

Návod na odstránenie certifikátov so zrušenou platnosťou

UPOZORNENIE:

Od 1. 1. 2019 sa mení názov odosielateľa správ z Úrad vlády Slovenskej republiky – ÚPVS na Ústredný portál verejnej správy.

Zoznam zmien:

Dátum vydania	Verzia	Popis zmien
07. 11. 2017	1	Pôvodná verzia dokumentu.
10. 04. 2019	2	Str. 1 – 5 - zjednotenie návodu.

Obsah

Obsah.....	1
Pre koho je návod určený.....	2
Postup	2

Pre koho je návod určený

Návod je určený pre používateľov, ktorí elektronicky podpisujú dokumenty v operačnom systéme MS Windows novými kvalifikovanými certifikátmi pre elektronický podpis SVK eID ACA s 3 072-bitovými kľúčmi, ktoré sa vydávajú od 30. októbra 2017.

Postup

MS Windows - po získaní nového certifikátu odporúčame používateľom, ktorí elektronicky podpisujú dokumenty v tomto operačnom systéme, aby si zo systému odstránili staré uložené certifikáty so zrušenou platnosťou podľa návodu nižšie.

GNU/Linux a Mac OS - v týchto operačných systémoch sa certifikáty automaticky neukladajú, a preto ich používatelia nemusia odstraňovať.

V operačnom systéme MS Windows po vložení eID karty alebo inej obdobnej karty do čítačky kariet a po zadaní BOK kódu v okne „Propagácia certifikátov“ aplikácie eID klient sa certifikáty obsahujúce verejný kľúč automaticky vždy skopírujú do úložiska osobných certifikátov v používateľskom účte MS Windows. Tieto certifikáty zostávajú uložené aj po zrušení ich platnosti a vydaní nových certifikátov a zobrazujú sa v niektorých aplikáciách v ponuke certifikátov (napríklad v aplikácii D.Signer/XAdES .NET). Uvedené spôsobuje používateľom komplikácie pri podpisovaní, konkrétne pri výbere platného certifikátu. V prípade, že používateľ pri podpisovaní vyberie certifikát s už nedostupným privátnym kľúčom, zobrazí sa chyba a podpisovanie zlyhá.

Certifikáty so zrušenou platnosťou preto odporúčame odstrániť zo zoznamu osobných certifikátov používateľa. K spravovaniu certifikátov sa dostanete jedným z nasledujúcich spôsobov:

Postup č. 1:

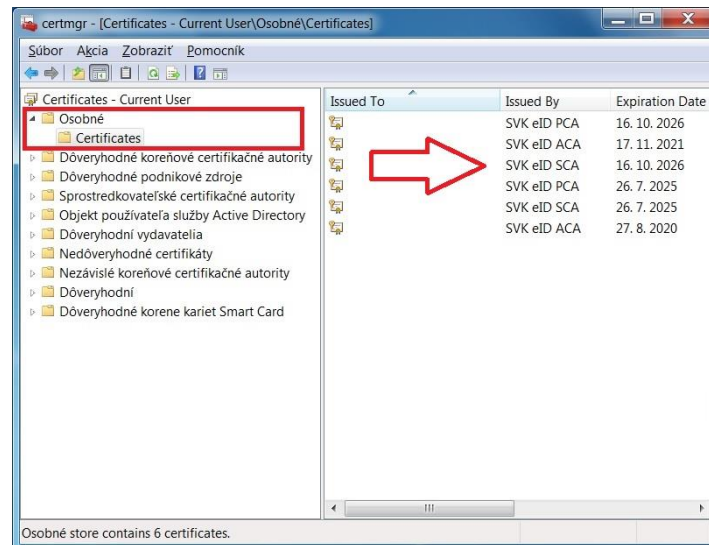
V ponuke „Štart“ napíšete názov „certmgr.msc“ a stlačíte „Enter“. Po spustení programu otvoríte položku „Osobné“ a jej podpoložku „Certifikáty“. V pravej časti okna sa zobrazí zoznam uložených certifikátov (obr. č. 1).

Návod na odstránenie certifikátov so zrušenou platnosťou

Dátum zverejnenia: 07. 11. 2017

Verzia: 2

Dátum aktualizácie: 10. 04. 2019



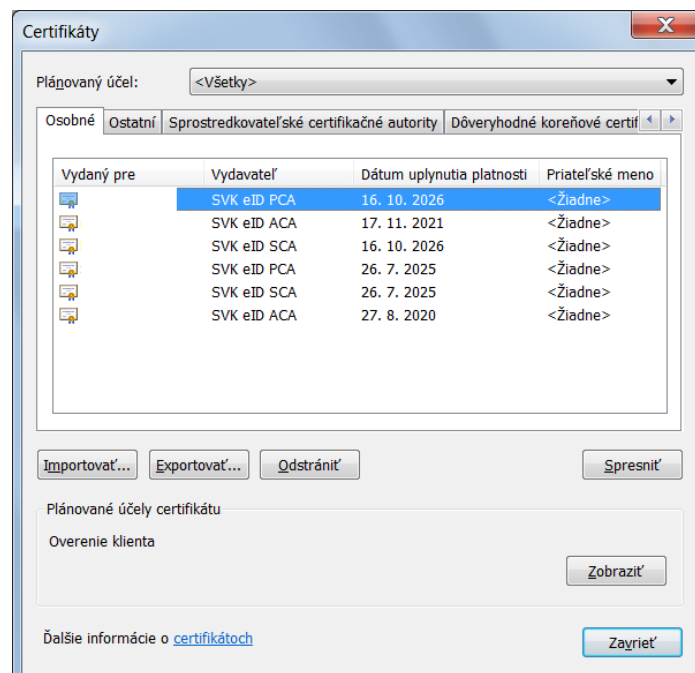
Obrázok č. 1 – Zobrazenie certifikátov po spustení programu

Postup č. 2:

V internetovom prehliadači Google Chrome otvorte „Nastavenia“, prejdite na „Rozšírené“ a otvorte „Spravovať certifikáty“ (Obr. č. 2).

