Integrovaný informační systém Státní pokladny (IISSP)

Příručka uživatele

Historie dokumentu

Historie revizí

Číslo revize	Datum revize	Sumarizace změn	Změny označeny
1.0	3. 7. 2020	Finální verze dokumentu	Ne
2.0	13. 7. 2020	Finální verze dokumentu	Ne
3.0	5. 5. 2022	Finální verze dokumentu	Ne
4.0	3. 11. 2023	Finální verze dokumentu	Ne

Platnost dokumentu

Tento dokument je platný od:

- zprovoznění aktualizace technických komponent IISSP ke dni upgradu technických komponent RISRE 11. 6. 2022.

Obsah

Obsah:

1. Účel dokumentu ... 5
1.1 Rozsah ... 5
1.2 Definice pojmů a zkratek ... 5
2. Přístup uživatelů k IISSP ... 7
2.1 Identifikace a autentizace ... 7
2.2 Pravidla pro tvorbu a používání hesel ... 7
2.3 Certifikáty, zásady jejich použití a správy ... 8
3. Přihlášení do Portálu IISSP ... 9
3.1 Přihlášení uživatelským jménem a heslem ... 9
3.2 Změna iniciálního hesla ... 11
3.3 Změna hesla uživatelem ... 12
3.4 Přihlášení komerčním certifikátem ... 12
3.5 Prvotní registrace komerčního certifikátu ... 13
3.6 Přihlášení do Portálu IISSP pomocí komerčního certifikátu ... 15
3.7 Smazání komerčního certifikátu a nastavení iniciálního hesla ... 15
3.8 Sledování historie uživatele ... 17
3.9 Dokumentace ... 17
3.10 Odhlášení z Portálu IISSP ... 18
3.11 Komunikace s Kompetenčním centrem IISSP ... 19
4. Elektronický podpis v prostředí IISSP ... 20
4.1 Aplikace ASD WebSigner ... 20
4.2 Vytvoření elektronického podpisu v prostředí portálu IISSP ... 20
5. Bezpečnost ... 22
5.1 Základní doporučení ... 22
5.2 Ochrana klientských stanic proti škodlivým kódům ... 22
5.3 Bezpečnostní pravidla pro práci s internetovým prohlížečem ... 22
5.4 Ochrana proti phishingu ... 23
5.5 Ochrana proti clickjackingu ... 23
5.6 Pravidla pro práci více uživatelů na jednom počítači ... 23
5.7 Důvěrnost ... 23
5.8 Zásada prázdného stolu a prázdné obrazovky ... 24
5.9 Zvládání bezpečnostních incidentů ... 24
5.10 Fyzická bezpečnost ... 24

Seznam obrázků:

Obrázek 1: Přihlašovací obrazovka Portálu IISSP 10
Obrázek 2: Obrazovka pro změnu hesla 11
Obrázek 3: Personalizace 12
Obrázek 4: Personalizace – Změna hesla 12
Obrázek 5: Personalizace 13
Obrázek 6: Personalizace – Nahrání nového certifikátu 14
Obrázek 7: Odkaz na Certifikát 14
Obrázek 8: Nahrání komerčního certifikátu 14
Obrázek 9: Volba digitálního certifikátu 15
Obrázek 10: Odkaz na Personalizaci 16
Obrázek 11: Smazání komerčního certifikátu – Výběr certifikátu 16
Obrázek 12: Smazání komerčního certifikátu 17
Obrázek 13: Úvodní obrazovka Portálu – Historie uživatele 17
Obrázek 14: Přístup k dokumentaci 18
Obrázek 15: Přístup k dokumentaci – otevření souboru 18
Obrázek 16: Odhlášení z Portálu 18
Obrázek 17: Korektní odhlášení z Portálu IISSP 19
Obrázek 18: Uživatelské prostředí pro vytvoření elektronického podpisu 20

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
DS	Dokumentační server
ABO-K	Internetová aplikace ČNB, poskytující klientům ČNB službu „Internetbanking“
CSUIS	Centrální systém účetních informací státu
ČNB	Česká národní banka
EDS/SMVS	Evidenční dotační systém (EDS)/ Správa majetku ve vlastnictví státu (SMVS)
EKIS	Ekonomický informační systém
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IAM	Identity and Access Management (Centrální správa identit)
IISSP	Integrovaný informační systém Státní pokladny
ISDP	Informační systém o datových prvcích
ISVZUS	Informační systém veřejných zakázek uveřejňovací subsystém
KVS	Kryptografické a validační služby
MF	Ministerstvo financí
NNV	Nároky z nespotřebovaných výdajů
NUTS	Normalizovaná klasifikace územních celků v České republice
OO	Oprávněná osoba
OSS	Organizační složka státu
PKI	Public Key Infrastructure
PO	Pověřená osoba
PVS	Příjmová a výdajová struktura
RIS	Rozpočtový informační systém
RISPR	Rozpočtový informační systém Příprava rozpočtu
RISRE	Rozpočtový informační systém Realizace rozpočtu
ROP	Rozpočtové opatření
RZAM	Regulace zaměstnanosti
SDR	Střednědobý rozpočet
SOAP	Simple Object Access Protocol
SR	Státní rozpočet
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
TLS	Trasport Layer Security
ÚJ	Účetní jednotka
ÚSC	Územně samosprávný celek
W3C	The World Wide Web Consortium
WSDL	Web Service Definition Language
XML	Extensible Markup Language

Zkratka	Vysvětlení
XSD	XML Schema Definition

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 takto označené Vlastníkem daného procesu či Vlastníkem dané aplikace. 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 „Incident". 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**.

2. Přístup uživatelů k IISSP

2.1 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 IISSP pro autentizaci používal přihlašovací certifikát. Tento certifikát musí být vydán schválenou certifikační autoritou (viz kap. 2.3 Certifikáty, zásady jejich použití a správy),
- přihlašovací a kvalifikovaný certifikát Uživatele IISSP a k nim náležející privátní klíče uložené na kryptografickém prostředku (čipová karta, USB token) vydaném schválenou certifikační autoritou (viz kap. 2.3 Certifikáty, zásady jejich použití a správy).

Uživatel IISSP musí:

- dodržovat dále uvedená pravidla pro použití hesel a certifikátů a další 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 pracovníky (viz kap. 5.9 Zvládání bezpečnostních incidentů).

Uživatel 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).

2.2 Pravidla pro tvorbu a používání hesel

Pravidla pro tvorbu a používání hesel jsou platná pro všechny typy autentizace v IISSP. Řídí se Vyhláškou o kybernetické bezpečnosti č. 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 IISSP dodržovat následující pravidla:

- heslo nesmí být založeno na informacích vztahujících se k osobě, které by mohl kdokoliv další jednoduše uhodnout nebo získat, např. jména, uživatelské 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, platnost hesla je maximálně 12 měsíců,
- heslo nesmí být shodné jako minimálně 12 posledních hesel,
- ID uživatele nesmí být použito jako součást hesla, 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.

2.3 Certifikáty, zásady jejich použití a správy

Certifikáty jsou v IISSP využívány k následujícím účelům:

- autentizace Uživatele IISSP pro přístup do vybraných částí Portálu IISSP,
- elektronické podepisování aplikačních dat (vybraných transakcí).

