Integrovaný informační systém Státní pokladny (IISSP)

Technický manuál

Příručka administrátora

Historie dokumentu

Historie revizí

Číslo revize	Datum revize	Sumarizace změn	Změny označeny
1.0	15. 5. 2020	Finální verze dokumentu	Ne
2.0	9. 6. 2020	Finální verze dokumentu	Ne
3.0	11. 8. 2020	Finální verze dokumentu	Ne
4.0	3. 3. 2021	Finální verze dokumentu	Ne
5.0	9. 3. 2021	Finální verze dokumentu	Ne
6.0	8. 12. 2021	Finální verze dokumentu	Ne
7.0	3. 2. 2022	Finální verze dokumentu	Ne
8.0	5. 5. 2022	Finální verze dokumentu	Ne
9.0	5. 10. 2022	Finální verze dokumentu	Ne
10.0	19. 4. 2023	Finální verze dokumentu	Ne
11.0	15. 12. 2023	Finální verze dokumentu	Ne
12.0	5. 8. 2024	Finální verze dokumentu	Ne
13.0	17. 9. 2024	Finální verze dokumentu	Ne
14.0	3. 3. 2026	Finální verze dokumentu	Ne

Platnost dokumentu

Tento dokument je platný od:

- 3. 3. 2026.

Obsah

Seznam tabulek:

Seznam obrázků:

1. Účel dokumentu

1.1 Rozsah

Tento dokument popisuje základní pravidla, principy a postupy spojené s přístupem koncových uživatelů prostřednictvím uživatelských rozhraní IISSP.

1.2 Definice pojmů a zkratek

Vysvětlení zkratek použitých v dokumentu:

Zkratka	Vysvětlení
CSUIS	Centrální systém účetních informací státu
EKIS	Ekonomický informační systém
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
HW	Hardware
IISSP	Integrovaný informační systém Státní pokladny
MF	Ministerstvo financí
OS	Operační systém
OSS	Organizační složka státu
PC	Personal computer
PO	Pověřená osoba
RIS	Rozpočtový informační systém
RISPR	Rozpočtový informační systém příprava rozpočtu
RISRE	Rozpočtový informační systém realizace rozpočtu
RF	Registrační formulář
SSL	Secure Sockets Layer
TLS	Trasport Layer Security
URL	Uniform Resource Locator
ZO/NZO	Zodpovědná osoba, resp. Náhradní zodpovědná osoba zasílá výkazy účetní jednotky do CSÚIS

Vysvětlení pojmů použitých v dokumentu:

Pojem	Vysvětlení
Uživatelská dokumentace	Uživatelskou dokumentací se pro účely tohoto dokumentu rozumí dokumentace koncového uživatele, školicí materiály, novinky v aplikaci, otázky a odpovědi, případně další dokumenty určené pro uživatele IISSP. Uživatelská dokumentace je součástí Provozní dokumentace.
Provozní dokumentace	Veškerá dokumentace, informace a znalosti shromážděné a sdílené během implementace a produktivního provozu IISSP.
Incident	SD hlášení „Porucha“ nebo „Incident“, které upozorňuje na stav systému, kdy není možné vykonávat aktivity v IISSP dle **Provozní dokumentace IISSP** a tento stav systému není možné opravit běžným zásahem pracovníka podpory dle **Provozní dokumentace IISSP**.
Produktivní prostředí IISSP	Prostředí IISSP přístupné uživatelům IISSP. Jedná se o soubor technických komponent, které zajišťují podporu procesů zpracovávaných v IISSP.
Prostředí pro testování 3. stran	Prostředí IISSP s omezenou funkcionalitou pro testování aplikací externích subjektů a spolupracujících organizací. Toto prostředí je organizačně, technicky i datově odděleno od Produktivního prostředí IISSP.
Centrální správa uživatelů IISSP	Soubor procesů, které zajišťují správu a řízení životního cyklu uživatelských účtů v rámci IISSP.

2. Technické parametry přístupu k IISSP

2.1 Požadavky na hardware PC

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

2.1.1 Minimální konfigurace PC

Tabulka 1 - Minimální konfigurace PC uživatele

Verze operačního systému	Windows 10, Windows 11
Rychlost procesoru	1,5 GHz
Velikost operační paměť RAM	4 GB RAM
Velikost diskového prostoru	500 MB
Rozlišení obrazovky	1440 x 900

2.1.2 Doporučená konfigurace PC

Tabulka 2 - Doporučená konfigurace PC uživatele

Verze operačního systému	Windows 10, Windows 11
Rychlost procesoru	2 GHz
Velikost operační paměť RAM	8 GB RAM
Velikost diskového prostoru	1000 MB
Rozlišení obrazovky	1920 x 1080

Doporučované konfigurace vychází z požadavků, které pro konkrétní sestavy uvádí výrobce HW nebo výrobce OS (v daném případě Microsoft). Podporovány jsou pouze 64-bitové verze OS Windows 10 a Windows 11.

Pro přístup prostřednictvím portálového rozhraní IISSP není nutné zvláštní HW nebo infrastrukturní vybavení nad rámec těchto doporučení.

2.2 Požadavky na software

2.2.1 Portálový přístup

Přístupové adresy:

- portálový přístup k aplikacím IISSP:
  - https://portal.statnipokladna.cms2.cz
- portálový přístup pro předávání výkazů:
  - https://portalcsuis.statnipokladna.gov.cz
- webová stránka s detailními informacemi o řešení IISSP na webu Ministerstva financí:
  - http://www.statnipokladna.gov.cz

2.2.2 Zabezpečení

V rámci IISSP jsou nyní provozovány následující webové stránky:

- Produktivní prostředí IISSP:
  - Uživatelské rozhraní:
    - portal.statnipokladna.cms2.cz,
    - portal2.statnipokladna.cms2.cz,

        - portal5.statnipokladna.cms2.cz,
        - portalcsuis.statnipokladna.gov.cz,
        - downloads.statnipokladna.cms2.cz,
        - downloads.statnipokladna.gov.cz,
    - Rozhraní webových služeb:
        - portal3.statnipokladna.cms2.cz,
        - portal3.statnipokladna.gov.cz,
- Prostředí pro Testování 3. stran (T3S):
    - Uživatelské rozhraní:
        - t3sportal.statnipokladna.gov.cz,
    - Rozhraní webových služeb:
        - t3sportal3.statnipokladna.cms2.cz,
        - t3sportal3.statnipokladna.gov.cz.

Poznámky a upozornění:

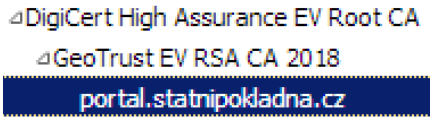
- Tyto odkazy jsou platné okamžikem platnosti dokumentu.
- Pro potřeby testování budou služby v prostředí Testování 3. stran zpřístupněny s předstihem. Pro služby dostupné v doméně cms2.cz budou s předstihem zpřístupněny statické stránky pro ověření jejich dostupnosti z prostředí přistupujících organizací.
- Služby dostupné v doméně gov.cz budou nadále veřejně dostupné z prostředí Internetu. **Služby dostupné v doméně cms2.cz budou dostupné pouze v prostředí Komunikační infrastruktury veřejné správy**.
- Testování 3. stran je dostupné nadále v doméně gov.cz pro zajištění dostupnosti testovacích rozhraní pro komerční společnosti vyvíjející informační systémy.
- Používejte odkazy uvedené výše. Odkazy uvedené v jednotlivých obrázcích tohoto dokumentu jsou pouze ilustrativní a po převedení služeb IISSP na nové domény nebudou nadále platit.
- Pro podrobnější informace sledujte prosím dokumentaci a novinky na stránkách www.statnipokladna.gov.cz.

