Práce s certifikátem

Základní informace k certifikátům
Pro účely přihlašování a odesílání výkazů na CSÚIS je zapotřebí vlastnit platný **KOMERČNÍ** certifikát.
Pozor, existuje více druhů např. kvalifikovaný, ale ten je primárně určen k podepisování dokumentů).

Trocha teorie :

Komerční certifikát se skládá ze 2 částí :

a) Veřejná část
Obsahuje informace o subjektu (jméno, platnost apod.). Stáhli a uložili jste ji kliknutím na odkaz v mailu, který vám zaslala certifikační autorita, nejspíše Česká pošta a bude to soubor VCAxxxxxx.cer. Tuto část lze kdykoliv později stáhnout i z webu PostSignum, resp. z této stránky https://www.postsignum.cz/certifikaty_uzivatelu.html zadáním mailu, který jste při žádosti uvedli. Je tedy jasné, že se nejedná o nic tajného, protože bez soukromého klíče je téměř k ničemu.

b) Soukromý klíč
Je automaticky uložen v počítači, ze kterého byla generována žádost o jeho vydání a s ním je třeba zacházet opatrně a bezpečně (v digitálním světě reálně nahrazuje náš podpis). A aby se k němu někdo nedostal, je třeba chránit přístup k počítači.

Obě části se tvoří při generování žádosti o certifikát, která se odešle k certifikační autoritě. Ta následně pošle zpět veřejnou část. Soukromý klíč ale celou dobu zůstává ve vašem počítači.
Když jsou obě části v jednom počítači, propojí se a klíč plní svou funkci.

Komerční certifikát je pak použitelný v případě, že jsou k dispozici obě části, které jsou navzájem propojené šifrovanými klíči. Další technické podrobnosti nejsou pro naše potřeby důležité.

Instalace

Instalace certifikátu je na počítači, kde byla žádost o vydání vygenerována, naprosto jednoduchá. **Stačí na stažený soubor VCAxxxxxx.cer 2x kliknout (spustit) a odsouhlasit instalaci.**

Tím je hotovo a nainstalováno, můžete se přihlásit na Portál CSUIS.

Přenesení certifikátu do jiného počítače

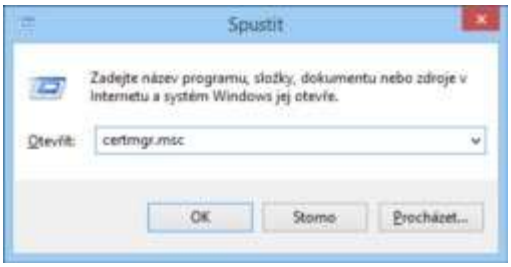
Z výše uvedeného vyplývá, že soukromý klíč je důležitý a není jednoduše k dispozici. Systém Windows jej proto obvykle nastaví jako neexportovatelný, aby jej chránil.

Ale aby bylo možné s Portálem CSÚIS pracovat i z jiného počítače, je třeba certifikát do něj přenést a instalovat. K tomu potřebujeme obě části a ty získáme na výchozím počítači, kde již certifikát nainstalovaný je. Není to složité, průměrný uživatel počítače to zvládne.
Nejdříve je třeba certifikát na výchozím počítači exportovat, a to včetně soukromého klíče.

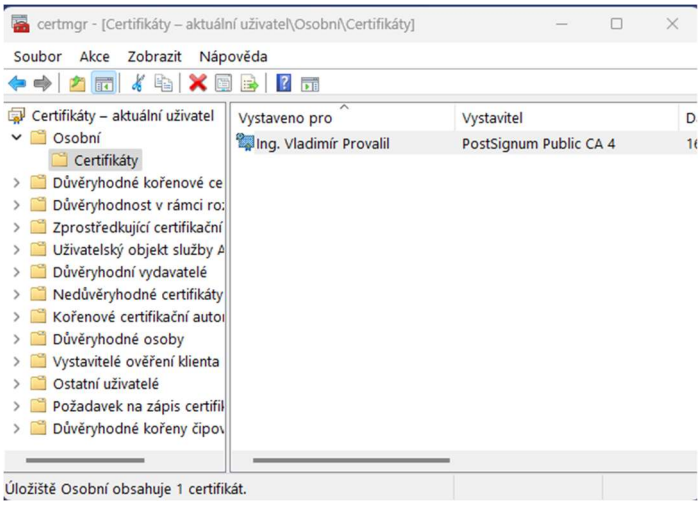
Export certifikátu s privátním klíčem

Pro správu certifikátů slouží konzole *Správa certifikátů uživatelů (pokud možno v režimu Správce).*

