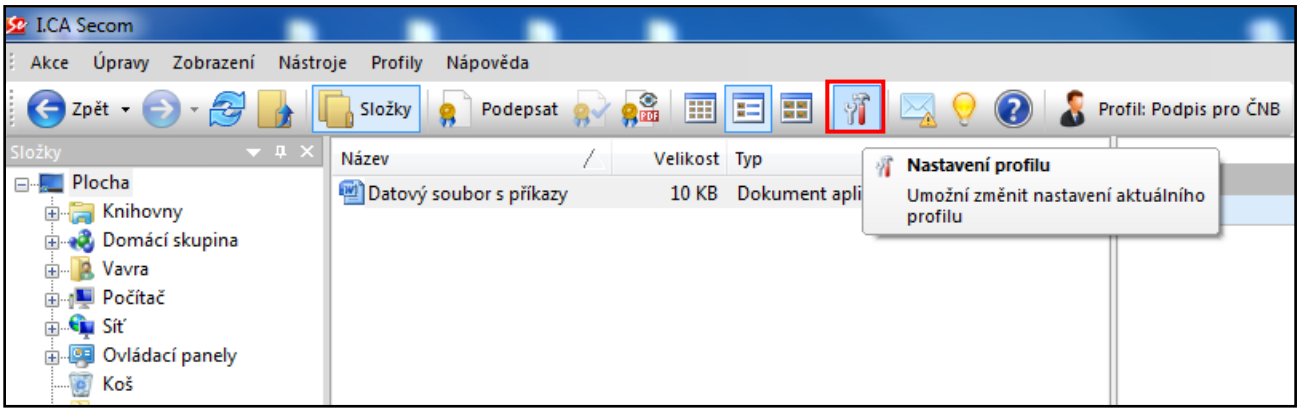
Ukázka vytvoření externího podpisu ve formátu PKCS#7 v DER kódování prostřednictvím aplikace ICA Secom PDF

1. Úvodní spuštění aplikace

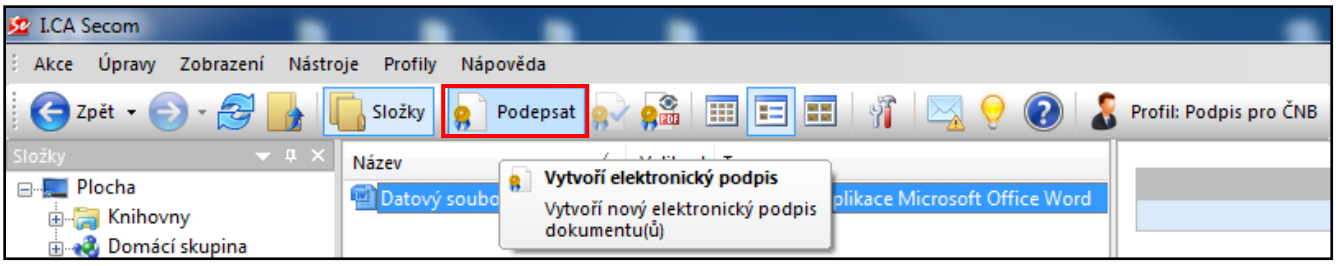
- Aplikace je po založení podepisovacího profilu plně připravena k vytváření všech druhů podpisů.



- Zvolením ikony  se uživatel může přesvědčit, že je v podepisovacím profilu nastaven požadovaný formát podpisu.
- Dle metodiky ČNB je požadováno podepisovat datové soubory externím podpisem ve formátu PKCS#7 v DER kódování, čemuž odpovídá volba v aplikaci "P7S formát (externí podpis)".

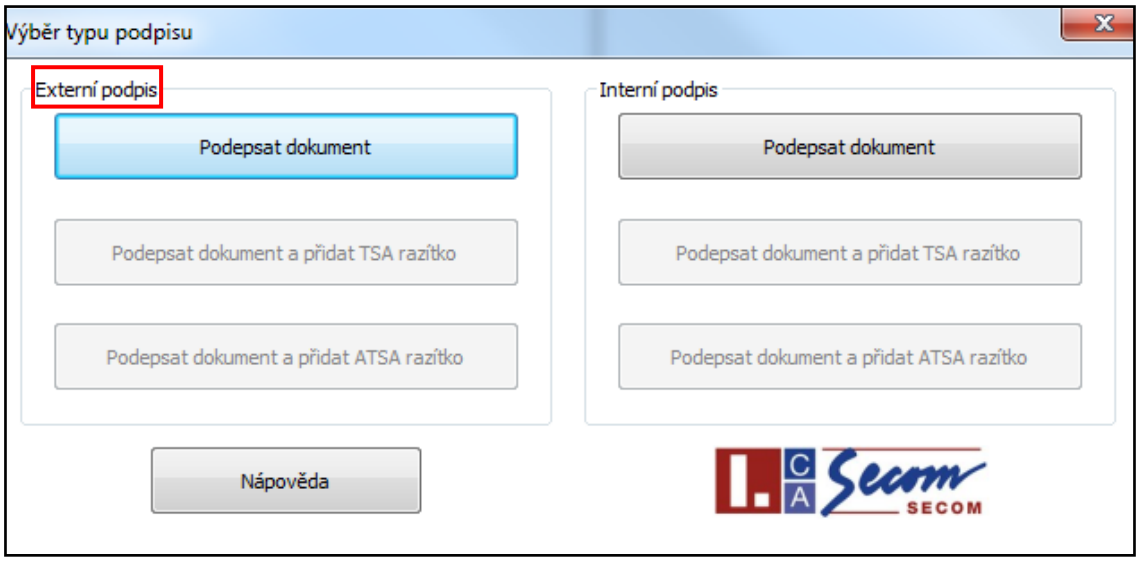
2. Podepsání datového souboru požadovaným externím podpisem

