

Národní elektronický nástroj

Metodický pokyn pro práci s certifikáty pro šifrování/dešifrování v NEN

V 1.1
20.1.2016

Tesco SW a.s.
tř. Kosmonautů 1288/1, 772 00 Olomouc
www.tescosw.cz

Obsah

1	Metodický pokyn.....	3
2	Vytvoření vlastní CA a generování certifikátu.....	5
2.1	Nastavení příkazového řádku	6
2.2	Generování certifikátu CA	7
2.3	Generování vlastního certifikátu	7

1 METODICKÝ POKYN

Národní elektronický nástroj (NEN) umožňuje elektronické podávání nabídek dle § 149, odstavce 3 zákona č. 137/2006 Sb.. V této situaci ukládá zadavateli povinnost poskytnout dodavatelům, kteří mohou mít zájem účastnit se řízení či soutěže, k dispozici veškeré informace technické povahy, včetně kódování a šifrování, které jsou nezbytné pro komunikaci elektronickými prostředky, zejména pro elektronické podání nabídek a žádostí o účast.

Technické řešení v NEN využívá principu asymetrické kryptografie a provádí šifrování nabídek, veřejným klíčem certifikátu dodaným zadavatelem a následné dešifrování privátním klíčem, který je v páru s veřejným klíčem v certifikátu. Použití certifikátů je vymezeno dokumentem „Principy práce s certifikáty v aplikaci NEN z pohledu dodavatelů a zadavatelů“ uveřejněným v uživatelských příručkách systému NEN (<https://nen.nipez.cz/>).

Jedná se o certifikáty typu C3 dle značení NEN:

Komerční certifikát zadavatele není vydán pro účely zákona č. 227/2000 Sb.
Certifikát si zajišťují a obnovují všichni zadavatelé využívající NEN na vlastní náklady.

Výše uvedená definice vylučuje využití kvalifikované certifikáty vydané kvalifikovaným akreditovaným poskytovatelem certifikačních služeb (dle zákona č. 227/2000 Sb.), neboť tyto certifikáty mají v certifikačních politikách zakázáno použití certifikátu pro účely šifrování dat.

Zadavatel není při výběru poskytovatele certifikačních služeb, který vygeneruje příslušný certifikát k veřejné části klíčového páru, zásadně omezen. Certifikát musí být vystaven podle bezpečnostní politiky, které umožňují certifikát využít k šifrování.

Je možné využít jak českých veřejných komerčních certifikačních autorit (CA), tak zahraničních, nebo si příslušný certifikát vygenerovat vlastní certifikační autoritou.

Pokud je využita certifikační autorita, která není obecně považována za důvěryhodnou (hlavně v programu Microsoft Root Certificate Program), doporučujeme k certifikátu přidat i všechny nadřazené certifikáty daného certifikátu C3 tak, aby byl celý řetězec certifikátů úplný.

Přesto doporučujeme využívat certifikáty vydané certifikačními autoritami zavedenými v programu Microsoft Root Certificate.

Jednak z důvodu, že tyto certifikáty se od počátku jeví uživatelům jako vydané důvěryhodnou certifikační autoritou a nemusí si pro případ, že chtějí mít tyto certifikáty považovány za vydané důvěryhodnou certifikační autoritou, do svého úložiště přidat apriori neveřejné a neznámé certifikační autority, u kterých je zvýšená pravděpodobnost možného zneužití například ve formě podpisu programů a dokumentů, které by pak systém a uživatel mohl považovat za důvěryhodné.

Je možné si vytvořit vlastní CA a generovat certifikáty zdarma. Jejich nevýhodou je, že nejsou ihned důvěryhodné uživatelům. Existuje více programů k jejich vygenerování. Je možné použít například funkcionalitu firmy Microsoft nebo OpenSSL a další. V kapitole 2 je popsán detailnější postup při využití programu firmy Microsoft.

