1. Požadavky na pracovní stanice

1.1 Přístup k IISSP

Převážná část uživatelů přistupuje k IISSP prostřednictvím portálu. Jedná se o uživatele systému z kapitol, OSS a jiných organizací. Pro portálový přístup uživatelé využívají webového klienta.

1.2 Požadavky na hardware PC

Klíčové požadavky na HW jsou uvedeny pro doporučení platformy OS Windows. Pro jiné platformy OS se mohou požadavky na HW lišit.

1.2.1 Minimální konfigurace

Verze operačního systému	**Windows 2000**	**Windows XP** **Windows 2003 Server**	**Windows Vista** **Windows 2008 Server** **Windows 7** **Windows 8**
Rychlost procesoru	1 GHz	1,5 GHz	1,5 GHz
Velikost operační paměť RAM	512 MB	512 MB	1 GB
Velikost diskového prostoru	300 MB		
Rozlišení obrazovky	1024 x 768		

Tabulka 1 - Minimální konfigurace PC uživatele

1.2.2 Doporučená konfigurace PC

Doporučená konfigurace PC pro práci v prostředí s IISSP je následující

Verze operačního systému	**Windows 2000**	**Windows XP** **Windows 2003 Server**	**Windows Vista** **Windows 2008 Server** **Windows 7** **Windows 8**
Rychlost procesoru	1,5 GHz	2 GHz	2 GHz
Velikost operační paměť RAM	1 GB	1 GB	1,5 GB
Velikost diskového prostoru	500 MB		
Rozlišení obrazovky	1280 x 1024		

Tabulka 2 - Doporučená konfigurace PC uživatele

Minimální požadované CPU by měly odpovídat modelům a vyšším, např. dle benchmarku http://www.cpubenchmark.net/low_end_cpus.html

- 1 GHz Intel Celeron 1000MHz
- 1,5 GHz Intel Celeron 420 @ 1.60GHz
- 2 GHz Intel Core2 Duo E4400 @ 2.00GHz

1.3 Požadavky na software

1.3.1 Portálový přístup

1.3.1.1 Přístupová adresa

- Portálový přístup k aplikacím IISSP

  https://portal.statnipokladna.cz

- Webová stránka s detailními informacemi o řešení IISSP RIS na webu Ministerstva Financí

  http://www.statnipokladna.cz

1.3.1.2 Zabezpečení

Pro přístup koncových uživatelů k portálu IISSP je využíván standardní protokol HTTPS. Pro zajištění této zabezpečené komunikace jsou na straně serverů využívány certifikáty vydané společnostmi *„GeoTrust“* pro Portál IISSP (centrální místo pro přihlášení do IISSP) a *„PostSignum“* pro ostatní rozhraní pro koncové uživatele. Pro správné ověření platnosti těchto certifikátů je nutné mít v PC instalované kořenové certifikáty PostSignum:

- Kořenová certifikační autorita PostSignum Root QCA 2
- Komerční certifikační autorita PostSignum Public CA 2

*Poznámka: Rozhraní webových služeb jsou zabezpečeny certifikáty vydanými **První certifikační autoritou (I.CA)**. Systémy konzumující webové služby IISSP musí důvěřovat certifikátům této autority.*

Kořenové certifikáty GeoTrust i PostSignum jsou součástí operačních systémů Windows v rámci programu „Microsoft Root Certificate Program.” Pokud nejsou kořenové certifikáty PostSignum již v PC instalovány, je možné spustit jejich instalaci z následujícího odkazu:

http://www.postsignum.cz/files/CA_postsignum.exe

V případě manuální instalace kořenových certifikátů PostSignum (je vyžadována také pro Mozilla Firefox) je před potvrzením důvěryhodnosti kořenového certifikátu nutné ověřit kontrolní otisky pro každý z instalovaných certifikátů podle webových stránek autority:

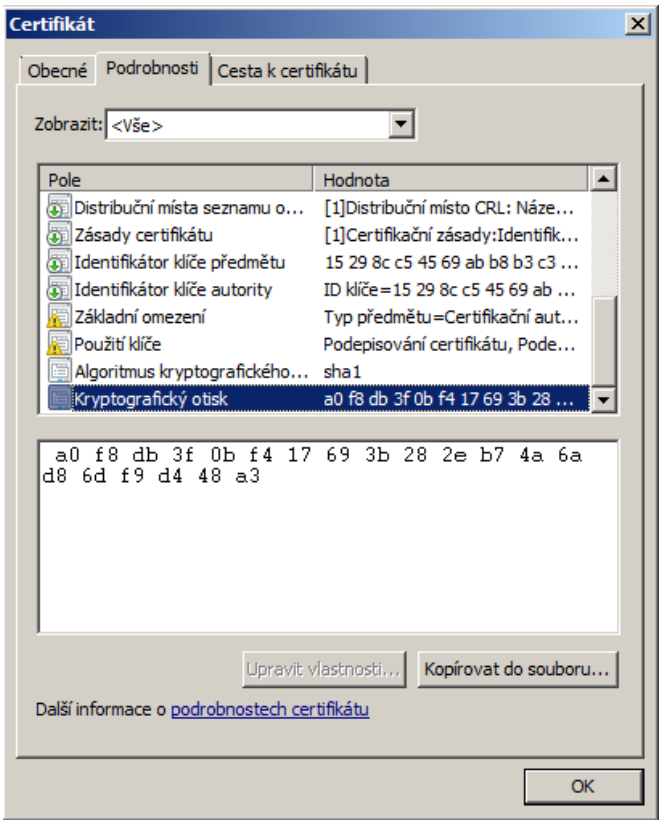
Kořenová certifikační autorita PostSignum Root QCA 2

http://www.postsignum.cz/certifikaty_autorit.html?step=2#RQCA2

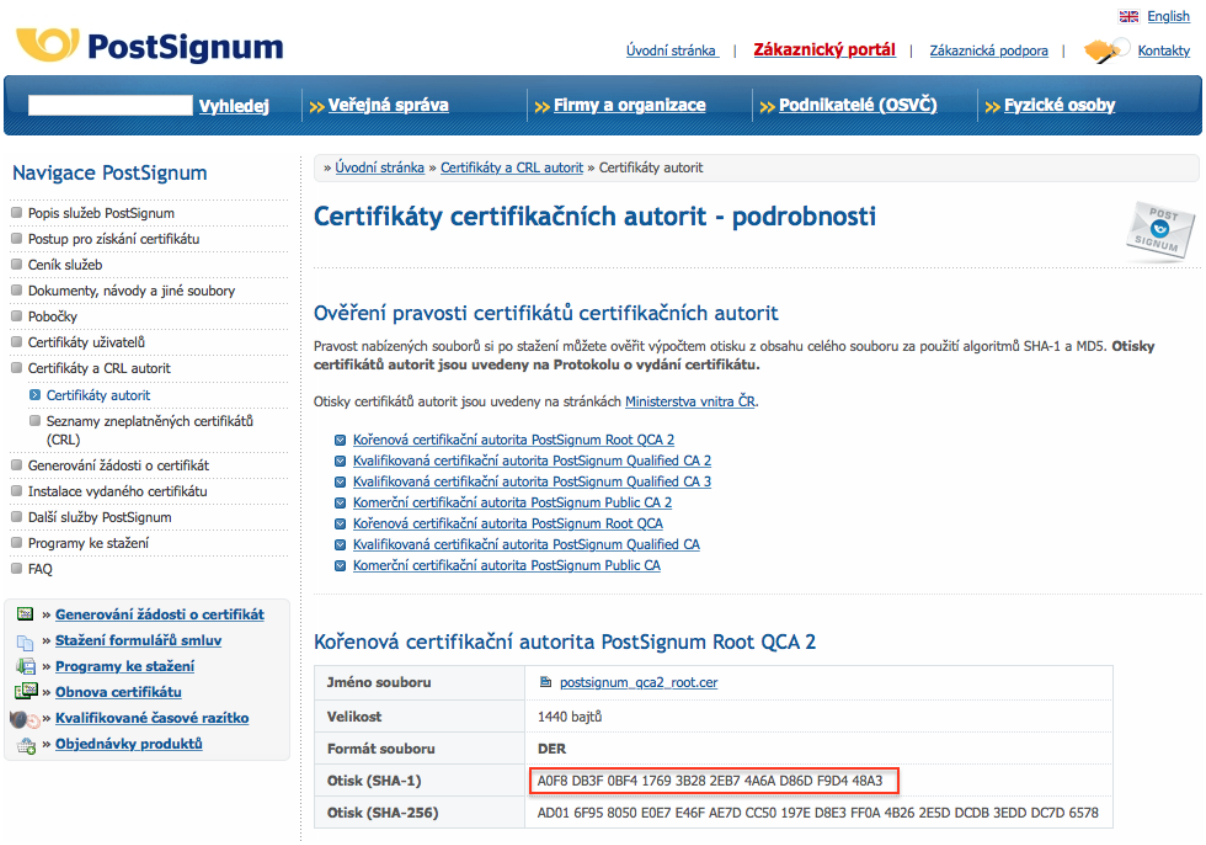
Komerční certifikační autorita PostSignum Public CA 2

