Elektronický podpis - manuál

TLP:CLEAR

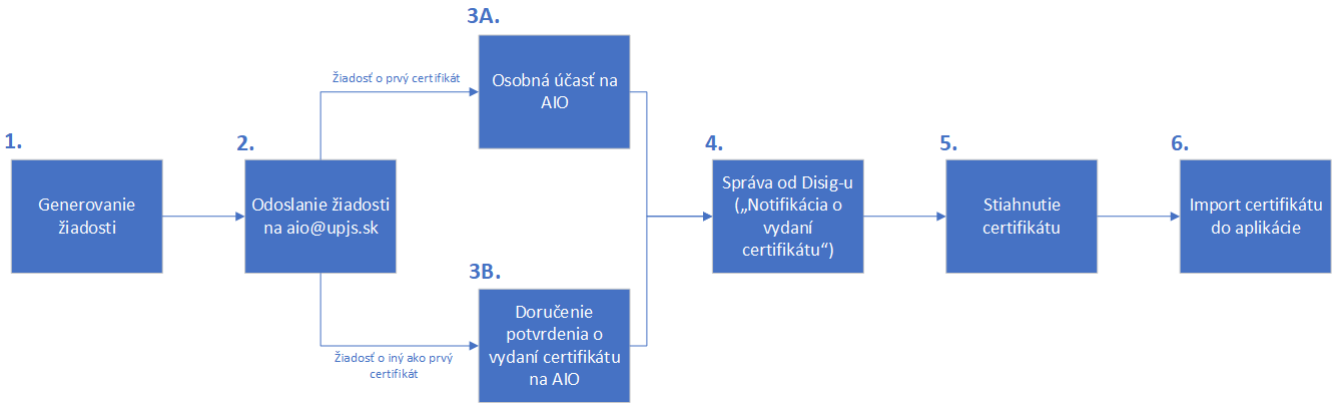
Elektronický podpis (EP) stavia podpísaný elektronický dokument na rovnakú úroveň, ako fyzicky podpísaný dokument. Na jeho vyhotovenie je potrebné získať certifikát pre EP. Nárok na certifikát majú všetci zamestnanci a doktorandi Univerzity Pavla Jozefa Šafárika v Košiciach, ktorí ho potrebujú k práci. V prípade typu certifikátu na podpis pre zamestnanca právnickej osoby je vyhotovenie bez poplatkov. Študentom sa takýto certifikát nevydáva.

Obsah

Generovanie žiadosti o vydanie certifikátu v prehliadačoch Chrome a Edge

Upozornenie

Pri generovaní žiadosti majte na zreteli, že Váš osobný certifikát musí byť nainštalovaný na tom istom počítači a v tom istom prehliadači, na ktorom bola generovaná žiadosť. Po vyexportovaní už nainštalovaného osobného certifikátu ho však budete môcť používať aj na iných počítačoch.

