Administrativní bezpečnost a certifikační politika (eGON)

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
OPERAČNÍ PROGRAM LIDSKÉ ZDROJE A ZAMĚSTNANOST
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
PODPORUJEME VAŠI BUDOUCNOST
www.esfcr.cz

Rozsah:

8 hodin

Anotace:

Kurz podává podrobný návod na administraci účtu Czech POINT pro nové obce a na pořízení certifikátů potřebných pro práci s portálem Czech POINT. Poskytuje základní informace o certifikátech a administrativní bezpečnosti při práci s informačními systémy obsahujícími osobní údaje nebo citlivá data.

Průvodce kurzem:

Tento kurz obsahuje moduly Certifikáty, Administrace Czech POINT a Administrativní bezpečnost.

V prvním modulu najdete podrobný návod, jak si zařídit komerční a kvalifikovaný certifikát, které potřebujete pro přístup do Czech POINT. Je zde popsán celý proces od objednání tokenů a obslužného software, přes uzavření smlouvy s certifikační autoritou až po vlastní instalaci certifikátů.

Druhý modul slouží jako pomůcka obcím, které ještě nemají dostatek zkušeností s administrací účtu u Czech POINT.

Administrativní bezpečnost je aktualizovaná verze modulu Czech POINT - Aministrativní bezpečnost z roku 2008.

Seznam modulů:

- Certifikáty
- Administrace Czech POINT
- Administrativní bezpečnost

Přílohy ke kurzu:

- Pracovní sešit Czech POINT 2010
- Administrativní bezpečnost

Obsah modulu Certifikáty

Obsah modulu Administrace Czech POINT

Obsah modulu Administrativní bezpečnost

MODUL: Certifikáty

Kvalifikovaný a komerční certifikát, způsob pořízení certifikátů a jejich instalace pro přístup do Czech POINTu, certifikační autority.

Po prostudování modulu bude absolvent rozeznávat rozdíl mezi komerčním a kvalifikovaným certifikátem, bude znát postup pořízení obou certifikátů a způsob jejich instalace.

1 Úvod

Projekt je spolufinancován z ESF z OP LZZ Vzdělávání úředníků a zaměstnanců veřejné správy, metodiků a školitelů a politiků v oblasti zavádění eGovernmentu do veřejné správy,

reg. č. CZ.1.04/4.1.00/38.00001

V tomto kurzu se seznámíme se základními pojmy z oblasti kryptologie, certifikátů a systému Czech POINT. Budeme se také věnovat administraci účtu Czech POINT z pohledu obce, postupu při získávání certifikátů a zprovoznění Czech POINTu na obci.

2 Základní pojmy

2.1 Asymetrická kryptografie a klíče

Asymetrická kryptografie je souhrn kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče. Kromě možnosti použití pro utajení komunikace se asymetrická kryptografie používá také pro elektronický podpis.

V nejběžnější formě asymetrické kryptografie se používají dva typy klíčů:

1. **Veřejný (pubic key)** - tento klíč je jeho majitelem uvolněn uživatelům, kteří s ním chtějí komunikovat - šifrovat** zprávy, které jsou tomuto majiteli určeny.
2. **Soukromý (private key)** - tento klíč jeho majitel drží v tajnosti a pomocí tohoto klíče dešifruje** zprávy, které jsou mu doručeny a šifrovány jeho vlastním veřejným klíčem (bod 1).

** - v případě digitálního podpisu je to obráceně

Je jasné, že šifrovací a dešifrovací klíč musí být spolu matematicky svázány, ale z důvodu praktického využití této metody nesmí být možno z šifrovacího klíče vyvodit klíč dešifrovací.

2.2 Autentizace a Autorizace

Autentizace

- proces ověření identity entity (člověka, programu, systému)
- Dvě formy
    1. Identifikace - entita se aktivně identifikuje, systém potvrdí shodu
    2. Verifikace - systém aktivně hledá v databázi odpovídající záznam

Autorizace

- oprávnění přístupu k informačním zdrojům
- v průběhu autorizace se určuje k jakým zdrojům má uživatel přístup

2.3 Digitální certifikát

- je soubor dat ve stanoveném formátu (norma X.509), který identifikuje osobu nebo server a může během elektronické komunikace mezi dvěma subjekty zajistit šifrování přenášených dat, ověření jedné a/nebo druhé strany, rozpoznání neoprávněné modifikace dat.
- je vydávaný certifikační autoritou, která jeho vydáním zajišťuje a stvrzuje, že daný subjekt skutečně tento certifikát vlastní.
- Náležitosti certifikátu:
    - Unikátní sériové číslo
    - Termín platnosti
    - Identifikační údaje subjektu, který je vlastníkem tohoto certifikátu
    - Identifikační údaje certifikační autority, která certifikát vydala
    - Veřejný klíč
    - Další informace (o omezení použití, použití k testování a další ...)

Jelikož digitální certifikát je datový soubor jako každý jiný, musí být také zajištěn proti zfalšování. Z tohoto důvodu certifikační autorita tento soubor podepíše svým soukromým klíčem a tento podpis připojí k certifikátu. Pro ověření tohoto podpisu potřebujeme mít k dispozici certifikát certifikační autority. Ten bývá obvykle k dipozici na WWW stránkách certifikační autority ke stažení. Z matematické podstaty digitálních certifikátů je pak následně možno ověřit, že certifikát podepsala právě uvedená certifikační autorita.

2.4 Typy digitálních certifikátů

Existuje několik typů digitálních certifikátů, my však uvedeme jen ty nejdůležitější:

1. Komerční certifikát
2. Kvalifikovaný certifikát

Komerční certifikát

Komerčním certifikátem se nazývá takový certifikát, který vystaví certifikační autorita za poplatek a ověří žadatele. V případě osobních certifikátů ověří identitu žadatele, v případě serverových certifikátů pak kromě identity žadatele i vlastnictví domény, pro kterou je certifikát vystavován. Komerční certifikát je určen například pro komunikaci mezi různými subjekty, kteří se vzájemně dohodli na akceptování těchto certifikátů. V oblasti eGovernmentu se komerční certifikát používá zejména pro bezpečné přihlášení k Centrále Czech POINT. Autentizují se obě komunikující strany a právě k autentizaci klientské strany se tento certifikát používá (autentizaci provádí protokol SSL).

Kvalifikovaný certifikát

Kvalifikovaný certifikát je takový certifikát, který má náležitosti podle § 12 zákona č. 227/2000 Sb., o elektronickém podpisu. Pomocí tohoto certifikátu je možné vytvořit zaručený elektronický podpis, který má stejnou právní váhu jako osobní podpis na papírovém dokumentu. Slouží k ověřování

identifikace a autentifikace podepisující osoby a také k zajištění integrity zpráv. V oblasti eGovernmentu se kvalifikovaný certifikát používá ke garanci neprovedených změn v dokumentu. Dále také je využíván např. při podpisu žádostí, které se posílají na Rejstřík trestů.

2.5 Token

Token je malé USB zařízení, které slouží jako bezpečné úložiště osobních certifikátů, komerčního a kvalifikovaného. Výhoda použití tohoto hardwarového úložiště je v tom, že privátní klíč vygenerovaný uvnitř zařízení jej nikdy neopustí. Navíc je použití tokenu chráněno bezpečnostním kódem (PIN), čímž je zaručeno, že příslušný osobní certifikát nemůže být zneužit.

2.6 Certifikační autorita

Certifikační autorita je subjekt, který vydává digitální certifikáty. Placené certifikační autority získávají od svých klientů peníze, které používají především na zajištění vlastní činnosti.

Kvalifikovaná certifikační autorita je certifikační autorita, která je v rámci České republiky definována Zákonem o elektronickém podpisu.

V České republice existují 3 kvalifikované certifikační autority:

- První certifikační autorita, a.s. - http://www.ica.cz/
- Certifikační autorita PostSignum - http://www.postsignum.cz/
- eIdentity a.s. - http://www.ie.cz/

3 Postup zřízení certifikátů pro přístup do Czech POINT

1. Objednání USB tokenů a ovládacího software
2. Smlouva o poskytování certifikačních služeb
3. Instalace ovládacího software k USB tokenu, inicializace tokenu
4. Instalace certifikátů certifikačních autorit
5. Vydání certifikátů žadatelům

3.1 Objednání USB tokenů a ovládacího software

Objednávku je možné realizovat na webové adrese elektronického obchodu http://qca.postsignum.cz/shop/shop.php?Deleni=Czech%20POINT

Systém Vás provede třemi kroky elektronické objednávky.

1. Výběr zboží
2. Doplnění adresy
3. Rekapitulace objednávky, potvrzení

3.2 Smlouva o poskytování certifikačních služeb

Nejprve je potřeba s Českou poštou uzavřít smlouvu o poskytování certifikačních služeb a dodat seznamy žadatelů s údaji pro vydání certifikátů.

Pokud již má obec uzavřenou smlouvu na vydávání kvalifikovaných i komerčních certifikátů, můžete tuto kapitolu přeskočit.

3.2.1 Vyhledávání a stažení formulářů

Pokud nevíme, jestli má obec nějaké smlouvy uzavřené, můžeme použít vyhledávací aplikaci na stránce http://qca.postsignum.cz/projects/czechpoint/getforms.php

Pokud nemáme žádné smlouvy uzavřené, zaklikneme políčko **Neprohledávat databázi, zobrazit všechny dostupné formuláře** *a* pokračujeme tlačítkem **Vyhledat**.

V dalším kroku se už dostaneme na seznam všech formulářů, které jsou k dispizici.

3.2.2 Příprava objednávky nebo dodatku ke smlouvě

3.2.2.1 Příprava objednávky

Jako první stáhneme a vyplníme formulář **Smlouva o poskytování certifikačních služeb**, který nalezneme pod odkazem objednavka.doc. Tento formulář vyplníme. Zadáme údaje o obci, informace o lhůtě platnosti smlouvy, informace o objednaných službách, souhlas nebo nesouhlas využití poskytnutých údajů pro marketingové účely a v poslední řadě seznam oprávněných osob. Dokument vytiskneme ve 2 kopiích.

3.2.2.2 Příprava dodatku ke smlouvě

Pokud má obec uzavřenou smlouvu na poskytování služeb pouze kvalifikované nebo pouze komerční autority, musí provést postup uvedený v této kapitole.

Z webových stránek si stáhneme vzor změnového dodatku ke smlouvě - soubor dodatek zmenovy.doc. Do dodatku doplníme číslo dodatku a číslo současné smlouvy s Českou poštou. Pokud si nejsme těmito údaji jisti, ponecháme jejich doplnění na pracovníka České pošty. Dále doplníme údaje o obci. Zbytek dokumentu je již nastaven pro rozšíření služeb na obě autority. Na druhé straně doplníme údaje o zástupci zákazníka.

Dodatek vytiskneme ve dvou exemplářích. Na oba vytištěné dodatky se podepíše na straně 2 statutární zástupce obce.

Pokud jsme v dodatku v bodě 6 (Změna seznamu oprávněných osob) zvolili ANO, je potřeba vyplnit a podepsat přílohu dodatku. V opačném případě není potřeba přílohu dodatku vyplňovat.

