DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Návod na vytvoření žádosti o digitální certifikát s aplikací DIA

Verze dokumentu:	2.3
Datum vydání:	9. září 2024
Klasifikace:	Veřejný dokument

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Obsah

1. Vydávání certifikátů

Certifikáty vydávané Certifikační autoritou (CA) Digitální a informační agentury (DIA) jsou určené 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. **Pro testovací prostředí** základních registrů a ISSS certifikační politika neexistuje, ale DIA postupuje při vydávání certifikátů pro testovací prostředí 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. Správce AIS určuje v žádosti, zda žádá certifikát pro produkční nebo testovací prostředí.

Žádost o certifikát podává správce AIS pro konkrétní AIS.

Pro vytvoření žádosti je možné použít jakýkoli software, který vytváří žádosti o digitální certifikát podle příslušných standardů.

DIA doporučuje pro vytváření žádostí o certifikáty použít aplikaci GeneratorCertRAZR.

Tento dokument popisuje vytvoření žádosti o certifikát s použitím aplikace GeneratorCertRAZR, kterou vytvořila DIA.

2. Postup pro získání certifikátu

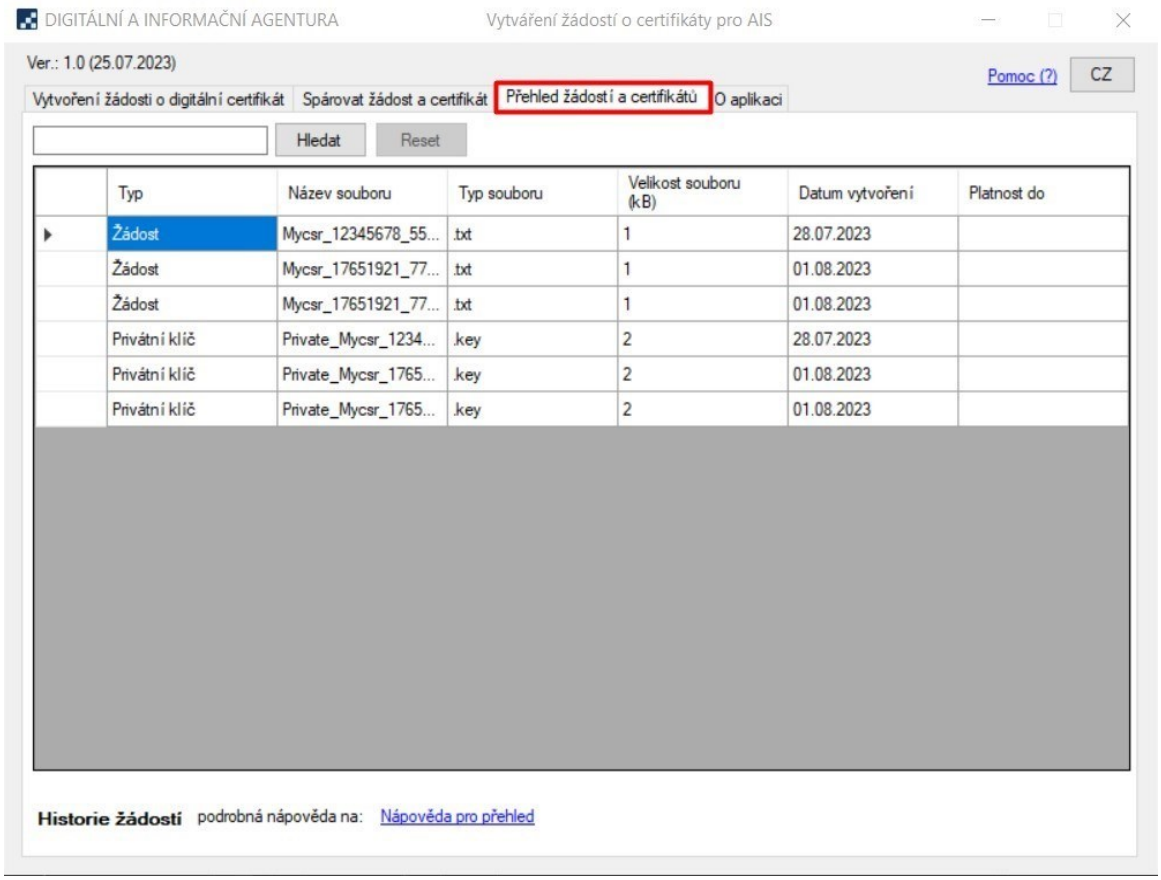
Aplikace GeneratorCertRAZR je volně dostupná a je možné ji stáhnout z webu DIA. Aplikace se neinstaluje, stačí ji nahrát na nějaký počítač s MS Windows a spustit ji otevřením souboru GeneratorCertRAZR.exe.

