Obecné základy práce s portálem Czech POINT (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:

4 hodiny

Anotace:

Kurz je zaměřen na získání obecných znalostí potřebných pro práci s portálem Czech POINT. Jednotlivé moduly kurzu jsou věnovány problematice administrativní bezpečnosti, správních poplatků, práce s certifikáty.

Průvodce kurzem:

Kurz je zaměřen na získání obecných znalostí potřebných pro práci s portálem Czech POINT. Jednotlivé moduly kurzu jsou věnovány problematice administrativní bezpečnosti, správních poplatků, práce s certifikáty.

Seznam modulů:

- CZECH POINT - INFORMAČNÍ GRAMOTNOST V KONTEXTU CZECH POINT
- CZECH POINT - ADMINISTRATIVNÍ BEZPEČNOST A SPRÁVNÍ POPLATKY (eGON)

Přílohy ke kurzu:

- CzP certifikáty
- Czech POINT a statistiky
- Pracovní sešit Czech POINT 2010
- Administrativní bezpečnost

Obsah modulu CZECH POINT - INFORMAČNÍ GRAMOTNOST V KONTEXTU CZECH POINT

1 Úvod do studia informační gramotnosti 5
2 Bezpečnostní prvky Czech POINT 5
3 Obecně o certifikátech 10
4 Kryptografie neboli šifrování 11
5 Souhrn 11

Obsah modulu CZECH POINT - ADMINISTRATIVNÍ BEZPEČNOST A SPRÁVNÍ POPLATKY (eGON)

1 Úvod do studia administrativní bezpečnosti a správních poplatků 13
2 Ochrana informací 13
3 Napadení informačního systému 15
4 Režimová bezpečnost – ochrana spisové agendy 16
5 Automatizované prostředky spisové služby 17
6 Zabezpečení pracoviště (objektu) – ukládání klíčů, ostraha, EZS 18
7 Správní poplatky 18
8 Souhrn 22
9 Informační zdroje 22

MODUL: CZECH POINT - INFORMAČNÍ GRAMOTNOST V KONTEXTU CZECH POINT

Filosofie Czech POINTu a práce s certifikáty.

Po prostudování modulu budou mít studující přehled o certifikátech používaných pro zabezpečený přenos dat při práci s terminálem Czech POINT a o šifrování zpráv všeobecně. Získají návod, jak certifikáty objednat a instalovat, jak uzavřít smlouvu o poskytování služeb certifikační autority.

1 Úvod do studia informační gramotnosti

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 modulu se zaměříme na znalosti práce s tokenem a certifikáty při práci na portálu Czech POINT.

Vysvětlíme si

- co všechno musíme splnit, abychom získali certifikáty
- jak se s tokenem a certifikáty pracuje
- jak si certifikáty nainstalujeme a inicializujeme

A dozvíme se něco o certifikátech a způsobech šifrování obecně.

V materiálech ke stažení najdete další studijní materiály, včetně úvodu do filosofie Czech POINTu.

Na úvodní straně celého kurzu si můžete v části Materiály ke kurzu stáhnout seznam rychlých kontaktů
pro práci s portálem Czech POINT.

2 Bezpečnostní prvky Czech POINT

Do provozu terminálů Czech POINT byly zavedeny nové bezpečnostní prvky:

- komerční certifikát - používá se pro bezpečné **přihlášení obsluhy k centrále CzP**. Jde tedy o autentizaci na straně serveru i klienta. Komerční certifikát říká serveru, **že daný člověk je oprávněn přistupovat** k centrále CzP. Certifikát **platí pro jedu osobu.**
- kvalifikovaný certifikát - na rozdíl od komerčního certifikátu se jeho význam neprojevuje na vstupu do CzP, ale **na výstupu** z něj. Používá se pro autorizaci dat a dokumentů a **zaručuje, že data a dokumenty byly vystaveny osobou, která je k jejich vystavení oprávněná** a že **nebyly před ověřením změněny**. Elektronicky se tak **podepisují žádost**i odesílané **do Rejstříku trestů**.

USB token iKey 4000

Certifikáty jsou kódy, které existují pouze v elektronické podobě. Jsou uloženy na zvláštním zařízení podobném USB Flash, nazvaném USB token iKey 4000.

Na tokenu jsou uloženy vedle certifikátů také jim odpovídající privátní klíče. Privátní klíč vygenerovaný uvnitř zařízení jej nikdy neopustí.

Používání tokenu je navíc chráněno bezpečnostním PINem. Zneužití tohoto hardwarového klíče je tedy v běžném režimu pracoviště téměř nemožné.