3.2.3 Příprava seznamů žadatelů

Ze stejné stránky stáhneme vzor úvodního listu seznamu žadatelů (soubor sz uvodni list.doc) a přílohu seznamu žadatelů pro vydání dvou certifikátů v rámci projektu Czech POINT (soubor sz ca dual.doc).

3.2.3.1 Vyplnění úvodního listu seznamu žadatelů

- Evidenční číslo smlouvy nevyplňujeme, protože ještě není smlouva uzavřena.
- Doplníme údaje o obci, údaje o oprávněné osobě a uvedeme počet příloh.

Úvodní list vytiskneme, ale nepodepisujeme.

3.2.3.2 Vyplnění přílohy seznamu žadatelů

- Vyplníme osobní údaje žadatele o certifikát.
- Vyplníme údaje certifikátu.
    - Jako údaj CN můžeme zadat jméno a příjmení zaměstnance.
    - Jako údaj číslo žadatele v organizaci můžeme zadat zaměstnanecké číslo.
    - Jako údaj organizační jednotka můžeme zadat "Czech POINT".
- Dále můžeme nastavit doplňkové služby jako jsou zveřejnění certifikátu na WW stránkách, odeslání eMailové zprávy s upozorněním na končící platnost certifikátu.

Přílohu vytiskneme v jedné kopii a necháme ji podesat žadateli.

3.2.4 Doručení objednávky a seznamu žadatelů na kontaktní místo

Na webových stránkách si najdeme nejbližší kontaktní místo a telefonicky se informujeme, kdy se můžeme dostavit uzavřít smlouvu.

S sebou budeme potřebovat:

- vytištěnou a vyplněnou objednávku ve dvou exemplářích (včetně vytištěné a podepsané přílohy objednávky ve dvou exemplářích),
- zakládající listinu obecního úřadu, nebo jiný dokument, kde je **IČ**,
- doklad o volbě nebo jmenování statutárního zástupce obce,
- vytištěný a žadatelem podepsaný seznam žadatelů,
- svůj doklad totožnosti.

Operátorka kontaktního místa zkontroluje vyplněnou objednávku, zkopíruje si zakládací listinu a uzavře smlouvu. Obdržíme jeden podepsaný exemplář objednávky a přílohy objednávky.

Operátorka dále ověří identitu žadatele vůči osobnímu dokladu. Před operátorkou se podepíšeme jako oprávněná osoba na úvodní list seznamu žadatelů a operátorka potvrdí ověření podpisu na úvodním listu. Operátorka nás pak propustí s tím, že o zavedení uživatelů budeme informováni.

3.3 Instalace ovládacího software k USB tokenu, inicializace tokenu

Po doručení objednaných USB tokenů je potřeba na počítač žadatele nainstalovat ovládací software, který je umístěn na instalačním CD (to je rovněž potřeba zakoupit přes objednávkový systém).

Instalační příručku najdeme na webové stránce http://qca.postsignum.cz/projects/czechpoint/files/prirucka.pdf a provedeme instalaci software a inicializaci daných USB tokenů (kapitoly 2 a 3).

3.4 Instalace certifikátů certifikačních autorit

Aby byly vydané certifikáty považované za důvěryhodné, musí si žadatel do počítače nainstalovat certifikáty certifikačních autorit PostSignum QCA a PostSignum VCA. Na webové stránce pro Czech POINT http://qca.postsignum.cz/projects/czechpoint/ klikneme na odkaz Instalace certifikátů certifikačních autorit PostSignum v kapitole 4 příručky.

Pokud je možné na počítači provést automatickou instalaci certifikátů autorit, stačí stisknout tlačítko **Instalovat certifikáty**. V opačném případě toto tlačítko není přístupné a je nutné provést ruční postup instalace certifikátů, který je na stránce rovněž uveden.

3.5 Vydání certifikátů žadatelům

Vydání certifikátů je připraveno až po obdržení eMailu od certifikační autority, kde informuje, že žadatel byl zaveden do systému a může se dostavit na kontaktní místo k vydání certifikátu.

3.5.1 Generování klíčů a žádostí o certifikát

Žadatel si na svém počítači vygeneruje klíčový pár a elektronickou žádost o certifikát za použití webové stránky. Zadá stejné údaje, jaké byly uvedeny při tvorbě seznamu žadatelů.

Dále kline na odkaz **Vygenerovat** a po potvrzení několika dialogových oken se vypíše informace, že vygenerované žádosti o certifikát byly odeslány na server PostSignum.

Telefonicky si domluvíme s kontaktním místem termín návštěvy a vydání certifikátů. Ve stanoveném termínu se vydáme na kontaktní místo s občanským průkazem.

3.5.2 Vydání certifikátů na kontaktním místě České pošty

Na kontaktním místě zkontroluje operátorka totožnost žadatele podle občanského průkazu, který si zkopírovala.

Operátorka si ze serveru PostSignum stáhne uložené žádosti o vydání certifikátů. Vytiskne písemnou žádost o certifikát, kterou žadatel odsouhlasil svým podpisem. Operátorka následně vydá dva certifikáty (kvalifikovaný a komerční) a sepíše protokol o vydání certifikátů.

3.5.3 Instalace certifikátů na USB token

Žadatel opustí kontaktní místo a ve své kanceláři spustí webové stránky

- https://qca.postsignum.cz/projects/czechpoint/crtinst.php
- https://vca.postsignum.cz/wizards/crtinstall.php

pro instalaci certifikátů na token.

Na protokolech najde informaci, že kvalifikovaný certifikát má sériové číslo **XXXXXX** a komerční **YYYYYY**.

Číslo certifikátu vyplníme do příslušného políčka a klikneme na odkaz **Instalovat**. Následně ten samý postup provedeme s druhým certifikátem.

V této chvíli jsou již certifikáty úspěšně instalovány na token.

3.6 Doplňující informace

Dodání dalších seznamů žadatelů

Pokud budeme v budoucnu potřebovat vydat certifikáty ještě dalším osobám, připravíme seznam žadatelů podle postupu v přecházejících kapitolách a doručíme jej na kontaktní místo České pošty.

V rámci uzavřené smlouvy je možné požádat i o certifikáty určené k jiným účelům než pro projekt Czech POINT. K tomu je potřeba použít jiné formuláře seznamu žadatelů, které lze stáhnout z oficiálních stránek

- http://qca.postsignum.cz/ nebo
- http://vca.postsignum.cz/

4 Používání certifikátů v prostředí Czech POINT

4.1 Podmínky pro přihlášení do systému Czech POINT pomocí komerčního certifikátu

Pro přihlášení do Czech POINT pomocí komerčního certifikátu musíme splňovat dvě podmínky:

1. zasunutý USB token v počítači
2. údaje o tomto certifikátu musí být zavedeny v Administraci Czech POINTU v daném profilu uživatele. Zavedení těchto údajů provádí Administrátor Czech POINTu.

Do administrace se zavádí tyto údaje:

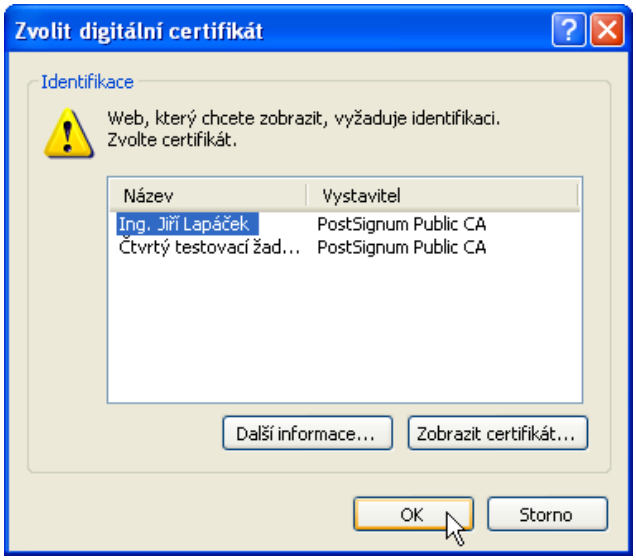
1. sériové číslo certifikátu - najdeme jej na protokolu o vydání certifikátu v části **Údaje o certifikátu.**
2. název certifikační autority, která certifikát vydala.

4.2 Přihlášení k centrále Czech POINT

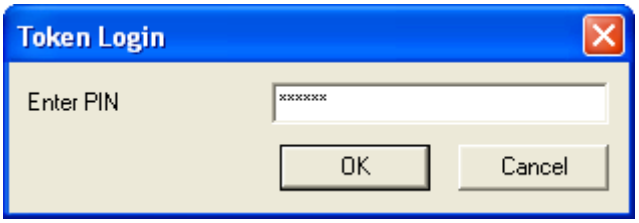
Připojíme USB token k počítači.

K aplikaci Czech POINT se přihlásíme na adrese https://www.czechpoint.cz/

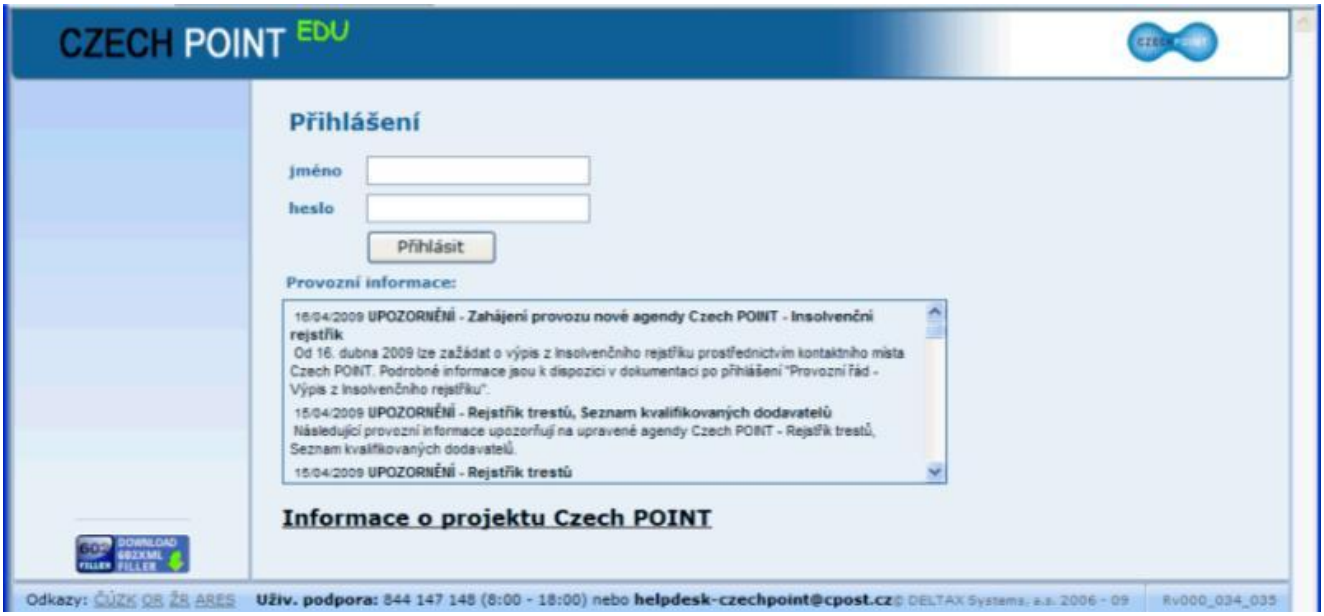
Po otevření stránky budeme požádáni o volbu komerčního certifikátu.