http://www.postsignum.cz/certifikaty_autorit.html?step=2#VCA2

Kontrolní otisk (sha1) ve vlastnostech certifikátu musí být stejný, jako kontrolní otisk daného certifikátu na webu certifikační autority (viz. výše uvedené odkazy):



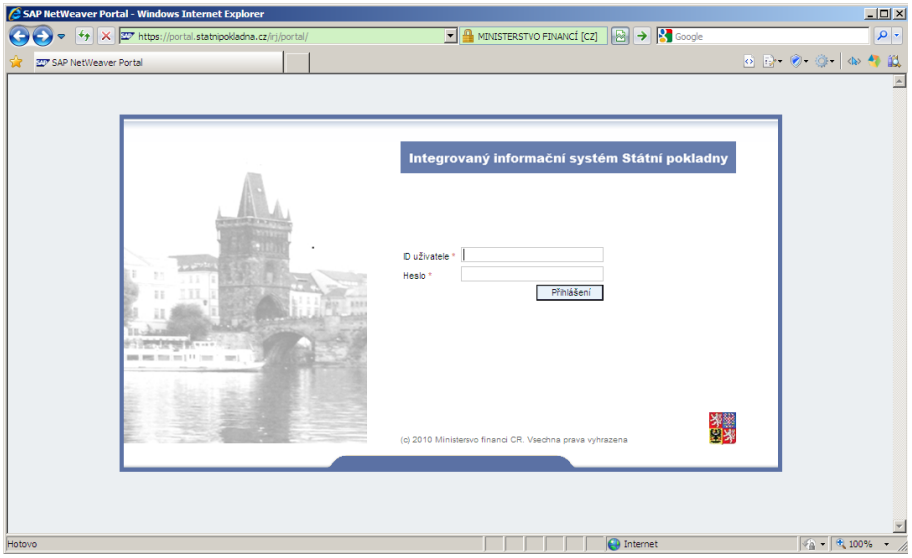
Obrázek 1 – Vlastnosti certifikátu – Kryptografický otisk