Z českých CA jsou v programu Microsoft root:

- První certifikační autorita, a.s. (I.CA) – od 395kč - <https://www.ica.cz/Komerčni-Certifikaty>
- Postsignum CA – od 348kč - http://www.postsignum.cz/komerčni_certifikaty.html

Česká CA, která není v programu Microsoft root:

- eidentity a.s. – od 359kč - <http://www.eidentity.cz/Kservices.html>

Ze zahraničních CA například (ale ne zejména):

- RapidSSL – od 49\$ - <https://www.rapidssl.com/>
- Comodo SSL – od 79\$ - <https://ssl.comodo.com/>
- Geotrust – od 149\$ - <https://www.geotrust.com/ssl/>
- Thawte – od 149\$ - <https://www.thawte.com/ssl/>
- Globalsign – od 179\$ - <https://www.globalsign.com/en/ssl/>
- Symantec – od 399\$ - <http://www.symantec.com/ssl-certificates/>

Výše uvedené ceny nemusí být aktuální, pro jejich ověření je nutno rozkliknout příslušný web certifikační autority.

Certifikáty je umožněno v systému NEN využívat opakovaně, tedy použít stejný certifikát pro šifrování více nabídek. Privátní klíč by měl mít k dispozici pouze minimálnímu počet osob a měl by být do doby otevírání nabídek bezpečně uložen zadavatelem a chráněn proti zneužití. Z toho důvodu doporučujeme používat certifikáty pro šifrování pouze pro účely elektronického podávání v systému NEN a nevyužívat jej k dalším činnostem. Použití certifikátu v rámci otevírání nabídek v systému NEN znamená jeho použití jednotlivými členy komise otevírání nabídek. Případně sdělení PINu/hesla při použití tokenu nebo systémového úložiště.

Systém NEN je navržen tak, že kryptografické operace jsou prováděny výlučně na počítači uživatele/člena komise a klíče a hesla nejsou v žádném případě předávány serverům NEN.

Použití privátního klíče členy komise znamená jeho zpřístupnění více osobám. To má za následek zvýšení rizika kompromitace klíče.

Z toho důvodu doporučujeme pro každý zadávací postup v NEN využít vlastní šifrovací certifikát a jeho odpovídající privátní a veřejné klíče.
Šifrovací certifikát by měl mít dostatečnou platnost tak, aby mohla být veškerá podání činěna s platným certifikátem.

Princip práce s certifikáty v systému NEN je uveden v uživatelské příručce „Principy práce s certifikáty v aplikaci NEN z pohledu dodavatelů a zadavatelů“, dostupné na <https://nen.nipez.cz/>.

2 VYTVOŘENÍ VLASTNÍ CA A GENEROVÁNÍ CERTIFIKÁTU

Pokud si chcete vygenerovat vlastní certifikáty a tím ušetřit na nákladech na jejich zakoupení, doporučujeme vygenerovat si nejdříve vlastní certifikační autoritu a následně si podle této CA generovat výsledné certifikáty. Tento postup umožňuje možnost zdůvěřhodnění generovaných certifikátů v systémovém úložišti certifikátů systému Windows u jednotlivých uživatelů.

Také existuje možné generovat pouze jednotlivé certifikáty.