- Uživatel v aplikaci jednoduše nalezne datový soubor určený k podpisu.
- Vybraný datový soubor uživatel prostřednictvím volby "Podepsat" podepíše.
- Aplikace umožňuje vícenásobný podpis a podporuje všechny formáty dokumentů a datových souborů jako např.: doc, docx, xls, xlsx, jpg, gif, txt, xml..

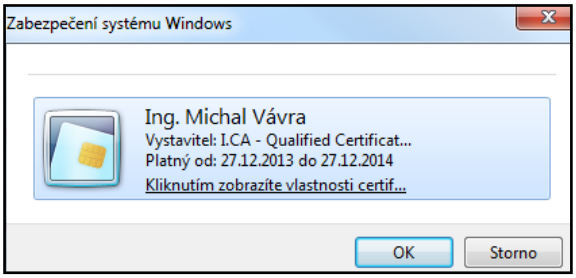


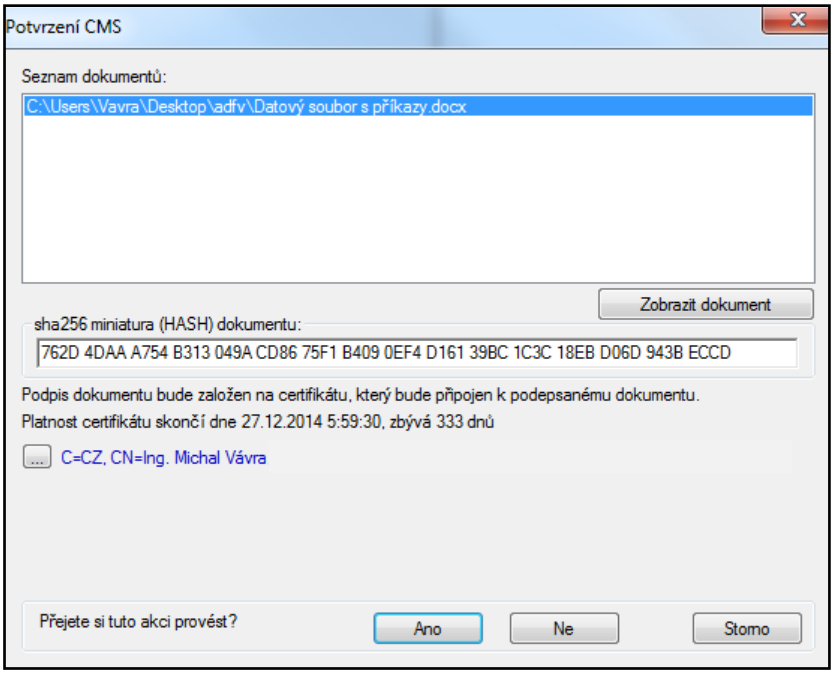
- Ještě před samotným podpisem je uživatel vyzván v podepisovacím menu, aby uvedl formát požadovaného podpisu (externí nebo interní).

- V případě, že bude uživatel k podpisu požadovat i časové razítko, může mít aktivní i druhou volbu u externího podpisu a to dle typu razítka (TSA - klasická časová kvalifikovaná razítka, ATSA - archivní kvalifikovaná časová razítka).

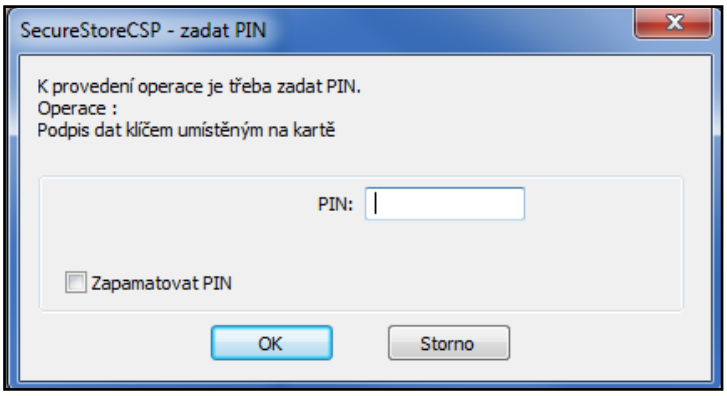


- Po výběru typu podpisu je uživatel vyzván k potvrzení podepsání požadovaných souborů podpisovým certifikátem.