Postup č. 3:

V internetovom prehliadači Internet Explorer otvorte „Možnosti siete internet“, prejdite na „Obsah“ a otvorte „Certifikáty“ (Obr. č. 2).



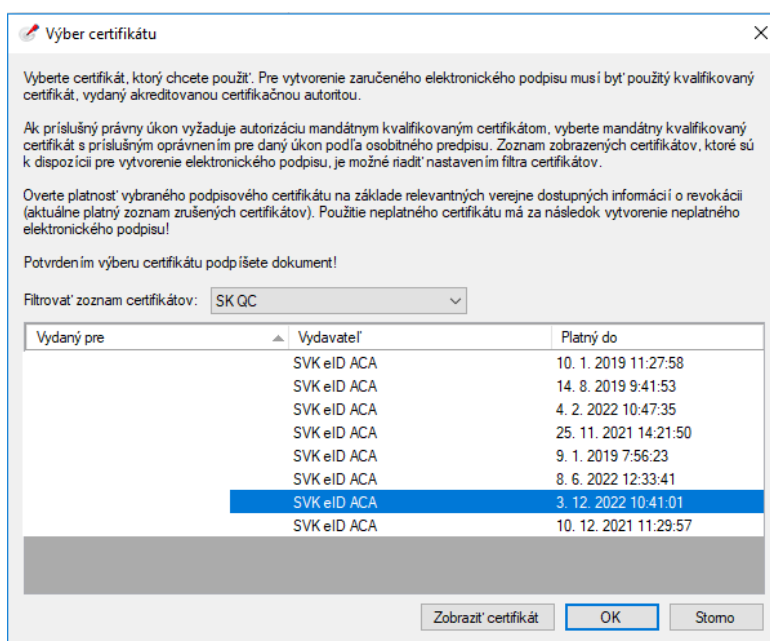
Obrázok č. 2 - Zobrazenie certifikátov v internetových prehliadačoch Google Chrome a Internet Explorer

Otvorením jednotlivých certifikátov môžete zistiť dátum ich vydania. Cez tlačidlo „Odstrániť“ alebo klávesou „Delete“ odstráňte tie certifikáty, ktorých vydavateľom je SVK eID ACA / SCA / PCA a ktoré boli vydané do **23. 10. 2017** s koncom platnosti do **22. 11. 2022**.

Vysvetlenie:

Nové kvalifikované certifikáty pre elektronický podpis SVK eID ACA s 3 072-bitovými kľúčmi sa vydávajú od 30. októbra 2017 s platnosťou na 5 rokov a 1 mesiac, t. j. koniec ich platnosti je minimálne 29. novembra 2022. Posledné kvalifikované certifikáty SVK eID ACA s 2 048-bitovými kľúčmi boli vydané 23. októbra 2017 s platnosťou do 22. novembra 2022.

Aplikácia pre kvalifikovaný elektronický podpis D.Signer/XAdES .NET v systéme MS Windows **pre podpisovanie** ponúka **zoznam všetkých** certifikátov, ktoré sa v **minulosti** uložili v systéme (Obrázok č. 3).



Obrázok č. 3 – Výber certifikátu

V prípade, ak používateľ v minulosti pripojil eID alebo eDoPP kartu pod rovnakým používateľským účtom v systéme a neskôr mu boli na tejto karte vydané nové certifikáty, tak sa mu v ponuke zobrazujú oba certifikáty.

Na samotné podpísanie sa následne použije privátny kľúč z eID karty alebo eDoPP karty, ktorý prislúcha k zvolenému certifikátu.

Tlačidlom „Zobraziť certifikát“ je možné zobraziť dátum začiatku a konca platnosti certifikátu, ako aj veľkosť kľúča. V ponuke certifikátov v aplikácii D.Signer/XAdES .NET sa nezobrazuje informácia o skutočnom konci platnosti certifikátu, ktorého platnosť bola zrušená 31. októbra 2017, nakoľko táto aplikácia neoveruje aktuálnu platnosť certifikátu.

V prípade, že je pri podpisovaní zvolený certifikát, ktorého privátny kľúč už nie je dostupný, aplikácia zobrazí chybu.

Príklad:

„Nastala chyba počas podpisovania - Core Sign 2: CryptHashData - Unable to create the SHA256 hash. An internal error occurred.“

Ak sa používateľovi po získaní nového certifikátu v systéme MS Windows nezobrazuje nový certifikát v ponuke certifikátov pre podpisovanie s koncom platnosti od 29. novembra 2022, pravdepodobnou príčinou je, že propagácia certifikátov z aplikácie eID klient neprebehla korektne. V takom prípade odporúčame odpojiť čítačku kariet, ukončiť aplikáciu eID klient, opätovne spustiť aplikáciu eID klienta, pripojiť čítačku, vložiť do nej eID alebo eDoPP a po výzve v okne propagácie certifikátov zadať BOK kód.

Informácie súvisiace so zrušením platnosti certifikátov na eID a eDoP karte nájdete v článku [Praktické informácie súvisiace s hromadným zneplatnením certifikátov na eID karte a eDoPP karte.](#)