Z nabízeného seznamu vybereme ten, který budeme chtít použít a volbu potvrdíme klepnutím na tlačítko **OK**. Následně budeme vyzváni k zadání bezpečnostního hesla (PIN) k USB tokenu.



Po ověření PIN se zobrazí stránka s formulářem pro **Přihlášení** do samotné aplikace Czech POINT. Zadáme uživatelské jméno a heslo pro přístup.



Po úspěšném přihlášení se zobrazí standardní nabídka pracovních formulářů aplikace Czech POINT.

4.3 Podmínky pro podepsání žádosti elektronickým podpisem kvalifikovaného certifikátu

Pro podepsání žádosti pomocí kvalifikovaného certifikátu musíme splňovat dvě podmínky:

1. zasunutý USB token v počítači
2. údaje o tomto certifikátu musí být zavedeny v Administraci Czech POINTu v daném profilu uživatele. Zavedení těchto údajů provádí Administrátor Czech POINTu.

Do administrace se zavádí tyto údaje:

1. sériové číslo kvalifikovaného certifikátu - najdeme jej na protokolu o vydání certifikátu v části **Údaje o certifikátu.**
2. název certifikační autority, která certifikát vydala.

4.4 Podepisování žádosti elektronickým podpisem kvalifikovaného certifikátu

Elektronickým podpisem kvalifikovaného certifikátu se podepisují žádosti z neveřejných rejstříků – např. z Rejstříku trestů.

V takovém případě se nejprve běžně přihlásíme do systému Czech POINT komerčním certifikátem. Dále pak otevřeme klepnutím na řádek s položkou Rejstřík trestů formulář.

Sestavenou žádost odešleme stiskem tlačítka **Zažádat o výpis z evidence rejstříku trestů**. Při odeslání se otevře dialog s nabídkou kvalifikovaných certifikátů. Musíme vybrat položku potřebného certifikátu a stiskem tlačítka **OK** žádost elektronicky podepíšeme.

Po zadání správného PIN k USB tokenu se žádost fyzicky odešle na Rejstřík trestů.

5 Použité zdroje

- Provozní řád Czech POINT
- Webové stránky PostSignum, eIdentita, První certifikační autorita
- Webové stránky Katedry telekomunikační techniky, FEL - ČVUT

MODUL: Administrace Czech POINT

Správa uživatelského účtu pro Czech POINT od získání přístupových údajů pro administrátora po zavedení dalších uživatelů, portál ePUSA, iManager, správa účtu u Katastru nemovitostí.

Po prostudování bude absolvent umět spravovat uživatelský účet pro Czech POINT, včetně správy účtu u Katastru nemovitostí. Bude umět zadat potřebné údaje do portálu ePUSA a do iManažeru.

1 Příprava PC k přihlášení do Czech POINT

Klient CP může být provozován na libovolném počítači ověřujícího úřadu, na kterém je nainstalováno následující softwarové vybavení:

1. operačním systémem Microsoft Windows 2000, XP nebo Vista
2. prohlížeč Microsoft Internet Explorer ve verzi 6.0, SP3 a vyšší
3. program 602XML Filler
4. program pro čtení PDF souborů – Adobe Reader
5. Certifikáty (kořenová a podřízená certifikační autorita *PostSignum VCA, PostSignum QCA*, kvalifikovaného certifikátu I.CA)

Odkazy na zdroje, způsob a popis instalace tohoto softwarového vybavení nejsou předmětem tohoto kurzu, jsou podrobně popsány v dokumentaci k systému Czech POINT dostupné při přihlášení do systému v roli správce skupiny.

2 Získání přístupových údajů do Czech POINT

Vydávat výstupy podle zákona 365/2000 Sb. a jeho novely 269/2007 Sb. mohou krajské úřady, matriční úřady, zastupitelské úřady a dále další úřady, které jsou uvedeny ve vyhlášce 388/2007 Sb. Ta stanoví seznam obecních úřadů a seznam zastupitelských úřadů, které vydávají ověřené výstupy z informačních systémů veřejné správy.

Obce, které se přihlásily o udělení dotace na zřízení kontaktního místa veřejné správy v rámci Integrovaného operačního programu (žádosti bylo možné podávat od 1.12.2008 do 31.5.2009), budou automaticky uveřejněny v novelizované **Vyhlášce o kontaktních místech veřejné správy** a poté obdrží od MVČR přístupové údaje k systému Czech POINT. Tento proces probíhal v říjnu – listopadu 2009. Více informací na http://www.czechpoint.cz – odkaz Pro kontaktní místa - Zřiďte si Czech POINT.

Obce, které se nepřihlásily o udělení dotace na zřízení kontaktního místa a chtějí nově zřídit na svém úřadě Czech POINT, musí vyplnit formulář „Žádost o zařazení do Czech POINTu“. Tato žádost je ve formátu formuláře ZFO. Pro otevření formuláře je nutná instalace programu 602XML Filler. Stažení tohoto softwaru je bezplatné. Formulář na vyžádání poskytne MVČR.

3 Zákaznický účet u ČÚZK

Pro vydávání výpisů z Katastru nemovitostí je potřeba mít založen zákaznický účet u ČÚZK.

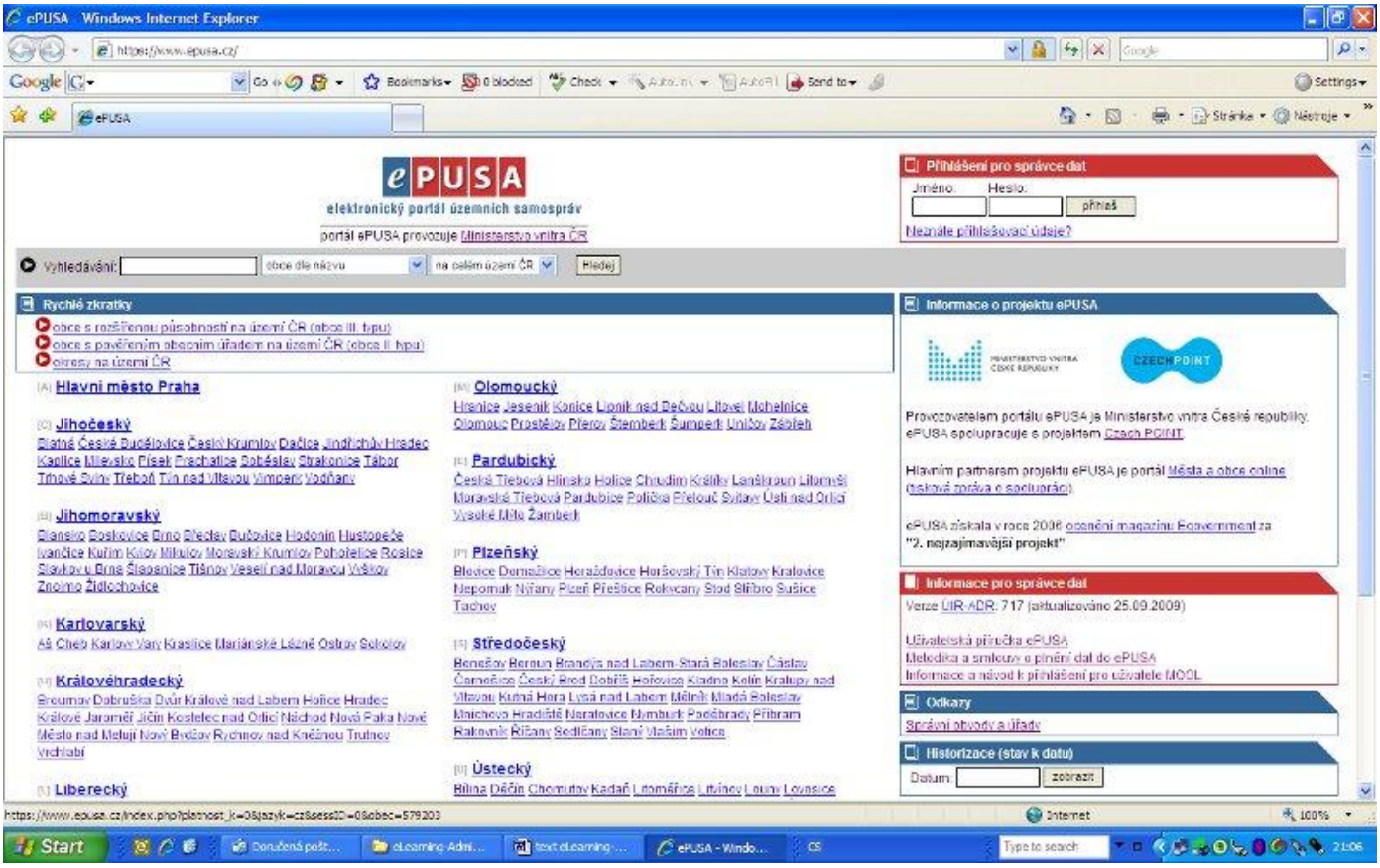
Žádost o založení zákaznického účtu

Obce s rozšířenou působností mohou mít již smlouvu podepsanou na přímý přístup do KN. Pro výpisy z Czech POINT je potřeba mít uzavřenou ještě jednu smlouvu s poznámkou "Czech POINT".

4 Přihlášení se k administraci Czech POINT v ePUSA

Každému ověřujícímu úřadu byly zaslány od MVČR přístupové údaje k systému ePUSA **tzv. lokální administrátorský přístup** skládající se z uživatelského jména a hesla. Pro tyto administrátory ze samosprávy (krajské úřady, obce, statutární města a jejich obvody) je určeno integrované rozhraní **ePusa** neboli Elektronický portál územních samospráv (www.epusa.cz). Administrátor zde může kromě jiného zřídit uživatelské účty svých pracovníků pověřených vydáváním ověřených výstupů v Czech POINT a vydáváním výstupů v režimu CZECHPOINT@office, dále provést konfiguraci formuláře Czech POINT.

Do ePUSA se přihlašujete pomocí uživatelského jména a hesla lokálního administrátora CzechPOINTu, které vám byly zaslány (pokud neznáte přihlašovací údaje, požádejte helpdesk Czech POINTu o radu).



Po úspěšném přihlášení se Vám zobrazí vaše obec a vy můžete upravovat údaje:

- Základní údaje
- Statistika
- Další údaje
- Struktura organizace
- Kontaktní osoby
- Záložka "Zřizované organizace"
- Správní obvody a úřady
- Czech POINT
- Odkazy
- Datové schránky
- Sestava dle 106/1999 Sb.
- Export dat
- Krizové řízení
- Kontaktní osoby krizového řízení

- Mapa územního celku

V následujících částech kurzu se budeme zabývat pouze volbami **Kontaktní osoby** a **Czech POINT**, podrobná práce v ePUSA a funkce ostatních záložek je popsána v Uživatelské příručce ePUSA.