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. Přihlášení do Portálu IISSP

Uživatel IISSP se přihlašuje do Portálu IISSP pomocí uživatelského jména a hesla, případně za využití certifikátu. Uživatelské jméno a heslo tvoří přihlašovací údaje. Přihlašovací údaje Uživatel IISSP získá na základě žádosti o registraci uživatele a po následném absolvování školení nebo souboru školení nezbytných k získání oprávnění vykonávat činnosti v IISSP. Zmíněná žádost o registraci Uživatele IISSP se formálně nazývá Registrační formulář.

Uživatelské jméno bude po ukončení školení zasláno na e-mail uživatele uvedený v registračním formuláři. Iniciální heslo bude uživateli po ukončení školení zasláno rovněž dopisem v bezpečnostní obálce na adresu uvedenou v registračním formuláři.

Registrační formulář každého jednotlivého Uživatele IISSP předává správci IISSP zmocněný pracovník každé jednotlivé Kapitoly. V procesu Registrace uživatele je zmocněný pracovník nazýván Pověřenou osobou. Pověřená osoba je formálně odpovědná za úplnost a obsahovou správnost údajů uvedených v registračním formuláři Uživatele IISSP.

Z bezpečnostních důvodů je Uživatel IISSP při prvním přihlášení do Portálu automaticky vyzván ke změně obdrženého iniciálního hesla. Po změně hesla se stává iniciální heslo neplatné. V případě zapomenutí změněného hesla se uživatel nebude moci nadále přihlásit do Portálu. V takovém případě musí kontaktovat Kompetenční centrum IISSP (dále KC IISSP) prostřednictvím Service Desku (**servicedesk@spcss.cz**), které Uživateli IISSP poskytne nové iniciální heslo.

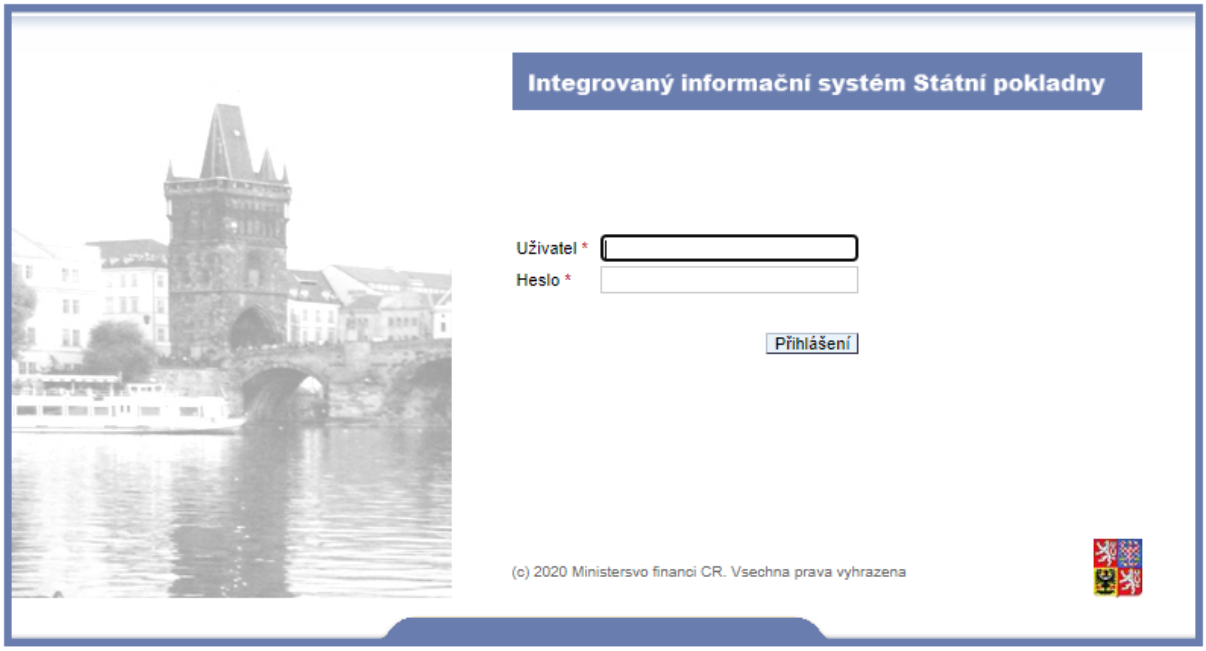
Postup pro přihlášení do Portálu IISSP a adresa Portálu IISSP jsou uvedeny v následujících kapitolách tohoto materiálu. V rámci školení bude Uživatel IISSP používat adresu tzv. školicího Portálu IISSP. Adresa školicího Portálu IISSP bude Uživateli IISSP sdělena na školení a je platná a využitelná pouze pro účely školení.

3.1 Přihlášení uživatelským jménem a heslem

Pracovní postup:

1. Uživatel IISSP spustí internetový prohlížeč.
2. Do adresního řádku uvede adresu Portálu IISSP (https://portal.statnipokladna.cz).
3. V závislosti na typu a verzi internetového prohlížeče uživatele a v případě existence registrovaného podporovaného komerčního certifikátu v prohlížeči se zobrazí uživateli hlášení s možností zadání komerčního certifikátu. Uživatel zvolí tlačítko „Storno“, případně „Zrušit“.
4. Uživatel se přihlásí do Portálu IISSP prostřednictvím uživatelského jména a hesla.

Obrázek 1: Přihlašovací obrazovka Portálu IISSP



5. Uživatel vyplní pole ***Uživatel*** (uživatelské jméno) a ***Heslo*** (iniciální heslo v případě prvního přihlášení).
6. Uživatel stiskne tlačítko ***Přihlášení***.
7. V případě prvního přihlášení provede uživatel změnu iniciálního hesla dle postupu v následující kapitole 3.2 – Změna iniciálního hesla.
8. **Výsledek:** Po prvním přihlášení do Portálu IISSP se uživateli zobrazí **Závazné podmínky** pro přístup do Portálu IISSP. Uživatel si přečte **Závazné podmínky** pro přístup do Portálu IISSP a užívání jeho funkcionalit.
9. Uživatel pokračuje stisknutím tlačítka ***Souhlasím***.
10. **Výsledek**: Uživatel je přihlášen do Portálu IISSP.

Poznámka: Seznam podporovaných internetových prohlížečů je uveden v technických podmínkách provozu v tzv. Technickém manuálu – Příručka administrátora, který je zveřejněn na webových stránkách www.statnipokladna.cz v sekci Kompetenční centrum -> Technické informace.

Poznámka: Upozorňujeme uživatele na několik bodů, které je nutné zohlednit **během prvního přihlášení do nového Portálu IISSP** po jeho zprovoznění 8. 6. 2020:

- uživatelské jméno a heslo je stejné, jaké jste používali na původní verzi Portálu IISSP,
- poté, co zadáte svoje uživatelské jméno a heslo, budete vyzváni ke změně hesla (důvodem je zachování bezpečnosti připojení),
- změna hesla proběhne stejně jako v minulosti – budete dotázáni na staré heslo a na nové heslo, které bude nutné zadat 2x pro potvrzení správnosti,
- oproti pravidlům pro strukturu hesla na původním Portálu IISSP byla z důvodu požadavků legislativy prodloužena minimální délka hesla na 17 znaků,

Prosíme tedy Uživatele IISSP, aby si připravil přihlašovací údaje, zejména staré a nové heslo, před zadáním přihlašovacích údajů (doba pro autentizaci je nyní z bezpečnostních důvodů omezena).