Obrázek 2 - Kořenový certifikát certifikační autority PostSignum

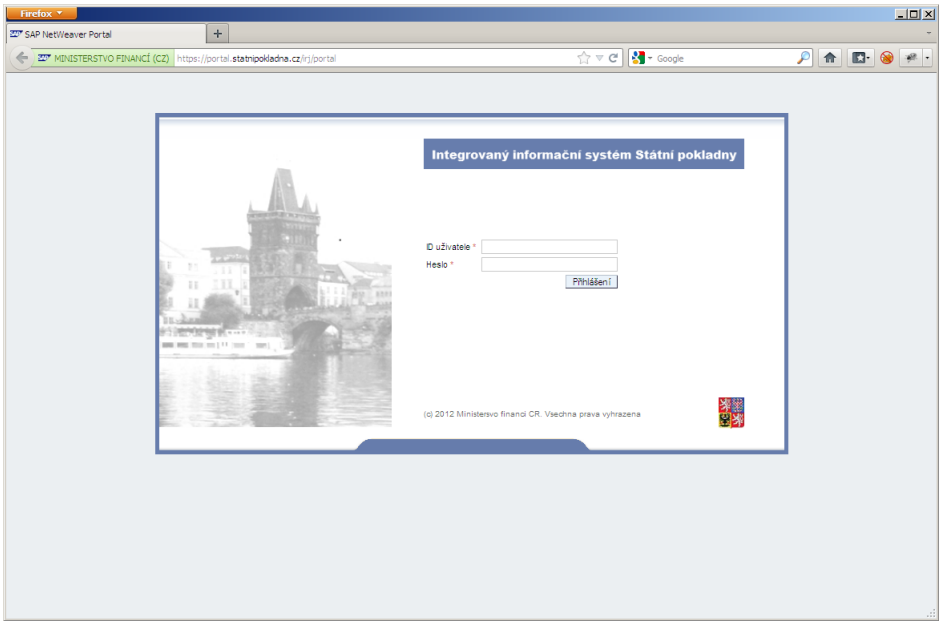
Certifikát s rozšířenou validací

Pro vyšší úroveň zabezpečení a poskytnutí vyšší úrovně záruky toho, že uživatel přistupuje ke skutečnému Portálu IISSP, jsou přihlašovací stránka a Portál IISSP chráněny certifikátem s rozšířenou validací. To umožňuje uživateli snadno si ověřit, že přistupuje opravdu do IISSP a komunikuje se správným serverem. K využití této možnosti je nutné přistupovat podporovaným prohlížečem s doporučeným nastavením (viz následující podkapitola). Korektní přístup a ověření certifikátu s rozšířenou validací na přihlašovací stránce IISSP je indikováno **zeleně podbarveným adresním řádkem a zobrazením názvu organizace „MINISTERSTVO FINANCÍ [CZ]"** v případě použití Internet Exploreru verze 7 a vyšší:



Obrázek 3 - Přihlašovací stránka Portálu IISSP - Internet Explorer

V podporovaném prohlížeči Mozilla Firefox se zobrazuje **zeleným textem název Organizace MINISTERSTVO FINANCÍ (CZ)**, nebo se tentýž název organizace zobrazuje v zeleně podbarveném poli:



Obrázek 4 - Přihlašovací stránka Portálu IISSP - Firefox

Upozornění:

Neuvidíte-li adresní řádek zeleně nebo v poli se zámečkem název organizace MINISTERSTVO FINANCÍ (CZ) nezadávejte prosím přihlašovací informace a kontaktujte pracovníka podpory IT ve vaší organizaci nebo servicedesk IISSP.

1.3.1.3 Web prohlížeč

Jsou podporovány internetové prohlížeče **Internet Explorer (IE) verze 9, 10 a 11**.

Volitelně je možné využít prohlížeč **Mozilla Firefox ESR** na platformě Widows XP SP3 - Windows 7, avšak zde může za určitých okolností docházet k odlišnostem oproti IE8 projevujících se nestandardním chováním aplikace IISSP.

Z pohledu aplikační kompatibility a současně zajištění splnění aktuálních požadavků na bezpečnost komunikace s aplikacemi IISSP je jako standardní prohlížeč doporučený **Internet Explorer verze 9 nebo 10** na platformě Windows 7 - Windows 8 s posledními aktualizacemi prohlížeče i operačního systému.

