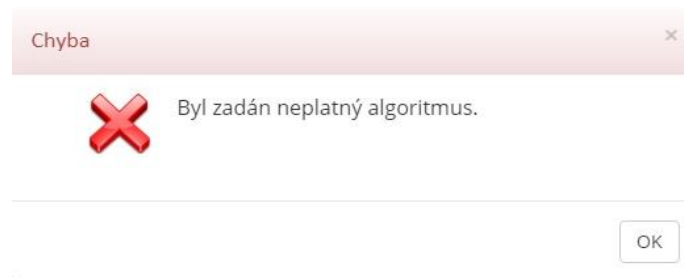
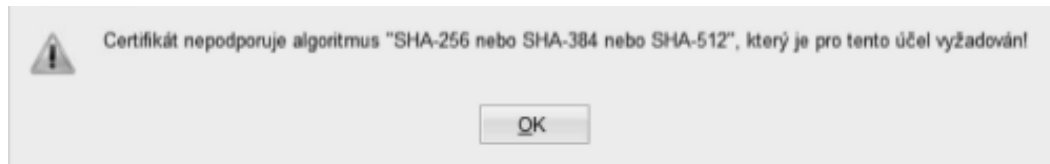


## Certifikát nepodporuje algoritmus SHA-256 nebo SHA-384 nebo SHA-512

Množí se případy, kdy se lékař či lékárník snaží nastavit v lékařském či lékárenském software elektronický podpis vystavený Českou poštou, s.p. (Postsignum), První certifikační autoritou, a.s. nebo eIdentity a.s. nebo tímto elektronickým podpisem podepsat vystavovaný či vydávaný eRecept, a zobrazí se chybová hláška: „Certifikát nepodporuje algoritmus SHA-256 nebo SHA-384 nebo SHA-512, který je pro tento účel vyžadován!“



Na stránkách poskytovatelů certifikačních služeb je návod na provedení opravy.

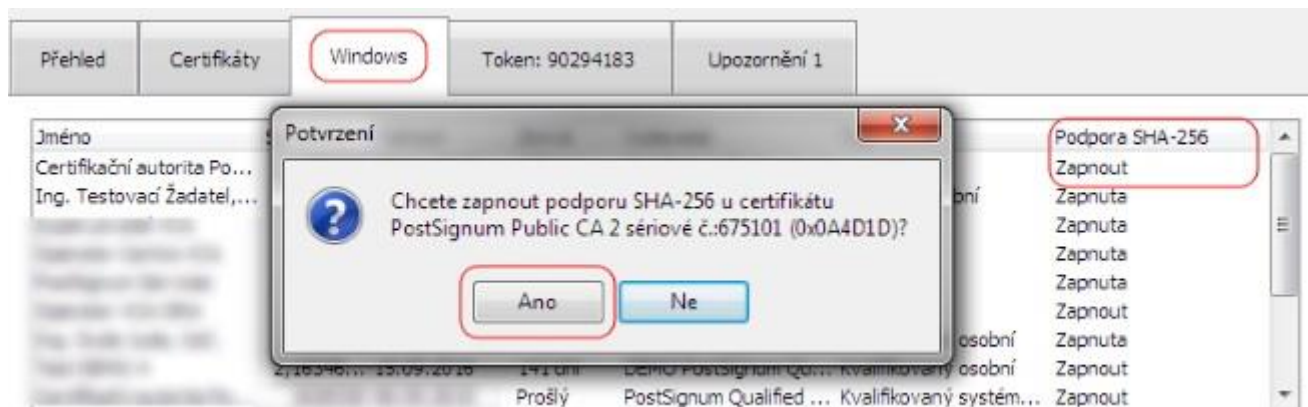
### PostSignum (Česká pošta, s.p.)

#### Změna uložení klíče v operačním systému (podpora SHA 256 podepisování)

Některá úložiště operačního systému Windows nepodporují vytváření elektronického podpisu s použitím algoritmu SHA 256. V aplikaci iSignum je možné tuto podporu zapnout. Upozorňujeme, že změnou se manipuluje s klíči a měla by být vytvořena záloha.

#### Postup opravy:

- Stáhnout aplikaci **iSignum** – jednoduchý nástroj pro správu certifikátů <http://www.postsignum.cz/isignum.html>.
- Přepněte se na záložku Windows
- Posuvníkem přejeďte doprava na sloupeček "Podpora SHA-256"
- Jestliže je vypsáno Zapnout, tak na dané slovo a řádek klikněte a potvrďte změnu.



## První certifikační autorita, a.s.

### Postup opravy

- Stáhnout aplikaci I.CA PFX TOOL <http://www.ica.cz/Aplikace-stazeni>.