2.2.2.1 Produktivní prostředí IISSP

Pro přístup koncových uživatelů k Portálu IISSP je využíván standardní protokol HTTPS. Pro zajištění zabezpečené komunikace je na straně serverů využíván multi-doménový SSL certifikát (SAN) s rozšířenou validací od vydavatele GeoTrust (DigiCert).

Pro správné ověření platnosti certifikátu je nutné mít v PC instalované kořenové certifikáty vydavatele (v prostředí Microsoft Windows jsou tyto certifikáty standardní součástí distribuce OS, resp. jeho patchů).

Nasazený certifikát je vydán v následující struktuře:



Podrobnosti k root certifikátům a jejich veřejné části jsou ke stažení zde:

DigiCert High Assurance EV Root CA

https://dl.cacerts.digicert.com/DigiCertHighAssuranceEVRootCA.crt.pem

https://dl.cacerts.digicert.com/DigiCertHighAssuranceEVRootCA.crt

DigiCert High Assurance EV Root CA Download PEM | Download DER/CRT	Valid until: 10/Nov/2031 Serial #: 02:AC:5C:26:6A:0B:40:9B:8F:0B:79:F2:AE:46:25:77 SHA1 Fingerprint: 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25 SHA256 Fingerprint: 74:31:E5:F4:C3:C1:CE:46:90:77:4F:0B:61:E0:54:40:88:3B:A9:A0:1E:D0:0B:A6:AB:D7:80:6E:D3:B1:18:CF Demo Sites for Root: Active Certificate expired revoked

GeoTrust EV RSA CA 2018

https://dl.cacerts.digicert.com/GeoTrustEVRSACA2018.crt.pem

https://dl.cacerts.digicert.com/GeoTrustEVRSACA2018.crt

GeoTrust EV RSA CA 2018 Download PEM | Download DER/CRT	Issuer: DigiCert High Assurance EV Root CA Valid until: 06/Nov/2027 Serial #: 03:FE:EF:1B:B5:B6:48:34:9A:20:95:0F:8B:C6:97:53 SHA1 Fingerprint: A3:99:04:64:17:B6:7E:32:0D:3E:FA:69:D7:DC:E6:B8:BF:E8:A9:F2 SHA256 Fingerprint: 18:5C:0A:E4:70:42:3B:9D:46:78:A7:C1:05:5B:5B:48:D9:07:05:50:5B:79:4E:21:5C:06:38:51:33:69:81:F4

2.2.2.2 Prostředí pro Testování 3. stran

Prostředí pro Testování 3. stran je testovacím prostředím pro přistupující organizace nebo pro externí subjekty, které zajišťují provoz a rozvoj informačních systémů přistupujících organizací.

Pro přístup k prostředí T3S je využíván standardní protokol HTTPS. Pro zajištění zabezpečené komunikace je na straně serverů využíván multi-doménový SSL certifikát (SAN) s rozšířenou validací od vydavatele GeoTrust (DigiCert).

Pro správné ověření platnosti certifikátu je nutné mít v PC instalované kořenové certifikáty vydavatele (v prostředí Microsoft Windows jsou tyto certifikáty standardní součástí distribuce OS, resp. jeho patchů).

Detail k certifikátu i kořenovým certifikátům vydavatele jsou shodné s certifikáty produkčního prostředí, které jsou popsány v kapitole 2.2.2.1 Produktivní prostředí IISSP.

2.2.3 Certifikát s rozšířenou validací

Pro vyšší úroveň zabezpečení a poskytnutí vyšší úrovně záruky toho, že uživatel přistupuje ke skutečnému Portálu IISSP, jsou portály 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 ikonou zamčeného zámku:

Obrázek 1 – Identifikace stránky zajištěné certifikátem s rozšířenou validací

Upozornění:

Neuvidíte-li ikonku zamčeného zámku nebo uvidíte ikonu odemčeného zámku, nezadávejte prosím přihlašovací informace a kontaktujte pracovníka podpory IT ve vaší organizaci nebo ServiceDesk IISSP.

2.2.4 Web prohlížeč

Pro přístup k IISSP je podporován internetový prohlížeč MS Edge, optimálně v poslední uvolněné verzi. Prohlížeče Chrome a Firefox nejsou testovány v plném rozsahu funkcionalit IISSP a nemůžeme tedy garantovat všechny funkčnosti aplikace.

Upozornění:

Podporované verze prohlížečů nerespektují 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 tyto prohlížeče na pracovní stanici uživatele ukládají přihlašovací jméno i heslo uživatele do IISSP. Uživatelé proto musí velmi pečlivě dbát na udržování bezpečnosti klientského operačního systému a programů, které v něm pracují (včetně inkriminovaného internetového prohlížeče). Uživatelům z bezpečnostních důvodů doporučujeme, aby tuto bezpečnostně nevhodnou vlastnost internetového prohlížeče vypnuli a již uložené přístupové údaje ze své pracovní stanice odstranili:

- *Pro Microsoft Edge:*

  Přizpůsobit a ovládat / Nastavení / Automatické vyplňování, políčko " Nabídnout uložení hesel" musí zůstat nezaškrtnuté.

  Výmaz se provede pomocí: Další akce / Odstranit.

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).