3.2 Změna iniciálního hesla

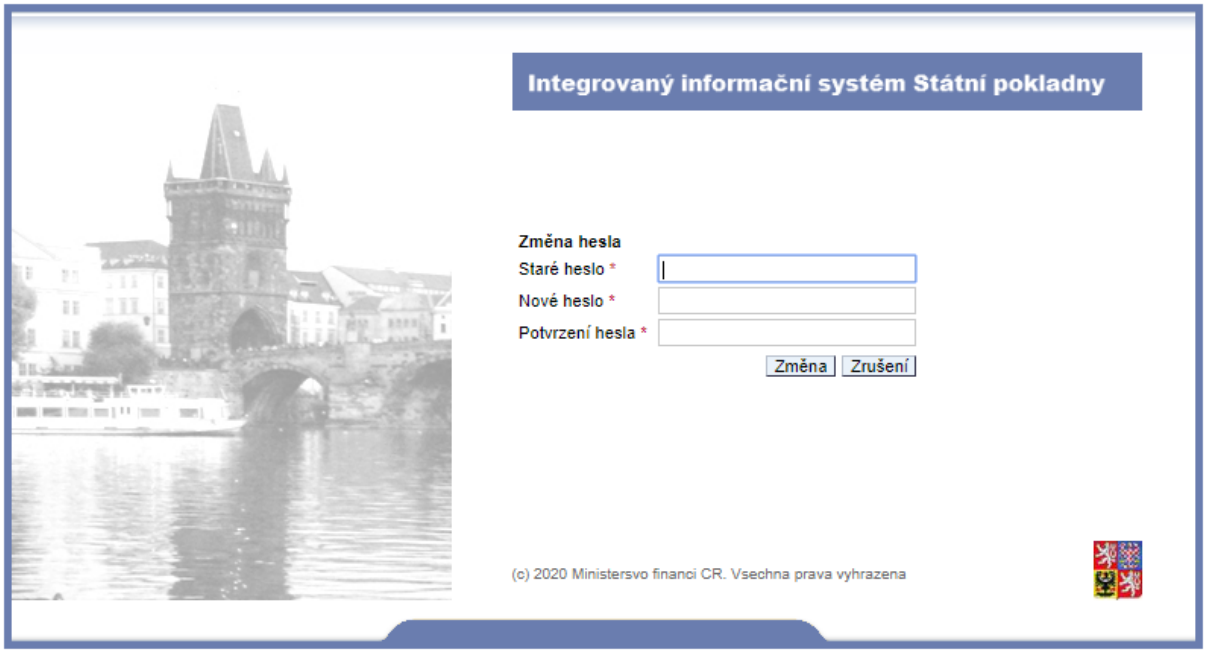
Po prvním přihlášení do Portálu IISSP se Uživateli IISSP zobrazí obrazovka pro změnu iniciálního hesla. Tato obrazovka se zobrazí i v případě, kdy bylo Uživateli IISSP vystavené nové iniciální heslo (např. po jeho ztrátě a po vystavení nového hesla) a dále pak z bezpečnostních důvodů vždy po uplynutí doby 90 kalendářních dnů.

Pracovní postup:

1. Uživatel do příslušných polí zadá **Staré heslo**, **Nové heslo** a **Potvrzení hesla**. Obsah polí **Nové heslo** a **Potvrzení hesla** musí být shodný, v opačném případě nedojde ke změně hesla a systém zobrazí chybové hlášení.

2. Uživatel stiskne tlačítko ***Změna*** [Změna].

   Obrázek 2: Obrazovka pro změnu hesla



<u>Poznámka</u>: Pro tvorbu hesla platí následující konvence. Heslo, které nebude při změně vyhovovat dále popsaným konvencím, bude systémem odmítnuté:

- minimální délka hesla je **17** znaků,
- maximální délka hesla je **40** znaků,
- heslo musí obsahovat minimálně **2** písmena a **2** číslice,
- heslo musí být pravidelně měněno, platnost hesla je maximálně **12** měsíců,
- heslo nesmí být shodné jako minimálně **21** posledních hesel
- ID uživatele nesmí být použito jako součást hesla
- staré heslo nesmí být použito jako část nového hesla.
- v případě **6** po sobě následujících neúspěšných pokusů o přihlášení bude heslo **zablokováno** na dobu **1** hodiny.
- 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).

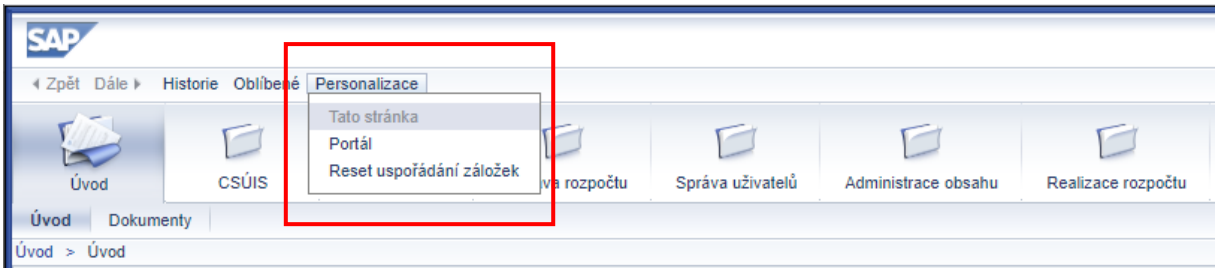
3.3 Změna hesla uživatelem

Uživatel IISSP má možnost kdykoliv změnit svoje heslo. Pravidla pro změnu hesla jsou totožná s pravidly pro změnu iniciálního hesla.

Pracovní postup:

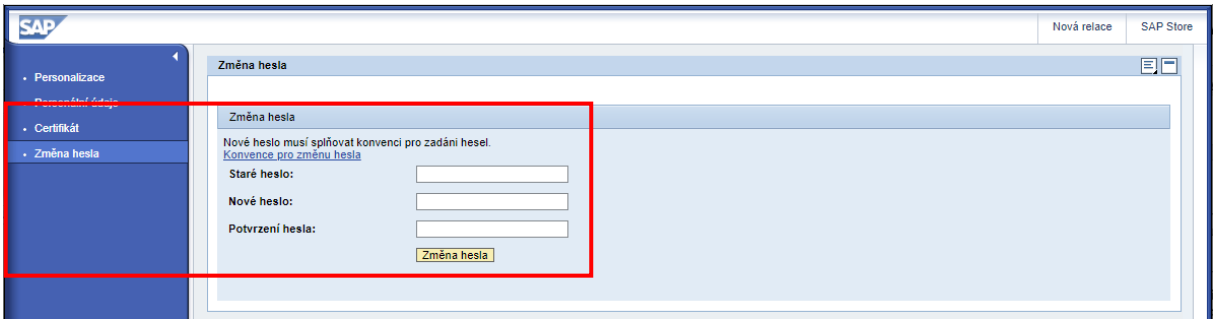
1. Po přihlášení uživatel vybere v menu Personalizace položku Portál.

