Slezská univerzita v Opavě
Obchodně podnikatelská fakulta v Karviné

INFORMAČNÍ SYSTÉMY VE VEŘEJNÉ SPRÁVĚ

Pro prezenční formu studia

Jindřich Vaněk, Roman Šperka

Karviná 2014

Projekt OP VK č. CZ.1.07/2.2.00/28.0017
„Inovace studijních programů na Slezské univerzitě,
Obchodně podnikatelské fakultě v Karviné“

Obor: Informatika.

Anotace: Učební text „Informační systémy ve veřejné správě“ je určen pro posluchače Obchodně podnikatelské fakulty v Karviné, Slezské univerzity v Opavě. Obsahová náplň předloženého textu začíná objasněním základních pojmů z teorie informací, informačních systémů (IS) a informačních systémů ve veřejné správě (ISVS). Na této teorii je založeno přehledné představení jednotlivých aspektů využití informačních technologií s cílem objasnit jejich využití jako nástroje pro podporu procesů, probíhajících ve veřejné správě. Jejich přínosem by mělo být ulehčení výkonu veřejné správy a zlepšení vztahu mezi občanem a veřejnou správou. Učební text poskytuje taky informace o základních předpisech a dokumentech, ze kterých ISVS vycházejí. Zejména se jedná o zákony o informačních systémech ve veřejné správě, o elektronických úkonech, o ochraně osobních údajů a jiné. Čitatel bude také obeznámen o základních registrech, agendách a o informační koncepci. Rozsáhlá část textu je věnována bezpečnosti ISVS a identifikaci. Závěrem se text zmiňuje o aktuální situaci v oblasti eGovernmentu, portálu veřejné správy a informuje o situaci ISVS v Evropské unii a ve Slovenské republice. Celý text je proložen množstvím praktických příkladů.

Klíčová slova: Informační systém, IS, informační systém veřejné správy, veřejná správa, státní správa, eGovernment., datová schránka, registr, agenda, informační koncepce, dokumentace, bezpečnost, identifikace

Autor: **RNDr. Jindřich Vaněk, Ph.D.**
RNDr. Ing. Roman Šperka, Ph.D.

Recenzenti: Doc. Mgr. Petr Suchánek, Ph.D.
Doc. Ing. Eva Wagnerová, CSc.

ISBN Doplní oddělení vědy a výzkumu.

OBSAH

ÚVOD

Učební text „Informační systémy ve veřejné správě“ je určen pro posluchače Obchodně podnikatelské fakulty v Karviné, Slezské univerzity v Opavě. Je zaměřen mezioborově, neboť se v něm hovoří o technických, programových, manažerských, legislativních, právních a bezpečnostních aspektech informačních technologií (IT), které se navzájem ovlivňují.

Po prostudování učebního textu by měl čtenář získat přehled o informačních systémech veřejné správy (ISVS) a o elektronizaci v této oblasti nejenom v České republice, ale i v Evropské unii. Cílem textu je seznámení s možnostmi, které ISVS nabízejí občanům, podnikatelským subjektům i zaměstnancům veřejné správy.

Publikace začíná objasněním základních pojmů z teorie informačních systémů (IS) a ISVS, na které je postaveno chápaní jakéhokoliv IS a která je nezbytným předpokladem povědomí o funkci IT. Informační technologie by měly sloužit jako nástroj pro podporu procesů, probíhajících ve veřejné správě a měly by ulehčit její vykonávání. Jádrem textu jsou informace o základních předpisech a dokumentech, ze kterých ISVS vycházejí a které musí naplňovat. Zejména jde o zákony o informačních systémech ve veřejné správě, o elektronických úkonech, o ochraně osobních údajů a jiné.

Rozsáhlý prostor je věnován základním registrům, agendám a informační koncepci, který je proložen množstvím praktických příkladů. Čtenář bude mít možnost se seznámit také se zásadami bezpečnosti ISVS a problematikou identifikace, autentizace a autorizace. Další kapitoly jsou věnovány aktuální situaci v oblasti eGovernmentu a portálu veřejné správy.

Poslední dvě kapitoly mapují situaci na poli ISVS v Evropské unii a ve Slovenské republice, kde došlo od 1.1.2014 ke zpuštění provozu elektronických občanských průkazů a portálu, kde jsou nabízeny mnohé služby právě v souvislosti s elektronizací.

Učební text je provázán s aktuálními, především internetovými prameny a poskytuje skutečně současný náhled do problematiky informačních systémů ve veřejné správě.

1 INFORMAČNÍ SYSTÉMY

NEPŘEHLÉDNĚTE

Informační systém (IS) budeme chápat jako komplex lidí, informací, systému řízení chodu IS, který zabezpečuje těsné a logické propojení na prostředí, systému organizace práce spojeného s provozem a využitím IS, technických prostředků a metod zabezpečujících sběr, přenos, aktualizaci, uchování a další zpracování dat pro tvorbu a prezentaci informací pro potřeby uživatelů a použité informační technologie.

Ke **komponentám IS** patří:

- hardwarového vybavení včetně síťových a komunikačních prostředků (hardware),
- operační a databázové systémy (základní software),
- datové zdroje (dataware),
- lidé, aktivní součást IS (peopleware),
- zakomponování IS do podnikového systému řízení a jeho konzistence s podnikovými procesy (orgware).

Obrázek 1-1 Komponenty informačního systému

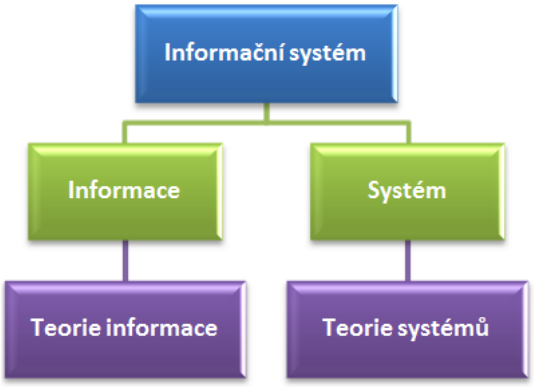
Informační systém musí zabezpečovat tzv. **informační činnosti.** Pod tímto termínem je skryto získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na hmotných nosičích. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů prostřednictvím technických a programových prostředků.

Informační systém je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností.

Správcem informačního systému je subjekt, který určuje účel a prostředky zpracování informací a za informační systém odpovídá.

Provozovatelem informačního systému je subjekt, který provádí alespoň některé informační činnosti související s informačním systémem. Provozováním informačního systému veřejné správy může správce pověřit jiné subjekty.

Obrázek 1-2 Pojem informační systém



1.1 ZÁKLADNÍ POJMY

Data jsou jen potenciální informace, které na informace zhodnocuje až informační proces (subjekt řízení), takže bezchybně i včas doručená zpráva nemusí mít pro řídícího pracovníka informační charakter. Data představují odraz jevů, procesů a vlastností, které existují a probíhají v části reálného světa, kterou odrážejí. Jsou vyjádřením skutečnosti a myšlenek v předepsané podobě tak, aby je bylo možné přenášet a zpracovávat.

Datový prvek je jednotka dat, která je v daném kontextu dále považována za nedělitelnou a je jednoznačně definována.

Datový soubor je množina datových vět, má shodný význam s pojmem **datový objekt.**

Datovou základnu představuje množina datových souborů. Jedním ze souborů by měl být **katalog dat**, tj. soubor, který nese informace o struktuře ostatních datových souborů. Jde o základnu, zásobu údajů, které slouží jako informační podpora určitého procesu (obvykle se jedná o proces rozhodovací). Může se jednat o např. o databáze faktografické, textové, grafické apod.

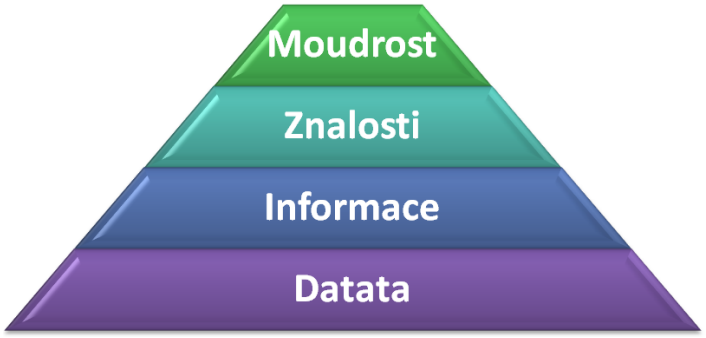
Databáze tvoří data, které slouží více aplikacím, jsou v nich minimalizovány redundance a existuje vhodně centralizovaná správa těchto dat. Cílem **databázového systému** je uspořádat datové zdroje (datovou základnu) na počítači tak, aby tyto zdroje mohly být využívány více uživateli a mohly být využity na různých počítačích zapojených do sítě.

Základní komponentou databázové koncepce je programový systém umožňující práci s databází - **systém řízení bází dat** (**SŘBD**) angl. Data Base Management Systém (DBMS). Je to soustava programů, která umožňuje organizování dat, efektivní správu dat, centrální popis dat a umožňuje přístup k datům z různých aplikací.

Datový sklad (DataWarehouse) je informační technologie založená převážně na kombinaci relačních a multidimenzionálních databází, umožňující uložení velkého objemu dat, a to v definovaných časových řezech. Je to integrovaný a konzistentní systém pro poskytování informací pro podporu rozhodování. Jde tak o proces, v němž organizace

extrahují ze svých informačních zdrojů takové informace, které mají zásadní význam pro úspěšné řízení firmy. Datové sklady řeší některé stávající překážky současných informačních systémů z hlediska potřeb analytických úloh.

Obrázek 1-3 Data, informace, znalosti, moudrost



Databanka má obdobný význam jako datová základna, vystihuje však i vnitřní strukturu dat a vazby mezi datovými objekty.

Obecně pojem **metasystém** označuje systém, který popisuje, resp. modeluje jiný systém. V případě informačního systému jde o metainformační systém. Metainformační systém je jednotou metadatabáze (metadat) a operací, které umožňují uchování a zpracování metadat. **Metadata** popisují informační systém a jeho jednotlivé komponenty, jako data, vazby mezi nimi, funkce informačního systému, procesy a případně jeho programové a technické komponenty.

Informace jsou výsledkem zpracování dat. Tento proces přetváří data tak, aby mohl příjemce výsledek použít, aby zvýšil svou „úroveň vědění“. Je nutné zahrnout nejen data, které slouží na vypracování vybrané varianty, ale všechna data použitá na vypracování všech variant, ze kterých se vybírá řešení. Informací rozumíme přetvořená data, kterým uživatel připisuje určitý význam, které uspokojují konkrétní informační objektivní potřebu svého příjemce.

Příjemce posuzuje kvalitu obdržených informací z hlediska obsahu a formy.

Z **hlediska obsahu** hodnotí:

- relevantnost (do jaké míry jsou významné pro daný účel),
- aktuálnost,
- přesnost,
- úplnost (jsou-li kompletní),
- podrobnost (jak postihují detaily),
- správnost, pravdivost,
- spolehlivost (zda zdroje informací jsou dostatečně spolehlivé).

Z **hlediska formy** posuzuje:

- kompetentnost (zda informace byly předány správným osobám),
- včasnost (zda byly informace k dispozici v okamžiku jejich potřeby),

- srozumitelnost (zda byly informace vhodně prezentovány),
- nákladová přiměřenost (zda náklady odpovídaly přínosům plynoucím z použití informací.

Znalosti představují zobecněné poznání reality dané vzájemnou interakcí zkušeností, faktů, vztahů, hodnot, myšlenkových procesů a významů. Znalosti tedy souvisejí s vymezováním pojmů, s kategorizací a s definováním hypotéz a s odvozováním závěrů. Znalosti vytvářejí systémový rámec pro vznik nových informací spočívajících v tom, že umožňují rozpoznat potřebný informační obsah dat. Na rozdíl od dat, která se neustále mění, jsou znalosti relativně stálejší, protože představují vyšší stupeň abstrakce.

1.2 POŽADAVKY NA INFORMAČNÍ SYSTÉM

Nároky na informační systém jsou ovlivňovány celou řadou faktorů. Jedná se např. o velikost organizace a s tím spojený objemem dat a informací, různé geografické členění, různé hierarchické členění s celou řadou vztahů a souvislostí, úroveň otevřenosti systému vůči externím uživatelům atd.

Informační systém, jako nástroj na zpracování informací a pro podporu řízení organizace proto musí splňovat následující požadavky:

- **integrovanost**, kdy informační systém musí věrně zobrazovat a přesně popisovat to, že všechny jevy a procesy v podniku nebo organizaci spolu souvisí a vzájemně se ovlivňují,
- **pružnost a otevřenost,** znamená to, že software musí být schopen reagovat na vývoj v oblasti informačních technologií a musí být propojitelný s jinými systémy,
- **konzistentnost a nezávislost**, zahrnují především hladký přechod na nový systém, nízké náklady na zaškolení a správu, jednotné prostředí, komunikace s ostatními softwarovými platformami firmy nebo jejích partnerů, podpora mobilních nebo vzdálených uživatelů, nezávislost znamená provozovatelnost v různých databázových prostředích a pod různými operačními systémy,
- **standardizace**, systém vyhovuje standardům daným státními, oborovými, firemními a dalšími normami,
- **adaptabilita**, systém dovoluje použití v různých organizačních strukturách s různým počtem organizačních úrovní,
- **parametrizovatelnost**, pomocí parametrů jsou nastavitelné možnosti, které systém poskytuje a to jak o systémová, tak i uživatelská,
- **přístupnost**, do systému je umožněn současný přístup více uživatelů na různých úrovních,
- **distribuovanost**, zpracování dat je prováděno na místech, požadovaných organizací, obvykle přímo u koncových uživatelů nebo u nadřízené organizační složky,
- **bezpečnost a stabilita**, zde se jedná především o zabezpečení proti vnitřnímu i vnějšímu zneužití, zamezení provozním výpadkům, zabezpečení rekonstrukce dat atd., přístup k datům je umožněn autorizovaným uživatelům a pomocí vestavěných funkcí, transakčního zpracování a replikací je zajištěna integrita dat i v rozsáhlých sítích,

- **komplexnost**, zahrnuje celý komplex na sebe navazujících údajů a uceleně řeší problematiku organizace,
- **dlouhá životnost**, zaručuje delší dobu provozu bez nároků na jeho zásadní restrukturalizaci v průběhu několika let,
- **jednoduchost a ergonomičnost**, řešení musí vycházet z praxe, musí být jednoduché, uživatelsky přátelské, přinášet ulehčení rutinní administrativy, zamezovat možnosti odložení nebo ztráty dokumentů,
- **dynamičnost a otevřenost**, systém je připravený na spolupráci s jinými systémy a vychází takové spolupráci vstříc, otevřenosti se dosahuje důsledným dodržováním všeobecně uznávaných standardů, nepoužíváním vlastních a nestandardních přístupů a řešení.

1.3 KLASIFIKACE INFORMAČNÍCH SYSTÉMŮ

Klasifikaci informačních systémů můžeme provádět podle řady hledisek, jako je např. podle informačního prostředí, organizační úrovně řízení, převládající funkce IS, podle režimu činnosti, hlavního zaměření, architektury atd.

Při členění podle informačního prostředí se zaměřujeme na **typu objektů**, což mohou být:

- informační zdroje, např. knihy, časopisy atd. v knihovních systémech,
- hmotné objekty, např. evidence majetku, oběh zásob atd.
- peníze, např. ekonomické systémy,
- osoby, personální systémy, systémy pro práci s klienty atd.

Jednotlivá prostředí si mohou být podobná, čili i řešení IS si jsou podobná. Je proto výhodné vytvářet typové projekty.

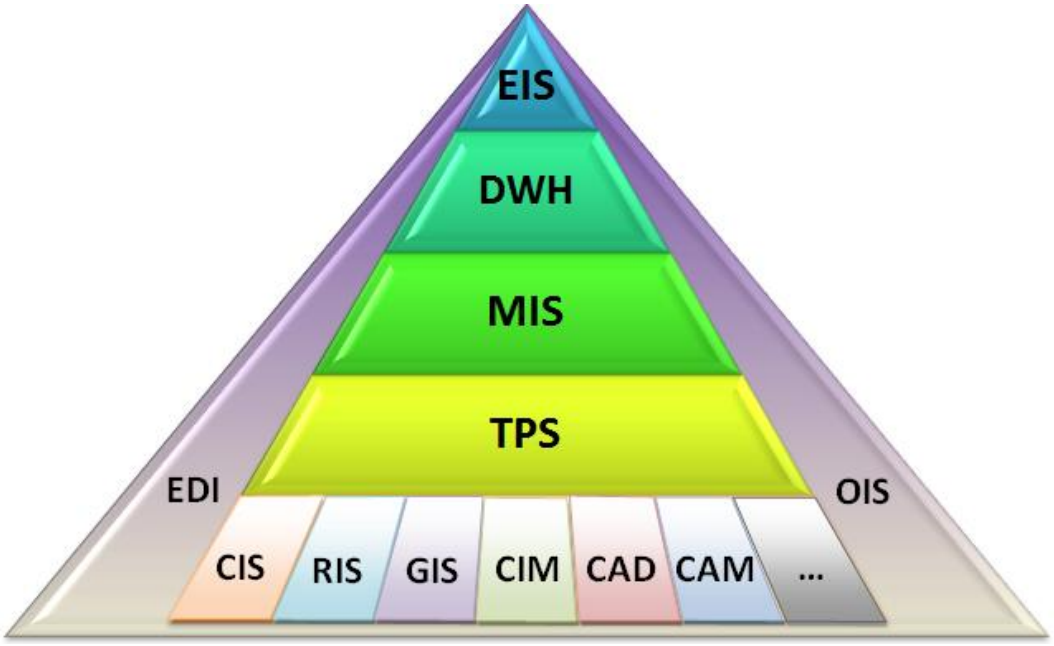
V členění **podle organizační úrovně** řízení se uplatňuje hierarchie řízení, resp. vertikální členění organizací nebo třídění objektů, např.:

- úrovně řízení organizace, např. podpora vrcholového, středního popř. nižšího managementu,
- organizační struktura, např. centrála, závody, pobočky atd.
- hierarchie institucí, např. ministerstvo, územní orgán,
- určení dle typických znaků, např. soukromé a státní firmy nebo členění dle počtu zaměstnanců atd.

Podle převládající funkce lze informační systémy členit na:

- **dokumentografické**, někdy také nazývané dokumentačně-rešeršní nebo textové, data jsou částečně nebo zcela nestrukturovaná, mají formu volného textu, obrázků, zvuků, pracujeme s přibližnými dotazy, vyhledáváme textové informace dle vzorků (klíčových slov) nebo pomocí metod vyhledávání s předzpracováním textů nebo vzorků nebo obojího apod.,
- **faktografické**, informace jsou strukturované, ale i nestrukturované, relativně stálé, mají funkce pro provádění operací s informacemi vybranými z databáze,
- **měřicí, regulační**, používané v IS pro řízení technologických procesů.

Obrázek 1-4 Příklad architektury podnikového informačního systému



Podle režimu činnosti lze IS dělit na systémy:

- individuálního zpracování požadavků, např. PC,
- dávkového zpracování dat (střediskové počítače, zpracování dat po sběru v terénu apod.),
- zpracování dat v reálném čase (rezervace letenek, technologické procesy, diagnostické systémy, automatizované knihovnické procesy),
- zpracování dat v centralizovaných databázích,
- zpracování dat v distribuované bázi dat.

Dle zaměření můžeme systémy členit na:

- informační systémy organizací, kde informace je ekonomický zdroj,
- veřejné informační systémy (TV, tisk, rozhlas, knihovny, zpravodajské agentury), informace je zboží,
- informační systém veřejné správy (government IS), informace je veřejný statek.

Z pohledu architektury můžeme systémy rozdělit např. na:

- systémy centralizované, aplikace běží na hlavním počítači, aplikace využívající databázi i komunikační software, který přenáší data na uživatelské terminály, které obvykle mají velmi omezené možnosti lokálního zpracování nebo žádné, tyto systémy představují jednovrstvou architekturu,
- personální počítače, decentralizované, mohou v oblasti zpracování dat plnit řadu stejných úkolů jako větší systémy, jsou však vhodné pouze pro menší rozsah zpracování,

- architektury klient/server (K/S) využívají různých typů technologií, umožňují distribuovat aplikační software, data nebo služby v rámci prostředí, ve kterém některé výpočetní zdroje plní funkci klientů požadujících služby a jiné plní funkci serverů tyto služby poskytujících, dochází k oddělení prezentační, aplikační a transakční logiky,
- systémy distribuované, data se sdílejí mezi různými hostitelskými systémy tak, že se mezi nimi posílají změny v interní síti nebo po datových linkách, aplikace, která běží na jednom nebo několika počítačích, vybírá data změněná v definovaném časovém intervalu a posílá tato data centrálnímu počítači nebo jiným hostitelským počítačům v počítačové síti, databáze se aktualizují, aby všechny systémy byly synchronizovány.

2 INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

Veřejná správa je široký komplex činností zabezpečovaných na jednotlivých úrovních ve veřejném zájmu, zahrnující spravování, služby, dozor a organizování. Veřejnou správu můžeme rozlišit na státní správu a samosprávu (územní a zájmovou). Tvoří souhrn institucí, které tyto činnosti vykonávají a které potřebují informační podporu, a to jak směrem dovnitř, jako právnické osoby nebo jejich součásti, tak vně, směrem k občanům, popř. právnickým osobám, nebo dalším orgánům veřejné moci. V této kapitole se po stručné charakteristice veřejné správy zaměříme na informační systémy veřejné správy a legislativní dokumenty, které je ovlivňují. Veřejná správa je široký komplex činností zabezpečovaných na jednotlivých úrovních ve veřejném zájmu, zahrnující spravování, služby, dozor a organizování. Veřejnou správu můžeme rozlišit na státní správu a samosprávu (územní a zájmovou). Tvoří souhrn institucí, které tyto činnosti vykonávají a které potřebují informační podporu, a to jak směrem dovnitř, jako právnické osoby nebo jejich součásti, tak vně, směrem k občanům, popř. právnickým osobám, nebo dalším orgánům veřejné moci. V této kapitole se po stručné charakteristice veřejné správy zaměříme na informační systémy veřejné správy a legislativní dokumenty, které je ovlivňují.

2.1 STÁTNÍ A VEŘEJNÁ SPRÁVA

V obecném pojetí můžeme pojem správa chápat jako činnost, jejíž podstatou je zabezpečování výkonu a řízení určitých záležitostí. Tato činnost musí být zaměřena na určitý cíl. Proto tyto činnosti musí být systematické, organizované a soustavné. Mezi tyto činnosti mimo jiné patří zabezpečení administrativy, administrace, institucionalizované kontrolní a regulativní činnosti atd.

Právo vymezuje pojem správa jako činnost, kterou vykonávají státní orgány společně s orgány jiných veřejnoprávních případně soukromě právních subjektů. Všechny tyto subjekty jsou vázány příkazy a nařízeními. Orgány veřejné správy plní výkonné funkce, které se projevují především jako rozhodnutí. Jejich činnost je zakotvena v ústavě a v dalších právních normách, které na ni navazují. Hlavním úkolem VS je zajištění její legality na všech jejích stupních.[1]

NEPŘEHLÉDNĚTE

Veřejná správa je správa veřejných záležitostí uskutečňovaných v rozhodující míře jako projev výkonné moci ve státě.

Je to soubor významných procesů řízených, regulovaných a zabezpečených specifickými institucemi zaměřenými na řízení veřejných záležitostí. Jsou to:

- v širším slova smyslu: úřady VS, vláda, parlament, soudy;
- v užším slova smyslu: úřady, které veřejnou správu vykonávají.

Dělíme ji na

- výkon státní správy;
- výkon územní samosprávy.

[1] http://verejna-sprava.blogspot.cz/2011/05/14-pojem-verejna-sprava.html

NEPŘEHLÉDNĚTE

Státní správa je veřejná správa uskutečňovaná státem. Svým charakterem představuje realizaci moci výkonné.

Stát vykonává státní správu zejména prostřednictvím státních orgánů:

- vlády (vrcholný ústavní orgán moci výkonné)
- ministerstev a ostatních ústředních správních úřadů
- odborných územních správních úřadů (odvětvová působnost)
- veřejných ozbrojených sborů a jiných veřejných sborů

Státní správa je činnost:

- podzákonná (je vázána zákony);
- výkonná (vykonává zákony);
- nařizovací (uplatňuje mocenské nástroje – závaznost a vynutitelnost správních aktů – vyhlášky, nařízení,…).

Výkon státní správy lze svěřit orgánům územní samosprávy jen prostřednictvím zákona, hovoříme o přenesené působnosti obcí a krajů.

Samosprávu můžeme rozčlenit na:

- územní samosprávu tvořenou obcemi, kraji a hlavním městem Prahou, která je veřejnou správou uskutečňovanou jinými subjekty, než je stát, a která má oprávnění vykonávat určité náležitosti samostatně, stát zasahuje pouze při porušení zákona;
- profesní, zájmovou samosprávu, jejímiž nositeli jsou např. profesní komory.

NEPŘEHLÉDNĚTE

Veřejnou moc reprezentuje ze zákona orgán veřejné moci (OVM). Dle § 2 písm. c) Zákona 111/2009 Sb., o základních registrech je to státní orgán, územní samosprávný celek a fyzická, nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy.

OVM je oprávněn autoritativně rozhodovat o právech a povinnostech fyzických či právnických osob nebo jinak zasahovat do jejich právní sféry, a to buď přímo, zejména v případě orgánů moci výkonné nebo soudní, nebo zprostředkovaně, pokud jde o orgány moci zákonodárné. Seznam orgánů veřejné moci a detailní informace ke každému z nich jsou dostupné na Portálu veřejné správy (http://portal.gov.cz/portal/rejstriky/ogd/x-sovm.html).

Instituce vykonávající přímo veřejnou správu:

- ministerstva;
- ústřední správní úřady (Český statistický úřad, Český báňský úřad, Úřad průmyslového vlastnictví, Úřad pro ochranu hospodářské soutěže, Správa státních hmotných rezerv, Státní úřad pro jadernou bezpečnost, Komise pro cenné papíry, Národní bezpečnostní úřad, Energetický regulační úřad, Úřad vlády české republiky);
- územní správní úřady (finanční úřady…);
- veřejné ozbrojené a neozbrojené sbory (policie, hasiči);
- orgány obcí (zastupitelstvo, rada obce, starosta, obecní úřad, výbory, komise), krajů (zastupitelstvo, krajská rada, hejtman, krajský úřad, výbory, komise) a hl. m. Prahy (zastupitelstvo, rada, primátor, magistrát atd.);
- další instituce (profesní komory, vysoké školy, nadace…).

2.2 INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

Informační činnosti státních orgánů se do roku 2000 označovaly pojmem „Státní informační systém“. Nyní je nahrazen pojmem „Informační systém veřejné správy“ (ISVS).

ISVS jsou vymezeny souborem zákonných norem. Hlavními jsou:

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ve znění pozdějších předpisů);
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím;
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (ve znění pozdějších předpisů);
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (ve znění pozdějších předpisů);
- Zákon č. 329/2012 Sb., úplné znění zákona o archivnictví a spisové službě.

NEPŘEHLÉDNĚTE

Informační systémy veřejné správy[2] jsou souborem informačních systémů sloužících pro výkon veřejné správy včetně informačních systémů podle zvláštních zákonů:

a) zpravodajskými službami;
b) Policií České republiky při plnění jejích úkolů;
c) celními orgány při plnění jejich úkolů, s výjimkou správy cel, daní a jiných peněžitých plnění a správního řízení,
d) orgány činnými v trestním řízení v souvislosti s trestním řízením, s výjimkou evidence Rejstříku trestů;
e) Policií České republiky a Vězeňskou službou České republiky při poskytování zvláštní ochrany a pomoci ohroženým osobám podle zvláštního právního předpisu;
f) Ministerstvem financí v rámci činnosti podle zvláštního právního předpisu o boji proti legalizaci výnosů z trestné činnosti nebo zvláštního právního předpisu o provádění mezinárodních sankcí za účelem udržování mezinárodního míru a bezpečnosti, ochrany základních lidských práv a boje proti terorismu;
g) Národním bezpečnostním úřadem, zpravodajskou službou nebo Ministerstvem vnitra při provádění bezpečnostního řízení a vedení evidencí podle zvláštního zákona;
h) v působnosti Ministerstva obrany, při činnostech vykonávaných podle zvláštních právních předpisů;
i) Ministerstvem vnitra, Ministerstvem financí a Ministerstvem spravedlnosti při zpracování osobních údajů příslušníků bezpečnostních sborů podle zvláštního právního předpisu;
j) správními úřady a orgány územních samosprávných celků v přenesené působnosti při činnostech souvisejících se zajišťováním obrany státu podle zvláštního právního předpisu;
k) orgány veřejné správy a právnickými osobami, pokud jsou používané výlučně k podpoře krizového řízení.

[2] § 3 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

Mají-li IS uvedené v bodech b) až k) vazby na jiné ISVS realizované prostřednictvím informačních činností, vztahuje se na ně zákon pouze v rozsahu těchto vazeb, nestanoví-li zvláštní právní předpisy jinak.

Snahou je docílit provázání autonomních ISVS do jednotné sítě. To ovšem především vyžaduje zajistit:

- ochranu dat obsahujících osobní údaje proti zneužití, legislativně i technicky;
- kontrolovaný přístup ke společně sdíleným údajům, vytvoření systému oprávnění.

U ISVS hrají rozhodující roli subjekty:

- správci ISVS, což jsou subjekty, které podle zákona určují účel a prostředky zpracování informací a za IS odpovídají, jsou to ministerstva a jiné správní úřady a územní samosprávné celky (orgány veřejné správy)
- provozovatelé ISVS jsou subjekty, které provádí alespoň některé informační činnosti související s informačním systémem, provozováním ISVS může správce pověřit i jiné subjekty, pokud to jiný zákon nevylučuje, provozovatelé jsou také povinen při provozování IS zajišťovat ochranu a bezpečnost informací v rámci provozovaného IS.

NEPŘEHLÉDNĚTE

Referenční rozhraní je souhrn právních, technických, organizačních a jiných opatření vytvářejících jednotné integrační prostředí ISVS, které poskytuje kvalitní soustavu společných služeb, včetně služeb výměny oprávněně vyžadovaných informací mezi jednotlivými informačními systémy orgánů veřejné správy a dalšími subjekty.

Územní samospráva se vyznačuje při výkonu veřejné správy specifickými formami. V rámci své činnosti využívá prostředky, které nemají povahu státních mocenských prostředků (samospráva), i donucovací a sankční opatření (výkon státní správy). Požívá určitou autonomií, např. vydává vlastní právní předpisy. Jejím hlavním úkolem je přiblížit řešení věcí veřejného zájmu občanovi. Tyto činnosti mají za úkol podporovat informační systémy územní samosprávy.

Pojem **informační systémy územní samosprávy** v sobě zahrnuje zejména dva typy systémů:

- informační systémy krajů;
- informační systémy měst a obcí.

Jedná se o ISVS, proto musí splňovat všechny standardy a zákonné normy, které se týkají ISVS.

Informační systém města/obce (ISMO) zobrazuje daný územní celek jako komplex jeho základních funkčních částí (subsystémů). Umožňuje místní správě a samosprávě optimalizaci zdrojů a zjednodušení řídících a rozhodovacích činností města/obce.

Základem každého ISMO jsou databáze, včetně základních registrů, které jsou vztaženy k danému území. Registry jsou pak pomocí komunikační vrstvy propojeny s dalšími typizovanými subsystémy. Registr je společná zdrojová základna dat pro orgány státní správy, fungující na základě obecně závazných právních předpisů.

Informační systém kraje (ISK) plní na úrovni kraje obdobné funkce, jako ISMO. Samozřejmě konkrétní požadavky na funkcionalitu a strukturu těchto systémů jsou dány potřebami krajských orgánů. Struktura informačního systému kraje vychází proto z obdobné struktury jako ISMO, jedná se o použití typizovaných informační systémů.

Oba typy systémů (ISMO i ISK) nemají a ani nebudou mít jednotnou podobu. Je to dáno mimo jiné i tím, že úřady mají možnost výběru vlastní IS (dle stanovených pravidel).

PŘÍKLAD 1 PŘÍKLADY ISVS

Stát:

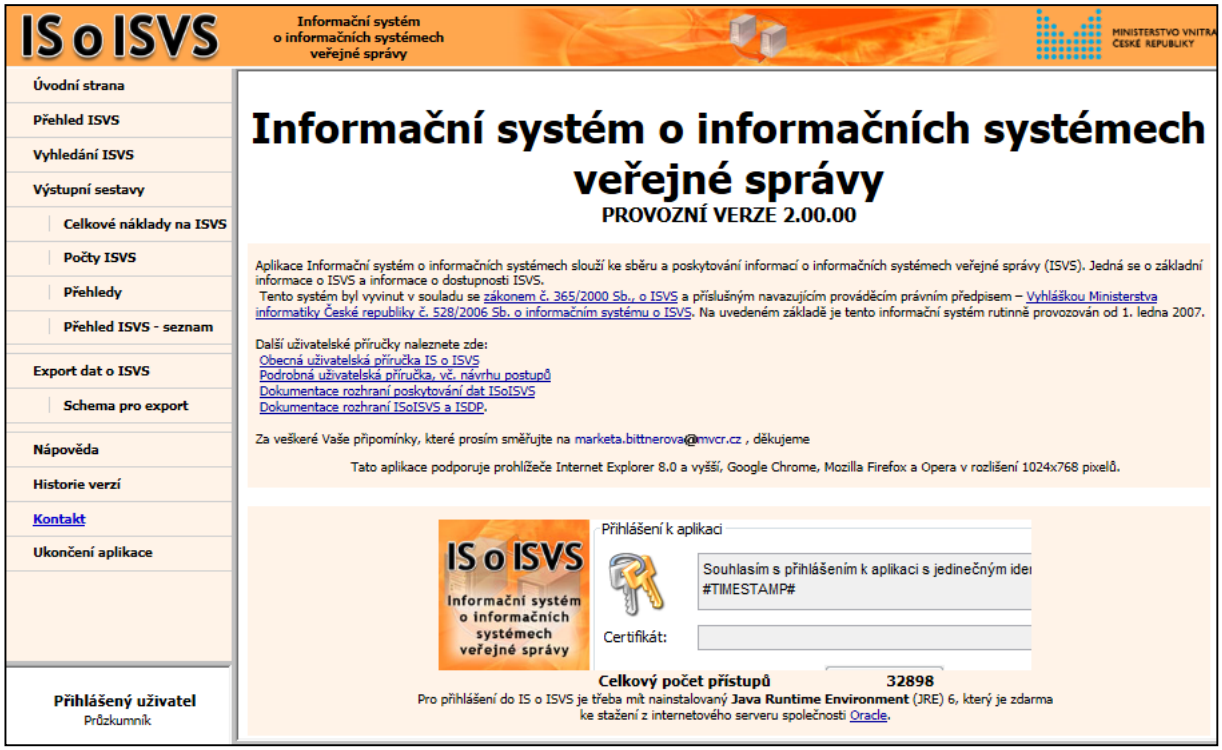
- informační systém o datových prvcích,
- informační systém o informačních systémech veřejné správy (ISoISVS),
- informační systém evidence obyvatel (stát),
- registr rodných čísel – ISVS, který je samostatnou funkční částí informačního systému evidence obyvatel.

Obec:

- evidence uložených pokut (správních sankcí) podle § 58 a 59 zákona č. 128/2000 Sb., o obcích,
- evidence plátců místních poplatků podle zákona č. 565/1990 Sb., o místních poplatcích,
- evidence obyvatel.

2.3 INFORMAČNÍ SYSTÉM O INFORMAČNÍCH SYSTÉMECH VEŘEJNÉ SPRÁVY

Obrázek 2-1 Vstupní stránka aplikace Informační systém o informačních systémech



Zdroj: https://www.sluzby-ISVS.cz/ISoISVS/Applets/DefaultSSL.aspx

Informační systém o informačních systémech[3] slouží ke sběru a poskytování informací o informačních systémech veřejné správy (IS o ISVS). Jedná se o základní informace o ISVS a informace o dostupnosti ISVS. Byl vyvinut v souladu se zákonem č. 365/2000 Sb., o ISVS a Vyhláškou Ministerstva informatiky České republiky č. 528/2006 Sb. o informačním systému o ISVS. Rutinně provozován od 1. ledna 2007.

Do IS o ISVS orgány veřejné správy předávají základní údaje o jimi spravovaných ISVS a jimi poskytovaných službách a používaných datových prvcích. Zpřístupňovanými datovými prvky jsou rovněž provozní údaje, pokud jsou využity pro realizaci vazby jimi spravovaných ISVS na informační systémy jiného správce. Forma a technické náležitosti předávání údajů (a to včetně popisu jednotlivých předávaných položek) jsou stanoveny vyhláškou č. 528 /2006 Sb., o informačním systému o informačních systémech veřejné správy.

Funkce IS o ISVS[4]:

- vkládání záznamů o nových ISVS, změna záznamů o ISVS nebo vkládání záznamů o ukončení činnosti ISVS;
- vyhledávání, lze vyhledávat podle hledisek:
    - kategorie, charakterizuje zaměření ISVS, je rozdělena podle působnosti všech centrálních orgánů státní správy, přičemž působnost byla pro větší centrální orgány rozdělena na konkrétní oblasti reálného života (např. zdravotnické, daňové apod.;
    - kraj, položka slouží pro vyhledávání ISVS, které mají zpravidla regionální působnost např. ISVS krajského nebo obecního úřadu, popř. ISVS OVS s centrální působností, které jsou provozovány v konkrétních oblastech.
    - stav, indikuje, v jakém stadiu procesu se záznam nachází, např. příprava, předložen, zveřejněn atd.
    - název ISVS;
    - název správce ISVS;
    - veřejný (alespoň část)/ neveřejný ISVS;
    - ISVS poskytuje služby
    - číslo legislativního předpisu, podle kterého je OVS veden (speciálně pro státní správu);
    - podle rozmezí nákladů, které byly na jeho vybudování potřeba atd.
- výstupní sestavy, poskytují přehledy o celkových nákladech na ISVS, počtech ISVS zveřejněných v IS o ISVS v konkrétní kategorii a přehledy ISVS, buď seznamy, nebo pomocí vyhledávání je možné tvořit sestavy dle konkrétních zadaných podmínek.

V IS o ISVS existují role:

- průzkumník je uživatel, který nemá právo vkládat do IS o ISVS záznamy, je oprávněn pouze číst záznamy vložené ostatními uživateli a tvořit výstupní sestavy;
- osoby jednající za správce má právo vkládat záznamy o nových ISVS, měnit záznamy ISVS a vkládat záznamy o ukončení činnosti ISVS;
- administrátor je ISVS pracovník, který provádí kontrolu předložených záznamů v redakční systém, který zamezí vkládání nesmyslných a zavádějících informací, po kontrole zveřejní příslušný záznam nebo tento záznam vrátí osobě jednající za správce k dopracování, případně tento záznam odstraní.

[3] https://www.sluzby-ISVS.cz/ISoISVS/Applets/DefaultSSL.aspx

[4] IS o ISVS. Obecná uživatelská příručka IS o ISVS Dostupné z: https://www.sluzby-ISVS.cz/ISoISVS/Dokumentace/obecna_prirucka_IS_o_ISVS.pdf

Pro výkon všech uživatelských rolí, kromě role průzkumníka, je potřeba se do IS o ISVS přihlásit za použití kvalifikovaného certifikátu.

2.4 ZÁKLADNÍ PŘEDPISY A DOKUMENTY

2.4.1 ZÁKON O INFORMAČNÍCH SYSTÉMECH VE VEŘEJNÉ SPRÁVĚ

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ve znění pozdějších předpisů) stanovuje práva a povinnosti osob souvisejících s provozem informačních systémů veřejné správy.

Byl zřízen Úřad pro veřejné informační systémy (nahradil Úřad pro státní informační systém), který byl později nahrazen Ministerstvem Informatiky ČR. Nyní vše patří do gesce Ministerstva vnitra.

Definovány jsou povinnosti orgánů veřejné správy ve vztahu k informačním systémům, tj. práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. Stanovuje, že mezi správce informačních systémů veřejné správy patří ministerstva, jiné správní úřady, orgány územní samosprávy a další státní orgány. Právní úprava se týká rovněž měst/obcí a krajů. Zákon se nevztahuje na provozní informační systémy.

Zákon dále stanovuje pravidla dlouhodobého řízení ISVS, tj. vytváření a vydávání informační koncepce a provozní dokumentace, zajišťování atestací dlouhodobého řízení, popř. uplatňování opatření vyplývajících z bezpečnostních požadavků, a kontroly dodržování povinností orgánů veřejné správy.

V zákonu jsou popsány oprávnění a postupy pro akreditace a provádění atestací. Atestacemi se rozumí stanovení shody:

- způsobilosti k realizaci vazeb ISVS s jinými IS prostřednictvím referenčního rozhraní;
- dlouhodobého řízení ISVS s požadavky zákona a prováděcích právních předpisů k zákonu.

Akreditace je postup, na jehož základě se vydává osvědčení o tom, že právnické nebo fyzické osoby, které jsou podnikateli, splňují ve vymezeném rozsahu technické, organizační, ekonomické a personální předpoklady k provádění atestací, v našem případě ISVS.

Zákonem jsou rovněž vymezeny portál veřejné správy a centrální místo služeb (viz kap. 6) a kontaktní místa veřejné správy (viz kap. 5).

Se zákonem souvisí řada vyhlášek.

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 (vyhláška o informačním systému o informačních systémech veřejné správy), stanovuje formu a technické náležitosti předávání údajů do veřejného informačního systému. Předávají se údaje o vytvoření ISVS, změně údajů, které jsou o ISVS v informačním systému o ISVS uvedeny nebo o ukončení činnosti ISVS prostřednictvím elektronického formuláře.

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 (vyhláška o dlouhodobém řízení informačních systémů veřejné

správy), jak dlouhý název napovídá, se zabývá strukturou a obsahem informační koncepce a provozní dokumentací.

Stanovuje požadavky na strukturu a obsah informační koncepce a postupy orgánů VS při jejím vytváření, vydávání, při hodnocení jejího dodržování. Dále se zabývá požadavky na řízení bezpečnosti a kvality informačních systémů veřejné správy, na strukturu a obsah a provozní dokumentace a rozsah provozní dokumentace předkládané při atestaci.

Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy, se při posuzování dlouhodobého řízení ISVS zabývá:

- zkouškou (co atestační středisko posuzuje);
- stanovením výsledků zkoušky (záznamy o zjištěních, postupy při stanovení výsledků).

Vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní, stanovuje, že posuzování způsobilosti se sestává z:

- zkoušky (posuzuje soulad realizace vazby s technickou dokumentací služby a soulad datových prvků použitých při realizaci vazby s datovými prvky vyhlášenými prostřednictvím informačního systému o datových prvcích);
- stanovení výsledku zkoušky (zaznamenávání údajů o průběhu zkoušky, postup při stanovení výsledků zkoušky.

Vyhláška č. 53/2007 Sb., o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní (vyhláška o referenčním rozhraní) stanoví:

- technické náležitosti (mezi kterými systémy lze vazbu uskutečnit, jaké lze použít datové prvky a další náležitosti popsané v technické dokumentaci)
- funkčních náležitosti (zaznamenávání a uchovávání záznamů o událostech spojených s uskutečňováním vazeb v souladu s provozní dokumentací IS).

2.4.2 ZÁKON O ELEKTRONICKÝCH ÚKONECH A AUTORIZOVANÉ KONVERZI DOKUMENTŮ

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů upravuje:

- elektronické úkony státních orgánů, orgánů územních samosprávných celků, Pozemkového fondu České republiky a jiných státních fondů, zdravotních pojišťoven, Českého rozhlasu, České televize, samosprávných komor zřízených zákonem, notářů a soudních exekutorů vůči fyzickým osobám a právnickým osobám, elektronické úkony fyzických osob a právnických osob vůči orgánům veřejné moci a elektronické úkony mezi orgány veřejné moci navzájem prostřednictvím datových schránek;
- dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob prostřednictvím datových schránek;
- informační systém datových schránek;
- autorizovanou konverzi dokumentů.
- Zákon se nevztahuje na dokumenty, které obsahují utajované informace.

Problematikou se budeme podrobněji zabývat v kap.0.

2.4.3 ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ

Normou nejvyšší právní síly v oblasti ochrany dat v ČR je Listina základních práv a svobod. **Zákon č. 101/2000 Sb**., o ochraně osobních údajů a o změně některých zákonů (ve znění pozdějších předpisů) upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států. Naplňuje právo každého na ochranu před neoprávněným zasahováním do soukromí. Tímto zákonem byl zřízen Úřad pro ochranu osobních údajů se sídlem v Praze.

Zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci i fyzické a právnické osoby a na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky. Naopak se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu, a na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

Znamená přenesení zodpovědnosti za ochranu osobních údajů na samotného občana, což je realizováno udělením nebo neudělením souhlasu se zpracováváním informace, vyžádáním informací o údajích, které jsou o něm evidovány, vznesením požadavku na výmaz či opravu apod.

2.4.4 ZÁKON O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

Zákon 106/1999 Sb., o svobodném přístupu k informacím (ve znění pozdějších předpisů) upravuje podmínky práva svobodného přístupu k informacím a stanoví základní podmínky, za nichž jsou informace poskytovány. Základním principem svobody informací je tzv. publicita veřejné správy.

Státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce (povinné subjekty) jsou povinny poskytovat informace vztahující se k jejich působnosti a to i prostřednictvím zařízení umožňujícím dálkový přístup (internet). Po přijetí tohoto zákona platí, že se poskytnou všechny informace, pouze s tou výjimkou, k níž dává oprávnění konkrétní zákonné ustanovení (např. ochrana osobních údajů, utajované skutečnosti, průmyslové vlastnictví apod.). Povinnost poskytovat informace se netýká dotazů na názory, budoucí rozhodnutí a vytváření nových informací.