Organizace a uživatelé používající MSIE 11 varujeme, že zvolili internetový prohlížeč, který nerespektuje direktivu autocomplete="off" u pole input type="password", která brání lokálnímu ukládání hesla na pracovní stanici uživatele. Bez ohledu na to, že IISSP tuto bezpečnostně správnou direktivu používá, prokázaly naše testy, že MSIE 11 na pracovní stanici uživatele, který zmíněný internetový prohlížeč používá, ukládá přihlašovací jméno i heslo uživatele do IISSP. Uživatelé s touto verzí internetového prohlížeče proto musí velmi pečlivě dbát na udržování bezpečnosti klientského operačního systému a programů, které v něm pracují (včetně inkriminovaného internetového prohlížeče). Uživatelům MSIE z bezpečnostních důvodů doporučujeme, aby tuto bezpečnostně nevhodnou vlastnost internetového prohlížeče vypnuli a aby pomocí Správce pověření (je dostupný přes Ovládací panely) zkontrolovali již uložená hesla a dále aby v případě, že mezi uloženými hesly bude uvedené heslo do IISSP, toto heslo ze své pracovní stanice odstranili.

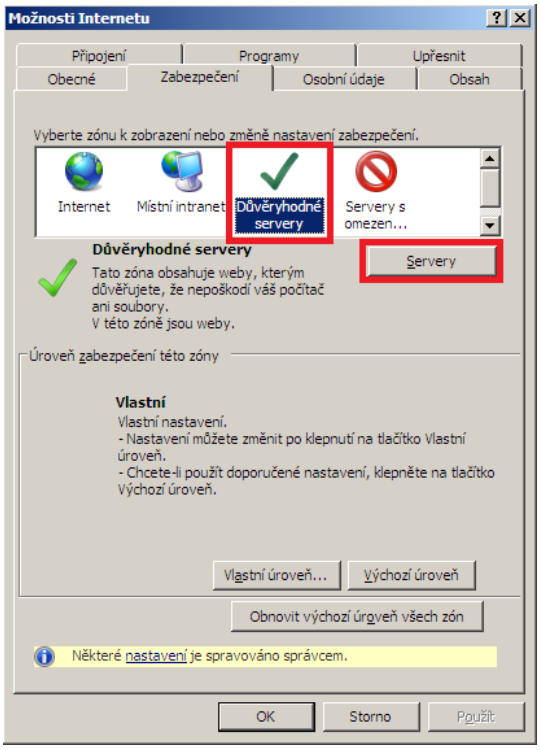
Z hlediska dodržení základních bezpečnostních pravidel je vždy nutné příslušný web prohlížeč na daném operačním systému zabezpečit podle vydaných oprav, eventuálně dodatečných rozšíření v podobě rozšiřujících modulů (zásuvný modul/plugin).

Obecné webového prohlížeče společné pro portálové aplikace IISSP RIS:

- povolení pop-up oken
- povolit stahování souborů bez upozornění (pouze v IE)

Specifické nastavení webového prohlížeče IE:

- nastavení automatického otevírání pop-up oken:
  menu *Nástroje / Možnosti Internetu – záložka Obecné – sekce Záložky (Změnit zobrazení webových stránek na záložkách)* stlačit tlačítko *Nastavení – sekce "Při zjištění automaticky otevíraného okna"* vybrat volbu: *"Aplikace Internet Explorer určí jak se budou otevírat automaticky otevíraná okna"*
- nastavení zóny Důvěryhodné servery (pouze v IE) – menu *Nástroje / Možnosti Internetu – záložka Zabezpečení – tlačítko Servery* - přidání https://*.statnipokladna.cz do seznamu důvěryhodných serverů:



Obrázek 5 - Nastavení IE - důvěryhodné servery

- nastavení stahování souborů bez upozornění:
  menu *Nástroje / Možnosti Internetu – záložka Zabezpečení – Důvěryhodné servery* – tlačítko *Vlastní úroveň – Stažení – Stažení souboru – Povolit*
- nastavení zobrazování okna s Certifikáty: menu *Nástroje / Nastavení / Zabezpečení - Vlastní úroveň - Nastavení - Nezobrazovat výzvu k výběru klientského certifikátu*, jestliže je k dispozici jeden nebo žádný certifikát - *Zakázat*
- nastavení režimu kompatibilního zobrazení: po zadání odkazu pro přístup k IISSP stiskem ikonky pro kompatibilní zobrazení dojde k přidání této stránky do seznamu.