Důležité upozornění: V současné době není možné přihlašovat se do ePUSA pomocí certifikátů a ani není možné v rozhraní ePUSA spravovat certifikáty kontaktních osob používajících CzechPOINT. Certifikáty je potřeba spravovat v nástroji iManager. Funkce správy certifikátů však bude v brzké době do rozhraní ePUSA doplněna. Administraci v nástroji iManager je věnována jedna kapitola tohoto kurzu.

Přihlášení do ePusa se nezdařilo?

Pak je možné, že zadáváte údaje špatně. Zkuste dodržet následující postup při zadávání přihlašovacích údajů:

1. Jméno zadávejte přesně tak, jak je napsáno v dopisu, tedy malými písmeny.
2. Při zadávání hesla zkontrolujte na klávesnici, zda nemáte zapnutý CapsLock.
3. Jsou-li součástí hesla i číslice, ujistěte se, že píšete opravdu číslice a ne písmena s diakritikou. Například vypadá-li heslo nějak takto: "abc234", je dost možné, že píšete "abcěšč".

Nedaří-li se přihlášení ani při dodržení výše uvedeného postupu, obraťte se na službu helpdesk CzechPOINTu s žádostí o radu.

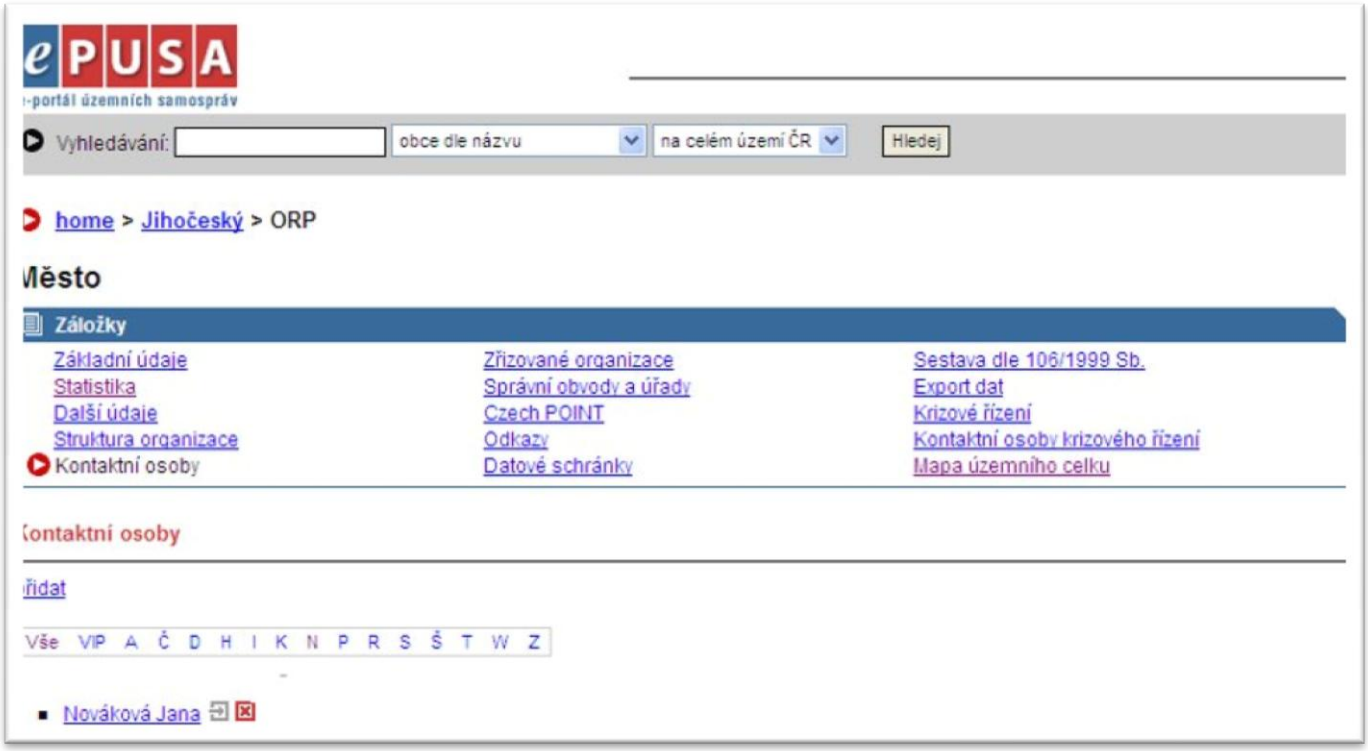
5 Editace údajů v ePusa

Pro administraci Czech POINT slouží v menu Záložky odkazy: **Kontaktní osoby** a **Czech POINT**.

5.1 ePUSA - Kontaktní osoby - přidat

Pro potřeby Czech POINT lze ve formuláři Kontaktní osoby založit nového uživatele, přiřadit mu uživatelské jméno, heslo a přístup do Czech POINT.

Záložky – Kontaktní osoby (zobrazí se dříve již zadané kontaktní osoby, zpravidla je to starosta, místostarosta, informatik) – volbou přidat lze zadat další kontaktní osobu a její práva pro práci s Czech POINT



5.2 Kontaktní osoby – zadání nových údajů o osobě

Ve formuláři je potřeba zadat funkci, příjmení, jméno, titul, adresu, účet v Czech POINTU, roli v Czech POINTU, uživatelské jméno, heslo a další údaje.

Uživatelské jméno
Musí obsahovat nejméně 5 znaků, kterými mohou být alfanumerické znaky bez diakritiky, podtržítko, pomlčka, tečka. Pokud potřebujete změnit uživatelské jméno, je potřeba se obrátit na hotline ePUSA.

Heslo pro uživatele
Musí obsahovat nejméně 7 znaků, kde minimálně 4 musí být jedinečné a musí být obsažena minimálně jedna číslice. Nesmí být shodné s uživatelským jménem, křestním jménem či příjmením (příklad „bflm3ps“)

Účet v Czech POINTU

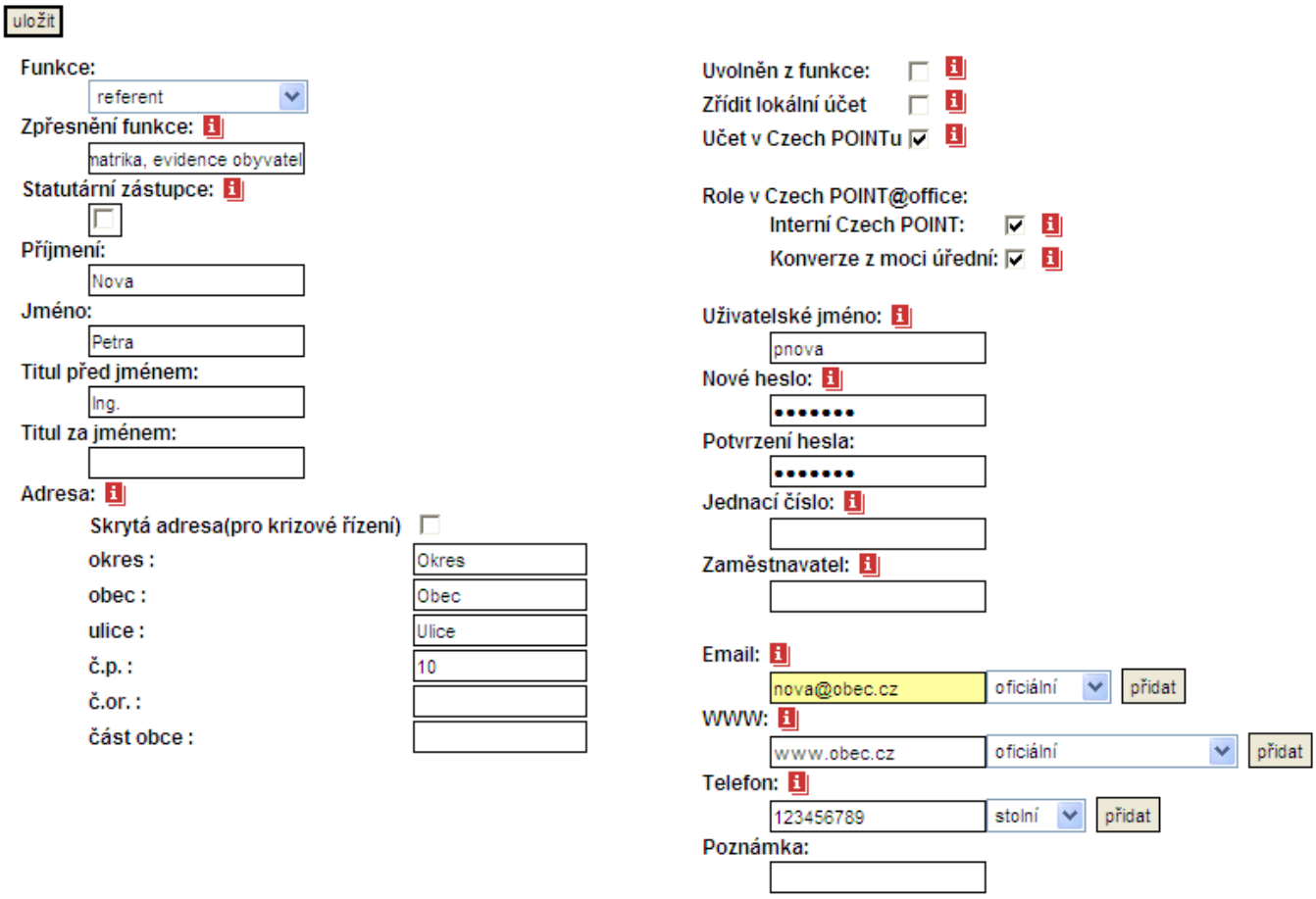
Zaškrtnutím osoba získává přístup do Czech POINT – ikona CzP

Role v Czech POINT@office – Interní Czech POINT

Zaškrtnutím osoba získává přístup do interního Czech POINT- ikona iCzP (dříve nazývaný vnitřní Czech POINT, prostřednictvím kterého se provádí výpisy z rejstříku trestů pro vnitřní potřebu úřadu dle Zákona č. 124/2008 Sb.)