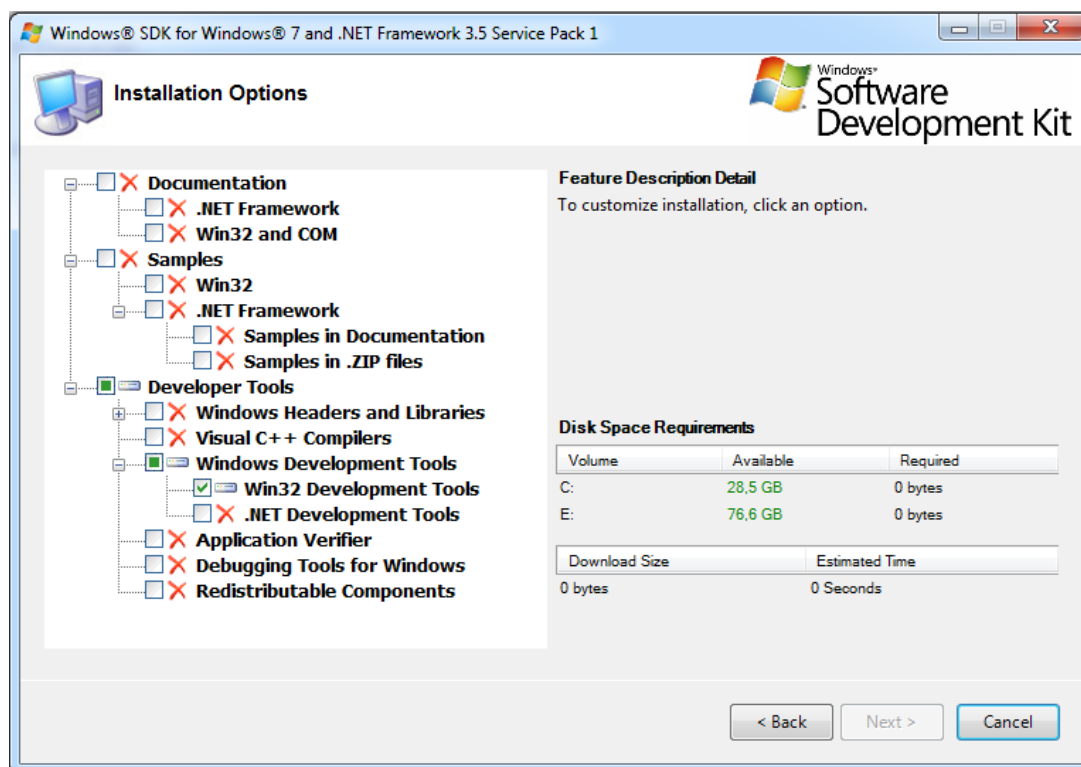
Níže je uveden příklad pomocí programu MakeCert.exe, který je součástí balíku programů s názvem „Microsoft SDKs“. Je možné jej získat i instalací produktu Microsoft Visual studio. Programy je nutné nainstalovat pouze na počítač, na kterém dochází ke generování certifikátů. Jedná se o volně dostupné programy.

Microsoft SDK lze získat z adresy <https://msdn.microsoft.com/en-us/windows/desktop/ff851942.aspx>. Vyberte si na stránce odpovídající verzi operačního systému. Pokud je k dispozici více verzí, verze .NET Frameworku je na Vašem výběru. Stáhněte si příslušný program a proveďte instalaci.

Na Windows 7 byla instalace odzkoušena na verzi s .NET Framework 3.5 SP1.

Po spuštění instalátoru klikněte dále, než se zobrazí příslušné okno pro výběr, jaké komponenty nainstalovat. V rámci průchodu uvidíte i adresu, kam se aplikace instaluje (více viz níže).

Pro funkcionality postačuje nainstalovat pouze „Win32 Development Tools“. V jiných verzích bude volba obdobná. Například ve verzi pro Windows 8.1 se jmenuje „Windows Software Development Kit“.



Z Microsoft SDK se budou využívat tyto programy:

- Makecert.exe - popis na [https://msdn.microsoft.com/cs-cz/library/bfskty3\(v=vs.110\).aspx](https://msdn.microsoft.com/cs-cz/library/bfskty3(v=vs.110).aspx)
 - o Výsledkem je soubor s příponou .pvk (obsahuje privátní klíč) a soubor s příponou .cer (obsahuje certifikát s veřejným klíčem). CER soubor slouží k šifrování.
- Pvk2pfx.exe – popis na [https://msdn.microsoft.com/cs-cz/library/ff550672\(v=vs.85\).aspx](https://msdn.microsoft.com/cs-cz/library/ff550672(v=vs.85).aspx)
 - o Výsledkem je spojení .pvk a .cer souborů do souboru s příponou .pfx, který obsahuje jak certifikát, tak oba klíče. Tento soubor slouží k dešifrování.