Základní postup.

- Vyplníte potřebné údaje pro žádost do aplikace GeneratorCertRAZR a vytvoříte žádost o certifikát. V tomto kroku se zároveň vytvoří soubor s privátním klíčem.
- V aplikaci RAZR (webová aplikace pro správu přístupů do základních registrů) požádáte o vydání certifikátu pro AIS a soubor s žádostí připojte jako přílohu.
- RAZR předá žádost o certifikát CA DIA.
- CA DIA vydá certifikát a předá ho aplikaci RAZR.
- RAZR zařídí odeslání certifikátu do vaší datové schránky a umožní vám stažení certifikátu přímo z aplikace RAZR.
- V aplikaci GeneratorCertRAZR můžete certifikát spárovat s privátním klíčem, který vznikl při tvorbě žádosti.
- Certifikát a soukromý klíč nainstalujete na všechna zařízení (servery, firewally, komunikační sběrnice, SSL koncentrátory, HSM apod.) tak, aby AIS mohl komunikovat s ISZR anebo s ISSS anebo s jinými AIS.

První spuštění aplikace.

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

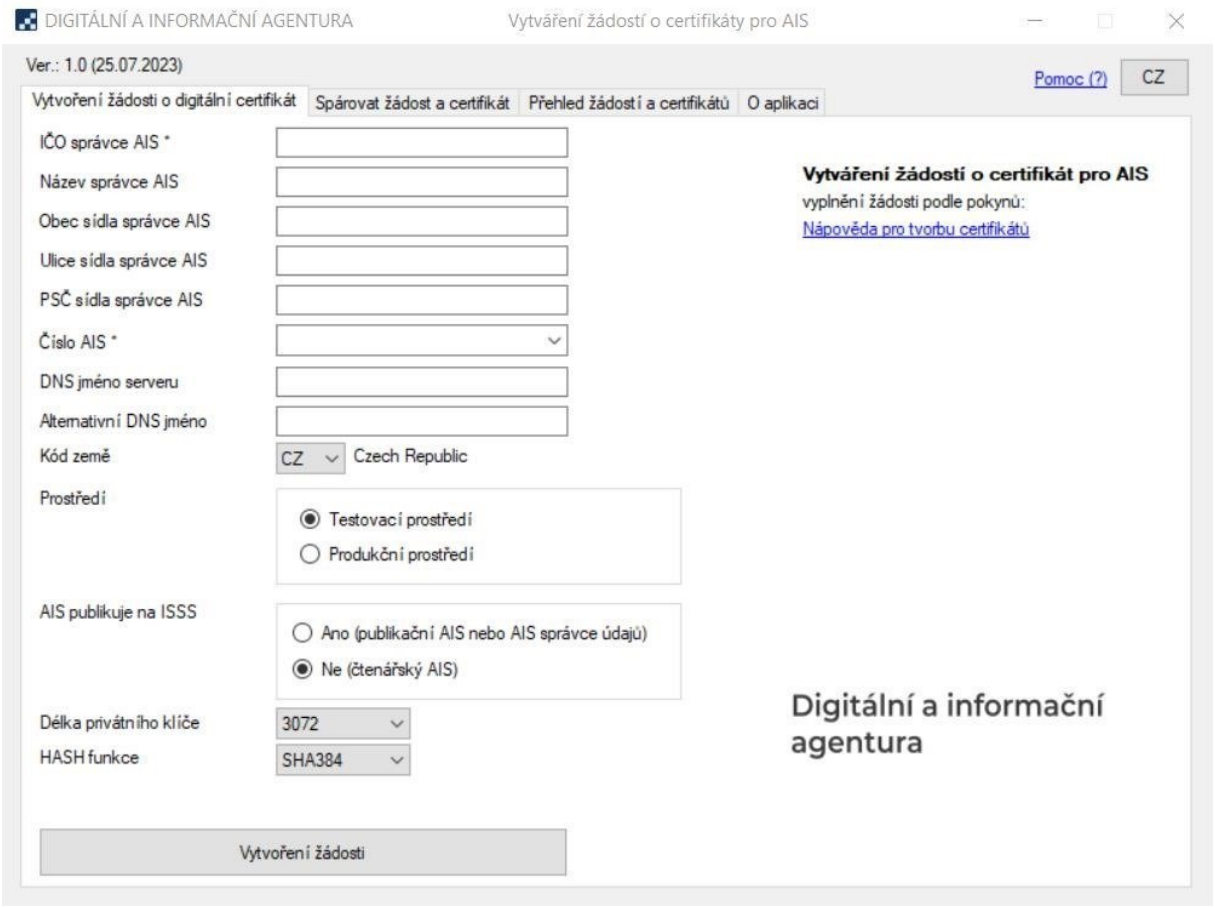


- Aplikace si zároveň vytvoří konfigurační soubor s názvem **GeneratorCertRAZR.ini**, ze kterého čte konfigurační data (mj. kódy zemí).

2.1 Vytvoření žádosti o certifikát

Aplikace obsahuje uživatelské rozhraní, kde uživatel vyplňuje všechny potřebné informace k žádosti.

Při zadávání vstupních dat je nutné vyplnit alespoň povinné položky (jsou označené hvězdičkou): IČO správce AIS a Číslo AIS.



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

Do jednotlivých položek zadáte:

IČO správce AIS

IČO správce AIS nebo identifikátor správce AIS 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. Digitalni a informacni agentura

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, **číslo 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, např. 584.