Obrázek 3: Personalizace



2. Uživatel do příslušných polí zadá **Staré heslo**, **Nové heslo** a **Potvrzení hesla**. Obsah polí **Nové heslo** a **Potvrzení hesla** musí být shodný, v opačném případě nedojde ke změně hesla a systém zobrazí chybové hlášení.
3. Uživatel stiskne tlačítko ***Změna hesla.***

Obrázek 4: Personalizace – Změna hesla



3.4 Přihlášení komerčním certifikátem

Pro přihlášení do Portálu IISSP je doporučeno využití autentizačního mechanismu s vyšší úrovní zabezpečení – autentizace prostřednictvím komerčního certifikátu. Pro využití možnosti autentizace prostřednictvím komerčního certifikátu musí být v Portálu IISSP pro daného Uživatele IISSP registrován veřejný klíč komerčního certifikátu. Proces registrace veřejného klíče certifikátu je popsán v kapitole 3.5 – Prvotní registrace komerčního certifikátu.

V případě, že má uživatel v IISSP registrovaný komerční certifikát, je mu z důvodu zajištění bezpečnosti znemožněno přihlašovat se prostřednictvím uživatelského jména a hesla. V případě, že uživatel požaduje obnovit možnost přihlašování se do Portálu IISSP prostřednictvím uživatelského

jména a hesla, musí vymazat uložený komerční certifikát pro autentizaci přístupu na Portál IISSP viz kapitola 3.7 – Smazání komerčního certifikátu a nastavení iniciálního hesla.

Komerční certifikát lze získat u libovolné akreditované certifikační autority schválené pro státní správu. Postup získání komerčního certifikátu je podrobně popsán na stránkách konkrétních certifikačních autorit. Aktuální podporované komerční certifikáty jsou uvedeny v kapitole 2.3 Certifikáty, zásady jejich použití a správy. Pro přístup k IISSP **uživatel musí používat certifikáty chráněnné při použití dalším faktorem** dle technických možností poskytovaných vydávajícími autoritami, tedy buď **uložením na zabezpečené HW zařízení** (čipová karta, USB token) nebo **ochranu přístupu k certifikátu prostřednictvím PINu nebo hesla**. Kromě zcizení certifikátu zamezí ochrana certifikátu dalším faktorem i komunikaci prohlížeče se službami IISSP bez vědomí uživatele.

Poznámka: Přihlášení Uživatele IISSP komerčním certifikátem výrazně přispívá ke zvýšení úrovně zabezpečení přihlášení k účtu. Za přihlašovaného Uživatele IISSP se zaručuje certifikační autorita, která certifikát vydala. Pokud není zcizen privátní klíč komerčního certifikátu Uživatele IISSP, není prakticky možné, aby se za Uživatele vydávala osoba neoprávněná. Ochrana privátního klíče komerčního certifikátu, který je zpravidla ještě navíc chráněn heslem, je povinností osoby, na kterou je certifikát vydán certifikační autoritou (viz podmínky užívání komerčních certifikátů každé jednotlivé certifikační autority).

3.5 Prvotní registrace komerčního certifikátu

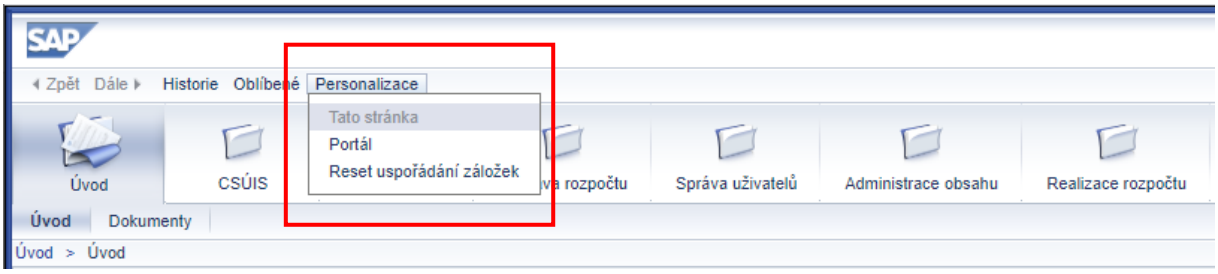
V rámci uživatelské aktualizace certifikátu na Portálu IISSP je možné ukládat (i smazat) komerční certifikát pro autentizaci Uživatele IISSP při přihlášení do Portálu IISSP.

V případě, že uživatel má v IISSP registrovaný komerční certifikát určený pro autentizaci uživatele v Portálu IISSP, je mu znemožněno přihlašovat se do Portálu IISSP uživatelským jménem a heslem.

Pracovní postup:

1. Po přihlášení uživatel vybere v menu Personalizace položku Portál.

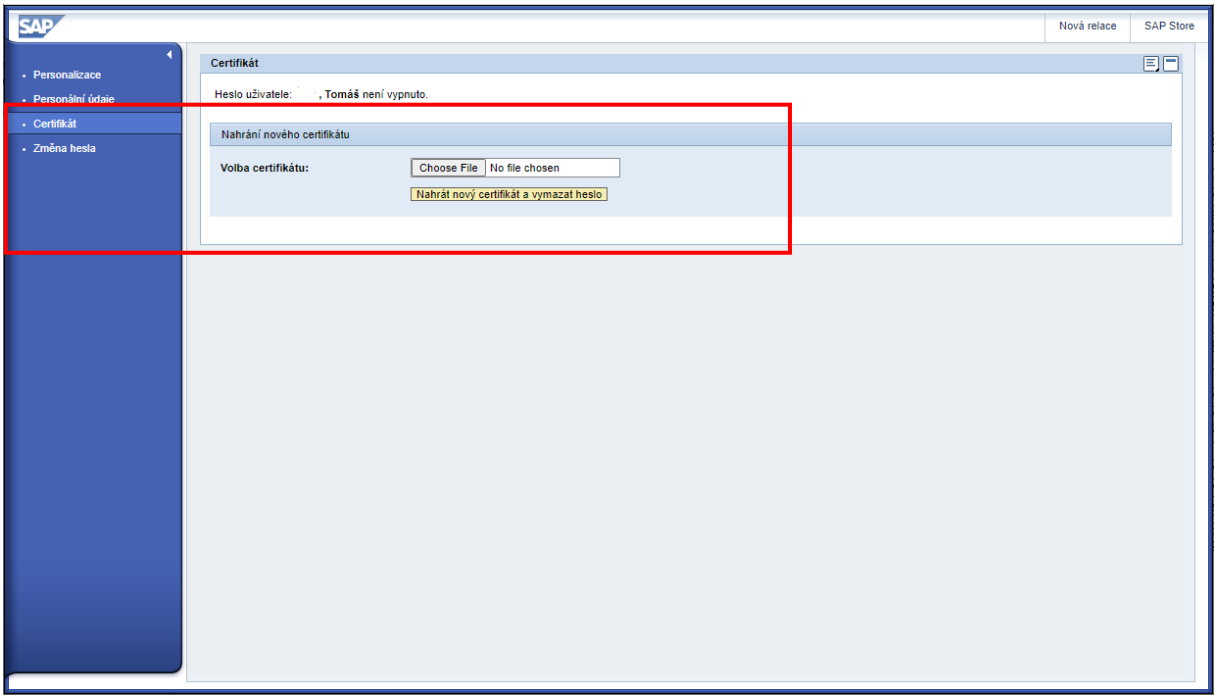
Obrázek 5: Personalizace



2. **Výsledek**: Otevře se další okno internetového prohlížeče se stránkou umožňující prohlížení a změny osobních údajů uživatele.
3. Uživatel vybere položku ***Certifikát***, která zpřístupní možnost nahrání souboru s certifikátem ve formátu PEM.

