

Postup pro vytvoření žádosti o digitální certifikát pro přístup k ISZR a ISSS pomocí aplikace

Verze dokumentu:	2.0
Datum vydání:	18. srpna 2023
Klasifikace:	Veřejný dokument

Obsah

1. Žádost o certifikát	3
2. Postup s aplikací Vytváření žádostí o certifikáty pro AIS v OS Microsoft Windows	3
2.1 Tvorba žádosti o certifikát	4
2.2 Alternativní DNS jméno	6
2.3 Generování klíčového páru	7
2.4 Vytvoření žádosti o certifikát	7
2.5 Spojení certifikátu se soukromým klíčem	9
2.6 Opětovné uložení certifikátu vytvořeného v minulosti	13
3. Použití certifikátu a soukromého klíče	13

1. Žádost o certifikát

Certifikáty vydávané Certifikační autoritou (CA) Digitální a informační agentury (DIA) slouží k identifikaci a autentizaci agendových informačních systémů (AIS) vůči ISZR (Informační systém základních registrů), ISSS (Informační systém sdílené služby, dříve eGSB) a vůči jiným AIS.

Vydávání certifikátů Certifikační autoritou DIA **pro produkční prostředí** základních registrů a ISSS se řídí Certifikační politikou DIA pro vydávání certifikátů pro AIS. Tato politika je dostupná na webu DIA (<https://www.szrcr.cz>). **Pro testovací prostředí** základních registrů a ISSS certifikační politika neexistuje, ale DIA postupuje při vydávání certifikátů pro testovací prostředí základních registrů a ISSS obdobně jako pro produkční prostředí.

Technický postup pro generování klíčů a žádosti o certifikát je pro produkční a testovací prostředí základních registrů a ISSS stejný. Žádosti pro jednotlivá prostředí se liší v položce CisloAIS - viz dále. Správce AIS vyznačuje ve formuláři žádosti o vydání certifikátu, zda žádá certifikát pro produkční nebo testovací prostředí.

Žádost o certifikát podává správce AIS pro konkrétní AIS.

2. Postup s aplikací Vytváření žádostí o certifikáty pro AIS v OS Microsoft Windows

Aplikace obsahuje uživatelské rozhraní za pomoci kterého uživatel vyplňuje všechny potřebné informace k žádosti.

Aplikaci spustíte otevřením souboru GeneratorCertRAZR.exe.

První spuštění aplikace:

- Aplikace uživatele vyzve o vybrání adresáře, do kterého se budou následně vytvářet kopie všech žádostí (.txt nebo .csr), privátních klíčů (.key) a certifikátů spárovaných s privátním klíčem (.pfx). Obsah tohoto adresáře je v aplikaci následně zobrazen v záložce **Přehled žádostí a certifikátů**. Cestu k adresáři si aplikace uloží do konfiguračního souboru **FileSavePath.config**

Ver.: 1.0 (25.07.2023)

[Pomoc \(?\)](#)

CZ

Vytvoření žádosti o digitální certifikát

Správat žádost a certifikát

Přehled žádostí a certifikátů

O aplikaci

Hledat

Reset

	Typ	Název souboru	Typ souboru	Velikost souboru (kB)	Datum vytvoření	Platnost do
▶	Žádost	Mycsr_12345678_55...	.txt	1	28.07.2023	
	Žádost	Mycsr_17651921_77...	.txt	1	01.08.2023	
	Žádost	Mycsr_17651921_77...	.txt	1	01.08.2023	
	Privátní klíč	Private_Mycsr_1234...	.key	2	28.07.2023	
	Privátní klíč	Private_Mycsr_1765...	.key	2	01.08.2023	
	Privátní klíč	Private_Mycsr_1765...	.key	2	01.08.2023	

Historie žádostí podrobná nápověda na: [Nápověda pro přehled](#)