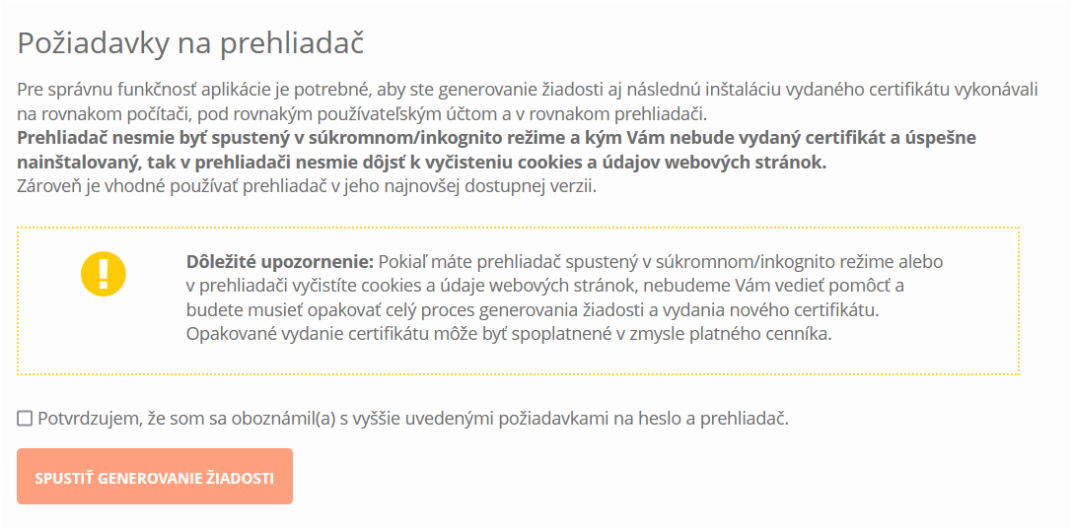


Postup generovania žiadosti

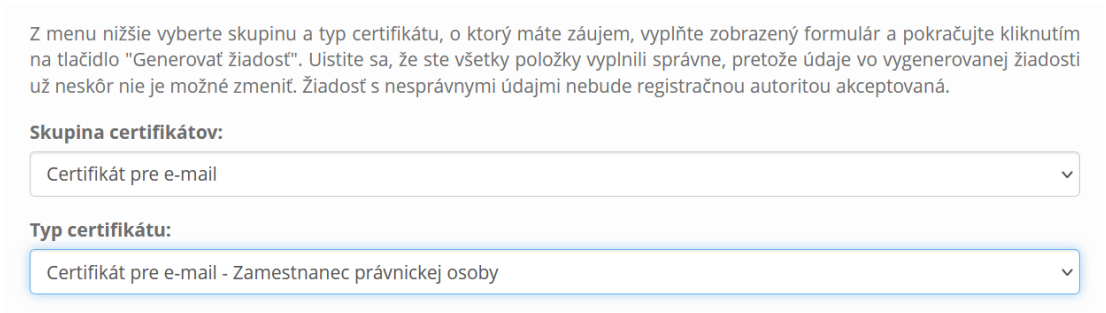
1. Navštívte stránku, z ktorej je možné generovanie žiadosti: https://eidas.disig.sk/sk/poskytovatel/certifikacna-autorita/generovanie-ziadosti/.

Na tomto mieste sú uvedené minimálne požiadavky na heslo a prehliadač. Pri generovaní žiadosti prehliadač nesmie byť spustený v súkromnom/inkognito režime. Pri zabudnutí hesla je potrebné vygenerovať novú žiadosť, preto si heslo dôkladne uchovajte. Ak používate v prehliadači doplnok na mazanie cookies (napr. Cookie AutoDelete), vypnite si pre stránku Disig-u automatické mazanie cookies.

V dolnej časti stránky nájdete možnosť *Spustiť generovanie žiadosti*. Predtým, ako si zvolíte túto možnosť, je potrebné zakliknúť, že ste sa oboznámili s požiadavkami na heslo a prehliadač. Po potvrdení je už možné zvoliť možnosť *Spustiť generovanie žiadosti*.



2. V časti *Generovanie žiadosti* je potrebné zvoliť typ certifikátu, o ktorý chcete požiadať. Ako skupinu certifikátov zvoľte ***Certifikát pre e-mail*** a ako typ certifikátu vyberte ***Certifikát pre e-mail – Zamestnanec právnickej osoby***.



3. Ďalej je potrebné si zvoliť heslo podľa požiadaviek a vyplniť Vaše nasledujúce údaje:

Meno a priezvisko *(povinná položka):* Zadajte údaje z občianskeho preukazu. Pokiaľ máte titul zapísaný v OP a požadujete ho mať uvedený aj v certifikáte, zapíšte ho pred Vaše krstné meno **bez použitia čiarky**.

Meno *(povinná položka):* Uveďte Vaše krstné meno.

Priezvisko (*povinná položka*): Uveďte Vaše priezvisko.

Organizácia *(povinná položka):* Táto položka musí byť vyplnená hodnotou „Univerzita Pavla Jozefa Šafárika v Košiciach“.

ID organizácie *(povinná položka):* Ostáva predvolená možnosť *NTR (IČO)* a ako hodnota sa vkladá číslo *00397768.*