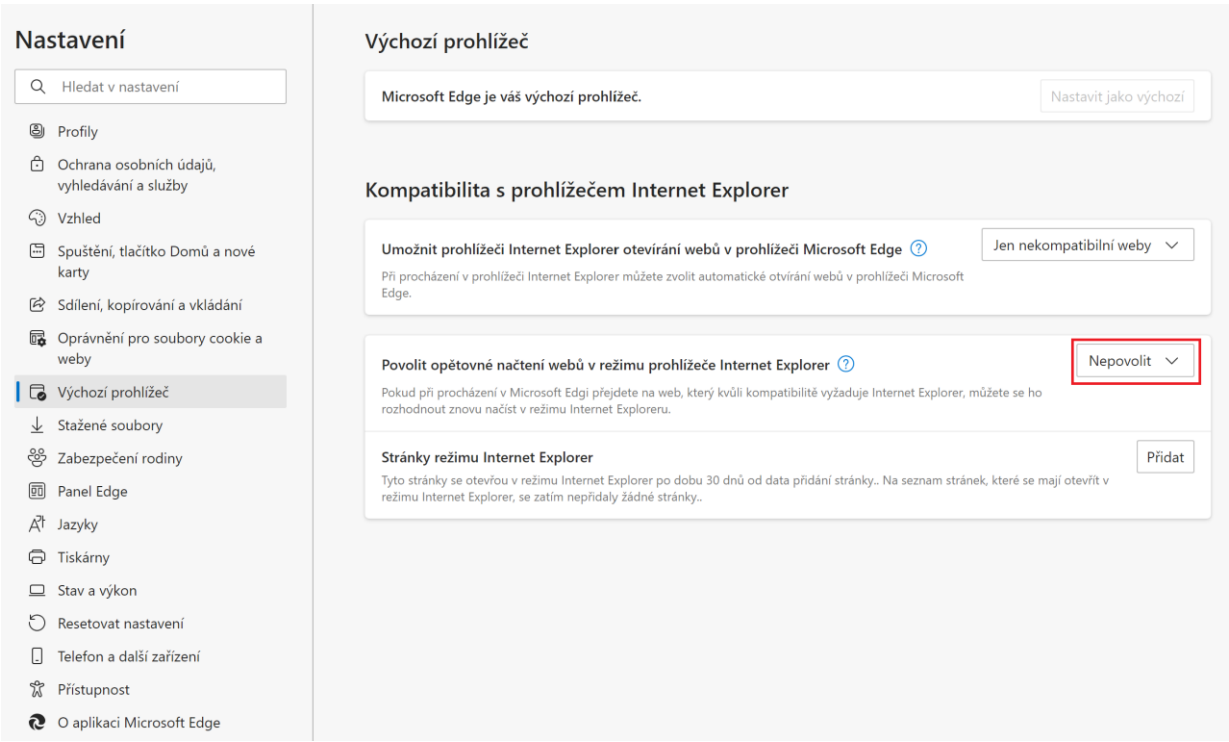
Upozornění:

Na základě ověření z praxe upozorňujeme, že historicky odkazy uložené v prohlížeči mezi Oblíbené nemusí být funkční. Doporučujeme proto, aby se uživatelé ujistili, že uložené odkazy v prohlížeči obsahují pouze řetězec https://portal.statnipokladna.cms2.cz.

Nastavení prohlížeče Microsoft Edge

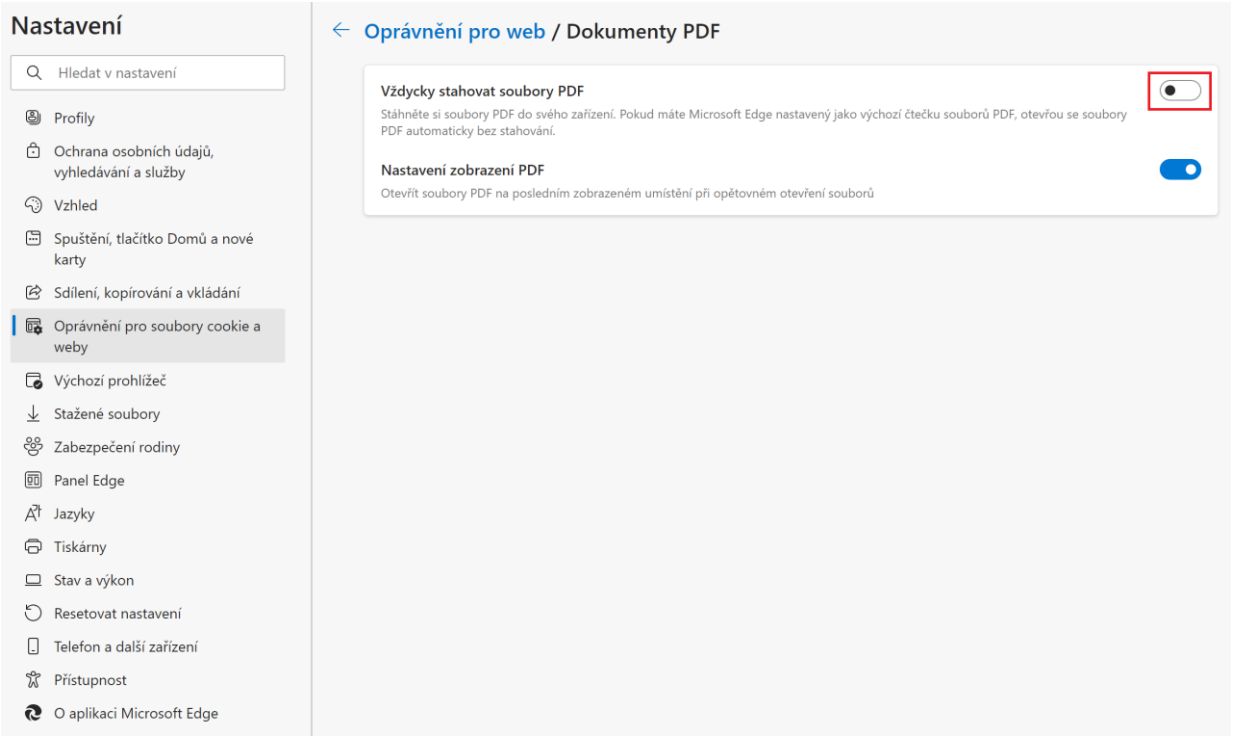
Specifická nastavení webového prohlížeče Microsoft Edge:

- Microsoft Edge nesmí běžet v Microsoft Internet Explorer módu (parametr “Enable IE Integration”).



Obrázek 2 – Nastavení parametru kompatibility prohlížeče

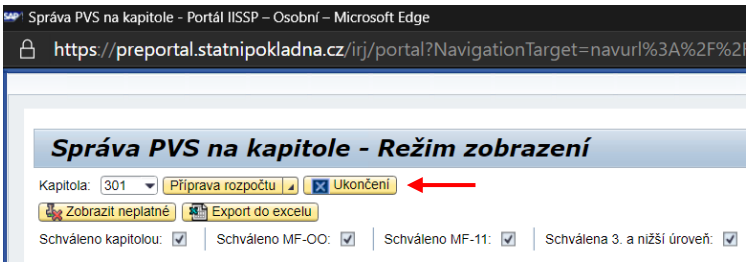
- Pro správné zobrazení PDF souborů (např. Přílohy č. 4 v RISPR) je nutné, aby byla v prohlížeči povolena interní čtečka PDF.



Obrázek 3 – Nastavení parametru interní čtečky PDF

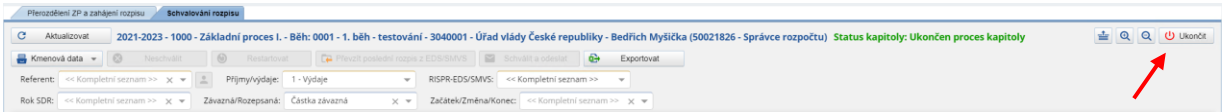
- Stahované RF (obecně jakýkoliv interaktivní PDF formulář) je nutné ukládat pomocí kontextového menu. Uložit je pomocí volby Uložit jako a následně je otevřít v Adobe Readeru. Interní čtečka MS Edge / Chrome neumí interaktivní PDF formulář zobrazit.
- Uživatelům IISSP doporučujeme uzavírat aplikace **<u>výhradně</u>** pomocí tlačítek „Ukončit“ uvnitř aplikace, nikoliv uzavírání okna aplikací křížkem v pravém horním rohu okna aplikace. Tlačítko „Ukončit“ se nachází jak ve všech hlavních aplikacích IISSP (např. v aplikacích pro správu kmenových dat RISPR, ve formulářích hlavního procesu RISPR atd.) – viz následující příklady:

1) Aplikace **Správa PVS na kapitole**:



Obrázek 4 – Správa PVS na kapitole – tlačítko „Ukončení“

2) Formulář hlavního procesu **Přerozdělení ZP a schvalování OSS**:



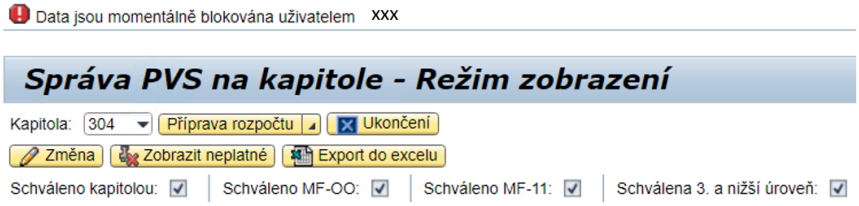
Obrázek 5 – Formulář Přerozdělení ZP a schvalování OSS – tlačítko „Ukončit“

Aby docházelo v prohlížeči **Microsoft Edge** ke správnému ukončení aplikací a k uvolnění aplikačních zámků i při zavření celého okna aplikace křížkem v pravém horním rohu okna aplikace, je potřeba mít v prohlížeči nastaven parametr FetchKeepaliveDurationSecondsOnShutdown. Bez nastavení tohoto parametru nebo s hodnotou „0“ sekund se prohlížeč okamžitě zavře, aniž by bylo zaručeno odeslání nevyřízeného požadavku sendBeacons, který back-end aplikace potřebuje k uzavření relací. Výrobce specifikuje přípustné hodnoty „1“ až „5“ sekund, doporučujeme nastavit hodnotu na 2 sekundy.

Aby nebylo nutné nastavit popsané parametry individuálně každému uživateli IISSP, doporučujeme nastavit tyto parametry administrátorským zásahem prostřednictví doménových GPO.

Více informací k nastavení naleznete zde: https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#fetchkeepalivedurationsecondsonshutdown

Pokud uživatel nebude mít nastaven tento parametr v prohlížeči Microsoft Edge, uzavře aplikaci pouze křížkem okna a znovu spustí stejnou aplikaci či formulář v režimu změny, tak obdrží hlášku, že data jsou momentálně blokována jeho vlastním uživatelem (toto je pak možné řešit pouze administrátorsky prostřednictvím Kompetenčního centra a podpory systému IISSP):



Obrázek 6 – Chybové hlášení – Data jsou momentálně blokována uživatelem xxx

2.2.5 Java

Pro využití aplikace Klient CSÚIS je nutné, aby bylo na pracovní stanici dostupné, resp. pravidelně aktualizované prostředí Java Runtime Environment, konkrétně JAVA OpenJDK verze 13 nebo vyšší. Podrobný popis postupu získání a instalace je popsán v dokumentu Uživatelský manuál – Klient CSÚIS.

2.2.6 ASD WebSigner

Komponenta ASD WebSigner slouží pro vytvoření elektronického podpisu pomocí osobního certifikátu v prostředí web prohlížeče u všech funkcionalit, kde uživatelské rozhraní IISSP tuto funkcionalitu poskytuje. Jedná se zejména o podpis relevantních objektů modulu RISRE.

2.2.6.1 Požadavky na klientskou stanici

Požadavky a postupy používání komponenty ASD WebSigner uvádíme pro platformu OS Windows. Komponenta podporuje i řadu dalších platforem (viz. dále). Požadavky pro jiné platformy se mohou v některých detailech lišit, podrobné informace zde.

Operační systém
Elektronický podpis lze provádět na těchto operačních systémech klienta (uváděny minimální verze):

- MS Windows 10 či novější,
- MS Windows Server 2016 či novější,
- Mac OSX 10.12 či novější,
- Red Hat Enterprise Linux 6 či novější,
- Oracle Linux 7 či novější,
- Ubuntu 14 či novější,
- Debian 8 či novější,
- Fedora 27 či novější,
- CentOS 7 či novější,
- OpenSUSE 15 či novější,
- SUSE Enterprise Linux (SLES) 12 SP2 či novější,

- Alpine Linux 3.7 či novější,
- Android 6 či novější,
- iOS 9 či novější,
- Web prohlížeč.

Webové prohlížeče
Pro provoz komponenty ASD WebSigner jsou podporované prohlížeče uvedené v kapitole 2.2.4 Web prohlížeč.

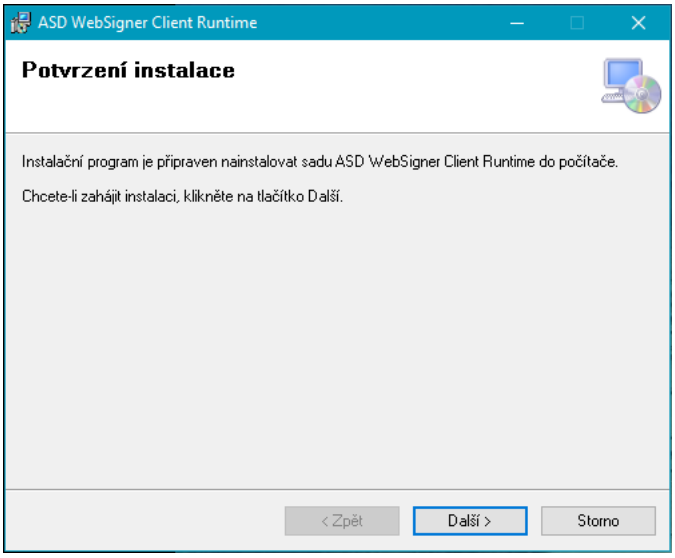
Podpůrný framework (balíček)
Pro provoz komponenty ASD WebSigner musí být v prostředí MS Windows k dispozici instalovaná SW komponenta .NET Framework 4.5 či novější. Pro ostatní podporované operační systémy nejsou specifické komponenty nutné.

2.2.6.2 Návod k instalaci komponenty na klientský počítač

Pro elektronický podpis ve web prohlížeči musí být na klientském počítači nainstalována aplikace ASD WebSigner. Vlastní instalaci provádějte dle následujícího návodu v závislosti na tom, jaký operační systém používáte. Instalace se provádí pouze pro aktuálního uživatele, pro instalaci nejsou v tom případě vyžadována administrátorská oprávnění. V případě, že počítač používá více uživatelů, každý pod svým účtem, tak instalaci musí provést každý uživatel samostatně.

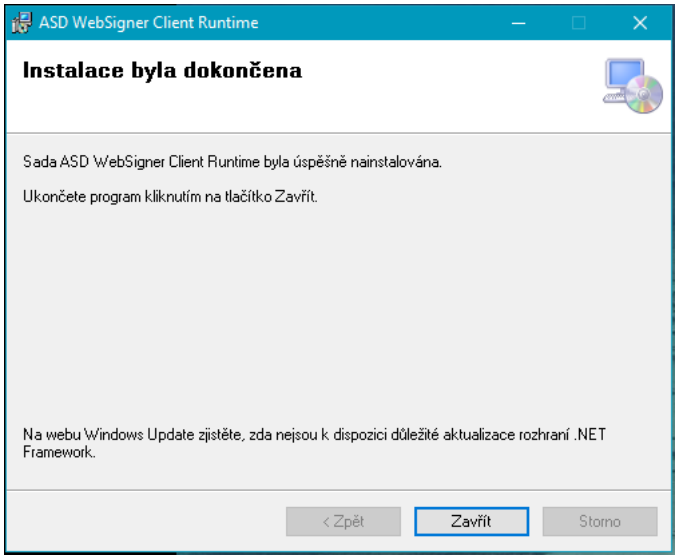
Postup instalace:
Stáhněte si instalační MSI balíček.