- Aplikace si zároveň vytvoří konfigurační soubor, ze kterého čerpá slovník a kódy zemí s názvem **appConfiguration.config**. Základní postup:
 - Vyplníte potřebné údaje pro žádost do formuláře a následně vytvoříte žádost o certifikát. V tomto kroku se zároveň vytvoří soubor s privátním klíčem, který použijete v následujícím kroku.
- V aplikaci RAZR požádejte o vydání certifikátu pro vámi spravovaný AIS a soubor s žádostí připojte jako přílohu.
- Žádost o certifikát se odešle do webové služby s certifikační autoritou a nechá se podepsat.
- Podepsaný certifikát se následně nahraje do vámi vytvořené žádosti. • V aplikaci podepsaný certifikát spárujete s privátním klíčem, který vám vznikl při tvorbě žádosti. (Aplikace se pokusí o automatické vyhledání privátního klíče v adresáři s privátními klíči a pokud ho nalezne, přiřadí ho automaticky. Pokud klíč nalezen nebyl, můžete jej vyhledat ručně na jiném místě v počítači)
- Certifikát a soukromý klíč nainstalujete na server s AIS.

2.1 Tvorba žádosti o certifikát

Při vyplňování polí je nutné vyplnit alespoň pole označené hvězdičkou. Bez vyplnění těchto polí žádost vytvořena být nemůže.

Ver.: 1.0 (25.07.2023)

[Pomoc \(?\)](#) [CZ](#)

Vytvoření žádosti o digitální certifikát Spárovat žádost a certifikát Přehled žádostí a certifikátů O aplikaci

IČO správce AIS *

Název správce AIS

Obec sídla správce AIS

Ulice sídla správce AIS

PSČ sídla správce AIS

Číslo AIS *

DNS jméno serveru

Alternativní DNS jméno

Kód země CZ Czech Republic

Prostředí

☒ Testovací prostředí

☐ Produkční prostředí

AIS publikuje na ISSS

☐ Ano (publikační AIS nebo AIS správce údajů)

☒ Ne (čtenářský AIS)

Délka privátního klíče 3072

HASH funkce SHA384

Vytvoření žádosti

Vytváření žádosti o certifikát pro AIS
vyplnění žádosti podle pokynů:
[Nápověda pro tvorbu certifikátů](#)

Digitální a informační agentura

Požadovaný obsah jednotlivých položek je definován Certifikační politikou DIA pro vydávání certifikátů pro AIS.

Do jednotlivých položek uveďte:

IČO správce AIS

IČO správce AIS nebo identifikátor OVM v RPP, pokud správce AIS nemá IČO, (**číslo bez mezer**), délka maximálně 8 číslic, lze včetně nul na začátku i bez nich, např. 00345678 nebo 345678.

Název správce AIS

Název správce AIS (**bez diakritiky – je odstraněna po opuštění pole**), maximální délka 128 znaků, např. Sprava zakladnich registru

Obec sídla správce AIS

Jméno obce (**bez diakritiky – je odstraněna po opuštění pole**), např. Hradec Kralove

Ulice sídla správce AIS

Jméno ulice (**bez diakritiky – je odstraněna po opuštění pole**), např. Milady Horakove

PSČ sídla správce AIS

PSČ (**bez mezer**), např. 11025

Číslo AIS

Identifikace (**číslo**) AIS v RPP, nebo identifikátor přidělený DIA (nebo dříve SZR) v případě, že AIS není v RPP.

DNS jméno serveru

Do položky vyplňte nějaké jméno, ze kterého bude poznat, o jaký AIS se jedná. Maximální délka 64 znaků.

Příklady: spis.subjekt.cz **Upozornění.**

DNS musí být ve validním FQDN formátu. V případě, že chcete, aby AIS vystupoval vůči ISSS jako publikační, uveďte DNS jméno, které je součástí URL, na kterém ISSS s AIS komunikuje. A toto jméno musí být z domény cms2.cz.

Příklad: server.vaseovm.cms2.cz

Poznámka.

Doporučujeme uvádět DNS jméno, které odpovídá IP adrese, ze které bude AIS komunikovat s ISZR, respektive ISSS. Pokud bude spojení navazováno v KIVS, mělo by jít o jméno, pod kterým je počítač dosažitelný v síti KIVS. Pokud bude spojení navazováno v Internetu, pak by mělo jít o DNS jméno z veřejné domény.