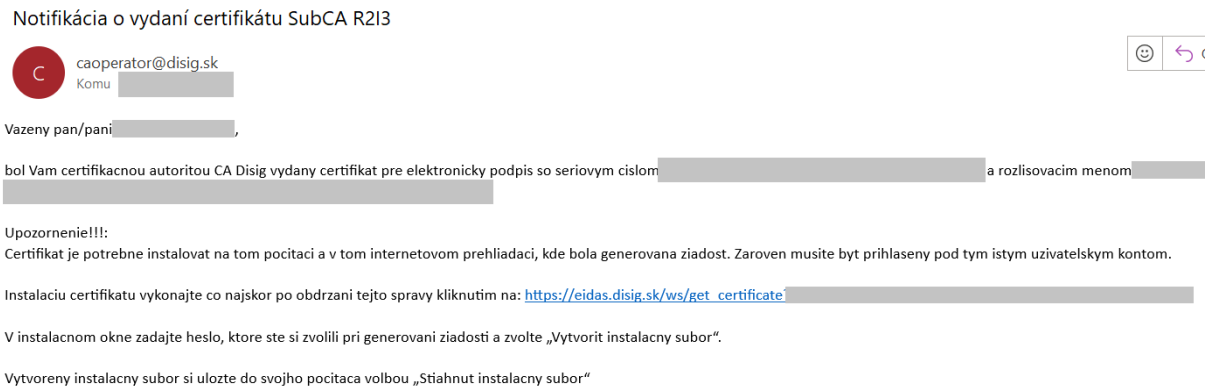
Mesto *(povinná položka):* Vypĺňa sa hodnotou Košice (aj keď je vo formulári uvedené že, je to podľa trvalého bydliska).

Štát *(povinná položka):* Hodnotu položky nie je potrebné meniť, ostáva SK - Slovakia.

E-mail *(povinná položka):* Uveďte pracovný (školský) e-mail, NIE súkromný.

4. Po vyplnení potrebných údajov vygenerujte žiadosť a zvoľte možnosť ***Stiahnuť žiadosť o certifikát***. Túto žiadosť o certifikát je potrebné poslať na **aio@upjs.sk.**

Po spracovaní žiadosti na AIO obdržíte informačný e-mail o vystavení Vášho certifikátu (viď. obrázok).



Inštalácia certifikátu

Postupujte podľa krokov popísaných v e-mailovej správe, resp. ich nájdete aj na odkaze https://eidas.disig.sk/sk/certifikaty/podpora/navody-k-certifikatom/instalacia-cert/.

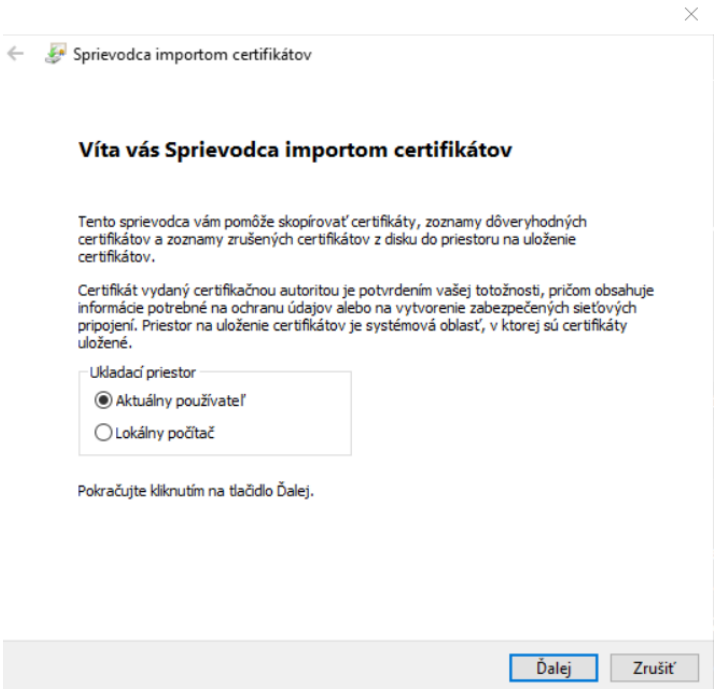
Inštalačný súbor odporúčame zálohovať (exportovať a uložiť na inú pamäťovú jednotku) pre prípad potreby opätovnej inštalácie. Prístup k súboru je chránený heslom, ktoré ste zadali pri generovaní žiadosti.