DNS jméno serveru

FQDN, ze kterého AIS komunikuje. Maximální délka 64 znaků. Např. spis.subjekt.cz

V případě, že chcete, aby AIS vystupoval vůči ISSS jako publikační, uveďte DNS jméno, které je součástí URL, na kterém ISSS s AIS komunikuje. Toto jméno musí být z domény cms2.cz s uvedeným číslem vašeho AIS, tj.

- aisXXXX.egsb.cms2.cz – produkční prostředí
- aisXXXX-test.egsb.cms2.cz – testovací prostředí

Příklady:

- ais1234.egsb.cms2.cz
- ais1234-test.egsb.cms2.cz

Pokud zde publikační AIS nebude mít jednu z výše uvedených možností, je potřeba ji uvést do alternativního DNS jména, viz dále.

Alternativní DNS jméno

Jedno nebo více FQDN oddělených středníky.

Rozšíření SAN (Subject Alternative Name) je potřebné v následujících situacích:

- Potřebujete vydat certifikát pro více DNS jmen.
- Pokud se jedná o publikační AIS a potřebujete vyplnit DNS jméno, které je součástí URL, na kterém ISSS s AIS komunikuje (a nebylo možné toto jméno uvést v rámci položky DNS jméno serveru). Uveďte jej ve formátu:
  - aisXXXX.egsb.cms2.cz – produkční prostředí
  - aisXXXX-test.egsb.cms2.cz – testovací prostředí

  Příklady:
  - ais1234.egsb.cms2.cz
  - ais1234-test.egsb.cms2.cz
- Potřebujete použít certifikát pro komunikaci s nějakým AIS, který vyžaduje mít vyplněný atribut SAN.
  Poznámka: ISZR ani ISSS nevyžadují vyplněný atritbut SAN.

Kód země

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

Prostředí

Určuje, pro jaké prostředí (produkce, test) ISZR a ISSS je žádost připravována.

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. Tj. DNS jméno nebo SAN je v takovém případě povinná položka.

Pokud jde o žádost pro čtenářský AIS, položka je nepovinná a kontroly na domény se neprovádí.