Povinné subjekty poskytují informace žadateli na základě žádosti nebo zveřejněním. Informace poskytovaná zveřejněním se poskytuje ve všech formátech a jazycích, ve kterých byla vytvořena. Pokud je taková informace zveřejněna v elektronické podobě, musí být zveřejněna i ve formátu, jehož specifikace je volně dostupná a použití uživatelem není omezováno. Je-li informace poskytována na základě žádosti, poskytuje se ve formátech a jazycích podle obsahu žádosti o poskytnutí informace, pokud tento zákon nestanoví jinak. Povinné subjekty nejsou povinny měnit formát nebo jazyk informace, pokud by taková změna byla pro povinný subjekt nepřiměřenou zátěží; v tomto případě vyhoví povinný subjekt žádosti tím, že poskytne informaci ve formátu nebo jazyce, ve kterých byla vytvořena. Veřejnosti musí být informování na místě, které je všeobecně přístupné, jakož i umožnit pořízení jejich kopie.

2.4.5 ZÁKON O ELEKTRONICKÉM PODPISU

Zákon 227/2000 Sb., o elektronickém podpisu (ve znění pozdějších předpisů) upravuje používání elektronického podpisu, poskytování certifikačních služeb a souvisejících služeb, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. Dochází k faktickému zrovnoprávnění psaného a elektronického dokumentu.

Každý občan má právně platnou možnost podepisovat se elektronickým podpisem, a tedy identifikovat se vůči úřadům na dálku. Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila. Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

Zákon o elektronickém podpisu byl doplněn nařízeními vlády, která stanovily pravidla pro jeho provádění.

Pro obce bylo významné zejména **Nařízení vlády č. 304/2001 Sb.,** které ukládalo povinnost zřídit tzv. elektronickou podatelnu. Bylo zrušeno 1. 1. 2005 a nahrazeno nařízením vlády 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů. Stanovily povinnost orgánů veřejné moci zřídit e-podatelny (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu), vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací. Změna zákon o archivnictví a spisové službě a o změně některých zákonů (167/2012 Sb.) toto nařízení zrušila.

Vyhláška č. 496/2004 Sb., o elektronickým podatelnách upravovala postup, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelny. I toto nařízení zrušila změna zákona 167/2012 Sb.

Tuto oblast doplňuje Vyhláška 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb), kterou doplňují:

- seznam norem a standardů;
- struktura certifikační politiky a certifikační prováděcí směrnice.

Vyhláška 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu), mimo jiné v přílohách obsahuje standardy:

- kryptografických asymetrických algoritmů;
- kryptografických hashovacích funkcí.

2.4.6 ZÁKON O ARCHIVNICTVÍ A SPISOVÉ SLUŽBĚ

Zákon 329/2012 Sb., úplné znění zákona č. 499/2004 Sb., o archivnictví a spisové službě1, upravuje:

- výběr, evidenci a kategorizaci archiválií;
- ochranu archiválií;
- práva a povinnosti vlastníků archiválií;
- práva a povinnosti držitelů a správců archiválií (dále jen „držitel archiválie“);
- využívání archiválií;
- zpracování osobních údajů pro účely archivnictví;
- soustavu archivů;
- práva a povinnosti zřizovatelů archivů;
- spisovou službu;
- působnost Ministerstva vnitra a dalších správních úřadů na úseku archivnictví a výkonu spisové služby;
- správní delikty.

3 ZÁKLADNÍ REGISTRY VEŘEJNÉ SPRÁVY

Přestože využívání informačních technologií zaznamenalo významný pokrok, současný stav v oblasti dat není uspokojující. Setkáváme se s tím, že:

- některé často užívané údaje v informačních systémech veřejné správy jsou získávány a vedeny duplicitně;
- nejsou konzistentní;
- mají rozdílnou kvalitu z hlediska přesnosti, aktuálnosti a úplnosti;
- používané evidence jsou roztříštěné
- existují problémy s časovou synchronizací aktualizace užívaných údajů;
- ISVS nejsou dostatečně integrovány, nespolupracují, a tím nelze zajistit efektivní sdílení dat;
- občané jsou často nuceni opakovaně dokládat úřadům různé skutečnosti, které by si úřad mohl ověřit sám.

NEPŘEHLÉDNĚTE

Základní registry jsou informační systémy veřejné správy. Jsou to bezpečné databáze, sjednocující data vedená úřady o občanech a státních i nestátních subjektech. Sdílení dat mezi jednotlivými základními registry navzájem, základními registry a agendovými informačními systémy a agendovými informačními systémy navzájem a správa oprávnění přístupu k datům, popř. další činnosti jsou zajišťovány informačním systémem základních registrů, což je také informační systém veřejné správy.

Obsah základních registrů, informačního systému základních registrů a informačního systému územní identifikace vymezuje Zákon 111/2009 Sb., o základních registrech[5]. Ten také a stanovuje práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem.

Registry můžeme chápat jako centrální databáze, které by měly sdružovat všechny podstatné informace o všech subjektech (občané, organizace) a objektech (pozemky, dopravní prostředky atd.), kterých se dotýká státní a veřejná správa. Jsou to nástroje, umožňující nabízet relevantní a nezpochybnitelná data, tzv. referenční údaje. Obsah registru tvoří údaje o objektech, které jsou v něm vedeny a jsou v něm vedeny referenční a ostatní údaje.

NEPŘEHLÉDNĚTE

Referenční údaj je jedinečný a důvěryhodný údaj, vedený v příslušném základním registru veřejné správy, který je určen ke sdílení všemi relevantními ISVS podle jednoznačně stanovených pravidel.

Referenční údaje jsou takové údaje, které jsou povinně využívány dalšími informačními systémy veřejné správy. To je stanoveno zvláštními právními předpisy, které upravující správu registru. Práva k datům obsaženým v registru vykonává správce registru.

Registr musí být veden tak, aby zachycoval stav údajů k jakémukoliv datu a času od založení registru, popř. zachycuje stanovené údaje k datu dřívějšímu, pokud to stanovuje zvláštní právní předpis.

Úkolem registrů je zabezpečit dostupnost zdrojů dat v soustavě informačních systémů ve veřejné správě. Registrem veřejné správy je databáze spravovaná v rámci informačního systému, kterou za registr veřejné správy označuje zvláštní zákon. Správcem registru je

[5] Zákon 111/2009 Sb., o základních registrech (ve znění pozdějších předpisů).

správce informačního systému registru. Správce registru odpovídá za provoz a obsah registru. Aby registry plnily svou úlohu, musí být v elektronické podobě, snadno dosažitelné, ale naopak těžce zneužitelné.

Správcem registru je správce informačního systému, ve kterém je registr veden.

Provozovatelem registru se rozumí osoba, která bude pověřena technickým a organizačním zabezpečením provozu registru. Objekt je osoba, občan, věc, právo, nebo povinnost, o které jsou na základě zákona vedeny údaje v registru.

Editor registru je osoba výhradně oprávněná do registru zapisovat. Je to orgán veřejné moci, který je stanoven podle zákona upravujícího vedení příslušného základního registru.

Navrhovatel změny dat v registru je osoba, která bude oprávněna navrhovat změny v registru. Kontaktním místem registru má být místo odkud je možné provádět zápisy nebo změny v zápisu do registru.

Původce dat je osoba, která je ze zákona v konkrétním případě povinna oznámit změnu skutečností, uvedených v registru.

Okruhy registrů ve veřejné správě ukazuje schéma (viz Obrázek 3-1).

Obrázek 3-1 Okruhy registrů ve veřejné správě

Zdroj: vlastní

Pro všechny instituce by mělo platit, že všechny vyžadované informace se musí úřad nejdříve pokusit nalézt v jednom z výše zmíněných registrů a teprve v případě, že je nenalezne, se může obrátit na fyzickou nebo právnickou osobu. Naopak, každou novou informaci, kterou úřady získají (případně každou změnu) musí do těchto registrů zanést. Údaje v registrech veřejné správy musí být ve většině případů přístupné veřejnosti.

Referenční data jsou údaje, které jsou o daném objektu v rámci veřejné správy jedinečné. V případě vložení nového údaje bude třeba vytvořit i nové referenční údaj (identifikátor). V rámci registru není možné údaj smazat, lze pouze změnit jeho stav. Registry

jsou řešeny tak, že všechna data, která byla do příslušného registru od jeho založení zadána, je možné zpětně vyhledat.

Referenční vazby jsou kódy nebo identifikátory, kterými se odkazujeme na referenční údaje v základních registrech.

Zákon zřizuje rovněž Správu základních registrů[6]. Ta je správcem informačního systému základních registrů a zajišťuje jeho provoz a provoz jednotlivých registrů, realizuje vazby prostřednictvím služeb informačního systému základních registrů mezi jednotlivými základními registry, mezi základními registry a agendovými informačními systémy prostřednictvím a mezi jednotlivými agendovými informačními systémy. Zpřístupňuje referenční údaje obsažené v základních registrech a údaje obsažené v agendových informačních systémech v rozsahu oprávnění obsažených v registru práv a povinností. Vede záznamy o událostech souvisejících s provozováním informačního systému základních registrů.

Správa základních registrů zajišťuje, aby referenční údaje zapsané editory byly předávány prostřednictvím informačního systému základních registrů správcům základních registrů v nezměněné podobě. Sama není oprávněna k přístupu k obsahu referenčních údajů obsažených v základních registrech. V případě důvodné pochybnosti, že orgán veřejné moci neoprávněně přistupuje k osobním údajům, informuje neprodleně Úřad pro ochranu osobních údajů.

3.1 ZÁKLADNÍ REGISTRY

3.1.1 REGISTR OBYVATEL

Registr obyvatel1 je určen pro fyzické osoby, jeho správcem je Ministerstvo vnitra, a konkrétně obsahuje údaje o:

- všech občanech ČR;
- cizincích s povolením k pobytu v ČR;
- občanech jiných států, vedených v základních registrech;
- jiných fyzických osobách, o nichž jiný právní předpis stanoví, že budou vedeny v Registru obyvatel.

Nalezneme v něm referenční údaje (identifikační a lokalizační údaje, vztahujících se k fyzickým osobám):

- příjmení, jméno;
- datum narození a úmrtí;
- datum nabytí právní moci rozhodnutí soudu o prohlášení za mrtvého a den, který je v rozhodnutí uveden jako den smrti;
- státní občanství;
- čísla elektronicky čitelných identifikačních dokladů;
- údaj o tom, zda má osoba zpřístupněnu datovou schránku;
- odkaz do registru územní identifikace na adresu místa pobytu, příp. na adresu pro doručování;
- odkaz do registru územní identifikace na místo a okres narození a úmrtí; popřípadě stát narození a úmrtí.

Podrobný seznam referenčních údajů je uveden v § 18 zákona o základních registrech.

[6] http://www.mvszr.cz/

Odkazy zabezpečí, že do Registru obyvatel budou automatizovaně přebírány také veškeré údaje, týkající se změn adres, např. změna názvu ulice či přečíslování domu atd.

Základem je Informační systém evidence obyvatel, který je v působnosti Ministerstva vnitra (gestor), spolupracují MPSV a ČSÚ.

3.1.2 ZÁKLADNÍ REGISTR OSOB

V registru osob jsou zapsány všechny právnické (tuzemské, zahraniční i mezinárodní) osoby a jejich organizační složky a podnikající fyzické osoby. Tuzemské právnické osoby jsou rozděleny na obchodně-právní (za účelem výdělku), veřejnoprávní (veřejné instituce) a občanskoprávní (vycházejí s práva na sdružování).

Registr obsahuje údaje o všech osobách, tedy ekonomických jednotkách či subjektech podnikatelského i nepodnikatelského charakteru, a dále integrační propojení jednotlivých evidencí osob (struktura, klasifikace, místo a způsob evidence, komunikační rozhraní, ověřování a kontrola dat, aktualizace a využívání dat). Obsahuje základní identifikační údaje o osobách, jejich provozovnách a statutárních zástupcích. Seznam referenčních údajů je uveden v § 26 zákona o základních registrech.

Základním principem, podle něhož je možné daný subjekt považovat za osobu, která bude k nalezení v tomto registru, je registrace či evidence osoby před tím, než zahájí svoji činnost u některého správního subjektu či jiného úřadu.

Správcem registru je Ministerstvo spravedlnosti, spolupracují ČSÚ a MPSV.

ROS využívají všechny orgány veřejné správy, které mají oprávnění z Registru práv a povinností. Editoři provádí veškeré záznamy do ROS a v rámci jejich role přidělují osobám IČO a zapisují a aktualizují příslušné referenční údaje. Hlavní zdroje dat: obchodní rejstřík, rejstřík živnostenského podnikání a dále informační systémy nebo evidence vybraných ministerstev a ústředních orgány státní správy, profesní komory, obce, kraje nebo veterinární správa.

3.1.3 ZÁKLADNÍ REGISTR ÚZEMNÍ IDENTIFIKACE, ADRES A NEMOVITOSTÍ

Do územní identifikaci patří uzemní a správní členění státu, ulice, domy a adresní body. Změny mohou vzniknou buď změnou správního členění nebo na základě rozhodnutí orgánů veřejné moci (změny adresy, výstavba domu apod.)

Ve všech ostatních registrech je uvedená adresa odkazem do registru nemovitostí a územní identifikace. Jedná se o základní registr, který bude obsahovat nejčastěji užívané údaje ve veřejné správě. Jedná se zejména o údaje o adresách, které při své činnosti potřebuje většina orgánů veřejné správy.

V registru budou obsaženy údaje o základních územních prvcích, kterými jsou:

- území státu;
- region soudržnosti,
- vyšší územní samosprávní celek,
- kraj;
- okres;
- správní obvod obce s rozšířenou působností a obce s pověřeným obecním úřadem;
- území obce;
- vojenský újezd;
- správní obvod v hlavním městě Praze;
- městský obvod a městská část ve statutárních městech a v hlavním městě Praze;

- základní sídelní jednotka;
- katastrální území;
- stavební objekt;
- adresní místo
- pozemek v podobě parcely.

Jsou zde rovněž údaje o územně evidenčních jednotkách (část obce a ulice a jiné veřejné prostranství). Údaje vedené o těchto jednotkách budou identifikační (kód, název) a lokalizační (definiční bod, hranice). O územních prvcích parcela a stavební objekt budou v registru vedeny některé další údaje, včetně zprostředkovaných údajů z informačního systému katastru nemovitostí o vlastnictví a vlastnících. Podrobnosti o obsahu registru územní identifikace v § 31 až 38 zákona o základních registrech.

Nahlížet a získávat data základního registru RÚIAN a také některá data editačních agendových informačních systémů ISÚI (Informační systém územní identifikace) a ISKN (Informační systém katastru nemovitostí) umožňuje aplikace Veřejný dálkový přístup[7].

Správcem registru je Český úřad zeměměřický a katastrální, spolupracují MV, MŽP, MZe, MMR, orgány samosprávy.

3.1.4 ZÁKLADNÍ REGISTR PRÁV A POVINNOSTÍ

Jedná se o registr, jehož pomocí je realizována bezpečnost sdílených dat. Registr práv a povinností mimo jiné sleduje, jakou roli a jaké oprávnění má úřad při konkrétní agendě. Sleduje tedy působnost orgánů veřejné moci. Působnost úřadů se vždy vztahuje ke konkrétním agendám, které úřady vykonávají, a pro výkon každé agendy potřebují přístup k některým údajům v základních registrech a informačních systémech (tzv. agendových informačních systémech). Za tímto účelem jsou úřadům přiděleny role, které vymezuje právě v registru práv a povinností. Registr práv a povinností vytváří propojení mezi informací o typu oprávnění a danou rolí, čili jak může pracovat s údaji v daném základním registru nebo informačním systému (např. číst, zapisovat apod.).

Registr obsahuje přehled agend vykonávaných orgány veřejné správy, informaci o tom, který úřad konkrétní agendu vykonává, a definuje role, které jsou pro výkon agend potřebné. Rovněž obsahuje oblast práv a povinností fyzických a právnických osob. Údaje slouží registrů při řízení přístupu uživatelů k údajům v jednotlivých registrech a agendových informačních systémech. Referenční údaje vedené v registru práv a povinností nalezneme v § 50 až 52 zákona.

Správcem registru je Ministerstvo vnitra ČR, spolupracují všechny ústřední správní úřady i orgány samosprávy.

[7] http://vdp.cuzk.cz/

4 AGENDY

Každý subjekt veřejné správy zabezpečuje zpracování zákonem svěřených agend. V dnešní době se většina agend zpracovává elektronicky, avšak pro maximální zefektivnění jednotlivých procesů je třeba promyslet možné alternativy a rizika.

NEPŘEHLÉDNĚTE

Agenda je souhrn činností spočívajících ve výkonu vymezeného okruhu vzájemně souvisejících činností v rámci působnosti příslušného orgánu, v našem případě v rámci státní a veřejné správy.

Informační systémy ve veřejné správě jsou tvořeny moduly, které slouží k výkonu jednotlivých agend. Systém je tedy tvořen příslušnými agendovými informačními systémy.

NEPŘEHLÉDNĚTE

Agendový informační systém je informační systém veřejné správy, sloužící k výkonu agendy. Sdílí data se základními registry.

Agendový systém[8] by měl být modulární a konfigurovatelný tak, aby dával možnost jednoduše přidávat zpracování dalších nových agend, a současně také rychlou a nenákladnou úpravu stávajících agend (tak aby byly v souladu se změnami legislativy). Musí být jednoduše rozšiřitelný pro takový počet uživatelů, který úřad nebo celý resort aktuálně potřebuje. Musí umět zpracovávat elektronická podání, která jsou úřadu doručena systémem datových schránek a dále zpracována elektronickou spisovou službou. Agendový systém by měl být dále integrován s dalšími provozními systémy (viz kap. 6) tak, aby bylo snadné automatizovat vstupy a výstupy dat z různých interních zdrojů bez nutnosti manuálních operací "kopíruj a vlož" mezi několika otevřenými okny na monitoru. Agendové systémy by také měly umožnit vizuální konfiguraci úředních procesů tak, aby průběžné změny v procesech mohly být nastaveny oprávněnými uživateli, bez nutnosti změn softwarového kódu.

V agendovém informačním systému jsou implementovány interní služby, zabezpečující komunikaci prostřednictvím ISZR s ostatními AIS a ZR.

Agendové informační systémy mohou být z hlediska komunikace se základními registry:

- jednoagendové (výkon 1 agendy);
- integrované (výkon více agend).

V rámci OVM může být implementována tzv. integrační platforma, která může zefektivnit výměnu informací mezi jednotlivými AIS a dalšími IS úřadu v rámci OVM apod.

NEPŘEHLÉDNĚTE

Činnost je soubor úkonů, které jsou za účelem výkonu veřejné moci vykonávány orgány veřejné moci v rámci jejich agendy.

Role je souhrn oprávnění úřední osoby, která vykonává určitou činnost, k přístupu k referenčním údajům v základních registrech nebo k údajům v agendových IS.

Činnostní role je činnost s vydefinovanou rolí (oprávněním).

[8] Velké organizace: Státní správa. *Microsoft* [online]. [cit. 2013-09-03]. Dostupné z: http://www.microsoft.com/cs-cz/enterprise/verejna-sprava/statni-sprava.aspx

4.1 REGISTRACE AGENDY

Dle Zákona 111/2009 Sb., o základních registrech, je nutné každou agendu ohlásit a registrovat, a to:

- ústřední správní úřad nebo jiný správní úřad s celostátní působností ohlásí agendu ve své působnosti Ministerstvu vnitra;
- je-li správní úřad podřízen ústřednímu správnímu úřadu, ohlášení agendy ve své působnosti provede prostřednictvím příslušného ústředního správního úřadu;
- je-li agenda vykonávána orgány územních samosprávných celků v přenesené působnosti nebo jinými OVM, ohlášení agendy Ministerstvu vnitra provede věcně příslušný ústřední správní úřad nebo jiný správní úřad s celostátní působností, není-li, pak ústřední správní úřad, jehož oblasti působnosti je tato agenda nejbližší.
- je-li agenda vykonávána orgány územních samosprávných celků v rámci samostatné působnosti ohlášení agendy Ministerstvu vnitra provede ústřední správní úřad nebo jiný správní úřad s celostátní působností, jehož oblasti působnosti je tato agenda nejbližší.

Obsah ohlášení je stanoven zákonem:

- název orgánu veřejné moci, který ohlašuje agendu, a jeho identifikátor vedený v registru osob;
- název agendy, která je předmětem registrace;
- číslo a název právního předpisu a označení jeho ustanovení, na jehož základě je agenda vykonávána;
- výčet orgánů veřejné moci, které agendu vykonávají, nebo jejich souhrnné označení;
- výčet a popis činností, které mají být vykonávány v rámci agendy;
- výčet základních registrů nebo agendových informačních systémů, do kterých je pro výkon agendy nezbytné zajistit přístup k údajům v nich vedeným a o nichž byly zpřístupněny Ministerstvu vnitra informace podle jiného právního předpisu, což se nevztahuje na agendový informační systém provozovaný za účelem výkonu agendy, která je předmětem registrace;
- výčet rolí nezbytných pro výkon agendy;
- údaj o rozsahu oprávnění k přístupu k jednotlivým referenčním údajům v základních registrech určených jednotlivými rolemi;
- údaj o rozsahu oprávnění k přístupu k jednotlivým údajům v agendových informačních systémech určených jednotlivými rolemi;
- číslo a název právního předpisu a označení jeho ustanovení, na jehož základě je orgán veřejné moci, který vykonává agendu, oprávněn získávat referenční údaje ze základních registrů nebo vykonávat jejich zápis;
- číslo a název právního předpisu a označení jeho ustanovení, na jehož základě je orgán veřejné moci, který vykonává agendu, oprávněn získávat údaje z agendového informačního systému
- stanovisko správce agendového informačního systému k rozsahu oprávnění k přístupu k jednotlivým údajům v tomto agendovém informačním systému;
- údaj o tom, zda ohlašovatel agendy požaduje, aby jemu nebo správci agendového informačního systému byly zaslány ke stanovisku oznámení o vykonávání působnosti v agendě, na jejichž základě má dojít k registraci pro výkon agendy, ve stanovisku se ohlašovatel agendy nebo orgán veřejné moci, který je správcem agendového informačního systému, vyjadřuje k oprávněnosti požadavku na přístup k údajům;

- formuláře v elektronické podobě pro podání a jiné úkony, nevylučuje-li právní předpis stanovící náležitosti výkonu agendy použití formulářů v elektronické nebo listinné podobě nebo nepožaduje-li právní předpis stanovící náležitosti výkonu agendy použití zvláštního formuláře, který není možno bez omezení tisknout, zpřístupnit či distribuovat, anebo není-li použití formulářů v elektronické nebo listinné podobě s ohledem na povahu úkonu v agendě účelné; formuláře se předloží ve formátu umožňujícím jejich zaslání datovou schránkou a jejich automatizované zpracování.

Orgán veřejné moci oznámí Ministerstvu vnitra vykonávání působnosti v agendě do 30 dnů ode dne registrace agendy, pokud

- je editorem referenčních údajů,
- požaduje získávání údajů ze základních registrů,
- požaduje získávání údajů z agendových IS jiných správců.

Toto oznámení obsahuje:

- název orgánu veřejné moci, který žádá o registraci pro výkon agendy, a jeho identifikátor vedený v registru osob;
- kód agendy podle číselníku agend;
- označení rolí určených pro danou agendu, které OVM pro výkon agendy požaduje přiřadit, a počet úředních osob, které budou roli zastávat.

4.2 OSOBY A JEJICH IDENTIFIKACE

NEPŘEHLÉDNĚTE

Správce agendového IS zajišťuje realizaci vazby mezi agendovým IS a IS základních registrů za účelem zapisování údajů.

Zajistí používání kódu agendy přiděleného správcem základního registru práv a povinností při komunikaci agendového IS s IS základních registrů. Používá vlastní identifikátory fyzických osob a právnických osob a za účelem komunikace s IS základních registrů používá agendové identifikátory fyzických osob a identifikátory právnických osob vedené v registru osob

Pro zabránění neoprávněnému přístupu k osobním údajům se používají identifikátory:

- kód agendy - veřejný identifikátor, který je jednoznačně přiřazen záznamu o agendě v číselníku agend v registru práv a povinností;
- agendový identifikátor fyzické osoby.

Agendový identifikátor fyzické osoby (AIFO) je neveřejným identifikátor, který je jednoznačně přiřazen záznamu o fyzické osobě v příslušném agendovém IS nebo základním registru. Je odvozen ze zdrojového identifikátoru fyzické osoby a kódu agendy. Využívá se výlučně k jednoznačnému určení fyzické osoby pro účely výkonu agendy, pro kterou byl přidělen. Z AIFO nelze odvodit zdrojový identifikátor fyzické osoby a nelze z něj ani dovodit osobní nebo jiné údaje o fyzické osobě, jíž byl přiřazen.

Zdrojový identifikátor fyzické osoby (ZIFO) je neveřejný identifikátor. Nelze z něho dovodit osobní ani jiné údaje o fyzické osobě, jíž byl přiřazen.

AIFO v jednotlivé agendě odvozený z jednoho zdrojového identifikátoru fyzické osoby nesmí být přidělen více fyzickým osobám a nelze ho po přidělení měnit, pokud zákon nestanoví jinak. Pokud dojde k přidělení stejného AIFO v dané agendě záznamům o dvou

nebo více fyzických osobách, je těmto záznamům přidělen nový AIFO. Pokud dojde k přidělení dvou nebo více AIFO záznamu o jedné fyzické osobě v dané agendě, postupuje se obdobně.

Zjistí-li orgán veřejné moci (OVM) nedostatky v přidělení AIFO, oznámí tuto skutečnost bez zbytečného odkladu správci agendového IS, v němž byl nedostatek zjištěn, příslušný správce agendového IS prošetří, zda lze zjištěné nedostatky odstranit v agendovém IS, a pokud je to možné, nedostatky odstraní. Zjistí-li správce agendového IS nedostatky v přidělení AIFO, které nelze odstranit, oznámí tuto skutečnost bez zbytečného odkladu správci registru obyvatel a ten ve spolupráci se správcem agendového IS prošetří, zda lze zjištěné nedostatky odstranit, a pokud je to možné, nedostatky odstraní.

Úřad pro ochranu osobních údajů vytváří a AIFO a zajišťuje převod AIFO v agendě na AIFO této fyzické osoby v jiné agendě, a to na základě zákonného požadavku.

4.3 AGENDY ORGÁNŮ VEŘEJNÉ MOCI

Co je nutné u každé agendy stanovit (referenční údaje v registru práv a povinností):

- název agendy a její číselný kód, které jsou součástí číselníku agend;
- právního předpis a označení jeho ustanovení, který působnost stanovuje;
- výčet a popis činností, které mají být vykonávány v agendě;
- výčet OVM, které agendu vykonávají, nebo jejich souhrnné označení;
- název ústředního správního úřadu nebo jiného správního úřadu s celostátní působností, jehož agenda byla registrována, a identifikátor tohoto orgánu;
- výčet OVM, které byly pro výkon agendy registrovány, a identifikátor příslušného orgánu;
- výčet základních registrů nebo agendových IS, do kterých je pro výkon agendy nezbytné zajistit přístup k údajům v nich vedeným;
- výčet rolí nezbytných pro výkon agendy;
- údaj o rozsahu oprávnění k přístupu k jednotlivým referenčním údajům v základních registrech;
- rozsah oprávnění k přístupu k jednotlivým údajům v agendových IS;
- číslo a název právního předpisu a označení jeho ustanovení, na jehož základě je OVM oprávněn k přístupu k údajům vedeným v základním registru nebo v agendovém IS jiného správce.

OVM žádá o umožnění přístupu k referenčním údajům tak, že žádá správu ZR o vydání elektronického certifikátu, a to pro každý AIS zvlášť. Každý AIS připojený k IS ZR, je jednoznačně identifikován údaji:

- IČ úřadu - identifikační číslo OVM, který je správcem AIS;
- AIS_ID - identifikátor AIS podle IS o ISVS;
- SN - číslo certifikátu (SerialNumber);
- seznam agend - seznam agend v AIS obsažených.

Agendové IS můžeme rozdělit na:

- centrální, které umožňují sdílený přístup, který je většinou realizován formou portálového řešení;
- lokální, které OVM používají pro podporu výkonu svých agend a které mohou být poskytnuty pro podporu výkonu činností v agendách zřizovaných a příspěvkových organizací.

Jednotlivé AIS pracují především se svými lokálními daty. V systému základních registrů jsou uloženy referenční údaje. Lokální data představují hodnoty údajů, jejichž referenční hodnoty jsou vedeny v ZR. Pojem se nevztahuje na ostatní data AIS. AIS provádí pravidelně aktualizaci lokálních údajů, tím zajistí, že stav lokálních dat v AIS odpovídá stavu referenčních údajů k datu a času poslední aktualizace. AIS aktualizuje pouze data, která eviduje a která pro svoji činnost využívá. Online dotazy do registrů používá AIS pouze v případech, kdy je to nezbytné.

Funkce agendových systémů můžeme rozčlenit[9] na:

- **editační**, které slouží pro přístup editorů k referenčním údajům v příslušném registru, editačními funkcemi jsou zápis, změna a likvidace záznamů;
- **informační**, které sloužící pro přístup k referenčním údajům, uloženým v registru, informačními funkcemi registru jsou čtení údajů, poskytnutí změn referenčních údajů, hromadný výdej údajů, autentizace fyzické osoby podle elektronického identifikačního dokladu a výdej informací o využití dat v registru;
- **správní**, které jsou určeny pro správce registru, jsou jimi znepřístupnění výdeje, zrušení znepřístupnění výdeje a čtení informace o znepřístupnění výdeje informací o využití referenčních údajů., výdej editora údaje, zveřejňování závazných číselníků, výdej statistik registru obyvatel, likvidace záznamů v registru obyvatel podle skartačních pravidel, zápis provozních a auditních údajů a kontroly konzistence datových údajů.

Každý referenční údaj má svého editora. Editorem je OVM, který má v rámci některé agendy činnostní roli editora referenčního údaje. Editační agendové IS můžeme rozdělit na:

- **primární editační AIS**, které vytváří nebo ruší v základním registru celé záznamy, např. pro ROB IS evidence obyvatel (ISEO) a cizinecký IS (CIS).
- **sekundární editační AIS**, které mohou v již existujícím záznamu v základním registru měnit pouze některé referenční údaje, např. pro ROB IS občanských průkazů (ISOP), IS cestovních dokladů (ISCD) a IS datových schránek (IS DS).

Integrovaný agendový IS (IAIS ROS), jehož správcem je Český statistický úřad, je určen pro ty, kteří nepřistupují k vnějšímu rozhraní ROS IS ZR přímo. Má přímé připojení na základní registry a je sdílený pro více agend a agendových míst. Umožňuje paralelní a nezávislý provoz více agend v rámci jedné centrální instance systému a komunikuje se všemi relevantními službami základních registrů.

Pokud to bude třeba i pro celkové vedení agendy. Umožní totiž evidenci jakýchkoliv údajů o osobách podle specifických požadavků příslušného uživatele. IAIS ROS bude dále zaznamenávat historii změn o jednotlivých osobách a jeho součástí budou také sdílená data (např. lokální obraz RUIAN, nebo sdílené číselníky obecného či technologického charakteru).

Tzv. čtenářský agendový IS využívá „publikační“ služby. Může mít přímý přístup k vnějšímu rozhraní IS ZR.

Existují agendy, ve kterých mají OVM (obce) působnost, ale k základním registrům v rámci těchto agend přistupovat nemohou, a to ani v roli čtenáře.

[9] SPRÁVA ZÁKLADNÍCH REGISTRŮ. *Globální architektura ROB verze 1.0 - Příloha č. 1b zadávací dokumentace.* [online] Praha: Správa základních registrů, 2010 [cit. 25. 5. 2012]. Dostupné z: http://www.szrcr.cz/file/8/

4.4 PŘÍKLADY AGENDOVÝCH IS

Škála partnerských registrů je široká. Spravovat je mohou různé orgány veřejné správy nebo jimi pověřené organizace. Zde si uvedeme alespoň některé.

4.4.1 REGISTR ŽIVNOSTENSKÉHO PODNIKÁNÍ

Registr živnostenského podnikání byl vytvořen jako centrální systém v garanci Ministerstva průmyslu a obchodu ČR vykonávající působnost Živnostenského úřadu České republiky. Umožňuje zabezpečování procedurálních záležitostí souvisejících s vydáváním živnostenských oprávnění, vedením správního řízení a kontrolní činností pro subjekty podnikající v režimu živnostenského zákona.

Registr obsahuje řadu vazeb do jiných registrů provozovaných orgány veřejné správy, které přímo vyplývají z konkrétních ustanovení živnostenského zákona, nebo z obecně platných zásad výkonu státní správy.

Jedná se o předávání kopií dokumentů, přebírání údajů z jiných registrů VS, ověřování správnosti údajů při výkonu státní správy a vyžádání dokladu. Většina vazeb je realizována formou elektronické komunikace a výměny dat a to on-line nebo dávkami předávanými v pravidelných intervalech.

Do registru jsou údaje přebírány ze systémů Obchodního rejstříku, Českého statistického úřadu a Územně identifikačního systému.

Registr mimo jiné obsahuje

- jméno a příjmení,
- občanství
- bydliště,
- místo podnikání
- identifikační číslo,
- živnostenská oprávnění:
    - předmět podnikání
    - obory činnosti
    - druh živnosti
    - vznik oprávnění
    - zahájení provozování živnosti
    - doba platnosti oprávnění
- provozovny k předmětu podnikání číslo
- atd.

4.4.2 CENTRÁLNÍ REGISTR SILNIČNÍCH VOZIDEL

Ministerstvo vede centrální registr silničních vozidel, který obsahuje údaje předávané obecními úřady obcí s rozšířenou působností a registr silničních vozidel členů diplomatické mise. Ministerstvo zajišťuje pro Policii České republiky výdej informací z centrálního registru vozidel způsobem umožňujícím dálkový a nepřetržitý přístup.

Centrální registr silničních vozidel v souladu se zákonem je veden Ministerstvem dopravy. Z pověření Ministerstva dopravy provozuje centrální registr silničních vozidel Odbor centrálních informačních systémů MV, který vydává údaje z tohoto registru a provádí porovnání dat pro Českou kancelář pojistitelů.

Jsou zde obsaženy nejen údaje předávané obecními úřady obcí s rozšířenou působností, ale je zde veden i registr silničních vozidel členů diplomatické mise. S těmito údaji poté pracuje nejen samo ministerstvo, které tyto údaje využívá ke svým účelům, ale údaje jsou využívány i ve vztahu k příslušným orgánům členských států a jsou zpřístupněny nepřetržitě formou dálkového přístupu Policii ČR.

V registru jsou obsaženy především údaje:

- provozovatel vozidla,
- poznávací značka,
- tovární značka, typ a druh vozidla,
- ostatní základní technické údaje o vozidle,
- datum zápisu do registru vozidel,
- datum výmazu z registru vozidel.

Vojenská policie eviduje vozidla ozbrojených sil v registru vozidel. Tento registr vozidel není veřejně přístupný a zapisují se do něj tyto údaje.

4.4.3 CENTRÁLNÍ REGISTR ŘIDIČŮ

Evidence údajů o řidičích, shromažďovaných z registru řidičů, je vedena v centrálním registru řidičů, který je informačním systémem, jehož správcem je ministerstvo dopravy, evidence údajů o řidičích je vedena v registru řidičů prostřednictvím pověřených úřadů. Registr řidičů obsahuje:

- osobní údaje o řidiči
- evidenci
    - vydaných řidičských průkazů,
    - skupin a podskupin udělených řidičských oprávnění, mezinárodních řidičských průkazů,
    - řidičských průkazů vydaných výměnou za řidičský průkaz vydaný cizím státem nebo řidičský průkaz Evropských společenství,
    - odevzdaných řidičských průkazů a mezinárodních řidičských průkazů,
    - ztracených, odcizených, poškozených a zničených řidičských průkazů a mezinárodních řidičských průkazů,
- evidenci spáchaných přestupků,
- záznamy o počtu bodů dosažených řidičem v bodovém hodnocení a záznamy o odečtu bodů,
- údaje o odnětí řidičských oprávnění,
- údaje o zákazech činnosti,
- atd.

4.4.4 REGISTR EKONOMICKÝCH SUBJEKTŮ

Registr ekonomických subjektů je veřejným seznamem, který je veden podle zákona o státní statistické službě Českým statistickým úřadem. Zápis do registru má pouze evidenční význam.

Registr má strukturu:

- identifikační číslo
- datum vzniku
- datum zániku
- způsob zániku

- datum aktualizace
- právní forma
- převažující činnost
- kategorie dle počtu pracovníků
- identifikační číslo základní územní jednotky sídla organizace
- firma, název
- zkrácený obchodní název
- adresa sídla: PSČ, obec, část obce, ulice a číslo domu.

4.4.5 REGISTR LÉKŮ

Registr slouží k identifikaci léčivých přípravků a jsou v něm léčivé přípravky, které prošly procesem schvalování, tzv. registrace.

V registru jsou:

- indikační skupina,
- přírůstkové číslo rozhodnutí o registraci v daném kalendářním roce, ve kterém bylo rozhodnutí o registraci vydáno
- označení kalendářního roku, ve kterém bylo rozhodnutí o registraci vydáno,
- vyjádření, zda se jedná o humánní či veterinární přípravek nebo jiný,
- číslo varianty přípravku
- atd.

4.4.6 INTEGROVANÝ REGISTR ZNEČIŠŤOVÁNÍ ŽIVOTNÍHO PROSTŘEDÍ

Integrovaný registr znečišťování životního prostředí je zřízen a spravován Ministerstvem životního prostředí jako veřejný informační systém veřejné správy. Provozovatelem je CENIA, česká informační agentura životního prostředí.

Registr je databází údajů o:

- únicích vybraných znečišťujících látek (do ovzduší, vody, půdy),
- přenosech znečišťujících látek v odpadech a odpadních vodách.
- přenosech množství odpadů, které jsou každoročně ohlašovány za jednotlivé provozovny na základě splnění kritérií stanovených příslušnými právními předpisy.

Registr obsahuje údaje o:

- uživateli ohlašované látky,
- provozovně,
- emisích látek,
- přenosech látek
- atd.

4.5 PŘÍKLADY OSTATNÍCH REGISTRŮ

4.5.1 REGISTR ADVOKÁTŮ

Registr advokátů shromažďuje všechny renomované advokáty v dané zemi. Výhodou tohoto rejstříku je evidence počtu případných kárných žalob k danému advokátovi nebo významné úspěchy daného právníka či právní kanceláře. Dodatečné služby zajišťuje Centrální registr dlužníků z veřejně dostupných zdrojů. Tím se tento registr stává prestižní záležitostí pro dobré advokáty.

4.5.2 REGISTR EXEKUTORŮ

Registr exekutorů shromažďuje všechny renomované exekutory v dané zemi. Výhodou tohoto rejstříku je evidence počtu případných kárných žalob u exekutorské komory, nebo významné úspěchy daného exekutora či exekutorské kanceláře. Dodatečné služby zajišťuje Centrální registr dlužníků z veřejně dostupných zdrojů. Tím se tento registr stává prestižní záležitostí pro dobré exekutory.

4.5.3 CENTRÁLNÍ REGISTR PRODUKTŮ A FIREM

Centrální registr produktů a firem provozuje Hospodářská komora ČR. Poskytuje služby v oblasti navazování nových obchodních kontaktů a prostor pro výměnu informací mezi firmami.

Obsahuje:

- popis předmětu činnosti,
- adresu firmy a další kontakty,
- všeobecné informace:
    - právní forma,
    - rok založení,
    - registrační číslo,
    - certifikáty kvality:
    - členství v asociacích, oborových svazech apod.:
    - auditor,
    - bankovní spojení,
    - jazyky pro komunikaci
- vedení firmy:
- výrobky, služby, činnosti, obchodní značky
- ekonomické údaje za poslední rok
- atd.

4.6 PŘÍKLADY ZVLÁŠTNÍCH REGISTRŮ

4.6.1 CENTRÁLNÍ REGISTR ZBRANÍ A MUNICE

V AČR je od r. 1995 zaveden Centrální registr zbraní a munice (CRZM), který eviduje zbraně podle výrobních čísel ve smyslu Směrnice pro vedení registrů střelných zbraní

a munice v rozpočtovém úseku resortu obrany (č.j. 20/2-280-OM z r. 1998). CRZM vede přehled i o ztracených, zničených, odprodaných a zlikvidovaných (fyzicky zrušených) zbraních. V centrálním registru lze dále zjistit pohyby prováděné s danou zbraní a kde se zbraň nachází. Vojenský centrální registr zbraní a munice není veřejně přístupný.

4.7 EVIDENČNÍ A SPRÁVNÍ AGENDY

Evidenční a správní agenty představují širokou škálu modulů. Celkem ucelený přehled poskytuje nabídka informačního systému Munis[10], ze které budeme v následujícím textu vycházet.

4.7.1 ELEKTRONICKÁ PODATELNA A ELEKTRONICKÝ PODPIS

Elektronická podatelna je vlastně emailový klient. Musí zohledňovat zákonné podmínky pro provoz elektronické podatelny. Elektronická podatelna umožňuje číst došlá elektronická podání z libovolné schránky elektronické pošty prostřednictvím protokolů definovaných příslušnými standardy. Elektronická podatelna umožňuje přijímat elektronická podání pomocí e-mailu nebo technického nosiče podle Zákona o elektronickém podpisu a vyhovuje standardu ISVS pro provoz elektronických podatelen.

V kombinaci s dalšími moduly jsou veškerá doručená elektronická podání jednotně spravována s ostatními podáními přijatými úřadem.

Elektronická podatelna zajišťuje funkce předepsané standardem ISVS:

- stahování zpráv protokolem POP3 a odesílání zpráv protokolem SMTP,
- přijímání podání na technickém nosiči,
- zařazení přijatých zpráv do archívu přijaté pošty,
- zapsání podání do evidence doručených podání,
- bezpečnostní kontrola obsahu zprávy (antivirová ochrana)
- test akceptovatelnosti příloh v podání podatelnou,
- ověření elektronického podpisu a platnosti certifikátu.

V případě, že je podání po všech stránkách korektní, je možné jej přijmout do podatelny. Při přijetí jsou využity informace o předkladateli podání, které jsou uvedeny v jeho certifikátu (např. jméno a adresa). Tyto informace jsou zapsány do adresáře a mohou být použity při další komunikaci.

V případě přijetí nebo odmítnutí podání do podatelny je vygenerována zpráva, která je předkladateli podání elektronicky doručena. Tato zpráva může obsahovat automaticky vložené popisné informace o přijatém podání atd. Jakmile je doručené elektronické podání přijato do podatelny, je s ním nakládáno jako s jakýmkoliv jiným podáním.

Zaručený elektronický podpis (dle zákona o elektronickém podpisu) musí být elektronickou podatelnou využíván. Při přijetí podepsaného podání je provedena kontrola podpisu, zobrazení certifikátu a ověření jeho platnosti. Pro ověřování certifikátů je potřeba funkční připojení k internetu. Pro uložení certifikátů pověřených pracovníků je možné využívat i čipové karty.

4.7.2 EVIDENCE ČÍSEL POPISNÝCH

Modul evidence čísel popisných slouží k evidenci budov a dalších souvisejících údajů jako jsou údaje o parcele, technické údaje, byty, nebytové prostory. Dále je možná evidence rozhodnutí stavebního úřadu (datum, typ, název, číslo jednací, právní moc), např. stavební povolení nebo kolaudační rozhodnutí atd.

Modul by měl umožňovat přebírání adres z celostátního registru územní identifikace. Je nutné rovněž využívat údaje o občanech z evidence obyvatel.

[10] http://www.munis.cz/

Při řešení problémů je možné použít různé přístupy. Jednou z možností je, že zvolíme za základní evidovaný datový element budovu, která je charakterizována zejména svým číslem (popisným, evidenčním nebo náhradním). Dalšími atributy jsou parcela, část obce, ulice (i více než jedna, např. rohové budovy), katastr, charakter přidělení čísla, druh (rodinný, bytový, garáž) a status (obydlený, neužívaný, demolice objektu) apod.

Dále je možné evidovat technické údaje o budově jako druh svislé konstrukce (panel, cihla), způsob odkanalizování, zdroj vody, topné médium, vytápění, vybavení (kotelna, kryt CO, výtah).

Každá budova může mít několik podlaží, na každém podlaží mohou být byty, u každého bytu je možné evidovat kromě standardních atributů jako je číslo, typ bytu a výměra i libovolný počet dalších atributů např. balkony, lodžie apod.

U nebytových prostor je možné evidovat typ (prádelna, sušárna, kanceláře) a druh (vestavěné v domě, přistavěné k domu) a jejich počet.

Budova může mít několik vlastníků, každý vlastník by se měl zadávat pouze jednou.

4.7.3 EVIDENCE OBYVATEL

Evidence obyvatel umožňuje kompletní možnosti sledování řady údajů o občanovi s trvalým bydlištěm v dané obci, tzv. živá kartotéka. Na základě prováděných změn vzniká tzv. mrtvá kartotéka, kde jsou uchovávány veškeré události, týkající se občanů vedených v agendě.

Musí umožňovat vytváření přehledů o pohybu obyvatelstva v obci během stanoveného časového období, např. počty narozených a zemřelých lidí, stěhování v rámci obce i stěhování za hranice katastru. Měl by umožňovat statistické funkce, např. počty obyvatel v jednotlivých částech obce, sledování věkového složení obyvatel včetně možnosti grafické interpretace, rodinné vztahy, přehled jubilantů apod.

Aplikace by měla umožňovat provádění aktualizace údajů z dat centrálních orgánů.

Do této agendy patří modul ohlašovna, který provádí přihlašování občanů k trvalému pobytu. Zařazení občané se stávají součástí evidence obyvatel. I zde by měla být možnost předávání dat ohlašovny do celostátní evidence obyvatel elektronickou cestou.

Z volebního zákona vyplývá pro obce a města povinnost vést stálý a zvláštní seznam voličů a v některých případech dodatek ke stálému seznamu voličů. Zpracování volebních seznamů tedy souvisí a evidenci obyvatel. Systém vy měl vycházet z jednotném registru adres, kde každá adresa si nese informaci o přiřazení do volebního i doručovacího okrsku. Při stěhování občanů v rámci obce potom občan spadá do volebního okrsku podle adresy, na které je momentálně trvale hlášen a není potřeba se jeho přiřazováním již dále zabývat. Máme různé typy voleb, např. v jednom termínu se konají volby do různých orgánů (na základě různé legislativy). Proto program musí podporovat vytváření různých volebních seznamů.

