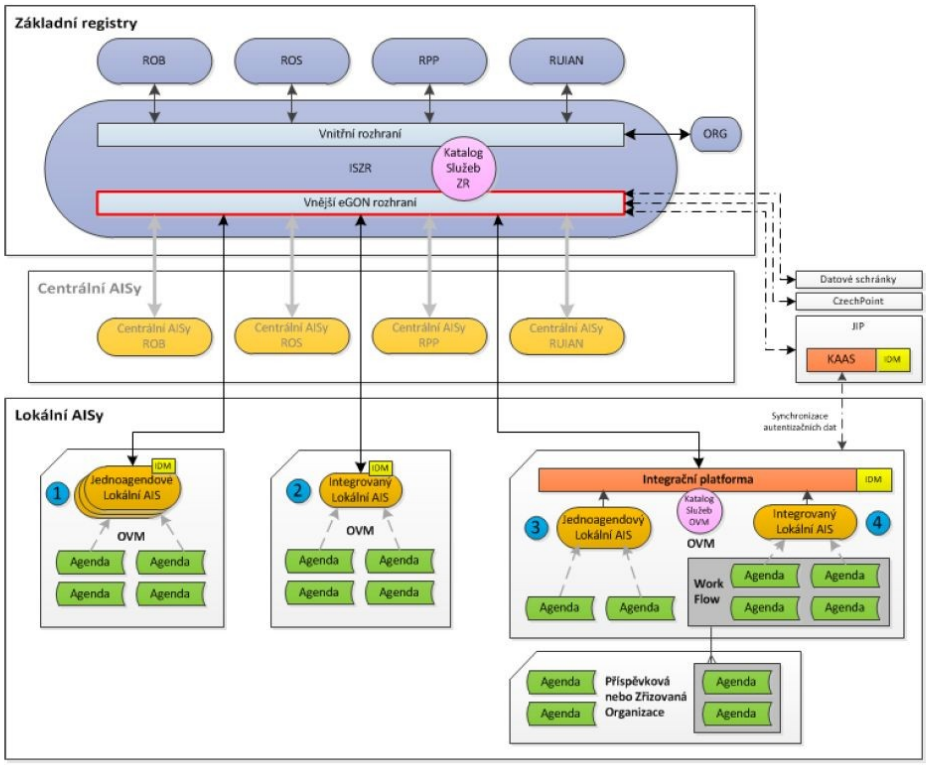
Každý AIS, který je připojen k základním registrům, je jednoznačně identifikován následujícími údaji:

- IČ úřadu – IČ správce AIS,
- AIS_ID – identifikátor AIS z informačního systému o informačních systémech veřejné správy (IS o ISVS),
- SN – číslo certifikátu (SerialNumber),
- Seznam agend – seznam agend v AIS obsažených

Využívání základních registrů prostřednictvím AIS

eGON služby jsou publikovány na vnějším eGON rozhraní ISZR (na schématu níže – červeně označené rozhraní). Po předchozím Ohlášení OVM k výkonu Agendy, mohou pracovníci zařazení do Agend OVM tyto služby používat na základě oprávnění, prostřednictvím centrálních AISů, či svých vlastních AISů.

Na obrázku je zobrazeno celé komunikační schéma pro využívání služeb ISZR ze strany agendových informačních systémů.



Základní podmínky připojení do ostrého prostředí ISZR:

V případě, že chce OVM pro komunikaci se základními registry využít vlastní agendový informační systém, je základní podmínkou provedení registrace každého takového AIS orgánem veřejné moci do Informačního systému o informačních systémech veřejné správy (ISoISVS). Pouze registrovaný AIS v ISoISVS je možné následně (po získání certifikátu pro komunikaci s ISZR a provedení příslušných úprav) připojit k rozhraní ISZR.

Obecně platí, že je třeba splnit tyto kroky:

1. AIS musí být zaregistrován v informačním systému o informačních systémech veřejné správy (IS o ISVS).
2. Úřad musí mít oznámenou působnost ve všech (zaregistrovaných) agendách, které AIS obsahuje.
3. Úřad se musí seznámit s dokumentem “Certifikační politika SZR” a zavázat certifikační politiku SZR dodržovat.
4. AIS musí splňovat podmínky dokumentu “Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí Základních registrů” (pozn. součástí požadavků je úspěšné otestování AIS v testovacím prostředí).
5. Úřad musí přijmout svou odpovědnost za jednoznačnou autentizaci a autorizaci všech osob, které budou při výkonu působnosti v zaregistrované agendě prostřednictvím AIS přistupovat ke službám vnějšího rozhraní informačního systému základních registrů, a že tyto osoby budou k dané činnosti oprávněny.