Certifikáty uložené na tokenu jsou osobní, vázané na konkrétního pracovníka. Provozovatel Czech POINTu si musí vyžádat tolik tokenů, kolik pracovníků bude terminál CzP obsluhovat.

2.1 Vyžádání USB tokenu a instalace uživatelského software

Abychom mohli USB token používat, musíme o něj zažádat, uzavřít smlouvu o poskytování služeb certifikační autority, instalovat do počítače uživatelský software k tokenu a token inicializovat.

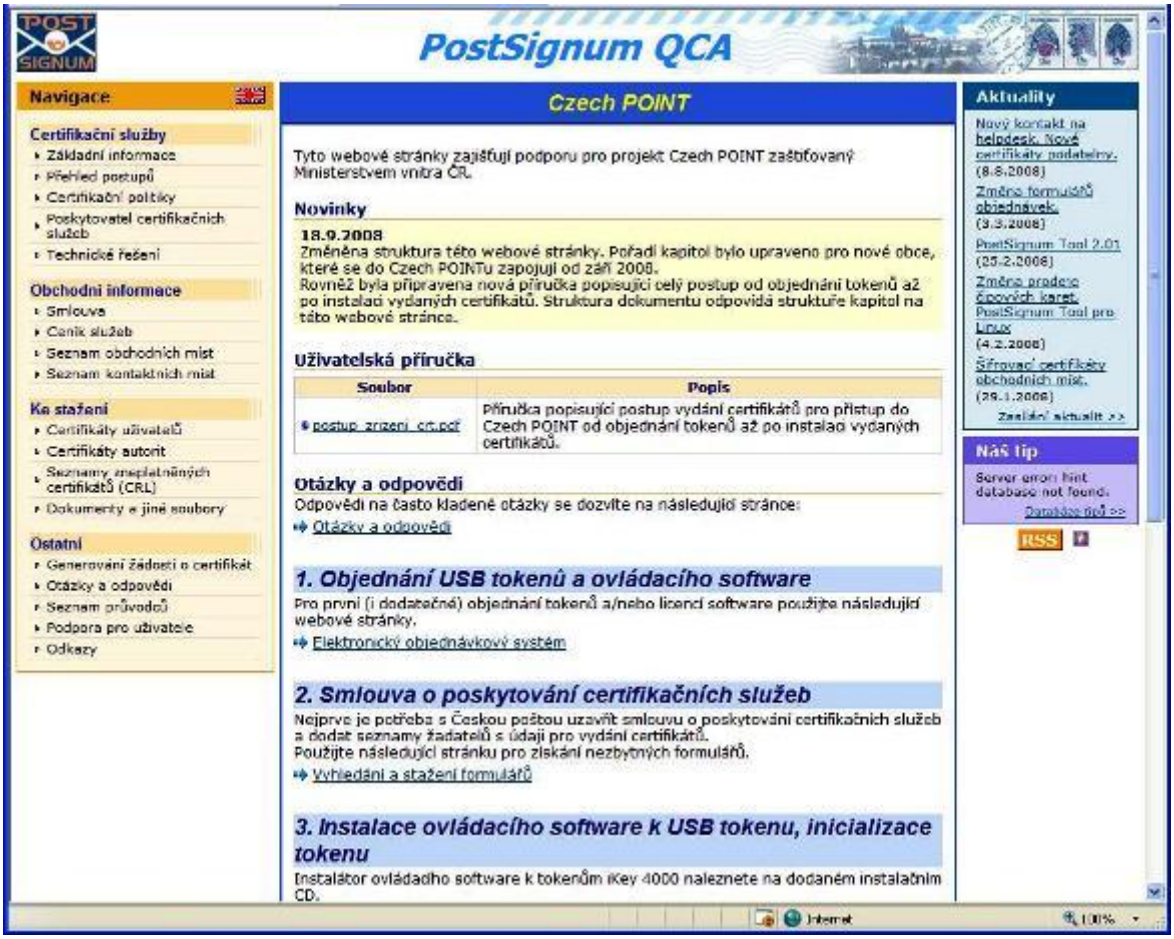
Proces je to poněkud zdlouhavý, tak si ho postupně popíšeme.

1. Po vstupu do projektu Czech POINT je nutné objednat USB token iKey 4000. K tomu lze využít elektronický objednávkový systém na adrese: http://www.postsignum.cz/. Pro práci s tokenem je potřeba software od výrobce tokenů (software od jiného výrobce nemusí fungovat!). V elektronickém objednávkovém systému můžete objednat samostatně instalační CD a licence software. Za běžných okolností postačí objednat jedno instalační CD a licence software v počtu odpovídajícím počtu stanic, na které bude software instalován. Licence ovládacího software je vázána na počítač. Pokud tedy máte jednu licenci software, můžete jej nainstalovat a provozovat pouze na jednom počítači. K tomuto počítači ale můžete připojit libovolné množství.