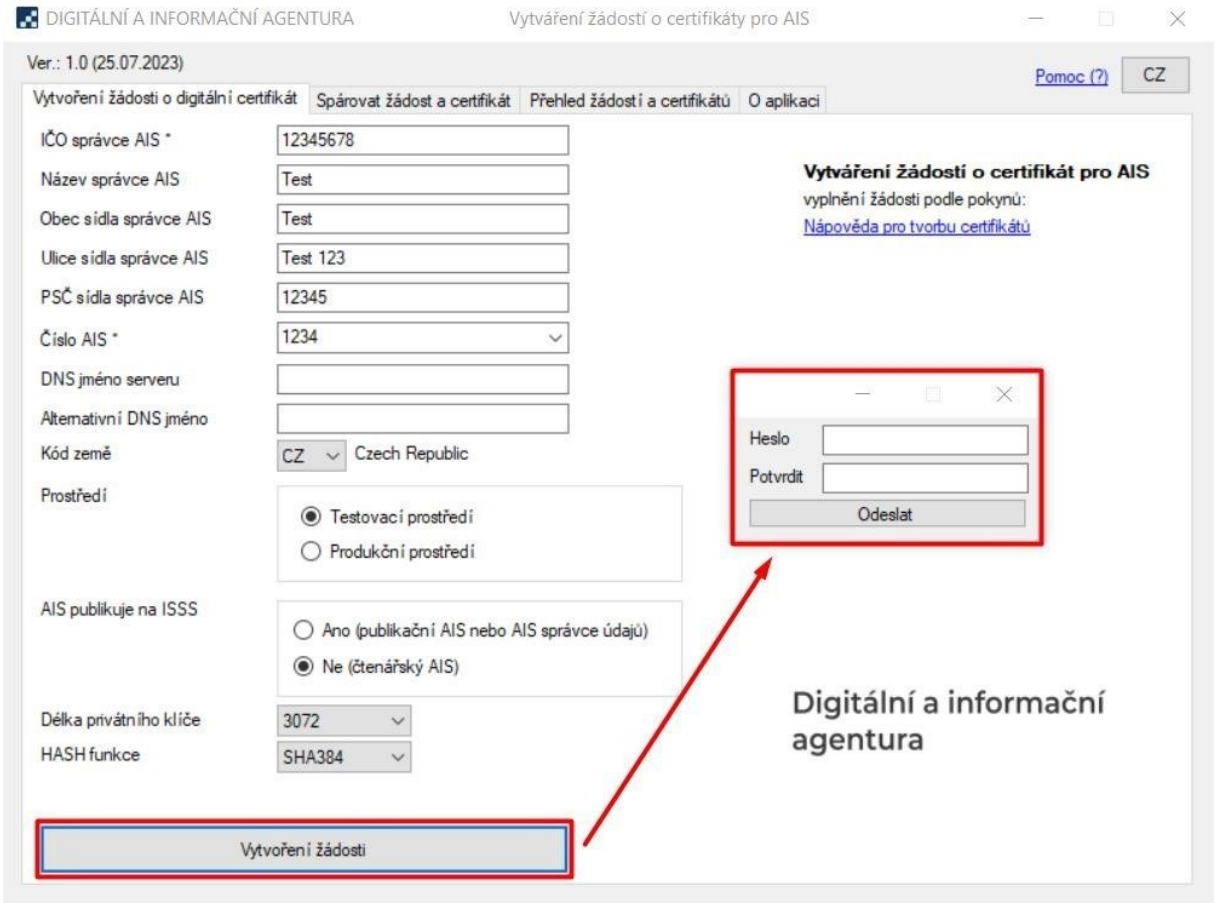
Délka privátního klíče

Určuje délku privátního (i veřejného) klíče RSA. Výchozí (a aktuálně neměnná) hodnota je 3072 bitů.

HASH funkce

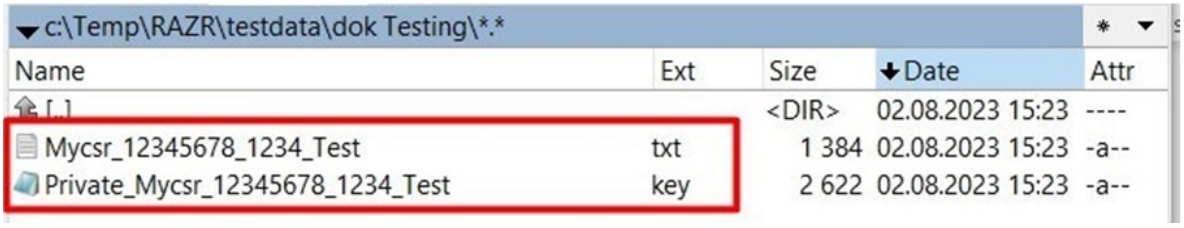
Určuje, jaká hash funkce bude použitá pro podpis žádosti. Výchozí hodnota je SHA384.

O vytvoření žádosti požádáte stisknutím tlačítka **Vytvoření žádosti**. Po stisknutí tlačítka budete vyzváni k zadání hesla, kterým bude chráněný soubor s privátním klíčem.