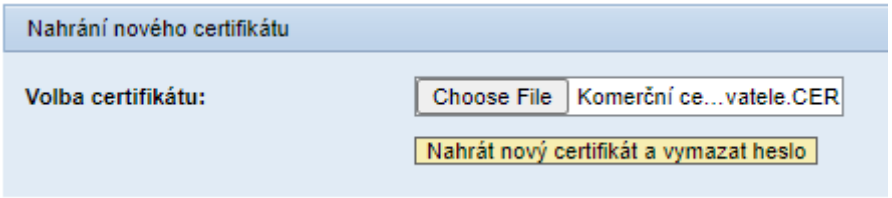
   Upozorňujeme na to, aby se Uživatel IISSP ujistil, že nahrává skutečně pouze veřejnou část certifikátu (bez privátního klíče) a že se jedná o komerční certifikát vystavený jednou z certifikačních autorit akreditovaných v České republice.

Obrázek 6: Personalizace – Nahrání nového certifikátu



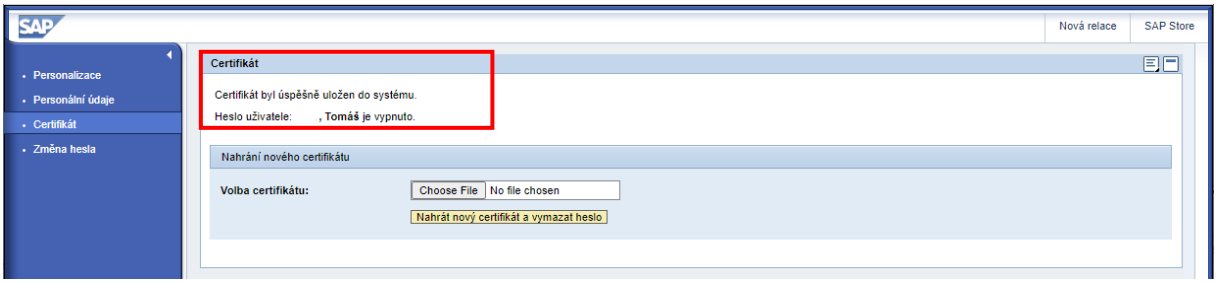
4. Uživatel klikne na odkaz Vybrat soubor.

Obrázek 7: Odkaz na Certifikát



5. **Výsledek**: Zobrazí se záložka se správou komerčních certifikátů.
6. Uživatel stiskne tlačítko Procházet a zadá cestu k vybranému komerčnímu certifikátu.

Obrázek 8: Nahrání komerčního certifikátu



7. Uživatel již nebude moci použít heslo.
8. **Výsledek**: Komerční certifikát pro autentizaci je nahrán (heslo vymazáno).
9. Uživatel zavře okno Personalizace.
10. Uživatel se odhlásí z Portálu IISSP.

11. **Výsledek**: Uživatel při příštím přihlašování do Portálu IISSP vybere odpovídající komerční certifikát a přihlásí se již pomocí komerčního certifikátu.

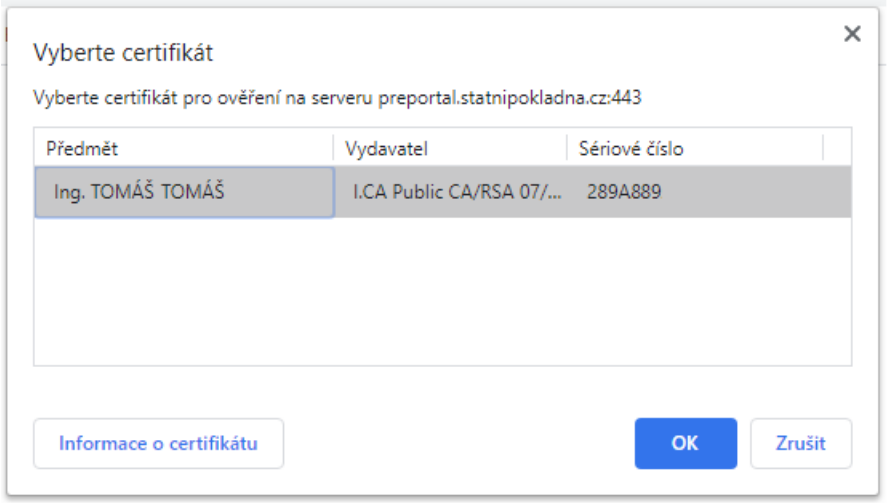
Poznámka: Seznam podporovaných internetových prohlížečů je uveden v technických podmínkách provozu v tzv. Technickém manuálu, který je zveřejněn na internetových stránkách MF.

3.6 Přihlášení do Portálu IISSP pomocí komerčního certifikátu

Pracovní postup:

1. Uživatel spustí internetový prohlížeč.
2. Do adresního řádku uvede adresu Portálu IISSP.
3. Uživateli se zobrazí hlášení s možností zadání komerčního certifikátu.
4. Uživatel vybere odpovídající komerční certifikát, který ke svému uživatelskému účtu nahrál (viz kapitola 3.5 – Prvotní registrace komerčního certifikátu).

   Obrázek 9: Volba digitálního certifikátu



5. **Výsledek:** V případě, že uživatel vybere platný komerční certifikát, který má přiřazený ke svému účtu v Portálu IISSP, je autentizován pomocí tohoto komerčního certifikátu bez nutnosti zadání jména a hesla. Pokud se nezobrazí možnost přihlášení pomocí komerčního certifikátu, nebo pokud tuto možnost uživatel zamítne, dojde k přesměrování na přihlašovací obrazovku Portálu IISSP - viz kapitola 3.5 - Prvotní registrace komerčního certifikátu.

Poznámka 1: Seznam podporovaných internetových prohlížečů je uveden v technických podmínkách provozu v tzv. Technickém manuálu – Příručka administrátora, který je zveřejněn na internetových stránkách Státní pokladny.

Poznámka 2: Výzva ke zvolení certifikátu se uživateli zobrazí automaticky v případě, že má v PC nainstalovaný vyhovující komerční certifikát, a to nezávisle na tom, jestli si ho registroval pro přihlašování do Portálu IISSP nebo ne. Pokud není komerční certifikát správně registrován výše uvedeným postupem, dojde po jeho potvrzení k přesměrování uživatele na standardní přihlašovací obrazovku.