2. Oprávněná osoba (např. tajemník úřadu, starosta,...) musí připravit Smlouvu o poskytování služeb certifikační autority. Tou je v našich podmínkách Česká pošta. Ta musí vašemu úřadu oba certifikáty (komerční a kvalifikovaný) vydat. Ve smlouvě jste uveden jako žadatel o certifikát, protože certifikát se vydává na konkrétní osobu.

3. Podepsaná smlouva se doručí na kontaktní místo České pošty. Odpovědný pracovník pošty zavede vaše identifikační údaje do systému PostSignum a oznámí vašemu úřadu, že si můžete přijít pro certifikáty.

4. Nejlépe ještě před vyzvednutím certifikátu si do počítače nainstalujete uživatelský software k tokenu. Ten je volně k dispozici na internetu. Ze stejné stránky si stáhnete certifikáty certifikačních autorit. Pokud jste už s Czech POINTem pracovali, máte pravděpodobně tyto certifikáty již v počítači. Na uvedených stránkách PostSignum najdete podrobný návod k instalaci tokenu.



2.2 Inicializace tokenu

Po instalaci uživatelského software můžeme token oživit. Inicializační proces zahrnuje několik automatizovaných kroků, které postupně potvrdíme pouze kliknutím.

Inicializační proces spustíme z již uvedené stránky PostSignum. Doporučujeme postupovat podle uživatelské příručky, kde jsou všechny postupy včetně odkazů na potřebné soubory.

Během inicializace zadáváme osobní PIN a odblokovávací kódy PUK. PIN používáme při každé operaci s tokenem. Pokud zadáme 5x po sobě špatný PIN, token se zablokuje. Odblokovat ho můžeme pomocí kódu PUK a zase máme 5 pokusů.

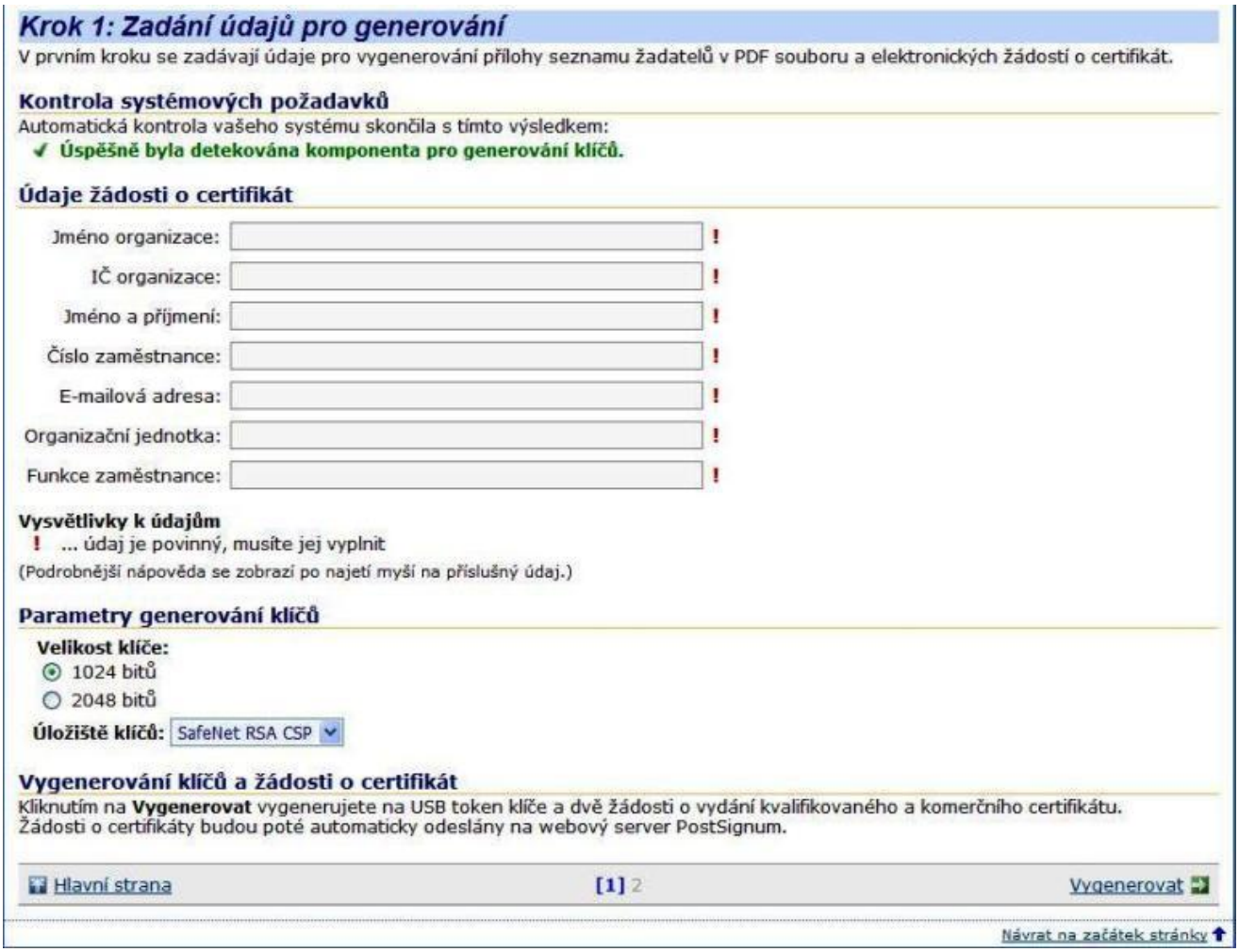
Důležité upozornění:

Po zadání Unblocking PINu (PUKu) již tento použitý PUK nelze znovu použít. Pokud vyčerpáme všechny Unblocking PINy, nelze již token odblokovat, ale pouze znovu inicializovat. Při inicializaci tokenu ale dochází ke ztrátě dat uložených v tokenu.

Po dokončení inicializace jsou všechna data smazána a token je dostupný pouze přes PIN.

Po inicializaci tokenu musíme s jeho pomocí vygenerovat dvojici klíčů a elektronickou žádost o certifikát.

- připojíme token k počítači
- přihlásíme se na základní webovou stránku projektu http://qca.postsignum.cz/projects/czechpoint/
- z odkazu Vygenerování klíčů a žádosti o certifikát si otevřeme formulář, který vyplníme a odešleme tlačítkem *Vygenerovat*



2.3 Vydání certifikátů kontaktním místem České pošty

Po odeslání žádosti si můžeme vyzvednout na kontaktním místě České pošty certifikáty. Budeme potřebovat dvě poštovní certifikační poukázky pro vydání kvalifikovaného a komerčního certifikátu zdarma. Tyto poukázky dostal úřad spolu s tokeny.

Na kontaktní místo České pošty si vezmeme občanský průkaz k prokázání naší totožnosti.

Pracovník kontaktního místa

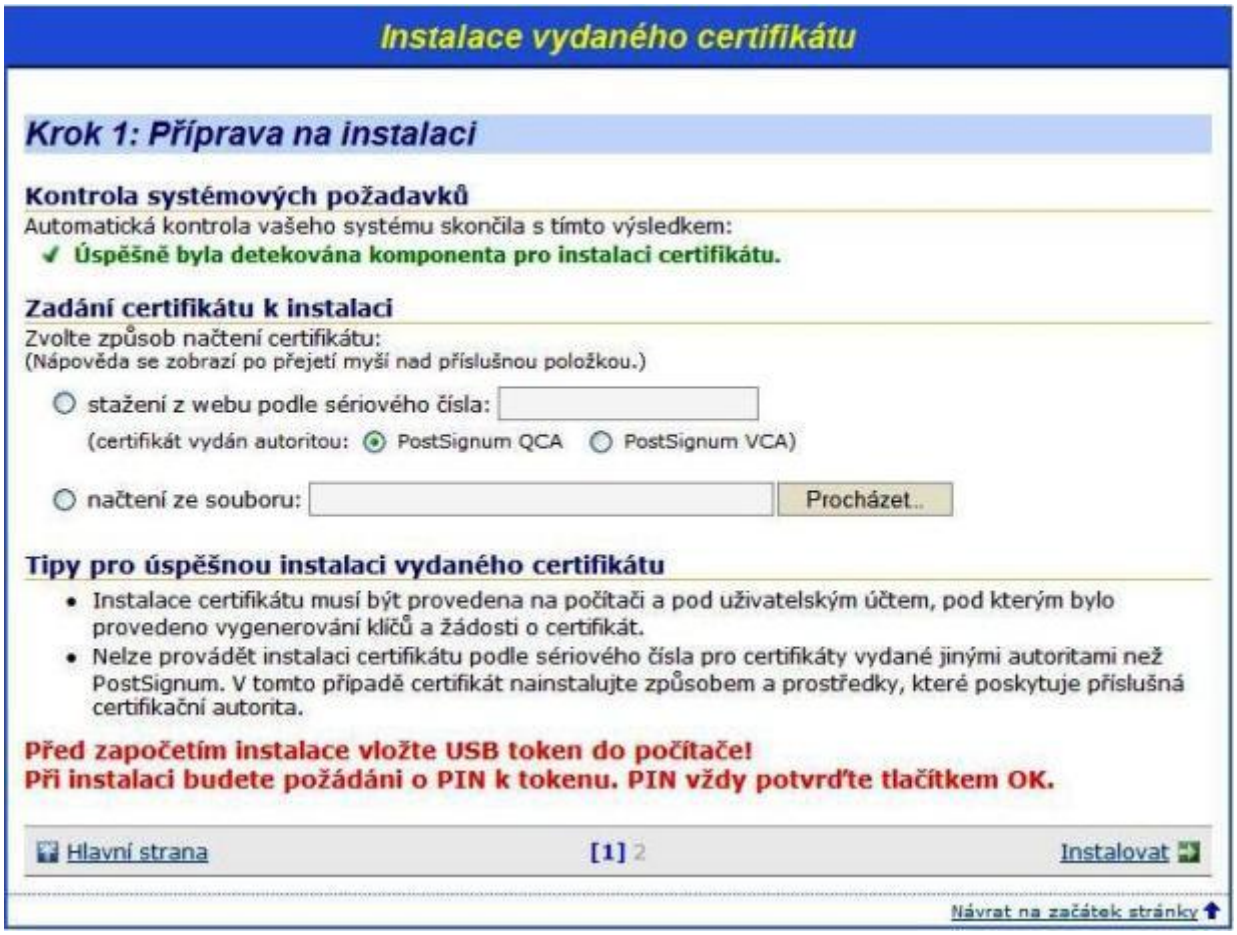
- si zkopíruje náš průkaz totožnosti a ponechá si obě poukázky
- ze stránek PostSignum si stáhne naši žádost o vydání certifikátů, vytiskne ji a předloží nám ji k podpisu
- certifikáty nám nahraje na přinesený nosič (USB flash, disketa), ale NE PŘÍMO NA TOKEN
- případně nám předá číslo, pod kterým si certifikáty stáhneme z webu