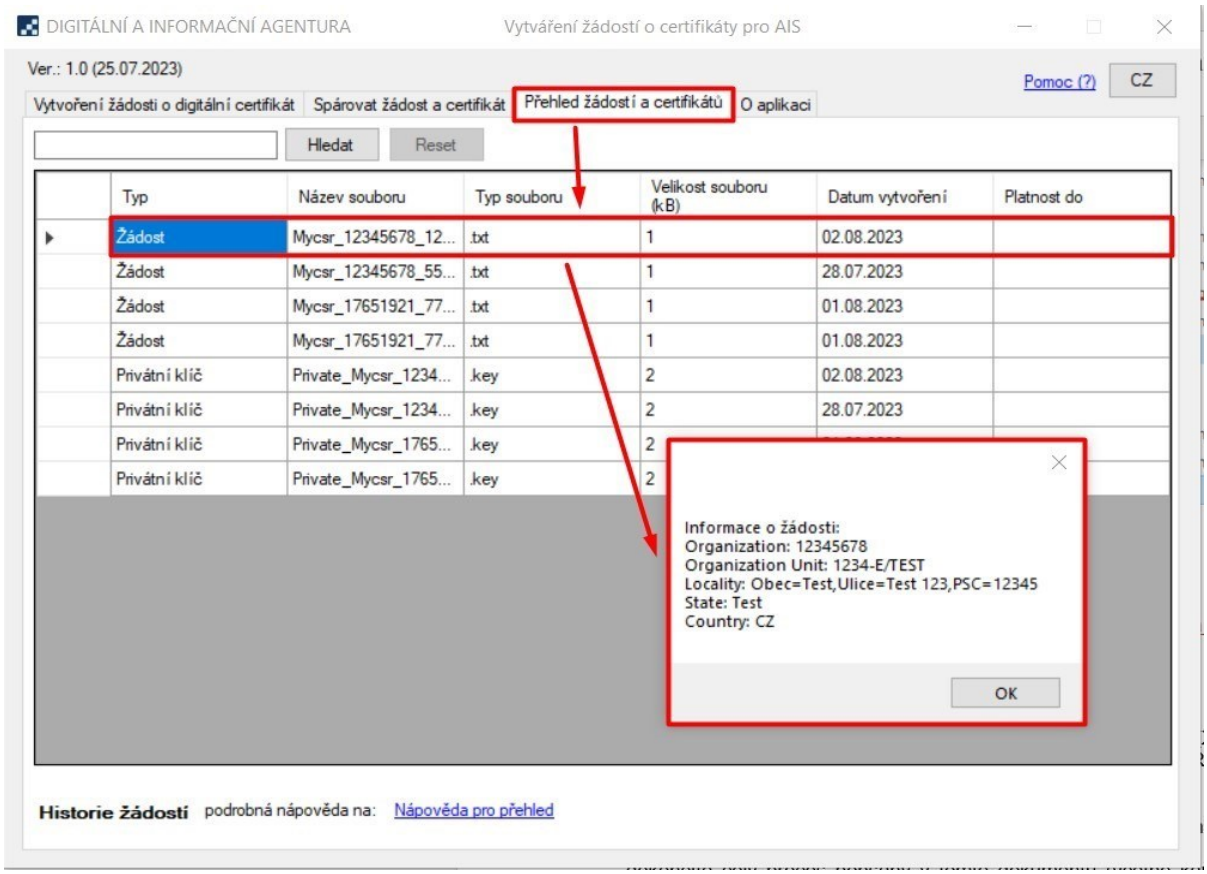
Aplikace vygeneruje dvojici klíčů (privátní a veřejný) a vytvoří žádost o certifikát.

Výsledkem jsou 2 soubory. První je soubor s žádostí (jméno souboru má příponu .txt) a druhý je soubor s privátním klíčem (jméno souboru má příponu .key). Tyto dva souboru aplikace uloží na místo vybrané uživatelem a zároveň je uloží do výchozího adresáře.



Pokud ve výchozím adresáři již soubor(y) se stejným jménem je (jsou), aplikace přidá do jména číslici, aby nedošlo k přepsání existujícího souboru. Tedy např.: Mycsr_2345678_1234_Test_1, Mycsr_2345678_1234_Test_2 atd.