Role v Czech POINT@office – Konverze z moci úřední
Zaškrtnutím je této osobě umožněno provádět konverzi z moci úřední (úřady, které již mají zřízen libovolný účet v rámci projektu Czech POINT, mohou autorizovanou konverzi z moci úřední zpřístupnit bez omezení svým úředníkům zavedeným v rámci jejich skupiny do projektu Czech POINT)

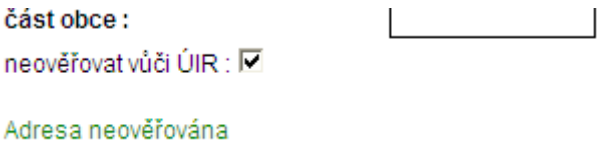
Zadané údaje uložíte tlačítkem **uložit**



5.2.1 Chyba při ukládání

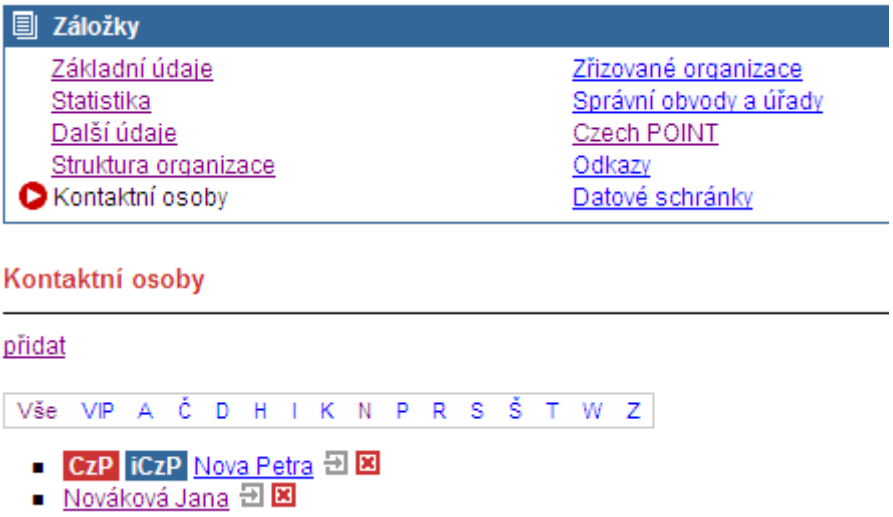
Uložení neproběhne, pokud je chybně zadaná adresa, nesouhlasí heslo s potvrzením hesla, chybí některý důležitý údaj, či jste zadali uživatelské jméno, které již někdo v Czech POINT používá. Musíte tyto údaje opravit a formulář znovu uložit.

Pokud se Vám nedaří zadat správně adresu, lze v položce Adresa zrušit ověřování zadané adresy vůči ÚIR (Územně identifikační registr):



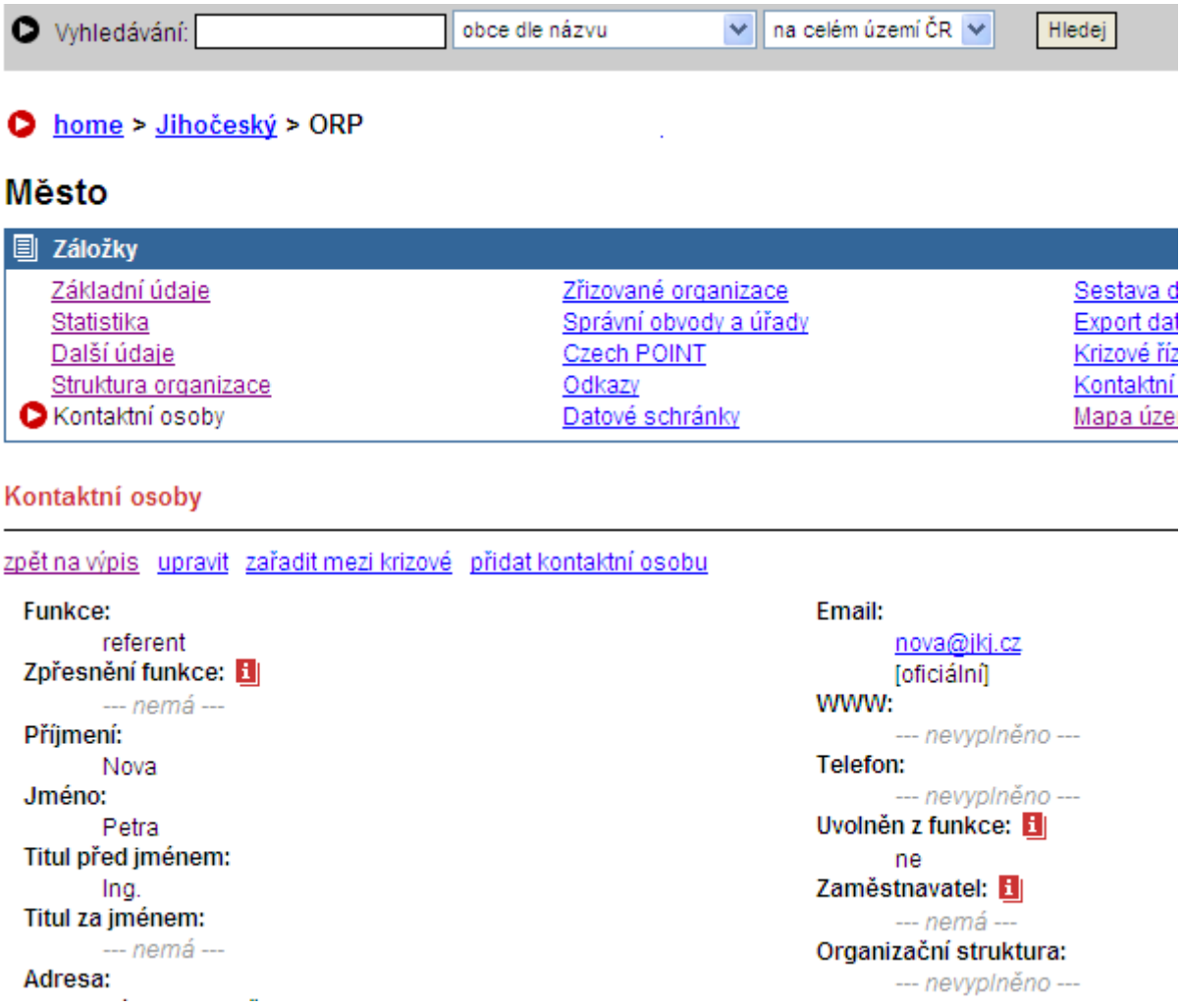
Kontaktní osoba se po přidání zobrazí v seznamu kontaktních osob ikony CzP a iCzP informují o přístupu této osoby do Czech POINT a Czech POINT@office.

Po správném zadání a uložení se zobrazí nová kontaktní osoba v seznamu:



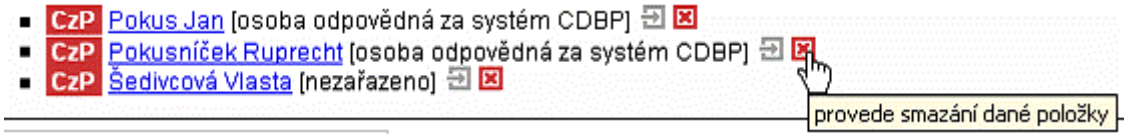
5.3 Kontaktní osoby – editace údajů o osobě

U dříve založených kontaktních osob lze upravit (editovat) zadané údaje, přidat novou roli apod. v detailu osoby volbou upravit.



5.4 Zrušení práva přístupu kontaktní osoby do Czech POINT

Zrušení přístupových práv se provede v editaci kontaktní osoby smazáním zaškrtnutí políčka Účet v Czech POINTu, obdobně pro interní Czech POINT a pro konverzi dokumentů. Kontaktní osobu jako takovou vymažete včetně jejího kompletního popisu klepnutím na políčko s červeným proškrtnutím v seznamu kontaktních osob vpravo od jejího jména.



5.5 5.5 | ePUSA - Czech POINT

Volbou Záložky – Czech POINT – Upravit lze zadat některé údaje, týkající se provozu tzv. konfigurace formuláře Czech POINT např.:

- Předvyplnění místa (názvu úřadu), kde se vydává ověřovací doložka.
- Propojení formuláře se spisovou službou.
- Automatické ukládání formuláře do určeného místa na lokální nebo síťový disk.
- Předvyplnění čísla jednacího (pořadového čísla) ověřeného výpisu.
- Hodnotu správních poplatků. Pokud tento parametr není uveden nebo je potlačen převedením do formy komentáře, pak cena za správní poplatky je podle zákona o správních poplatcích (100,- Kč za první stánku, za každou další je 50,- Kč).

Upozornění: změny v poplatcích se mohou v jednotlivých aplikacích projevit se zpožděním až několika hodin.

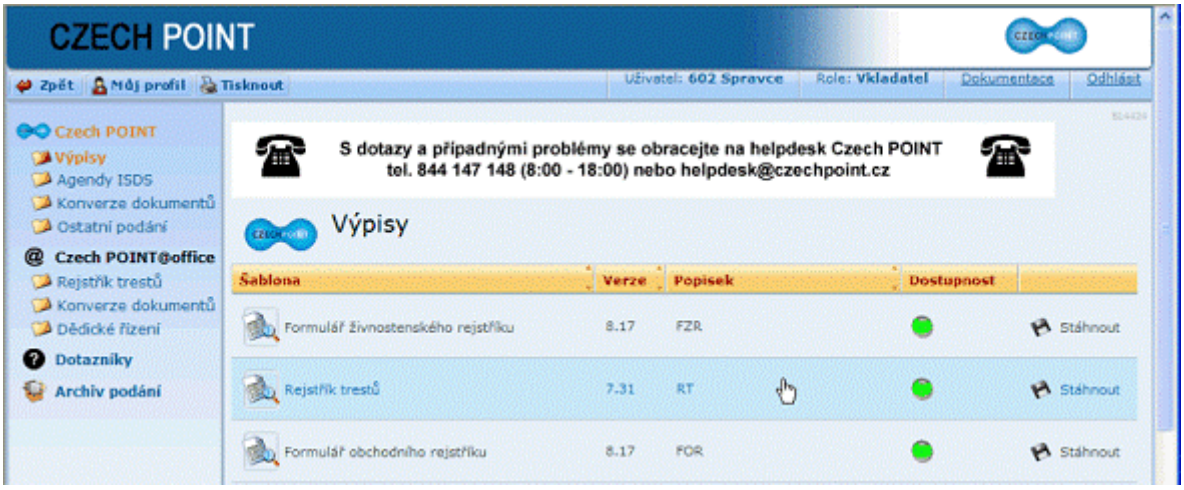
6 Administrace Czech POINT v nástroji iManager

Dalším krokem při administraci Czech POINT je zadání certifikátů uživatelů Czech POINT. V současné době lze toto provádět pouze v prostředí iManager. Předpokládá se, že funkce správa certifikátů uživatelů Czech POINT bude z důvodu zjednodušení administrace v brzké době integrována do rozhraní ePUSA. Prozatím je níže popsán způsob správy s využitím iManagera.