- Instalace je dostupná zde. Po stažení na klientskou stanici je instalační balíček uložen na obvyklém místě, ve standardním nastavení v adresáři „Stažené soubory“.
- Spusťte a potvrďte instalaci staženého MSI balíčku.



Obrázek 7 – Spuštění instalace ASD WebSigner

- Aplikace provede kontrolu prostředí klientské stanice a v případě problémů upozorní na problém.
- Instalace proběhne automaticky, o provedení instalace je uživatel informován.



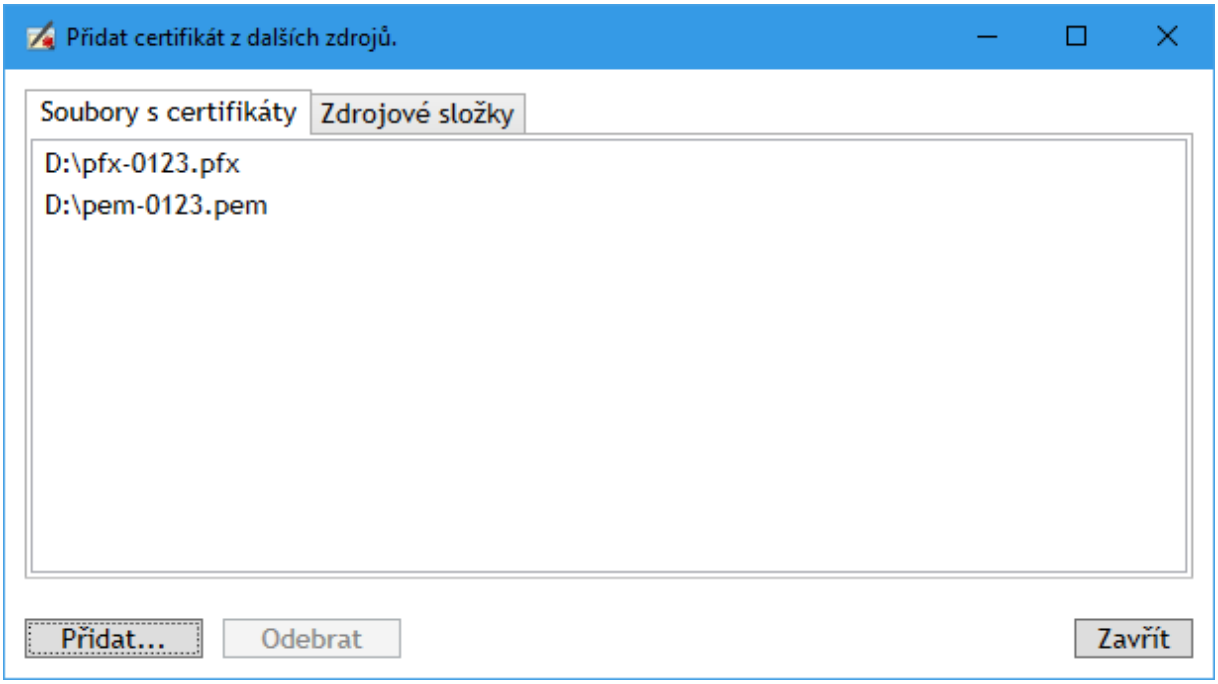
Obrázek 8 – Instalace o dokončení instalace ASD WebSigner

- Aplikace je po instalaci připravená ke spuštění.
- Při prvním použití můžete být web prohlížečem upozorněni na spouštění aplikace. Spuštění je nutno povolit, přičemž další zobrazování upozornění můžete zakázat.
- Pro použití certifikátu je nutné mít připravené technické zařízení s kvalifikovaným zařízením, přístupným klientské stanici.

Instalaci není bezpodmínečně nutné provádět před prvním použitím funkcionality elektronického podpisu, systém při prvním použití zkontroluje dostupnost aplikace na klientské stanici a pokud ji nenalezne, nabídne uživateli instalaci. Pokud ji uživatel povolí, proběhne instalace automaticky (instalační balíček se stáhne přímo z aplikačního serveru IISSP jako součást instalace) stejným způsobem, jaký je popsán výše. Pro tento způsob instalace ale musí mít uživatel alespoň minimální práva opravňující ho k instalaci softwaru (administrátorská práva nejsou nutná).

2.2.6.3 Konfigurace certifikátů pro podpis

Preferovanou a doporučovanou variantou vytvoření elektronického podpisu je použití připojených HW Tokenů / karet napojených na Windows úložiště certifikátů CSP, vydaných jednou z podporovaných certifikačních autorit.
Aplikace ASD WebSigner umožňuje i vytvoření elektronického podpisu certifikátem s privátním klíčem uloženým v souboru typu PFX/p12 nebo PEM. V tom případě je nutné příslušný certifikát přidat kliknutím na ikonu „+“ v sekci „Podepsat osobním certifikátem:“



Obrázek 9 – Registrace certifikátů v aplikaci ASD WebSigner

2.2.6.4 Použití ASD WebSigner pro vytvoření elektronického podpisu

Aplikaci nespouští uživatel, je spuštěna automaticky při vyvolání funkcionality vytvoření elektronického podpisu v uživatelském prostředí portálu IISSP.
Aplikace si hlídá update prostřednictvím serverové komponenty, která je provozovaná v rámci prostředí IISSP a se kterou aplikace komunikuje. Ve výjimečných případech (při velké změně verze aplikace) je nutné provést instalaci nové verze manuálně, o čemž bude Kompetenční centrum informovat s dostatečným předstihem.

2.2.7 Microsoft Excel

Pro možnost přípravy rozpisu rozpočtu off-line je požadována verze Microsoft Excel 2010 a vyšší.

IISSP umožňuje pro zobrazení standardních reportů využívat aktuálně i 64bitovou verzi Microsoft Excel.
Pouze pro použití nástroje BEx Analyzer (Excel Add-In v SAP Business Explorer Suite) v rámci CSÚIS a MIS je možné používat pouze 32bitovou verzi Microsoft Excel (resp. Microsoft Office).

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

Konfigurace aplikace Internet Explorer pro otevírání souborů sady Microsoft Office v příslušné aplikaci sady Microsoft 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.

2.2.8 Automatické rozhraní

V souvislosti s aktualizací komponent IISSP dochází od 22. 3. 2021 ke změně vraceného response asynchronní služby – tento typ komunikace se v rámci IISSP týká pouze rozhraní pro předávání výkazů do CSÚIS. Změna je způsobena standardním chováním nové verze komponenty, která zajišťuje zprostředkování komunikace mezi klientskou aplikací a backend systémem CSUIS. Změna nemá dopad na způsob přístupu a využití uživatelského prostředí prostřednictvím webové aplikace CSÚIS.