O vydání certifikátu se sepíše protokol.

2.4 Instalace vydaných certifikátů na USB token

1. Token připojíme k počítači
    1. pokud jsme si nechali vydat certifikát formou stažení z webu, připojíme se opět na stránku PostSignum a klikneme na odkaz Instalace vydaných certifikátů

Poklepáním na odkaz se nám otevře formulář, ve kterém označíme možnost **stažení z webu podle sériového čísla,** vyplníme číslo, které jsme dostali na kontaktním místě České pošty a klepneme na tlačítko *Instalovat.*



2. Pokud jsme si nechali certifikáty uložit na nějaký nosič, zaškrtneme možnost **načtení ze souboru**. Instalace proběhne po kliknutí na tlačítko *Instalovat.*

Na konci instalace se nám zobrazí dialogové okno s hlášením.

Před prvním přihlášením musí ještě náš správce zapsat čísla našich certifikátů do našeho uživatelského profilu a můžeme se přihlásit k Czech POINTu. Při přihlašování na stránce https://www.czechpoint.cz se nás systém zeptá na certifikát. Volbu potvrdíme OK.

Pomocí svého tokenu, uživatelského jména a hesla se můžeme k Czech POINTu připojit z každého počítače, který má nainstalovaný uživatelský software k USB tokenu.

2.5 Modelový postup, vzory smluv

Univerzální postup zřízení certifikátů pro přístup do Czech POINT včetně

- odkazů na elektronický objednávkový systém
- vzoru objednávky poskytování služeb certifikační autority
- vzorů dodatků ke smlouvě
- vzorů příloh ke smlouvě

je popsán v manuáluvydaném Českou poštou.

3 Obecně o certifikátech

Certifikáty:

- Řeší problém správy, distribuce a uchování klíčů, jsou obdobou průkazu totožnosti
- Vydává je certifikační autorita

Certifikáty obsahují:

- Jméno a další údaje zajišťující jednoznačnou identifikaci subjektu, kterému byl certifikát vydán
- Datum počátku platnosti
- Datum ukončení platnosti
- Jméno certifikační autority
- Sériové číslo

Struktura certifikátu:

- Určení podle které verze normy X.509 byl certifikát vydán
- Číslo certifikátu
- Užité algoritmy k podpisu certifikátu (např. hashovaní funkce SHA-1, RSA)
- Jména vystavitele a vlastníka
- Platnost certifikátu
- Určení pro jaký algoritmus byl veřejný klíč vytvořen, vlastní hodnoty klíče
- Rozšíření certifikátu
- Identifikátory klíče CA

- Identifikátor politiky, podle které byl certifikát vydán
- Podpis CA

4 Kryptografie neboli šifrování

Rozeznáváme dvě základní **metody** kryptografie - **symetrickou a asymetrickou**.