Importovanie certifikátu

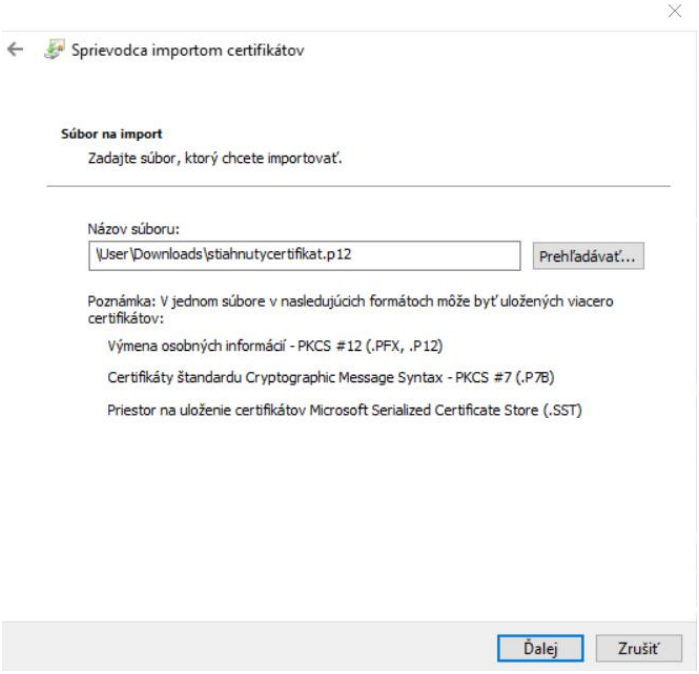
Návod na importovanie certifikátu je dostupný aj na stránke Disigu https://eidas.disig.sk/sk/certifikaty/podpora/navody-k-certifikatom/import-msie/.

V prípade potreby je možné importovať certifikát napr. aj do úložiska prehliadača Mozilla, návod je dostupný na https://eidas.disig.sk/sk/certifikaty/podpora/navody-k-certifikatom/import-mozilla/.

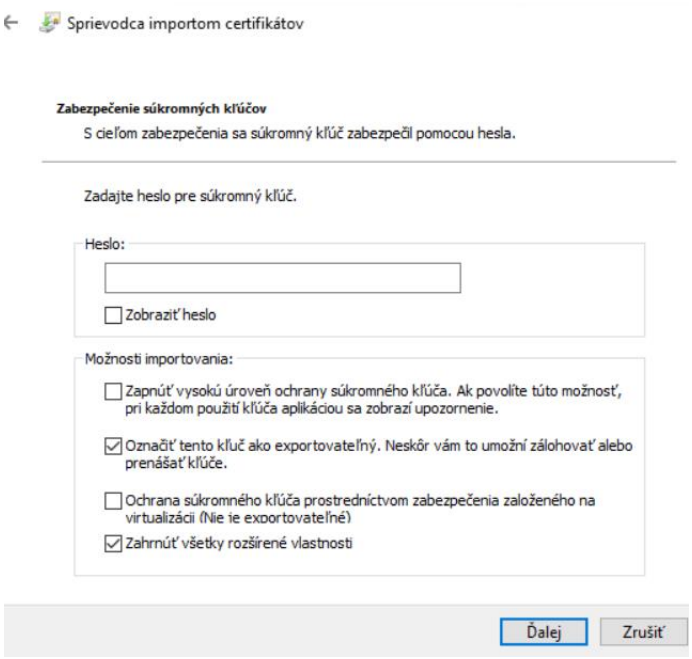
1. Import Vášho certifikátu začnete tak, že na súbor certifikátu 2x kliknete. Následne zvolíte možnosť ***Aktuálny používateľ*** a kliknete na tlačidlo ***Ďalej***.



2. Ďalej vyberiete súbor, ktorý chcete importovať, teda certifikát s koncovkou p12. Cez možnosť ***Prehľadávať*** sa viete dostať k miestu, kde ho máte uložený. Po vybratí súboru zvoľte možnosť ***Ďalej***.