Stávající řešení vrací jako odpověď na asynchronní volání HTTP kód „202 Accepted“ a prázdné tělo odpovědi.

Nová komponenta vrací při odpovědi na asynchronní volání HTTP kód „200 OK“, tělo odpovědi obsahuje SOAP obálku (SOAP Envelope) s prázdným elementem SOAP Body

Oba způsoby jsou standardní a validní odpovědí na volání asynchronní služby. Podstatný pro rozhodnutí o úspěšném doručení je návratový kód HTTP 2xx (viz https://www.w3.org/TR/2000/NOTE-SOAP-20000508/#_Toc478383529).

Ukázky odpovědí jsou uvedeny níže (hlavičky se mohou v konkrétních případech lišit, podstatný je HTTP kód a tělo).

Ukázka stávající response (pouze hlavičky, tělo response je prázdné):

```
HTTP/1.1 202 Accepted
Date: Fri, 05 Mar 2021 10:11:40 GMT
Server: SAP NetWeaver Application Server 7.22 / AS Java 7.10
content-length: 0
Via: 1.1 portal5.statnipokladna.cms2.cz
set-cookie: saplb_*=(J2EE7427420)7427450; Version=1; Path=/; HttpOnly;Secure
set-cookie: JSESSIONID=Tq_-
mhxm2qkB6ywtP42Br3wODt8BeAF6VXEA_SAPOswgl_4CtZwMALkVlYTS3k43; Version=1; Path=/;
HttpOnly;Secure
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain
Strict-Transport-Security: max-age=16070400; includeSubDomains
```

Ukázka nové response (hlavičky a tělo):

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server 7.22 / AS Java 7.10
date: Fri, 05 Mar 2021 08:31:45 GMT
content-type: text/xml; charset=utf-8
content-id: <soap-3848e5ea7d8d11ebb82a0000001df812@sap.com>
content-disposition: attachment;filename="soap-
3848e5ea7d8d11ebb82a0000001df812@sap.com.xml"
content-description: SOAP
content-length: 112
set-cookie: saplb_*=(i1tc1t_I1T_00)1964050; Version=1; Path=/
set-cookie: JSESSIONID=Co4EkJEG4gv9pPVQPAixJPYLmYMBeAES-
B0A_SAPc0jvdvKTl3MqB71x1qMgHnLN; Version=1; Path=/
```

```
set-cookie: JSESSIONMARKID=RrYsywDOX-XtsaoFZUBQ014VN2Rxj-AUYaZRL4HQA; Version=1;
Path=/