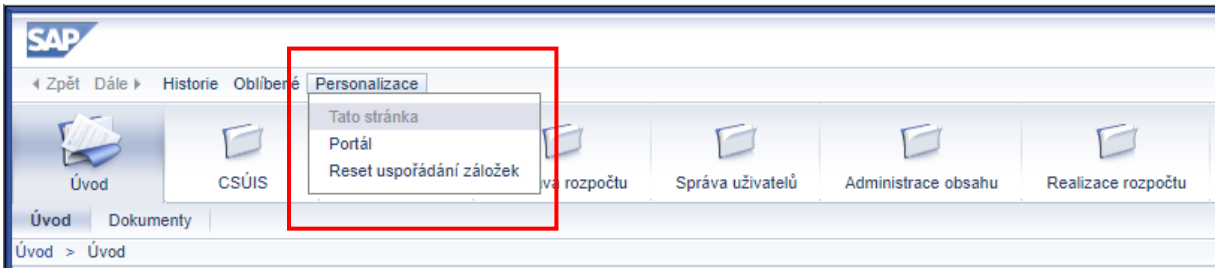
3.7 Smazání komerčního certifikátu a nastavení iniciálního hesla

Po smazání komerčního certifikátu bude Uživatel IISSP vyzván k zadání nového hesla, kterým se bude nadále prokazovat při přihlašování do Portálu IISSP. Z důvodu zvýšení bezpečnosti je zadávané nové heslo nastaveno jako iniciální. Systém vyzve uživatele při příštím přihlášení ke změně tohoto hesla na jiné.

Pracovní postup:

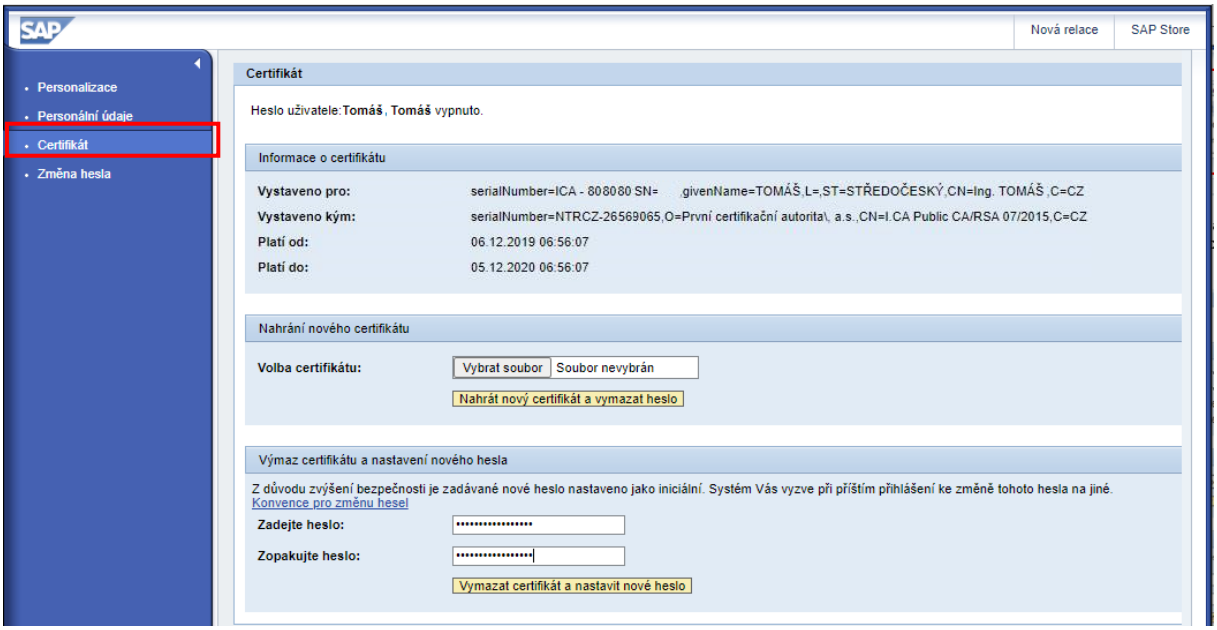
1. Uživatel spustí internetový prohlížeč.
2. Do adresního řádku uvede adresu Portálu IISSP.
3. Uživateli se zobrazí hlášení s možností zadání komerčního certifikátu.
4. Uživatel vybere odpovídající komerční certifikát, který ke svému uživatelskému účtu registroval (viz kapitola 3.5 – Prvotní registrace komerčního certifikátu).
5. **Výsledek**: Uživatel je přihlášen do Portálu IISSP.
6. Uživatel klikne na odkaz ***Personalizace*** v horní liště portálového rozhraní.

Obrázek 10: Odkaz na Personalizaci



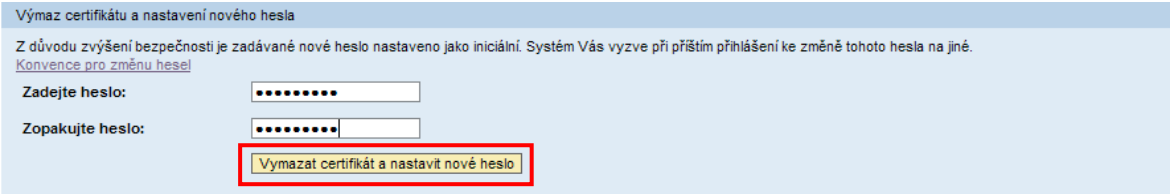
7. **Výsledek:** Otevře se další okno v internetovém prohlížeči se stránkou umožňující prohlížení a změny údajů, vztahující se k uživateli.
8. Uživatel klikne na odkaz ***Certifikát***.

Obrázek 11: Smazání komerčního certifikátu – Výběr certifikátu



9. Uživatel zadá v sekci Výmaz certifikátu a nastavení nového hesla iniciální heslo (2x).

Obrázek 12: Smazání komerčního certifikátu



10. Uživatel stiskne tlačítko ***Vymazat certifikát a nastavit nové heslo*** Vymazat certifikát a nastavit nové heslo.
11. **Výsledek:** Iniciální heslo je nastaveno (certifikát smazán). Při dalším přihlášení do Portálu IISSP bude Uživatel IISSP povinen provést změnu iniciálního hesla dle konvence pro zadání hesla (viz kapitola 3.2 Změna iniciálního hesla).

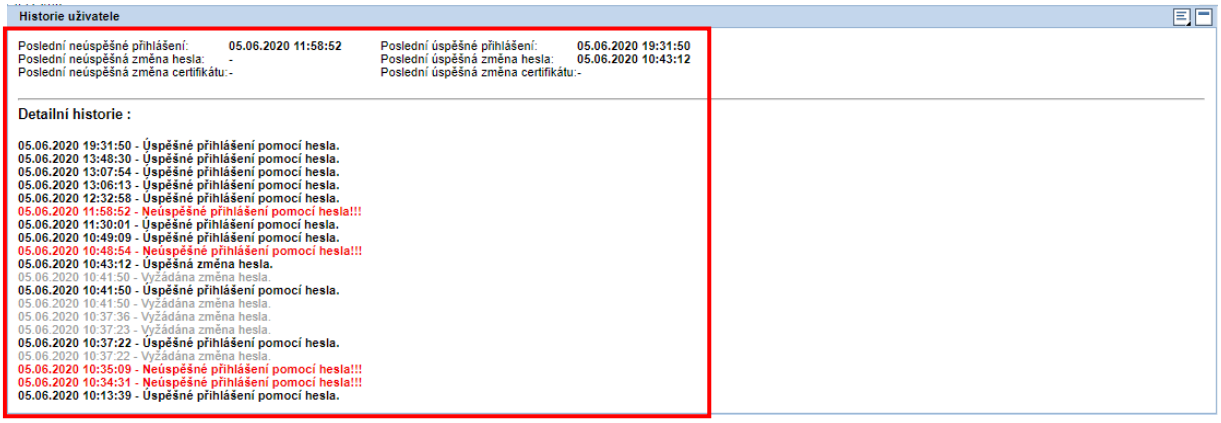
Poznámka: Seznam podporovaných internetových prohlížečů je uveden v technických podmínkách provozu v tzv. Technickém manuálu, který je zveřejněn na internetových stránkách Státní pokladny.