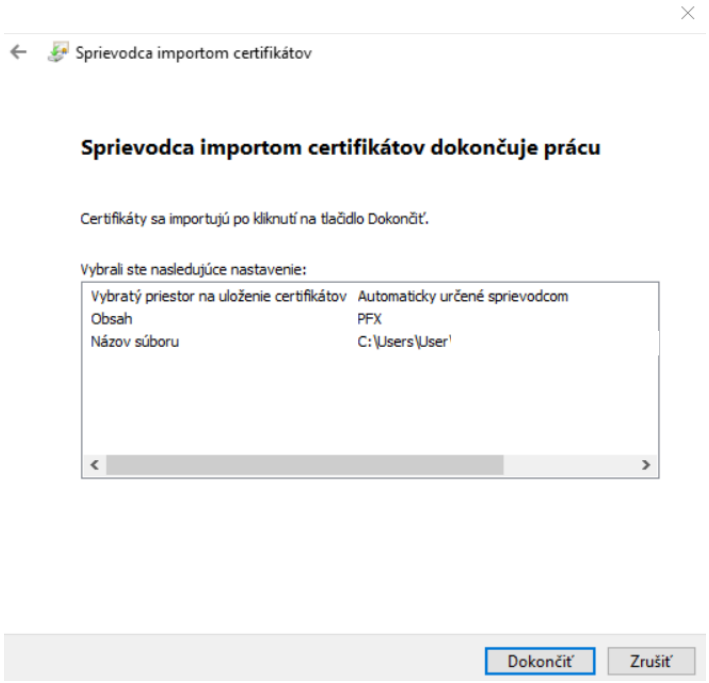


3. V časti *Zabezpečenie súkromných kľúčov* je nutné zadať *heslo*, ktoré ste zadali pri žiadosti, a zvoliť *Možnosti importovania*. V tomto prípade zaškrtnite možnosti **Označiť kľúč ako exportovateľný** (túto možnosť neodporúčame zvoliť iba v prípade, že certifikát importuje do zariadenia, ktoré nie je Vaše) a **Zahrnúť všetky rozšírené vlastnosti**. Následne zvoľte možnosť **Ďalej**.



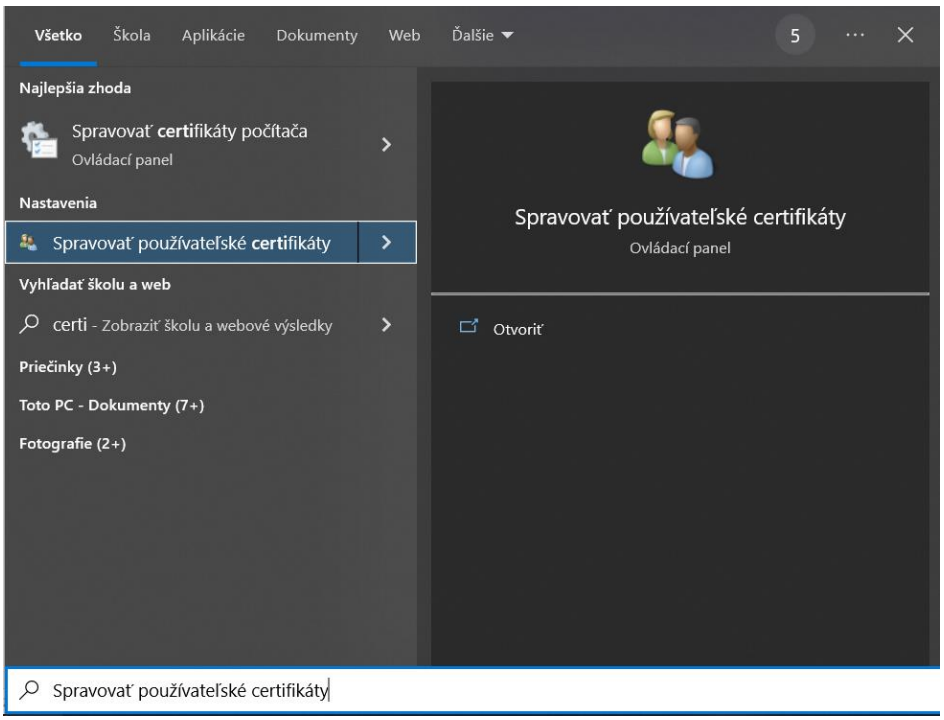
4. V časti *Priestor na uloženie certifikátov* zvoľte možnosť **Automaticky vybrať priestor na uloženie certifikátov podľa typu certifikátu**. Následne zvoľte možnosť **Ďalej**.

5. V poslednej časti sa nachádza zhrnutie nastavení, ktoré ste zvolili v predchádzajúcich krokoch. Ak je všetko správne, tak ako to vidíte na obrázku nižšie, môžete zvoliť možnosť **Dokončiť.** Toto je záverečný krok importovania Vášho certifikátu.