V rámci instalace Microsoft SDK se zobrazí cesta, kam se program nainstaluje. Příklady umístění souborů:

- C:\Program Files (x86)\Microsoft SDKs\Windows\v7.0\Bin
- C:\Program Files (x86)\Microsoft SDKs\Windows\v7.1A\Bin
- C:\Program Files (x86)\Windows Kits\8.1\bin\x86

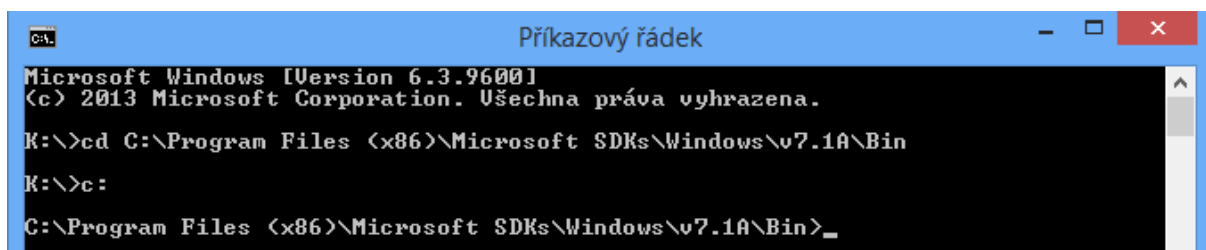
Ukázky níže jsou prováděny na Windows 8.1 s adresou C:\Program Files (x86)\Microsoft SDKs\Windows\v7.1A\Bin. Pokud máte jinou adresu, upravte si příklady.

Postup vyžaduje základní znalost příkazového řádku. Příkazy příkazového řádku jsou podbarveny.

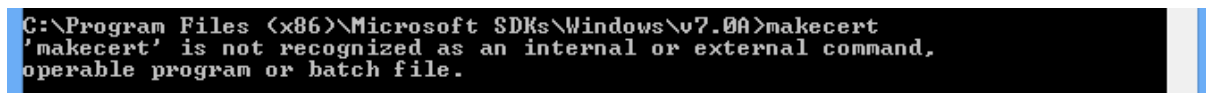
2.1 NASTAVENÍ PŘÍKAZOVÉHO ŘÁDKU

Spustíte příkazový řádek (Nabídka start – volba Spustit – napsat slovo *cmd* a potvrdit), případně jiným způsobem dle vašeho operačního systému (například v nabídce start pouze napište *příkazov* a položka příkazový řádek se nabídne).

Napište příkaz `cd C:\Program Files (x86)\Microsoft SDKs\Windows\v7.1A\Bin`. Pokud nejste na disku C, spustě dále příkaz `c:`



Pokud zde napíšete příkaz `makecert` a dostanete tuto hlášku, vyzkoušejte jinou adresu. Program `makecert` není v této složce přítomen.

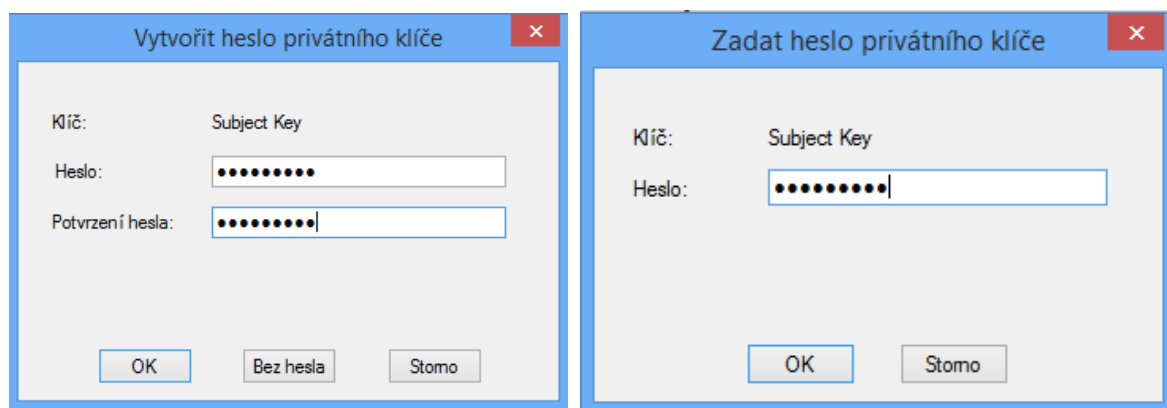


2.2 GENEROVÁNÍ CERTIFIKÁTU CA

Spustě příkaz `makecert -r -n "CN=Ministerstvo pro místní rozvoj" -pe -sv ca.pvk -a sha256 -m 120 -len 4096 -cy authority ca.cer`