6.1 Přihlášení administrátora do prostředí iManager

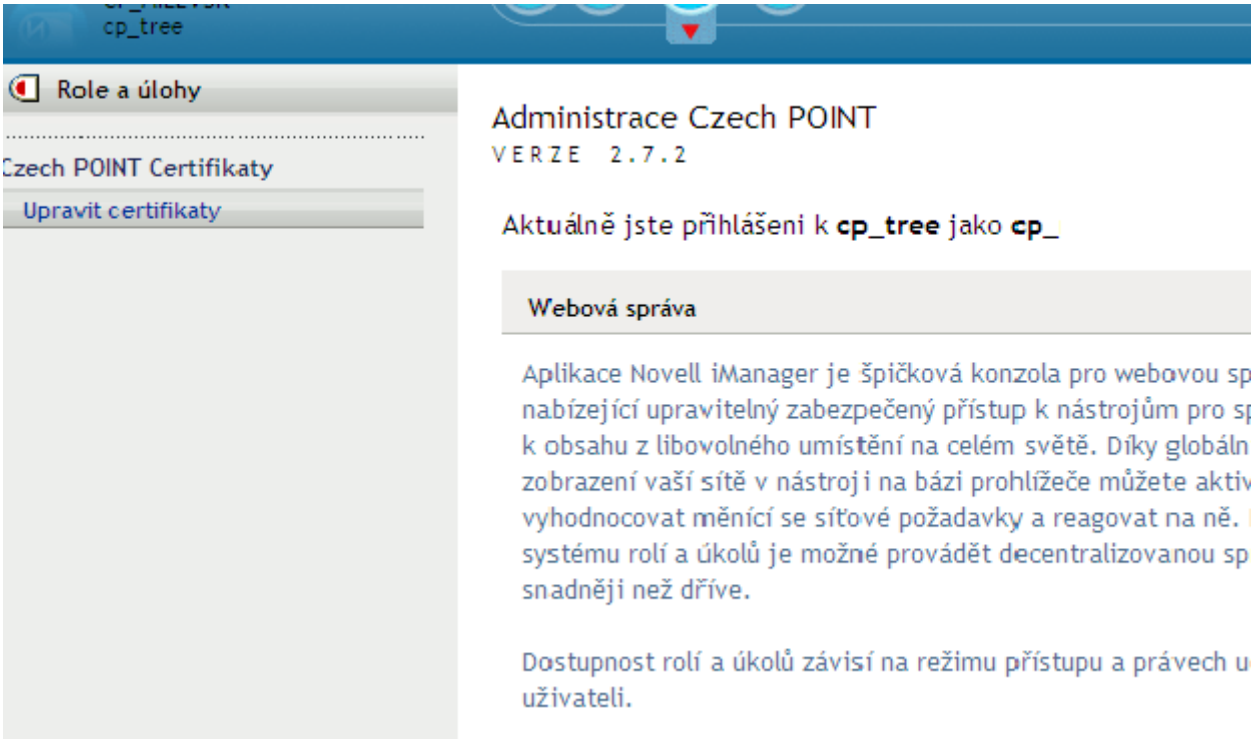
Webová adresa pro přístup k administraci je https://www.czechpoint.cz/nps/. Přihlášení je stejné jako k portálu ePUSA pomocí administrátorského jména (Uživatelské jméno) a hesla (Heslo). Stiskem tlačítka **Přihlásit** přejdete do okna pro administraci Czech POINTu.

Přihlášení se do iManagera je možné také přímo z hlavních stránek, načtených na adrese https://www.czechpoint.cz. Stačí v levé horní části okna klepnout myší na odkaz **Můj profil**; tím přejdete do výše uvedeného okna Administrace Czech POINT, kde pro kontrolu identifikace znovu zadáte administrátorské přihlašovací jméno a heslo:

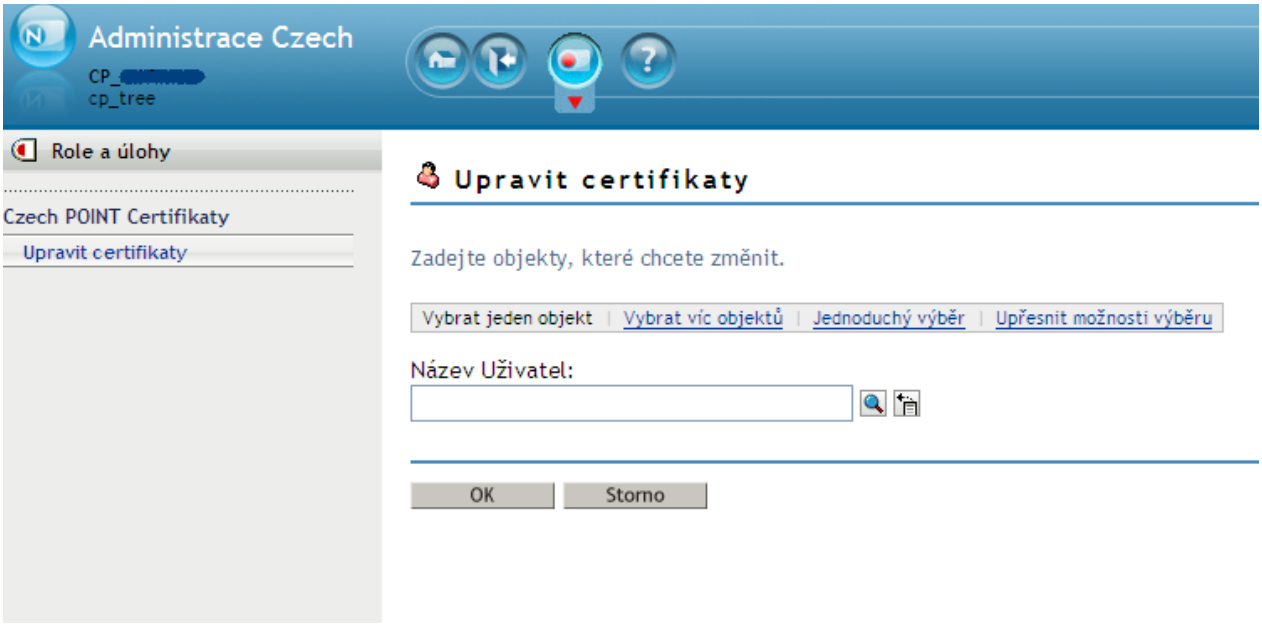


6.2 Upravit certifikáty

Po přihlášení do iManagera vyberete možnost upravit certifikáty:

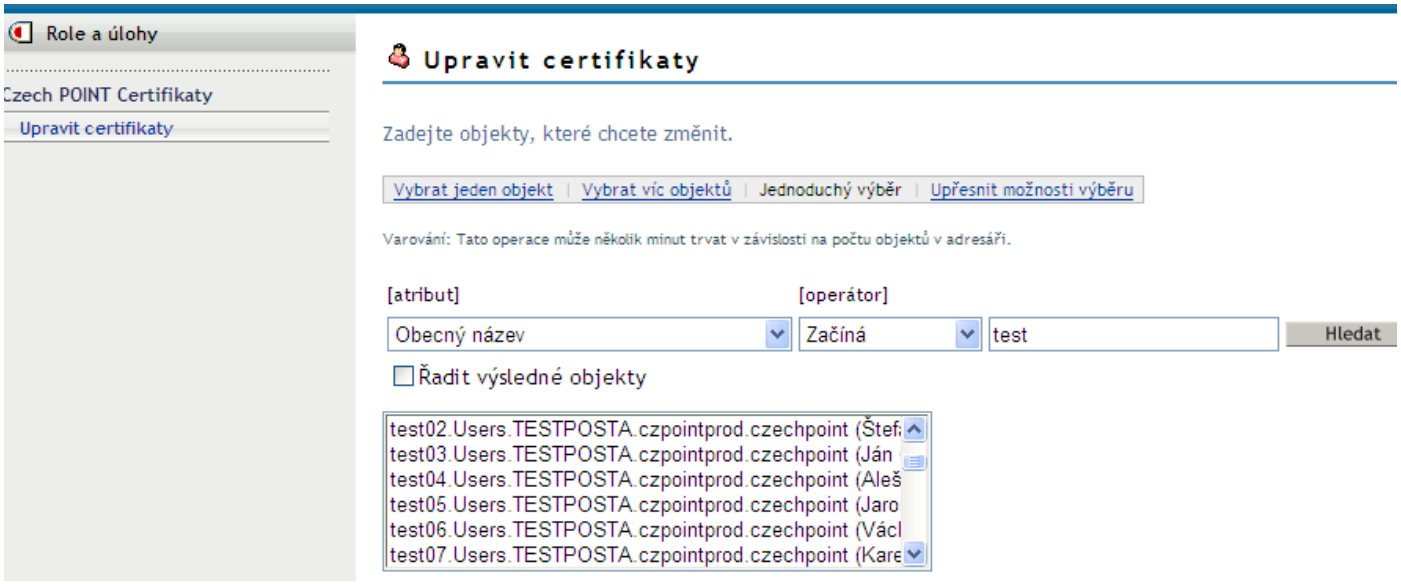


Dále je potřeba vyhledat uživatele, pro kterého certifikáty hodláte zadat:



6.3 Zavedení údajů uživatele

Zvolíte **Jednoduchý výběr**, do pole zadáte uživatelské jméno uživatele, pro kterého certifikáty budete zadávat (v našem případě je to „test“), zobrazí se seznam nalezených uživatelů, vyberete toho, který má v názvu za slovem .users. jméno vaší obce (např. pro uživatele novák z Prahy vypadá výsledek asi takto: novak.users.praha.czpointprod.czechpoint)



Po vyběru osoby (objektu) administrátor Czech POINTu provádí zavedení údajů o certifikátech uživatele (VCA-komerčním, QCA-kvalifikovaném) v daném profilu uživatele. Zavádí údaje:

- Sériové číslo certifikátu – najdete jej na protokolu o vydání certifikátu v sekci Údaje certifikátu.
- Název certifikační autority, která certifikát vydala
- Typ certifikátu kvalifikovaný (Q), komerční (V)

Tyto údaje zapisuje ve speciálním tvaru, složením ze tří informaci:

1. Sériové číslo certifikátu – naleznete jej na protokolu o vydání certifikátu v sekci údaje o certifikátu. Pokud vidíte informaci o sériovém čísle v podobě dvojčíslí oddělených dvojtečkami, zapište bez dvojteček. Tj. 12:34:56 zápis 123456
2. Název certifikační autority – v současné době jsou tři akreditované MV ČR. PostSignum, První Certifikační autorita, eIdentity. Pro zápis použijte názvy: postsignum, 1ca, eidentity.
3. Údaj o tom, zda se jedná o komerční nebo kvalifikovaný certifikát. Naleznete též na protokolu o vydání certifikátu v sekci údaje o certifikátu – Název certifikační politiky: certifikát pro ověření elektronického podpisu fyzické osoby – kvalifikovaný (zápis Q) certifikát fyzické osoby – komerční (zápis V)

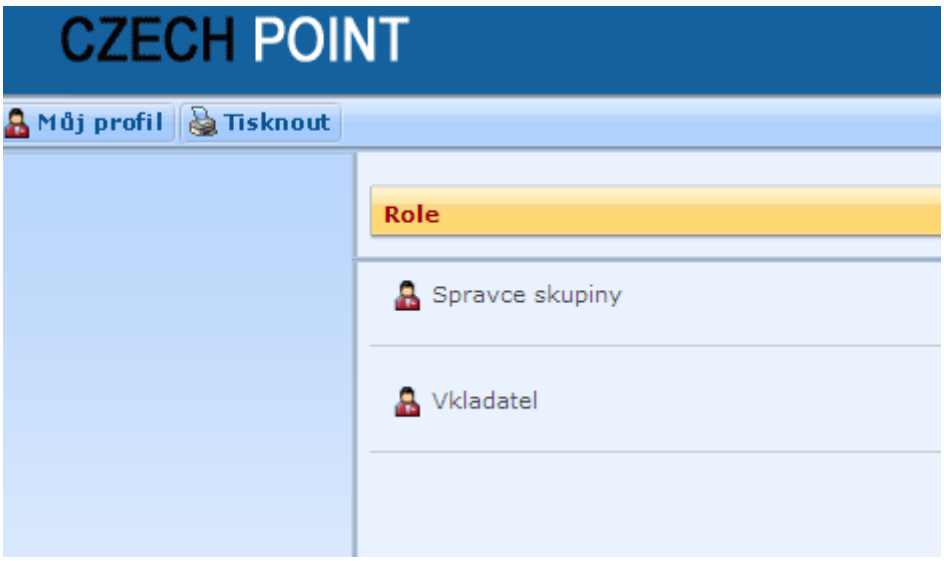
Poznámka: Jako oddělovače jsou použity znaky @ a #