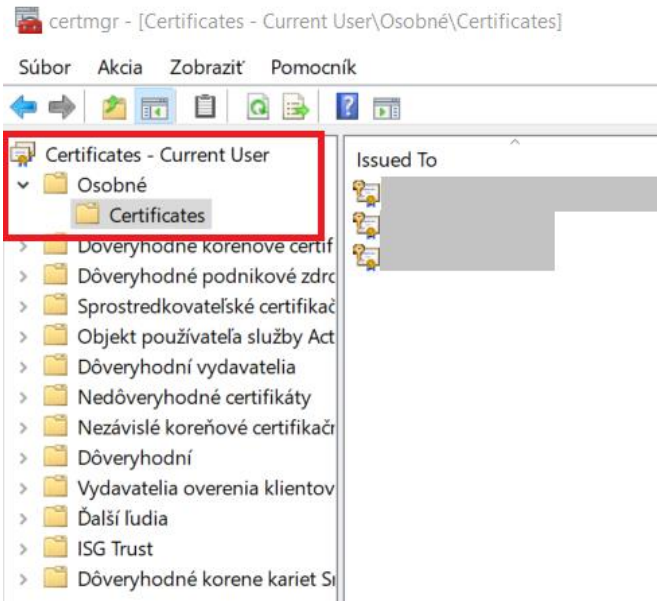


Exportovanie certifikátu

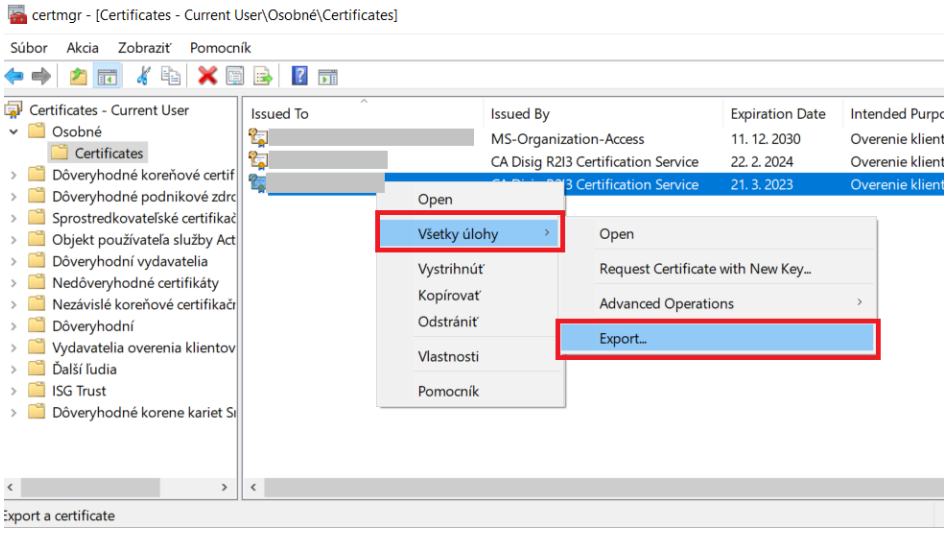
1. Otvorte aplikáciu *Spravovať používateľské certifikáty*