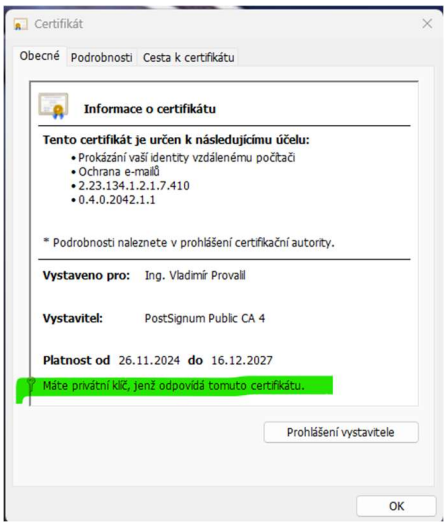
a) WIN+R a příkaz ‚certmgr.msc'
b) Do pole vyhledat napište ‚*Správa certifikátů uživatelů*'



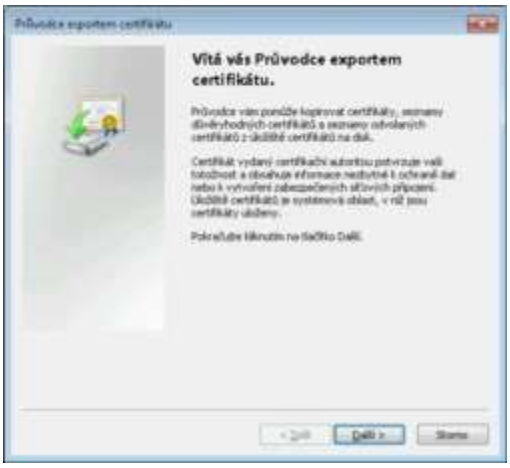
Objeví se konzole *Certifikáty - aktuální uživatel*, zde vyberte kategorii *Osobní, poté Certifikáty*.



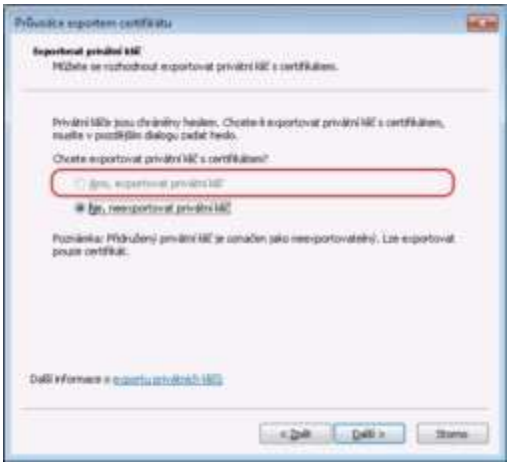
Poklepáním na požadovaný záznam zobrazíme vlastnosti certifikátu a zároveň ověřit, že k certifikátu existuje i privátní klíč. **Pokud tam tato informace není, pak export neuděláme**. Zřejmě je privátní klíč na jiném počítači anebo je potřeba o požádat znovu o vydání certifikátu.



Na záložce *Podrobnosti* zvolte *Kopírovat do souboru..., následuje Průvodce exportem certifikátu*. Stiskneme Další...



Poté je potřeba zvolit, že chceme spolu s certifikátem exportovat také privátní (soukromý) klíč.

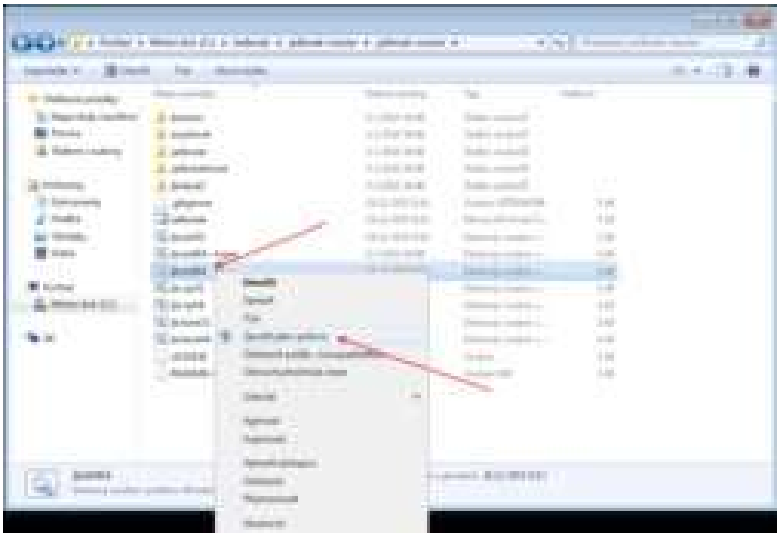


Pokud není možné zvolit variantu *Ano, exportovat privátní klíč*, nelze pokračovat běžným způsobem, protože sice je dostupný ale systém jej označil jako *neexportovatelný*.

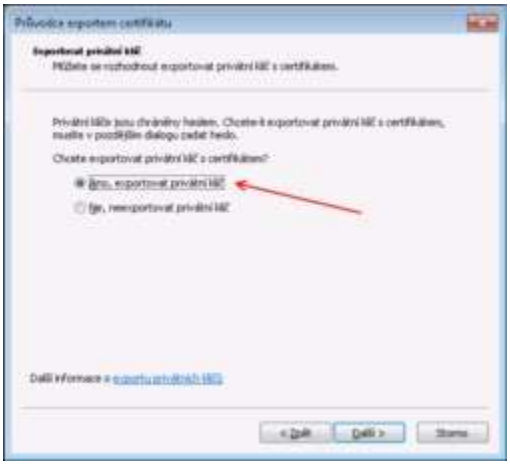
Certifikát není exportovatelný?