Ověřování údajů z registru obyvatel a adresních bodů obce lze využívat v dalších modulech. Vyhledávání by mělo být možné např. podle příjmení, rodného čísla nebo podle adresy apod. Všechna vyhledávání z registru obyvatel by měla být striktně omezena na zadání celých podmínek, aby je nebylo možné využít k jiným účelům než ověřování jednotlivých záznamů z registru. Při ověření údajů se jedná pouze o zobrazení dat, jde o bezpečný přístup k datům.

Díky vazbě na celostátní registr územní identifikace, který vytváří a průběžně aktualizuje Ministerstvo práce a sociálních věcí, lze jednoduše provázat evidenci obyvatel např. s geografickým informačním systémem apod.

4.7.4 EVIDENCE OZNÁMENÍ (ZÁKON O STŘETU ZÁJMŮ)

Tato agenda umožňuje provádět všechny činnosti zahrnuté do pojmu vedení registru oznámení podle zákona č. 159/2006 Sb., o střetu zájmů. Z jednotlivých oznámení vzniká registr oznámení, jehož vedením jsou pro oblast oznámení veřejných funkcionářů obcí a měst pověřeni tajemníci, případně starostové.

Mezi základní funkce programu patří:

- přijímání a evidence oznámení ve smyslu zákona (na 5 let od skončení výkonu funkce),
- uchovávání žádostí o nahlížení do registru, vedení protokolu o nahlížení do registru,
- přijímání sdělení o nepravdivosti nebo neúplnosti údajů v oznámeních,
- ověřování žádostí a přidělování uživatelského jména a přístupového hesla k nahlížení do registru v elektronické podobě na centrální adrese prostřednictvím veřejné datové sítě,
- zabezpečené zpřístupnění registru prostřednictvím portálu iMunis.cz.

4.7.5 EVIDENCE ŽÁDOSTÍ O OP

Mezi základní funkce tohoto programu patří:

- evidence žádostí o vydání občanských průkazů,
- rozlišení stavů žádosti (přijato, odesláno, připraveno, předáno),
- rychlé vyplňování formulářů za pomoci číselníků (důvody změny OP,…)
- přesný tisk do formuláře žádosti o vydání občanských průkazů,
- evidence vydaných občanských průkazů,
- statistické přehledy.

4.7.6 KANCELÁŘSKÝ SYSTÉM – SPISOVÁ SLUŽBA

Program Kancelářský systém -- spisová služba je výkonný nástroj pro vedení spisové agendy organizací veřejné správy v souladu se zákonem č. 499/2004 Sb., o archivnictví a spisové službě a vyhláškou č. 646/2004 Sb., o podrobnostech výkonu spisové služby. Program řeší tyto základní okruhy činností:

Schéma elektronické spisové služby:

- vazba na datové schránky;
- adresář subjektů;
- podatelna, evidence a třídění došlé pošty;
- elektronická podatelna;
- oběh dokumentů;
- kategorizace dokumentů;
- vyřizování, ukládání a tvorba spisů;
- korespondence a texty;
- elektronické podepisování;
- vypravování zásilek;
- vazba na Czech POINT;
- podpora frankovacích strojů;
- evidence úkolů a diář;
- sekretariát;
- plánování jízd služebních vozidel;
- kniha jízd;
- správní řízení;
- vazba na datové schránky.

4.7.7 KATASTR NEMOVITOSTÍ

Program slouží k prohlížení dat poskytovaných katastrálním úřadem. Zobrazuje všechny objekty včetně jejich vztahů (parcely, sousední parcely, budovy, oprávněné subjekty, jednotky) a poskytuje přehledy a tiskové sestavy. Umožňuje s daty provádět standardní databázové operace (třídění podle různých kritérií, možnost výběru dat pomocí libovolných výběrových podmínek, tisky a exporty dat atd.). Ke každé parcele v seznamu je okamžitě možno zjistit všechny její vlastníky a naopak ke každému vlastníkovi je možné okamžitě zjistit seznam parcel, které v katastru obce vlastní. Připojování vlastních poznámek k jednotlivým pozemkům lze využít například k evidenci nájemních smluv na pozemky ve vlastnictví obce, doplnění chybných údajů v evidenci a podobně. V případě, že data předaná katastrálním úřadem obsahují i grafické informace, program nabízí i nalezení sousedních parcel a vykreslení parcely s nejbližším okolím.

4.7.8 LEGALIZACE A VIDIMACE

Program slouží k tisku "ověřovacího razítka" na štítky. Zahrnuje legalizaci (ověřování pravosti podpisu) a vidimaci (ověřování shody opisů nebo kopie s listinou). Ruční provádění legalizace a vidimace znamená několikanásobné ruční psaní stejných údajů. Platná legislativa však umožňuje využití výpočetní techniky pro zjednodušení a urychlení předepsaného postupu. Otisk ověřovacího razítka lze nahradit vytištěným štítkem se stejnými údaji, pokud se při tom dodrží následující pravidla:

- obsahuje všechny povinné údaje jako na otisku ověřovacího razítka,
- přes jeden roh nalepeného štítku se umístí otisk kulatého razítka,
- přidá se vlastnoruční podpis odpovědného pracovníka.

4.7.9 MATRIKA

Modul řeší všechny náležitosti vedení matričních agend na počítači ve smyslu zákona 301/2000 Sb. o matrikách, jménu a příjmení, související vyhlášky Ministerstva vnitra č. 207/2001 Sb. a směrnice k jednotnému postupu matričních úřadů při souběžném vedení matričních knih pomocí výpočetní techniky. Program umožňuje vedení všech třech matričních knih (narození, manželství a úmrtí), do kterých se zadávají všechny zákonem stanovené druhy zápisů (matriční události, matriční skutečnosti a změny a opravy zápisů). Lze vést souběžně více než jeden svazek pro jeden druh matriční knihy.

Program umožňuje tisk matričního listu nebo jeho části, potvrzení o údajích zapsaných ve svazku matriční knihy, doslovného výpisu v rozsahu uvedeném ve svazku matriční knihy rukopisně vedené a tisk dalších formulářů, jako je protokol o uzavření manželství, osvědčení k uzavření církevního sňatku, abecední jmenný rejstřík apod.

4.7.10 POHLEDÁVKY

Program umožňuje vymáhat pohledávky podle zákona o správě daní a poplatků. Umožňuje také sledovat stav a termíny v soudních sporech týkajících se vymáhání pohledávek. V obou případech následně pomáhá při výkonu rozhodnutí. Umožňuje:

- sledování průběhu soudního řízení od podání žaloby soudu, přes jednání, rozhodnutí, odvolání, nabytí právní moci soudního rozhodnutí, až po výkon rozhodnutí;
- vedení řízení podle zákona o správě daní a poplatků;

- sledování vymáhaných částek, soudních poplatků a dalších nákladů s případem spojených, výpočet vymáhaných částek včetně příslušenství;
- hlídání termínů pomocí kalendáře, ve kterém jsou chronologicky zaznamenány jednotlivé termíny;
- automatizované generování dokumentů s možností následné editace;
- postupné vytváření archivu údajů o případech včetně dokumentů;
- využití údajů z registru obyvatel, ekonomických subjektů.

4.7.11 PŘESTUPKY

Program umožňuje zpracovávat přestupky a jiné správní delikty, tisknout předvolání, rozhodnutí, dožádání, podklady pro roční výkaz MVČR apod. Obsahuje funkce:

- nabídka přestupků a jiných správních deliktů podle legislativního stavu k určitému datu (obvykle datu spáchání);
- postoupení, odložení věci, zastavení řízení;
- vedení přestupkového, příkazního či blokového řízení;
- vedení řízení o správním deliktu;
- odvolací řízení, obnova řízení, přezkumné řízení, elektronická komunikace mezi prvoinstančním a odvolacím orgánem;
- sledování termínů pomocí kalendáře úkolů;
- evidence spisů v elektronické podobě;
- přestupky proti majetku, veřejnému soužití, dopravní přestupky, přestupky proti stavebnímu řádu atd.;
- evidence podezřelých, obviněných, svědků, navrhovatelů atd.;
- tisk adres, složenek;
- automatizované generování dokumentů ze zadaných údajů do textového editoru s možností následné editace;
- využití údajů z registru obyvatel, ekonomických subjektů;
- postupné vytváření archivu údajů včetně dokumentů;
- využití údajů z registru obyvatel, ekonomických subjektů;
- vedení podacího deníku a možnost propojení se spisovou službou.

4.7.12 SILNIČNÍ ÚŘAD

Program slouží pro podporu činnosti silničního správního úřadu -- speciálního stavebního úřadu a zvláštního užívání komunikací. Pro speciální stavební úřad poskytuje všechny funkce jako stavební úřad, pro zvláštní užívání komunikací je rozšířen o další typy řízení. Základní funkce jsou následující:

- průběh řízení dle zákona o pozemních komunikacích, stavebního zákona a předpisů souvisejících;
- odvolací řízení, obnova řízení, mimo odvolací řízení, elektronická komunikace mezi prvoinstančním a odvolacím orgánem;
- sledování termínů pomocí kalendáře úkolů;
- aktuální informace o účastnících, dotčených orgánech a ostatních;
- automatizované generování dokumentů ze zadaných údajů do textového editoru s možností následné editace;
- postupné vytváření archivu údajů včetně dokumentů;
- využití údajů z registru obyvatel, ekonomických subjektů;
- využití údajů z územně identifikačního registru, registru nemovitostí;
- tisk adres v řízení nebo posílání tisku sekretářce.

4.7.13 SOCIÁLNÍ DÁVKY

Modul Sociální dávky slouží k vedení agendy související s poskytováním sociálních dávek na úrovni obcí a krajských úřadů. Program umožňuje evidenci žadatelů o sociální dávku, tvorbu, přijetí a další opravy žádostí. V žádosti je možné zaznamenat informace o osobách žijících ve společné domácnosti, případně dalších rodinných příslušnících žijících mimo společnou domácnost, údaje o příjmech žadatele i dalších společně posuzovaných osobách, majetkové či bytové poměry žadatele a další uživatelem definované údaje.

Při tvorbě rozhodnutí program navrhne položky životního minima, umožní zadat další posuzované náklady (např. skutečné náklady na domácnost) a vypočítá sociální potřebnost. Ke každému rozhodnutí, které přiznává dávku, je možné nadefinovat výši a způsob výplat (materiálních i peněžitých).

Na základě rozhodnutí o přiznání dávky je možné vytvářet výplaty. Systém hlídá, aby některá výplata nebyla vytvořena vícekrát a naopak umožňuje vyhledání rozhodnutí, na základě kterých ještě nebyla pro daný měsíc vytvořena přiznaná výplata. Pro výplaty složenkou je možné v prostředí programu vytvořit datový soubor pro předání České poště.

Modul umožňuje přebírání adres z celostátního registru územní identifikace UIR-ADR (přes modul Správa adres). Je možné načtení údajů o občanech vedených v modulu Evidence obyvatel.

4.7.14 SPRÁVA DOMŮ A BYTŮ

Zahrnuje komplexní systém pro správu domů s libovolnými typy prostor -- nájemní byty, vlastnické byty, nebytové prostory, garáže, družstevní byty a podobně s možností propojení na okolní systémy (účetnictví, centrální evidence atd.). Základními vlastnostmi sytému jsou zejména:

- základní "technická" evidence domů/pasporty (byty, nebytové prostory,…), místností a ploch, zařízení, konstrukčních prvků, slevy apod.;
- rozšířená evidence libovolných dokumentů: výkresy domu, prostoru, fotografie domu nebo uživatele, kopie podepsané smlouvy, tabulky Excelu, dokumenty Wordu nebo jakýkoliv jiný dokument;
- evidence libovolných poznámek domu, prostoru, uživatele (typy záznamů jsou volitelné);
- evidence uživatelů (nájemníků/vlastníků/družstevníků), majitelů domů atd.;
- evidence pro nájemné dle zákona č. 107/2006 Sb.;
- daňová evidence pro DPH ze zaplacených záloh dle zákona o DPH;
- evidence a možnost tvorby libovolného počtu předpisů s libovolným typem úhrady a s libovolným počtem položek předpisu
- evidence upomínek;
- evidence sporů (žaloby, napomenutí, vyloučení,…) a jejich průběhu (veškeré termíny, náklady na spory atd.);
- evidence fondů, kaucí,…
- evidence libovolných dalších jednotek prostoru, uživatele (dle uživatelsky definovaných jednotek pak lze provést vyúčtování);
- sledování uživatelsky definovaných revizí domu, prostoru;
- správa měřidel a odečtů poměrových měřidel SV, TUV a tepla, elektřiny (odečtové karty, směrná čísla atd.);
- sledování a vyhodnocování požadavků a objednávek, plánování nákladů, evidence a vyhodnocení nákladů ve zvolené skladbě a třídění;
- variabilně volitelné vyúčtování nákladů (libovolný počet vyúčtování;
- uživatelsky tvořené předlohy výpisů (smlouvy, upomínky, výpočtové listy, potvrzení a podobně;

- systém automatického upozorňování na termíny (konec smlouvy, plánovaná revize, apod.;
- automatické rozesílání výkazů mailem.

4.7.15 •SPRÁVNÍ ŘÍZENÍ

Modul podporuje agendu správního řízení, zejména:

- přidání k evidenci spisu evidenci všech účastníků řízení
- doplnění evidenci spisu o další parametry, jejichž název a obsah je pro dané řízení typický;
- příprava vzorových dokumentů, které v rámci jednotlivých řízení vznikají;
- nastavení stavu řízení a přesné sledování termínů.

4.7.16 STAVEBNÍ ÚŘAD

Program podporuje provádění činností, které se řídí stavebním zákonem a předpisy souvisejícími. Umožňuje vést všechny typy správních řízení, které na stavebním úřadě přicházejí v úvahu. Podporuje i činnosti odvolacího orgánu. Základní jeho funkce jsou:

- evidence správních řízení -- územní, stavební, kolaudační a další, evidence ohlášení;
- odvolací řízení, obnova řízení, mimo odvolací řízení, elektronická komunikace mezi prvoinstančním a odvolacím orgánem;
- sledování termínů pomocí kalendáře úkolů;
- aktuální informace o účastnících, dotčených orgánech a ostatních;
- automatizované generování dokumentů ze zadaných údajů do textového editoru s možností následné editace;
- postupné vytváření archivu údajů včetně dokumentů;
- využití údajů z registru obyvatel, ekonomických subjektů;
- využití údajů z územně identifikačního registru, registru nemovitostí.

4.7.17 ÚŘEDNÍ DESKA

Slouží pro evidenci dokumentů na úřední desce, proces schvalování, vyvěšení, svěšení, změny, upozorňování na termíny vyvěšení a svěšení.

4.7.18 VODOPRÁVNÍ ÚŘAD

Program pro podporu činností vodoprávního úřadu, včetně speciálního stavebního úřadu. Evidence rozhodnutí a dalších činností podle vodního zákona, vedení vodoprávní evidence. Základní vlastnosti jsou následující:

- evidence správních řízení a dalších úkonů dle vodního zákona;
- vedení vodoprávní evidence včetně předávání dat na MZE;
- odvolací řízení, obnova řízení, mimo odvolací řízení, elektronická komunikace mezi prvoinstančním a odvolacím orgánem;
- sledování termínů pomocí kalendáře úkolů;
- aktuální informace o účastnících, dotčených orgánech a ostatních;
- automatizované generování dokumentů ze zadaných údajů do textového editoru s možností následné editace;
- postupné vytváření archivu údajů včetně dokumentů;
- využití údajů z registru obyvatel, ekonomických subjektů
- využití údajů z územně identifikačního registru, registru nemovitostí
- tisk adres v řízení nebo posílání tisku sekretářce

5 INFORMAČNÍ KONCEPCE

NEPŘEHLÉDNĚTE

Informační koncepce je dokument, v němž orgány veřejné správy stanoví své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných ISVS a vymezí obecné principy pořizování, vytváření a provozování ISVS.

Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy[11] požaduje v koncepci uvést:

- charakteristiku každého ISVS, jehož je správcem, stručnou charakteristiku jeho současného stavu a předpokládané změny v tomto systému;
- záměry na pořízení nebo vytvoření nových ISVS;
- dlouhodobé cíle v oblasti řízení kvality ISVS, požadavky na kvalitu a plán řízení kvality;
- dlouhodobé cíle v oblasti řízení bezpečnosti informačních systémů veřejné správy, požadavky na bezpečnost a plán řízení bezpečnosti;
- soubor základních pravidel pro správu ISVS a to včetně postupů, které vedou k jejich naplňování;
- způsob financování záměrů, dlouhodobých cílů a správy ISVS;
- postupy při vyhodnocování dodržování informační koncepce a při provádění jejích změn;
- 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.

Informační koncepce tedy stanovuje zásady pro správu ISVS, včetně postupů, které vedou k jejich naplňování. Orgán veřejné správy stanoví zásady vždy pro oblasti:

- pořizování a vytváření informačních systémů veřejné správy;
- provozování informačních systémů veřejné správy, a to včetně jejich změn a rozvoje.

Informační koncepci je nutné zpracovat s ohledem na potřeby konkrétního orgánu veřejné správy.

5.1 STRUKTURA INFORMAČNÍ KONCEPCE

Ministerstvo vnitra ČR nechalo vypracovat řadu metodických materiálů pro vypracování informační koncepce (IK) pro různé úrovně veřejné správy[12]:

- ústřední orgán veřejné správy;
- obec s rozšířenou působností;
- obec s pověřeným obecním úřadem;
- obec s výkonem přenesené působnosti v základním rozsahu.

[11] Vyhláška 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 (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

[12] http://www.mvcr.cz/clanek/priklady-informacnich-koncepci.aspx

Tyto materiály sice mají informativní a doporučující charakter, ale mohou posloužit orgánům veřejné správy při tvorbě jejich vlastní Informační koncepce.

NEPŘEHLÉDNĚTE

Doporučená **struktura informační koncepce** je následující[13]:

- identifikace informační koncepce;
- informační systémy ve správě orgánu veřejné správy;
- záměry na pořízení nebo vytvoření nových ISVS;
- řízení kvality ISVS;
- řízení bezpečnosti ISVS;
- zásady a postupy pro správu ISVS;
- způsob financování ISVS;
- naplňování informační koncepce;
- osoba, která řídí provádění činností podle IK a zákona, nebo její funkční zařazení.

5.1.1 IDENTIFIKACE INFORMAČNÍ KONCEPCE

Základní údaje IK jsou většinou uvedeny ve formě tabulky která obsahuje:

- orgán veřejné správy (organizace), který IK vydává, uvádí se název, sídlo, typ (ústřední úřad, KÚ, ORP, POÚ,...);
- časové ohraničení IK, např. označení počáteční verze, datum vzniku IK, datum počátku platnosti, doba platnosti resp. datum konce platnosti;
- údaje o dokumentu, čili označení verze dokumentu, název a umístění elektronické podoby, počet stran a příloh apod.
- označení důvěrnosti dokumentu;
- autorství, tedy útvar, jména a funkce při interním zpracování nebo organizace a další údaje při externím zpracování;
- schválení, čili jméno resp. jména, útvar, funkce, datum schválení IK popř. další údaje.

IK musí reagovat na různé změny, např. v legislativě, vývoj technologií apod., proto vytváříme její nové verze, které musíme sledovat a identifikovat. Proto uvádíme chronologický seznam všech verzí. Identifikace verze musí obsahovat obdobnou strukturu údajů, jako základní údaje:

- označení verze, datum vzniku, datum počátku platnosti;
- údaje o dokumentu, tj. název a umístění elektronické podoby, počet stran a příloh apod.;
- autorství a schválení.

U změn provedených ve verzi IK uvádíme popis a odůvodnění změny a identifikaci míst v dokumentu, která byla změněna.

[13] KONERO. *Dlouhodobé řízení ISVS: Úplná struktura informační koncepce*. Dostupné z: http://www.mvcr.cz/soubor/dalsi-dokumenty-uplna-struktura-informacni-koncepce.aspx

5.1.2 INFORMAČNÍ SYSTÉMY VE SPRÁVĚ ORGÁNU VEŘEJNÉ SPRÁVY

Příslušný orgán veřejné správy by měl charakterizovat všechny IS, které využívá. Může zvolit přístup, že každý ISVS charakterizuje zvlášť nebo že více IS považuje za subsystémy jednoho ISVS. U provozních IS s vazbami na ISVS může orgán ISVS popisovat pouze vazby těchto IS na ISVS, popř. je popsat obdobně jako ISVS. V případě potřeby může uplatnit daný postup na všechny provozované IS bez ohledu na to, zda mají či nemají vazbu na ISVS.

Úvod této části by měl obsahovat, jakým způsobem jsou charakterizovány a popisovány jednotlivé ISVS a provozní IS, které mají vazby na ISVS, popř. zda jsou zahrnuty všechny provozní IS, tedy i ty, které nemají vazby na ISVS.

Vhodné je uvést přehledný seznam všech IS, které jsou dále popsány s rozlišením, o jaký typ se jedná (ISVS, provozní IS s vazbou na ISVS provozní IS bez vazby na ISVS).

Pak by měly být podrobněji popsány jednotlivé IS ve členění:

- informační systémy veřejné správy;
- provozní informační systémy.

Popis každého ISVS by měl obsahovat název systému, popis jeho určení (včetně případného odkazu na zřizující legislativu), identifikaci útvaru odpovědného za jeho správu, případně osobu správce. Charakteristika rovněž musí obsahovat:

- data, která jsou v něm zpracovávána;
- služby, jsou jeho prostřednictvím zajišťovány;
- použité technické a programové prostředky.

Dále je vhodné uvést stručnou charakteristiku stávajícího stavu a následně charakteristiku předpokládaných změn IS, včetně jejich časového horizontu a finančních nároků, popř. konstatování, že se se žádnými změnami nepočítá nebo záměr na ukončení činnosti IS.

V případě, že se provozní IS popisují obdobně jako ISVS, pak popis by měl obsahovat stejné údaje, u provozních IS s vazbami na ISVS by měly být popsány také tyto vazby.

5.1.3 ZÁMĚRY NA POŘÍZENÍ NEBO VYTVOŘENÍ NOVÝCH IS

V úvodu by měly být shrnuty informační potřeby příslušného orgánu a z toho plynoucí záměry pořízení nových IS nebo konstatování, že zatím žádný takový záměr neexistuje.

Pro každý záměr nového IS se následně uvede popis každého zamýšleného systému, který by měl obsahovat:

- název IS, popř. zkratka;
- typ (ISVS, provozní IS s vazbami na ISVS, provozní IS bez vazeb);
- budoucí správce, útvar zajišťující správu IS;
- způsob realizace (pořízení nebo vytvoření);
- důvod včetně odkazu na legislativu, usnesení vlády apod.;
- základní finanční a časové specifikace projektu budování IS,
- stručnou charakteristiku (zpracovávaná data, zajišťované služby, technické a programové prostředky);
- charakteristiku stávajícího stavu řešení oblasti, konstatování stavu budování (např. pobíhá veřejná soutěž) případně odkazy na existující dokumentaci (např. koncepce řešení apod.);
- případné další doplňující informace, okolnosti či poznámky.

5.1.4 ŘÍZENÍ KVALITY ISVS

Pro řízení kvality ISVS je nutné stanovit dlouhodobé cíle kvality, ty pak transformovat do konkrétních požadavků na kvalitu a následně stanovit plán, jak má být těchto cílů resp. naplnění požadavků dosaženo. Základní požadavky stanovuje Vyhláška č. 529/2006 Sb.[14]

DLOUHODOBÉ CÍLE

Dlouhodobé cíle musí být stanoveny pro zajištění kvality:

- dat, která jsou v IS zpracovávána;
- služeb, které jsou prostřednictvím IS poskytovány;
- technických a programových prostředků.

KVALITA DAT

Aktuálnost dat je jedním z významných prvků kvality dat. Požadavky na ni jsou dány typem a provedením IS, např. on-line systémy, kde se změny projevují okamžitě, nebo systémy, kde je např. zapotřebí replikace dat, která způsobuje časovou prodlevu. Vliv má i spolupráce s jinými systémy nebo mezi subsystémy.

Správnost dat může být zajišťována např. vizuální kontrolou nebo kontrolou zajišťovanou administrativně či technicky (od jednoduché kontroly typu ověření modulo 11 u rodného čísla po složité křížové kontroly dat z více zdrojů).

Integrita dat (konzistence) je zabezpečována hlavně na technologické úrovni, aby se minimalizovaly chyby lidského faktoru.

Významným prvkem je **stanovení odpovědnosti** v celém procesu zpracování dat, tj. od vkládání dat, přes úpravy dat až po konečné zpracování.

KVALITA SLUŽEB

Dostupnost služeb je mimo jiné závislá na kvalitě technických prostředků. Jde o zaručení funkčnosti služeb tak, aby požadovaná informace byla přístupná ve stanoveném místě, v požadované formě a v určeném časovém rozmezí.

Přehlednost služeb je dána kvalitou uživatelského rozhraní IS, které by mělo být intuitivní. Uživatel by měl vždy vědět, ve které části rozhraní se nachází, a pro všechny systémy by měla platit jednotná pravidla.

Srozumitelnost služeb znamená, že všechny prvky rozhraní jsou jednoznačné, popisky nejsou matoucí atd. Postupy by měly být logické a v rozumné míře srozumitelné i neznalému uživateli.

Rozhraní služby by mělo být **přístupné i handicapovaným uživatelům** a odpovídat např. pravidlům pro tvorbu přístupného webu (viz kap. 10.1).

Kompatibilita s běžně používanými klientskými prostředími a standardy umožňuje bezproblémovou spolupráci s dalšími informační systémy.

KVALITA TECHNICKÝCH A PROGRAMOVÝCH PROSTŘEDKŮ

Kvalita IS je přímo závislá na kvalitě technických a programových prostředků, protože chyby těchto prostředků mají přímý vliv na kvalitu dat a služeb.

[14] Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy.

Kvalita technických prostředků zahrnuje kvalitu samotného technického vybavení, a také prvky potřebné k odvrácení technických rizik. Záleží na volbě vhodných technických komponent systémů (včetně jejich firmware), zařízení schopných omezit rizika výpadku vnějších prvků (např. výpadek energie, výpadek připojení k internetu) nebo výpadku samotného zařízení (disková pole, clustery, počítače se znásobenými komponentami pro případ jejich výpadku, apod.). Mezi prvky k zajištění kvality technických prostředků rovněž patří další podpůrné systémy, jako např. zálohovací systémy, ale i routery, firewally apod.

Požadavky na **kvalitu programových prostředků** zahrnují škálu softwarového vybavení, kterou lze rozdělit do úrovní:

- základní vrstva (operační systémy, certifikované ovladače, servisní balíčky či "záplaty" atd.);
- podpůrná vrstva (databázové, aplikační a webové servery, run-time prostředí typu Java apod.);
- aplikační vrstva (konkrétní programového vybavení, zajišťující vlastní funkčnost systému, můžeme zde zařadit i programové prostředky spolupracujících systémů).

POŽADAVKY NA KVALITU ISVS

Požadavky na kvalitu obsahují souhrn požadavků, které jsou konkretizací obecných cílů kvality. Požadavky by měly být pokud možno formulovány tak, aby byly měřitelné. Měly by být vázány na cíle kvality, k jejichž naplnění směřují. Požadavky mohou být specifické pro jeden IS nebo společné pro několik IS, resp. pro záměry na vybudování nových IS. Součástí vyhodnocování IK by mělo být mj. též vyhodnocování míry a způsobu naplnění stanovených požadavků na kvalitu IS.

PLÁN ŘÍZENÍ KVALITY ISVS

Plán řízení kvality obsahuje popis činností, které orgán veřejné správy vykonává pro naplnění stanovených cílů kvality a uplatnění konkrétních požadavků na kvalitu IS. Součástí je též předpokládaný časový harmonogram plnění cílů a požadavků v oblasti kvality.

Činnosti lze shrnout do skupin:

- stanovení cílů kvality (stanovení odpovědnosti, vymezí obecných cílů kvality, jejich popis, přidělení příslušných atributů včetně termínu naplnění atd.);
- stanovení požadavků na kvalitu (předání cílů kvality správcům IS, popř. projektovým manažerům, kteří sestaví požadavky, jejichž postupným splněním bude tento cíl naplněn, nebo konstatují, že IS již cíl splňuje, stanoví dílčí termíny plnění požadavků);
- implementace požadavků na kvalitu (provádí odpovědní pracovníci);
- prověrka dodržování požadavků na kvalitu (prověřuje se implementace požadavku na IS)
- vyhodnocení řízení kvality (součástí je vyhodnocení závěrů z provedených prověrek dodržování požadavků na kvalitu, revize dlouhodobých cílů kvality a jejich aktualizace, vyřadí se implementované a prověřené požadavky na kvalitu a vytvoří se nové, vyhodnocení může být podnětem k vydání nové verze IK).

5.1.5 ŘÍZENÍ BEZPEČNOSTI ISVS

Podobně jako u řízení kvality je pro řízení bezpečnosti IS nutné stanovit dlouhodobé cíle bezpečnosti, ty transformovat do konkrétních požadavků na bezpečnost a následně stanovit plán, jak má být těchto cílů resp. naplnění požadavků dosaženo.

My se těmito otázkami budeme zabývat v kapitole 0

Informační koncepce - řízení bezpečnosti ISVS.

5.1.6 ZÁSADY A POSTUPY PRO SPRÁVU ISVS

Vymezení problematiky je uvedeno ve Vyhlášce č. 529/2006 Sb. Stanovují se pravidla a postupy, které vedou k jejich naplňování, pro nejdůležitější fáze životního cyklu IS:

- pořizování a vytváření IS;
- pro provozování IS;
- pro plánování rozvoje IS.

POŘIZOVÁNÍ A VYTVÁŘENÍ IS

VYPRACOVÁNÍ ZÁMĚRU NOVÉHO IS

Před pořízením, popř. vytvořením IS, musí orgán veřejné správy provést a v IK popsat základní kroky:

- definování potřeby IS a analýza zdrojů pro jeho pořízení (vytvoření) včetně očekávané finanční náročnosti a časové dostupnosti zdrojů apod.;
- analýza výchozího stavu na základě stávající IK a provozní dokumentace (možnosti stávajících IS v daných podmínkách, zda nedochází k duplicitám, zda není na možnost využití služeb nebo zdrojů jiných IS téhož správce apod.), popis realizace dané činnosti v současnosti;
- stanovení požadovaného cílového stavu IS, vyplývající z definice potřeby IS, musí posloužit i pro jasné zadání tvůrci IS;
- stanovení kvalitativních požadavků a požadavků na zajištění bezpečnosti, vyplývajících z dlouhodobých cílů a obecných požadavků, např. z pohledu nároků na zajištění důvěrnosti dat, požadavků na poskytované služby veřejnosti apod.;
- analýza důsledků, které pořízení (vytvoření) IS může vyvolat, např. dopad na procesy a činnosti úřadu, organizační opatření, vazby na jiné IS apod.).

POŘIZOVÁNÍ IS

Pokud orgán veřejné správy hodlá pořizovat IS od dodavatele, v IK uvede:

- požadavky na dokumentaci IS, požadavky na oprávnění nezbytná pro provádění údržby a změn v IS, a to i s ohledem na to, zda hodlá správce IS údržbu a případní změny provádět vlastními silami, požadavky na certifikaci systému, certifikaci bezpečnosti či jakosti, atestaci apod.;
- požadavky na projektové řízení u dodavatele (nemusí být definovány, je možné ponechat výběr metody na dodavateli), pokud jsou definovány, je vhodné vycházet z obecně uznávaných českých norem v této oblasti;
- požadavky na testování IS a podmínky akceptace (jakým způsobem, na základě jakých kritérií a kým), měly by vycházet z rozsahu systému, počtu poskytovaných služeb apod.

VYTVÁŘENÍ IS

Pokud orgán veřejné správy hodlá vytvářet IS vlastními silami, v IK uvede:

- definované postupy pro činnost tvůrců
- zásady řízení projektu, případně jiné vhodné normy;
- náležitosti dokumentování procesů vytváření IS (apelovat na průběžnou tvorbu dokumentace), komentáře ke zdrojovému kódu atd., každá vývojová fáze musí být

zakončena schválením výstupních dokumentů, které se stanou vstupním podkladem pro fázi následující.

PROVOZOVÁNÍ IS

Vyhláška č. 529/2006 Sb. vymezuje minimální oblasti, pro které je nutné stanovit zásady a postupy při provozování.

PROVOZ A ÚDRŽBA IS

Do této části se zahrnují zásady a postupy pro vlastní provoz a údržbu IS. Patří sem mimo jiné podávání a vyřizování požadavků na provoz a údržbu, řešení poruch apod., vytváření a údržbu provozní dokumentace a zajištění souladu provozování IS s IK a provozní dokumentací. Je nezbytné stanovit povinnosti jednotlivých zaměstnanců nebo jiných fyzických osob ve vztahu k činnostem z oblasti zajištění provozu a údržby IS

Údržba IS zahrnuje činností, které vedou k zachování funkcí IS v požadovaném a nezměněném stavu (například opravy chyb, bezpečnostní záplaty apod.).

Proces vyhodnocování by se měl soustředit na všechny dílčí aspekty, jako je soulad provozní dokumentace s legislativou a informační koncepcí a soulad procesů provozování IS s informační koncepcí a provozní dokumentací.

ŘÍZENÍ ZMĚN V ISVS

Provádění změn v IS zahrnuje kvalitativní změny vždy spojené se změnami funkčnosti nebo datového rozhraní (např. potřeba rozšíření funkcionality, změna datového obsahu, změna datových rozhraní, změna procesů ve kterých je IS používán, reagování na novelizaci právních předpisů apod.). Řízením změn představuje zajištění činností při řízení navrhování, schvalování a realizace změn IS. Řízení změn musí být dokumentováno.

Součástí postupů ve fázi návrhu jsou vždy:

- definování potřeby změn v IS;
- analýza výchozího stavu pro rozvoj IS;
- stanovení cílového stavu ISVS;
- stanovení požadavků na kvalitu a bezpečnost vztahujících se k cílovému stavu IS;
- návrh transformace z výchozího do cílového stavu IS (i více alternativ, které orgán veřejné zprávy vyhodnotí na základě informací o výhodách a nevýhodách);
- analýza důsledků, které změna může vyvolat (dle navržených alternativ);
- fáze realizace (schválená alternativa), provedení změn a promítnutí změn do provozní dokumentace a jiných dokumentů, kterých se změna dotýká.

V oblasti realizace změny je třeba v provozní dokumentaci řešit tyto oblasti:

- pravidla pro změnové řízení;
- používané nástroje pro řízení verzí a konfigurační management;
- postupy provádění změn;
- pravidla pro podrobné dokumentování změny;
- promítnutí změn do provozní dokumentace a jiných dokumentů, kterých se změna dotýká.

Kromě zásad a postupů být definovány role a odpovědnosti za navrhování změn, oprávnění ke schvalování změn, řízení a vlastní provádění změn.

UKONČENÍ ČINNOSTI IS

Vlastní ukončení provozu IS by mělo být řízeným procesem s definovanými rolemi a odpovědnostmi. V IK musí být popsán i postup předcházející vyvolání tohoto procesu (např. pravidelné vyhodnocování informační koncepce a ověřování využívání systému). Dříve, než je ukončena činnost IS, musí být bezpečně naloženo s daty, která IS zpracovává, včetně nosičů těchto dat, s cílem zabránit neoprávněnému přístupu k těmto datům. Obvykle se jedná o:

- převedení dat do jiného IS;
- uchování dat, je nutné definovat, kde a jak budou data uchována, jak bude zajištěna jejich čitelnost, kdo bude odpovědný za dostupnost dat;
- zničení dat, dle skartačního řádu.

PLÁNOVÁNÍ ROZVOJE IS

Orgán veřejné správy by měl vytvářet a průběžně udržovat plán rozvoje IS, který by měl obsahovat plány:

- pořizování a vytváření nových IS;
- provozování a údržby provozovaných IS;
- provádění změn do stávajících IS,
- ukončení činnosti rušených IS (s náhradou nebo bez náhrady).

Součástí plánu by měl být časový harmonogram provádění akcí. Plán rozvoje IS vyžaduje pravidelnou aktualizaci. V závažných změn nebo požadavků na vytvoření nových významných IS může při aktualizaci plánu rozvoje IS vzniknout požadavek na zpracování nové verze informační koncepce.

5.1.7 ZPŮSOB FINANCOVÁNÍ ISVS

Provoz, údržba, změny a rozvoj IS jsou úzce spojeny s financováním. Proto musí být oblast financování zahrnuta v IK, obsah je ovlivněn předpisy, jako je Vyhláška č. 529/2006 Sb., Zákon č. 365/2000 Sb. nebo Zákon č. 137/2006 Sb., o veřejných zakázkách.

Financování IS se řeší v oblastech:

- pořízení nebo vytvoření nových IS;
- naplnění dlouhodobých cílů;
- správa IS.

FINANCOVÁNÍ ZÁMĚRŮ NA POŘÍZENÍ NEBO VYTVOŘENÍ NOVÝCH ISVS

Je nezbytné vycházet ze záměrů na pořízení nebo vytvoření nových IS. Z přehledu všech plánovaných nových IS plynou finančních specifikace. Je třeba naplánovat zdroje financování záměrů (vlastní rozpočet, dotační programy apod.). V IK je třeba zakotvit také povinnosti, které v této oblasti vyplývají v oblasti schvalování investičních záměrů.

FINANCOVÁNÍ NAPLNĚNÍ DLOUHODOBÝCH CÍLŮ

Naplnění dlouhodobých cílů představuje ve své podstatě realizaci požadavků na kvalitu a požadavků na bezpečnost, a to formou změn stávajících IS nebo specifických požadavků na budování nových IS. Tato část se zaměřuje na stávající IS. Popisuje se způsob financování projektů rozvoje IS a také zajištění potřebných zdrojů. Vytvoří se příslušný plán.

FINANCOVÁNÍ SPRÁVY ISVS

Financování správy IS zahrnuje provoz, údržbu a rozvoj samotných IS a další podpůrné činnosti včetně dlouhodobého řízení ISVS, hrazené z provozních finančních prostředků. Je popsán způsob financování činností a vytvoří se příslušný plán a popíše se způsob zajištění potřebných zdrojů.

5.1.8 NAPLŇOVÁNÍ INFORMAČNÍ KONCEPCE

Za naplňování IK považujeme praktické naplnění postupů a zásad uvedených v informační koncepci, udržování informační koncepce v aktuálním stavu a pravidelné vyhodnocování dodržování informační koncepce a realizaci opatření pro odstranění zjištěných nedostatků. Pro zajištění tohoto je třeba stanovit osobní odpovědnosti za jednotlivé oblasti IK a kontrolovat plnění. Jsou zde rovněž popsány postupy pro vyhodnocování IK a její údržbu (provádění změn), dále jsou konkretizovány odpovědnosti v oblasti naplnění IK a zákonných povinností v oblasti dlouhodobého řízení ISVS.

POSTUPY PŘI PROVÁDĚNÍ ZMĚN IK

V této kapitole se popíší konkrétní postupy pro

- zajištění včasné změny IK (tak, aby byl zachován soulad obsahu IK se skutečným stavem a aktuálními požadavky orgánu veřejné správy), je nutné stanovit periodu revidování a události, které povedou na nutnost aktualizace IK i mimo stanovenou periodu;
- zápis změny do dokumentu IK, technické postupy pro vydávání změn IK, postup a způsob identifikace verzí IS, popis a odůvodnění změny a identifikace změněné části IK atd.;
- schvalování změny IK, změny podléhají obdobnému postupu schvalování, jako původní verze IK;
- příprava nové IK, měla by proběhnout před uplynutím platnosti předchozí IK, stanovení rolí.

POSTUPY PŘI VYHODNOCOVÁNÍ DODRŽOVÁNÍ INFORMAČNÍ KONCEPCE

Vyhodnocování dodržování informační koncepce je základním kontrolním mechanizmem zajišťujícím zpětnou vazbu. Je třeba popsat konkrétní postupy. Vyhodnocování by mělo probíhat periodicky (max. 24 měsíců). Je třeba dodržovat zásadu, že vyhodnocování by mělo být nezávislé na realizaci (vyhodnocuje jiný pracovník, než ten, který je zodpovědný za realizaci IK).

Oblasti pro vyhodnocování IK:

- charakteristiky všech orgánem veřejné správy spravovaných IS, včetně jejich aktualizací;
- záměry na pořízení nebo vytvoření IS, jsou obsaženy všechny záměry a jsou náležitě charakterizovány;
- včasná aktualizaci IK, aktuální verze je schválena, náležitě označena včetně vyznačení provedených změn, všichni relevantní pracovníci mají k dispozici aktuální verzi IK a je zajištěno, aby neplatná verze nebyla používána;
- jsou v rámci jednotlivých IS dodržovány a vyhodnocovány požadavky na kvalitu;
- jsou v rámci jednotlivých IS dodržovány a vyhodnocovány požadavky na bezpečnost;
- správa ISVS je vykonávána v souladu s přijatými zásadami a postupy;

- jsou vykonány všechny potřebné kroky před pořízením nebo vytvořením ISVS, při pořizování ISVS jsou naplňovány všechny stanovené požadavky, které jsou následně zakotveny ve smlouvě, při vytváření ISVS jsou všechny procesy náležitě dokumentovány a v případě projektového řízení jsou prakticky uplatňovány zásady a postupy projektového řízení;
- jsou uplatňovány zásady a postupy pro plánování rozvoje ISVS, zajištění provozu a údržby ISVS, řízení změn ISVS a ukončování činnosti ISVS;
- financování ISVS probíhá v souladu se schválenými postupy a platnými předpisy, existuje pravidelně aktualizovaný plán;
- vyhodnocení nastalo v předepsaném čase, jsou dostupné aktuální verze IK a zápisy z minulých vyhodnocení, opatření přijatá v minulých hodnoceních byla promítnuta do aktualizované verze IK, přijatá opatření jsou uplatňována v praxi a jaký mají účinek.

Dále by mělo být popsáno vyhotovení zápisu o vyhodnocení. Zápis o vyhodnocení by měl obsahovat následující části:

- identifikace zápisu, datum vyhodnocení;
- hodnotitelé (jméno resp. jména, funkce, útvar nebo externí organizace);
- průběh vyhodnocení;
- poznatky a závěry z vyhodnocení;
- přijatá opatření;
- schválení zápisu z vyhodnocení a jeho zpřístupnění.

5.1.9 OSOBA, KTERÁ ŘÍDÍ PROVÁDĚNÍ ČINNOSTÍ

Stanovení odpovědností v oblasti dlouhodobého řízení ISVS. Ty lze rozdělit:

- odpovědnosti za realizaci informační koncepce;
- odpovědnosti za splnění zákonných povinností.

ODPOVĚDNOSTI ZA REALIZACI INFORMAČNÍ KONCEPCE

Jsou určeny osoby (zaměstnanec nebo jiná fyzická osoba) případně organizační útvar, kteří odpovídají za tuto oblast jako celek. Dále lze specifikovat dílčí role a povinnosti, kterým mohou být přiřazeny jiné odpovědné osoby nebo útvary. Základní přehled dílčích odpovědností vyplývá ze struktury IK.

- vytváření záměrů na pořízení nebo vytvoření nových IS a jejich schvalování;
- řízení kvality IS;
- řízení bezpečnosti IS;
- koordinace činností v oblasti rozvoje IS, příprava plánu rozvoje IS, schvalování plánu rozvoje IS,
- řízení postupů při pořizování a vytváření IS;
- vyhodnocování dodržování souladu provozování IS;
- koordinace a vyhodnocování řízení změn;
- řízení ukončování provozu IS;
- vytváření a údržba plánu financování IS a jeho schvalování;
- příprava změn IK, schvalování změn IK a jejích nových verzí;
- příprava nové IK před ukončením platnosti stávající;
- provádění vyhodnocování dodržování IK a vyhotovení zápisu o vyhodnocování,
- návrh opatření na základě zjištění při vyhodnocování a jejich schvalování;
- schválení zápisu z vyhodnocení.

SPLNĚNÍ ZÁKONNÝCH POVINNOSTÍ

Základní rolí je splnění povinností, které orgánu veřejné správy stanoví zákon. Měl by být jmenován zaměstnanec nebo jiná fyzická osoba případně organizační útvar, který za tuto oblast odpovídá. Užitečné je uvést výčet dílčí odpovědnosti za splnění zákonných povinností podle jednotlivých legislativních norem.

5.2 DOKUMENTACE

Dokumentace provází celý životní cyklus informačního systému. Z tohoto hlediska ji můžeme rozdělit na okruhy:

- zadávací dokumentace;
- projektová a programová dokumentace;
- implementační dokumentace;
- provozní dokumentace.

Obecně každá dokumentace by měla obsahovat:

- určení;
- historii dokumentu;
- vlastní dokument;
- přílohy.

My se budeme zabývat především provozní dokumentací.

5.2.1 ZADÁVACÍ DOKUMENTACE

Informační koncepce v sobě zahrnuje i záměry na pořízení informačních systémů (viz kap. 5.1.3). Na tomto základě se zpracovává i zadávací dokumentace. Termín "zadávací dokumentace" je užíván především v souvislosti se Zákon č. 137/2006 Sb., o veřejných zakázkách.

NEPŘEHLÉDNĚTE

Zadávací dokumentace je soubor dokumentů, údajů, požadavků a technických podmínek zadavatele vymezujících předmět veřejné zakázky v podrobnostech nezbytných pro zpracování nabídky.

I když v této chvíli zadávání veřejných zakázek není hlavním předmětem našeho zájmu, měli bychom vzít na vědomí, že zadávací dokumentace musí obsahovat alespoň:

1. Technické podmínky, což je objektivní a jednoznačné vymezení charakteristik a požadavků na dodávky nebo služby, stanovující účel využití požadovaného plnění zamýšlený zadavatelem, který je formuluje s využitím odkazu na české technické normy přejímající evropské normy nebo jiné národní technické normy přejímající evropské normy, evropská technická schválení, obecné technické specifikace stanovené v souladu s postupem uznaným členskými státy Evropské unie a uveřejněné v Úředním věstníku Evropské unie a mezinárodní normy, nebo jiné typy technických dokumentů než normy, vydané evropskými normalizačními orgány. Není-li to možné, pak se využijí odkazy na české technické normy nebo národní technické podmínky.
2. Požadavky na opatření k ochraně utajovaných informací, je-li to odůvodněno předmětem veřejné zakázky.
3. Kvalifikační předpoklady dodavatele.