Příklady: server.vaseovm.cz
server.vaseovm.cms2.cz

Kód země

Kód státu (**dvě velká písmena**), např. CZ, musí jít o členský stát EU

Prostředí

Určuje, pro jaké prostředí je žádost vystavována. Pokud se jedná o **Testovací prostředí**, je do organizationUnitName k Číslu AIS přidáno /TEST. Pokud se jedná o **Produkční prostředí**, je k Číslu AIS přidáno /PROD

AIS publikuje na ISSS

Určuje, zda jde o AIS který publikuje na ISSS. Pokud se jedná o AIS publikační, musí být **DNS jméno serveru** NEBO první DNS z **Alternativní DNS jméno** z domény cms2.cz. Pokud jde o žádost pro čtenářský AIS, kontroly na domény se neprovádí.

Pokud se jedná o publikační AIS, je do organizationUnitName za Číslo AIS přidána hodnota -P.

Pokud se jedná o čtenářský AIS, je do organizationUnitName za Číslo AIS přidána hodnota -E.

Délka privátního klíče Určuje délku privátního klíče použitého pro zašifrování žádosti. Výchozí hodnota je 3072..

HASH funkce

Určuje jakou hash funkcí bude žádost zašifrována

Povinné položky jsou:

- IČO správce AIS: musí přesně odpovídat IČO správce AIS nebo identifikátoru OVM v RPP, pokud OVM nemá IČO
- Číslo AIS: musí přesně odpovídat číslu AIS

2.2 Alternativní DNS jméno

Alternativní DNS jméno je potřebné v následujících situacích:

- Potřebujete vydat certifikát pro více DNS jmen.
- Potřebujete použít certifikát pro komunikaci s nějakým AIS, který vyžaduje mít vyplněný atribut SAN.

Poznámka: ISZR ani ISSS nevyžadují vyplněný atribut SAN.

V obou případech použijte pole **Alternativní DNS jménu**. Jednotlivé DNS jména oddělte středníky.

2.3 Generování klíčového páru

Po vytvoření žádosti se na stejné místo jako soubor s žádostí zároveň vytvoří soubor s privátním klíčem. Soubor má vždy stejný název jako korespondující žádost o certifikát s předponou "Private_" a má příponu .key.

Příklad:

Certifikát: Myscr_12345678_1234_Test.txt

Privátní klíč: Private_Myscr_12345678_1234_Test.key

2.4 Vytvoření žádosti o certifikát

Vytvoření žádosti provedete stisknutím tlačítka **Vytvoření žádosti**. Po stisknutí tlačítka budete vyzváni k zadání hesla a jeho kontrole.

Ver.: 1.0 (25.07.2023)

Vytvoření žádosti o digitální certifikát | Spárovat žádost a certifikát | Přehled žádostí a certifikátů | O aplikaci

Vytváření žádosti o certifikát pro AIS
vyplnění žádosti podle pokynů:
[Nápověda pro tvorbu certifikátů](#)

IČO správce AIS * 12345678

Název správce AIS Test

Obec sídla správce AIS Test

Ulice sídla správce AIS Test 123

PSČ sídla správce AIS 12345

Číslo AIS * 1234

DNS jméno serveru

Alternativní DNS jméno

Kód země CZ Czech Republic

Prostředí

☒ Testovací prostředí

☐ Produkční prostředí

AIS publikuje na ISSS

☐ Ano (publikační AIS nebo AIS správce údajů)

☒ Ne (čtenářský AIS)

Délka privátního klíče 3072

HASH funkce SHA384

Vytvoření žádosti

Heslo

Potvrdit

Odeslat

Digitální a informační agentura

Výsledkem provedení vytvoření žádosti jsou 2 soubory. První je soubor s žádostí ve formátu .txt a druhý je soubor s privátním klíčem ve formátu .key. Tyto dva soubory se uloží na místo vybrané uživatelem a zároveň se vytvoří do výchozího adresáře pro zobrazení v přehledu.