3.8 Sledování historie uživatele

Z důvodu zvýšení bezpečnosti má Uživatel IISSP možnost kontrolovat potenciální zneužití svého uživatelského účtu. Systém umožňuje zobrazit a kontrolovat historii pro následující typy informací:

- datum a čas posledního úspěšného přihlášení uživatele,
- datum a čas posledního neúspěšného přihlášení uživatele,
- datum a čas poslední úspěšné změny hesla,
- datum a čas poslední neúspěšné změny hesla,
- datum a čas poslední úspěšné změny certifikátu,
- datum a čas poslední neúspěšné změny certifikátu,
- seznam posledních transakcí vyvolaných pomocí menu Portálu IISSP.

Obrázek 13: Úvodní obrazovka Portálu – Historie uživatele

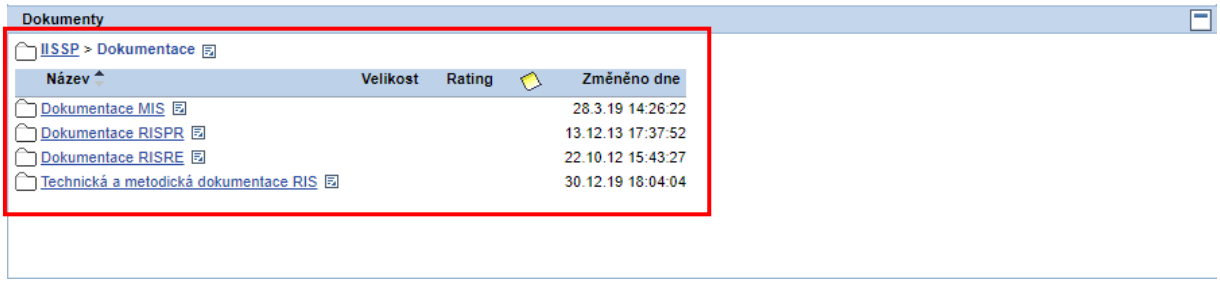


3.9 Dokumentace

Uživatelům IISSP je v prostředí Portálu IISSP zpřístupněna příslušná dokumentace. Jedná se zejména o uživatelskou dokumentaci, školicí materiály a další podklady související s prací uživatelů v prostředí IISSP.

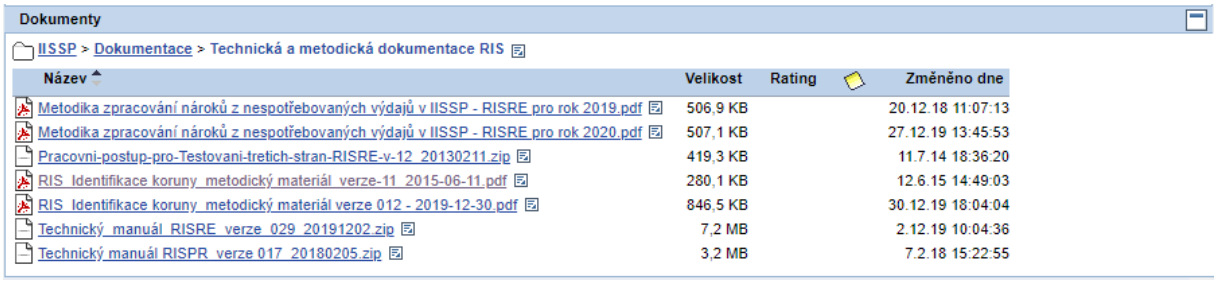
Uživateli je tato dokumentace zpřístupněna pomocí záložek, díky kterým může nalézt a vybrat příslušný dokument.

Obrázek 14: Přístup k dokumentaci



Pro přístup na dokument stačí kliknout na příslušný název souboru.

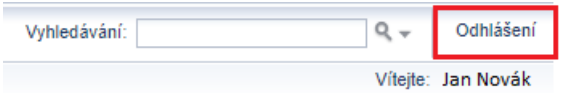
Obrázek 15: Přístup k dokumentaci – otevření souboru



3.10 Odhlášení z Portálu IISSP

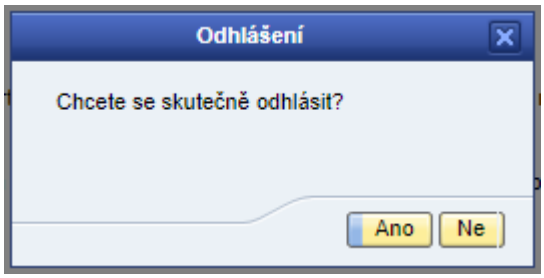
Pro ukončení práce s Portálem se Uživatel IISSP musí odhlásit pomocí portálového tlačítka Odhlášení. **Nepostačuje pouze zavřít okno internetového prohlížeče.**

Obrázek 16: Odhlášení z Portálu



Pracovní postup:

1. Uživatel stiskne tlačítko ***Odhlášení***.
2. Uživatel je dotázán, zda se chce skutečně odhlásit:



3. **Výsledek**: Uživatel IISSP je odhlášen z Portálu IISSP a všechny jeho činnosti jsou ukončeny. Z bezpečnostních důvodů uživatel pokračuje dle následujícího informačního sdělení. Pokud to verze internetového prohlížeče umožňuje, dojde k pokusu o automatické uzavření okna. V opačném případě je nutné, aby tuto akci provedl uživatel ručně.

Obrázek 17: Korektní odhlášení z Portálu IISSP

Uživatelům IISSP doporučujeme uzavírat aplikace <u>výhradně</u> pomocí tlačítek „Ukončit“ uvnitř aplikace, nikoliv uzavírání okna aplikací křížkem v pravém horním rohu okna aplikace.

3.11 Komunikace s Kompetenčním centrem IISSP

V případě problémů, nejasností nebo nutnosti asistence ze strany podpory provozu kontaktujte Kompetenční centrum IISSP, a to :

- Telefonicky:
  - **225 515 890** (pro MF a IISSP),
  - **225 515 891** (pro GFŘ),
- E-mailem:**servicedesk@spcss.cz.**

4. Elektronický podpis v prostředí IISSP

4.1 Aplikace ASD WebSigner

IISSP umožňuje při vytvoření nebo změně vybraných datových objektů opatřit je elektronickým podpisem. Pro zajištěné této funkcionality je používána nově komponenta ASD WebSigner.
Komponenta ASD WebSigner slouží pro vytvoření elektronického podpisu pomocí osobního certifikátu v prostředí web prohlížeče. Jedná se zejména o podpis relevantních objektů modulu RISRE.