4. Obchodní podmínky, včetně platebních podmínek, případně též objektivních podmínek, za nichž je možno překročit výši nabídkové ceny.
5. Požadavky na varianty nabídek, pokud je zadavatel připustil.
6. Požadavek na způsob zpracování nabídkové ceny.
7. Podmínky a požadavky na zpracování nabídky.
8. Požadavky na zabezpečení dodávek, je-li to odůvodněno předmětem veřejné zakázky.
9. Způsob hodnocení nabídek podle hodnotících kritérií.

Z hlediska obsahu by zadávací dokumentace informačního systému měla především obsahovat:

1. Popis stávajícího stavu, který by měl obsahovat východiska pro nový systém, tedy principy stávajícího modelu, využívané technologie, oblasti zpracování, vazby a způsoby komunikace mezi jednotlivými moduly, struktura dat apod.
2. Globální architektura IS, která by měla také zahrnovat:
   - funkční dekompozici na úroveň jednotlivých systémů, souhrnný popis globální funkcionality systému a služeb vnějších i interních komunikačních rozhraní;
   - popis datového obsahu a datové architektury, tj. koncepce datové architektury, datový model, datová rozhraní, distribuce dat externím subjektům atd.;
   - základní procesy a procesní architekturu, tj. řídící procesy, práce s daty (zadávání, čtení, úpravy a zápisy dat), komunikace mezi moduly atd.;
   - technologická architektura, čili HW schéma a jeho souhrnný popis (komponenty technologické architektury, specifikace jednotlivých HW položek technologické infrastruktury a jejich rozložení) SW architektura (specifikace základního SW, specifikace platforem použitých pro aplikační SW, způsob zajištění požadavků na dostupnost a škálovatelnost řešení).
3. Katalog služeb a provozních a kapacitních parametrů systému, který obsahuje seznam služeb, které jsou realizovány prostřednictvím informačních systémů a slouží pro přístup a editaci dat v nich vedených. Zajišťuje i mapování služeb IS ke službám poskytovaným, např. orgány VS občanům. Katalog by měl obsahovat popis služby (co zabezpečuje a jakým způsobem), vstupní a výstupní parametry.

5.2.2 *PROJEKTOVÁ A PROGRAMOVÁ DOKUMENTACE*

Dokumentace spadající do tohoto okruhu je zpracována vývojovými pracovníky a určena pro vývojové pracovníky.

NEPŘEHLÉDNĚTE

Projektová a programová dokumentace vychází ze zadávací dokumentace a je tvořena komplexem dokumentů vzniklých v procesu analýzy a návrhu systému. Obsahuje modely na konceptuální a technologické úrovni a jejich popis, např.:

- hrubý technický návrh IS;
- detailní technický návrh IS;
- struktura programových modulů;
- zdrojové kódy programových modulů s komentáři a odkazy;

- atd.

5.2.3 IMPLEMENTAČNÍ DOKUMENTACE

NEPŘEHLÉDNĚTE

Implementační dokumentace obsahuje popis způsobu implementace.

Zahrnuje především:

- metodiku a nástroje a způsob implementace aplikační logiky a rozhraní;
- způsob implementace jednotlivých funkcí systému, obsažených v katalogu služeb;
- postup naplnění systému daty (popis zdrojových dat a jejich zpracování, detailní postup naplnění daty a způsob kontroly kvality dat);
- testování implementovaného systému (způsob provedení funkčních testů všech subsystémů, funkčních testů napojení na další systémy, zátěžových testů, integračních testů celého systému v provozním prostředí, bezpečnostní testy atd.);
- způsob realizace funkcí pro publikaci dat, poskytování veřejných dat veřejnosti dálkovým přístupem;
- popis realizace pilotního a ověřovacího provozu;
- organizaci a návrh školení (školení správců a jejich certifikace, školení uživatelů apod.);
- popis přípravy na ostrý provoz;
- způsob realizace nástrojů pro správu a monitoring provozu celého IS, např. logování systému, zapojení IS do posloupnosti zpracování služeb, způsob komunikace IS s jednotlivými subsystémy a agendami, transakční zpracování, vytvoření helpdesku atd.

5.2.4 PROVOZNÍ DOKUMENTACE

Obsah a strukturu provozní dokumentace ISVS stanovuje Vyhláška 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy. Zpravidla je zpracovávána k jednotlivým informačním systémům.

NEPŘEHLÉDNĚTE

Provozní dokumentace je nástrojem pro efektivní správu IS. Je určena osobám, které se systémem pracují, a to ať už jako osoby určené pro jeho správu nebo jako uživatelé, kteří například využívají dat, která jsou v systému uložena. Provozní dokumentace ISVS popisuje funkční a technické vlastnosti informačního systému

Základním principem náležité správy informačního systému je zachování jeho požadovaného stavu, bez možností provádění neschválených a nekoordinovaných změn v tomto systému. Z tohoto důvodu je nezbytné, aby byl stav systému popsán, byla stanovena oprávnění a povinnosti vztahující se k systému a zároveň byl dán návod uživatelům, jak se systémem efektivně a náležitě pracovat.

Požadavky na strukturu provozní dokumentace jsou definovány vyhláškou (§ 10).

NEPŘEHLÉDNĚTE

Provozní dokumentaci informačního systému veřejné správy tvoří tyto dokumenty:

- bezpečnostní dokumentace informačního systému veřejné správy;
- systémová příručka;
- uživatelská příručka.

Podle potřeb, a to vždy s ohledem na počet uživatelů, lze sloučit dokumenty do jednoho dokumentu, části provozní dokumentace pak budou tvořit jednotlivé kapitoly dokumentu provozní dokumentace.

Je možné zpracovat jednu provozní dokumentaci pro více ISVS za předpokladu, že:

- zásady a postupy pro provozování těchto systémů jsou shodné;
- žádný z obsažených ISVS nemá vazbu na IS jiného správce;
- práva na zápis, změnu nebo vymazání dat, která tyto systémy zpracovávají, jsou omezena na konečný počet jmenovitě určených zaměstnanců orgánu veřejné správy.

V tomto případě musí být v provozní dokumentaci výslovně uvedeno, pro které ISVS je provozní dokumentace společná, aby bylo jasné, kteří uživatelé a správci mohou podle daného dokumentu postupovat.

Provozní dokumentaci ISVS mohou tvořit i další dokumenty, které zvýší efektivitu správy ISVS, např. u zpracování velkých objemů dat, provádění změn v IS, v souladu s technickými normami, které zpracování jiných dokumentů předpokládají apod. Zejména u informačních systémů s vysokou úrovní zabezpečení bývá obvyklé, že je zpracováván např. provozní deník.

V provozní dokumentaci orgán veřejné správy uvádí aktuální stav ISVS, jehož je správcem. Obsahem je popis funkčních a technických vlastností ISVS (funkcí a služeb, jejichž využití systém umožňuje), a to včetně organizačně technických opatření, která zajišťují zachování těchto vlastností. Jde tedy o popis jak má být systém používán, provozován, jak probíhá údržba systému, jak je možné v něm provádět změny funkcionality apod. Provozní dokumentace musí být zpracována tak, aby odpovídala zásadám a postupům stanoveným v informační koncepci, čili postupy v provozní dokumentaci nesmí být v rozporu s postupy v informační koncepci. S tím souvisí, že dokumentace musí být aktuální a její obsah musí odrážet reálný stav IS.

Bezpečnostní dokumentací informačního systému veřejné správy se budeme věnovat v kapitole věnované bezpečnosti IS (viz kap.7.2).

SYSTÉMOVÁ PŘÍRUČKA

Systémovou příručku využívá zejména správce systému.

Systémová příručka obsahuje

- popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v ISVS, včetně návodu, jak je využívat;
- stanovené parametry kvality, vycházející z požadavků na kvalitu, které jsou součástí informační koncepce;
- podrobný popis ISVS nebo odkaz na dokument, ve kterém je popis uveden a který je správci systému dostupný, zejména u rozsáhlejších IS by měl obsahovat i schémata architektury systému (dle použité metodiky pro vytvoření IS);
- popis jednotlivých činností vykonávaných při správě ISVS, včetně činností definovaných pro role osob, které tyto činnosti vykonávají, a oprávnění nezbytných pro výkon těchto činností (v IS může existovat více rolí, které mohou správci zastávat);
- definice uživatelů nebo skupin uživatelů a jejich oprávnění, povinnosti a odpovědnosti při využívání ISVS.

Tuto část provozní dokumentace většinou zpracovává dodavatel IS a je určena úseku, který má na starosti dohled a správu IS. Dokumentace[15] musí pokrýt potřebu správců IS ve všech oblastech jejich činností:

- instalace a konfigurace systémů (základní popis provozní technologie vztahující se k danému IS, popisy instalace, konfigurace a ovládání systému);
- dohled nad funkčností a bezpečností systémů (popisy, týkající se dohledu nad funkčností systému a administrace systému);
- operátorské činnosti, tj. obsluha systémů, archivace a zálohování systémů atd.;
- administrátorské zásahů do systémů;
- reakce při nestandardních či havarijních situací (popisy, týkající se bezpečnosti, řešení nestandardních stavů);
- poradenství koncovým uživatelům.

Měla by tedy zahrnovat:

- základní funkční specifikace IS;
- technologický postup práce s daným IS;
- technický návrh IS;
- organizačně provozní zajištění IS;
- instalace a konfigurace serverových komponent;
- instalace a konfigurace klientských komponent;
- konfigurace bezpečnostních prvků v systému;
- popis bezpečnostního zálohování dat a programů IS;
- popis provozního archivování dat a rušení dat z provozní databáze;
- dohled a prověřování stavu systému;
- řešení nestandardních stavů systému, scénáře řešení;
- organizace práce v etapě zavádění informačního systému do provozu;
- přílohy

Dokumentace musí být dostatečným podkladem pro tvorbu provozního řádu správy příslušného informačního systému (subsystému).

UŽIVATELSKÁ PŘÍRUČKA

NEPŘEHLÉDNĚTE

Uživatelská příručka 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.

Uživatelská příručka musí obsahovat vymezení a popis funkcí, včetně bezpečnostních, které jsou pro uživatele k dispozici a návod na jejich použití. Samozřejmostí je i vymezení oprávnění a povinností uživatelů v daném informačním systému, které musí být v souladu se systémovou příručkou.

[15] KAJZAR, Dušan. Administrátorská dokumentace k informačnímu systému. *Tvorba softwaru 2002: celostátní konference.*

Popis funkcí aplikace obsahuje:

- pokrytí provozu funkcemi IS;
- pracovní postupy, druhy zpracování;
- charakteristiky vstupů:
    - význam jednotlivých vstupních položek;
    - jejich struktura, atributy, možné zadávané hodnoty;
    - vliv zadávaných hodnot na výpočet apod.
- charakteristiky výstupů:
    - sestavy, jejich popis a použití;
    - příklady řešení standardních i specifických situací.

Někdy je zpracována rovněž tzv. referenční příručka, která obsahuje většinou příklady řešení standardních i specifických situací, postupy vkládání dat (např. postup zpracování faktur, zaevidování osoby apod.).

6 PROVOZNÍ INFORMAČNÍ SYSTÉMY

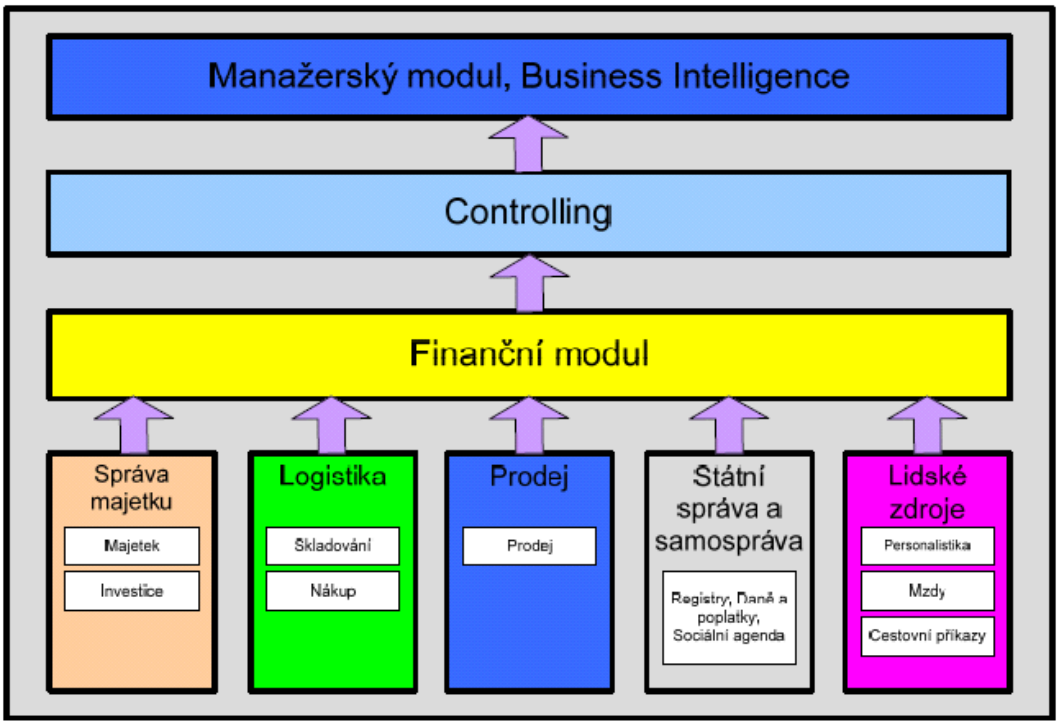
NEPŘEHLÉDNĚTE

Provozní informační systémy zajišťují informační činnosti nutné pro vnitřní provoz příslušného orgánu nesouvisející bezprostředně s výkonem veřejné správy.[16]

Jedná se např. o účetnictví, správu majetku, evidenci docházky zaměstnanců, evidenci došlých faktur aj. Činnosti, pro jejichž zajištění se tyto IS používají, bezprostředně neslouží pro výkon (vrchnostenské) veřejné správy. Byly by ISVS pouze v případě, kdy je předmětná činnost vrchnostenskou kompetencí daného orgánu veřejné správy, např. IS o (správních) rozhodnutích o přidělení nebo odnětí dotací.

Provozní informační systémy, které mají vazby na ISVS jsou popisovány v informační koncepci obdobně jako ISVS, popř. jsou popisovány pouze tyto vazby. Provozní systémy, které nemají vazby na ISVS, nemusí být popisovány v informační koncepci.

Obrázek 6-1 Systém Orsoft RADNICE



Zdroj: http://web.ortex.cz/docs/orsoft_radnice_8_brozura.pdf

Za příklad architektury IS nám může posloužit Systém Orsoft RADNICE.[17]

Modul „správa majetku“ řeší investice a správu dlouhodobého i drobného majetku.

[16] viz § 2 písm. u) Zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ve znění pozdějších předpisů)
[17] http://web.ortex.cz/produkty/orsoft-radnice/

Podmodul majetek je určen pro:

- dokladovanou evidence majetku;
- vedení databáze účetních, daňových, statistických, technicko-výrobních a obecně evidenčních informací;
- operativní evidenci drobného (neinvestičního) majetku;
- evidence majetkových daní;
- sledování cyklické údržby majetku.

Podmodul „investice“ je určen pro dokladovanou účetní, investiční a statistickou evidenci investic - nedokončených i dokončených:

- likvidace investičních faktur;
- dokončené investice (investiční majetek);
- nedokončené investice, případně částečně;
- neinvestiční náklady.

Modul „logistika“ v sobě zahrnuje skladovou evidenci a řízení nákupu.

Podmodul „skladování“ umožňuje vedení skladové evidence pro různé typy skladů:

- skladové pohyby - příjemky, výdejky, přecenění atd.;
- přehledy a statistiky, opisy dokladů;
- vyhledávání v databázi skladu, možnosti různých pohledů;
- inventarizace, sledování stavu minimálních a maximálních zásob;
- účtování pohybů;
- vazba na další moduly.

Podmodul „nákup“ je určen pro podporu řízení a zpracování činností souvisejících s objednáváním a nákupem materiálů, zboží a služeb:

- evidence dodavatelů;
- udržování dodavatelských ceníků, artiklů;
- informace o skladech, stavu zásob;
- objednávky;
- evidence dodavatelských smluv;
- evidence došlých faktur;
- hodnocení dodavatelů atd.

Modul „prodej“ umožňuje řízení prodeje:

- nabídky;
- poptávky;
- objednávky;
- smlouvy;
- dodací listy;
- faktury;
- statistiky.

Modul „samospráva a státní správa“ zahrnuje:

- registry;
- ohlašovnu;
- volební agendu;

- daně a poplatky, např.:
    - poplatky ze psů, za komunální odpad, za lázeňský a rekreační pobyt a za ubytovací kapacitu, užívání veřejného prostranství, ze vstupného, za povolení vjezdu, popř. za parkování atd.
- místní poplatky;
- přestupkové řízení;
- sociální agendu“
    - zpracování agendy sociálních dávek všech typů (příspěvek na výživu dítěte, mimořádné výhody pro těžce zdravotně postižené, jednorázové účelové příspěvky, bezúročné půjčky, příspěvek na provoz motorového vozidla, dávky sociální pomoci pro občany sociálně potřebné, pro občany staré a zdravotně postižené, příspěvek při péči o blízkou a jinou osobu, příspěvek při živelné pohromě nebo požáru, příspěvky pěstounům a dětem v pěstounské péči atd.)
    - agendy sociálně právní ochrany dětí, péče o nepřizpůsobené, koordinátora národnostních menšin, umisťování do domů a bytů zvláštního určení, pohřbívání.

Modul „lidské zdroje“ zahrnuje personální agendu a rozvoj, zpracování mezd včetně vazeb na docházkové a stravovací systémy, cestovné, vazbu na Portál veřejné správy atd.

Podmodul „personalistika“ je určen k podpoře důležitých personálních rozhodnutí a patří sem:

- personální evidence a administrativa;
- kvalifikace a vzdělávání;
- pracovní místa;
- hodnocení pracovníků;
- uchazeči o zaměstnání;
- sociální program.

Podmodul „mzdy“ zajišťuje výpočet mezd zaměstnanců a vše, co s tím souvisí:

- mzdová agenda (základní mzdy a prémiové nadstavby);
- daně;
- zdravotní i sociální pojištění, nemocenské, sociální i státní dávky;
- srážky zaměstnanců;
- mzdové uzávěrky;
- rozbory;
- penzijní fondy.

Podmodul „cestovní příkazy“ zajišťuje:

- tuzemské i zahraniční cestovní příkazy;
- výpočty cestovních náhrad;
- vazba na další podsystémy.

Finanční modul obsahuje:

- rozpočtové účetnictví;
- knihy analytické evidence a dílčích činností;
- rozpočetnictví;
- pohledávky;
- závazky;
- banka;
- pokladna.

Modul „controlling“ zahrnuje:

- modelování;
- rozpočtového výhledu;
- rozpočtu;
- schvalování rozpočtu a jeho rozpis;
- úpravy schváleného rozpočtu;
- controlling rozpočtu.
- Manažerský modul je určen pro:
- podpora strategického a taktického rozhodování
- dimenzionální modelování
- typové skupiny úloh:
- finanční účetnictví.
- majetek.
- lidské zdroje.
- prodej.
- nákup.

PŘÍKLAD 2

Další příklady provozních IS:

IS Munis (http://www.munis.cz/art/info);

CityWare (http://www.cityware.cz/cz/produkty-a-sluzby/majetkovy-subsystem/2);

Obis (http://www.mhmp.cz/index.php);

Vita (http://www.vitasw.cz/);

R-INFO (http://www.r-info.cz/index.htm);

Vera (http://www.vera.cz/reseni).

7 BEZPEČNOST IS

NEPŘEHLÉDNĚTE

Bezpečnost je schopnost informačního systému chránit data a informace tak, aby neautorizované osoby neměly možnost je číst nebo je modifikovat a zároveň aby autorizovaným subjektům nebyla zamítnuta možnost přístupu k datům na stanovené úrovni.

Data a informace patří k nejdůležitějším aktivům organizace. Je třeba chránit informace, jejichž ztráta, zneužití nebo neoprávněná modifikace mohou způsobit škodu:

- před lidmi vně organizace;
- před neoprávněnými osobami uvnitř organizace.

Informace s nezanedbatelnou hodnotou musí být chráněny, aby:

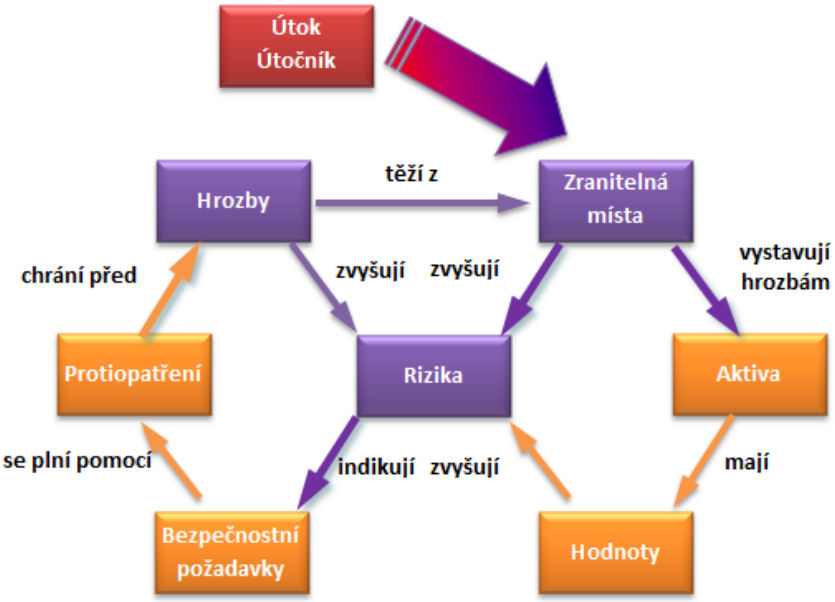
- k nim měly přístup pouze oprávněné osoby;
- se zpracovávaly nefalšované informace;
- se dalo zjistit, kdo je vytvořil, změnil nebo odstranil;
- nebyly nekontrolovaným způsobem vyzrazeny;
- byly dostupné tehdy, když jsou potřebné.

Jedná se o oblast diskutovanou a zdůrazňovanou. Přesto je to mnohdy podceňována a zanedbávaná oblast provozu IS. Obvykle řešena pouze na základní úrovni a jsou využívány pouze základní bezpečnostní funkce a mechanismy, jako jsou bezpečnostní prvky operačních systémů a bezpečnostní prvky dodané dodavatelem v rámci řídicích modulů komponenty, např. definování přístupových práv, hesla apod.

Každá firma by však měla mít svou bezpečnostní politiku, která by měla definovat podrobné principy zabezpečení provozu IS na všech úrovních uživatelů. Samozřejmě, tyto podrobnosti jsou důvěrné. Je potřebné řešení bezpečnostní problematiky ve všech činnostech v rámci IS, včetně potřebných opatření v personální oblasti. Z toho plyne nutnost věnovat bezpečnostní problematice velkou pozornost při školení všech typů koncových uživatelů, kde jim musí být řečena a vysvětlena potřebná bezpečnostní opatření. Bezpečnostní opatření obvykle znamenají omezení, což snižuje komfort koncového uživatele a prodražuje provoz IS.[18]

[18] HANÁČEK, P., STAUDEK J. *Bezpečnost informačních systémů.*

Obrázek 7-1 Vztahy v rámci systému bezpečnosti



Zdroj: VANĚK, Jindřich a Roman ŠPERKA. Informační systémy..

Vztahy mezi prvky systému bezpečnosti jsou znázorněny na obrázku.

Úkolem systému bezpečnosti je chránit aktiva organizace. Aktivum je cokoliv, co má pro organizaci nějakou cenu. Jeho hodnota musí odpovídat rozsahu systému bezpečnosti. Mezi aktiva u IS patří datové soubory a informace v nich uložené, dokumentace, počítače, média, software atd. Identifikace aktiva je proces, během kterého je vytvořen seznam aktiv a jsou určeni vlastníci daného aktiva (jednotlivec, kterým byla přidělena odpovědnost za dané aktivum). V rámci hodnocení aktiv se stanoví hodnoty aktiva v závislosti na dopadech na činnost organizace, které kterých by mohly vyplynout ztráty důvěrnosti, integrity nebo dostupnosti aktiv.

NEPŘEHLÉDNĚTE

Kritické body bezpečnosti IS jsou:

- zranitelné místo;
- hrozba;
- riziko;
- útok;
- útočník.

Hrozba je možnost využít zranitelné místo IS k útoku na něj ke způsobení škody na aktivech. Je to potenciální příčina incidentu, která může mít za následek poškození organizace. Je to potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace. Hrozby lze rozdělit na objektivní (přírodní, fyzické, fyzikální, technické nebo logické) a subjektivní, hrozby plynoucí z lidského faktoru, (neúmyslné nebo úmyslné.

Zranitelné místo je slabina IS využitelná ke způsobení škod nebo ztrát útokem na IS. Jde o důsledek chyb, selhání v analýze, v návrhu nebo v implementaci IS. Příčina může být rovněž ve vysoké hustotě uložených informací, ve složitosti softwaru, v existenci skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod. Zranitelná místa jsou vlastnosti (součásti) IS, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se IS provozuje, představují pro něj nebezpečí.

Existence hrozby představuje riziko. **Riziko** je pravděpodobnost zužitkování zranitelného místa IS (hrozba se uplatní s takovou a takovou pravděpodobností). Lze charakterizovat vedle pravděpodobnosti výskytu bezpečnostního incidentu i potenciálně způsobenou škodou.

Při analýze rizik identifikujeme a hodnotíme aktiva, hrozby, zranitelná místa a dopady na aktiva. Na základě bezpečnostních rizik se připravují potřebná bezpečnostní opatření, která umožňují plnit bezpečnostní požadavky.

Útok nazýváme bezpečnostní incident, při kterém jde o úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod, ztrát na aktivech IS apod. nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Útočit lze např. přerušením, odposlechem, změnou a přidáním hodnoty.

Útočník vede útok a může být vnější, ale v i vnitřní. Podle znalosti a vybavenosti rozeznáváme útočníky slabé, střední a velké síly.

Bezpečnostní politika v oblasti IT je nedílnou součástí všeobecné bezpečnostní politiky organizace, která představuje souhrn bezpečnostních zásad a předpisů definujících způsob zabezpečení organizace, zahrnující např. fyzickou ostrahu, ochranu profesních zájmů, popř. ochranu soukromí a lidských práv. Zabývá se výběrem bezpečnostních zásad a předpisů splňujících bezpečnostní politiku organizace a obecně definujících bezpečné používání informačních zdrojů v rámci organizace, nezávisle na konkrétně použitých informačních technologiích. Určuje, která data jsou pro organizaci citlivá, kdo je za ně odpovědný, předpisuje infrastrukturu zabývající se v rámci organizační struktury organizace bezpečností, vymezuje základní omezení, která se musí respektovat apod.

Stanovuje konkrétní normy, pravidla a předpisy konkrétně definující způsob správy, ochrany, distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci organizace. Zahrnuje specifikace bezpečnostních opatření a způsobu jejich implementace, určení způsobu jejich použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky IT organizace, při respektování konkrétně použitých IT pro realizaci IS organizace, to vše je náplní bezpečnostní politiky IS organizace.

NEPŘEHLÉDNĚTE

Bezpečnostní politika je deklarace cílů a požadavků na úroveň bezpečnosti v organizaci a stanovení rámce co, kdo a jakým způsobem se má dosáhnout. Obecně vymezuje:

- co vyžaduje ochranu;
- proti jakým hrozbám je ochrana budovaná;
- jak budeme chránit to, co vyžaduje ochranu.

Každá **změna v konfiguraci** se vždy musí posoudit z hlediska dopadu na jeho bezpečnost. Systematičnost zaručí promítnutí změn i do všech relevantních dokumentů, např. do havarijního plánu, do přijatých administrativních opatření atd. Kriticky rozsáhlá změna

může vyvolat přepracování systémové bezpečnostní politiky. Smyslem správy konfigurace je přitom mít vědomost o tom, co se změnilo a ne zabránit změnám.

Správa změnového řízení představuje pomocný řídicí nástroj pro identifikaci nových požadavků na bezpečnost po změně vlastností IS. Změny mohou představovat zařazení nových provozních procedur, inovaci softwaru, revize hardwaru, zařazení nových uživatelů, nových skupin uživatelů, nová síťová spojení. Každá změna se opět musí posoudit z hlediska dopadu na bezpečnost. Výsledek projednání dopadu změn a případné manažerské rozhodnutí se musí dokumentovat.

Přístup k zabezpečení IT je ovlivňován potřebnými náklady, citlivostí dat, typy útoků apod. Varianta bezpečnostní politiky by měla vycházet z přijaté bezpečnostní politiky organizace. Podle požadované úrovně zabezpečení rozpoznáváme bezpečnostní politiky:

- **promiskuitní** (nikoho neomezující, která každému v zásadě povoluje dělat vše, tedy i to, co by dělat neměl);
- **liberální** (každému povoluje dělat vše, až na věci explicitně zakázané);
- **opatrná**, resp. racionální (zakazující dělat vše, co není explicitně povoleno, je nákladnější na zavedení, avšak zaručuje vyšší stupeň bezpečnosti);
- **paranoidní** (zakazující dělat vše potenciálně nebezpečné, tedy i to, co by nemuselo být explicitně zakazováno, zaručuje nejvyšší stupeň bezpečnosti).

Zabezpečujeme-li IS, je třeba nejprve stanovit **bezpečnostní cíle** a způsob jejich dosažení. Bezpečnostní cíle jsou dílčí přínosy k bezpečnosti, kterou dosahuje IS z hlediska udržení důvěrnosti, integrity, dostupnosti, odpovědnosti uživatele IS za jeho činnost v něm a zpracování informací v souladu s požadavky právních předpisů, norem, smluv a s nimi spjatých bezpečnostních požadavků, interních předpisů, nadřízené bezpečnostní politiky apod. Abychom mohli bezpečnostní cíle stanovit, je potřeba znát zranitelná místa, jak lze tato zranitelná místa využitkovávat, možné formy útoků, kdo může zranitelná místa využitkovat nebo jejich prostřednictvím způsobit neúmyslnou škodu, kdo jsou potenciální útočníci, s jakou pravděpodobností dochází k útoku, jak se lze proti útokům bránit a jaké škody mohou útoky způsobit.

Pro dosažení bezpečnostních cílů se používají tzv. bezpečnostní funkce (bezpečnostní opatření). **Bezpečnostní funkce** přispívá buďto ke splnění jednoho bezpečnostního cíle, nebo ke splnění několika bezpečnostních cílů. Mohou být administrativního, fyzického nebo logického typu, tj. mohou být implementovány takovými mechanismy, jakými jsou administrativní akce, hardwarová zařízení, procedury, programy.

Pro implementaci bezpečnostních funkcí se používá bezpečnostních mechanismů. **Bezpečnostní mechanismus** je logika nebo algoritmus, který technicky, logicky, fyzicky nebo administrativně implementuje bezpečnostní funkci. Mohou být při implementaci různými způsoby kombinovány tak, aby implementace byla co nejvíce přesná, účinná a ekonomická. Bezpečnostní funkce mohou být implementovány jediným mechanismem nebo i více mechanismy současně, např. přístup k aplikacím může být kontrolován hardwarovým klíčem a heslem. Podle ITSEC můžeme bezpečnostní mechanismy členit podle toho, jak silným útokům jsou bezpečnostní mechanismy schopné odolávat a podle způsobu implementace je kategorizujeme na základní, střední a velké síly.

7.1 INFORMAČNÍ KONCEPCE - ŘÍZENÍ BEZPEČNOSTI ISVS

Pro řízení bezpečnosti IS se v rámci Informační koncepce (viz kap. 5.1) stanovují dlouhodobé cíle bezpečnosti, které se transformují do konkrétních požadavků na bezpečnost, a následně se stanovuje plán, jak má být těchto cílů resp. naplnění požadavků dosaženo. Každý požadavek by se měl opírat o projektovou bezpečnostní a provozní bezpečnostní dokumentaci. Základní požadavky stanovuje Vyhláška č. 529/2006 Sb.[19]

DLOUHODOBÉ CÍLE

Dlouhodobé cíle můžeme rozdělit na oblasti zajištění bezpečnosti:

- dat;
- služeb;
- technických a programových prostředků.

BEZPEČNOST DAT

Dostupnost dat by měla být zajištěna vhodnou kombinací technických a programových prostředků úměrně potřebě dat. Patří sem např. použití diskových polí, clusterů, i softwarových nástrojů. Je nutné stanovit politiku zálohování a archivací (periodicita, způsoby zálohování a archivací dat, způsoby uložení dat apod.

Důvěrnost dat představuje zabezpečení dat tak, aby k nim oprávněné osoby měly přístup v rozsahu svého oprávnění (umožnění čtení popř. manipulaci a úpravy) a neoprávněné osoby neměly přístup vůbec. K datům je nutné zavést řízený přístup. Jde o aplikace základních atributů zabezpečení přístupu:

- identifikace, každý uživatel je jednoznačně identifikován jménem nebo kódem;
- autentizace, uživatel prokáže svoji totožnost (heslem, otiskem prstu apod.);
- autorizace, každý uživatel je oprávněn k úkonům odpovídajícím roli, kterou zastává.

Integrita dat je zajištěna volbou vhodných nástrojů pro zpracování dat (řízení databází zajišťující referenční integritu, archivační nástroje atd.).

BEZPEČNOST SLUŽEB

Dostupnost služeb je zajištěna vhodnou kombinací technických a programových prostředků úměrně potřebnosti služeb. Patří sem prostředky zajišťující odolnost proti výpadku elektrické energie, komunikačních sítí, hardwarových a softwarových prvků apod. a také nástroje pro ochranu proti útokům atd.

Důvěrnost služeb vyžaduje, aby procesy služeb a přenosu informací mezi zdrojem a cílem byly chráněny odpovídajícím způsobem. Opět se jedná o aplikaci základních atributů zabezpečení přístupu, tedy identifikace, autentizace a autorizace.

Integrita služeb se týká např. sdílení informací o uživateli, sdílení služeb datových zdrojů apod. Tento bezpečnostní cíl pokrývá zajištění integrity služeb samostatných a spolupracujících systémů.

[19] Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy.

BEZPEČNOST TECHNICKÝCH A PROGRAMOVÝCH PROSTŘEDKŮ

Zabezpečení **dostupnosti technických prostředků** zahrnuje záložní zdroje napájení, záložní síťová připojení, duplikace hardware duplikováním, popř. násobení důležitých prvků, umístění záložních zařízení do geograficky různých lokalit atd.

Dostupnost programových prostředků zahrnuje zejména používání výrobcem certifikovaných softwarových komponent, testování a včasnou aplikaci záplat programového vybavení, nasazení prostředků monitorování provozu a včasného upozornění jak na prostředky vlastního informačního systému, tak i na prostředky síťové infrastruktury, použití nástrojů softwarové ochrany (antiviry apod.), logické umístění do bezpečné zóny sítě apod.

Důvěrnost technických prostředků zahrnuje především fyzickou bezpečnost (umístění technických prostředků do zabezpečeného prostoru, fyzická ochrana před riziky prostředí, další opatření), zabezpečení telekomunikační infrastruktury (nastavení switchů, routerů apod.).

Důvěrnost programových prostředků se týká zejména zajištění odolnosti proti úmyslně či neúmyslně chybným vstupním datům (např. odolnost proti buffer overflow, SQL injection apod. útokům), zajištění ochrany proti parazitním kódům, zajištění ochrany proti podvržení identity spolupracujících systémů.

Integrita technických prostředků se týká zejména: ochrany proti přetížení a proti zničení či poškození.

Integrita programových prostředků zahrnuje ochranu proti smazání softwarové komponenty, modifikaci či podvržení softwarové komponenty a modifikaci konfigurace softwarové komponenty.

POŽADAVKY NA BEZPEČNOST ISVS

Požadavky na bezpečnost obsahují souhrn požadavků, které jsou konkretizací obecných cílů bezpečnosti. Požadavky by měly být pokud možno měřitelné a měly by být vázány na cíle bezpečnosti, k jejichž naplnění směřují. Požadavky mohou být specifické pro jeden IS nebo společné pro několik IS daného správce, resp. záměry na vybudování nových IS nebo jejich skupiny. Součástí vyhodnocování IK by mělo být mj. též vyhodnocování míry a způsobu naplnění stanovených požadavků na bezpečnost IS. Konkrétní bezpečnostní požadavky by měly být výsledkem bezpečnostní analýzy (analýza rizik) a návrhu opatření odpovídajících míře rizika velikosti s ním svázané škody.

PLÁN ŘÍZENÍ BEZPEČNOSTI ISVS

Plán řízení bezpečnosti obsahuje popis činností, které orgán veřejné správy vykonává pro naplnění stanovených cílů a uplatnění konkrétních požadavků. Součástí je také předpokládaný časový harmonogram plnění cílů a požadavků v oblasti bezpečnosti. Plán bezpečnosti má obdobnou strukturu jako plán kvality:

- stanovení cílů bezpečnosti;
- stanovení požadavků na bezpečnost;
- implementace požadavků na bezpečnost;
- prověrka dodržování požadavků na bezpečnost;
- vyhodnocení řízení bezpečnosti.

7.2 BEZPEČNOSTNÍ DOKUMENTACE INFORMAČNÍHO SYSTÉMU VEŘEJNÉ SPRÁVY

Součástí provozní dokumentace dle Vyhlášky 529/2006 Sb.[20] je bezpečnostní dokumentace informačního systému veřejné správy (viz kap. 5.2.4). Tvoří ji:

- bezpečnostní politika ISVS;
- bezpečnostní směrnice pro činnost bezpečnostního správce systému.

BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika musí být vytvořena, vždy pokud systém má vazby s ISVS jiného správce nebo pokud orgán veřejné správy (správce ISVS) není provozovatelem tohoto systému. Obsahuje popis bezpečnostních opatření, která orgán veřejné správy uplatňuje při zajišťování bezpečnosti tohoto systému a která odpovídají požadavkům na bezpečnost stanoveným v informační koncepci.

Jedná se spíše o globálnější pohled na informační systém veřejné správy, uvedená opatření mohou být i organizační či personální (např. je uvedeno, že čipovou kartu, která se používá pro označování výstupů z informačního systému, ukládá pracovník oddělení informatiky každý večer do určeného trezoru – nejedná se tedy přímo o funkcionalitu systému; dalším příkladem může být povinnost určeného zaměstnance pravidelně zálohovat data a určení místa uložení záloh).

BEZPEČNOSTNÍ SMĚRNICE

Bezpečnostní správce systému je zaměstnanec nebo jiná fyzická osoba, která zajišťuje kontrolu bezpečnosti ISVS a provádí další činnosti, které mají zajistit bezpečnost daného IS. Činnost bezpečnostního správce systému omezuje činnost správce systému.

Roli správce systému a současně roli bezpečnostního správce systému může vykonávat jedna fyzická osoba pouze v případě, že se jedná o informační systém veřejné správy, který nemá vazby s informačním systémem veřejné správy jiného správce, a orgán veřejné správy stanovil a uplatňuje odpovídající bezpečnostní opatření, která vyloučí rizika, která by z vykonávání obou rolí jednou fyzickou osobou mohla vyplývat. Ke spojení rolí se přistupuje v případě menších systémů, kdy rozdělení funkce správce a bezpečnostního správce by bylo neefektivní. Zároveň musí být uplatněna bezpečnostní opatření, která eliminují rizika spojená se sloučením těchto rolí (např. kontrola činnosti pověřené osoby, vedení a kontrola záznamů o veškerých zásazích této osoby v systému apod.).

Pokud roli správce systému a roli bezpečnostního správce sytému vykonává jedna fyzická osoba, lze sloučit bezpečnostní směrnici pro činnost bezpečnostního správce systému se systémovou příručkou (viz kap. 5.2.4).

Bezpečnostní směrnice pro činnost bezpečnostního správce systému podle 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. Tyto funkce slouží např. ke kontrole událostí, které v systému proběhly nebo ke sledování neoprávněných pokusů přistoupit do systému apod. Zároveň definuje pro každou roli souhrn určených činností a potřebných oprávnění pro provádění těchto činností v ISVS.

[20] Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy.

ROZSAH PROVOZNÍ DOKUMENTACE PŘEDKLÁDANÉ PŘI ATESTACI

Orgán veřejné správy předkládá při atestaci bezpečnostní politiku ISVS, pokud je povinen ji zpracovat. Předkládání jiných částí provozní dokumentace není nutné, slouží k operativnímu řízení provozu IS, proto podléhají relativně častým změnám. Atestace jsou zaměřeny na problematiku dlouhodobého řízení IS.

7.3 KRYPTOGRAFIE A ELEKTRONICKÝ PODPIS

Většina principů autentizace uživatele je založena na šifrování dat.

7.3.1 KRYPTOGRAFIE

Šifrování je nezbytnou potřebou transparentních mechanismů pro uživatele. Státní a veřejná správa je jednou z oblastí, kde se pracuje s velmi citlivými informacemi. Kryptografie, jako jeden z důležitých bezpečnostních mechanizmů, se používá k zabezpečení:

- důvěrnosti (utajení) informace, tedy ochrany před neautorizovaným zpřístupněním důvěrné informace;
- prokazování integrity informace, čili ochrany před neautorizovanými změnami dat nebo proti nasazení virů apod.;
- autentizaci, tj. prokázání totožnosti subjektu;
- řízení přístupu k objektům (datům, programům atd.);
- zaručeného prokazování původu zprávy, nepopiratelnosti.

Šifrování spočívá v převedení zprávy (otevřeného textu) do některé z možných reprezentací (šifrového textu). Cílem šifrování je skrýt obsah zprávy před každým, komu tato zpráva není určena. Konkrétní šifrový text je určen klíčem.

NEPŘEHLÉDNĚTE

Kryptografický systém si můžeme představit jako pětici podmnožin:

- konečná množina srozumitelných textů - prostor zpráv,
- konečná množina možných šifer - prostor šifer,
- konečná množina možných klíčů - prostor klíčů,
- množina šifrovacích funkcí (pravidel, algoritmu),
- množina dešifrovacích funkcí.
-

Samotné šifrování je založeno na dvou komponentách:

- šifrovací algoritmus;
- klíč.

Šifrovací (kryptografický) algoritmus je matematická funkce, která převádí srozumitelný text na nesrozumitelný šifrový text. K zašifrování otevřeného textu používají šifrovací algoritmy jako vstup klíč.

Při využití jednoho konkrétního klíče (z množiny možných klíčů) získáme pro určitý otevřený text jednu jeho konkrétní transformaci na šifrový text. Zpětnou transformaci šifrového textu na otevřený text můžeme provést pouze pokud potom známe správný klíč. Tím, že množina možných klíčů je dostatečně veliká, zajistíme, že pro narušitele není možné získat otevřený text prostým ozkoušením všech možných klíčů. Pravděpodobnost volby každého konkrétního klíče by měla být stejná.

V současných kryptografických systémech mají klíče vlastnost difuze, čili při změně jednoho bitu klíče dojde v každém bitu šifrového textu k jeho změně s pravděpodobností jedna polovina.

Délkou klíče rozumíme počet bitů jednotlivého klíče. Tento počet je roven logaritmu se základem 2 velikosti množiny klíčů.

NEPŘEHLÉDNĚTE

Kryptografie představuje mechanizmus, který je tvořen:

- dvěma samostatnými algoritmy:
  - algoritmus šifrování,
  - algoritmus dešifrování,
- kryptografickým klíčem, který spolu se šifrovanou zprávou tvoří vstupní parametry algoritmů šifrování a dešifrování.

Jak klíč tak použité funkce mají rozhodující význam pro šifrování. V současné době se používají dvě základní třídy šifrovacích algoritmů:

- symetrické;
- asymetrické.

SYMETRICKÁ KRYPTOGRAFIE

Při symetrické kryptografii komunikující partneři používají stejný kryptografický klíč. Hovoříme také o kryptografii s tajným klíčem. Znalost tajného klíče může sloužit jako důkaz identity.

Různé symetrické algoritmy používají různé délky klíčů. Delší klíč obvykle znamená větší bezpečnost algoritmu. Symetrickou kryptografii mimo služby zajištění důvěrnosti lze použít i pro autentizaci.

Problematické je předání šifrovacího klíče mezi komunikujícími před začátkem komunikace. K tomu je nutné použít důvěryhodného, chráněného, neveřejného kanálu, nejlépe osobního předání.

ASYMETRICKÁ KRYPTOGRAFIE

Při asymetrické kryptografii se klíče komunikujících partnerů liší. Klíče musí splňovat dvě důležité vlastnosti:

- klíče jsou navzájem neodvoditelné, čili ze znalosti jednoho klíče nemůžeme vypočíst druhý;
- zpráva se jedním klíčen zašifruje, dešifrování stejným klíčem už není možné a provede se až druhým klíčem.

Příkladem aplikace je kryptografie s veřejným klíčem a soukromým klíčem. Veřejný klíč se zveřejní, soukromý je nutné udržet v tajnosti a bezpečí.

PŘÍKLAD 3

Potřebuje-li odesilatel předat příjemci zašifrovanou zprávu, zašifruje data jeho veřejným klíčem. Takto upravená data zašle příjemci, který je rozšifruje svým soukromým klíčem. Z principu asymetrické kryptografie plyne, že to není možné provést žádným jiným klíčem.

HYBRIDNÍ ŠIFROVÁNÍ

Symetrické šifra je lepší pro zajištění důvěrnosti, asymetrická šifra pro zajištění integrity a neodmítnutelnosti. Hybridní šifrování spojuje výhody obou řešení.

Nejprve se náhodně vygeneruje klíč pro symetrickou šifru, kterým se zašifruje zpráva. Symetrický klíč se zašifruje pomocí asymetrické šifry a spolu se šifrovanou zprávou se odešle příjemci. Příjemce nejdříve klíč dešifruje klíč a pak pomocí klíče k symetrické šifře dešifruje i zprávu samotnou.

Výhodou řešení je, že pomocí asymetrické šifry, která má složitější algoritmy a je pomalejší, se dešifruje pouze krátký klíč, zatímco mnohem delší zpráva, se šifruje rychlejším algoritmem pro symetrickou šifru. Bezpečnost systému je závislá na bezpečnosti obou použitých šifer.