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



2.2 Odeslání žádosti o certifikát

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

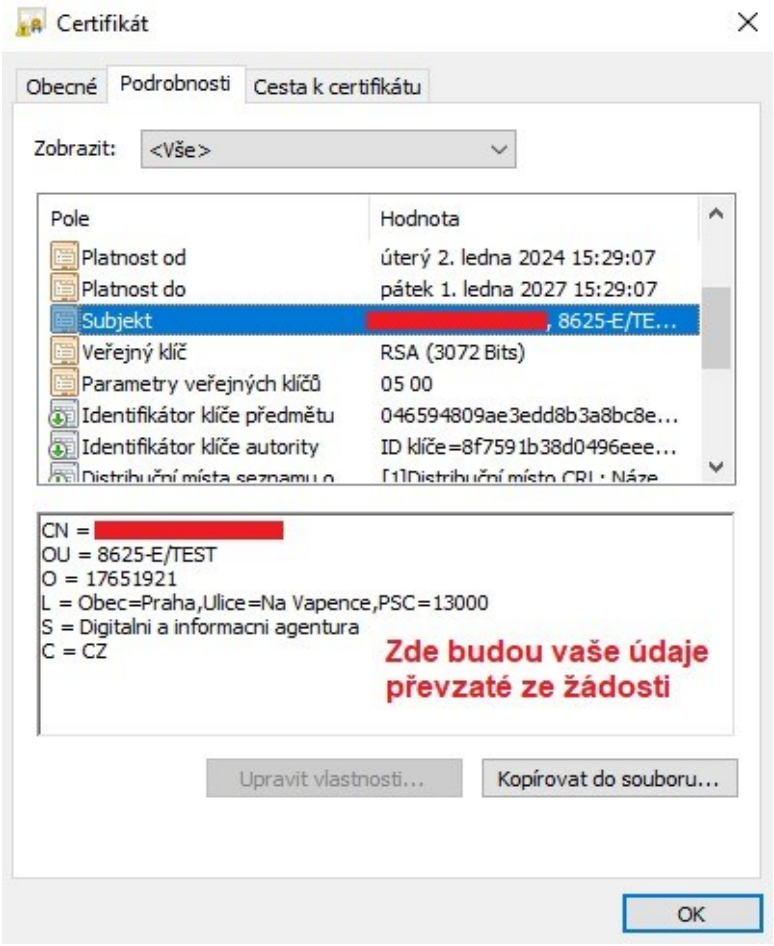
- RAZR z Internetu: https://razr.egon.gov.cz/
- RAZR z KIVS: https://razr.egon.cms2.cz/

2.3 Převzetí certifikátu

Pokud bude certifikace úspěšná, obdržíte do aplikace RAZR a do datové schránky soubor s certifikátem (se stejným názvem jako měla žádost). Certifikát si uložte na svůj počítač pro další zpracování.

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

Případně použijte standardní prohlížeč certifikátů MS Windows:

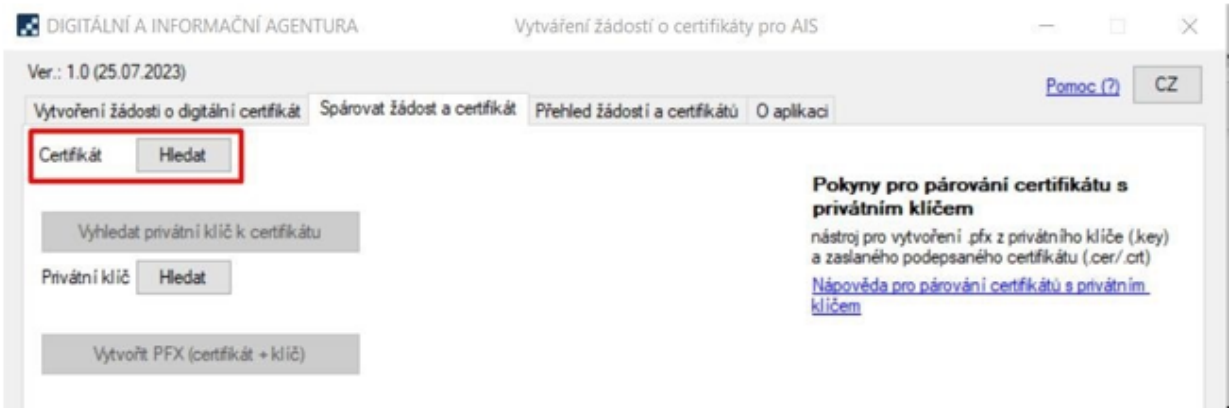


Poznámka: CN = Common name, tj. DNS jméno serveru.