Symetrická - stejný šifrovací klíč je na straně příjemce i odesilatele.

- Obecné schéma symetrické kryptografie
- Bezpečná komunikace s využitím elektronického podpisu a šifrováním zprávy symetrickou šifrou

Asymetrická - používá dva klíče, (asymetrické algoritmy RSA, DSA)

1. **soukromý klíč** - osobní vlastnictví
2. **veřejný klíč** – umožňuje dešifraci (zpráva není zašifrována v plném slova smyslu, je pouze autorizovaná (nepopiratelná) – princip elektronického podpisu

U asymetrické kryptografie mohou nastat **následující procesy**:

- Přenos neadresované, nezašifrované, ale autorizované zprávy
- Přenos adresované, zašifrované, ale neautorizované zprávy
- Přenos adresované, zašifrované a autorizované zprávy
- Bezpečná komunikace s využitím elektronického podpisu

5 Souhrn

V tomto modulu jsme si vysvětlili, **jaké certifikáty** používáme pro **zabezpečený přenos dat** při práci s Czech POINTem. Zmínili jsme se o:

- **komerčním** certifikátu
- **kvalifikovaném** certifikátu
- **USB tokenu**

Také jsme si zjednodušeně vysvětlili postup získávání a oživení certifikátu a uvedli jsme si, **kde najdeme podrobné informace** o celém postupu.

MODUL: CZECH POINT - ADMINISTRATIVNÍ BEZPEČNOST A SPRÁVNÍ POPLATKY (eGON)

Po prostudování modulu bude studující seznámen s ochranou informací, režimovou bezpečnosti spisové agendy a zabezpečením pracoviště při práci s agendami Czech POINT.

Dále získá povědomí o systémem správních poplatků a jeho aplikaci při pořizování ověřených výpisů a podání prostřednictvím portálu Czech POINT. Bude znát výši správních poplatků za jednotlivé úkony, možnosti jejich snížení, příp. osvobození od poplatků.

Seznámení se Zákonem č. 634/2004 Sb., o správních poplatcích a jeho aplikaci v podmínkách Czech POINT.

1 Úvod do studia administrativní bezpečnosti a správních poplatků

V tomto modulu se budeme zabývat **dvěma oblastmi**

1. **ochranou informací**, režimovou bezpečností a zabezpečením pracoviště Czech POINT
2. legislativou určující **správní poplatky**, jejich výší za jednotlivé činnosti a možnostmi snížení, případně odpuštění správních poplatků

Pod ikonou Soubory ke stažení najdete doplňující materiály ke studiu tohoto modulu.

Na úvodní straně celého kurzu si můžete v části Materiály ke kurzu stáhnout seznam rychlých kontaktů
pro práci s portálem Czech POINT.

2 Ochrana informací

Základním hlediskem pro ochranu citlivých informací a osobních údajů je práce s personálem, který v rámci svých pracovních povinností má přístup k informačnímu systému Czech POINT (dále jen informační systém).

Žádná dále uvedená opatření nejsou dostatečně účinná v případě nedbalosti nebo zlého úmyslu. Jedině kombinace těchto opatření a důsledné kontroly ze strany nadřízeného mohou rizika snížit.

Přehled opatření k ochraně informací:

- režimová bezpečnost
- bezpečnost technických prostředků
- bezpečnost programových prostředků
- bezpečnost dat
- bezpečnost komunikačních cest
- fyzická bezpečnost

Aktivní ochrana proti úniku informací - kontroly pracovníků a prostředí.

Žádné opatření není samo o sobě dostatečným řešením, pokud není kombinováno s dalšími a jejich dodržování je dostatečně objasněno a kontrolováno.

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 Kontroly pracovníků a prostředí

Důležité jsou průběžné kontroly dodržování bezpečnostních předpisů pracovníky. Kontroly se týkají jednak nakládání s informacemi a jednak dodržování bezpečnostních opatření v provozu pracoviště.

Vždy má existovat někdo, kdo má přehled o práci konkrétního pracovníka a kdo posoudí korektnost jeho jednání. Pracovník si musí být vědom, že jeho **práce** je i **zpětně dohledatelná** a všechny **provedené kroky** jsou **zaznamenány**.

Kontrola je **dvojsměrná** - ze strany **nadřízeného** a ze strany **poskytovatele dat**.