CERTIFIKAČNÍ AUTORITA

Důvěru v pravost asymetrických klíčů komunikujících stran poskytuje **certifikační autorita**. Ta vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče). Svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. Certifikační autorita ověří totožnost majitele asymetrických klíčů a digitálně podepíše jeden z dvojice klíčů.

Certifikát představuje datovou strukturu, která je svázána s určitou osobou. Pomocí certifikátu lze tedy tuto osobu jednoznačně identifikovat. Pomocí certifikátu lze ověřit elektronický podpis dané osoby. Součástí vydaného certifikátu většinou jsou:

- identifikátor certifikátu (sériové číslo, nemusí být)
- informace o držiteli certifikátu;
- doba platnosti:
    - datum počátku platnosti;
    - datum konce platnosti certifikátu;
- použitý algoritmus;
- účel použití;
- veřejný klíč;
- atd.

Obsah **certifikátu** je podepsán vydávající certifikační autoritou, aby bylo možné prokázat, že byl touto autoritou skutečně vydán.

Zákonem 227/2000 Sb.[21] definován tzv. **kvalifikovaný certifikát**, který může vydat pouze akreditovaná **kvalifikovaná certifikační autorita**. Ministerstvo vnitra uděluje akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb a přehled udělených akreditací zveřejňuje[22].

Řada neakreditovaných organizací poskytuje své certifikáty, většinou pro potřebu svých systémů, které můžeme nazvat komerční certifikáty.

[21] Zákon č. 227/2000 Sb., o elektronickém podpisu (ve znění pozdějších předpisů).
[22] http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx

VYUŽÍVANÉ ALGORITMY

Seznam využívaných algoritmů nalezneme v Příloze 2 Vyhlášky 194/2009 Sb.[23]:

- RSA 2048 bitů (RFC 3447):
  - iniciály autorů Rivest, Shamir, Adleman;
  - kryptosystémy založené na úloze faktorizace (RSA, Rabin-Williams);
  - algoritmus pro výměnu klíčů a tvorbu elektronického podpisu využívá klíče 512-4096 bitů dlouhé;
  - Ministerstvo vnitra stanovilo od 1. 1. 2010 minimální přípustnou délku kryptografického klíče pro algoritmus na 2048 bitů;
  - bezpečnost RSA je založena na tom, že je obtížné rozložit velká čísla (z nichž každé je součinem dvou velkých prvočísel);
  - šifrování stejné jako dešifrování;
- DSA (FIPS PUB 186-2):
  - Digital Signature Algorithm;
  - kryptosystémy založené na problému diskrétního logaritmu (DSA, Diffie-Hellmanovo schéma pro výměnu klíčů, El-Gamalovo schéma pro šifrování);
  - využívá se u elektronického podpisu;
  - generuje se soukromý klíč i hodnoty nezbytné pro podepisování jednotlivých zpráv, je použit náhodný výstup po předání jednocestné funkci, jednotlivé kroky jsou:
    - vytváření klíčů, nejdříve se vyberou parametry algoritmu, které mohou být sdíleny více různými uživateli systému, pak se vytvoří samotné klíče;
    - podepisování;
    - ověřování.
- ECDSA-Fp (ANSI X9.62) a ECDSA-F2m (ANSI X9.62):
  - Elliptic Curve Digital Signature Algorithm;
  - varianty DSA protokolu, která využívá eliptických křivek, používá se k digitálním podpisům.

7.3.2 ELEKTRONICKÝ PODPIS

NEPŘEHLÉDNĚTE

Při předávání dokumentů je třeba zajistit jejich:

- autentičnost (původ, autora);
- neporušenost (integritu);
- nepopiratelnost (podepsaná strana nemůže později popřít, že daný dokument podepsala).

Pojem **elektronický podpis** do našeho právního řádu zavedl Zákon č. 227/2000 Sb., zákon o elektronickém podpisu (ve znění pozdějších předpisů). Tímto pojmem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a umožňují ověření totožnosti podepsané osoby.

Je tvořen řetězcem bajtů, který je připojen k podepisovanému dokumentu. Délka tohoto řetězce bývá obvykle 50 až 300 bajtů podle použitého algoritmu a požadovaného stupně

[23] Vyhláška 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

bezpečnosti a nezávisí na délce podepisovaného dokumentu. Od podepsaného dokumentu se nedá oddělit a následně použít k podepsání jiného dokumentu. To v podstatě vylučuje možnost zneužití podpisu na jiný dokument, než pro který byl původně určen. Jedna osoba může mít několik různých elektronických podpisů (např. soukromý a v zaměstnání). Vyhláška č. 212/2012 Sb.[24] stanovuje, že údaj, který umožňuje jednoznačnou identifikaci podepisující osoby, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295.

V Zákoně č. 227/2000 Sb. se můžeme setkat také s pojmem **elektronická značka** (EZ), což jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují požadavky:

- jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu;
- byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou;
- jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Prvním krokem vytváření elektronického podpisu je vytvoření tzv. otisku (hash) pomocí **hash funkce**. Do výpočtu se zahrnují údaje o:

- podepisující se osobě;
- podepisovaném dokumentu (včetně jeho obsahu).

Seznam využívaných **hashovacích funkcí** nalezneme v Příloze 2 Vyhlášky 194/2009 Sb.:

- SHA-1 (FIPS 180-2):
  - Secure Hash Algorithm,
  - rozsekává vstupní zprávu na bloky o délce 512 bitů, poslední blok zprávy doplňuje a zarovnává, včetně přidání údaje o délce zprávy, na nějž je vyhrazeno posledních 64 bitů;
  - vytváří 160 bitový obraz zprávy s maximální délkou 2^{64}-1 bitů;
  - je ukončeno jeho používání pro oblast elektronického podpisu;
- SHA-2 - 256, 384, 512 bitů (FIPS 180-2):
  - společné označení pro algoritmy SHA-224, SHA-256, SHA-384 a SHA-512;
  - délky otisku pojmenovaných jsou uvedeny v jednotlivých názvech algoritmů;.
  - Ministerstvo vnitra stanovilo, že kvalifikovaní poskytovatelé certifikačních služeb od 1. 1. 2010 vydávají kvalifikované certifikáty podporující některý z algoritmů SHA-2;
  - používá ho informační systém datových schránek pro certifikáty;
- RIPEMD-160:
  - na vstupu přijímá blok dat do délky 2^{64} bitů;
  - rozsekává vstupní zprávu na bloky o délce 320 bitů, poslední blok zprávy doplňuje a zarovnává;
  - vytváří 160 bitový obraz zprávy.

[24] Vyhláška č. 212/2012 Sb., vyhláška o ověřování platnosti zaručeného elektronického podpisu

Z libovolně velké zprávy či dokumentu se vypočte otisk pevné velikosti. Ten se zašifruje soukromým klíčem podpisující osoby. Tím vzniká elektronický podpis, který se připojí k dokumentu.

Příjemce při ověřování dokumentu pomocí veřejného klíče odesílatele dešifrováním elektronického podpisu zjistí otisk daného dokumentu, který byl pořízen před podpisem. Pomocí hash funkce vypočte otisk přijatého dokumentu a pokud oba otisky souhlasí, znamená to, že po podpisu nebylo do dokumentu zasahováno.

Jako vyšší formu elektronického podpisu lze chápat zaručený elektronický podpis. Náležitosti zaručeného elektronického podpisu upravuje především zákon č. 227/2000 Sb..

NEPŘEHLÉDNĚTE

Zaručeným elektronickým podpisem (ZEP) je elektronický podpis, který splňuje následující požadavky:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

K podepisování nebo označování dokumentu v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči:

- státu;
- územnímu samosprávnému celku;
- právnické osobě zřízené zákonem, zřízené nebo založené státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem;
- právnické osobě nepatřící mezi předchozí a vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti;
- fyzické osobě vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti;

lze použít pouze **uznávaný elektronický podpis** nebo **uznávanou elektronickou značku.**

Uznávaným elektronickým podpisem se rozumí:

- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby;
- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je

poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie[25].

Uznávanou elektronickou značkou se rozumí elektronická značka založená na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

Časové razítko spojuje dokument v elektronické podobě s časovým okamžikem jeho vzniku a zaručuje, že konkrétní data v elektronické podobě existovala před daným časovým okamžikem. „Razítkuje" elektronický dokument v konkrétním čase a je vhodným doplňkem elektronického podpisu.

Kvalifikované časové razítko (KČR) je podle zákona č. 227/2000 Sb.[26] datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb. Využívá se u elektronických dokumentů nebo dat, u kterých je nutné jednoznačné doložení času. Propojuje elektronický dokument s okamžikem jeho vzniku, což zaručuje existenci konkrétních dat v elektronické podobně v daný okamžik.

U časových razítek je také nejprve vytvořen otisk (hash) celé zprávy či dokumentu a ten je pak odeslán poskytovateli služby časových razítek. Tento poskytovatel přidá garantovaný údaj o čase a vše zašifruje svým soukromým klíčem. Výsledek, představující samotné časové razítko, vrátí žadateli zpět a ten jej připojí (stejně jako elektronický podpis) k dokumentu, ze kterého byl vytvořen otisk.

Časové razítko vypovídá pouze o tom, že příslušná zpráva či dokument existovala ještě před okamžikem, kdy byl otisk zaslán k vytvoření časového razítka. Nepotvrzuje však, od koho požadavek na časové razítko přišel, tedy zda data prošla např. systémem datových schránek. To potvrzuje až elektronický podpis, ale bez časového razítka je časem problém prokazovat jeho platnost.

Časové razítko prodlouží platnost dokumentu s elektronickým podpisem minimálně o 5 let. Lze ho využít tam, kde je nutné prokázat, jak elektronický dokument vypadal v určitém okamžiku, např.:

- při archivaci elektronických dokumentů;
- při elektronických transakcích;
- pro elektronické formuláře atd.

OVĚŘENÍ PLATNOSTI

Postupy pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka stanovuje Vyhláška č. 212/2012 Sb.

Platnost zaručeného elektronického podpisu, kterým je podepsána datová zpráva, nebo elektronické značky, kterou je označena datová zpráva, se ověřuje pomocí kryptografického asymetrického algoritmu a kryptografické hashovací funkce, jejichž standardy jsou uvedeny v přílohách vyhlášky, které odpovídají schématu použitému při vytváření zaručeného elektronického podpisu nebo elektronické značky.

[25] Rozhodnutí Komise Evropských společenství 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst" podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu.
[26] Zákon č. 227/2000 Sb., o elektronickém podpisu (ve znění pozdějších předpisů).

Ověření platnosti kvalifikovaného certifikátu (KC) nebo kvalifikovaného systémového certifikátu (KSC) zahrnuje ověření:

- zda je KC nebo KSC v intervalu doby platnosti;
- platnosti elektronické značky označující KC nebo KSC;
- zda KC nebo KSC nebyl zneplatněn, a ověření elektronické značky, kterou kvalifikovaný poskytovatel certifikačních služeb označil seznam zneplatněných certifikátů nebo informaci o stavu KC, a KSC poskytovatele[27];
- platnosti všech KSC a elektronických značek označujících KSC v certifikační cestě[28];
- zda byl certifikát vydán jako KC nebo jako KSC[29].

Ověření platnosti kvalifikovaného časového razítka zahrnuje ověření:

- vazby mezi datovou zprávou a připojeným KČR;
- platnosti elektronické značky označující KČR;
- platnosti KSC, na kterém je založena elektronická značka označující KČR.

Ověření vazby mezi datovou zprávou a připojeným KČR se provádí podle standardu kryptografické hashovací funkce odpovídající funkci použité při výpočtu otisku datové zprávy uvedeného v KČR.[30]

Okamžikem, ke kterému je ověřována platnost KC nebo KSC, je okamžik doručení datové zprávy, případně nejčasnější časový okamžik, ve kterém již prokazatelně existoval zaručený elektronický podpis nebo elektronická značka založené na certifikátu, jehož platnost je ověřována. Není-li KC nebo KSC v daném okamžiku platný, a je-li k datové zprávě podepsané elektronickým podpisem nebo označené elektronickou značkou připojeno platné KČR, ověřuje se platnost KC nebo KSC k časovému údaji uvedenému v kvalifikovaném časovém razítku.

Okamžikem, ke kterému je ověřována platnost KSC, na kterém je založena elektronická značka označující KČR, je okamžik doručení datové zprávy, případně nejčasnější časový okamžik, ve kterém již prokazatelně existovalo KČR. Není-li KSC, na kterém je založena elektronická značka označující KČR, v okamžiku, ke kterému je ověřována jeho platnost,

[27] Ověření se provádí v souladu s certifikační politikou poskytovatele, který certifikát vydal. Je-li k ověření užit seznam zneplatněných certifikátů, pro ověření je rozhodným seznamem poslední seznam, který byl vydán ve lhůtě 24 hodin od okamžiku, ke kterému je platnost certifikátu ověřována, případně každý následující seznam vydaný před koncem intervalu platnosti ověřovaného certifikátu. Pokud lhůta 24 hodin přesahuje interval platnosti ověřovaného certifikátu, jsou rozhodnými seznamy všechny seznamy vydané od posledního seznamu vydaného v intervalu platnosti certifikátu po poslední seznam, který byl vydán ve lhůtě 24 hodin od okamžiku, ke kterému je platnost certifikátu ověřována.

[28] Hierarchicky uspořádaná posloupnost certifikátů, která zahrnuje ověřovaný kvalifikovaný certifikát nebo ověřovaný kvalifikovaný systémový certifikát a kvalifikovaný systémový certifikát poskytovatele, na němž je založena elektronická značka ověřovaného kvalifikovaného certifikátu nebo ověřovaného kvalifikovaného systémového certifikátu, každý další kvalifikovaný systémový certifikát poskytovatele, na kterém je založena elektronická značka kvalifikovaného systémového certifikátu poskytovatele, který byl naposledy zahrnut do certifikační cesty, a končí kvalifikovaným systémovým certifikátem poskytovatele označeným elektronickou značkou, která je založena na něm samém. (§ 4 odst. 3 vyhlášky)

[29] Ověření se provádí ověřením kvalifikovaného systémového certifikátu poskytovatele, na kterém je založena elektronická značka ověřovaného certifikátu, v evidenci vydaných kvalifikovaných systémových certifikátů, které používá poskytovatel, vedené MV. Pokud byl certifikát vydán poskytovatelem certifikačních služeb usazeným v jiném státu, považuje se za kvalifikovaný, byl-li vydán v rámci služby vydávání kvalifikovaných certifikátů vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle přímo použitelného předpisu Evropské unie.

[30] Vyhláška č. 212/2012 Sb., § 5

platný, a bylo-li k ověřovanému KČR nebo k datové zprávě opatřené ověřovaným KČR následně připojeno v době platnosti tohoto KSC další KČR označené elektronickou značkou založenou na KSC, který byl v daném okamžiku, ověřuje se platnost KSC, na kterém je založena elektronická značka označující ověřované KČR k časovému údaji uvedenému v následně připojeném KČR.

Je-li k ověřovanému KČR nebo k datové zprávě opatřené ověřovaným KČR připojeno více dalších KČR, lze předchozím postupem ověřit platnost KČR k časovému údaji uvedenému v KČR připojeném následně po ověřovaném KČR.[31]

7.4 BEZPEČNOST INFORMAČNÍHO SYSTÉMU DATOVÝCH SCHRÁNEK

Informační systém datových stránek (ISDS) je informačním systémem veřejné správy. Proto musí splňovat veškeré požadavky, kladené na tyto informační systémy zákon 365/2000 Sb., který klade především důraz na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných IS. Je však jasné, že ISDS musí i celou řadu dalších požadavků.

Řízení bezpečnosti IS jsme se zabývali v kap. 0.

7.4.1 BEZPEČNOSTNÍ KRITÉRIA

ISDS a informace, které poskytuje, by měly splňovat kritéria

DOSTUPNOST

Zahrnuje včasný přístup k údajům obsaženým v datových zprávách nebo k dalším službám ISDS, neodmítnut přístupu autorizovaným uživatelům a nebránění zpracovávání příkazů autorizovaných subjektů. Slouží tedy k zajištění dostupné, bezpečné a vysoce efektivní elektronické komunikace mezi držiteli datových schránek a zachování kontinuity dat.

Krátkodobé výpadky nebo krátká nedostupnost mohou být přípustné, ale požadavky na dostupnost by měly být stanoveny provozovatel datových schránek v provozním (provozován nepřetržitě, s výjimkou plánovaných odstávek, které jsou předem zveřejňovány).

BEZPORUCHOVOST

Úzce souvisí s dostupností. Jde o schopnost informačního systému zachovat si specifickou úroveň výkonu při používání systému za stanovených podmínek. Systém musí vykazovat:

- zralost, tedy schopnost vyvarovat se poruchám (selháním) v důsledku závad nebo důsledky takovýchto závad minimalizovat;
- odolnost vůči vadám, schopnost zachovat si při selhání systému nebo při nedodržení požadovaného rozhraní ze strany uživatele určitou úroveň výkonu, popř. poskytovaných služeb;
- zotavení, čili schopnost obnovit úroveň výkonu a zachovat data po odstranění poruchy.

[31] Vyhláška č. 212/2012 Sb., § 3

INTEGRITA

Integrita shrnuje požadavky, týkající se přesnosti a kompletnosti informace. Zajištění integrity dokumentu znamená zajištění jeho neměnnosti v průběhu zpracování a přenosu. Úroveň ochrany integrity dat odráží přesnost a spolehlivost IS. Ochranné mechanismy zabraňují neautorizovanému přístupu nebo nepatřičné modifikaci dat. Informaci není možné v elektronickém dokumentu pozměnit tak, aby přijímací strana o této změně nevěděla.

ISDS užívá kombinaci kryptografických mechanismů (viz kap. 7.3), ty umožňují následnou detekci případné změny datového obsahu. Pokud by byla detekována změna datového obsahu, dokument je považován za nedůvěryhodný.

DŮVĚRNOST

Důvěrnost představuje požadavky na ochranu důležitých informací proti neautorizovanému použití (prozrazení). Důvěrné informace obsažené v elektronickém dokumentu nesmí být přístupné neautorizovaným osobám. Zajištění důvěrnosti dat znamená, že jakýkoliv neautorizovaný subjekt nemůže vniknout do systému. Systém tady musí sledovat oprávnění konkrétní osoby k přístupu do informačního systému a především ochranu před neoprávněným vniknutím do systému. Tím je naplněn požadavek, že doručování dokumentů prostřednictvím datových schránek musí odpovídat ústavnímu principu „neporušitelnosti listovního tajemství“ („předávání dokumentu v zalepené obálce“ po celou cestu od odesílatele k příjemci).

Důvěrnosti dokumentů doručovaných prostřednictvím datových schránek je dosaženo pomocí šifrování (viz kap. 7.3), mechanismy jsou obdobné, jako u aplikací elektronického bankovnictví apod.

IDENTIFIKACE, AUTENTIZACE A AUTORIZACE

Abychom do systému umožnili přístup pouze oprávněnému uživateli, musíme dostatečně ověřit jeho identitu. Nejdříve musí proběhnout identifikace, v níž uživatel prohlašuje, kým je, a tuto skutečnost je nutné potvrdit. Autentizace znamená ověřování identity, čili pravosti deklarované identity osoby přistupující do IS. Autorizace je proces, při němž se ověřují práva pro přístup do určité oblasti pro vykonání akce. Autentizace je základním předpokladem autorizace (podrobněji viz kap. 8.1).

U ISDS je primárním autentizačním prostředkem uživatelské jméno a příslušné bezpečnostní heslo (minimálně 8 znaků s komplikovanou strukturou minimálně 1 velkého písmena, jednoho malého písmena jednou číslicí). Tyto údaje jsou pro první přihlášení generovány jeho provozovatelem a je vyžadována jejich změna po prvním přihlášení. Navíc je automaticky vynucována změna hesla každých 90 dní. Dalším bezpečnostním opatřením posilující autorizaci je zablokování přístupu k datové zprávě po pěti chybných pokusech přihlášení.

NEODMÍTNUTELNOST ODPOVĚDNOSTI

Subjekty využívající elektronický dokument se nemohou zbavit přímé odpovědnosti před nezávislou třetí stranou za odeslání zprávy. Standardní technologií zajišťující neodmítnutelnost odpovědnosti je elektronický podpis (viz. kap. 7.3).

URČENÍ PŘESNÉHO ČASU

Označení datové zprávy přesným časem je nezbytné. Z hlediska úkonů prováděných v rámci informačního systému datových stránek je nezbytné zaznamenávat dobu, kdy

proběhly, s přesností na sekundy. Souvisí to s platností certifikátů a v závislosti na tom i elektronických podpisů, protože vypršení jejich platnosti může vést ke zneplatnění úkonu.

Datové zprávy mnohdy mají obsah, u kterého je rozhodující datum odeslání, popř. datum převzetí. Jedná se především o záležitosti správního nebo soudního řízení.

Nezbytným nástrojem pro zajištění tohoto požadavku je elektronický podpis. Čas transakce dokazuje časové razítko. Podrobněji se elektronickým podpisem zabýváme v kap. 7.3.

BEZPEČNÝ KLÍČ

Bezpečný klíč k datové schránce zajišťuje vyšší stupeň bezpečnosti při přístupu k datovým schránkám a umožňuje elektronické dokumenty v příloze datových zpráv opatřit zaručeným elektronickým podpisem. Jedná se o USB token, který slouží k bezpečnému uložení soukromého klíče a certifikátu. K uloženému soukromému klíči se může dostat pouze jeho uživatel, který vlastní příslušný software pro komunikaci s tokenem a zná PIN, pomocí kterého k soukromému klíči, uloženém na tokenu přistupuje. Je rovněž zajištěno, že soukromý klíč nemůže být z tokenu zkopírován ani v případě, že jej vlastník ztratí, a není jej ani možné získat z počítače, z nějž se uživatel hlásí do systému. Bezpečné klíče k datové schránce dělíme na:

- přístupové, jsou určeny pro zákazníky, kteří chtějí pouze zvýšit bezpečnost přístupu ke svým datovým schránkám nebo pro zákazníky, kteří jsou již majiteli kvalifikovaného certifikátu;
- podpisové, jsou určeny pro zákazníky, kteří jsou již majiteli komerčního certifikátu a chtějí získat kvalifikovaný certifikát a USB token pro bezpečné uložení soukromých klíčů a certifikátů.

8 IDENTIFIKACE

Pro bezpečné fungování jakéhokoliv systému je spolehlivá nezbytná identifikace. My se budeme zabývat identifikací osob v různých oblastech souvisejících se státní a veřejnou správou.

8.1 IDENTIFIKACE, AUTENTIZACE, AUTORIZACE

8.1.1 IDENTIFIKACE

Obecně řečeno se jedná o přiřazení známé veličiny v rámci systému neznámé entitě, takže ta se stane systému známou. Zmíněná známá veličina se nazývá identifikátorem (často označovaným ID), což je ve většině případů jméno nebo nějaké kódové označení. Aby nedocházelo ke komplikacím, je požadováno, aby identifikátor byl jedinečný alespoň v rámci daného systému.

PŘÍKLAD 4

Příkladem identifikace je představení se.

8.1.2 AUTENTIZACE

Tento proces stvrzuje pravost (autenticitu) identifikace. U autentizace osob se jedná o ověření, zda se jedná opravdu hlásicí se osobu, autentizace objektů zpravidla znamená potvrzení jejich původu.

Způsoby autentizace osob můžeme rozdělit na autentizace:

- na základě znalosti vstupních kódů, popř. postupů (textový login, textové heslo, PIN, posloupnost operací atd.);
- na základě vlastnictví identifikačního předmětu (karta, čárový kód, hardwarový klíč identifikační doklad apod.);
- na základě toho, že člověk má určitou jedinečnou vlastnost, biometrika (biologické vlastností uživatele, např. otisky prstů, sítnice apod.).

PŘÍKLAD 5

Při přihlašování do počítačové sítě po identifikaci vložením jména, popř. kódu, se autentizujeme vložením hesla.

Pokud využijeme kombinaci několika způsobů autentizace, hovoříme o vícesložkové autentizaci.

ZNALOSTNÍ IDENTIFIKACE

Současné systémy identifikace uživatele vycházejí stále ještě ze zadávání **hesla, PINu** apod. Tento řetězec si uživatel musí zapamatovat a pokud možno nevyzradit svému okolí.

Každý uživatel se na začátku práce s aplikací musí přihlásit. Přihlášení uživatele proběhne po zadání uživatelského jména a hesla definovaného při registraci do systému.

Ke zvýšení bezpečnosti při styku s informacemi obsaženými v informačním systému slouží vhodně zvolené přístupové heslo, které zamezuje přístupu do aplikace nekompetentním osobám. Volíme heslo, které je dostatečně dlouhé, obsahující kombinaci písmen, cifer popř. dalších povolených znaků, které se dobře pamatuje, ale které je pro ostatní těžko určitelné.

Nedoporučují se hesla, která se dají poměrně lehce vydedukovat z informací o jeho držiteli, např. vlastní jméno, jméno firmy, jméno manželky či datum narození. Na druhé straně není doporučováno používání složitých hesel, která se těžko pamatují. Užívání takových hesel vede autora k vedení poznamenání hesla a záznam se většinou nachází na dostupných místech.

Ke změně hesla je nutné přistoupit, má-li přihlášený uživatel podezření nebo jistotu jeho prozrazení. Také je vhodné provést změnu hesla, je-li již v platnosti delší dobu. Z různých důvodů občas systémy připouštějí hesla společná skupinám uživatelů, tato hesla jsou však málo bezpečná, bývají často vyzrazena.

Znalostní metoda autentizace typu **výzva – odpověď** je založena na tom, že žadatel potvrdí vhodnou odpovědí znalost reakce na výzvu. Bezpečnost této metody je založena na tom, že výzva je vysílána pouze jednou a mění se. Výzva a odpověď jsou spojeny, je vytvořen jejich „otisk“, který je zaslán k ověření. V ověřovacím systému je postupováno stejně
a v případě shody otisků je povolen vstup do systému.

U autentizace **nulové znalosti** (v angl. Zero-Knowledge) žadatel prokazuje pouze znalost hesla, ale nevyzrazuje žádnou jeho část. Při této proceduře jedna strana transakce přesvědčuje s určitou pravděpodobností druhou stranu, že má určitou znalost bez toho, že by prozradila, co zná. Dokazovatel (ten, kdo se autentizuje) je schopný dokázat platnost nějaké skutečnosti právě tehdy, když je tato skutečnost pravdivá. Ověřovatel (ten, kdo vyžaduje autentizaci) na rozdíl od výše zmíněných metod heslo žadatele nezná. Metoda zachovává anonymitu uživatele.

IDENTIFIKAČNÍ PRVKY

NEPŘEHLÉDNĚTE

Mezi identifikační prvky se řadí metody identifikace na základě vlastnictví identifikační prvků, tokenů, což jsou předměty, které autentizují svého vlastníka. Musí být jedinečné a nepadělatelné. Patří sem:

- systémy čárových kódů;
- systémy karet;
- systémy radiofrekvenční identifikace;
- hardwarové klíče;
- elektronické klíče.

Je k dispozici cca 50 druhů čárových kódů, navržených pro nejrůznější aplikace (např. v maloobchodě, výrobě, skladování, přepravě, evidenci objektů a činností apod.). Často posuzován jen vnější efekt čárového kódu (urychlení operací a odstranění chyb obsluhy pokladny) Dobře navržený a správně aplikovaný IS však poskytuje daleko cennější služby, tj. informace např. přesný a okamžitý přehled o struktuře a množství prodaného zboží, o pohybu osob apod.

Značení s využitím čárového kódu je nejpropracovanější formou automatické identifikace vůbec. U nás nejznámější je soustava značení kódem EAN, která znamená jednoznačnou identifikaci jakéhokoliv zboží, které se objeví ve světové obchodní síti, rychle se rozšiřuje i značení sdružených obalových jednotek.

Do systémů karet patří magnetické snímací karty a čipové inteligentní karty.

Magnetické snímací karty se masově využívají v praxi, např. platební karty, docházkové a objednávkové systémy, kopírovací karty atd. Základ karty tvoří magnetický pásek nesoucí identifikační údaje o majiteli karty. Bezpečnost těchto karet je ale malá vzhledem k tomu, že není relativně žádný technický problém pořídit si kopii magnetického proužku.

Čipové inteligentní karty jsou vlastně o miniaturní počítač velikosti kreditní karty, který spolehlivě autentizuje uživatele a chrání data při velmi nízkých nákladech na pořízení a udržování. Mikročip může pracovat jako pouhá paměť typu EPROM (například telefonní karty), nebo jako plnohodnotný mikroprocesor. Mikroprocesor pak poskytuje celou řadu služeb, jako je autentizace pomocí uloženého hesla, či kryptografické operace.

Tyto karty obsahují několik základních prvků zachování bezpečnosti:

- dvoufaktorová autentizace uživatele, přístup do sítě je umožněn, pouze pokud se vloží karta do čtečky a zadá číslo PIN,
- bezpečné uchování digitálních certifikátů na přenosném a programovatelném mediu, karta umožňuje vygenerovat a uložit držitelův soukromý klíč a digitální certifikáty se zabezpečením proti neautorizovanému přístupu nebo kopírování,
- odpovědnost uživatele za elektronické transakce, lze s jistotou určit, kdo a které elektronické operace provádí, uživatelé tak jsou plně zodpovědní za svoje aktivity online,
- strategie single sign-on (jediného přihlášení), zhuštění přihlašovací procedury do jediné metody řeší problém velkého počtu uživatelských jmen hesel bez ztráty na stupni zabezpečení.

Systémy radiofrekvenční identifikace jsou to karty nebo přívěsky, opatřené integrovaným obvodem reagujícím na elektromagnetické a rádiové vlny. Mají vlastní paměť, z níž lze data číst i je do ní rádiem ukládat. Používají se na osobní identifikační karty a identifikační přívěsky pro nejrůznější pohyblivé objekty jako jsou automobily, vagóny, kontejnery a podobně.

Využívají se také u obalových jednotek, pro jejichž identifikaci čárového kódu nelze využít, např. pivních sudy, sudy s nealkoholickými nápoji apod. Hygienické předpisy nařizují vymývání chemickými roztoky, které po čase zničí i etiketu s čárovým kódem. Manipulace s těžkým sudem rovněž přináší riziko poškození identifikačního prvku. V tomto oboru se prosazuje systém automatické identifikace za pomoci radiofrekvenční identifikace.

Radiofrekvenční identifikace umožňuje speciálním snímacím zařízením přečíst číslo (kód) zboží, resp. obalové jednotky. Nositelem kódu je subminiaturní elektronický čip (transpondér), který vysílá příslušný kód na vzdálenost několika centimetrů do svého okolí. Je tvořen elektronickým obvodem, který obsahuje přijímací/vysílací anténu, nabíjecí kondenzátor a paměť obsahují naprogramované údaje. Potřebnou energii většinou čipu dodá čtecí zařízení (vysílač/snímač). Konstrukce čipu pak umožňuje jeho pevné zabudování do tělesa obalové jednotky, kde je zcela chráněn před vlivy prostředí. Životnost moderních radiofrekvenčních čipů je prakticky neomezená a v této aplikaci zdaleka přesahuje životnost obalové jednotky. Systémy radiofrekvenční identifikace

Hardwarový klíč je zařízení, které se připojí na počítač nebo jiné zařízení prostřednictvím paralelního nebo sériového portu, USB apod. Hardwarový klíč lze použít v lokálním nebo síťovém provedení. Lokální klíč musí být připojen přímo na počítači, síťový klíč je připojen většinou na serveru. Některé umožňují přístup k paměti v klíči, který je chráněn pomocí PIN.

Nenalezne-li aplikace klíč, nespustí se nebo spustí pouze omezený modul (informace, demonstrační režim atd.).

Podle úrovně zabezpečení, které nám poskytují je můžeme rozdělit:

- tokeny pouze s pamětí, jsou obdobou mechanických klíčů, paměť může obsahovat jednoznačný identifikační řetězec,
- tokeny udržující hesla, po zadání jednoduchého uživatelského hesla vydají určený kvalitní klíč, který udržují,
- tokeny s logikou, umí zpracovávat jednoduché podněty typu vydej následující klíč, vydej cyklickou sekvenci klíčů, může mít omezen počet použití, pomocí těchto tokenů lze realizovat systém s one-time hesly, k ochraně programů, přístupům k nejrůznějším placeným službám apod.

Hardwarové klíče jsou nejpoužívanější ochranou pro komerční software vyšších cenových kategorií, ochraně aplikací již nainstalovaných na počítači a dat.

Elektronické klíče mohou plnit funkce autentizace a certifikace (jednoznačné potvrzení správnosti předávaných dat) za pomoci šifrování.

Mobilní elektronický klíč se používá prostřednictvím mobilního telefonu. Umožňuje to technologie GSM SIM Toolkit, kterou je dnes vybavena většina přístrojů. Přístup k Mobilnímu Elektronickému klíči v telefonu je chráněn speciálním osobním identifikačním číslem (BPIN), veškerá komunikace s bankou probíhá šifrovaně.

PIN kalkulátor je technicky autonomní zařízení s kódovanou čipovou sadou, která generuje autentizační kód. Kalkulátor pracuje samostatně bez jakéhokoli přímého propojení s počítačem nebo bankou. Na základě vnitřních hodin PIN kalkulátoru (datum a čas) je generován v časovém intervalu cca 30s autentizační kód. Pro každý tento časový interval a PIN kalkulátor je vygenerovaný kód jiný. Ověření správnosti kódu probíhá v zabezpečeném prostředí banky.

Použití SSL umožňuje autentizaci založenou na asymetrické kryptografii (typ 3), konkrétně X.509 certifikátech. Uživatel obdrží osobní certifikát od certifikační autority. S tímto certifikátem se pak může autentizovat v rámci skupiny serverů, které této certifikační autoritě důvěřují. Zřejmou výhodou tohoto přístupu je to, že uživatel může bez rizika použít jeden certifikát pro autentizaci na více místech (web serverech). Za možnou nevýhodu pak lze považovat to, že na rozdíl od jména/hesla, které je možno si lehce zapamatovat, certifikát nemusí mít uživatel vždy po ruce. Osobní certifikáty obsahují základní údaje o uživateli a jsou tedy velmi vhodné pro "instantní registraci", tj. uživatel je ušetřen zdlouhavého vyplňování formulářů, protože základní údaje jsou převzaty právě přímo z certifikátu.

BIOMETRIKA

NEPŘEHLÉDNĚTE

Biometrika je metoda identifikace podle biologických vlastností uživatele. Mezi tyto metody patří:

- otisky prstů;
- oční sítnice;
- oční duhovka;
- tvář;
- hlas;
- podpis;
- geometrie ruky.

Využití **otisků prstů** patří k nejstarším identifikačním technikám, i proto jsou systémy využívající otisků prstů poměrně pokročilé také v oblasti verifikace přístupů do různých prostorů a k počítačům a sítím. Snímače otisků využívají nejčastěji elektrický, optický, ultrazvukový, tepelný a tlakový princip snímání.

Křemíkové snímače, využívající měření elektrické kapacity pomocí matice malých kondenzátorů, tvořených prvky křemíkového čipu a přiloženým prstem. Optické snímače využívají změny odrazu světla v místech dotyku papilárních čar se snímačem. Ultrazvukový snímač využívá různou zvukovou vodivostí papilárních linií a vzduchu v mezipapilárních mezerách. Tepelný a tlakový princip je využíván zejména jako doplněk jiných principů pro ověřování „živosti“ prstů (snímání jejich teploty a pulsace krve).

Metoda identifikace pomocí **sítnice** využívá unikátnosti rozložení krevních cév a vlásečnic v oční sítnici (retina) jednotlivých osob.

Pro sejmutí tohoto rozložení musí být použity speciální snímače, využívající obvykle laserové paprsky, což není příjemné. Sejmutý obraz však obsahuje dostatek informací pro jednoznačnou identifikaci osob.

Metoda identifikace pomocí **duhovky** využívá unikátnosti duhovky lidského oka (iris). Dle udávaných údajů je pravděpodobnost existence dvou shodných duhovek nesrovnatelně menší než u otisků prstů. Vzorec duhovky je téměř neměnný od jednoho roku věku a mění se jen při některých nemocech, rovněž není závislý na rozšíření zornice.

Snímání je prováděno kamerou, uloženou za zrcadlem. Při snímání systém nejprve zaregistruje drobné mimoděčné pohyby pro ověření „živosti“ oka. Pak proběhne zaostření sejmutí a vyhodnocení.

Systémy **na rozpoznávání obličeje** využívají programově simulovaných neuronálních sítí a prvků umělé inteligence. Při videoanalýze napodobují algoritmy lidského mozku. Tím je dodávána novým systémům schopnost „naučit“ se podobu jednotlivých osob a následně ji porovnávat se snímaným obrazem.

Technologie používá jako základ pro biometrickou identifikaci obličejovou charakteristiku. Pro zakódování obličeje jsou používány speciální algoritmy. Matematické transformace zajistí převod do indexu, který může být uložen ve standardní databázi pro velmi rychlé následné prohledávání.

Uvedené vlastnosti umělé inteligence a schopnosti učení dávají možnost je využít i řadě jiných verifikací a identifikací, např. ochrana uměleckých předmětů, verifikace dodávek drahých koní, kontrola úplnosti strojních sestav a zvuková analýza.

Systémy lze konstruovat v široké paletě výkonnostních i cenových parametrů. K hlavním výhodám patří nenáročnost na uživatele a přirozený způsob verifikace a identifikace odpovídající lidským postupům. U špičkových systémů lze dosáhnout velmi vysoké bezpečnosti a spolehlivosti bez možnosti oklamání. Předností jsou i široké možnosti použití.

Verifikace **lidského hlasu** je elektronická metoda identifikace osoby pomocí rozšířené analýzy digitálního „otisku hlasu“. Tvar hlasivek, ústní dutiny, jazyka a zubů způsobují, že rezonance vokálního traktu je u různých osob dostatečně odlišná. Jednou z nejúspěšnějších technik je porovnávání vzorků pomocí analýzy signálů řeči.

Testovaný subjekt přečte systémem náhodně zvolenou frázi, sejmutá zvuková stopa je kmitočtově omezena (nejčastěji 3kHz) a je proveden rozbor zvuku na základě původu

jednotlivých složek zvuku v činnosti hlasového aparátu a jazykových pravidel[32]. Výsledek je komprimován na vzorek velikosti 1 až 2 kB a porovnán se srovnávacím vzorkem. Verifikace hlasu se používá zejména k řízení přístupu do informačních systémů prostřednictvím telefonu.

K ověření identity na základě **podpisu** je zapotřebí, aby se dotyčná osoba podepsala na speciální podložku pomocí speciálního pera. Systém ověřuje podpis osoby na základě porovnání s uloženým podpisovým vzorem, který popisuje, jak byl popis napsán.

Není důležitá jen podoba podpisu či tvar písmen, ale důraz je kladen na dynamiku podpisu, provedení tahů, sílu, kterou tlačíme při psaní na podložku, rychlost psaní, změny tlaku, zrychlení v jednotlivých částech, celkový průběh zrychlení, zarovnání jednotlivých částí podpisu, celková rychlost, celková dráha a doba pohybu pera na a nad papírem apod. To vše podává jednoznačnou charakteristiku libovolného podpisu. Ze získaných hodnot je opět vytvořen vzorek, který je porovnán se srovnávacím vzorkem. Do této skupiny bychom mohli zařadit i metody využívající sledování rytmu psaní na klávesnici.

Verifikace **tvaru ruky** se zaobírá měřením fyzikálních charakteristik ruky a prstů z hlediska třídimensionální perspektivy. Zkoumá se délka a šířka dlaně a jednotlivých prstů, boční profil ruky apod.

Tvar ruky je snímán speciálním skenerem, který produkuje třírozměrnou fotografii a redukuje tato data do malého vzorku.

Speciální systémy mohou využívat identifikaci podle tvaru chodidla, způsobu chůze atd.

8.1.3 AUTORIZACE

V tomto procesu přiřazujeme identifikované a autorizované osobě práva, kterými disponuje v daném systému. V praxi se jedná o přiřazení zařízení, přístupu k datům, rozsah funkcionality poskytované služby, práva vykonávat určité činnost v rámci systému atd. Většinou se to děje na základě přidělování registrovaných rolí přihlašovanému uživateli.

8.2 DOKLADY

Můžeme si vymezit dvě skupiny dokladů:

- doklady, jejichž primární funkcí je určení totožnosti majitele, např. občanský průkaz apod.;
- doklady, pomocí kterých majitel prokazuje určité oprávnění, např. řidičský průkaz apod.

Specifikace strojově čitelných cestovních dokladů jsou stanoveny v dokumentu 9303 Mezinárodní organizace pro civilní letectví[33] (ICAO). Podle těchto norem se u strojově čitelných cestovních dokladů strana s osobními údaji dělí na dvě zóny:

- zóna vizuální kontroly – Visual Inspection Zone, VIZ, obsahující označení dokladu, fotografii obličeje držitele, osobní údaje a údaje týkající se vydání dokladu a jeho platnosti;
- strojově čitelná zóna – Machine Readable Zone, MRZ, obsahující některé z informací obsažených v zóně vizuální kontroly v podobě alfanumerických znaků a symbolu „<", a to ve dvou či ve třech řádcích. Tuto posloupnost znaků lze přečíst pomocí čtecího zařízení a usnadnit tak kontroly cestovních dokladů.

[32] fonace (tvoření nebo vydávání hlasu), fonetika (studium fyzikálních vlastností hlásek, jejich vnímají atd.), fonologie (pravidla systému pro tvorbu smysluplných slov, zkoumá systematické uspořádání zvuků v určitém jazyce, změny hlásek, když jsou kombinovány atd.)

[33] International Civil Aviation Organization

(OCR – Optical Character Recognition (082) – speciální font písma pro strojově čitelné CD – OCR-B)

Strojově čitelné zóny mohou mít tři formáty:

- ID1 (86 x 54 mm) – 3 řádky, na každém 30 znaků, umístění na zadní straně (verso) dokladu;
- ID2 (105 x 74 mm): 2 řádky, na každém 36 znaků, umístění ve spodní části strany s osobními údaji či ve spodní části víza;
- ID3 (125 x 88 mm): 2 řádky, na každém 44 znaků, umístění ve spodní části strany s osobními údaji.

Strojově čitelné údaje čitelné údaje obsahují typ dokladu, kód vydávajícího státu, příjmení jméno, popřípadě jména občana, číslo cestovního dokladu, státní občanství, datum narození, pohlaví, dobu platnosti dokladu, rodné číslo a kontrolní číslice, které jsou číselným vyjádřením vybraných údajů ve strojově čitelné zóně.

Nosič dat (čip) pro uchování údajů o zobrazení obličeje, údajů o otiscích prstů rukou, údajů zpracovaných na datové stránce cestovního pasu a dalších bezpečnostních prvků stanovených přímo použitelnými právními předpisy Evropských společenství. Dále obsahuje digitálně zpracovanou fotografii občana a jeho podpisu. Uvedené biometrické údaje lze použít výlučně pro ověření totožnosti občana pomocí osobních údajů zapsaných v cestovním dokladu a prostřednictvím technického zařízení umožňuje srovnání aktuálně zobrazených biometrických údajů občana (zobrazení obličeje, otisky prstů) s údaji zpracovanými v nosiči dat cestovního dokladu. K žádosti o vydání cestovního pasu se nepředkládá fotografie, úředník pořídí fotografii žadatele přímo na oddělení cestovních dokladů.

Strojově čitelné údaje (typ dokladu, kód vydávajícího státu, příjmení jméno, popřípadě jména občana, číslo cestovního dokladu, státní občanství, datum narození, pohlaví, doba platnosti cestovního dokladu, rodné číslo a kontrolní číslice, které jsou číselným vyjádřením vybraných údajů ve strojově čitelné zóně) a nosič dat pro uchování údajů o zobrazení obličeje, údajů o otiscích prstů rukou, údajů zpracovaných na datové stránce cestovního pasu a dalších bezpečnostních prvků stanovených přímo použitelnými právními předpisy Evropských společenství. Dále obsahuje digitálně zpracovanou fotografii občana a jeho podpisu. Uvedené biometrické údaje lze použít výlučně pro ověření totožnosti občana pomocí osobních údajů zapsaných v cestovním dokladu a prostřednictvím technického zařízení umožňuje srovnání aktuálně zobrazených biometrických údajů občana (zobrazení obličeje, otisky prstů) s údaji zpracovanými v nosiči dat cestovního dokladu. K žádosti o vydání cestovního pasu se nepředkládá fotografie, úředník pořídí fotografii žadatele přímo na oddělení cestovních dokladů.

Pro elektronické doklady se obvykle využívá **rádio-frekvenční rozhraní** (RF rozhraní). Jeho přínosem je vyšší spolehlivost, jednoduchost obsluhy a vyšší přenosová rychlost. Nevýhodou jsou různé bezpečnostní hrozby a útoky:

- absence vědomého vložení karty do čtečky pro její použití;
- odposlouchávání komunikace mezi čtečkou a čipem (eavesdropping[34]);
- neoprávněné čtení údajů z čipu (skimming[35]);
- rádio-frekvenční manipulace, která má za cíl zabránit komunikaci mezi čipem a čtečkou:
    - poskytování podvržených dat, která se pro systém zdají jako platná (spoofing)[36]);

[34] neautorizované zachycení vyzařování obsahujícího informace
[35] zkopírrování údaje z čípu karty bez vědomí právoplatného držitele dokladu
[36] maskování uživatele

- vložení (maskování) příkazu do komunikace (insert);
- zachycení a uložení platných data a jejich odeslání čtečce znovu později, jako platná je systém bude akceptovat (replay);
- rušení šumovým signálem pro dané frekvenční pásmo (denial of service[37]).

Doklady nedisponují vlastním zdrojem energie. Tu čip získává z pole antény čtecího zařízení. Energie pokrývá spotřebu čipu, neměla by ale stačit na aktivní vysílání. Pro vysílání dat čtečkou na kartu a pro přenos dat z čipu do čtečky jsou využívány různé metody kódování dat a modulace. Využívá se standard ISO 14443[38].

Hrozby se snažíme eliminovat pomocí vhodně navržených kryptografických technologií a schémat.