Vysvětlivky jsou uvedeny u popisu Makecert.exe. Příkaz vygeneruje vlastní certifikát Vaší nové CA. Zvolte si odpovídající název. Doba platnosti CA je 10 let (120 měsíců). Budou do dané složky vygenerovány 2 soubory – ca.pvk a ca.cer.

Vyskočí okno pro zadání hesla i privátnímu klíči. Doporučujeme zadat nějaké heslo. Poznačte si jej. Budete jej potřebovat. Po stisku tlačítka OK vyskočí okno pro opětovné zadání zvoleného hesla. Pokud zvolíte bez, hesla, další okno již nevyskočí.



Po úspěšném dokončení se vypíše v příkazovém řádku slovo Succeeded.

Všechny vygenerované soubory naleznete ve složce, ve které se nachází Vámi spuštěný soubor makecert.exe. Soubory a heslo si uchovejte. Můžete je opakovaně použít při generování certifikátů pro jednotlivé zadávací postupy.

2.3 GENEROVÁNÍ VLASTNÍHO CERTIFIKÁTU

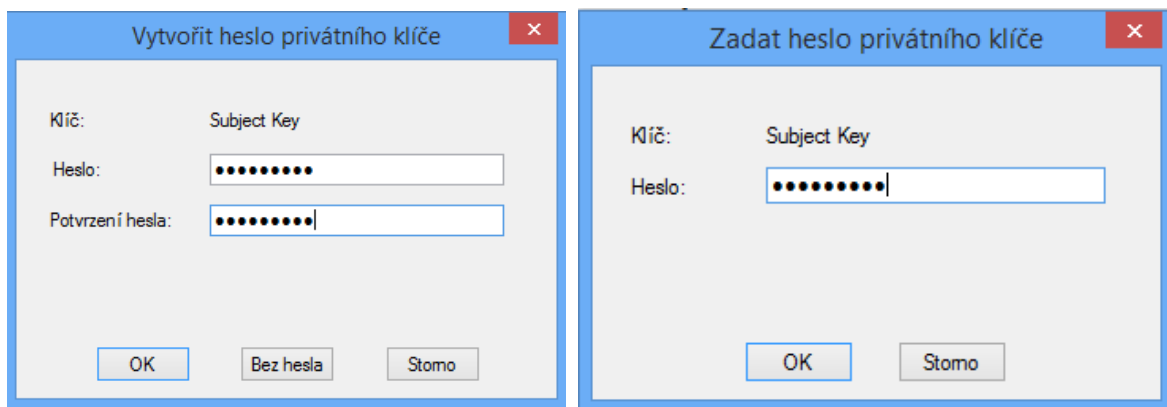
Postup je velmi obdobný jako při generování Vaší certifikační autority.

Certifikát a privátní klíč, který bude sloužit pro samotné šifrování a dešifrování si vygeneruje tímto příkazem.

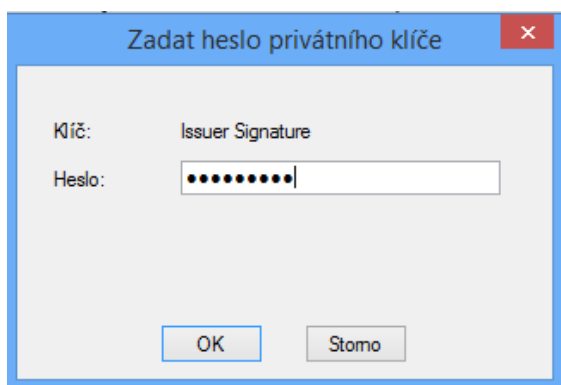
`makecert -iv ca.pvk -ic ca.cer -n "CN=veřejná zakázka N006/15/V00000002, E=nen@nipez.cz" -pe -sv clientcert.pvk -a sha256 -len 4096 -m 9 -sky 1 clientcert.cer`

Vysvětlivky jsou uvedeny u popisu Makecert.exe. Příkaz vygeneruje certifikát s názvem „Veřejná zakázka N006/15/V00000002“, v certifikátu bude uveden email nen@nipez.cz. Certifikát bude platit 9 měsíců. Budou do dané složky vygenerovány 2 soubory – clientcert.pvk a clientcert.cer.