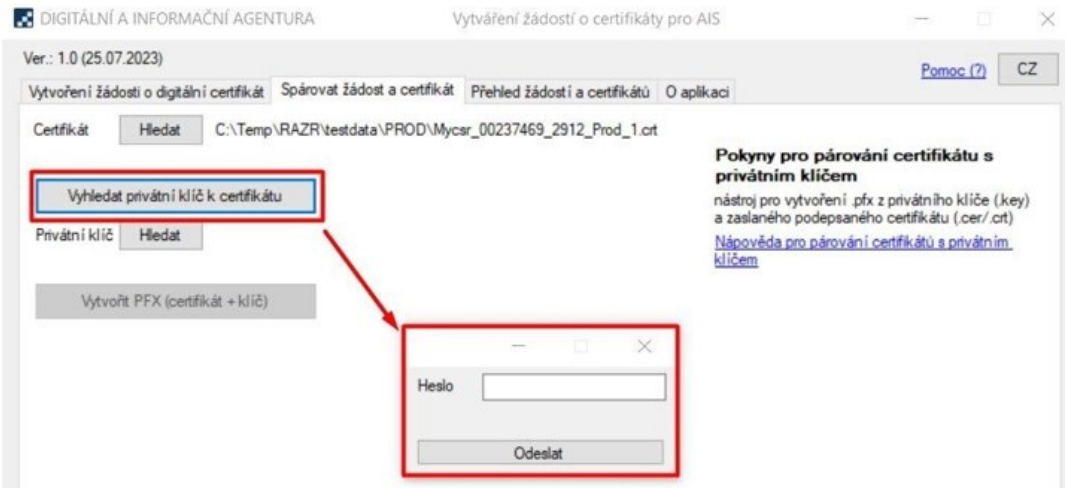
2.4 Spojení certifikátu se soukromým klíčem

Pokud váš AIS vyžaduje certifikát a privátní klíč v jednom souboru ve formátu PKCS12, můžete použít aplikaci GeneratorCertRAZR k vytvoření souboru v uvedeném formátu.

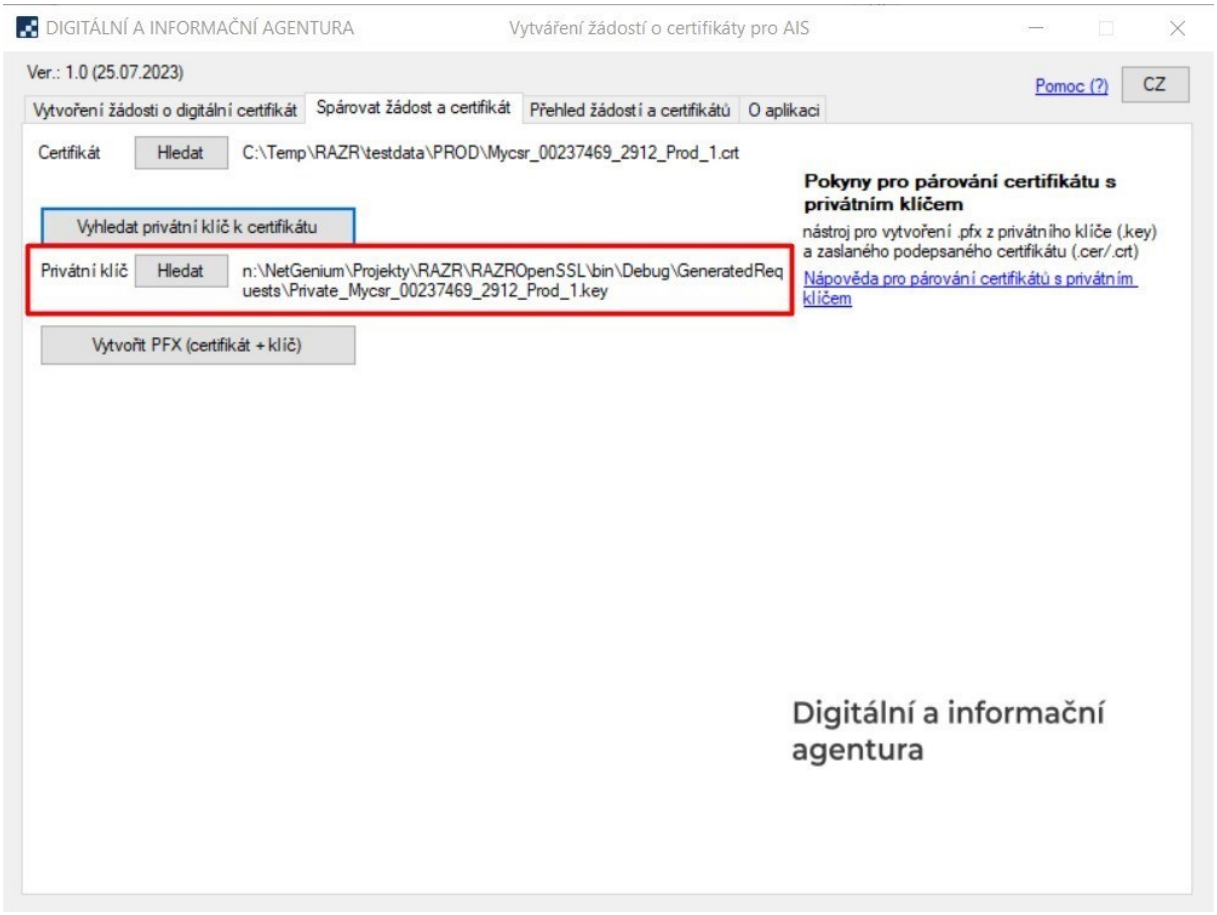
Na záložce **Spárovat žádost a certifikát** si v poli **Certifikát** vyhledejte soubor s certifikátem. Musí se jednat o soubor ve formátu .cer, .txt nebo .crt.