8.2.1 ZABEZPEČENÍ DOKLADŮ

Elektronická část dokladů je vybavena bezpečnostními prvky zamezujícími jejich falzifikaci. Kromě ochrany před kopírováním je zavedena ochrana před neoprávněným čtením dat z čipu, protože je využíváno bezkontaktního rozhraní (možnost čtení na dálku bez vědomí držitele). Mechanismus autentizace je realizován jako digitální podpis datových souborů označovaných DG1 až DG19, což jsou soubory nesoucí aplikační data pasu[39]. Na českých pasech jsou využívány:

- DG1 – kopie strojově čitelné zóny pasu;
- DG2 - biometrická fotografie držitele
- DG3 - otisk palce;
- DG15 - veřejný klíč aktivní autentizace.

Pro ochranu jsou využívány mechanismy.

BAC (BASIC ACCESS CONTROL - ZÁKLADNÍ ŘÍZENÍ PŘÍSTUPU)

Brání neoprávněnému čtení dat z čipu bez vědomí držitele pasu, zajišťuje tak bezdrátové čtení osobních údajů z dokladů pouze oprávněným stranám. Data v čipu jsou šifrována symetrickým klíčem. Protokol slouží k vygenerování dočasných klíčů, umožňujících vytvoření bezpečného komunikačního kanálu mezi čipem a terminálem (SM). Využívá k tomu dat, vytištěných v strojově čitelné zóně (MRZ):

- číslo dokladu (9 znaků);
- datum narození držitele dokladu (6 znaků)
- datum konce platnosti dokladu (6 znaků).

Vše je chráněno kontrolní číslicí, která umožňuje detekovat chyby při optickém čtení údajů.

Při čtení dat z dokladu jsou nejprve opticky přečtena data z MRZ. Z těchto dat je vypočítán symetrický klíč, kterým jsou následně dešifrována data z čipu. Data z čipu je možno číst pouze tehdy, pokud je pas přiložen datovou stránkou na čtečku pasu.

---

[37] nedostupnost služby, systém není schopnen správně rozpoznat příchozí data

[38] ČSN ISO/IEC 14443-1 dentifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s vazbou na blízko

[39] ICAO. *Machine Readable Passports. Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability.* 6. ed. Montreal: ICAO, 2006. ISBN 92-919-4757-1. Dostupné z: http://www.icao.int/publications/Documens/ 93039303_p1_v2_cons_en.pdf

ELEKTRONICKÝ PODPIS DAT ULOŽENÝCH V ČIPU

Data v čipu jsou elektronicky podepsána, takže není možné je změnit, aniž by to bylo čtečkou pasů detekováno. Data uložená v čipu jsou elektronicky podepsána při výrobě dokladu jeho vydavatelem pomocí privátního klíče certifikovaného národní certifikační autoritou. Každá výrobce má svůj certifikát, tzv. Document Signer.

Ze všech datových skupin jsou vypočteny hodnoty otisku a jsou shromážděny do struktury, která je datovým obsahem zprávy, ze které je vypočten rovněž otisk, který je uložen mezi podepisované atributy ve zprávě. Do zprávy je vložen certifikát a je provázán s obsahem struktury. S použitím odpovídajícího algoritmu pro otisk a elektronický podpis se vytvoří samotná hodnota elektronického podpisu z kódování podepsaných atributů zprávy.

V případě pozdější změny dat v čipu zjistí inspekční systém (čtečka dokladů), že data uložená v čipu nemají platný podpis a proto nejsou důvěryhodná.

AKTIVNÍ AUTENTIZACE (AA)

Elektronický podpis dat v čipu e-pasu nebrání tato data kopírovat. Doporučení ICAO proto specifikuje ještě volitelný mechanizmus tzv. aktivní autentizace (AA), který s využitím vlastností čipu bezpečně uchovat privátní klíč zajistí, že čip nebyl zkopírován. V čipu e-pasu je uložen privátní klíč (generovaný přímo v čipu nebo v rámci bezpečného prostředí personalizace).[40] Veřejný klíč příslušející k tomuto privátnímu je zapsán do DG15 a je zahrnut do dat vybavených elektronickým podpisem (viz kap. 7.3.2). Tímto elektronickým podpisem je zajištěn správný původ tohoto klíče. Pokud by se padělatel pokusil pas zkopírovat, nutně musí zkopírovat i DG15 beze změny a tedy i hodnotu veřejného klíče.

Odpovídající hodnota privátního klíče je však bezpečně uložena v čipu bez možnosti ji přečíst. Při kontrole takto falšovaného pasu pak mechanizmus AA selže (nebude v souladu veřejná část klíče v DG15 a privátní část v čipu).

Aktivní autentizace probíhá takto:

- čtečka provede čtení dat z pasu včetně DG15 a ověří jejich integritu a původ pomocí elektronického podpisu;
- čtečka vygeneruje náhodná data a pošle je do čipu;
- čip v pasu tato data podepíše s využitím privátního klíče pro AA a odešle podepsaná data do čtečky
- čtečka ověří elektronický podpis dat pomocí klíče získaného z DG15 - pokud se podpis podaří ověřit, je pas v pořádku, jinak se může jednat o falzifikát.

EXTENDED ACCESS CONTROL (EAC) - ADVANCED INSPECTION PROCEDURE

Nový koncept zabezpečení, kdy elektronický pas povoluje přístup k otiskům prstů pouze čtečce pasů, které se prokáže validním certifikátem.[41] Evropská komise rozhodla, že členské státy musí ukládat do elektronických pasů i otisky prstů (nasnímaná data zpracovaná ztrátovou kompresí a uložena v datové oblasti DG3 čipu v pasu). Standardy ICAO doporučují, vzhledem k vyšší citlivosti těchto údajů, aby byla implementována dodatečná ochranná opatření pro čtení těchto údajů.

[40] RAŠEK, L. Elektronické cestovní doklady, část 1
[41] BÍŽA, Z. Řízení přístupu k otiskům prstů v elektronických pasech.

Jsou zavedeny kontroly

- autentizace čipu;
- autentizace inspekčního systému (čtečky pasů).

Autentizace čipu je alternativou k aktivní autentizaci, tedy umožňuje inspekčnímu systému ověřit, že čip nebyl podvržen. Navíc zavádí silné šifrování a challenge-answer protokol.

Autentizace inspekčního systému umožňuje čipu v pasu ověřit, že inspekční systém je oprávněn přistupovat k citlivým datům v čipu v pasu (v tomto případě otisky prstů v DG3). Před autentizací inspekčního systému musí proběhnout autentizace čipu, aby byla zajištěna ochrana dat šifrováním. Pokud mají být zpřístupněna data otisků prstů v čipu, musí splňovat požadavky Advanced Inspection Procedure jak čip pasu, tak i inspekční systém (čtečka pasu). Pokud čip nebo inspekční systém požadavky nesplňují, je použita Standard Inspection Procedure a otisky prstů v čipu nejsou zpřístupněny.

Autentizace inspekčního systému vyžaduje, aby měl inspekční systém vlastní digitální certifikát, kterým se autentizuje vůči čipu v pasu. Tento certifikát proto musí být vydán certifikační autoritou, kterou má čip v pasu zavedenu v řetězci důvěryhodných CA.

V každém státě je zřízena právě jedna certifikační autorita CVCA (Country Verifying CA). CVCA vydává certifikáty podřízeným DVCA (Document Verifier CA). CVCA rozhoduje, které DVCA budou mít přístup k údajům v čipu, a to jak v rámci daného státu (výdejem certifikátů pro podřízené DVCA), tak i mezinárodně (výdejem certifikátů pro DVCA jiných států). Certifikát DVCA proto obsahuje informace, ke kterým datům v čipu jsou podřízení Inspekční Systémy oprávněny přistupovat.

Systém důvěry certifikátů inspekčních systémů nepracuje se seznamy zneplatněných certifikátů pro certifikáty inspekčních systémů. Namísto toho mají tyto certifikáty relativně krátkou dobu platnosti 1 až 30 dní.

V případě krádeže inspekčního systému včetně nahraných platných certifikátů je tak výrazně omezena doba, po kterou může útočník s tímto IS neoprávněně číst data otisků prstů z pasů.

8.2.2 IDENTIFIKAČNÍ DOKLADY

Existují dvě hlavní kategorie identifikačních dokladů:

- cestovní dokumenty;
- národní průkazy totožnosti.

Všechny, bez ohledu na využívané technologie musí být chráněny proti padělání a krádežím (usurpování) identity.

Situace není tak jednoduchá, jako by se na první pohled zdálo. Rozhodující roli zde hraje různost předpisů a zvyklostí nejen ve světě, ale i uvnitř Evropské unie. Jde především o to, že:

- v některých zemích je národní průkaz totožnosti dobrovolný, někde není využíván vůbec a jeho funkci plní pas;
- na území jednotlivých států platí zároveň několik typů dokumentů, založených na různých technologiích[42].

[42] O situaci v České republice se můžeme přesvědčit v úplném znění Vyhlášky 400/2011 Sb., kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech [cit. 12. 1. 2012]. Dostupné z:

O tom, jak široká škála dokladů se používá pouze v Evropské unii, se můžeme přesvědčit na stránkách Veřejného rejstříku pravých dokladů totožnosti a cestovních dokladů[43].

PRŮKAZ TOTOŽNOSTI

V České republice je znám pod názvem občanský průkaz.

Občanský průkaz, který již obsahuje strojově čitelné údaje je vydávaný od ledna 2005, viz Obrázek 8-1. Poslední verze občanský průkazu je vydávaná od ledna 2012 a průkaz je vydáván s čipem nebo bez čipu, oba průkazy jsou vzhledově stejné, liší se pouze tím, že na zadní straně je umístěn kontaktní elektronický čip, do kterého lze v současnost nahrát pouze elektronický podpis (podle § 17b odst. 1 zákona číslo 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů, § 17b, odstavec 1)), viz Obrázek 8-2. V případě zájmu o kvalifikovaný certifikát je nezbytné kontaktovat některého z akreditovaných poskytovatelů certifikačních služeb (vydání kvalifikovaného certifikátu je zpoplatněno).

Další údaje bude možné na elektronický kontaktní čip nahrát pouze, stanoví-li tak zvláštní právní předpis a pouze se souhlasem držitele. Mezi volitelné údaje patří rodinný stav, registrované partnerství a titul. Od 1.1.2017 bude volitelným údajem také trvalý pobyt.

Při převzetí občanského průkazu si volí občan bezpečnostní osobní kód, který je povinný. Bezpečnostní osobní kód je kombinací nejméně 4 a maximálně 10 číslic (obdoba PINu u platebních karet). Tento osobní kód slouží k autentizaci při elektronické identifikaci držitele občanského průkazu při komunikaci s informačními systémy veřejné správy. Kód je zabezpečen tak, že po třetím chybném po sobě jdoucím zadání bezpečnostního osobního kódu se další možnost elektronické identifikace zablokuje. Odblokování provádí na žádost držitele kterýkoliv obecní úřad obce s rozšířenou působností za správní poplatek.

Certifikáty uložené na čipové kartě je možné spravovat pomocí obslužné aplikace, která umožňuje změnu hodnoty PIN na čipu a slouží pro zápis dat do čipu (pro vytváření elektronických podpisů spolu s kvalifikovaným certifikátem obsahujícím data pro ověřování elektronických podpisů odpovídající těmto datům a dat nezbytně nutných pro užívání elektronického podpisu). Neoprávněné nahrání údajů do čipu je však přestupkem.

Klíče a certifikáty mohou být mazány z karty, exportovány do souboru a nebo importovány ze souboru. Program umožňuje také registrovat a odregistrovat certifikáty v systému. Program umožňuje změnu PINu a PUKu karty. Pro změnu PINu lze použít standardních systémových mechanismů.

---

http://www.uplnezneni.cz/vyhlaska/400-2011-sb-kterou-se-provadi-zakon-o-obcanskych-prukazech-a-zakon-o-cestovnich-dokladech/>

[43] http://prado.consilium.europa.eu/CS/searchbyissuingcountry.html

Obrázek 8-1 Občanský průkaz vydávaný od ledna 2005

Přední strana

Zadní strana

Laminované karty 74x105 mm se zaoblenými rohy
Rozměry papírového jádra jsou 68x99 mm (formát ID2).
Základní materiál pro výrobu jádra: ceninový papír s průběžným negativně - pozitivním vodoznakem, který tvoří písmena ČR a lipové lístky
Hlavní barvy OP: zelená a fialová.
Názvy položek na přední straně a některé názvy položek na zadní straně dokladu jsou v českém, anglickém a francouzském jazyce.

Obrázek 8-2 Občanský průkaz vydávaný od ledna 2012

Přední strana	**Zadní strana**	
	Bez čipu: 	Plastová karta 54 x 85,6 mm se zaoblenými rohy. Má gravírovanou černobílou fotografii a gravírovaný podpis držitele. Jméno, příjmení a číslo dokladu jsou provedeny taktilním gravírováním (lze poznat hmatem).
	S čipem: 	OP je vydáván s čipem nebo bez čipu. Jsou vzhledově stejné, liší se pouze tím, že na zadní straně je umístěn kontaktní elektronický čip, do kterého lze nahrát elektronický podpis (podle § 17b odst. 1 zákona číslo 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů).

Vzhledem k prvkům, které průkazy obsahují je nutné je chránit jej před poškozením, zničením, ztrátou, odcizením nebo zneužitím. Proto by měl být nošen ve vhodném obalu a chráněn proti škodlivým mechanickým, chemickým či elektromagnetickým vlivům, čili před:

- vystavováním nadměrným teplotám nižším než –10°C nebo vyšším než 50°C;
- vystavením nadměrnému mechanickému namáhání, které by mohlo plastovou kartu nebo elektronický kontaktní čip poškodit;
- vystavováním vlivu kapalin, chemikálií nebo agresivních plynů;
- dlouhodobým vystavováním intenzivnímu slunečnímu nebo světelnému záření;
- vystavováním elektrostatickým výbojům, neúměrnému elektromagnetickému poli či mikrovlnnému záření;
- spojováním se zařízeními či systémy, pro něž není určen.

Nefunkčnost kontaktního elektronického čipu není důvodem pro skončení platnosti občanského průkazu, ale se skončením platnosti občanského průkazu končí platnost elektronického čipu.

CESTOVNÍ DOKLADY

Cestovní doklady s biometrickými prvky se vydávají občanům České republiky na základě žádosti. Jednotný přístup Evropské unie k biometrickým identifikátorům nebo biometrickým údajům je dán nařízení Rady EU č. 2252/2004 (upravena nařízením č. 444/2009). Toto nařízení mimo jiné stanovuje minimální bezpečnostní normy, které musí cestovní pasy a cestovní doklady vydané členskými státy EU splňovat. V příloze stanoví minimální úroveň zabezpečení pro

- použitý materiál;
- stránku s biografickými údaji;
- techniky tisku;
- ochranu proti kopírování;
- techniky vydávání.

Dále stanovuje, že doklady musí obsahovat médium pro uchování údajů, které obsahuje zobrazení obličeje[44] a otisky prstů[45] v interoperabilních formátech. Údaje musí být zabezpečeny a médium musí mít dostatečnou kapacitu pro jejich uchování a schopnost zaručit neporušitelnost, pravost a utajení údajů.

Cestovní doklady musí být vydávány ve strojově čitelné formě. Grafická úprava stránky s biografickými údaji musí splňovat specifikace části 1 dokumentu ICAO 9303[46] a postupy vydávání musí splňovat specifikace, které tento dokument stanoví pro strojově čitelné doklady.

[44] 1. generace - od 28.8.2006 (Rozhodnutí Komise K (2005) 409 ze dne 28. února 2005)
[45] 2. generace - od 28.6.2009 (Rozhodnutí Komise K (2006) 2909 ze dne 28. června 2006)
[46] ICAO. *Machine Readable Travel Documents: Part 1 Machine Readable Passports.* 6. vyd. Montréal, 2006. Dostupné z: http:/www.icao.int/publications/Documents/9303_p1_v1_cons_en.pdf

Obrázek 8-3 Cestovní pas

VÍZA

Vízum je doklad, opravňující osobu k pobytu na daném území, vztahuje-li se na ni vízová povinnost.

Výrazem harmonizace vízové politiky států stran Schengenských dohod je zavádění systému společných víz ve formě jednotného schengenského víza[47], které opravňuje držitele v zásadě k volnému pohybu po celém schengenském prostoru. Existuje však možnost omezení platnosti schengenského víza pouze na některé členské státy, přičemž použitelnost tohoto víza je v rozmezí 1 - 6 měsíců; v určitých případech i déle. Délka povoleného pobytu se pak dělí mezi počet povolených vstupů. Držitel neomezeného schengenského víza je oprávněn pohybovat se volně na území všech států Schengenských dohod. Je-li vízum územně omezeno, smí se zdržovat pouze ve státech, pro něž je vízum platné. Cizinci ze třetích zemí bez vízové povinnosti se tedy mohou volně pohybovat na území Schengenu, maximálně však tři měsíce v rámci šestiměsíční lhůty od data prvního vstupu. Úmluva však nestanoví,

[47] Amsterodamská smlouvou o EU (1999) obsahuje vízovou politiku v hlavě IV Smlouvy o založení ES (článek 62 a násl.). Vízová problematika je obsažena rovněž v kapitole 3 hlavy II Schengenské prováděcí úmluvy.

kteří cizinci ze třetích zemí mají vízovou povinnost. Tato povinnost vyplývá z vnitrostátních předpisů, které přitom musí zohledňovat v souladu s předpisy ES společnou vízovou politiku.

Udělování víz je výhradně v kompetenci diplomatických misí a konzulárních úřadů států Schengenské dohody, přičemž ve výjimečných případech je mohou také udělit pohraniční orgány.

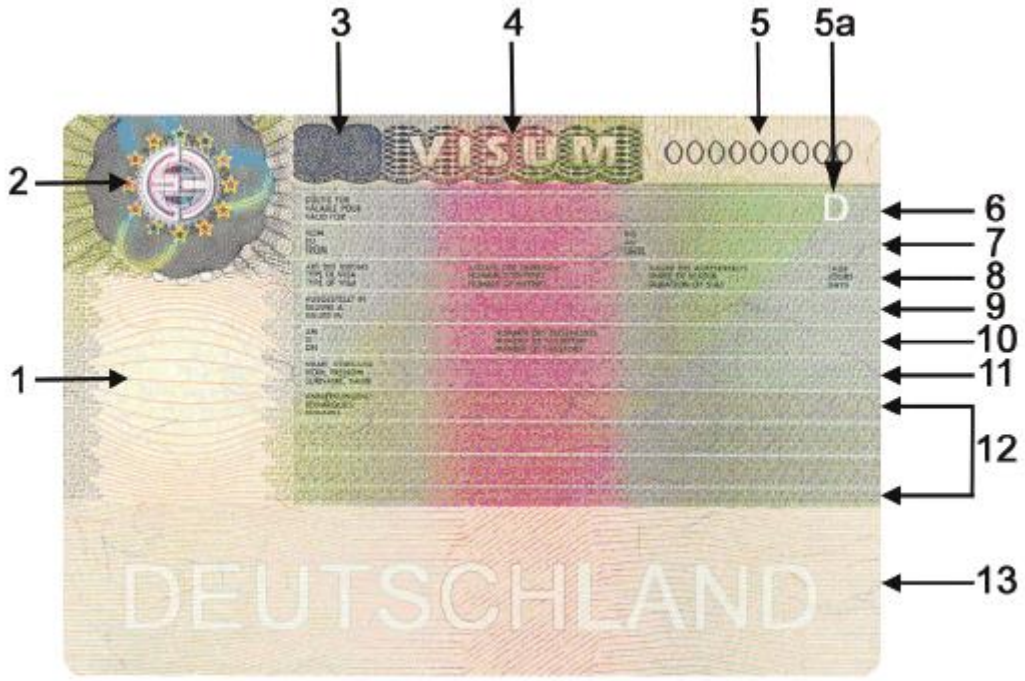
Schengenská víza se dělí na kategorie:

- vízum pro průjezd přes území členských států nebo předpokládaný pobyt na tomto území, který nepřesáhne tři měsíce během jakéhokoli šestiměsíčního období ode dne prvního vstupu na území dotyčných členských států;
- vízum pro průjezd přes mezinárodní tranzitní prostory na letištích členských států.

Udělovat lze jednotná víza umožňující držiteli pohyb po území všech členských států, víza s omezenou územní platností, která držiteli umožňují pohyb pouze po území jednoho či několika členských států, nebo letištní průjezdní víza umožňující průjezd tranzitními prostory mezinárodního letiště či letišť členských států.

Členské státy požadují i biometrické identifikátory žadatele. Proto při podání první žádosti se požaduje, aby se žadatel dostavil osobně. Při té příležitosti se od žadatele odebírají fotografie, naskenovaná nebo pořízená při podání žádosti a otisky deseti prstů, které byly odebrány na plocho a digitálně zaznamenány.

Obrázek 8-4 Vízový štítek



Bezpečnostní prvky		Oddíly, které mají být doplněny	
Pole	Obsah	Pole	Obsah
1	Integrovaná fotografie zhotovená podle přísných bezpečnostních norem.	6	Začíná slovy „platný pro“. Orgán udělující vízum uvede území, pro které nebo pro která je vízum platné.
2	Opticky se měnící značka („kinegram“ nebo jeho obdoba). V závislosti na úhlu pohledu se stává viditelným dvanáct hvězd, písmeno „E“ a zeměkoule v různých velikostech a barvách.	7	Začíná slovem „od“ a dále na řádku je slovo „do“. Orgán udělující vízum zde uvede dobu platnosti víza.
3	Kód státu tvořený písmenem nebo písmeny, která označují stát udělující vízum se sklopným efektem. Kód státu je světlý, drží-li se na plocho, a tmavý, otočí-li se o 90°.[48]	8	Začíná slovy „druh víza“. Orgán udělující vízum zde uvede kategorii víza. Dále zde jsou slova „počet vstupů“, „délka pobytu“ (tj. délka zamýšleného pobytu žadatele) a dále slovo „dní“.
4	Ve středu je slovo „vízum“ velkými písmeny v opticky se měnících barvách. V závislosti na úhlu pohledu je buď zelené nebo červené.	9	Začíná slovy „vydáno v“ a užívá se na uvedení místa vydání víza.
5	Devítimístné vnitrostátní číslo vízového štítku, které je předtištěno. Užívá se zvláštního písma.	10	Začíná slovem „dne“ (kde vyplní orgán udělující vízum datum jeho vydání) a dále na řádku jsou slova „číslo pasu“ (po nichž následuje číslo pasu držitele).
5a	Kód země tvořený třemi písmeny uvedený v dokumentu ICAO 9303 o strojově čitelných cestovních dokladech (1), který označuje členský stát udělující vízum.	11	Začíná slovy „příjmení, jméno“.
		12	Začíná slovem „poznámky“. Užívá jej orgán udělující vízum pro uvedení dalších informací, jež považuje za nutné, za předpokladu, že to odpovídá článku 4 tohoto nařízení. Pro tyto poznámky je ponecháno dva a půl prázdného řádku.
		13	Obsahuje strojově čitelné informace pro usnadnění kontrol na vnějších hranicích. Strojově čitelná zóna obsahuje text vytištěný v podtisku, který označuje členský stát udělující daný doklad. Tento text nemá vliv na technické vlastnosti strojově čitelné zóny ani na možnost jejího přečtení.

„Číslem vízového štítku“ je kód země tvořený třemi písmeny uvedený v rámečku 5a a vnitrostátní číslo uvedené v rámečku 5.

Papír je přírodní barvy s červenými a modrými znaky. Slova označující rámečky (pole) jsou v angličtině a francouzštině. Stát udělující vízum může přidat třetí úřední jazyk. Společenství. Slovo „vízum“ v horním řádku však může být v jakémkoliv úředním jazyce Společenství.

Víza se vypracovávají podle jednotného vzoru (štítek). Při vyplňování vízového štítku se vyplňují povinné údaje a strojově čitelné zóny. Členské státy mohou v oddíle „poznámky“ vízového štítku doplnit vnitrostátní údaje, které neopakují povinné údaje. Vytištěný vízový štítek se připojí do cestovního dokladu. Pokud členský stát, který vízum udělil, neuznává cestovní doklad žadatele, použije se pro připojení víza samostatný formulář pro připojení víza.

Všechny údaje, včetně biometrických jsou vkládány do VIS (viz kap. 11.2).

[48] Kódy států jsou A pro Rakousko, BG pro Bulharsko, BNL pro Benelux; CY pro Kypr, CZE pro Českou republiku, D pro Německo, DK pro Dánsko, E pro Španělsko, EST pro Estonsko, F pro Francii, FIN pro Finsko, GR pro Řecko, H pro Maďarsko, I pro Itálii, IRL pro Irsko, LT pro Litvu, LVA pro Lotyšsko, M pro Maltu, P pro Portugalsko, PL pro Polsko, ROU pro Rumunsko, S pro Švédsko, SK pro Slovensko, SVN pro Slovinsko a UK pro Spojené království.

PRŮKAZ O POVOLENÍ K POBYTU PRO CIZINCE Z TŘETÍCH ZEMÍ

Žádost o povolení k dlouhodobému pobytu je oprávněn podat cizinec, který na daném území pobývá na vízum k pobytu nad 90 dnů, hodlá na území přechodně pobývat po dobu delší než 6 měsíců a trvá-li stejný účel pobytu. Kdo, za jakých podmínek a jakým způsobem stanovuje zákon[49].

Od května 2011 v průkazech o povolení k pobytu pro cizince z třetích zemí jsou i biometrické údaje. Tento doklad:

- prokazuje totožnost držitele;
- osvědčuje druh povoleného pobytu (právní status) a v případě dlouhodobého pobytu i dobu povoleného pobytu;
- spolu s platným cestovním dokladem umožňuje držiteli za podmínek stanovených schengenskými předpisy pobyt i na území ostatních schengenských států.

Nařízení Rady Evropy[50] stanovuje členským státům EU povinnost vydávat jednotný vzor povolení k pobytu pro státní příslušníky třetích zemí a stanovuje bezpečnostní prvky a biometrické identifikátory. Povolení k pobytu musí obsahovat všechny nezbytné informace a splňovat technické požadavky, zejména v souvislosti s ochranou proti padělání a pozměňování.

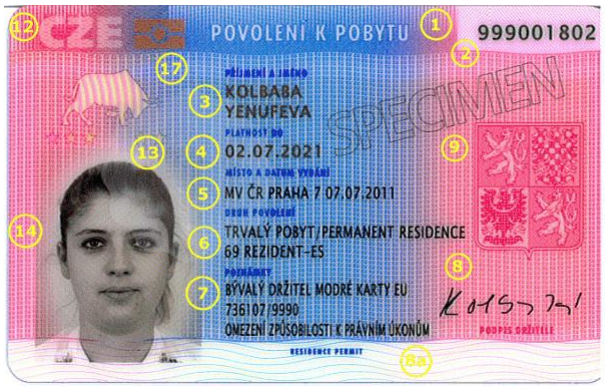
Doklad je polykarbonátová kartu typu ID 1 o rozměru 54,0±0,75 mm x 85,6±0,75 mm. Formát, barevné provedení a ochranné prvky jsou jednoznačně dány technickými specifikacemi. K personalizaci dokladu slouží jednotlivá pole pro uvádění údajů k osobě a typu dokladu. V těle dokladu je obsažen nosič elektronických údajů, bezkontaktní čip.

[49] ČR. Zákon 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=48225&fulltext=&nr=326~2F1999&part=&name=&rpp=15#local-content

[50] Nařízení Rady (ES) č. 380/2008 ze dne 18. dubna 2008, kterým se mění nařízení (ES) č. 1030/2002, kterým se stanoví jednotný vzor povolení k pobytu pro státní příslušníky třetích zemí

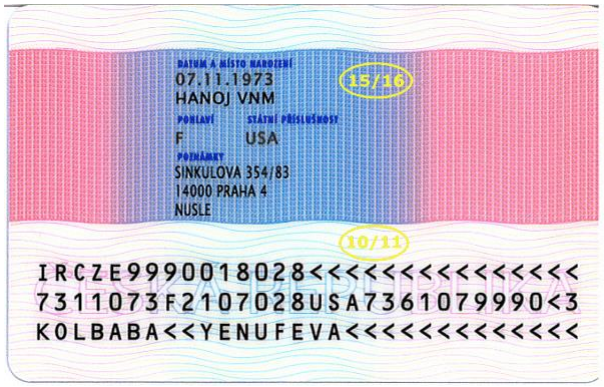
Obrázek 8-5 průkazech o povolení k pobytu pro cizince z třetích zemí platný od 2011

Přední strana



Pole	
1	Název dokladu – text „POVOLENÍ K POBYTU“
2	Číslo dokladu – devět numerických znaků v reliéfním provedení
3	Příjmení a jméno – příjmení a jméno držitele průkazu, velkými písmeny v reliéfním provedení
4	Platnost do – den skončení platnosti dokladu ve formátu DD.MM.RRRR v reliéfním provedení
5	Místo a datum vydání – název pracoviště MV ČR (velkými písmeny), které pořídilo biometrické údaje a doklad předalo, datum vydání dokladu ve formátu DD.MM.RRRR
6	Druh povolení – název druhu povolení k pobytu v českém a anglickém jazyce - „TRVALÝ POBYT/PERMANENT RESIDENCE“ - „DLOUHODOBÝ POBYT/LONG-TERM RESIDENCE“ - „ZELENÁ KARTA-A/GREEN CARD-A“ - „ZELENÁ KARTA-B/GREEN CARD-B“ - „ZELENÁ KARTA-C/GREEN CARD-C“ - „MODRÁ KARTA EU/BLUE CARD EU“ - „AZYL/REFUGEE STATUS“ - „DOPLŇKOVÁ OCHRANA/SUBSIDIARY PROTECTION“ Na druhém řádku tohoto pole je uveden příslušný druh pobytu kódem příslušné zpřesňující podkategorie, na tomto řádku může být rovněž kromě kódu uveden text „REZIDENT-ES“
7	Poznámky – toto pole je tvořeno celkem třemi řádky. Může zde být vyznačena skutečnost, že držitelem je „BÝVALÝ DRŽITEL MODRÉ KARTY EU“, dále zde může být uvedeno rodné číslo držitele průkazu v běžném formátu s lomítkem před koncovkou a rovněž je v této části dokladu vyznačena skutečnost týkající se změněné právní způsobilosti držitele, a to buď textem „OMEZENÍ ZPŮSOBILOSTI K PRÁVNÍM ÚKONŮM“ nebo textem „ZBAVENÍ ZPŮSOBILOSTI K PRÁVNÍM ÚKONŮM“.
8	Podpis držitele – pole obsahuje digitalizovaný podpis držitele tak, jak byl uveden na protokolu o pořízení biometrických údajů
8a	Název dokladu v cizím jazyce – fixní text „RESIDENCE PERMIT“
9	Státní znak – obraz státního znaku je obsažen v podkladovém tisku karty
12	Zkratka vydávajícího státu – „CZE“ – platná mezinárodní zkratka názvu České republiky
13	Opticky proměnlivý ukazatel – přes pravý horní roh fotografie držitele je umístěn opticky proměnlivý prvek, který je jedním z bezpečnostních prvků dokladu. Jedná se o transparentní kinegram v jednotném provedení podle vzoru EU.
14	Fotografie držitele – grafická data ve specifikované kvalitě
17	Symbol elektronického dokladu - v opticky proměnlivém provedení

Zadní strana



Pole	
10/11	Strojově čitelná zóna (MRZ), která obsahuje údaje sloužící k základní identifikaci držitele v digitalizované podobě.
15/16	V prvním řádku je uvedeno datum narození držitele ve formátu DD.MM.RRRR v reliéfním provedení. Místo narození je uvedeno celým názvem a dále je na řádku uvedena mezinárodně platná třípísmenná zkratka státu narození. Pohlaví – údaj F/M/X, v reliéfním provedení Státní příslušnost – mezinárodně platná třípísmenná zkratka státu, jehož je držitel státním příslušníkem, v reliéfním provedení Poznámky – platná adresa pobytu držitele dokladu na území ČR

Zdroj: http://www.mvcr.cz/clanek/zmeny-od-kvetna-2011-biometricke-udaje-v-prukazech-o-povoleni-k-pobytu-pro-cizince-z-tretich-zemi.aspx?q=Y2hudW09Mw%3d%3d

8.2.3 ŘIDIČSKÝ PRŮKAZ - PŘÍKLAD DOKLADŮ K PROKÁZÁNÍ OPRÁVNĚNÍ

Mezinárodní řidičská asociace (IDA) na základě Úmluvy OSN o silničním provozu a bezpečnosti[51] distribuuje mezinárodní řidičské průkazy (oficiální mezinárodní překlady původního řidičského průkazu do angličtiny, francouzštiny, ruštiny, španělštiny, čínštiny, němčiny, arabštiny a japonštiny).

Každý mezinárodní dokument se skládá z brožury ve formě cestovního pasu a plastové ID karty

.

Zdroj: http://international.drivingpermit.org.uk/licence/samples/idp_book_2.jpg

[51] http://drivingpermit.org/un/convention.phtml

9 EGOVERNMENT

Můžeme se setkat různými pohledy na e-government a jeho definicemi. Definice můžeme rozdělit do tří skupin[52]:

- eGovernment je definován jako poskytování služeb a zabezpečování dalších činnosti on-line prostřednictvím internetu;
- eGovernment je stavěn na úroveň využití informačních a komunikačních technologií ve vládě (státní a veřejné správě), nejširší definice zahrnují všechny aspekty její činnosti, i když je důraz kladen obecně na poskytování služeb a procesy.
- eGovernment je definován jako schopnost transformace veřejné správy s využitím informačních a komunikačních technologií, tento aspekt je obvykle spojován s využíváním internetu.

My se přikloníme k následující formulaci.

NEPŘEHLÉDNĚTE

eGovernment (e-vláda) je elektronickou formou výkonu státní a veřejné správy s využitím možností ICT, zejména internetu, v procesech státní a veřejné správy, s cílem optimalizovat tyto procesy.

Je to radikální změna, podpořená zákonem 300/2008 Sb., v komunikaci mezi veřejností a orgány veřejné správy a mezi orgány veřejné moci navzájem. V procesech veřejné správy funguje on-line komunikace[53]:

- v rámci institucí VS (G2E – Government to Employee);
- mezi institucemi VS navzájem (G2G – Government to Government);
- mezi veřejnou správou a občany (G2C - Government to Citizen);
- mezi veřejnou správou a podnikatelskou sférou (G2B - Government to Business);
- mezi veřejnou správou a administrativou (G2A - Government to Administration).

eGovernment představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. To znamená rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům. Nasazení ICT přináší značné úspory, lepší kvalitu služeb a transparentnost v oblasti veřejné správy a to nejen v komunikaci vláda-občan, ale zejména v segmentu komunikace vláda-vláda.

eGovernment by měl naplnit cíle:

- občan je klientem, zabezpečit snadný, bezpečný a důvěryhodný přístup ke službám všem občanům;
- vytvořit společnou datovou základnu pro ISVS, aby stačilo informace od občana získávat jen jednou;
- integrace služeb, omezení počtu komunikačních bodů při řešení různých záležitostí občanů;
- umožnit používání jedno kontaktního místa pro všechno („one stop shop“);

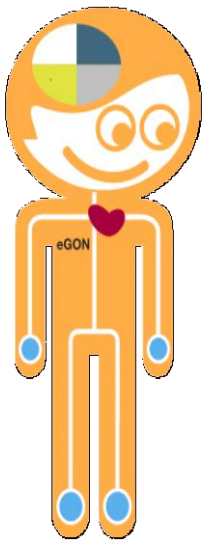
[52] OECD. The e-government imperative. Dostupné z: http://www.keepeek.com/Digital-Asset-Management/oecd/governance/the-e-government-imperative_9789264101197-en

[53] FÁBRYOVÁ, L. Informatizácia verejnej správy. *Informatizacia.sk* Dostupné z: http://www.informatizacia.sk/egovernment/519s

- občan by měl mít možnost volby místa a komunikačního kanálu (osobně, poštou, telefonicky, elektronicky) a využívat alternativní komunikační kanály;
- personalizace a flexibilita služeb;
- systém by měl podporovat proaktivní služby VS, tedy aby ona sama automaticky zařizovala věci, které zařídit může sama, aniž by občan s ní musel komunikovat;

Stupeň elektronizace poskytování služeb VS pro veřejnost můžeme rozdělit do pěti úrovní[54]:

1. Informace, informace zpřístupněny on-line (např. texty legislativních dokumentů, materiály pro jednání a zápisy samosprávných orgánů, postupy administrativních procedur, kontaktní informace úřadů atd.).
2. Jednostranná interakce (stahování formulářů), uživatelé si mohou např. stahovat formuláře, které musí vyplnit a vytisknout a odevzdat nebo zaslat v klasické papírové podobě.
3. Dvoustranná interakce (elektronické formuláře): uživatelům je umožněno nejen stahování formulářů, ale také jejich vyplnění a odevzdání zpět v elektronické podobě.
4. Transakce (úplné elektronické zpracování) umožňuje úplné vyřízení administrativy elektronickým způsobem (elektronická podání žádosti a jejich projednání, rozhodnutí o doručení odpovědi apod.).
5. Personalizace (proaktivní, automatizovaný přístup) samozřejmě umožňuje provést všechny výše popsané úkony. IS si však uživatele „pamatuje“, po jeho přihlášení provede nastavení systému a do příslušných dokumentů vyplní údaje, které jsou již o uživateli veřejné správě (IS) známy. Některé operace jsou provedeny, aniž by občan byl nucen tyto operace aktivně vyvolat.

Základní pilíře		**eGON**
Centrální databáze		Základní registry veřejné správy – databáze o občanech a státních i nestátních subjektech
Legislativní rámec a standardy		Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi(zákon o eGovernmentu - eGovernment Act)
Komunikační infrastruktura		KIVS – Komunikační infrastruktura veřejné správy, zajišťující bezpečný přenos dat
Instituce		Czech POINT - soustava snadno dostupných kontaktních míst

[54] CAPGEMINI. The User Challenge Benchmarking The Supply Of Online Public Services. Diegem: Capgemini Belgium NV/SA, 2007. [online]. [cit. 2013-05-28] Dostupné z: http://www.umic.pt/images/stories/publicacoes200709/egov_benchmark_2007.pdf

Zákon č. 300/2008 Sb. upravuje:

- elektronické úkony prostřednictvím datových schránek:
  - orgánů veřejné moci vůči fyzickým a právnickým osobám;
  - fyzických a právnických osob vůči orgánům veřejné moci;
  - mezi orgány veřejné moci navzájem.
- informační systém datových schránek;
- autorizovanou konverzi dokumentů.

Nevztahuje se na dokumenty, které obsahují utajované informace.

Cílem zákona je vytvoření optimálních podmínek pro elektronickou komunikaci mezi občany a úřady, mezi úřady navzájem, včetně sledování toho, jak se věci vyvíjejí uvnitř úřadů.

Systém budovaný na základě eGovernment Act se soustřeďuje na pojmy[55]:

- eDokument: listinné a elektronické podoby dokumentů budou zrovnoprávněny:
  - autorizované konverze písemností z listinné do elektronické podoby a zpět budou provádět notáři, krajské a obecní úřady s využitím elektronického podpisu;
  - převedeným písemnostem budou přiznány stejné právní účinky, jaké měly ty, které byly převáděny;
  - řeší se problémy s přístupem k informacím, jejich oběhem, nakládáním, archivováním či ztrátou;
- eIdentita: bezpečnější ochrana osobních údajů
  - úředník již nebude mít oprávnění nahlížet do agend a údajů, které nesouvisejí přímo s výkonem činnosti, ke které je zmocněn;
  - zvýší se transparentnosti správního rozhodování a snížení se možnosti zneužití dat (rodná čísla se vyčerpají do roku 2053, je připraven bezvýznamový identifikátor fyzických osob, který bude unikátní a nikdy se nevyčerpá);
  - umožňuje také identifikaci na dálku, elektronicky, což nyní nelze.
- elektronické spisy – elektronické schránky:
  - úřady budou mít povinnost komunikovat mezi sebou elektronicky;
  - úřady budou pod trvalou kontrolou, jak vyřizují podání;
  - zřídí se elektronické datové schránky nejen pro úřady, ale i pro firmy, kam jim budou úřady doručovat rozhodnutí, výzvy a podněty.

Musí být naplněny požadavky:

- zachování bezpečné elektronické identity občanů;
- důkladná ochrana osobních údajů;
- poskytnutí komplexního řešení pro všechny agendy, které jsou vykonávány orgány veřejné moci;
- elektronická komunikace člověk-úřad není povinná, čili každý má možnost komunikovat s úřady takovou formou, jaká mu vyhovuje;
- uvnitř úřadů a mezi úřady navzájem se však bude komunikovat pouze elektronicky.

Pro komunikaci s orgány veřejné správy se využívá elektronický podpis. Musí to být tzv. zaručený elektronický podpis založený na kvalifikovaném certifikátu, vydaném akreditovaným poskytovatelem certifikačních služeb.

[55] MINISTERSTVO INFORMATIKY ČESKÉ REPUBLIKY. EGovernment: Veřejná správa jako živý organizmus. Praha, 2010. [online]. [cit. 2013-05-28] Dostupné z: hhttp://www.czechpoint.cz/web/docs/eGon_brozura.pdf MINISTERSTVO INFORMATIKY ČESKÉ REPUBLIKY. EGovernment: Veřejná správa jako živý organizmus. Praha, 2010. [online]. [cit. 2013-05-28] Dostupné z: hhttp://www.czechpoint.cz/web/docs/eGon_brozura.pdf

9.1 DATOVÉ SCHRÁNKY

NEPŘEHLÉDNĚTE

Datová schránka je elektronické úložiště, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci a dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.

Datová schránka je tedy datovým prostorem vyhrazeným pro orgán veřejné moci nebo právnickou osobu nebo podnikající fyzickou osobu nebo pro fyzickou osobu, kam jsou orgány veřejné moci doručovány datové zprávy, kde jsou prováděny úkony vůči orgánům veřejné moci. Datová schránka je součástí ISDS.[56]

Datové schránky zřizuje a spravuje Ministerstvo vnitra. Člení se na:

- datová schránka fyzické osoby;
- datová schránka podnikající fyzické osoby;
- datová schránka právnické osoby;
- datová schránka orgánu veřejné moci, kam patří i datové schránky orgánů územních samosprávných celků.

K identifikaci datové schránky slouží identifikátor, který je pro každou datovou schránku jedinečný a není zaměnitelný s žádným jiným identifikátorem využívaným orgány veřejné moci. Správce informačního systému datových schránek vytváří identifikátor automatizovaně s využitím algoritmů pro generování náhodných čísel.

Osoby oprávněné k přístupu do datové schránky se do ní přihlašují prostřednictvím přístupových údajů. Přístupové údaje pro přihlašování do datové schránky tvoří uživatelské jméno a bezpečnostní heslo. Uživatelské jméno je pro každou osobu jedinečné a je to řetězec nejméně 6 a nejvýše 12 znaků vzniklý automatizovaným generováním. Bezpečnostní heslo je řetězec nejméně 8 a nejvýše 32 znaků. Vždy se jedná o kombinaci písmen, číslic a speciálních znaků. Bezpečnostní heslo nesmí být shodné s uživatelským jménem, se kterým tvoří přístupové údaje.[57] Osoba oprávněná k přístupu do datové schránky je povinna zacházet s přístupovými údaji tak, aby nemohlo dojít k jejich zneužití.

Do datové schránky mají přístup oprávněné osoby[58]:

- do datové schránky fyzické, popř. podnikající fyzické osoby, osoby fyzická osoba, pro niž byla datová schránka zřízena;
- do datové schránky právnické osoby statutární orgán právnické osoby, člen statutárního orgánu právnické osoby nebo vedoucí organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro něž byla datová schránka zřízena;
- do datové schránky orgánu veřejné moci vedoucí orgánu veřejné moci, pro něhož byla datová schránka zřízena;

Rozsah přístupu uvedených osob do datové schránky zahrnuje i přístup k dokumentům určeným do vlastních rukou adresáta. Tyto osoby mohou určit, že úkony, které jim jsou podle zákona vyhrazeny ve vztahu k pověřeným osobám a k ministerstvu, může činit fyzická osoba k tomu určená (administrátor).

---

[56] TESAŘ Pavel a Ondřej MENOUŠEK. MINISTERSTVO VNITRA ČR. *Provozní řád ISDS.*

[57] Vyhláška 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

[58] § 9 Zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

Do datové schránky jsou oprávněny přistupovat ve stanoveném rozsahu pověřené fyzické osoby[59]:

- fyzickou osobou a podnikající fyzickou osobou, pro něž byla datová schránka zřízena;
- statutárním orgánem právnické osoby nebo vedoucím organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro něž byla datová schránka zřízena;
- vedoucím orgánu veřejné moci, pro který byla datová schránka zřízena.

Pověřená osoba je oprávněna k přístupu k dokumentům určeným do vlastních rukou adresáta pouze, stanoví-li tak oprávněná osoba nebo administrátor.

Samozřejmě osoby přistupující do datové schránky jsou povinny ji využívat způsobem, který neohrožuje bezpečnost informačního systému datových schránek a uvědomit neprodleně MVČR o hrozícím nebezpečí zneužití. Pověřená osoba uvědomí rovněž toho, kdo ji určil pověřenou osobou.

Přístup k datové schránce je dán pravidly stanovenými zákonem[60]. Můžeme hovořit o:

- zpřístupnění datové schránky;
- znepřístupnění datové schránky;
- zneplatnění přístupových údajů;
- zrušení datové schránky.

Datová schránka je zpřístupněna prvním přihlášením oprávněné osoby, nejpozději však patnáctým dnem po dni doručení přístupových údajů zaslaných MVČR.

Znepřístupnění datové schránky znamená nemožnost doručování do datové schránky adresáta po stanovenou dobu. Znepřístupnění je provedeno na základě žádosti nebo při splnění důvodů stanovených zákonem[61]:

- u fyzické osoby a podnikající fyzické osoby, pro niž byla datová schránka zřízena, ke dni:
- úmrtí osoby;
- uvedenému v rozhodnutí soudu o prohlášení za mrtvého jako den úmrtí této osoby;
- nabytí právní moci rozhodnutí o zbavení nebo omezení způsobilosti této osoby k právním úkonům;
- kdy byla tato osoba omezena na osobní svobodě z důvodu vzetí do vazby, výkonu trestu odnětí svobody, výkonu zabezpečovací detence, ochranného léčení nebo ochrany zdraví lidu;
- u podnikající fyzické osoby a právnické osoby dnem výmazu ze zákonem stanovené evidence (obchodního rejstříku u právnické osoby a z živnostenského rejstříku u fyzické podnikající osoby);
- u orgánů státní moci a právnické osoby zřízené zákonem jejich zrušení;
- u notáře a soudního exekutora zániku jejich funkce.