▼ c:\Temp\RAZR\testdata\dok Testing*.*

Name	Ext	Size	↓ Date	Attr
<DIR> 02.08.2023 15:23 ----				
Mycsr_12345678_1234_Test	txt	1 384	02.08.2023 15:23	-a--
Private_Mycsr_12345678_1234_Test	key	2 622	02.08.2023 15:23	-a--

Obsah žádosti si můžete zobrazit na záložce **Přehled žádostí a certifikátů** kliknutím na řádek s žádostí:

DIGITÁLNÍ A INFORMAČNÍ AGENTURA Vytváření žádostí o certifikáty pro AIS

Ver.: 1.0 (25.07.2023) [Pomoc \(?\)](#) CZ

Vytvoření žádosti o digitální certifikát Spárovat žádost a certifikát **Přehled žádostí a certifikátů** O aplikaci

Hledat Reset

	Typ	Název souboru	Typ souboru	Velikost souboru (kB)	Datum vytvoření	Platnost do
▶	Žádost	Mycsr_12345678_12...	txt	1	02.08.2023	
	Žádost	Mycsr_12345678_55...	txt	1	28.07.2023	
	Žádost	Mycsr_17651921_77...	txt	1	01.08.2023	
	Žádost	Mycsr_17651921_77...	txt	1	01.08.2023	
	Privátní klíč	Private_Mycsr_1234...	key	2	02.08.2023	
	Privátní klíč	Private_Mycsr_1234...	key	2	28.07.2023	
	Privátní klíč	Private_Mycsr_1765...	key	2		
	Privátní klíč	Private_Mycsr_1765...	key	2		

Informace o žádosti:
Organization: 12345678
Organization Unit: 1234-E/TEST
Locality: Obec=Test,Ulice=Test 123,PSC=12345
State: Test
Country: CZ

OK

Historie žádostí podrobná nápověda na: [Nápověda pro přehled](#)

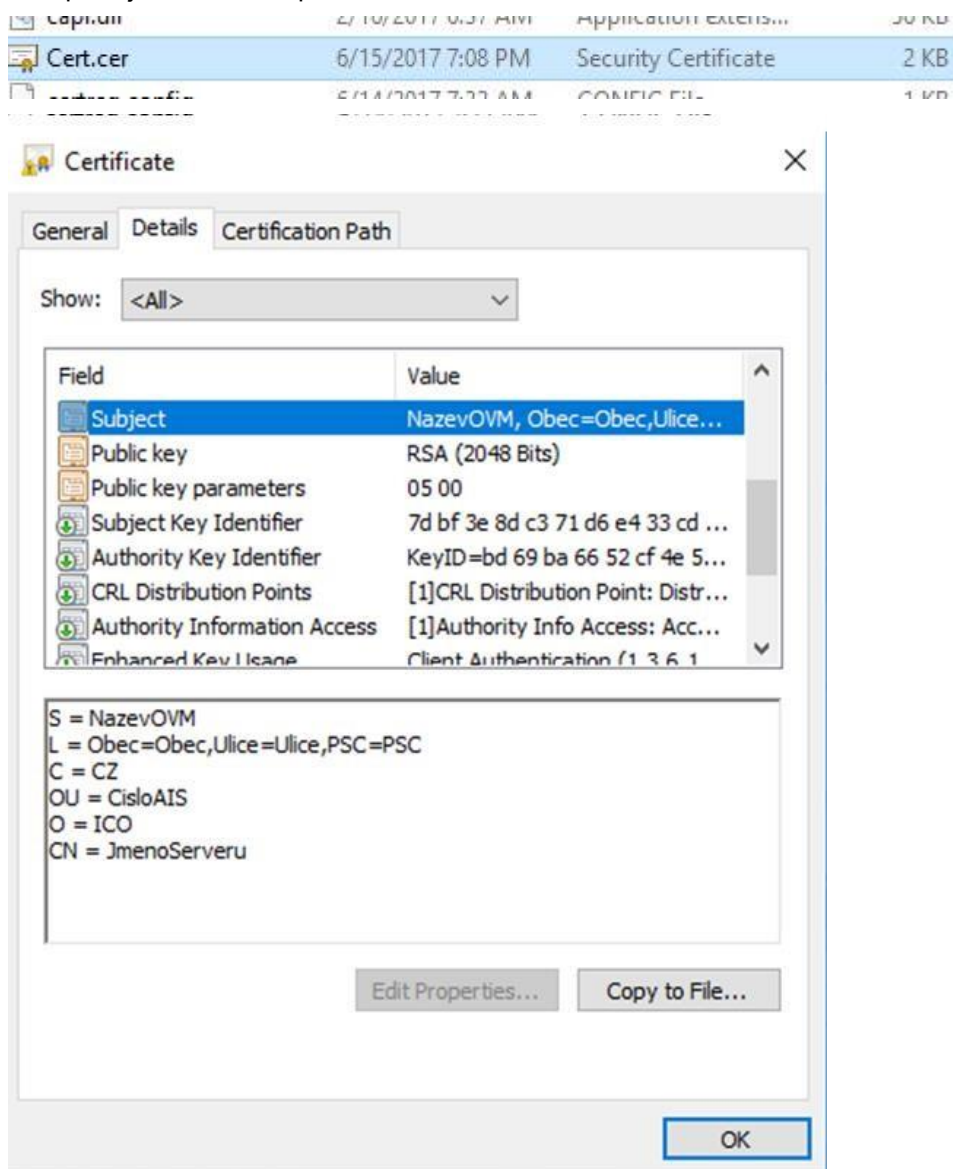
Soubor s žádostí pošlete v příloze formuláře vyplněného v aplikaci RAZR k certifikaci vašeho veřejného klíče.