2. Navigujte sa do časti *Osobné – Certificates*.

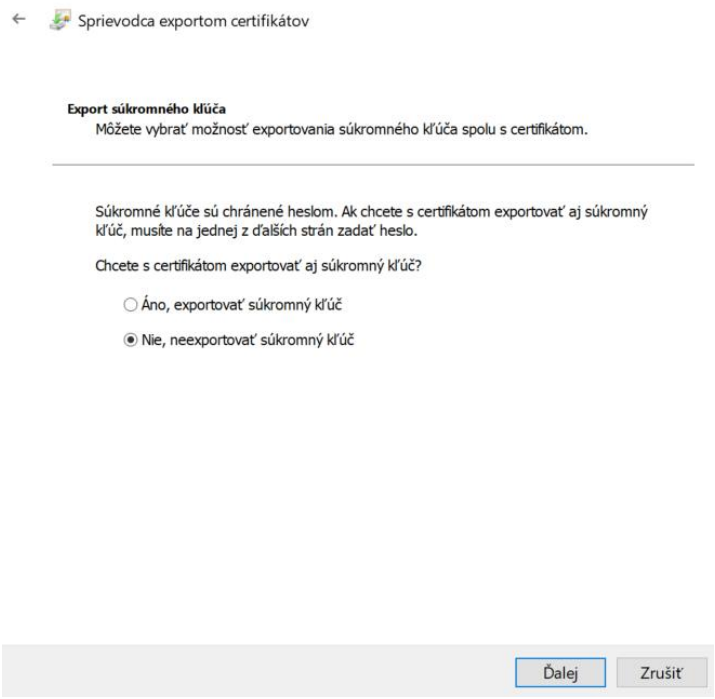


3. Kliknite pravým tlačidlom na certifikát, ktorý chcete exportovať. Kliknite na tlačidlo *Export*.



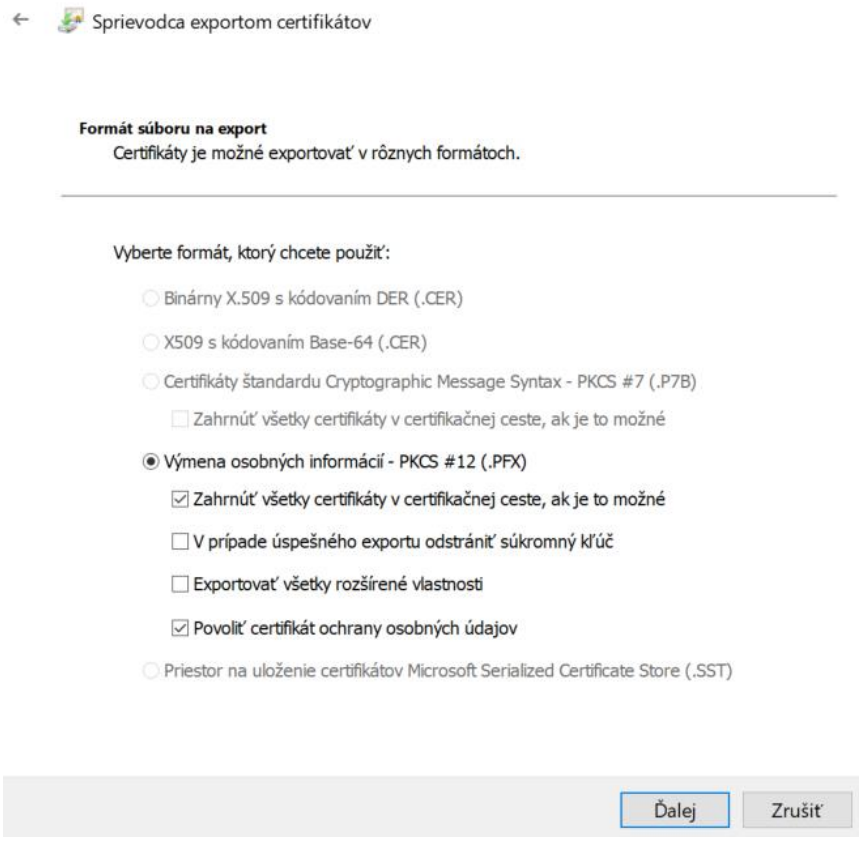
4. Otvoril sa sprievodca exportom certifikátu. Pokračujte kliknutím na *Ďalej.*

5. Podľa potreby vyberte z dvoch ponúkaných možností. Ak exportuje za účelom zálohy, zvoľte možnosť exportovať aj súkromný kľúč (táto možnosť je dostupná iba ak ste pri importe certifikátu označili certifikát ako exportovateľný). Ak chcete exportovať iba verejný kľúč (napr. s cieľom poslať ho niekomu inému), zvoľte možnosť *neexportovať súkromný kľúč.* Pokračujete kliknutím na *Ďalej.*