Znepřístupněnou datovou schránku je možné opět zpřístupnit na základě žádosti. Byla-li datová schránka na žádost znepřístupněna dvakrát za poslední rok, lze ji zpřístupnit nejdříve uplynutím 1 roku od jejího posledního znepřístupnění.

[59] § 8 Zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
[60] § 10 až § 13 Zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
[61] § 11 Zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

Zneplatnění přístupových údajů se provádí v případě, že byly ztraceny, odcizeny nebo zapomenuty přístupové údaje do datové schránky. MVČR zneplatní přístupové údaje oznámení (žádosti) a současně zašle této osobě do vlastních rukou nové přístupové údaje.

Přístupové údaje jsou zneplatněny pověřené osobě v případě zrušení pověření.

Statutárním orgánům, vedoucím organizačním složkám právnických osob nebo vedoucím orgánů veřejné moci apod. jsou zneplatněny přístupové údaje v případě, že přestanou plnit svou funkci. Současně jsou nové přístupové údaje zaslány novám orgánům.

Zrušení datové schránky MVČR provede po uplynutí 3 let ode dne:

- úmrtí fyzické osoby, případně dne, který je v rozhodnutí soudu o prohlášení za mrtvého uveden jako den úmrtí;
- výmazu podnikající fyzické osoby ze zákonem stanovené evidence;
- zániku právnické osoby nebo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, které nemají právního nástupce, případně ode dne jejich výmazu ze zákonem stanovené evidence;
- dne zrušení orgánu veřejné moci.

NEPŘEHLÉDNĚTE

Informační systém datových schránek (ISDS) je ISVS, který obsahuje informace o datových schránkách a jejich uživatelích.

Zajišťuje bezpečnou a průkaznou elektronickou komunikaci mezi orgány veřejné moci a fyzickými či právnickými osobami, popř. mezi orgány veřejné moci navzájem. ISDS je provozován nepřetržitě v režimu 24 x 7 s výjimkou plánovaných odstávek.

Správcem ISDS je Ministerstvo vnitra, provozovatelem ISDS je držitel poštovní licence (Česká pošta, s. p.). Ustanovení a pravidla závazné pro provoz ISDS jsou vymezena v Provozního řádu informačního systému datových schránek (ISDS).[62]

ISDS uchová datovou zprávu po dobu devadesáti dnů od okamžiku, kdy se do datové schránky přihlásila osoba, která má s ohledem na rozsah svých oprávnění přístup k dokumentu v datové zprávě obsaženém. Datovou zprávu doručenou fikcí uchovává ISDS po neomezenou dobu. Provozovatel má právo takové zprávy po devadesáti dnech od fikce doručení přemístit do off-line datového úložiště, ze kterého lze zprávu na žádost příjemce zprávy vrátit zpět do jeho datové schránky.

Datové zprávy i po 90 dnech lze automaticky uchovávat v **datovém trezoru.** Na rozdíl od dat archivovaných příjemcem, zprávy uložené datovém trezoru neztrácejí platnost. Datový trezor je doplňkovou (placenou) službou k datovým schránkám a lze ji objednat pouze k již existující datové schránce. Je nabízen ve dvou variantách:

- smluvní datový trezor, kdy smlouva je uzavírána na jeden rok a po roce je automaticky obnovována, je možné si vybrat ze 6 typů kapacit od 100 do 5 000 zpráv, popř. po dohodě archivovat i více než 5 000 zpráv;
- kreditní datový trezor lze aktivovat přímo v nastavení datové schránky, k dispozici jsou navíc tři kapacity (50, 150 a 250 zpráv) a volí se doba, po kterou jsou zprávy uloženy (6 měsíců, 1 nebo 2 roky).

Problematikou bezpečnosti ISDS se zabýváme v kap. 7.4.

[62] TESAŘ Pavel a Ondřej MENOUŠEK. MINISTERSTVO VNITRA ČR. *Provozní řád ISDS.*

9.1.1 DOKUMENTY

Jak lze využívat datové schránky pro doručování vidíme v následující tabulce.

Tabulka 9-1 Možnosti komunikace prostřednictvím datových stránek (

Příjemce / Odesilatel	Orgán veřejné moci	Právnická nebo fyzická osoba s datovou schránkou	Právnická nebo fyzická osoba bez datové schránky
Orgán veřejné moci	Vždy, umožňuje-li to povaha dokumentu	Vždy, umožňuje-li to povaha dokumentu	Není možné
Právnická nebo fyzická osoba s datovou schránkou	Může	Od 1. 7. 2010 je možná komunikace mezi datovými schránkami fyzických osob, podnikajících fyzických osob a právnických osob navzájem bez omezení obsahu (zpoplatněno)	Není možné
Právnická nebo fyzická osoba bez datové schránky	Není možné	Není možné	Není možné

Zdroj: vlastní

Dokumenty orgánů veřejné moci doručované prostřednictvím datové schránky, úkony prováděné vůči orgánům veřejné moci prostřednictvím datové schránky a dokumenty fyzických osob, podnikajících fyzických osob a právnických osob dodávané prostřednictvím datové schránky mají formu datové zprávy.

Pro doručování dokumentů orgánů veřejné moci prostřednictvím datové schránky platí. Umožňuje-li to povaha dokumentu, orgán veřejné moci:

- dokument doručuje jinému orgánu veřejné moci prostřednictvím datové schránky, pokud se nedoručuje na místě;
- má-li fyzická osoba, podnikající fyzická osoba nebo právnická osoba zpřístupněnu svou datovou schránku, doručuje dokument této osobě prostřednictvím datové schránky, pokud se nedoručuje veřejnou vyhláškou nebo na místě.

Dokument, který byl dodán do datové schránky, je doručen okamžikem, kdy se do datové schránky přihlásí oprávněná osoba. Nepřihlásí-li se do datové schránky oprávněná osoba ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty, pokud jiný právní předpis nevylučuje náhradní doručení, popř. je možné za podmínek stanovených jiným právním předpisem žádat o určení neúčinnosti doručení. Doručení dokumentu má stejné právní účinky jako doručení do vlastních rukou.

9.1.2 DATOVÁ ZPRÁVA

Systém datových schránek je určen pro doručování datových zpráv.

NEPŘEHLÉDNĚTE

Datovou zprávou jsou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou[63].

Můžeme se setkat s řadou názvů a typů datových zpráv.

Uživatel datové schránky, případně jiný subjekt, může hradit veškeré poštovní datové zprávy odeslané z datové schránky jiného uživatele, v tomto případě hovoříme o **dotované datové zprávě.**

Uživatel datové schránky může hradit dodání dokumentu, který je odpovědí na jeho poštovní datovou zprávu, pak se jedná o **odpovědní datovou zprávu.**

Poštovní datová zpráva je obchodní označení pro zprávy přenesené v rámci komerčního provozu dle § 18a Zákona 300/2008 Sb.[64], kdy za dodání dokumentu podle náleží provozovateli informačního systému datových schránek odměna a tyto zprávy jsou doručovány okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k tomuto dokumentu.

Pokud uživatel odesílá prostřednictvím klientského rozhraní datovou zprávu na více příjemců, použije se funkce hromadného zasílání datových zpráv. Způsob odesílání datové zprávy se může lišit v závislosti na způsobu implementace jednotlivých dodavatelů těchto aplikací. Jedna hromadná zpráva může mít maximálně 50 adresátů.

Systémová datová zpráva je specifický typ datové zprávy, odeslané buď ze systémové schránky správce nebo provozovatele. Slouží k notifikaci[65] o důležitých změnách služeb ISDS, je posílána při vybraných událostech, týkajících se datové schránky, a také jako „uvítací“ zpráva pro nové uživatele.

Datovou zprávu tvoří **obálka** a **obsah** zprávy. Na obálce je uvedeno jméno odesílatele, datum odeslání a datum přijetí. Datová zpráva mimo vlastního obsahu obsahuje elektronický podpis (pokud zákon vyžaduje, musí být dokument podepsán zaručeným elektronickým podpisem), časové razítko a informaci, zda-li tuto zprávu odeslala právnická osoba, orgán veřejné moci, fyzická osoba či podnikající fyzická osoba. Obsahem zprávy může být jedna či více příloh.

Zpráva musí být ve formátu, který je podporován datovými schránkami a příjemce tento typ formátu přijímá. Nelze odesílat spustitelné a komprimované soubory. Povolené formáty datových zpráv dodávaných do datových schránek jsou stanoveny v příloze č. 3 Vyhlášky 194/2009 Sb.[66] Provozovatel má právo nepřijmout k odeslání datovou zprávu obsahující škodlivý kód.

[63] Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů

[64] Ministerstvo umožní na žádost fyzické osoby, podnikající fyzické osoby nebo právnické osoby dodávání dokumentů z datové schránky jiné fyzické osoby, podnikající fyzické osoby nebo právnické osoby do datové schránky této osoby.

[65] Sdělení nějaké skutečnosti, upozornění na něco, např. na nově příchozí elektronickou poštu.

[66] Vyhláška 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

Informační systém datových schránek umožňuje kromě doručování vlastních dokumentů i doručování elektronických podpisů a časových razítek v běžně rozšířených formátech:

- CER, CRT, DER, PK7 - formáty certifikátů dle standardu X.509•
- P7B, P7C, P7F, P7M, P7S - formáty certifikátů a elektronických podpisů dle PKCS#7
- TST, TSR - formáty pro elektronické razítko•

Systém umožňuje odeslat pouze datovou zprávu s přílohami, jejichž celková velikost je maximálně 10 MB. Přípustné formáty datové zprávy[67] dodávané do datové schránky jsou:[68]:

- PDF (Portable Document Format);
- PDF/A (Portable Document Format for the Long-term Archiving);
- XMl (Extensible Markup Language Document)[69];
- FO/ZFO (602XML Filler dokument);
- HTMl/HTM (Hypertext Markup Language Document);
- ODT (Open Document Text);
- ODS (Open Document Spreadsheet);
- ODP (Open Document Presentation);
- TXT (prostý text);
- RTF (Rich Text Format);
- DOC/DOCX (MS Word Document);
- XLS/XSLX (MS Excel Spreadsheet);
- PPT/PPTX (MS PowerPoint Presentation);
- JPG/JPEG/JFIF (Joint Photographic Experts Group File Interchange Format);
- PNG (Portable Network Graphics);
- TIF/TIFF (Tagged Image File Format);
- GIF (Graphics Interchange Format);
- MPEG1/MPEG2 (Moving Picture Experts Group Phase 1/Phase 2);
- WAv (Waveform Audio Format);
- MP2/MP3 (MPEG-1 Audio Layer 2/Layer 3);
- ISDOC/ISDOCX (Information System Document) verze 5.2 a vyšší;
- EDI (mezinárodní standard EDIFACT, standardy ODETTE a EANCOM pro elektronickou výměnu obchodních dokumentů - EDI);
- DWG (AutoCAD DraWinG File Format) verze 2007 a vyšší;
- SHP/DBF/SHX/PRJ/QIX/SBN/SBX (ESRI Shapefile);
- DGN (Bentley MicroStation Format) verze V7 a V8;
- GML/GFS/XSD (Geography Markup Language Document).

K odesílané zprávě se připojí doručenka a dodejka a jsou viditelné jako datum a čas kdy byla zpráva dodána a doručena.

[67] Vyhláška č. 212/2012 Sb., Příloha 3

[68] Formáty jsou přípustnými formáty datové zprávy dodávané do datové schránky, obsahují-li odpovídající příponu.

[69] Formát je přípustným formátem datové zprávy dodávané do datové schránky, odpovídá-li veřejně dostupnému XSD schématu publikovanému příjemcem datové zprávy.

9.1.3 KONVERZE DOKUMENTŮ

NEPŘEHLÉDNĚTE

Konverzí se rozumí se úplné převedení dokumentu:

- v listinné podobě do dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky, nebo
- obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky.

Dokument, který provedením konverze vznikl, má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením vznikl. Má-li být podle jiného právního předpisu předložen dokument v listinné podobě, zejména aby byl užit jako podklad pro vydání rozhodnutí, je tato povinnost splněna předložením jeho výstupu.

Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy. Konverzi provádějí na žádost kontaktní místa veřejné správy nebo z moci úřední orgány veřejné moci pro výkon své působnosti. Odst. 5 § 24 Zákona 300/2008 Sb. stanovuje, kdy se konverze neprovádí:

- v případě provedení konverze na žádost, nebylo-li k dokumentu obsaženém v datové zprávě připojeno kvalifikované časové razítko,
- v případě provedení konverze na žádost, nebyl-li dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou toho, kdo dokument vydal nebo vytvořil,
- byl-li dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem oprávněné osoby nebo označen uznávanou elektronickou značkou toho, kdo příslušnou datovou zprávu vydal nebo vytvořil, a nebyla-li shledána shoda tohoto dokumentu s výstupem.

Podrobností provádění autorizované konverze dokumentů upravuje Vyhláška 193/2009 Sb.[70] Tato vyhláška obsahuje:

- technické náležitosti:
  - provádění autorizované konverze dokumentů;
  - dokumentu, který provedením konverze vznikl;
  - dokumentu, jehož převedením výstup při konverzi vznikl;
- vzor osvědčení o vykonání zkoušky zaměstnance provádějícího konverzi na žádost.

Konverze se provádí prostřednictvím elektronické aplikace systému kontaktních míst veřejné správy přístupné způsobem umožňujícím dálkový přístup.

Konverze do dokumentu obsaženého v datové zprávě se provádí za použití technického zařízení umožňujícího převod dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě, které má parametry:

- rozlišení snímání nejméně 300 x 300 dpi;
- barevnou hloubku nejméně 24 bitů nebo 256 stupňů šedi, jde-li výlučně o černobílé převádění;
- velikost formátu snímací plochy nejméně A4.

Formáty výstupu jsou PDF verze 1.7 a vyšší.

[70] Vyhláška 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů.

Konverze datového souboru (formáty PDF verze 1.3 a vyšší nebo PDF/A) do dokumentu v listinné podobě se provádí pomocí tiskárny, která umožňuje:

- rozlišení tisku nejméně 300 dpi
- tisk barevného výstupu (to neplatí, jde-li výlučně o černobílé převádění);
- velikost formátu výstupu nejméně A4

Vstup se převádí zpravidla černobíle. Ztratila-li by se informace vyjádřená barvou, vstup se převede barevně.

Vstupy a výstupy mohou také probíhat:

- prostřednictvím datového úložiště elektronické aplikace systému kontaktních míst veřejné správy přístupné způsobem umožňujícím dálkový přístup;
- na technickém nosiči dat s laserovým záznamem (CD, DVD).

Vstup obsažený v datové zprávě nesmí obsahovat škodlivý kód, který je způsobilý přivodit škodu na informačním systému subjektu provádějícího konverzi nebo na informacích zpracovávaných subjektem provádějícím konverzi.

Vstup v listinné podobě nesmí být ve stavu způsobilém poškodit snímací zařízení nebo ve stavu způsobilém přivodit provedením konverze své poškození.

9.2 CZECH POINT A KOMUNIKAČNÍ INFRASTRUKTURA VEŘEJNÉ SPRÁVY

CZECH POINT (Český Podací Ověřovací Informační Národní Terminál) je asistované místo výkonu veřejné správy, kde každý člověk může získat všechny informace o údajích, které o něm vede stát v centrálních registrech nebo učinit jakékoliv podání ke státu.

Např. se jedná:

- výpis z Katastru nemovitostí;
- výpis z Obchodního rejstříku;
- výpis z Živnostenského rejstříku;
- výpis z Rejstříku trestů;
- výpis z Rejstříku trestů právnické osoby;
- přijetí podání podle živnostenského zákona (§ 72);
- žádost o výpis nebo opis z Rejstříku trestů podle zákona č. 124/2008 Sb.;
- výpis z bodového hodnocení řidiče;
- vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů;
- podání do registru účastníků provozu modulu autovraků ISOH;
- výpis z insolvenčního rejstříku;
- datové schránky;
- autorizovaná konverze dokumentů;
- centrální úložiště ověřovacích doložek;
- úschovna systému Czech POINT;
- CzechPOINT@office;
- základní registry.

NEPŘEHLÉDNĚTE

Komunikační infrastruktura veřejné správy (KISV) jsou veškeré prostředky, kterými subjekty veřejné správy komunikují mezi sebou navzájem a ve vztahu k občanovi.

Představuje komunikační kanály veřejné správy, které tvoří jednotnou komunikační infrastrukturu pro elektronické úřadování. Cílem je sjednocení různých datových linek subjektů veřejné správy do jedné datové sítě.

Představuje základ fungování eGovernmentu a zabezpečuje bezpečné propojení mezi veřejností a veřejnou správou přes CZECH POINT, propojení sítí a systémů do společného prostředí a efektivní přístup k informacím pro ty, kteří k tomu mají oprávnění 1.

Centrální místo služeb (CMS) zajišťuje vzájemné řízené a bezpečné propojování subjektů veřejné a státní správy a komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích, jakými jsou internet nebo komunikační infrastruktura EU. Tvoří jediné logické místo propojení jednotlivých operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS.

CMS 2.0 by mělo znamenat zřízení propojovacího místa pro čtyři v současnosti existující základní komunikační prostředí:

- internet;
- KIVS;
- centrální eGON služby;
- komunikační prostředí EU (např. S-TESTA).

Pro každé z těchto prostředí definuje standardy komunikační, bezpečnostní, standardy poskytovaných služeb a jejich rozhraní.

10 PORTÁL VEŘEJNÉ SPRÁVY

Nepostradatelným prvkem výkonu veřejné správy je komunikace občanů a právnických osob s veřejnými orgány. Toto z velké části zajišťuje portál veřejné správy, který byl definován v § 6f Zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

NEPŘEHLÉDNĚTE

Portál veřejné správy[71] je ISVS zajišťující přístup k informacím státních orgánů, orgánů územních samosprávných celků, orgánů veřejné moci, které nejsou státními orgány ani orgány územních samosprávných celků a komunikaci s veřejnými orgány.

Správcem portálu je Ministerstvo vnitra ČR.

Komunikaci s veřejnými orgány zajišťuje portál prostřednictvím:

- datových schránek;
- kontaktních míst veřejné správy.

Portál zajišťuje přístup k informacím získaným na základě informační činnosti veřejných orgánů zejména v oblasti:

- sociálního zabezpečení;
- zdravotnického zabezpečení;
- správy veřejných financí;
- dotací;
- veřejných zakázek;
- státní statistické služby;
- evidence a identifikace osob, jejich součástí a práv a povinností těchto osob či jejich součástí;
- tvorby a publikace právních předpisů atd.

Portál rovněž zajišťuje přístup k informacím fyzických a právnických osob, zejména k formulářům v elektronické podobě komunikaci s fyzickými osobami a právnickými osobami.

Přístup k informacím fyzických osob a právnických osob je zajišťován na základě písemné smlouvy mezi správcem portálu osobou, k jejímž informacím je zajištěn přístup, přístup je za úplatu. Správce portálu stanovuje podmínky, za kterých budou informace prostřednictvím portálu zpřístupněny a pravidla pro stanovení výše úplaty a způsob její úhrady.

Portál veřejné správy[72] vznikl sloučením portálů do jednoho funkčního celku:

- Portál veřejné správy (původní);
- Portál datových schránek.

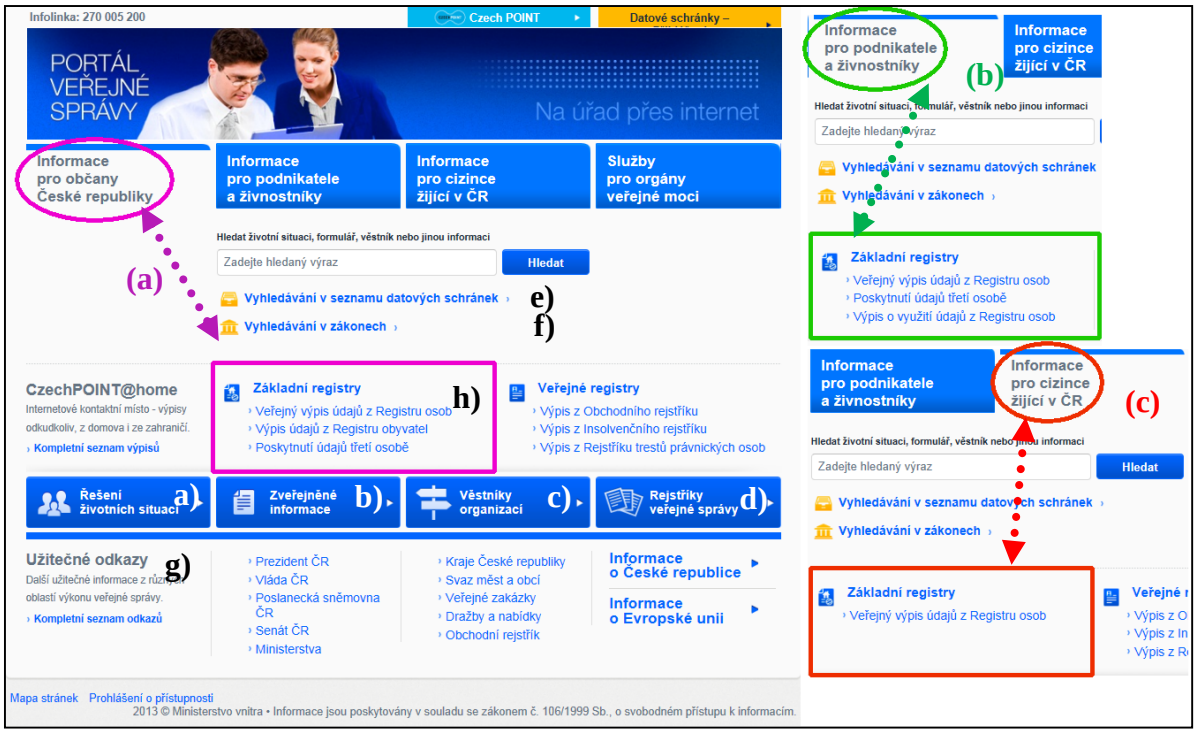
Je rozdělen na informační sekce:

(a) informace pro občany;
(b) informace pro podnikatele a živnostníky;
(c) informace pro cizince žijící v ČR;

[71] § 6f Zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
[72] http://www.mvcr.cz/clanek/portal-verejne-spravy.aspx

(d) služby pro orgány veřejné.

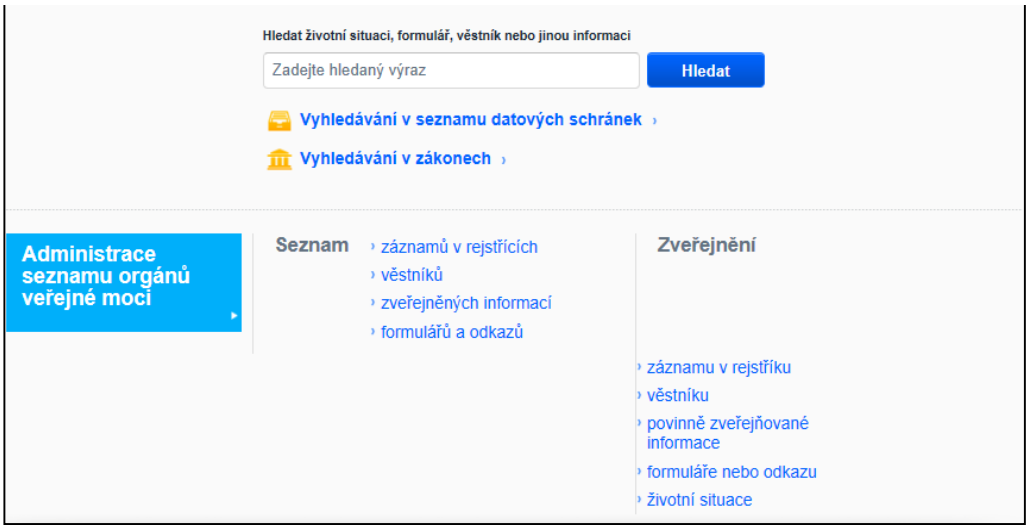
Obrázek 10-1 Portál veřejné správy - informace pro občany ČR, pro podnikatele a živnostníky, pro cizince žijící v ČR



Zdroj: http://portal.gov.cz/

Strukturu sekce „Služby pro orgány veřejné moci“ je poněkud jiná a je znázorněna na následujícím obrázku.

Obrázek 10-2 Portál veřejné správy - služby pro orgány veřejné moci



Zdroj: http://portal.gov.cz/portal/ovm/

Datové prvky portálu dodávají samy orgány veřejné moci a můžeme je rozdělit do okruhů:

a) Řešení životních situací, což jsou strukturované popisy řešení úkonů ve vztahu ke státní správě s přesně danou strukturu. Struktura informací se liší podle toho, pro koho jsou určeny (občan, podnikatel, cizinec atd.). U každého záznamu uveden:
   - odkaz na stránku úřadu nebo instituce v rámci portálu veřejné správy, kde lze nalézt, všechny ostatní životní situace, které daný úřad publikoval;
   - seznam všech dalších publikovaných informací včetně elektronických formulářů pro elektronické podání.

b) Zveřejněné informace jsou povinně zveřejňované informace, které jsou zveřejňovány na základě různých legislativních předpisů.

c) Věstníky organizací jsou publikační sbírky předpisů a metodických pokynů vydávané ústředními správními orgány a dalšími institucemi. Věstníky jsou v rámci portálu vydávány a jsou k dispozici ke stažení ve formátu PDF. Každý věstník obsahuje informaci o tom, která instituce jej zveřejnila a od kterého data je předpis nebo metodický pokyn účinný.

d) Rejstříky umožňují právnickým i fyzickým osobám získávat informace o státní správě z jediného zdroje. Orgány veřejné moci mohou zveřejňovat nejrůznější nestrukturované dokumenty v takové podobě, v jaké jim to ukládá platná legislativa, popř. zveřejňovat data, např. strojově zpracovatelné informace.

Portál veřejné správy zahrnuje i další funkcionality:

e) Vyhledávání v seznamu datových schránek, integrální součást informačního systému datových schránek, obsahuje aktuální údaje o držitelích datových schránek.

f) Vyhledávání v zákonech umožňující vyhledávání informací v databázi legislativních norem a zákonů právního informačního systému ASPI.

g) Užitečné odkazy obsahují další užitečné informace z různých oblastí výkonu veřejné správy, informace o České republice a o Evropské unii.

h) Registry, odkazy na získáváni informací ze základních registrů a veřejných registrů.

Na portálu je možné vyhledat různé formuláře elektronického podání orgánů veřejné moci, jejichž prostřednictvím je možné provést podání vůči konkrétnímu orgánu prostřednictvím datové schránky.

10.1 PŘÍSTUPNOST WEBU

V rámci Evropské unie je realizován dlouhodobý program eAccessibility, který se zaměřuje na práva hendikepovaných osob, s důrazem na elektronickou výměnu informací. V rámci tohoto programu je za výchozí metodiku považována metodika Web Content Accessibility Guidelines (WCAG)[73]. Členské státy Evropské unie však mohou mít vytvořeny vlastní metodiky, které však musí být po obsahové stránce v souladu s WCAG, což platí pro Českou republiku.

[73] http://www.w3.org/TR/WCAG20/

10.1.1 METODIKA WCAG

Metodika WCAG se zaměřuje na čtyři okruhy problémů (principy)[74]:

1. Zřetelnost (vnímatelnost):
   - poskytování textových alternativ pro veškerý netextový obsah tak, aby mohl být změněn na jiné formy, které lidé potřebují, např. velké písmo, Braillovo písmo, řeč, symboly, nebo jednodušší jazyk
   - poskytování alternativ multimédií závislých na čase
   - vytváření obsahu, který lze prezentovat různými způsoby (například jednodušší vzhled), aniž by došlo ke ztrátě informací nebo struktury
   - usnadňování uživatelům slyšet a vidět obsah, včetně odlišení popředí od pozadí
2. Ovladatelnost:
   - dostupnost kontroly všech funkcí z klávesnice
   - poskytování dostatku času uživatelům na přečtení a použití obsahu
   - nevytváření obsahu, o němž je známo, že způsobuje záchvaty
   - usnadnění uživatelům navigace, hledání obsahu a zjišťování, kde se nacházejí
3. Srozumitelnost
   - vytváření čitelného a srozumitelného textový obsahu
   - vytváření webových stránek, které se objevují a působí předvídatelným způsobem
   - pomoc uživatelům vyvarovat se chyb a opravovat chyby
4. Robustnost
   - maximalizace kompatibility se současnými i budoucími uživatelskými agenty, včetně podpůrných technologií (asistivních technologií).

Aby webové stránky jsou v souladu s WCAG 2.0, musí být splněny požadavky.

ÚROVEŇ SHODY

Jednotlivá pravidla (Guidelines) v rámci čtyřech principů obsahují tzv. kritéria úspěchu (Success Criteria), určená pro konkrétní testování a ověřování přístupnosti. Jednotlivým kontrolním kritériím je přiřazena určitá priorita:

- kritéria priority 1 (označená Level A) jsou nezbytná k dosažení minimální úrovně přístupnosti a mohou být adekvátně aplikována na veškerý webový obsah;
- kritéria priority 2 (označená Level AA) dále napomáhají zvýšit přístupnost a mohou být adekvátně aplikovány na veškerý webový obsah;
- kritéria priority 3 (označená Level AAA) pomáhají dosahovat ještě většího stupně přístupnosti, ale nemusí být nutně aplikovány na veškerý webový obsah.

[74] Podrobně na http://www.zdrojak.cz/serialy/wcag-2-0/

Míra shody prověřované webové stránky s pravidly je potom určena právě na základě splnění těchto kritérií úspěchu. Shoda se dělí do třech úrovní důležitosti:

- A (základní, nejnižší) – jsou splněna všechna kritéria priority 1;
- AA (rozšířený) – jsou splněna všechna kritéria priority 1 a 2;
- AAA (úplný, nejvyšší) – jsou splněna všechna kritéria priority 1, 2 a 3.

Kritéria musí být splněna pro celou webovou stránku, nikoliv pouze pro některou část. Pokud webové stránky představují určitý proces (posloupnost kroků, které je třeba splnit pro dosažení cíle), pak všechny tyto stránky musí odpovídat zadané úrovni nebo lepší. Musí být uplatňovány pouze dostupné technologie. Pokud v některé části využity technologie nevyhovujícím způsobem, pak nesmí zablokovat přístup ke zbytku stránky.

10.1.2 PRAVIDLA V ČESKÉ REPUBLICE

Ministerstvo vnitra stanovilo vyhláškou o přístupnosti[75] pravidla, která mají zajistit, aby se s informacemi souvisejícími s výkonem veřejné správy uveřejňovanými na webu mohly v nezbytném rozsahu seznámit i osoby se zdravotním postižením, popř. aby byl umožněn přístup k webovým stránkám, které tomuto požadavku vyhovují.

Příloha této vyhlášky stanovuje 33 pravidel rozdělených do 6 skupin. Tato pravidla jsou podrobněji zpracována v metodickém pokyn MVČR[76].

OBSAH WEBOVÝCH STRÁNEK MUSÍ BÝT DOSTUPNÝ A ČITELNÝ

1. Každý netextový prvek nesoucí významové sdělení musí mít svou textovou alternativu (P)[77].
   - všechny obrázky, které mají informační význam, musí mít alternativně textové vyjádření významového sdělení obrázku
   - do webové stránky se nesmí zařazovat text ve formě obrázku
   - ani pokud se jedná o ochranné pravidlo, třeba před "vykrádáním" adres elektronické pošty roboty
2. Multimediální prvky nesoucí významové sdělení musí být doplněny textovými titulky, jestliže nejsou jen alternativou k existujícímu textovému obsahu (P)
   - uživatelům musí být k dispozici textové titulky nebo jiný textový zápis
3. Pokud to charakter webových stránek nevylučuje, informace sdělované prostřednictvím skriptů, objektů, appletů, kaskádových stylů, cookies a jiných doplňků na straně uživatele, musí být dostupné i bez kteréhokoli z těchto doplňků a stránky musí být standardně ovladatelné. V opačném případě sdělí orgán veřejné správy tyto informace jiným způsobem. (PP)[78]
   - stránka musí obsahovat všechny podstatné informace, i když uživatel aktuálně nemůže používat tyto prvky

---

[75] Vyhláška 64/2008 Sb. o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti) Vyhláška 64/2008 Sb. o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)

[76] RADA, Michal a kol. MINISTERSTVO VNITRA ČR. *Metodický pokyn: k vyhlášce č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)*.

[77] (P) - povinné

[78] (PP) – podmíněně povinné, orgán veřejné správy má možnost tato pravidla neuplatnit, ale musí je v prohlášení o přístupnosti odůvodnit

- stránky musí být bez těchto doplňků standardně ovladatelné
- musí být k dispozici každá webová stránka
- všechny odkazy musí být funkční

4. Informace sdělované vizuální podobou webových stránek, tvary jednotlivých prvků, jejich velikostí, pořadím nebo umístěním musí být dostupné i v případě, že uživatel nemůže tyto aspekty vnímat. (P)
   - není možné vyjadřovat informační sdělení pouze vizuální podobou stránek či jednotlivých prvků
   - pokud mají vizuální aspekty důležitou informační hodnotu, musí být vždy uživatelům k dispozici i jiným způsobem, např. pomocí běžného textu nebo sémantickými (významovými) značkami zdrojového kódu
   - je tedy nutné si představit webovou stránku jako lineární seznam objektů
5. Informace sdělované barvou musí být dostupné i bez barevného rozlišení
6. Barvy popředí a pozadí textu (nebo textu v obrázku) musí být vůči sobě dostatečně kontrastní, jestliže text nese významové sdělení (P)
7. Velikost písma musí být možné zvětšit alespoň na 200 % a zmenšit alespoň na 50 % původní hodnoty pomocí standardních funkcí prohlížeče. Při takové změně velikosti nesmí docházet ke ztrátě obsahu nebo funkcionality. (P)
   - pokud je to možné, nezpůsobuje nutnost použití horizontálního posuvníku
   - předpisy definující velikost písma na webové stránce proto neobsahují jednotky

PRÁCI S WEBOVOU STRÁNKOU ŘÍDÍ UŽIVATEL

8. Obsah ani kód webové stránky nesmí předpokládat ani vyžadovat konkrétní výstupní či ovládací zařízení (P)
   - stránka proto nemůže předpokládat, že
   - uživatel používá konkrétní zařízení
   - určitá tlačítka klávesnice či myši existují a mají přiřazenu určitou funkci
   - stránka nesmí technicky omezit přístup k jejímu kódu
   - nesmí být nijak omezeno předání a zobrazení, či další zpracování zdrojového kódu stránky
   - nesmí být omezena (nebo zakázána) funkce kontextové nabídky
   - je-li stránky (i její část) optimalizována pro určitý prohlížeč, či rozlišení, musí být obsah stránky jasně interpretován i v ostatních technologiích
9. Obsah ani kód webové stránky nesmí předpokládat ani vyžadovat konkrétní způsob použití ani konkrétní programové vybavení. Pokud je předpokládáno či vyžadováno konkrétní programové vybavení, může to být pouze z důvodu technické nerealizovatelnosti přizpůsobení obsahu a kódu webové stránky všem programovým vybavením (PP)

10. Načtení nové webové stránky či přesměrování musí být možné jen po aktivaci odkazu nebo po odeslání formuláře (P)
    - obsah webové stránky se nesmí měnit, dokud uživatel neprovede akci, která je k takové změně jasným impulsem
    - pouhá změna hodnoty formulářového prvku, aniž by byl formulář odeslán, nebo kliknutí na prvek, který není odkazem, smí ovlivnit jenom stávající obsah webové stránky
11. Načtení nové webové stránky do nového okna prohlížeče musí být možné jen v odůvodněných případech a uživatel na to musí být předem upozorněn (P)
    - způsob otevírání nových webových stránek nesmí být v kódu nijak specifikován a je ponechán na volbě uživatele
    - pouze v odůvodněných případech mohou být webové stránky otevírány v novém okně, uživatel na to musí být jasně a předem upozorněn
12. Na webové stránce nesmí docházet rychleji než třikrát za sekundu k výrazným změnám barevnosti, jasu, velikosti nebo umístění prvku (P)
    - žádná animace či dynamicky se měnící prvek na webové stránce se trvale (více než třikrát po sobě) nemění s frekvencí větší než třikrát za sekundu
    - blikání nesmí být v HTML kódu použito vůbec
    - k těmto změnám může docházet v audiozáznamech či animacích, které budou na webových stránkách k dispozici
13. Zvuk, který zní na webové stránce déle než tři sekundy, musí být možné na této webové stránce vypnout nebo upravit jeho hlasitost (P)
    - znějící zvuk na pozadí webové stránky omezuje schopnost slyšet informace hlasového výstupu a způsobuje pokles či ztrátu koncentrace
    - stránka nesmí možnost omezit potlačit nebo zastavit přehrávání zvuku určitou klávesou, nebo kombinací kláves
14. Časový limit pro práci s webovou stránkou musí být dostatečný. Pokud to nevylučuje charakter webové stránky, může uživatel časový limit prodloužit nebo vypnout (P)

INFORMACE MUSÍ BÝT SROZUMITELNÉ A PŘEHLEDNÉ

15. Webové stránky musí sdělovat informace jednoduchým jazykem a srozumitelnou formou, pokud to charakter webové stránky nevylučuje (PP)
    - ke sdělení informací se nepoužívá odborná terminologie, cizí slova a méně obvyklé významy známých slov, jestliže nejsou v dokumentu řádně vysvětleny, nebo jestliže nejsou vysvětleny jinde dostupnou formou
    - v textu se používají kratší věty místo dlouhých a komplikovaných souvětí
    - pouze v případě, že jsou stránky určeny přímo určité skupině odborníků a není možné jejich obsah přeformulovat do jednoduchého a srozumitelného jazyka, není toto pravidlo nutné uplatnit
16. Rozsáhlé obsahové bloky musí být rozděleny do menších výstižně nadepsaných celků (P)

17. Bloky obsahu, které se opakují na více webových stránkách daného orgánu veřejné správy, je možné přeskočit. Pokud webové stránky nemají velký rozsah, nemusí být zajištěno přeskočení opakujících se bloků obsahu (PP)
    - jedná se např. o hlavičku, navigaci, postranní sloupec, hlavní obsah, patičku apod.
    - je podstatné, aby se na každé stránce rychle a pohodlně dalo dostat k obsahovému bloku

OVLÁDÁNÍ WEBOVÝCH STRÁNEK MUSÍ BÝT JASNÉ A SROZUMITELNÉ

18. Navigace musí být srozumitelná a konzistentní a na všech webových stránkách orgánu veřejné správy obdobná. Od ostatního obsahu webové stránky musí být zřetelně oddělena (P)
    - navigační odkazy nesmí být příliš dlouhé, musí být srozumitelné a dobře vyjadřovat, kam vedou
    - navigační odkazy musí být sdruženy do samostatných bloků a nesmí se mísit s vlastním obsahem stránky
19. Každá webová stránka (kromě úvodní webové stránky) musí obsahovat odkaz na vyšší úroveň v hierarchii webových stránek a odkaz na úvodní webovou stránku (P)
20. Pokud se jedná o rozsáhlejší webové stránky, musí být kromě navigace k dispozici rovněž vyhledávání nebo odkaz na mapu webových stránek. Odkaz na mapu webových stránek nebo vyhledávací formulář musí být k dispozici na každé webové stránce. (PP)
    - odkaz na mapu webu nebo vyhledávací formulář musí být k dispozici na každé webové stránce na stejném místě
    - mapa stránek by měla obsahovat strukturovaný seznam všech stránek (nebo sekcí na stránkách) a to tak, jak jsou jednotlivé stránky, nebo sekce řazeny v hierarchii webu
    - výsledky vyhledávání by měly dobře popisovat a uvádět jednotlivé stránky, které jsou vyhledány
21. Každá webová stránka musí mít výstižný název odpovídající jejímu obsahu (P)
    - v názvu webové stránky musí být proto vždy uveden jak název celého webu, tak název konkrétní stránky
22. Každý formulářový prvek musí mít popisek vystihující požadovaný obsah (P)
23. Pokud uživatel učiní chybu při vyplňování webového formuláře, musí být k dispozici informace o tom, ve které položce je chyba. Pokud to charakter webového formuláře nevylučuje, musí být k dispozici rovněž informace, jak tuto chybu odstranit (PP)
    - informace o chybě musí být přehledně a srozumitelně zobrazena před formulářem (co nejblíže začátku stránky) a může být doplňkově k dispozici i u chybně vyplněných polí
    - je-li to možné, oznámení o chybě rovněž obsahuje informaci o tom, proč chyba vznikla a jakým způsobem ji opravit
    - uživateli se musí umožnit, aby ve své práci navázal na předchozí stav, tedy nikoliv aby daný úkon musel provádět od začátku (pokud se nejedná bezpečnostní úkon, který by to znemožňoval)

24. Text odkazu nebo jeho přímo související text musí výstižně popisovat cíl odkazu. Jestliže odkaz vede na jiný typ souboru, než je webová stránka, musí být odkaz doplněn sdělením o typu, případně o velikosti tohoto souboru (P)
    - pokud odkaz vede na jiný typ obsahu, než je webová stránka, tj. například na soubory ve formátu PDF, RTF, XLS, které se obvykle zobrazují v jiné aplikaci, než je internetový prohlížeč, je tato skutečnost z označení odkazu zřetelná
25. Každý rám musí mít vhodné jméno či popis vyjadřující jeho smysl a funkčnost (P)
    - některá zobrazovací či hlasová zařízení neumějí s rámci pracovat a prezentují je jednotlivě
    - všechny rámce musí být pojmenovány tak, aby jejich název vystihoval smysl a funkčnost daného rámce, či objektu ve vloženém rámci

ZDROJOVÝ KÓD MUSÍ BÝT TECHNICKY ZPŮSOBILÝ A STRUKTUROVANÝ

26. Sémantické značky, které jsou použity pro formátování obsahu, musí být použity ve zdrojovém kódu tak, aby odpovídaly významu obsahu (P)
    - sémantické značky jazyka XHTML se používají pro vyjádření významu daného prvku (nadpis, citace, zdůraznění atp.)
    - pomocná výstupní zařízení umějí tyto značky používat a význam takto označených prvků zprostředkovávají svým uživatelům.
27. Prvky značkovacího jazyka, které jsou párové, musí mít vždy uvedenu počáteční a koncovou značku. Značky musí být správně zanořeny a nesmí docházet k jejich křížení (P)
    - syntaktická správnost vůči zvolené specifikaci značkovacího jazyka je klíčová po správnou funkcionalitu výstupních zařízení, některá nemusí být k chybám v syntaxi značkovacího jazyka tolerantní
28. Ve zdrojovém kódu musí být určen hlavní jazyk obsahu webové stránky (P)
29. Prvky tvořící nadpisy a seznamy musí být korektně vyznačeny ve zdrojovém kódu a musí být výstižné (P)
    - prostředcích asistivních technologií se používají specifické postupy, zpřístupňující uživateli strukturu nadpisů stránky umožňující snadný pohyb mezi nimi, proto musí být značkami označeny všechny prvky
30. Je-li tabulka použita pro zobrazení tabulkových dat, musí obsahovat značky pro záhlaví řádků nebo sloupců (P)
    - alternativní výstupní zařízení se snaží prezentovat tabulky co nejpochopitelnější formou (např. nevidomým)
    - tabulky musí obsahovat prvky vyznačující záhlaví řádků nebo sloupců před každým řádkem/sloupcem, popř. před každou buňkou tabulky.
31. Obsah všech tabulek musí dávat smysl čtený po řádcích zleva doprava (P)
    - pomocná výstupní zařízení obvykle prezentují obsah tabulek po řádcích, každý řádek pak po buňkách zleva doprava
    - obsah každé tabulky musí vždy dávat smysl, je-li čtený po řádcích

PROHLÁŠENÍ O PŘÍSTUPNOSTI WEBOVÝCH STRÁNEK

32. Každá webová stránka musí vždy obsahovat prohlášení o tom, že forma uveřejnění informací je v souladu s touto vyhláškou (prohlášení o přístupnosti) nebo odkaz na toto prohlášení (P)
    - orgán také v prohlášení přístupnosti sdělí, jakým způsobem budou informace, které nejsou na webových stránkách přístupné, sděleny tazateli jinou formou
33. Pokud orgán veřejné správy některá z podmíněně povinných pravidel uvedených pod čísly položek 3, 9, 14, 15, 17, 20 a 23 v souladu s uvedenou podmínkou neuplatní, musí uveřejnit tuto informaci v prohlášení o přístupnosti, a to jejich číselným výčtem, včetně příslušného odůvodnění (PP)
    - pravidla 3, 9, 14, 15, 17, 20 a 23 mají jsou podmíněně povinná
    - neuplatnění konkrétního pravidla musí být v prohlášení o přístupnosti odůvodněna tak, aby bylo jednoznačně patrné, že se podmínka uvedená v pravidle vztahuje či nevztahuje na orgán

11 INFORMAČNÍ SYSTÉMY EVROPSKÉ UNIE

Orgány Evropské unie přijímají řadu opatření, které přímo nebo zprostředkovaně souvisí s informačními systémy. Jsou zřizovány agentury, které mají za úkol řídit různé evropské informační systémy. Například 22. března 2012 byla otevřena v estonském Tallinnu Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva[79], jejímž hlavním úkolem je zajišťovat provoz Vízového informačního systému a systém Eurodac. Od roku 2013 bude agentura také řídit druhou generaci Schengenského informačního systému.

Společné řízení trojice uvedených systémů jedinou agenturou zlepší z dlouhodobého pohledu produktivitu a omezí provozní náklady, neboť řada činností spojených s jejich provozem bude společná pro všechny, jako např. zadávání veřejných zakázek nebo činnosti související s řízením projektů. Hlavním úkolem agentury bude provozní řízení těchto systémů a udržování jejich nepřetržitého provozu. Spolu s těmito provozními úkoly bude agentura vykonávat další související činnosti, k nimž patří přijímání bezpečnostních opatření, podávání zpráv, publikační činnost, monitorování a poskytování informací, jakož i organizace zvláštní odborné přípravy.