Komponenta ASD WebSigner vyžaduje instalaci klienta na stanici uživatele. Možnosti provedení instalace a její postup je uveden v dokumentu Technický manuál – Příručka administrátora, kapitola 2.2.6 ASD WebSigner.

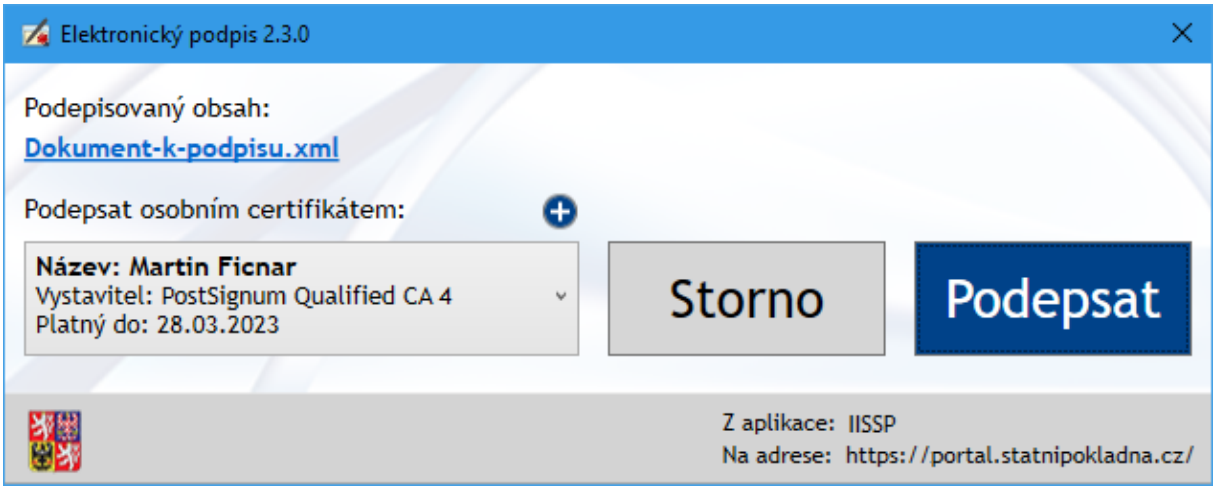
4.2 Vytvoření elektronického podpisu v prostředí portálu IISSP

Aplikaci nespouští uživatel, je spuštěna automaticky při vyvolání funkcionality vytvoření elektronického podpisu v uživatelském prostředí portálu IISSP.

Funkce vytvoření elektronického podpisu je uživatelům IISSP dostupná na příslušných místech portálu IISSP. Po aktivaci tlačítka „Elektronicky podepsat“ se systém pokusí spustit aplikaci na uživatelské stanici. Prohlížeč může zobrazit upozornění na spouštění externí aplikace, ve kterém je nutno spuštění povolit. V některých prohlížečích může být k dispozici volba pro zapamatování si volby, tak aby při příštím spuštění podpisu již toto upozornění nebylo zobrazeno.

V případě, že na klientské stanici není klient nainstalován, nabídne systém jeho instalaci (pro instalaci jsou potřebná běžná oprávnění uživatele k instalaci SW na stanici uživatele, v případě problémů kontaktujte svého administrátora koncových zařízení).

Po aktivaci se otevře okno aplikace pro vytvoření elektronického podpisu:



Obrázek 18: Uživatelské prostředí pro vytvoření elektronického podpisu

Pro uživatele jsou dostupné následující funkcionality:

Sekce „Podepisovaný obsah:“

V sekci „Podepisovaný obsah:“ je uveden název podepisovaného souboru. Kliknutím na tento název dojde ke zobrazení podepisovaného dokumentu v Internetovém prohlížeči (v nové záložce). Pro provedení podpisu není zobrazení dokumentu povinné, je to jen možnost.

Sekce „Podepsat osobním certifikátem:“

V sekci „Podepsat osobním certifikátem:“ je k dispozici rozbalovací seznam s nabídkou dostupných časově platných osobních certifikátů. Automaticky jsou nabídnuty všechny časově platné certifikáty z Windows úložiště certifikátů ze složky „Osobní“ a z aktuálně připojených HW Tokenů / karet napojených na Windows úložiště certifikátů CSP. Dále jsou nabídnuty certifikáty ze všech zaregistrovaných PXF/p12 a PEM souborů, postup jejich registrace (další certifikáty je možné přidat využitím ikony „+“) je v dokumentu Technický manuál – Příručka administrátora, kapitola 2.2.6.3 Konfigurace certifikátů pro podpis.

Před vlastním vytvořením elektronického podpisu je nutno zvolit, kterým certifikátem má být podpis proveden. Po prvním podpisu je volba certifikátu zapamatována tak, aby při dalších podpisech nebylo nutno certifikát znovu vybírat. Volbu lze kdykoliv změnit novým výběrem požadovaného certifikátu před podpisem. Pokud není zvolen žádný certifikát, tlačítko „Podepsat“ je nedostupné a nelze provést elektronický podpis.

Některé nabídnuté certifikáty mohou být označeny červenou barvou. Při jejich výběru je zobrazen text s důvodem, proč daný certifikát nemůže být použit dle požadavků aplikace IISSP. V případě volby takového certifikátu je tlačítko „Podepsat“ nedostupné a nelze provést elektronický podpis.

Tlačítko „Podepsat“

Pokud jsou splněny všechny výše uvedené podmínky, tak je tlačítko „Podepsat“ dostupné a kliknutím na něj se spustí proces elektronického podpisu. Pokud je privátní klíč chráněn heslem nebo HW Token/karta PINem, je zobrazeno okno pro zadání hesla či PINu. Při zadání chybného hesla/PINu je uživatel upozorněn a vyzván k opakovanému zadání. Pokud je přístup k privátnímu klíči certifikátu na HW Tokenu/kartě chráněn navíc sekundárním PINem, tak je uživatel vyzván i k zadání tohoto druhého PINu. Po dokončení elektronického podpisu je okno aplikace uzavřeno a uživatel je vrácen zpět do Internetového prohlížeče, odkud podepisování vyvolal a kde je zobrazen výsledek elektronického podpisu.

Tlačítko „Storno“

Pokud uživatel nechce dokument elektronicky podepsat, může celý proces přerušit bez podepsání kliknutím na tlačítko „Storno“. Stejný efekt má i kliknutí na křížek v záhlaví okna. Okno aplikace je tímto uzavřeno a uživatel je vrácen zpět do Internetového prohlížeče, odkud podepisování vyvolal a kde je zobrazena informace o přerušení podepisování uživatelem.

5. Bezpečnost

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

5.1 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.

5.2 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 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.

5.3 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.

5.4 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 e-maily z IISSP, které obsahují požadavek na okamžitou reakci, podle vzorů v platné dokumentaci, , 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.

5.5 Ochrana proti clickjackingu

Při útoku nazývanému 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 korektně odhlásil a následně zavřel okno internetového prohlížeče.

5.6 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.

5.7 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 o zpracování osobních údajů č. 110/2010 Sb. Mezi osobní údaje patří i jméno a příjmení ve spojení s trvalým bydlištěm uživatele.

5.8 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.

5.9 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, která má 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.

5.10 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.