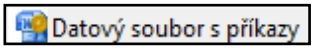




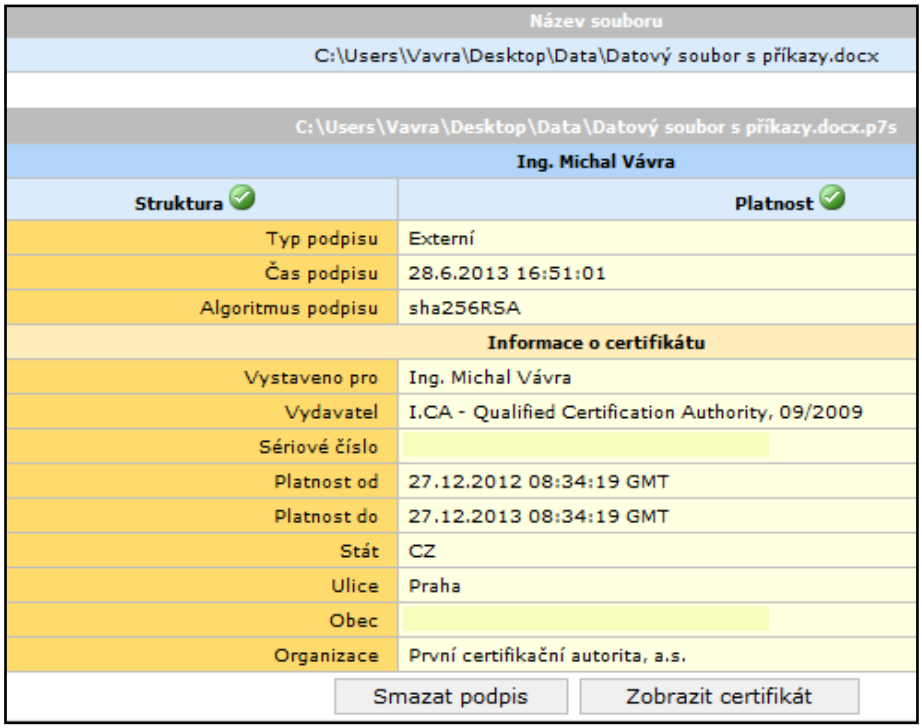
- Pokud je certifikát uložený na čipové kartě I.CA, je uživatel před samotným podpisem ještě vyzván k zadání PINu k čipové kartě.



3. Ověření podpisu

- Po podepsání je datový soubor označen žlutou pečetí. 

- Aplikace navíc poskytne uživateli o provedeném podpisu další dodatečné informace.

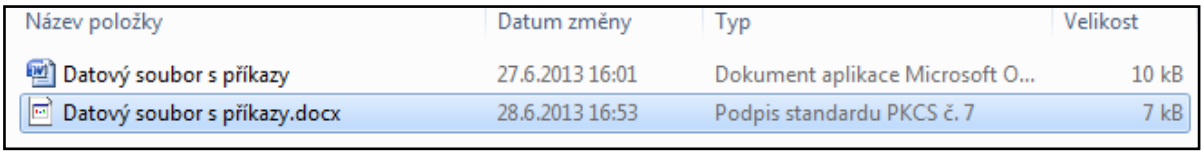


Název souboru	
C:\Users\Vavra\Desktop\Data\Datový soubor s příkazy.docx	
C:\Users\Vavra\Desktop\Data\Datový soubor s příkazy.docx.p7s	
Ing. Michal Vávra	
Struktura	**Platnost**
Typ podpisu	Externí
Čas podpisu	28.6.2013 16:51:01
Algoritmus podpisu	sha256RSA
Informace o certifikátu	
Vystaveno pro	Ing. Michal Vávra
Vydavatel	I.CA - Qualified Certification Authority, 09/2009
Sériové číslo	
Platnost od	27.12.2012 08:34:19 GMT
Platnost do	27.12.2013 08:34:19 GMT
Stát	CZ
Ulice	Praha
Obec	
Organizace	První certifikační autorita, a.s.

Smazat podpis | Zobrazit certifikát

4. Soubor s externím podpisem ve formátu PKCS#7 v DER kódování

- Vytvořený soubor s externím podpisem, je automaticky aplikací uložen do složky, ve které se nachází původní dokument.



- Po otevření souboru s externím podpisem se uživatel jednoduchým proklikem dostane až k samotnému podpisovému certifikátu autora, který je v DER kódování.