Schengenský informační systém (SIS) je systém, který napomáhá při zajišťování bezpečnosti v rámci prostoru svobody, bezpečnosti a práva EU. V zásadě se jedná o databázi s přísnými pravidly ochrany údajů, která umožňuje výměnu informací o osobách a předmětech mezi vnitrostátními donucovacími orgány. Modernizovaná verze tohoto systému, nazvaná SIS II, by měla být spuštěna v roce 2013.

Vízový informační systém (VIS), k jehož úplnému uvedení do provozu by mělo dojít na podzim tohoto roku, bude podporovat provádění společné vízové politiky a pomáhat při zajišťování účinné ochrany hranic. Tento systém umožní, aby členské státy schengenského prostoru zadávaly, aktualizovaly a vyhledávaly informace o vízech (včetně biometrických údajů) elektronickou cestou.

Eurodac je systém, který umožňuje srovnávání otisků prstů žadatelů o azyl a nelegálních přistěhovalců. Toto srovnávání je nezbytné pro rychlé určení členského státu, který bude zodpovědný za posouzení žádosti o azyl.

Úkoly agentury spojené s vývojem a provozem budou vykonávány ve francouzském Štrasburku, zatímco zálohové místo se bude nacházet v rakouském Sankt Johann im Pongau.[80]

Informační systém pro evropské veřejné zakázky (Simap) poskytuje přístup k nejdůležitějším informacím o veřejných zakázkách v Evropě.

Indect je komplexní monitorovací a vyhodnocovací systém Evropské unie, který má sloužit k vyhledávání a detekci lidí a předmětů.

[79] EU. Nařízení evropského parlamentu a rady (eu) č. 1077/2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:286:0001:0017:CS:PDF

[80] http://www.consilium.europa.eu/homepage/highlights/reducing-the-costs-of-managing-the-eus-large-scale-it-systems?lang=cs

11.1 SCHENGENSKÝ INFORMAČNÍ SYSTÉM

Systém SIS II byl zřízen podle ustanovení nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 (8) [81] a rozhodnutí 2007/533/SVV (9) ze dne 12. června 2007[82]. Představuje společný informační systém, který umožňuje příslušným orgánům v členských státech spolupracovat prostřednictvím výměny informací. Nahrazuje schengenský informační systém první generace, který začal fungovat v roce 1995 a byl rozšířen v letech 2005 a 2007.

Jde o bezpečnostní databázový systém, který provozují členské státy Schengenské smlouvy v souvislosti se zabezpečením hranic. Obsahuje záznamy o osobách a věcech. Je určen pro příslušníky pohraniční stráže, celníky, vízové a donucovací orgány v celém schengenském prostoru pro zajištění vysoké úrovně zabezpečení.

Právním základem SIS II jsou dva akty, které se navzájem doplňují. Oba mají řadu společných článků, které doplňuje soubor zvláštních ustanovení, podle nichž se řídí používání systému v dané oblasti zahrnuté příslušným nástrojem. Rozhodnutí definuje zejména kategorie údajů (záznamy o osobách a věcech), které se zadávají do systému pro podporu operativní spolupráce mezi policejními a justičními orgány v trestních věcech, účely jejich vkládání, kritéria a postupy pro vkládání a zpracovávání těchto údajů a orgány s právem přístupu k těmto údajům. Rozhodnutí také obsahuje zvláštní ustanovení o zpracování a ochraně údajů vzhledem k těmto kategoriím údajů.

V SIS II jsou zahrnuty kategorie záznamů:

- záznamy o osobách hledaných za účelem zatčení a předání na základě evropského zatýkacího rozkazu a osobách hledaných za účelem vydání;
- údaje o pohřešovaných osobách, které musí být umístěny pod dočasnou ochranu nebo jejichž místo pobytu je třeba zjistit;
- záznamy o osobách za účelem zajištění jejich spolupráce v soudním řízení;
- záznamy o osobách nebo vozidlech, plavidlech, letadlech a kontejnerech kvůli skrytým kontrolám nebo zvláštním kontrolám pro účely trestního stíhání a předcházení ohrožení veřejné bezpečnosti;
- údaje o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení.

SIS II se skládá ze složek:

- centrálního systému (dále jen „centrální SIS II“) sestávajícího z:
  - technické podpůrné funkce obsahující databázi, dále jen „databáze SIS II“;
  - jednotného vnitrostátního rozhraní;
- vnitrostátního systému v každém členském státě, sestávajícího z vnitrostátních datových systémů, které komunikují s centrálním SIS II a který může obsahovat soubor údajů obsahující úplnou nebo částečnou kopii databáze SIS II;

[81] EU. Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006,o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II). Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0023:CS:PDF

[82] EU. Rozhodnutí Rady 2007/533/SVV, o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II). Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:205:0063:0084:CS:PDF

- komunikační infrastruktury mezi CS-SIS a NI-SIS, která poskytuje šifrovanou virtuální síť vyhrazenou pro údaje SIS II a výměnu údajů mezi centrálami SIRENE[83].

V souvislosti se záznamy platí následující ustanovení a postupy:

- v případě hledané osoby bude záznam rovnocenný evropskému zatýkacímu rozkazu nebo žádosti o předběžnou vazbu (v případech vydávání); příslušný orgán bude náležitě jednat;
- v případě pohřešované osoby orgán nahlásí, kdy byla tato osoba nalezena, a podniknuté opatření vyžádané orgánem, který záznam vytvořil;
- v případě osoby hledané ve spojitosti se soudním řízením bude orgán jednat podle požadavků centrály SIRENE;
- v souvislosti se záznamy o závažné trestné činnosti nebo ohrožení veřejné bezpečnosti provede orgán skrytou nebo zvláštní kontrolu podle požadavku orgánu, který záznam vytvořil, a pokud je to v souladu s vnitrostátními právními předpisy členského státu, který tuto osobu nalezl;
- pokud orgán v členském státu odhalí věc, na kterou se vztahuje záznam v SIS II za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení, zabaví tuto věc nebo podnikne všechna nezbytná ochranná opatření.

Členský stát pořizující záznam odpovídá za zajištění správnosti a aktuálnosti údajů, a zda jsou vložené do SIS II v souladu se zákonem. Pouze členský stát, který vložil záznam, je oprávněn měnit, doplňovat, opravovat, aktualizovat nebo mazat údaje, které vložil.

Záznamy o osobách a věcech by se měly v SIS II uchovávat pouze po dobu požadovanou pro splnění účelů, pro které byly vloženy. Do tří let od vložení záznamu by měl členský stát, který záznam pořídil, přezkoumat nutnost jej zachovat. Členské státy mohou stanovit kratší doby pro přezkum v souladu se svými vnitrostátními právními předpisy. Osobní údaje musí být v příslušných záznamech SIS II chráněny

11.2 VÍZOVÝ INFORMAČNÍ SYSTÉM (VIS)

VIS[84] je elektronický databázový systém členských států EU, resp. členů Schengenu, který obsahuje všechny relevantní údaje o žadatelích o víza včetně biometrických údajů. Konzuláty zemí EU proto sbírají digitalizované fotografie obličeje a otisky prstů žadatelů o vízum.

VIS se skládá z centrální evropské databáze, která je napojena na národní systémy tak, aby konzulární úřady v zahraničí, orgány odpovědné za ochranu hranic a další kompetentní orgány členských států mohly vkládat a prohlížet data týkající se žádostí a žadatelů o víza. Za přípravu centrálního systému byla zodpovědná Komise, národní systémy budovaly jednotlivé členské státy.

VIS představuje systém pro výměnu vízových údajů mezi členskými státy, který umožňuje oprávněným vnitrostátním orgánům vkládat a aktualizovat vízové údaje a elektronicky je prohlížet. VIS funguje centralizovaně a skládá se z ústředního systému,

[83] EU. Rozhodnutí komise, kterým se přijímá příručka SIRENE a další prováděcí opatření k Schengenskému informačnímu systému druhé generace (SIS II). Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:123:0001:0038:CS:PDF

[84] Rozhodnutí Rady ze dne 8. června 2004 o zřízení Vízového informačního systému (VIS) (2004/512/ES). Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0060:0081:CS:PDF a Úřední věstník EU L 213/5 z 15.6.2004 (CS). Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:213:0005:0007:CS:PDF

nazývaného "Ústřední vízový informační systém", z uživatelského rozhraní v každém členském státě, nazývaného "národní uživatelské rozhraní", které umožní připojení příslušného ústředního vnitrostátního orgánu daného členského státu, a z vlastní komunikační infrastruktury mezi ústředím a národním rozhraním. Za vytvoření VIS zodpovídá Evropská komise, které je nápomocen výbor s vlastním jednacím řádem, zřízený k SIS II. Existují výjimky pro Dánsko, Spojené království a Irsko v souladu s příslušnými protokoly k Amsterodamské smlouvě a na spolupráci se podílejí rovněž přidružené země Schengenu Island a Norsko. Dále viz vízová politika.

11.3 SYSTÉM EURODAC

Systém „Eurodac“ umožňuje zemím Evropské unie pomoci identifikovat žadatele o azyl a osoby, které byly zadrženy v souvislosti s nezákonným překročením vnější hranice Unie. Porovnáním otisků prstů mohou země EU stanovit, zda žadatel o azyl je nebo není cizí státní občan, který se nachází protizákonně na území některé země EU, již předtím nepožádal o azyl v jiné zemi EU nebo zda žadatel o azyl nevstoupil na území Unie nelegálně.

Eurodac se skládá z ústřední jednotky v rámci Komise, vybavené počítačovou ústřední databází pro porovnávání otisků prstů, a ze systému pro elektronický přenos dat mezi zeměmi EU a databází. Kromě otisků prstů zahrnují údaje zasílané zeměmi EU:

- zemi původu v EU;
- pohlaví dané osoby;
- místo a datum podání žádosti o azyl nebo zadržení dané osoby;
- referenční číslo;
- datum sejmutí otisků prstů;
- datum předání údajů ústřední jednotce.

Údaje jsou shromažďovány o osobách, jimž je minimálně 14 let, a do ústřední jednotky jsou zasílány přes vnitrostátní přístupové body. V případě žadatelů o azyl jsou uchovávány po dobu deseti let, dokud jednotlivá osoba nezíská občanství jedné ze zemí EU, v níž pak musí být jejich údaje okamžitě vymazány. Údaje o cizích státních občanech, kteří byli zadrženi v souvislosti s nezákonným překročením vnější hranice, jsou uchovávány po dobu dvou let od data, kdy byly otisky prstů sejmuty. Údaje jsou okamžitě vymazány ještě před uplynutím dvou let, pokud cizí státní občan:

- obdrží povolení k pobytu;
- opustí území Unie;
- získá občanství některé země EU.

V případě cizích státních občanů, kteří jsou protiprávně přítomni v některé zemi EU, je možné porovnat jejich otisky prstů s otisky v ústřední databázi a určit, zda daná osoba již nepodala žádost o azyl v jiné zemi EU. Poté, co byly otisky prstů předány za účelem srovnání, nejsou již uloženy v systému Eurodac.

Pokud jde o ochranu osobních údajů, musí země EU, které do systému Eurodac posílají údaje, zajistit, aby všechny operace zahrnující zpracování, přenos, uchovávání nebo výmaz údajů probíhaly v souladu se zákonem. Komise musí dohlížet na řádné uplatňování nařízení ústřední jednotkou a musí přijmout nezbytná opatření pro zajištění její bezpečnosti. O přijatých opatřeních informuje též Evropský parlament a Radu. Činnosti související se zpracováním údajů v zemích EU sledují vnitrostátní kontrolní orgány a činnosti Komise sleduje Evropský inspektor ochrany údajů (EDPS). Vedle všech zemí EU uplatňují toto nařízení i země, které (na základě mezinárodních dohod) uplatňují Dublinské nařízení, konkrétně Island, Norsko a Švýcarsko.

Eurodac[85] se skládá z:

- počítačové ústřední databáze údajů o otiscích prstů (dále jen „ústřední systém“) složené z:
  - ústřední jednotky;
  - záložního plánu a systému;
- komunikační infrastruktury mezi ústředním systémem a členskými státy, která poskytuje šifrovanou virtuální síť vyhrazenou pro údaje systému Eurodac (dále jen „komunikační infrastruktura“).

Každý členský stát určí jeden národní přístupový bod. Údaje o osobách, které zpracovává ústřední systém, jsou zpracovávány jménem členského státu původu za podmínek stanovených v tomto nařízení a oddělovány vhodnými technickými prostředky.

Postup snímání otisků prstů se určí a uplatňuje v souladu s vnitrostátními zvyklostmi daného členského státu a v souladu se zárukami stanovenými Listinou základních práv Evropské unie, Úmluvou o ochraně lidských práv a základních svobod a Úmluvou Organizace spojených národů o právech dítěte.

Provozní řízení systému Eurodac sestává ze všech úkolů nezbytných pro zachování jeho nepřetržité funkčnosti v souladu s tímto nařízením, zejména z údržby a technického vývoje nezbytných k zajištění toho, aby systém fungoval na uspokojivé úrovni provozní kvality, zejména co se týče doby potřebné pro vyhledávání v ústředním systému. Při vypracovávání záložního plánu a systému se zohlední potřeby údržby i neočekávaný výpadek systému, včetně dopadu opatření k zajištění kontinuity provozu na zabezpečení a ochranu údajů.

Vnitrostátní orgány krajin EÚ činné v trestním řízení, například policie anebo Europol, by měli mít přístup k databáze Eurodac s otlačky prstů žadatelů o azyl, aby měli možnost účinněji zabránit, odhalovat anebo vyšetřovat závažnou trestní činnost. Poslanci Europarlamentu s návrhem souhlasí, požadují však přijetí přísných pravidel, které budou garantovat ochranu osobních údajů.[86]

11.4 INFORMAČNÍ SYSTÉM PRO EVROPSKÉ VEŘEJNÉ ZAKÁZKY (SIMAP)

Portál SIMAP[87] poskytuje přístup k nejdůležitějším informacím o veřejných zakázkách v Evropě. Ke zveřejnění oznámení o veřejných zakázkách mohou zadavatelé použít internetový nástroj eNotices, který zjednodušuje a urychluje přípravu a zveřejňování oznámení o nabídkovém řízení. Stránka eNotices poskytuje přístup ke všem jednotným formulářům používaným pro evropské veřejné zakázky. Tato bezplatná služba umožňuje pracovat v individualizovaném prostředí, kontrolovat možné chyby v oznámeních a shodu se směrnicemi EU, které řídí veřejná výběrová řízení. Jinou možností zveřejnění je zveřejnění přes eSenders, organizace oprávněné podávat oznámení ve formě XML souborů přímo Úřadu pro úřední tisky. V ČR je elektronickým odesílatelem TED Ministerstvo pro regionální rozvoj.

Oznámení o nabídkovém řízení jsou zveřejňována v dodatku k Úřednímu věstníku dostupném na webových stránkách Tenders Electronic Daily (TED)[88], oficiálním internetovém zdroji veřejných zakázek v Evropě.

[85] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:CS:PDF
[86] http://bratislava.adagio4.eu/view/sk/press-release/news/news-2012/news-2012-December/news-2012-December-37.html;jsessionid=912128D0F873E740927518309C53261C
[87] http://simap.europa.eu/index_cs.htm
[88] http://ted.europa.eu/TED/main/HomePage.do

11.5 INDECT

Projekt Indect[89] je komplexní monitorovací a vyhodnocovací systém Evropské unie, který má sloužit k vyhledávání a detekci lidí a předmětů. Měl by zajistit bezpečnost obyvatel ve městech. Pracuje se na něm od roku 2009. Na programu se podílí 17 evropských institucí a univerzit, v Česku je to VŠB - Technická univerzita Ostrava.

Projekt Indect má o lidech shromažďovat veškeré údaje a komunikační data z telefonů a internetu. Pomocí vyhledávačů na sociálních sítích, chatech, diskusních forech a blozích bude sledovat vše, co děláme, monitorovat všechny fotografie a videa, která se na nich objeví. Systém bude využívat také kamerové systémy. V důsledku propojení s údaji v biometrických pasech bude schopen rozpoznávat obličeje vytipovaných osob nebo je pomůže identifikovat v davu. Systém bude sám vyhodnocovat, jaké chování je normální a jaké ne. Jeho úkolem je předvídat chování jednotlivce, skupin osob nebo i celé společnosti. Svou roli může hrát i při protestních shromážděních.

Úkolem systému je včas zjistit případy podezřelého chování, které si zaslouží pozornost nebo reakci bezpečnostních složek. Za nenormální chování je považována potyčka, křik, klení nebo používání vulgarismů, střelba, exploze, krádež vozidla, opomenutí zavazadla, pád osoby, ale také časté scházení se s lidmi, běh, rychlá chůze, chůze nesprávným směrem či postávání na určitém místě delší dobu. Za špatné je považováno i to, když se někdo posadí na podlahu v prostředku veřejné hromadné dopravy, dále bezcílné potulování a zdržování se na některých místech.

[89] http://www.indect-project.eu/

12 INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY VE SLOVENSKÉ REPUBLICE

Informatizace společnosti je v současnosti často se vyskytujícím pojmem v Slovenské republice (SR). Právě z důvodu zabezpečení dostatečného informování o všech oblastech sdružujících pojem „informatizace společnosti“ přistoupilo Ministerství financí SR, jako ústřední orgán státní správy pro oblast informatizace společnosti k vytvoření internetového portálu (webového sídla) www.informatizacia.sk.

Webové sídlo poskytuje především aktuální informace o aktivitách Sekce informatizace společnosti zřízené na Ministerství financí SR, i o aktivitách Evropské unie v oblasti informatizace společnosti, dále o elektronických službách veřejné správy (eGovernment), o přínosech informatizace pro občany či podnikatele, podpoře širokopásmového internetu, poskytuje odborné texty, přehledy a charakteristiky oblastí informační společnosti, vládní dokumenty a materiály mimovládních organizací, průzkumy, statistiky a informace o událostech souvisejících z informatizací společnosti.[90]

Jelikož je Ministerství financí SR zprostředkovatelským orgánem pod řídícím orgánem pro Operační program informatizace společnosti[91], webové sídlo www.informatizacia.sk plní důležitou funkci při informovaní a publicitě pro Operační program informatizace společnosti.

Zákon č. 305/2013 Z. z. o elektronické podobě výkonu působnosti orgánů veřejné moci a o změně a doplnění některých zákonů (zákon o e-Governmentu) upravuje:

- některé informační systémy pro výkon působnosti orgánů veřejné moci v elektronické podobě;
- elektronická podání, elektronický úřední dokument a některé podmínky a způsob výkonu veřejné moci elektronicky a elektronické komunikace orgánů veřejné moci navzájem,
- elektronické schránky a elektronické doručování;
- identifikaci a autentizaci osob;
- autorizaci,
- zaručenou konverzi;
- způsob vykonání úhrady orgánu veřejné moci;
- referenční registry.

Aktuální legislativu pro oblast informatizace společnosti v gesci Ministerstva financí SR nalezneme na webu na adrese:

http://www.informatizacia.sk/legislativa-sr/684s.

12.1 INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

Základní normou v této oblasti je Zákon č. 275/2006 Z.z. o informačních systémech veřejné správy a o změně a doplnění některých zákonů (ve znění následujících změn). Podle tohoto zákona:

[90] http://www.informatizacia.sk/informatizacia-main/599s
[91] http://www.informatizacia.sk/opis/598s

NEPŘEHLÉDNĚTE

Informační systémem veřejné správy (ISVS) je informační systém v působnosti povinné osoby jako správce informačního systému veřejné správy podporující služby veřejné správy, služby ve veřejném zájmu a veřejné služby.

Slovenský zákon se zabývá obdobnými oblastmi, jako zákon český.

Za vytváření, správu a rozvoj informačního systému veřejné správy odpovídá povinná osoba, která je správcem, zabezpečující výkon veřejné správy na určeném úseku veřejné správy podle zvláštního předpisu.

Informační činnost vykonává povinná osoba, která je správcem nebo provozovatelem informačního systému veřejné správy. Provozovatelem ISVS je povinná osoba, fyzická osoba nebo právnická osoba určená správcem, která vykonává správcem určené informační činnosti; provozovatelem informačního systému veřejné správy může být i správce.

Povinnými osobami pro účely zákona jsou:

a) ministerstva a další ústřední orgány státní správy;
b) Generální prokuratura Slovenské republiky, Nejvyšší kontrolní úřad Slovenské republiky, Úřad pro dohled nad zdravotní péčí, Úřad na ochranu osobních údajů Slovenské republiky, Telekomunikační úřad Slovenské republiky, Poštovní regulační úřad, Úřad pro regulaci síťových odvětví a další státní orgány;
c) obce a vyšší územní celky;
d) Kancelář Národní rady Slovenské republiky, Kancelář prezidenta Slovenské republiky, Kancelář Ústavního soudu Slovenské republiky, Kancelář Nejvyššího soudu Slovenské republiky, Kancelář Soudní rady Slovenské republiky, Kancelář veřejného ochrance práv, Ústav paměti národa, Sociální pojišťovna, zdravotné pojišťovny, Tisková agentura Slovenské republiky, Slovenská televize, Slovenský rozhlas, Rada pro vysílání a retransmisi;
e) právnické osoby v zřizovatelské nebo zakladatelské působnosti povinných osob uvedených v předchozím;
f) komory regulovaných profesí a komory, na které je přenesen výkon veřejné moci s povinným členstvím;
g) fyzické osoby a jiné právnické osoby, jako jsou uvedené v odrážce e), na které je přenesen výkon veřejné moci nebo které plní úlohy na úseku přeneseného výkonu státní správy podle zvláštního předpisu.

12.2 ÚSTŘEDNÍ PORTÁL

Ústřední portál veřejné správy (ÚPVS)[92], jako informační systém veřejné správy na poskytování služeb a informací veřejnosti, zabezpečuje centrální a jednotní přístup k informačním zdrojům a službám veřejné správy. Informace z prostředí veřejné správy, které občan nebo podnikatel hledá, jsou mnohokrát součástí informačních serverů jednotlivých rezortů. Cílem ÚPVS je tyto informace a služby spájet a přehlednou a přístupnou formou poskytovat používateli. Hlavní úlohou portálu je (podle charakteru životní situace, ve které se právě nachází) nasměrovat uživatele na využití konkrétní elektronické služby veřejné správy s využitím relevantních informačních zdrojů.

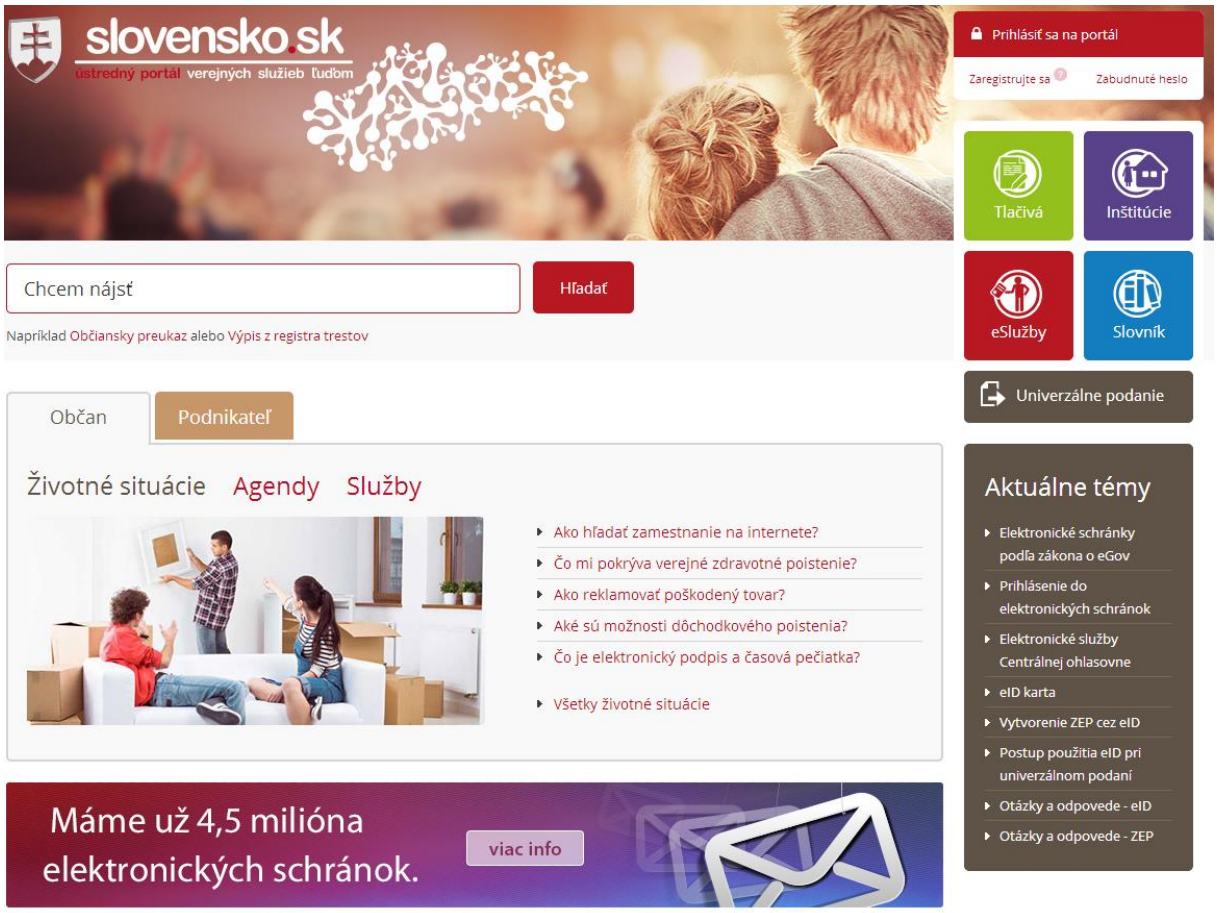
Ve smyslu zákona č. 275/2006 Z.z., o informačních systémech veřejné správy a o změně a doplnění některých zákonů je od 1. září 2013 správcem ÚPVS Úřad vlády SR.

[92] https://www.slovensko.sk/sk/titulna-stranka

Ministerství financí SR koordinuje přepojení informačních systémů s ústředním portálem. Provozovatelem ÚPVS je Národní agentura pro síťové a elektronické služby (NASES), jako příspěvková organizace zřízená Úřadem vlády SR.

Vytvoření v současnosti provozovaného řešení ÚPVS (v1.0) bylo spolufinancované Evropskou unií z prostředků Phare v rámci projektu "Transparency in Functioning of State administration and Public Self-administration".

Obrázek 12-1 Ústřední portál veřejné správy



Zdroj: https://www.slovensko.sk/sk/titulna-stranka

Na základě písemného vyzvání na národní projekt Elektronizace služeb společných modulů ÚPVS a přístupových komponentů (etapa 1. a 2.), zveřejněného dne 27. února 2012, se podpisem Smlouvy o NFP mezi Ministerstvím financí SR a NASES začala akcelerovat realizace národního projektu na nové řešení společných modulů ÚPVS (v2.0).

Cílem tohoto národního projektu je zpřístupnit elektronické služby společných modulů ÚPVS, jakými jsou:

- Identity and Access Management - registrace, autentifikace a autorizace;
- Platební modul - realizace platby;
- eDesk modul – elektronická schránka pro účely doručování, podepisování dokumentů, evidence komunikace (podání a výstupů), zprostředkování platby;
- eNotify – notifikace uživatelů o událostech vyžadujících akci;
- eForm modul – správa elektronického formuláře;

- Modul centrální elektronické podatelny - ověření elektronického podpisu podání a vystavení potvrzení o přijetí podání;
- Modul dlouhodobého ukládaní elektronických spisových záznamů - zabezpečení dlouhodobého ukládaní elektronických spisových záznamů;
- Modul elektronického doručování – směřování elektronických zásilek, úřední elektronická tabule;
- Modul BPM - procesně-integrační platforma BPM;
- Přístupový komponent – modul pro poskytování a management informačního obsahu, označovaný aj jako Portál ÚPVS;
- Kontaktní centrum – modul pro zprostředkované poskytování služeb VS prostřednictvím telefonické komunikace.

Od začátku listopadu 2012 probíhá taky realizace aktivit v rámci dalších dvou etap projektu (etapa 3. a 4.). Smlouva o NFP mezi Ministerstvím financí SR a NASES Elektronizace služeb společných modulů ÚPVS a přístupových komponentů (II. část) byla podepsána na základě písemného vyzvání zveřejněného 22. října 2012.

Cílem druhého projektu je dobudování společných modulů a přístupových komponentů a zpřístupnění jejich funkcí pomocí elektronických služeb. Po dobudování obou projektů bude plně nasazené funkční řešení elektronických služeb společných modulů ÚPVS, bude vybudovaná základní integrační platforma pro prostředí eGovernmentu a vytvořené podmínky pro napojení IS VS, kompletně se zpřístupní služby společných modulů pro ostatní služby eGovernmentu a zabezpečí se tak plná funkcionalita ÚPVS pro veřejnost.

12.3 STANDARDY

Standard je soubor pravidel spojených s vytvářením, rozvojem a využíváním ISVS, který obsahuje charakteristiky, metody, postupy a podmínky, zvláště pokud jde o bezpečnost a integrovatelnost ISVS. Standardy musí být otevřené a technologicky neutrální.

Standardy se vztahují především na:

- technické prostředky, infrastrukturu a systém procesního řízení;
- programové prostředky, kterými jsou operační prostředí, databázové prostředí, kancelářské programy, společné moduly a aplikační programové vybavení;
- údaje, registry, číselníky;
- formáty výměny údajů.

Integrovatelnost ISVS tvoří souhrn právních, technických, organizačných a jiných opatření vytvářejících jednotné prostředí umožňující výměnu a společné používání údajů a společných modulů mezi jednotlivými ISVS.

Standardy jsou podrobněji vymezeny v několika dalších výnosech.

12.4 INTEGROVANÉ OBSLUŽNÉ MÍSTO

Integrované obslužné místo vykonává činnost osvědčující[93] osoby a zabezpečuje přístup ke službám veřejné správy poskytovaným povinnými osobami, zvláště podávání návrhů, žádostí a jiných podání povinným osobám a jinou komunikaci s povinnými osobami.[94]

[93] Osvědčující osoba je povinná zjistit totožnost osoby žádající o vydání výstupu.
[94] Výnos č. 53/2012 Z. z. o integrovaných obslužných miestach a podmienkach ich zriaďovania, registrácie, označovania, prevádzky a o sadzobníku úhrad

12.5 OBČANSKÝ PRŮKAZ S ELEKTRONICKÝM KONTAKTNÍM ČIPEM

Od 2. prosince 2013 se začne vydávat nový typ občanského průkazu s elektronickým kontaktním čipem – tzv. elektronická identifikační karta (eID). O vydáni eID karty může občan požádat na kterémkoliv pracovišti oddělení dokladů Okresního ředitelství Policejního sboru (OR PZ) a to v případě, že má platný občanský průkaz ve formáte ID1, který se začal vydávat po 1.7.2008. Občané, kterých občanský průkaz byl vydán před tímto datem, musí o novou eID kartu požádat v místě trvalého bydliště.

Elektronická identifikační karta bude sloužit, tak jako doposud platný občanský průkaz, k prokazováni totožnosti při osobním styku s úřady a institucemi. Kromě toho s eID kartou bude možné prokazovat totožnost i v elektronickém prostředí při využívaní elektronických služeb veřejné správy prostřednictvím internetu. Mezi takové služby patří například: nahlašování změn, podávaní žádostí, stížností, žalob, aukci, veřejné obstarávaní, služby katastru, služby daňového úřadu, eHealth (elektronické zdravotnictví), eVoting (elektronické volby a referenda) a podobně.

Doba platnosti nového typu občanského průkazu – eID karty je 10 let. Občané nejsou povinní si svůj platný občanský průkaz bez elektronického čipu vyměnit před uplynutím jeho platnosti za novou eID kartu. Jestli tak plánuji, a mají stále platný občanský průkaz bez elektronického čipu, zaplatí správní poplatek 4,50 €.

eID karta se liší od starého občanského průkazu (vydávaného od července 2008) tím, že má na zadní straně navíc elektronický kontaktní čip. Na čipu jsou uložené údaje uvedené na občanském průkaze: jméno, příjmení, adresa, datum narozeni a údaje o platnosti dokladu. V případě zájmu si může občan zvolit, jestli má čip obsahovat aj jiné údaje, např. údaje potřebné pro vytváření zaručeného elektronického podpisu (ZEP). Ten bude v elektronické komunikaci občana s úřady anebo komerčními institucemi rovnocennou náhradou vlastnoručního podpisu. Jestli se občan rozhodne využívat ZEP, požádá příslušné pracoviště OR PZ o vydání kvalifikovaného certifikátu na jeho tvorbu. Tato možnost bude k dispozici kdykoliv během platnosti eID karty, nejenom při jejím vydaní. Kvalifikovaný certifikát se vydává bezplatně s platnosti na 5 let.

12.6 ELEKTRONICKÉ SCHRÁNKY

Od 1. ledna 2014 zpřístupnila NASES na ústředním portálu veřejné správy www.slovensko.sk pilotní provoz elektronických schránek podle zákona č. 305/2013 Z.z., o e-Governmente. Elektronické schránky jsou vytvořené pro občany Slovenské republiky, kteří dovršili k danému datu 18. rok života. Přihlašovaní do elektronických schránek je podle zákona o e-Governmente umožněné jenom prostřednictvím elektronického občanského průkazu – tzv. eID karty, vydané po 1. prosinci 2013. eID karta občana musí mít aktivovanou Online eID funkci. Do elektronických schránek není možné přihlásit se prostřednictvím přihlašovacího jména a hesla, jako to bylo doposud. Elektronické schránky zřízené podle zákona jsou dostupné na stránce https://schranka1.slovensko.sk.

Jedním z prvých využití elektronických schránek jsou pro držitele eID karet Elektronické služby Centrální ohlašovny zpřístupněné Ministerstvím vnitra SR od 1. ledna 2014. Služby Centrální ohlašovny jsou dostupné na stránce https://portal.minv.sk v záložce Životní situace.

Obrázek 12-2 Centrální ohlašovna

Zdroj: https://portal.minv.sk/wps/portal/

Držitelé aktivované eID karty a zaručeného elektronického podpisu mají od 1. ledna k dispozici některé služby z agendy hlášení trvalého a přechodného pobytu a to včetně získaní potvrzení online. Agenda hlášení pobytu je legislativně upravená zákonem č. 190/2013 Z.z., kterým se mění a doplňuje zákon č. 253/1998 Z. z., o hlášení pobytu občanů a registraci obyvatel SR.

Další zpřístupněnou službou z agendy dokladů, je Modifikace kontaktních údajů, která umožňuje přihlášenému uživateli modifikovat e-mailovou adresu, telefonní číslo a diskrétní údaj evidovaný v informačním systému agendy občanských průkazů. Diskrétní údaj může občan použít při případném nahlášení ztráty anebo odcizeni občanského průkazu prostřednictvím elektronické služby.

ZÁVĚR

Učební text „Informační systémy ve veřejné správě“ se vás pokusil seznámit se základními pojmy, metodami a přístupy k využívání informačních technologií ve veřejné a státní správě. Výchozím pojmem je nepochybně slovo informace, které je označením pro jakékoliv sdělení, které je obvykle kódováno v datové formě. Soustavu takových informací, které spolu souvisí přesně vymezeným způsobem, označujeme jako informační systém.

Významnou úlohu v této oblasti přikládáme bezpečnosti informací a zamezení zneužití ICT. Potenciál informačních technologií by měl být využíván pro podporu efektivnosti veřejné správy a pro zlepšení vztahu „veřejná správa – občan“. Informační technologie mohou taky výrazným způsobem napomoci koordinaci uvnitř veřejné správy. Jednotlivé složky ISVS – základní registry, agendy a informační systémy jednotlivých rezortů jsou v současné době v České republice na poměrně kvalitní úrovni. Trendem se jeví zefektivnění vzájemné spolupráce a provázanosti jednotlivých složek ISVS s možností předávaní a sdílení informací v nich obsažených. Jejich nedílnou součástí je legislativní zabezpečení základních podmínek jejich rozvoje.

SEZNAM POUŽITÉ LITERATURY

1. BÍŽA, Z. Řízení přístupu k otiskům prstů v elektronických pasech. *Konference Internet ve státní správě a samosprávě*. 2008, s. 71-72. Dostupné z: http://www.isss.cz/archiv/2008/download/ISSS2008.pdf.
2. BUDIŠ, P. a I. HŘEBÍKOVÁ. *Datové schránky: fungování, doručování, bezpečnost, návody*. 1. vyd. Olomouc: ANAG, 287 p. ISBN 80-726-3617-0.
3. Česká republika. Vyhláška 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů [online]. [cit. 2013-11-28]. Dostupné z: http://portal.gov.cz/app/zakony/zakon.jsp?page=0&fulltext=&nr=193~2F2009&part=&name=&rpp=15#seznam
4. Česká republika. Vyhláška 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek [online]. [cit. 2013-11-28]. Dostupné z: http://portal.gov.cz/app/zakony/zakon.jsp?page=0&fulltext=&nr=194~2F2009&part=&name=&rpp=15#seznam
5. Česká republika. Vyhláška 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu) [online]. [cit. 2013-11-28]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=77709&fulltext=&nr=212~2F2012&part=&name=&rpp=15#local-content
6. Česká republika. Vyhláška 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 (vyhláška o dlouhodobém řízení informačních systémů veřejné správy) [online]. [cit. 2013-11-28]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=63196&fulltext=&nr=529~2F2006&part=&name=&rpp=15#local-content
7. Česká republika. Vyhláška 64/2008 Sb. o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti) [online]. [cit. 2013-11-28]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=66763&fulltext=&nr=64~2F2008&part=&name=&rpp=15#local-content
8. Česká republika. Vyhláška č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému. *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=63195&fulltext=&nr=528~2F2006&part=&name=&rpp=15#local-content
9. Česká republika. Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy. *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=63196&fulltext=&nr=529~2F2006&part=&name=&rpp=15#local-content

10. Česká republika. Vyhláška č. 53/2007 Sb., o o referenčním rozhraní. *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=64637&fulltext=&nr=53~2F2007&part=&name=&rpp=15#local-content
11. Česká republika. Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy. *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=64636&fulltext=&nr=52~2F2007&part=&name=&rpp=15#local-content
12. Česká republika. Zákon 106/1999 Sb., o svobodném přístupu k informacím (ve znění pozdějších předpisů). *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=47807&fulltext=&nr=106~2F1999&part=&name=&rpp=15#local-content
13. Česká republika. Zákon 111/2009 Sb., o základních registrech (ve znění pozdějších předpisů). *Ministerstvo vnitra České republiky* [online]. [cit. 2013-10-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68500&fulltext=&nr=111~2F2009&part=&name=&rpp=15#local-content
14. Česká republika. Zákon 227/2000 Sb., o elektronickém podpisu (ve znění pozdějších předpisů). *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49532&fulltext=&nr=227~2F2000&part=&name=&rpp=15#local-content
15. Česká republika. Zákon 329/2012 Sb., úplné znění zákona č. 499/2004 Sb., o archivnictví a spisové službě. *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78298&fulltext=&nr=329~2F2012&part=&name=&rpp=15#local-content
16. Česká republika. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (ve znění pozdějších předpisů). *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49228&fulltext=&nr=101~2F2000&part=&name=&rpp=15#local-content
17. Česká republika. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=67315&fulltext=&nr=300~2F2008&part=&name=&rpp=15#local-content
18. Česká republika. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ve znění pozdějších předpisů). *Ministerstvo vnitra České republiky* [online]. [cit. 2013-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49763&fulltext=&nr=365~2F2000&part=&name=&rpp=15#local-content
19. HANÁČEK, P. a J. STAUDEK. *Bezpečnost informačních systémů*. Praha: Úřad pro státní informační systém, 2000.
20. IS o ISVS. *Obecná uživatelská příručka IS o ISVS* [online]. Praha: MVČR, 2012. [online]. [cit. 2013-11-28]. Dostupné z: https://www.sluzby-ISVS.cz/ISoISVS/Dokumentace/obecna_prirucka_IS_o_ISVS.pdf

21. KAJZAR, Dušan. Administrátorská dokumentace k informačnímu systému. *Tvorba softwaru 2002: celostátní konference*. Ostrava: Tanger, 2002, 217 s. ISBN 80-859-8874-7.
22. KONERO. *Dlouhodobé řízení ISVS: Úplná struktura informační koncepce.* Verze 3.0. Praha, 2011. [online]. [cit. 2013-11-28]. Dostupné z: http://www.mvcr.cz/soubor/dalsi-dokumenty-uplna-struktura-informacni-koncepce.aspx
23. KONERO. *Dlouhodobé řízení ISVS: Vzorová informační koncepce obce s rozšířenou působností.* Verze 3.0. Praha, 2011. [online]. [cit. 2013-11-28]. Dostupné z: http://www.mvcr.cz/soubor/informacni-koncepce-obce-s-vykonem-prenesene-pusobnosti-v-zakladnim-rozsahu.aspx
24. KONERO. *Dlouhodobé řízení ISVS: Vzorová informační koncepce obce s výkonem přenesené působnosti v základním rozsahu.* Verze 3.0. Praha, 2011. Dostupné z: http://www.mvcr.cz/soubor/informacni-koncepce-obce-s-rozsirenou-pusobnosti.aspx
25. KONERO. *Dlouhodobé řízení ISVS: Vzorová informační koncepce obce s pověřeným obecním úřadem.* Verze 3.0. Praha, 2011. [online]. [cit. 2013-11-28]. Dostupné z: http://www.mvcr.cz/soubor/informacni-koncepce-obce-s-poverenym-obecnim-uradem.aspx
26. KONERO. *Vzorové informační koncepce: Informační koncepce ústředního orgánu veřejné správy.* Verze 1.1. Praha, 2011. [online]. [cit. 2013-11-28]. Dostupné z: http://www.mvcr.cz/soubor/informacni-koncepce-ustredniho-organu-verejne-spravy.aspx
27. MVČR. *Dlouhodobé řízení ISVS: Základní principy a hlavní procesy dlouhodobého řízení ISVS.* Verze 1.01. Praha, 2009. [online]. [cit. 2013-11-28]. Dostupné z: http://www.mvcr.cz/soubor/procesni-model-rizeni-ISVS-211984.aspx
28. MVČR. *Globální architektura základních registrů: Příloha č. 1a zadávací dokumentace* [online]. Praha: MVČR, 2012. [online]. [cit. 2013-11-28]. Dostupné z: http://www.szrcr.cz/file/4_1_1/
29. MVČR. *Jak na základní registry?: Příručka pro kraje a obce* [online]. Praha: MVČR, 2012 [cit. 2013-05-21]. Dostupné z: http://www.mvcr.cz/soubor/prirucka-pro-kraje-a-obce-jak-na-zakladni-registry-dvoustranna-pdf.aspx.
30. OECD. *M-government: mobile technologies for responsive governments and connected societies*. Paris, France: OECD, 2011, 150 s. ISBN 92-611-3881-0. [online]. [cit. 2013-11-28]. Dostupné z: http://www.keepeek.com/Digital-Asset-Management/oecd/governance/m-government-mobile-technologies-for-responsive-governments-and-connected-societies_9789264118706-en#page153
31. OECD. *The e-government imperative*. Paris, France: OECD, 2003, 203 s. ISBN 92-641-0117-9. [online]. [cit. 2013-11-28]. Dostupné z: http://www.keepeek.com/Digital-Asset-Management/oecd/governance/the-e-government-imperative_9789264101197-en
32. RADA, Michal a kol. MINISTERSTVO VNITRA ČR. *Metodický pokyn: k vyhlášce č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti).* Verze 1.10. Praha, 2010. [online]. [cit. 2013-11-28]. Dostupné z: http://www.mvcr.cz/soubor/metodicky-pokyn-k-vyhlasce-c-64-2008-sb-o-forme-uverejnovani-informaci-souvisejicich-s-vykonem-verejne-spravy-prostrednictvim-webovych-stranek-pro-osoby-se-zdravotnim-postizenim-vyhlaska-o-pristupnosti.aspx

33. RAŠEK, L. Elektronické cestovní doklady, část 1. *Crypto-World: Informační sešit GCUCMP*. 2006, č. 10, s. 4-18. ISSN 1801-2140. Dostupné z: http://crypto-world.info/casop8/crypto10_06.pdf.
34. Slovenská republika. Výnos č. 53/2012 Z. z. o integrovaných obslužných miestach a podmienkach ich zriaďovania, registrácie, označovania, prevádzky a o sadzobníku úhrad [online]. [cit. 2014-01-19]. Dostupné z: http://www.informatizacia.sk/ext_dok-vynos_53-2012_iom/13806c
35. Slovenská republika. Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy (úplné znění) [online]. [cit. 2014-01-19]. Dostupné z: http://www.informatizacia.sk/index/open_file.php?ext_dok=12115
36. Slovenská republika. Zákon č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) [online]. [cit. 2014-01-19]. Dostupné z: http://www.informatizacia.sk/ext_dok-zakon.../16171c
37. SPRÁVA ZÁKLADNÍCH REGISTRŮ. *Globální architektura ROB verze 1.0 - Příloha č. 1b zadávací dokumentace*. [online]. [cit. 2013-11-28]. Praha: Správa základních registrů, 2010 [cit. 25. 5. 2012]. Dostupné z: http://www.szrcr.cz/file/8/
38. SPRÁVA ZÁKLADNÍCH REGISTRŮ. *Podmínky pro připojení agendových informačních systémů do ISZR: verze 2.06* [online]. Praha: Správa základních registrů, 2012. [online]. [cit. 2013-11-28]. Dostupné z: www.szrcr.cz/file/166_2_1/
39. TESAŘ Pavel a Ondřej MENOUŠEK. MINISTERSTVO VNITRA ČR. *Provozní řád ISDS*. Verze k 21. 4. 2013. Praha, 2013. [online]. [cit. 2013-11-28]. Dostupné z: http://www.datoveschranky.info/assets/ke-stazeni/provozni_rad_isds.pdf
40. VANĚK, Jindřich a Roman ŠPERKA. *Informační systémy*. Karviná: Slezská univerzita v Opavě, 2013, 140 s. ISBN 978-80-7248-855-1.