<SOAP:Envelope
xmlns:SOAP='http://schemas.xmlsoap.org/soap/envelope/'><SOAP:Header/><SOAP:Body/><
/SOAP:Envelope>
```

3. Přístup uživatelů k IISSP

3.1 Pravidla pro registraci OSS / EKIS a oprávněných osob do Centrální správy uživatelů IISSP

Základním předpokladem pro zdárný průběh procesu registrace subjektů a komunikace EKIS s IISSP je existence ujednání mezi MF a příslušnou OSS o přístupu do IISSP. Mimo jiné je v tomto ujednání specifikována role „Pověřené osoby" a zároveň je i uvedeno, která fyzická osoba je touto rolí zmocněna k následujícím úkonům:

- komunikovat za konkrétní OSS, skupinu OSS (například za rozpočtovou kapitolu) nebo kraj s kompetenčním centrem MFČR,
- žádat o registraci uživatele do IISSP nebo změnu jeho atributů, respektive vymazání uživatele,
- žádat o přiřazení veřejného klíče komerčního certifikátu k relevantnímu technickému uživateli, pod kterým se budou EKIS připojovat k IISSP.

Vlastnímu zprovoznění rozhraní mezi EKIS a IISSP je nutné vytvořit na straně IISSP sadu údajů o subjektech přistupujících do IISSP. Údaje jsou rozděleny na dva základní typy:

- Technický uživatel – technický účet v IISSP pro přihlášení EKIS. K technickému účtu jsou připojeny informace o EKIS, včetně jeho certifikátu, kterým se EKIS bude autentizovat během navazování komunikace.
- Oprávněná osoba – fyzický uživatel EKIS s uživatelským účtem v IISSP, který je pověřen přímým pořizováním dat na Portále IISSP nebo jejich odesíláním automatickým rozhraním z EKIS. EKIS je povinen uchovat vazbu „uživatel EKIS – ID uživatelského účtu IISSP“. Při sestavování zprávy určené pro odeslání do IISSP se doplní identifikátor uživatelského účtu IISSP do hlavičky zprávy dle popisu v příslušné kapitole Technického manuálu.

Více informací o pověřených osobách, způsobu registrace uživatelů nebo systémů jsou spolu s popisem procesu správy uživatelů v IISSP uvedeny v dokumentu „Manuál procesu registrace uživatelů IISSP“ v aktuální verzi.

3.2 Registrace Zodpovědných osob pro komunikaci s CSÚIS

Pravidla pro registraci Zodpovědných osob a Náhradních zodpovědných osob pro komunikaci vybraných účetních jednotek s CSÚIS a podrobný popis procesu registrace je uveden v Technické vyhlášce (Vyhláška č. 383/2009 Sb. ve znění pozdějších předpisů) a Technickém manuálu CSÚIS.
Pro autentizaci uživatele v systému CSÚIS je použito uživatelské jméno a heslo.

3.3 Identifikace a autentizace

Uživatel IISSP může použít pro autentizaci jednu ze dvou metod:

a. autentizace uživatelským jménem a heslem,
b. autentizace prostřednictvím zaregistrovaného přihlašovacího komerčního certifikátu uživatele.

Z důvodu vyšší úrovně zabezpečení je doporučeno, aby:

- uživatel pro autentizaci používal přihlašovací certifikát uživatele. Tento certifikát musí být vydán schválenou certifikační autoritou (viz kap. 3.5 Certifikáty, zásady jejich použití a správy),
- přihlašovací certifikát uživatele a kvalifikovaný certifikát uživatele a k nim náležející privátní klíče byly uloženy na kryptografickém prostředku (čipová karta, USB token) vydaném schválenou certifikační autoritou (viz kap. 3.5 Certifikáty, zásady jejich použití a správy).

Uživatel IISSP musí:

- dodržovat dále uvedená pravidla pro použití hesel a certifikátů a další relevantní interní řídící dokumenty,
- používat výhradně svůj uživatelský účet,

- po přihlášení do IISSP zkontrolovat výpis svých předchozích přihlášení, který se zobrazí na úvodní stránce. Pokud má uživatel podezření, že se k IISSP v některém z uvedených časů nepřihlašoval, musí okamžitě nastavit nové heslo do systému a informovat příslušné (viz kap. 4.9 Zvládání bezpečnostních incidentů).

Uživatel systému IISSP nesmí:

- jakýmkoliv způsobem sdílet uživatelský účet a heslo s jinými uživateli,
- zaznamenávat hesla, případně PIN k certifikátu, na papíře, v souborech nebo na přenosných zařízeních s výjimkou jejich bezpečného uložení (tj. uložení na místě, které je prokazatelně zabezpečeno proti přístupu jiných osob).

3.4 Pravidla pro tvorbu a používání hesel

Pravidla pro tvorbu a používání hesel jsou platná pro všechny typy autentizace v IISSP. Řídí se Vyhláškou 82/2018 Sb. v platném znění (dále jen Vyhláška), zejména se zaměřením na ustanovení § 19 Správa a ověřování identit, pro ověření identity uživatelů, administrátorů a aplikací.

Uživatelé IISSP musí vzhledem k používání hesel dodržovat následující pravidla:

- hesla musí být udržována v tajnosti,
- hesla nesmí být zaznamenána na papíře, s výjimkou jejich bezpečného uložení (tj. uložení na místě, které je prokazatelně zabezpečeno proti přístupu jiných osob),
- hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování,
- heslo nesmí být zahrnuto do žádného automatizovaného přihlašovacího procesu, např. uložení do makra nebo funkční klávesy,
- osobní uživatelská hesla nesmí být sdílena.

Při tvorbě nového hesla musí uživatel dodržovat následující pravidla:

- heslo nesmí být založeno na informacích vztahujících se k osobě, které by mohl kdokoliv další jednoduše uhodnout nebo získat, např. jména, uživatelského ID, telefonní čísla, data narození apod.,
- heslo nesmí obsahovat po sobě jdoucí stejné znaky a nesmí obsahovat pouze číselné nebo pouze písmenné skupiny,
- minimální délka hesla je 17 znaků,
- maximální délka hesla je 40 znaků,
- heslo musí obsahovat minimálně dvě písmena a dvě číslice,
- heslo musí být pravidelně měněno, maximálně po 12 měsících,
- heslo nesmí být shodné jako minimálně 12 posledních hesel,
- staré heslo nesmí být použito jako část nového hesla,
- heslo nesmí být založeno na názvu systému, nesmí být použita slova jako:
    - „pokladna“,
    - „statnipokladna“,
    - „mojepokladna“ apod.,
- dále jsou nepřípustná hesla vzniklá z nepovolených výrazů prostřednictvím následujících úprav:
    - vykřičník na začátku a na konci,
    - otazník na začátku a na konci,
    - uvozovky (pokud jsou povoleny) na začátku a na konci,
    - pomlčka případně tečka, vykřičník nebo otazník uprostřed víceslovných hesel,
    - heslo nesmí začínat nebo končit číslicemi 123
- zároveň nedoporučujeme používat jednoduchou záměnu znaků při tvorbě hesla:
    - záměna písmen za speciální znaky (a za @),
    - záměna písmen za číslice (o za 0, i za 1, e za 3).

Po 6 neúspěšných pokusech se uživatelský účet na 1 hodinu zablokuje, odblokování se provede automaticky po uplynutí lhůty.

3.5 Certifikáty, zásady jejich použití a správy

Certifikáty jsou v IISSP využívány k následujícím účelům:

- autentizace uživatele portálu pro přístup do vybraných částí Portálu IISSP,
- elektronické podepisování aplikačních dat (vybraných transakcí),
- navázání šifrované komunikace mezi systémy (oboustranně autentizované TLS spojení).

Uživatelé IISSP jsou odpovědní za pořízení, správu a případné zneplatnění svých přihlašovacích a kvalifikovaných certifikátů v souladu s certifikační politikou a dalšími předpisy vydávající certifikační autority.

Pořízení, aktualizace, správa a případné zneplatnění přihlašovacích a kvalifikovaných certifikátů jsou prováděny prostředky poskytovanými vydávající certifikační autoritou (kryptografické prostředky, čtečky, software, uživatelské příručky a manuály). IISSP neposkytuje pro tyto činnosti žádné prostředky.

Pro uvedené účely jsou využívány certifikáty vydávané akreditovanými certifikačními autoritami v ČR:

- První certifikační autorita a.s. (ICA) – http://www.ica.cz/,
- Česká pošta s.p.– https://qca.postsignum.cz/,
- eIdentity a.s.– http://www.eidentity.cz/,
- Národní certifikační autorita - https://www.narodni-ca.cz/.

3.6 Zabezpečení komunikace

Pro zabezpečení SOAP komunikace se využívá síťový protokol HTTPS s využitím oboustranně autentizovaného TLS spojení. Tzn., že obě strany se navzájem autentizují svými komerčními systémovými (serverovými) certifikáty, které jsou primárně určeny pro bezpečnou komunikaci mezi servery.

IISSP podporuje přístup prostřednictvím kryptografického protokolu TLS 1.2. (kryptografické protokoly TLS 1.0 a TLS 1.1 nejsou nadále podporovány).

Pro automatickou komunikaci pomocí webových služeb je před prvním navázáním komunikace z EKIS nezbytné, aby veřejná část certifikátu, kterým se daný EKIS autorizuje, byl zaregistrován v IISSP. Detailní popis procesu registrace nového certifikátu, případně jeho aktualizace nebo zneplatnění, je uveden v dokumentu „Manuál procesu registrace uživatelů IISSP“ v aktuální verzi.