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 Správní poplatky

Definice:

Správní poplatek je povinná nenávratná platba plynoucí do veřejných rozpočtů, za níž má poplatník nárok na ekvivalentní protiplnění ze strany správního orgánu, mající jednorázový a nahodilý charakter. V praxi to znamená, že okamžikem zaplacení poplatku správní orgán provede určitý úkon. Předmětem správního poplatku je správní řízení upravené zvláštním právním předpisem a další činnost správního úřadu související s výkonem státní správy prováděné orgány moci výkonné České republiky a orgány územních samosprávných celků a orgány právnických osob, pokud vykonávají působnost v oblasti státní správy.

V části vyhrazené správním poplatkům se budeme věnovat

- Sazebníku správních poplatků a platné legislativě
- Poskytování údajů z informačních systémů veřejné správy
- Vybírání správních poplatků

7.1 Sazebník správních poplatků od roku 2006

- Zákonem **č. 81/2006 Sb.**, bylo **do sazebníku zákona č. 634/2004 Sb., o správních poplatcích**, ve znění pozdějších předpisů, **doplněno do položky 3 nové písmeno d)** „Vydání ověřeného výstupu z informačního systému veřejné správy ve výši Kč 50 za každou i započatou stránku“.
- další **novela zákonem č. 269/2007 Sb.**, zvýšila tento poplatek na Kč 100 za první a Kč 50 za každou další vydávanou stránku od 1.1.2008
- Tento správní poplatek **vybírají** obecní úřady obcí s rozšířenou působností a obecní úřady, úřady městských částí nebo městských obvodů územně členěných statutárních měst a úřady městských částí hlavního města Prahy, a dalších, jejichž seznam stanoví vyhláška Ministerstva vnitra č. 550/2006 Sb.

7.2 Vydávání ověřených výstupů z informačních systémů veřejné správy

- Ověřené výstupy musí splňovat náležitosti **ustanovení § 9, § 9a až §9d** o vydávání ověřených výstupů z informačních systémů veřejné správy **zákona č. 365/2000 Sb., o informačních systémech veřejné správy** a o změně některých dalších zákonů, ve znění pozdějších předpisů.

- Podle **položky 3 písmeno a)** platného sazebníku zákona o správních poplatcích, se zpoplatňuje i nadále vydání stejnopisu, opisu, kopie, fotokopie nebo výpisu z úředních spisů, ze soukromých spisů v úřední úschově, z rejstříků, z registrů, z knih, ze záznamů, z evidencí, z listin nebo z dalšího písemného a obrazového materiálu, popřípadě sdělení o negativním nálezu. Výše poplatku za každou i započatou stránku v případě jejího pořízení na tiskárně počítače činí i nadále 15 Kč.

7.3 Platná právní úprava

1. **zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů**

   Vydávání ověřených výstupů z informačních systémů veřejné správy § 9, § 9a až § 9d

2. **Zákon č. 634/2004 Sb., o správních poplatcích**

   sazebník správních poplatků položka 3 písm. d) a položka 10

3. **zákon č. 344/1992 Sb., o katastru nemovitostí České republiky (katastrální zákon)**

   část sedmá Poskytování údajů z katastru

4. **zákon č. 513/1990 Sb., obchodní zákoník**

   hlava III Obchodní rejstřík

5. **zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon)**

   hlava IV Živnostenský rejstřík

6. **zákona č. 269/1994 Sb., o Rejstříku trestů**

   část druhá OPIS A VÝPIS Z EVIDENCE REJSTŘÍKU TRESTŮ

7.4 Poskytování údajů z informačních systémů veřejné správy

Poskytování údajů z informačních systémů veřejné správy tedy upravuje následující legislativa:

- **zákon č. 365/2000 Sb**., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- **novela zákon č. 269/2007 Sb.,** od 1.1.2008

Vydávání ověřených výstupů z informačních systémů veřejné správy upravuje

- **§ 9 a následně § 9a až § 9d zákona č. 365/2000 Sb.**

7.5 Kontaktní místa veřejné správy

§ 8a zákona č. 365/2000 Sb.

§ 8a odst. 1

(1) Podání správním orgánům lze činit v rozsahu a za podmínek stanovených jinými právními předpisy prostřednictvím kontaktního místa veřejné správy (Českého podacího ověřovacího informačního národního terminálu – Czech POINT).

(2) **§ 8a odst. 2 zákona č. 365/2000 Sb.**

a. notáři,
b. krajské úřady,
c. matriční úřady,
d. obecní úřady, úřady městských částí nebo městských obvodů územně členěných statutárních měst a úřady městských částí hlavního města Prahy, jejichž seznam stanoví prováděcí právní předpis,
e. zastupitelské úřady stanovené prováděcím právním předpisem,
f. držitel poštovní licence[1] a Hospodářská komora České republiky.