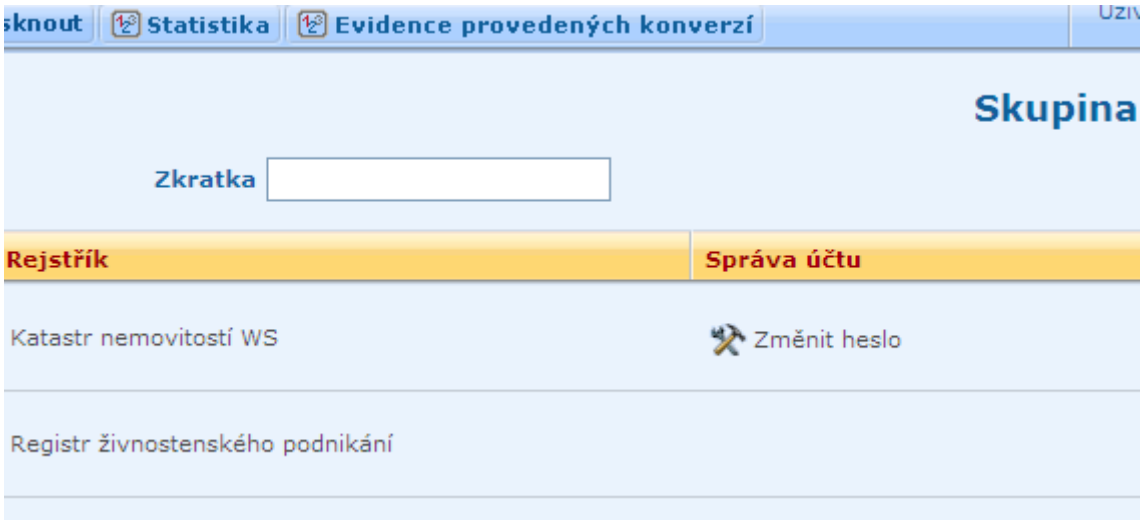
Výsledný řetězec zapsaný do políčka seznamu certifikátů bude tedy například ve tvaru 123456@postsignum#V pro komerční certifikát a například 789123@postsignum#Q pro kvalifikovaný.

Postup zavádění údajů je podrobně popsán v administrátorské části dokumentace CzechPoint dostupné při přihlášení do systému v roli správce skupiny.

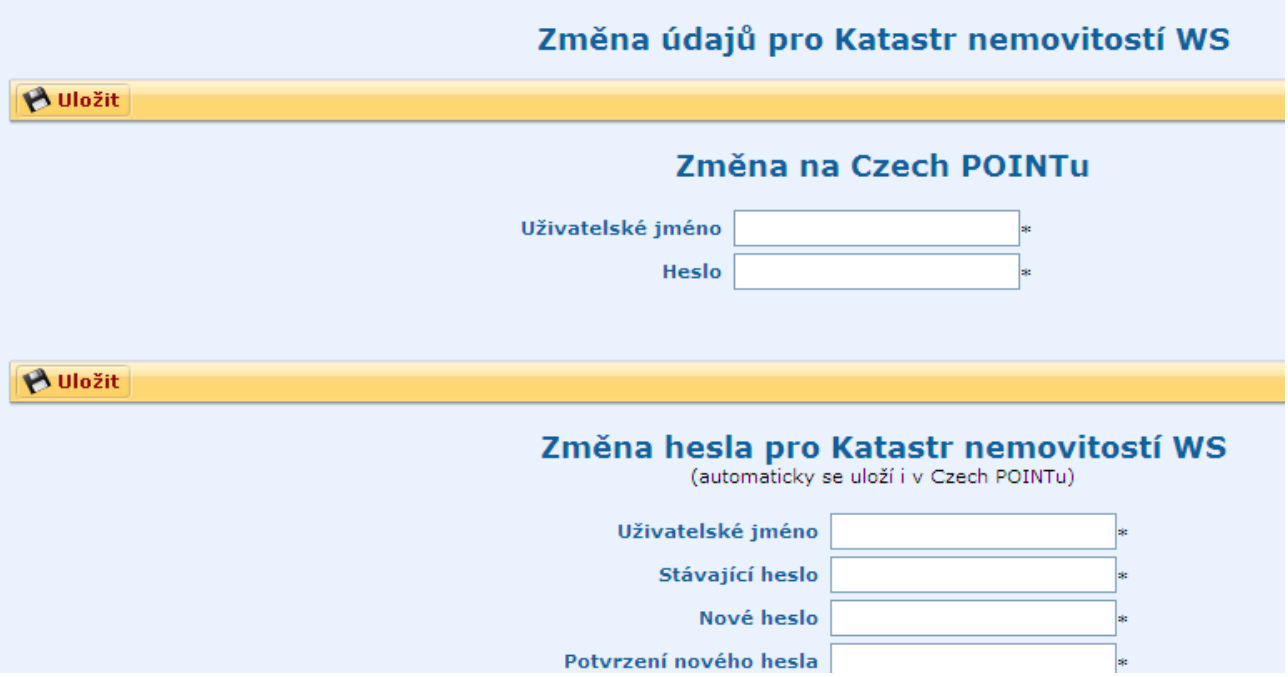
7 Zadání hesla Katastru nemovitostí

Jednou z činností administrátora je zadání hesla pro přístup do Katastru nemovitostí (a poté každý ½ rok pravidelná změna hesla). Tuto činnost provádí administrátor v Czech POINTU je v roli správce skupiny:





Ve smlouvě s ČÚZK je uvedeno uživatelské jméno a heslo, které bylo vašemu úřadu pro práci v Czech POINT přiděleno, uvedete je v polích uživatelské jméno a heslo. Při změně hesla, kterou systém požaduje každý ½ rok uvádíte stávající heslo a nové, které je nutné ještě jednou potvrdit.



8 Použité zdroje

- Portál ePUSA www.epusa.cz
- Portál Czech POINT http://www.czechpoint.cz , https://www.czechpoint.cz
- Ministerstvo vnitra www.mvcr.cz

9 Souhrn

V tomto modulu jsme se seznámili s Administrací posrtálu Czech POINT, získání a zavedení hesla pro přístup do Katastru nemovistostí, správu sytému na portálu ePUSA.

MODUL: Administrativní bezpečnost

Základní opatření na ochranu informací, zahrnující personální bezpečnost, fyzickou bezpečnost a režimovou bezpečnost, platná legislativa.

Seznámit se v základních bodech s ochranou informací a jejími složkami - režimovou, personální, technickou, fyzickou bezpečností.

1 Úvod do studia administrativní bezpečnosti a správních poplatků

V tomto modulu se zaměříme na zásady, které musíme dodržovat v případě, že pracujeme s informačními systémy, které obsahují osobní nebo citlivé údaje. Při práci s portálem Czech POINT se s takovými daty setkáváme, proto musíme jejich ochraně věnovat potřebnou pozornost. Musíme dodržovat opatření na ochranu osobních dat a také opatření administrativní bezpečnosti.

Seznámíme se s platnou legislativou v oblasti ochrany dat a administrativní bezpečnosti a upozorníme na různé oblasti zabezpečení dat a práce s nimi.

1.1 Přehled legislativy

Nakládání s osobními a citlivými údaji a bezpečnost informačních systémů je ukotvena v právních dokumentech:

- Vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.
- Vyhláška č. 527/2005 Sb., o personální bezpečnosti,
- Vyhláška č. 526/2005 Sb., o průmyslové bezpečnosti,
- Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků
- Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. dubna 2009.

1.2 Bezpečnostní rizika

Problematiku bezpečnosti dat je třeba vždy řešit komplexně. Tady více než kde jinde platí, že celý systém je jenom tak silný, jak silný je jeho nejslabší článek. Všechny součásti zabezpečení by měly být v souladu a vyvážené. Častou chybou je zaměření se na jeden z faktorů bezpečnosti, například na technické řešení a opominutí neméně důležitého lidského faktoru.

Bezpečnostní rizika se rozdělují na personální, administrativní, objektová a technická a na rizika vyplývající ze zabezpečení informačních systémů.

Personální rizika

Představují významný faktor v bezpečnostní politice. Jsou závislá na jednotlivých osobách, které s informačním systémem pracují, na jejich postoji, psychickém stavu, osobních vlastnostech. Už při výběru pracovníka na pozici, ve které bude přicházet do styku s osobními údaji nebo citlivými údaji je třeba toto zohlednit.

Administrativní rizika

Se výrazně zvyšují při nedodržování opatření vyplývajících z platných legislativních předpisů a z organizačních opatření organizace.

Objektová a technická rizika

Spočívají především ve výběru nevhodných objektů, umístění pracoviště do nevhodných prostor, kde hrozí nebezpeční poškození, znehodnocení nebo neoprávněného nakládání s daty.

Technická rizika

Se uplatňují v procesu zpracování, uchovávání a manipulaci s daty, kdy jsou používány takové technické prostředky, které nezaručují zamezení nebo alespoň výrazné snížení přístupu nepovolaných osob k datům.

V kurzu se zaměříme především na administrativní a personální rizika.

2 Ochrana informací

Přehled opatření k ochraně informací:

- režimová bezpečnost
- bezpečnost technických prostředků a programového vybavení
- bezpečnost dat a komunikačních cest
- fyzická bezpečnost
- personální bezpečnost

2.1 Režimová bezpečnost

Režimová bezpečnost - Představuje soubor opatření, kterým se stanoví podmínky provozu informačního systému, oprávnění přístupu jednotlivých osob na pracoviště informačního systému a k jeho pracovní stanici a způsoby nakládání se vstupy a výstupy informačního systému.

2.2 Bezpečnost technických prostředků a programového vybavení

Bezpečnost technických prostředků - Představuje soubor opatření k ochraně hardware informačního systému, jeho periferií (včetně dodržení jejich kompatibility) před jeho poškozením, zcizením nebo neoprávněnou úpravou.

- zabránit fyzickému poškození stanice (poškození vodou ap.).
- nepřipojovat k počítači nepovolené periferie (např. výměna tiskárny, připojení herních konzolí,...). Připojená zařízení nemusejí být kompatibilní a způsobí poruchu počítače, případně mohou znamenat nechráněný přístup k datům.

Bezpečnost programových prostředků - Představuje soubor pravidel pro instalaci, upgrade a odstraňování software v pracovní stanici informačního systému. Současně obsahuje pravidla pro ochranu informačního systému před napadením škodlivým softwarem.