***Poznámka**:*

Veřejná část certifikátu je v IISSP využita pro vytvoření vazby mezi certifikátem a technickým uživatelem (účtem). Při navazování zabezpečeného spojení mezi systémem EKIS a IISSP je definovaná vazba využita pro identifikaci daného systému EKIS.

Tento způsob provázání certifikátu s technickým účtem je výhodný z pohledu volné definice obsahu certifikátu. Znamená to tedy, že obsah jednotlivých polí certifikátu není ze strany IISSP nijak definován ani limitován.

3.7 Autentizace uživatelů na Portálu IISSP

Pro přístup k Portálu IISSP je vyžadována autentizace pomocí uživatelského jména a hesla. Přihlašovací údaje uživatel získá během procesu registrace uživatele IISSP.

Po prvním přihlášení si uživatel může zvolit variantu autentizace pomocí komerčního certifikátu. Pro potřebu autentizace uživatele komerčním certifikátem musí uživatel nahrát a následně aktualizovat veřejný klíč komerčního certifikátu ve svém uživatelském profilu. V případě, že uživatel zvolí variantu autentizace pomocí komerčního certifikátu, je zablokováno přihlašovací heslo. Pro návrat k základnímu způsobu autentizace pomocí jména a hesla musí uživatel ve svém profilu provést od-registrování klientského certifikátu a vygenerování nového iniciálního hesla.

Detailní postup pro registraci uživatele IISSP je popsán v dokumentu „Manuál procesu registrace uživatelů IISSP“.

Doporučujeme koncovým uživatelům, aby si v prohlížečích nepovolovali automatické doplňovaní certifikátů (např. u webového prohlížeče parametr AutoSelectCertificateForUrls).

Podle našich zjištění předává Edge s největší pravděpodobnostní bez vědomí uživatele při autentizaci EU uživatele certifikát (nezabezpečený PINem) do prostředí Portálu IISSP. Problém se vyskytuje u uživatelů, kteří se hlásí jménem a heslem. V případě zneužití může dojít k úspěšnému zalogování uživatele do systému bez jeho vědomí. Uživateli stačí zadat jakákoliv URL adresa státní pokladny a dojde k automatické autentizaci na pozadí bez vědomí uživatele.

3.8 Elektronické podepisování aplikačních dat

Zaručený elektronický podpis (aplikačních dat, transakcí, zpráv apod.) se používá pro zajištění integrity, autenticity a nepopiratelnosti autorství přenášených dat. Z tohoto důvodu je vyžadováno použití kvalifikovaných osobních certifikátů nebo elektronických značek založených na kvalifikovaných systémových certifikátech, které byly vydány akreditovanými certifikačními autoritami (viz výše).
V souladu s doporučením NUKIB zavádí nově IISSP omezení na podporované hashovací funkce a přestává podporovat digitální podpisy, které jsou vytvořeny pomocí hashovací funkce SHA-1. Nadále bude podporovat IISSP pro elektronický podpis pouze hashovací funkce třídy SHA-2 (SHA-256, SHA-384 a SHA-512), více informací viz. https://nukib.gov.cz/cs/ochrana-ui-v-ict/kryptograficka-ochrana/informace/).

3.9 Portál CSÚIS

Účelem portálu CSÚIS je poskytnout uživatelům zastupujícím vybrané účetní jednotky (Zástupce účetní jednotky / Zodpovědné osoby) uživatelský přístup k funkcím CSÚIS pro správu Zodpovědných osob, zasílání účetních záznamů a jiných výkazů do CSÚIS a monitoring jejich zpracování. Zodpovědné osoby nemají přístup k portálu IISSP.

Pro přístup k portálu CSÚIS platí stejné technické předpoklady a požadavky na zabezpečení jako pro přístupy k portálu IISSP.

Podrobný popis portálu CSÚIS je uveden v uživatelské příručce portálu CSÚIS na stránkách CSÚIS.

3.10 Klient CSÚIS

Klient CSÚIS je 64-bitová aplikace pro komunikaci mezi účetními jednotkami a CSÚIS určená pro běh na lokálním počítači uživatele. Aplikace nahrazuje původní aplikace Šifrovací utilita a DAVY, které nadále nejsou podporovány.

Aplikace slouží pro centralizaci a automatizaci činnosti spojené s odesíláním zpráv do CSÚIS a práci s osobními přístupovými údaji ZO/NZO.

Detailní informace o aplikaci Klient CSÚIS včetně jejího uživatelského manuálu a technických požadavků jsou dostupné na webové stránce CSÚIS.

4. Bezpečnost

Tato kapitola obsahuje bezpečnostní doporučení na údržbu a obsluhu hardwarového a softwarového vybavení pracovní stanice a pravidla pro práci s aplikacemi IISSP

4.1 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-li 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,
- věnoval pozornost procesu přihlašování tak, aby nedocházelo k vypršení časového limitu pro přihlášení a následným chybovým hlášením. Pro vlastní přihlášení je nastaven určitý časový limit, který je třeba dodržet, jinak se spojení ukončí.
- vypnul pracovní stanici nebo zamknul obrazovku pracovní stanice, pokud se od ní vzdaluje.

4.2 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.

Je doporučeno, aby uživatel IISSP:

- prováděl pravidelné aktualizace bezpečnostních oprav operačního systému,
- chránil svůj počítač zapnutím osobního firewallu,
- 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.

Uživatelům IISSP se nedoporučuje:

- uchovávat a/nebo zpracovávat jakákoli data osobního charakteru (nepracovní data) na pracovních stanicích a jiných zařízeních systémů IISSP (scannery, tiskárny apod.),
- provádět instalaci nelegálních programů a souborů. 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.

4.3 Bezpečnostní pravidla pro práci s internetovým prohlížečem

Doporučuje se, aby uživatel IISSP:

- zakázal ukládání hesel v prohlížeči,
- 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.

4.4 Ochrana proti phishingu

Phishingový útok slouží k podvodnému získání a zneužití přihlašovacích údajů. Útočníci obvykle zasílají podvržené e-mailové zprávy, které se jeví jako zprávy 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 proti vzorům v platné dokumentaci e-maily z IISSP, které obsahují požadavek na okamžitou reakci, jinak 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.

4.5 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 regulérně odhlásil a následně zavřel okno internetového prohlížeče.

4.6 Pravidla pro práci více uživatelů na jednom počítači

V případě, že jednu pracovní stanici sdílí více osob, měl by uživatel IISSP 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.

4.7 Důvěrnost

Uživatelům IISSP se zakazuje:

- prozrazovat jakékoli skutečnosti týkající se technického nebo organizačního zajištění bezpečnosti IISSP třetím osobám,

- vkládat do IISSP jakékoli osobní údaje, jak je definuje aktuální znění zákona č. 110/2010 Sb. – zákon o zpracování osobních údajů. Mezi osobní údaje patří i jméno a příjmení ve spojení s trvalým bydlištěm uživatele.

4.8 Zásada prázdného stolu a prázdné obrazovky

Uživatelům IISSP se doporučuje dodržovat zásady prázdného stolu a prázdné obrazovky monitoru:

- veškerá elektronická i neelektronická média obsahující informace zpracovávané v IISSP musí být v případě, že se nepoužívají, a zejména když je kancelář prázdná, uzamčena – ideálně v protipožárním trezoru nebo v uzamykatelných skříních nebo v jiném bezpečném druhu nábytku,
- neaktivní pracovní stanice, které umožňují přístup k IISSP, musí být po definovaném čase vypnuty nebo zamknuty, aby se předešlo přístupu neoprávněných osob. Časový mechanismus by měl po definované době nečinnosti smazat obsah obrazovky. Automatický časový interval pro zamčení stanice je stanoven na 10 minut,
- uživatel je povinen vypnout pracovní stanici nebo zamknout obrazovku pracovní stanice, pokud se od ní vzdaluje.

4.9 Zvládání bezpečnostních incidentů

Uživatel IISSP musí:

- okamžitě po zjištění jakéhokoliv nestandardního chování systému, selhání hardwaru nebo softwaru nebo vzniku jakéhokoliv bezpečnostního incidentu:
  - kontaktovat svého nadřízeného, lokálního technika, případně bezpečnostního správce,
  - v případě, že mohlo dojít k porušení bezpečnostních pravidel, poškození nebo ztrátě dat nebo jiné události, mající možný dopad na bezpečnost IISSP, neprodleně tuto skutečnost oznámit na ServiceDesk IISSP,
- v případě podezření na prozrazení přihlašovacích údajů (jméno, heslo), případně privátního klíče, náležejícího k certifikátu (komerčnímu nebo kvalifikovanému) neprodleně tuto skutečnost oznámit na ServiceDesk IISSP a svému nadřízenému a změnit heslo, případně revokovat certifikát dle procesů příslušné certifikační autority.

4.10 Fyzická bezpečnost

Uživatel IISSP musí:

- zajistit uchování všech tištěných výstupů, případně jiné dokumentace IISSP, pouze pro účely vykonávané pracovní činnosti a zabránit jejich zpřístupnění nepovolaným osobám;
- bezpečně uchovávat média nebo dokumenty obsahující neveřejné informace IISSP;
- bezpečně zničit všechny nepotřebné dokumenty obsahující neveřejné informace IISSP ve skartovacím stroji.