Obrázek 6 - Nastavení IE - kompatibilní zobrazení

Specifické nastavení webového prohlížeče Firefox (v menu Nástroje → možnosti):

- Na záložce *Obecné* zvolit *„U každého souboru se dotázat, kam ho uložit“*
- Na záložce *Obsah* nezaškrtnuto *„Blokovat vyskakovací okna“*
- Na záložce *Aplikace* pro *Typ obsahu „List aplikace Microsoft Excel“* zvolit *Akci „Použít Microsoft Office Excel“.* Pozor, je třeba nastavit novou aplikaci Microsof Office Excel (jinou než je standardně nabízená Microsoft Office Excel (výchozí)) – ve sloupci *„Akce“* vybrat položku *„Použít jinou“* poté zvolit *„Procházet“* najít a vybrat soubor *excel.exe* (například *C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE*).

1.3.1.4 Java

Pro využití některých funkcionalit na portálu (například export dat do souboru v rámci WebGUI, spouštění certifikovaného Java appletu pro vytvoření digitálního podpisu) a z bezpečnostních důvodů je nutné, aby byla na pracovní stanici pravidelně aktualizována Java Runtime Environment.

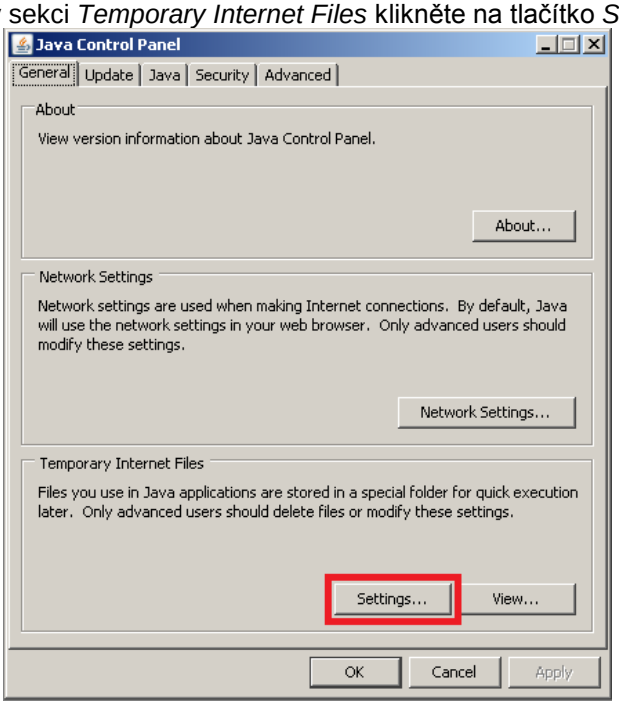
Další informace o nejnovějším instalačním balíčku naleznete na stránce:

http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html

Java applet pro vytvoření digitálního podpisu může v určitých situacích vykazovat dlouhé odezvy a digitální podpis není možné vytvořit. V takovém případě je nutné provést smazání dočasných souborů a operaci zopakovat.

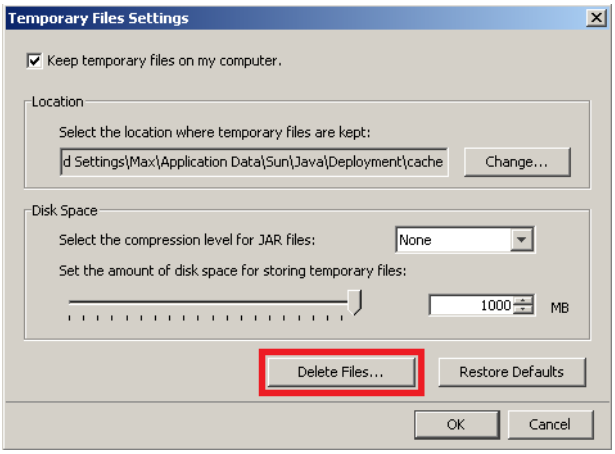
Postup mazání dočasných souborů:

- pomocí tlačítka *Start* a volby *Ovládací panely* otevřete okno s programy na nastavení počítače
- vyhledejte ikonu  s popisem Java a dvojklikem spusťte ovládací program pro nastavení Javy
- na záložce *General* v sekci *Temporary Internet Files* klikněte na tlačítko *Settings*



Obrázek 7 - Nastavení Java - ovládací panel

- v otevřeném dialogovém okně klikněte na tlačítko *Delete Files…*



Obrázek 8 - Nastavení Java - dočasné soubory

1.3.1.5 MS Excel

Pro možnost přípravy rozpisu rozpočtu off-line je požadována verze MS Excel: MS Office 2003 a výše.

Aby se z prohlížeče exportované XLS soubory korektně otevíraly v aplikaci MS Excel, je třeba nastavit MS Windows podle Microsoft support článku 162059, následovně:

Konfigurace aplikace Internet Explorer pro otevírání souborů sady Office v příslušné aplikaci sady Office pomocí nástroje Možnosti složky:

1. Otevřete složku Tento počítač.
2. V nabídce Nástroje (nebo v nabídce Zobrazit) klepněte na příkaz Možnosti složky (nebo příkaz Možnosti).
3. Klepněte na kartu Typy souborů.
4. V seznamu Registrované typy souborů klepněte na daný typ dokumentu - List aplikace Microsoft Excel a poté klepněte na tlačítko Upřesnit (nebo na tlačítko Upravit).
5. V dialogovém okně Upravit typ souboru zrušte zaškrtnutí políčka K procházení používat jen jedno okno (nebo políčka Otevírat webové dokumenty přímo).
6. Klepněte na tlačítko OK.

Detailní informace jsou uvedeny zde:

http://support.microsoft.com/kb/162059/cs

1.3.2 Bezpečnostní doporučení na údržbu a obsluh u hardwarového a softwarového vybavení pracovní stanice

1.3.2.1 Základní doporučení

Doporučuje se, aby uživatel IISSP:

- prováděl pravidelné aktualizace bezpečnostních oprav operačního systému a internetového prohlížeče,
- věnoval zvýšenou pozornost při příjmu e-mailů s přílohou. Příloha je velmi často prostředkem pro šíření škodlivého software,
- neprováděl instalaci programů a souborů z nedůvěryhodných zdrojů (jedná se zejména o amatérské produkty). Tyto programy bývají často spojeny se škodlivým software (viry, trojské koně, spyware ...) který může ohrozit bezpečnost dat uložených na počítači nebo bezpečnost systémů, ke kterým se počítač připojuje,
- nastavil pracovní stanici tak, že bude po definovaném čase vypnuta nebo zamknuta, aby se předešlo přístupu neoprávněných osob. Doporučený automatický časový interval pro zamčení stanice je 10 minut,
- vypnul pracovní stanici nebo zamknul obrazovku pracovní stanice, pokud se od ní vzdaluje.

1.3.2.2 Ochrana klientských stanic proti škodlivým kódům.

Na ochranu proti škodlivým programům doporučujeme na klientských stanicích uživatelů IISSP implementovat opatření na jejich prevenci, detekci a nápravu, s nastavenou automatickou aktualizací. Při detekci narušení musí být spuštěn proces pro jeho odstranění a po dobu, kdy je koncová stanice infikována nesmí být použita pro práci v systému IISSP.

1.3.2.3 Bezpečnostní pravidla pro práci s internetovým prohlížečem

Doporučuje se, aby uživatel IISSP:

- zakázal ukládání hesel v prohlížeči (např. nastavení v MS Internet Exploreru: Nástroje/Možnosti Internetu/Obsah/Osobní informace - Automatické dokončování, políčko "Uživatelská jména a hesla na formulářích" musí zůstat nezaškrtnuté),
- ověřoval platnost serverových certifikátů,
- nastavil v prohlížeči možnost upozornění na neplatné serverové certifikáty,
- nastavil v prohlížeči možnost upozornění na přechod ze zabezpečené do nezabezpečené oblasti.