Jestliže tato situace nastane, je potřeba změnit nastavení systému. To se dá provést pomocí speciálního programu Jailbreak, která dovolí exportovat soukromou část (zde ke stažení na GitHub)

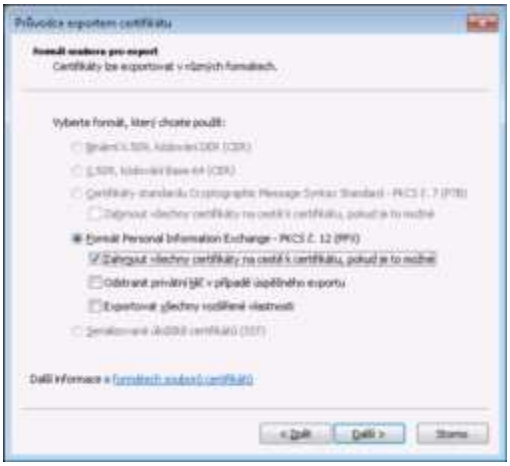
1. Na webu klikněte na zelené ‚CODE' a tlačítko *Download ZIP*
2. Soubor *jailbreak-master.zip* rozbalte do libovolné složky na disku.
3. Otevřete složku *jailbreak-master*
4. Spusťte dávkový soubor *jbcert32.bat nebo jbcert64* (podle verze OS Windows) **jako správce!**



Program zpřístupní všechny klíče a následně otevře okno *Správce certifikátů*.
Zde vyberte požadovaný certifikát a exportujte…



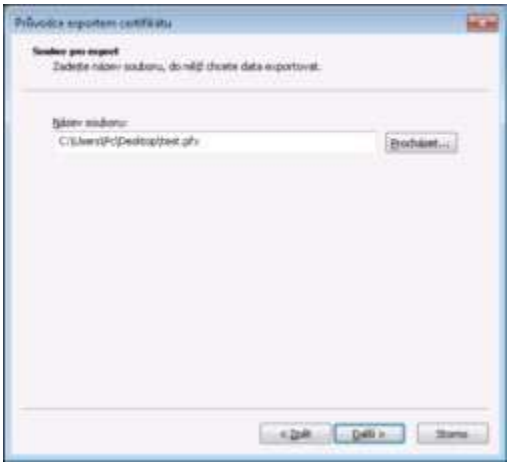
Poté pokračujte…



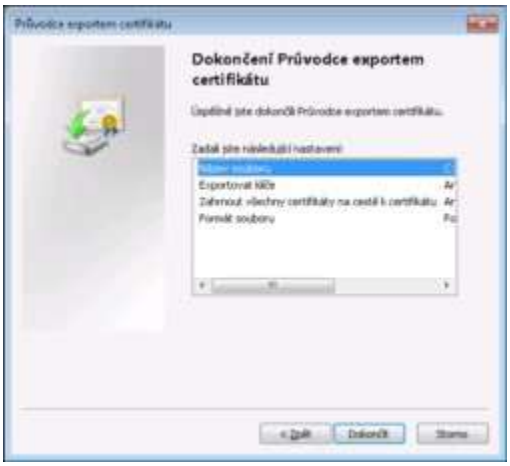
Potvrďte volbu *Formát PKCS č.12 (PFX)* a pro jistotu zaškrtněte i volbu *Zahrnout všechny certifikáty na cestě k certifikátu.*

Následně zadejte 2x vámi zvolené heslo (libovolné, ale ne úplně stupidní). Toto pak budete potřebovat při instalaci certifikátu na jiném počítači.

Zadejte cestu a názvu souboru klíče pro uložení a *Další*…



Potvrďte tlačítkem *Dokončit* (dojde k exportu)



Poznámka : po dokončení, resp. uložení do souboru PFX bude klíč na tomto počítači opět neexportovatelný a chráněný.
Právě vygenerovaný klíč (soubor PFX) uložte na USB nebo na dostupné místo v síti.

Nový počítač, resp. ten, na který chceme certifikát přenést

V počítači, do kterého budeme certifikát instalovat, najděte exportovaný soubor PFX (na USB apod.) a spusťte jej. Otevře se okno *Průvodce importem certifikátu.* Poté zadejte heslo, které jste použili při exportování. Můžete ještě dle vlastního uvážení zaškrtnout možnost *Označit tento klíč jako exportovatelný.* To pro případ, kdybyste jej chtěli někdy exportovat a přenést jinam. Ale na to vám bude sloužit už ten, který právě importujete a máte uložený ve formátu PFX.

Klikněte na *Další a dokončete instalaci.*