Soubor se soukromým klíčem si schovejte. Budete jej potřebovat při párování podepsaného certifikátu pro vytvoření .pfx.

Pokud bude certifikace úspěšná, obdržíte do aplikace RAZR soubor s certifikátem se stejným názvem jako byla žádost. Soubor se nahraje do záznamu s vámi vytvořenou žádostí v aplikaci RAZR. Podepsaný certifikát si uložte na svůj počítač pro další zpracování.

Zkontrolujte obsah certifikátu, že skutečně odpovídá vaší žádosti! Kontrolu můžete provést nakopírováním podepsaného certifikátu do adresáře, který jste vybral při prvním spuštění aplikace. Následným kliknutím na řádek s Podepsaným certifikátem v záložce Přehled žádostí a certifikátů se vám zobrazí informace o certifikátu.

nebo použijte standardní prohlížeč certifikátů MS Windows:



2.5 Spojení certifikátu se soukromým klíčem

Proces musíte dokončit spojením certifikátu se soukromým klíčem.

Ná záložce **Spárovat žádost a certifikát** si v poli **Certifikát** vyhledejte soubor s podepsaným certifikátem z certifikační autority. Musí se jednat o soubor ve formátu .cer, .txt nebo .crt.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA Vytváření žádosti o certifikáty pro AIS

Ver.: 1.0 (25.07.2023) Pomoc (?) CZ

Vytvoření žádosti o digitální certifikát Spárovat žádost a certifikát Přehled žádostí a certifikátů O aplikaci