7.6 Zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů

SPRÁVNÍ POPLATEK = DAŇ

- Správní poplatky jsou zařazeny pod legislativní zkratku „daň“ uvedenou v § 1 odst. 1 zákona č. 337/1992 Sb., o správě daní a poplatků.
- Při jejich správě se postupuje podle zákona o správních poplatcích a podpůrně dle zákona o správě daní a poplatků.

SPRÁVCE POPLATKU = SPRÁVCE DANĚ

7.7 Vybírání správních poplatků

Správní úřady vybírají správní poplatky za výstupy z ISVS a z Rejstříku trestů

- podle **položky 3 písmeno d)** a
- **položky 10 písmeno a)** sazebníku zákona č. 634/2004 Sb., o správních poplatcích ve znění **zákona č. 269/2007 Sb., od 1.1. 2008**

[1] Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů.

Podle **položky 3 písm. d)** sazebníku vybírají správní úřady za ověřené výstupy - **z katastru nemovitostí** (zákon č. 344/1992 Sb., o katastru nemovitostí České republiky (katastrální zákon)) (srovnej výpis z KN položka 119 pro KÚ) - **z živnostenského rejstříku** (pozor ještě nově vybírají i za ohlášení živnosti podle položky 24 (od 1.7. 2008 zákon č.130/2008 Sb., živnostenský) - **z obchodního rejstříku** (zákon č. 513/1991 Sb., obchodní zákoník)

Pro srovnání:

položka 3 **písm. a)** sazebníku, podle které vydávají všichni správci rejstříků, registrů atp.

a) Vydání stejnopisu, opisu, kopie, fotokopie nebo výpisu z úředních spisů, ze soukromých spisů v úřední úschově, z rejstříků, z registrů, z knih, ze záznamů, z evidencí, z listin nebo z dalšího písemného a obrazového materiálu, popřípadě sdělení o negativním nálezu

7.7.1 Položka 3 písm. a)

Podle položky 3 písm. a) se vybírá správní poplatek

- Kč 50 za každou i započatou stránku
- Kč 40 na přinesené disketě
- Kč 80 na přineseném CD nebo ZIP

Kč 15 za každou i započatou stránku, je-li pořizována na kopírovacím stroji nebo na tiskárně počítače

7.7.2 Položka 3 písm. d)

Správní poplatky za vydání ověřeného výstupu z ISVS řeší **Položka 3 písm. d)**

d) Vydání ověřeného výstupu z informačního systému veřejné správy

100 Kč za první stránku

50 Kč za každou další i započatou stránku

(Kč 50 za každou stránku bylo podle zákon č. 81/2006 Sb., od 1.1. 2007 do 31.12. 2007)

Poznámky:

Bod 2. Každou započatou stránkou se pro účely tohoto zákona rozumí vydaná stránka formátu A4 a menší.

7.7.3 Zmocnění

Správní úřad může snížit poplatek za vydání ověřeného výstupu z informačního systému veřejné správy až o 90% z částky podle písmene d) této položky.

(zákon č. 269 /2007 Sb., od 1.1.2008)

7.8 Správní poplatky u Rejstříku trestů

Vydání výpisu z Rejstříku trestu je upraveno zákonem č.269/1994 Sb., o rejstříku trestů, ve znění pozdějších předpisů V § 11a zákona o Rejstříku trestů se odkazuje co do místa podání žádosti na zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, výsledkem je však vydání výpisu ve smyslu zákona o Rejstříku trestů. Z tohoto důvodu není možné, aby se vydání výpisu z Rejstříku trestů dostalo do režimu položky 3 písm. d) sazebníku zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů. Podle písm. a) položky 10 sazebníku je předmětem správního poplatku pouze přijetí žádosti o vydání výpisu z evidence Rejstříku trestů.

Položka 10

a) Přijetí žádosti o vydání výpisu z evidence Rejstříku trestů Kč 50

Poznámka

Za přijetí žádosti o vydání výpisu z evidence Rejstříku trestů u českého zastupitelského úřadu, vybírá poplatek český zastupitelský úřad podle položky 162 tohoto sazebníku. Byl-li výpis z evidence Rejstříku trestů vydán kontaktním místem veřejné správy, vybírá správní poplatek stanovený v písmenu a) této položky kontaktní místo veřejné správy. Správní poplatek je jeho příjmem.

8 Souhrn

V modulu jsme probrali problematiku **administrativní bezpečnosti** a **správních poplatků**.

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.

U správních poplatků jsem si uvedli platné zákony upravující výběr poplatků.

9 Informační zdroje

Správní poplatky:

- Správní poplatky za výstupy z ISVS
- Poskytování údajů z ISVS