Doporučuje se dodržet rozdělení přístupových práv k počítači na administrátora a uživatele. Nový software může instalovat pouze administrátor.

2.3 Bezpečnost dat a komunikačních cest

Bezpečnost dat - Představuje stanovení postupů pro ochranu údajů, trvale uložených v pracovní stanici informačního systému nebo na vyjímatelných médiích (diskety, CD, DVD, pevné paměti), podmínky pro jejich ukládání v pracovní a mimopracovní době a podmínky pro řešení servisních zásahů, případně likvidaci poškozených pevných disků a vyjímatelných médií.

Je třeba dát pozor na **data**, která se při práci **ukládají do počítače** - kopie žádostí o výpisy, 602XML formuláře a další.

Data musí být zabezpečena tak, aby se k nim **nedostala nepovolaná osoba.**

To znamená, že v případě **opravy počítače** nebo jeho **výměny** je třeba všechna data odstranit.

Bezpečnost komunikačních cest - Představuje pravidla pro obezřetnost ve vztahu k existujícím nebo nově instalovaným přenosovým cestám a rozvodům. Pozornost je třeba věnovat nečekaným změnám ve vedení rozvodů, jejich úpravám, dodatečným montážím dalších zařízení nebo jejich poškození – zcizení.

Jakékoli změny nebo podezření **hlásíme svému nadřízenému**.

2.4 Fyzická bezpečnost

Fyzická bezpečnost - Představuje souhrn pravidel pro ochranu pracoviště, na kterém se nachází informační systém, před neoprávněným vniknutím, odcizením nebo poškozením s využitím mechanických a elektronických prostředků (dveře, zámky, mříže, elektronické zabezpečení, osvětlení apod.).

- hesla a uživatelská jména nikomu nesdělujeme a nepíšeme si je na místa, kde mohou být snadno objevena
- zamykáme dveře, když opouštíme pracoviště
- pokud je to nutné, máme zajištěná okna, např. mříží
- USB tokeny, razítka, dokumenty nenecháváme volně ležet. Např. během práce by měly být uloženy v zavřené zásuvce, při opuštění pracoviště je zamkneme do skříně, trezoru, odevzdáme na vyhrazené místo ap.

2.5 Personální bezpečnost

Personální bezpečnost je významnou součástí opatření k zajištění bezpečnosti informačních systémů. K hlavním zásadám personální bezpečnosti se řadí:

- Výběr personálu - je vybírán už s ohledem na práci, kterou bude vykonávat.

- Řádné poučení o bezpečnostních opatřeních a tyto také průběžně kontrolovat. Kontroly se týkají jednak nakládání s informacemi a jednak dodržování bezpečnostních opatření v provozu pracoviště.
- Bezpečností opatření mít stále viditelně vyvěšena na pracovišti, aby k nim měl pracovník kdykoliv přístup.

Pracovník si musí být vědom, že jeho práce je i zpětně dohledatelná a všechny provedené kroky jsou zaznamenány.

Porušení opatření často vede k zneužití identity uživatele neoprávněnou osobou, vyzrazení osobních nebo citlivých dat, neoprávněná modifikace dat ap.

Průběžné kontroly dodržování bezpečnostních předpisů pracovníky jsou také velmi důležité. Vždy má existovat někdo, kdo má přehled o práci konkrétního pracovníka a kdo posoudí korektnost jeho jednání. Kontrola je **dvojsměrná** - ze strany **nadřízeného** a ze strany **poskytovatele dat**.

2.5.1 Doporučení pro práci s informačními systémy

Uživatel informačního systému by měl dodržovat základní bezpečnostní opatření. Bezpečnostní politiku si tvoří organizace, ale můžeme uvést alespoň některá obecně platné zásady:

- zvolit si dostatečně bezpečné přístupové heslo tak, aby bylo zapamatovatelné, avšak současně dostatečně složité, aby je jiná osoba nemohla snadno uhodnout a zneužít.
- uchovávat heslo v tajnosti, nesdělovat je jiným osobám, ani kolegům, se kterými se vzájemně zastupujeme
- heslo si nezapisovat, zvláště ne na snadno přístupná místa jako je monitor, klávesnice, nástěnka ap.
- při opuštění počítače jej zajistit proti zneužití, např. počítač uzamknout prostředky, které nabízí operační systém.
- při práci mít monitor umístěný tak, aby z něho nemohla neoprávněná osoba číst zobrazené informace.

3 Napadení informačního systému

Napadení informačního systému může být

- **Úmyslné**
  Běžnými prostředky nelze informační systém dostatečně ochránit před odhodlaným a znalým útočníkem. Důsledným uplatňováním kombinace vhodných opatření lze často napadení alespoň následně rozpoznat.
- **Z nedbalosti**
  Představuje běžné riziko práce s informačním systémem při nedodržení pravidel bezpečnosti. Typickým případem nedbalostního chování je:
  - Umožnění přístupu neoprávněné osoby (známého, kolegy, člena rodiny) k informačnímu systému.
  - Ponechání informačního systému v zapnutém a přihlášeném stavu bez dozoru.
  - Použití nesprávně kombinovaných (snadno zjistitelných) přístupových prvků – přihlašovací jméno, heslo.

- Zapsání přístupových prvků na obecně dostupné místo nebo jejich sdělování jiným osobám.
- Pokusy o instalaci vlastního (soukromého) software nebo modifikaci programového vybavení informačního systému.
- Umožnění dalšího neoprávněného využití informací, získaných prostřednictvím informačního systému.

4 Režimová bezpečnost – ochrana spisové agendy

Z hlediska charakteru informačního systému je prioritou zajistit v rámci pracoviště dostatečnou a prokazatelnou znalost personálu při manipulaci s citlivými vstupy a výstupy v podobě dat, dokumentů, respektive informací, získaných i pouhým náhledem do informačního systému.

Zásady oběhu dokumentů a médií

Musí souviset se zavedeným způsobem distribuce přijatých a vytvářených dokumentů v rámci pracoviště (úřadu). Dokumenty a média bývají zpravidla zúčtovatelné, je sledováno jejich předávání a seznamování se s nimi. Dokumenty týkající se přímo informačního systému, nebo vzniklé v jeho souvislosti, musí být do zavedeného systému oběhu dokumentů řádně zapojeny.

Zásady pohybu zaměstnanců – přístup na pracoviště

Pracovníci úřadu musí být řádně vyškoleni a musí být kontrolován jejich přístup do jednotlivých částí pracoviště, a to zejména v době nepřítomnosti pracovníků, příslušných k informačnímu systému, nebo po skončení pracovní doby. Zpravidla bývá i řešena otázka pohybu pracovníků a jejich oprávnění v případě krizových situací.

Zásady pohybu návštěvníků – klientů

Stejně tak musí být zaměstnancům zřejmé zásady pro pohyb klientů na pracovišti s důrazem na jejich bezpečnost, zachování diskrétnosti, a zabránění neoprávněného seznámení s citlivými údaji.

Zásady ukládání dokumentů a médií v průběhu a po skončení pracovního dne

Pracovníci musí být seznámeni s možnostmi bezpečného ukládání dokumentů a médií v průběhu pracovní doby, v době přestávek v práci a po skončení pracovní doby.

Zásady skartace

Pracovníci musí být seznámeni s možnostmi a postupy při ničení vadných, nebo nepoužitých dokumentů, médií, poznámek apod. A to včetně možnosti ukládání takovýchto dokumentů od momentu jejich vzniku do okamžiku jejich skutečného zničení.

Zásady manipulace s pomůckami – razítka

Stejně tak musí být pracovníkům zřejmé, jak mají postupovat v případě, že je jim svěřeno k výkonu práce použití evidenčních pomůcek, razítek, pečetí nebo zúčtovatelných formulářů. Pravidla, obecně zavedená v úřadě musí zahrnovat i specifické podmínky, související s provozováním informačního systému.

Nestačí pouze existence pravidel, musí se provádět a kontrolovat!

5 Automatizované prostředky spisové služby

Použití a režimy provozu informačního systému – zejména vstup dokumentů (žádostí) a výstupy (tisk dokumentů a kompletace jednotlivých agend) vyžaduje propojení s evidenčním systémem spisové služby v rámci každého příslušného pracoviště – úřadu. Z hlediska bezpečnosti je žádoucí zhodnotit propojení informačního systému s elektronickým nebo částečně automatizovaným systémem spisové služby v následujících oblastech:

- **Korektní interface**

Propojení informačního systému a systému spisové služby musí zajistit vyloučení vzájemného ovlivnění obou systémů. Z hlediska uživatele se jedná o povinnost seznámit se s pravidly přenosu informací mezi oběma systémy a jejich přísné dodržování. Softwarová kompatibilita je úkolem odpovědných IT pracovníků.

- **Prokazatelná evidence zápisů a jejich případných změn**

Pracovníci si musí být vědomi povinností, souvisejících s evidencí přijatých a vzniklých dokumentů, zejména dodržování postupů jejich evidence, zpracování, poskytování dalším pracovníkům a nadřízeným, postupů při ukládání a následného výběru dokumentů v rámci skartačního řízení. Důraz je třeba při tom klást na znalost správného postupu v případech chybného záznamu v evidenci, respektive korektního postupu oprav chyb. Pracovník si musí být jist, jakým způsobem lze bez následků opravit chybně provedený záznam tak, aby původní záznam, provedenou změnu a osobu, která opravu provedla, bylo možno následně identifikovat.

- **Korektní výstupy**

Pravidla pro vedení spisové služby stanovují jednoznačně podobu evidenčních záznamů (jednací protokol). Interním rozhodnutím v rámci úřadu je pak stanovena osobní odpovědnost za plnění konkrétních prací v průběhu roku, při uzavření roční evidence a provedení kontroly spisové agendy atd. Již v období přípravy zavedení informačního systému musí být tato skutečnost zohledněna v pravidlech spisové služby (spisovém řádu úřadu) tak, aby při uzavření kalendářního roku nedošlo ke vzniku disproporcí v evidenci dokumentů.

6 Zabezpečení pracoviště (objektu) – ukládání klíčů, ostraha, EZS

V rámci pracoviště, provozujícího informační systém Czech POINT musí být pracovníci řádně seznámeni se všemi povinnostmi, týkajícími se zabezpečení pracoviště (objektu) před neoprávněným vstupem a manipulací.

Způsob použití jednotlivých opatření závisí na konkrétních místních podmínkách, zhodnocení rizik, disponibilních finančních prostředcích a dalších mnoha vlivech. Zprovoznění informačního systému musí být v rámci hodnocení zabezpečení pracoviště (objektu) bráno vždy v potaz a musí mu být věnována náležitá pozornost.

7 Souhrn

V modulu jsme probrali problematiku **administrativní bezpečnosti.**

U administrativní bezpečnosti je ústředním motem naší práce **PERSONÁL PŘEDEVŠÍM**.

Je potřeba pracovníky seznámit se všemi bezpečnostními opatřeními, vysvětlit jim možné důsledky porušení těchto opatření a důsledně dodržování všech opatření kontrolovat.