Následně se můžete pokusit o automatické vyhledání privátního klíče tlačítkem **Vyhledat privátní klíč k certifikátu**. Tlačítko se odblokuje, jakmile vyberete 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.

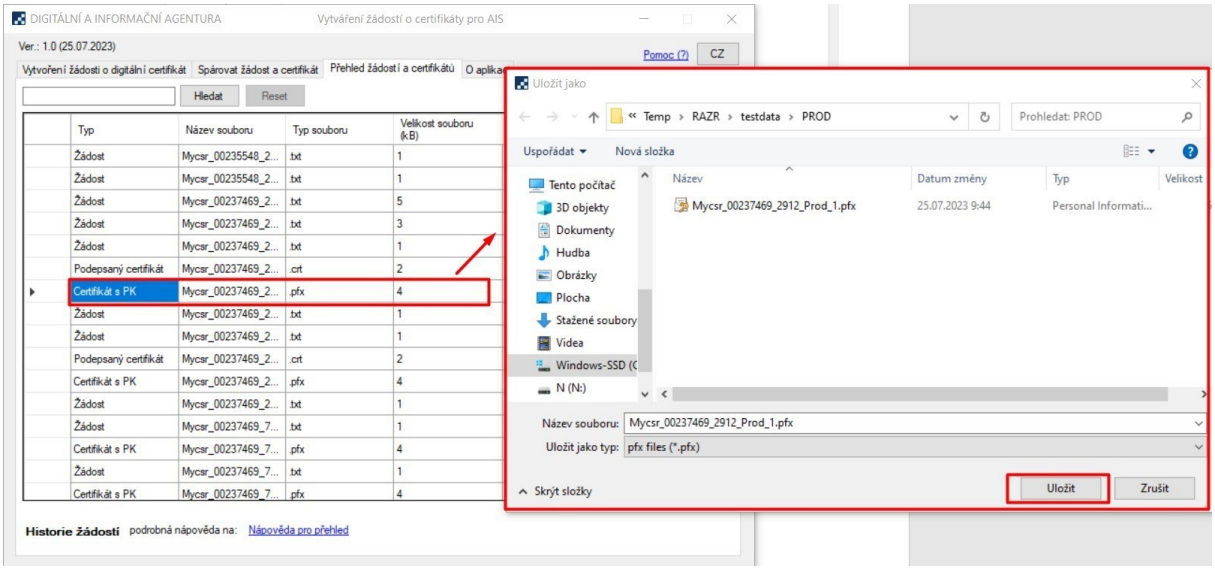


Po stisknutí tlačítka **Vytvořit PFX (certifikát + klíč)** vás aplikace vyzve k vybrání místa, kam se certifikát spárovaný s privátním klíčem uloží.

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 patří k vybranému certifikátu, umožní vám aplikace uložit pfx soubor na vámi vybrané místo.

2.5 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 nainstalujte na všechna zařízení (servery, komunikační sběrnice, SSL koncentrátory, firewally, HSM atd.), která zajišťují šifrovanou komunikaci s ISZR, ISSS nebo jinými AIS. Pokud váš AIS požaduje soukromý klíč a certifikát v oddělených souborech, použijte soubor se s privátním klíčem (.key) a soubor s certifikátem (.cer).

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.