Certifikát Hledat

Vyhledat privátní klíč k certifikátu

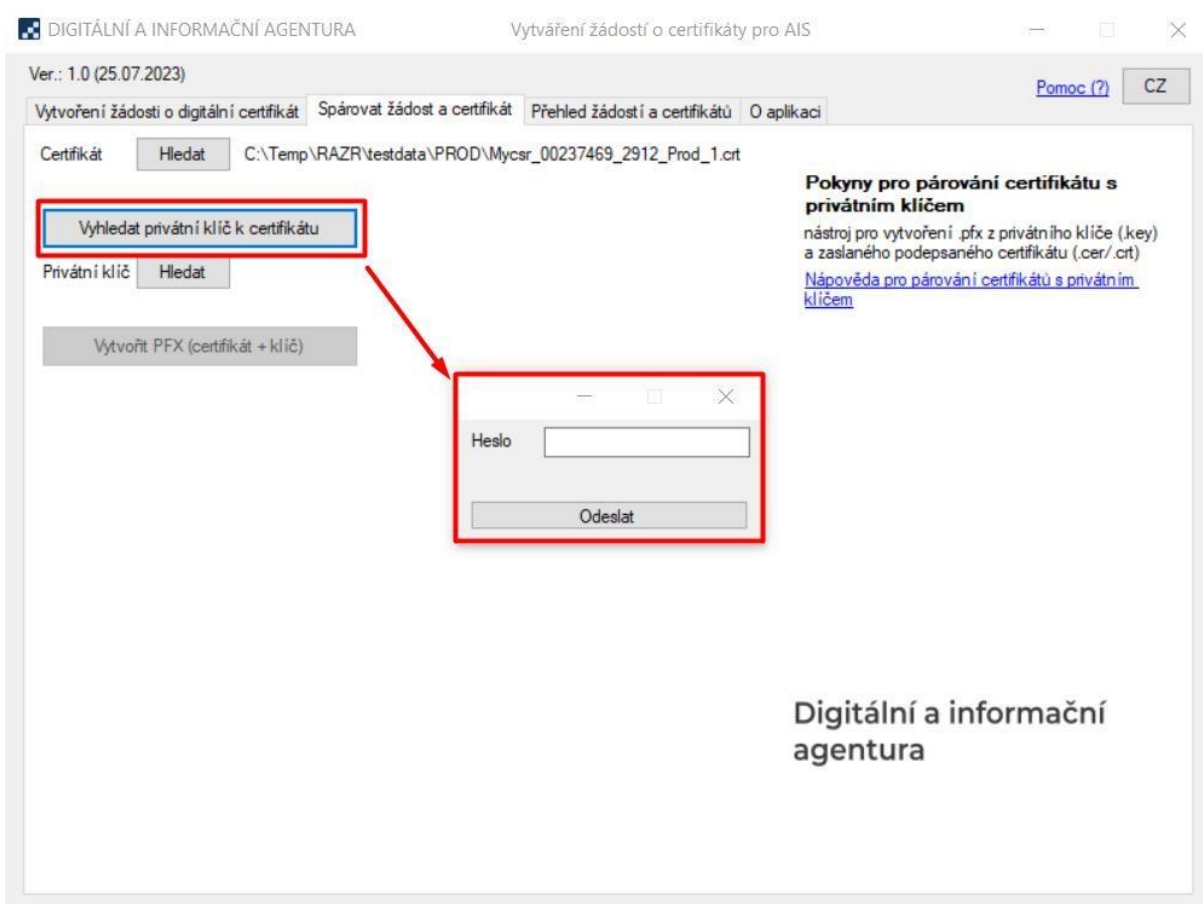
Privátní klíč Hledat

Vytvořit PFX (certifikát + klíč)

Pokyny pro párování certifikátu s privátním klíčem
nástroj pro vytvoření .pfx z privátního klíče (.key) a zaslaného podepsaného certifikátu (.cer/.crt)
[Nápověda pro párování certifikátů s privátním klíčem](#)

Digitální a informační agentura

Následně se můžete pokusit o automatické vyhledání privátního klíče tlačítkem **Vyhledat privátní klíč k certifikátu**. Tlačítko se odblokuje, jakmile nahrajete soubor s certifikátem. Po stisknutí tlačítka vás aplikace vyzve k zadání hesla pro privátní klíč (jedná se o heslo, které jste zadávali při vytváření žádosti).