Vyskočí okno pro zadání hesla k privátnímu klíči. Doporučujeme zadat nějaké heslo. Poznačte si jej. Budete jej potřebovat. Po stisku tlačítka OK vyskočí okno pro opětovné zadání zvoleného hesla. Pokud zvolíte bez hesla, další okno již nevyskočí.



Dále se program zeptá na heslo k privátnímu klíči certifikační autority. Zadejte její heslo a stiskněte OK.



Po úspěšném dokončení se vypíše v příkazovém řádku slovo Succeeded.

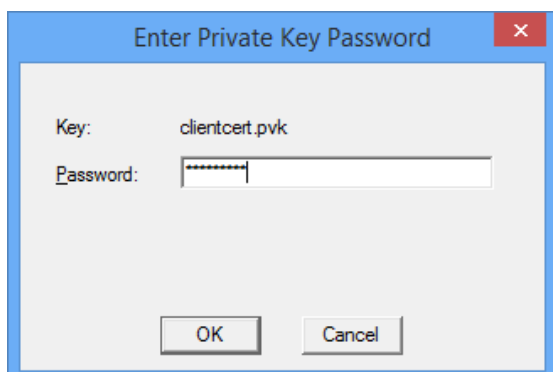
```
C:\Program Files (x86)\Microsoft SDKs\Windows\v7.1A\Bin>makecert -iv ca.pvk -ic
ca.cer -n "CN=veřejná zakázka N006/15/V00000002, E=nen@nipez.cz" -pe -sv clientc
ert.pvk -a sha256 -len 4096 -m 9 -sky 1 clientcert.cer
Succeeded
```

Abyste získali i soubor .pfx, spustě příkaz pvk2pfx.

```
pvk2pfx -pvk clientcert.pvk -spc clientcert.cer -pfx clientcert.pfx -po hesloprocertifikat
```

Vysvětlivky jsou uvedeny u popisu pvk2pfx.exe. Příkaz sloučí .pvk a .cer a vytvoří .pfx soubor, kterým lze dešifrovat podání.

Vyskočí okno pro zadání hesla k privátnímu klíči. Zadejte jej a stiskněte OK.



Nyní máte v dané složce 3 soubory:

- clientcert.pvk – soubor s privátním klíčem. Lze smazat.
- clientcert.cer – certifikát, který by měl být předán dodavatelům k zašifrování.
- clientcert.pfx – certifikát s privátním klíčem, který by měli použít pracovníci zodpovědní za dešifrování nabídek.

Poznámky a doporučení

- Spolu s clientcert.cer doporučujeme předat dodavatelům i ca.cer (certifikát certifikační autority). Soubory si můžete kdykoliv přejmenovat.
 - o Pokud si budete certifikáty importovat do systémového úložiště certifikátů Windows, naimportujte nejdříve certifikát CA (ca.cer) do „Důvěryhodné kořenové certifikační autority“. Poté naimportujte clientcert.cer (nebo clientcert.pfx – podle toho, jaký soubor máte k dispozici a k čemu jej chcete použít) do „Osobní“.
- Po vygenerování soubory smažte nebo přesuňte na bezpečné místo. Uložení privátních klíčů jako souborů není doporučeno.
- Pokud importujete do systémové úložiště certifikátů privátní klíč (soubor .pfx), nezapomeňte, že pokud budete chtít certifikát s privátním klíčem někomu předat (a vyexportovat z úložiště), musíte zvolit možnost, že je certifikát exportovatelný.
- Heslo k vytvářenému .pfx souboru volte pokaždé jiné a rozhodně ne stejné jako heslo k certifikační autoritě.

-