V internetovém prohlížeči Internet Exploreru 8 lze výše zmíněné kontroly nastavit na záložce Nástroje/Možnosti Internetu/Obsah/Osobní informace - Automatické dokončování (políčko "Uživatelská jména a hesla na formulářích" musí zůstat nezaškrtnuté) a na záložce Nástroje/Možnosti Internetu/Zabezpečení.

1.3.2.4 Ochrana proti phishingu

Phishingový útok slouží k podvodnému získání a zneužití přihlašovacích údajů. Útočníci obvykle zasílají podvržené e-mailové zprávy, které se jeví jako pocházející od legitimního odesilatele s platnými adresami odesílatele, odkazy a značkami. Takové e-maily většinou obsahují hypertextový odkaz na podvrženou webovou stránku a požadují od uživatelů, aby vložili údaje týkající se zabezpečení pod záminkou, že je třeba tyto údaje aktualizovat nebo změnit. Jestliže uživatel vloží údaje o svém zabezpečení, může dojít k neoprávněné činnosti v aplikaci IISSP s přihlašovacími údaji tohoto uživatele.

Doporučuje se, aby uživatel IISSP:

- zkontroloval digitální podpis e-mailu z IISSP,
- ověřil e-maily z IISSP, které obsahují požadavek na okamžitou reakci, jinak údajně hrozí vznik škody nebo postihu,
- ověřil v dokumentaci systému e-maily IISSP, které obsahují odkaz na stránky IISSP,
- zadával adresy v internetovém prohlížeči manuálně, nikoliv prokliknutím přímo z e-mailu.

1.3.2.5 Ochrana proti clickjackingu

Při útoku, kterému se říká clickjacking (viz: http://cs.wikipedia.org/wiki/Clickjacking) je použita webová stránka s na první pohled neškodným obsahem – např. vtipné obrázky a vedle nich odkazy na další stránky obrázků. Do této stránky je vložen rám s cílovou stránkou, která je ale pro uživatele neviditelná

Pokud uživatel klikne na odkaz, který má vést na další stránku s obrázky, ve skutečnosti kliká na vložený rám. Tím na cílové stránce útoku provede útočníkem zamýšlenou akci, aniž by o tom věděl.

Doporučuje se, aby uživatel IISSP:

- před tím, než se přihlásí k IISSP, uzavřel všechna jiná okna nebo panely internetových prohlížečů, kromě webových stránek s prokazatelně důvěryhodným obsahem nezbytných pro vykonávání dané pracovní činnosti (např. webové stránky intranet aplikací),
- během práce s IISSP neotevíral jiná okna nebo panely internetových prohlížečů, kromě webových stránek s prokazatelně důvěryhodným obsahem nezbytných pro vykonávání dané pracovní činnosti (např. webové stránky intranet aplikací),
- po ukončení práce s IISSP se uživatel odhlásil a zavřel okno internetového prohlížeče.

Doporučený internetový prohlížeč, který obsahuje ochranu proti clickjackingu je Microsoft Internet Explorer verze 8, alternativně Mozilla Firefox verze 10 ESR.

1.3.2.6 Pravidla pro práci více uživatelů na jednom počítači

V případě, že jednu pracovní stanici sdílí více osob, měl by uživatel IISSP RISRE dodržovat následující pravidla:

- při každém zahájení práce na pracovní stanici se přihlásit pod svým uživatelským jménem do operačního systému,
- při každém ukončení práce na pracovní stanici se odhlásit jako uživatel z operačního systému, případně pracovní stanici vypnout,
- spořič obrazovky, který si nastaví, musí být chráněn heslem,
- pracovní stanice by měla být nastavena tak, že pro opětovné spuštění po uspání nebo hibernaci, bude vyžadovat heslo uživatele do operačního systému.