Žádost o certifikát a připojení AIS k ISZR

Před podáním žádosti o certifikát si úřad připraví

1. Identifikátor AIS_ID (identifikátor podle IS o OSVS.)
2. Seznam agend obsažených AIS.
3. Pevnou veřejnou IP adresu, ze které bude AIS přistupovat; je-li úřad subjektem KIVS uvede adresu přidělenou v rámci KIVS.
4. Asymetrický klíčový pár (úřad přitom postupuje podle návodu uveřejněného na www.szrcr.cz v sekci Správci a vývojáři).

Úřad podá žádost o certifikát:

1. Úřad vyplní formulář, který je dostupný na webu SZR. Jedná se o stávající formulář pro registraci AIS do JIP rozšířený o funkcionalitu potřebnou pro registraci AIS do základních registrů; při vyplňování formuláře úřad využije připravené údaje a připojí k němu veřejnou část asymetrického klíčového páru.
2. V žádosti úřad uvede kontaktní údaje na osobu pro IT záležitosti a komunikační heslo. Tyto údaje slouží pro případnou telefonickou nebo e-mailovou komunikaci mezi SZR a úřadem.
3. Úřad odešle vyplněný formulář do datové schránky SZR.

Pro odeslání úřad vybere jednu ze dvou možností – Buď "Automaticky odeslat do datové schránky" nebo "Uložit pro odeslání spisovou službou"

Vygenerování certifikátu (týká se SZR)

Správa základních registrů zajistí: zajistí:

- vygenerování certifikátu,
- zřízení služby připojení (prostup z IP adresy úřadu k vnějšímu rozhraní ISZR),
- zavedení certifikátu do systému ISZR a ORG,
- odeslání certifikátů do DS úřadu.

Instalace certifikátu

Proces zpřístupnění AIS k základním registrům úřad dokončí instalací certifikátu na svém serveru. Při instalaci certifikátu postupuje podle návodu "Postup pro generování asymetrického klíčového páru", který je uveřejněn na internetových stránkách Správy základních registrů www.szrcr.cz v sekci pro vývojáře.

Certifikát v testovacím prostředí je vydáván s dobou platnosti 12 měsíců.

Certifikát v produkčním prostředí je vydáván s dobou platnosti 36 měsíců.

Autentizace a logování v rámci AIS

V rámci naplnění požadavku na zajištění evidence přístupů k údajům v základních registrech musí OVM přiřadit konkrétní zaměstnance k jednotlivým agendám a jejich činnostním rolím. OVM tedy musí dále zajistit i autentizaci uživatelů, přiřazení k rolím v agendách a následně musí zajistit i logování tak, aby bylo možno na žádost subjektu či kontrolního orgánu dohledat konkrétního úředníka a konkrétní důvod využívání údajů ze základních registrů u každé transakce mezi AIS a ISZR.

Právní rámec nespecifikuje jak konkrétně autentifikaci uživatelů AIS jako úředníků v dané agendě a jejich autorizaci zajistit, ale vesměs lze využít dva koncepty:

1. Využití služeb JIP/KAAS – Tato možnost řešení využívá služeb katalogu autentizačních a autorizačních služeb pro správu identit potřebných pro práci s lokálním AIS. Implementace této možnosti řešení spočívá buď v úpravě lokálního AIS, který bude komunikovat prostřednictvím webových služeb s JIP/KAAS za účelem autentizace uživatele, nebo v synchronizaci vybraných identit s lokálními adresářovými službami.
2. Zajištění životního cyklu identity vlastními prostředky – Lokální AIS řeší správu identit buď ve svém vlastním – nativním prostředí (v rámci daného informačního systému), nebo prostřednictvím lokálních adresářových služeb (LDAP), které nejsou synchronizovány s JIP.

Opět ale platí, že tyto technické podrobnosti musí v první řadě řešit dodavatel AIS.

Návody a vzorové příklady

Na webových stránkách Správy základních registrů doporučujeme pročíst sekce Připojení prostřednictvím vlastního AIS a Pro správce a vývojáře AIS, v nichž naleznete mnoho zajímavého.

Doporučujeme podrobně prostudovat metodické materiály Správy základních registrů.

Podmínky pro připojení agendových informačních systémů k ISZR

Dokument stanovuje jednoduchou a srozumitelnou formou podmínky pro připojení agendových informačních systémů orgánů veřejné moci k rozhraní ISZR, aby mohly využívat údaje ze základních registrů. Pro správce AIS je tento dokument naprostým minimem znalostí.

Referenční agent

Pro ty, kdo chtějí programovat vlastní agendové informační systémy a chtějí vědět, jak vypadá komunikace s ISZR a využívání webových služeb, je určen takzvaný referenční agent.

Jedná se o předpřipravený soubor programového kódu pro komunikaci s ISZR a využívání jeho služeb. Referenční agent obsahuje i popsané zdrojové kódy, které lze bez licenčního mezení volně využít. Agent je dostupný pro platformy .NET (Microsoft .NET platform) a Java.