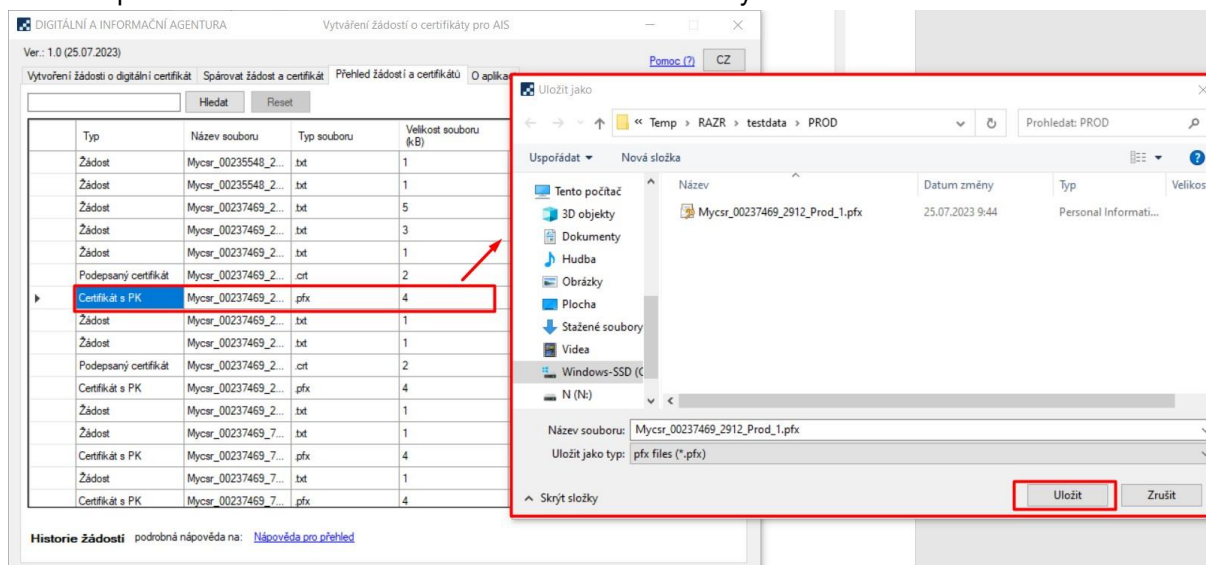
Pokud soubor s privátním klíčem v adresáři existuje a pokud jste zadali validní heslo, bude do pole **Privátní klíč** vyplněna cesta k souboru.

Následně je možné stisknout tlačítko **Vytvořit PFX (certifikát + klíč)**, čímž vás aplikace vyzve k vybrání místa, kam se certifikát spárovaný s privátním klíčem uloží.

Pokud klíč nebyl nalezen automaticky, je možné jej vybrat ručně. Kliknutím na tlačítko **Hledat** u pole **Privátní klíč**, vám aplikace umožní vybrat soubor s privátním klíčem kdekoliv v počítači. Po jeho ručním vybrání vám aplikace odblokuje tlačítko **Vytvořit PFX (certifikát + klíč)**. Po jeho stisknutí zadáte heslo pro vybraný privátní klíč a pokud je heslo validní a vybraný privátní klíč je validní k vybranému certifikátu, umožní vám aplikace uložit certifikát na vámi vybrané místo.

2.6 Opětovné uložení certifikátu vytvořeného v minulosti

Pokud si přejete uložit certifikát spárovaný s privátním klíčem, který jste vytvořili někdy v minulosti, můžete tak udělat na záložce **Přehled žádostí a certifikátů**. Kliknutím na řádek s typem **Certifikát s PK** vám aplikace umožní uložit soubor s certifikátem na vámi vybrané místo.



3. Použití certifikátu a soukromého klíče

Certifikáty jsou serverové, tj. vydávají se pro počítače, ne pro osoby.

Certifikát a soukromý klíč (Cert.pfx) nainstalujte na všechna zařízení (servery, komunikační sběrnice, SSL koncentrátoři, firewally atd.), která zajišťují šifrovanou komunikaci s ISZR, ISSS nebo jinými AIS. Pokud váš AIS požaduje soukromý klíč a certifikát v oddělených souborech, použijte Private.key a Cert.cer.

DIA doporučuje instalovat certifikáty a odpovídající soukromé klíče na pouze nezbytný počet serverů.

Soukromý klíč chraňte před zneužitím.

Certifikát používejte pouze pro ty účely, pro které byl vydán. Je zakázáno ho používat pro jiné AIS.

Povolené použití certifikátů vydaných pro produkční prostředí základních registrů je vymezeno Certifikační politikou DIA pro vydávání certifikátů pro AIS.