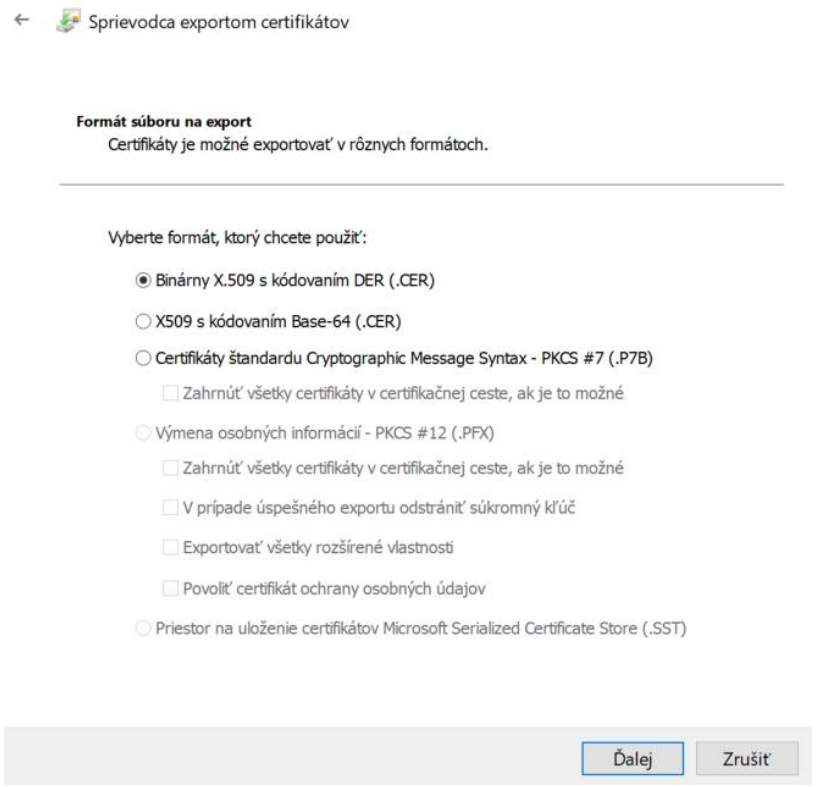


6.

a) Ak ste v predchádzajúcom kroku zvolili exportovanie súkromného kľúča, nastavte možnosti podľa obrázka (tieto nastavenia by mali byť predvolené). Kliknite na *Ďalej*.

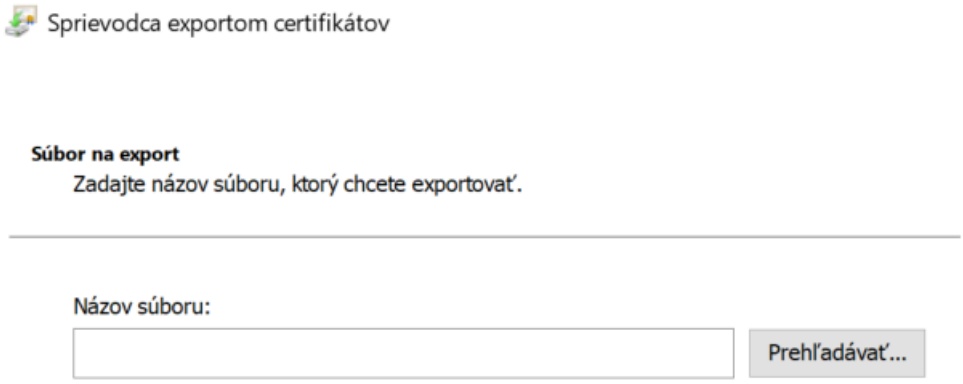


b) Ak ste v kroku 5. zvolili možnosť neexportovať súkromný kľúč, zvoľte nastavenie podľa obrázka (malo by to byť predvolené nastavenie). Kliknite na *Ďalej* a pokračujte krokom 8.



7. Napíšte heslo, ktorým bude chránený Váš privátny kľúč. Pokračujte voľbou "**Ďalej >**":

8. Zvoľte umiestnenie a názov pre váš exportovaný certifikát. Pokračujte kliknutím na *Ďalej*.



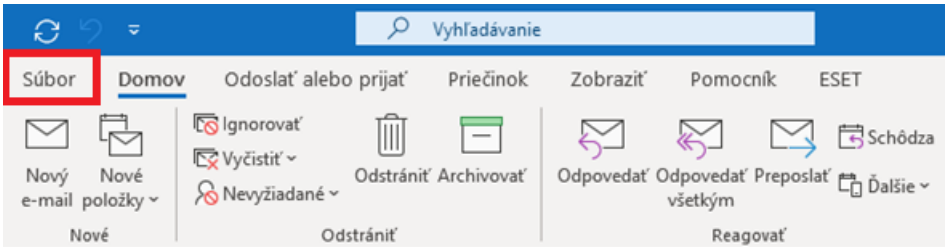
9. Zobrazí sa zhrnutie Vašich nastavení, ktoré si skontrolujte a export ukončite kliknutím na *Dokončiť.*

Využívanie certifikátu s poštovým klientom MS Outlook

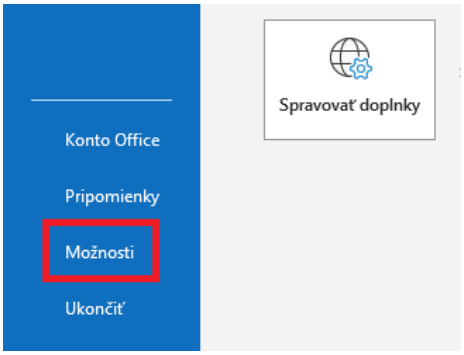
Poznámka: Nová verzia aplikácie Outlook, tzv. Outlook New zatiaľ nepodporuje S/MIME a teda ani používanie certifikátov na podpis.

Importovanie certifikátu

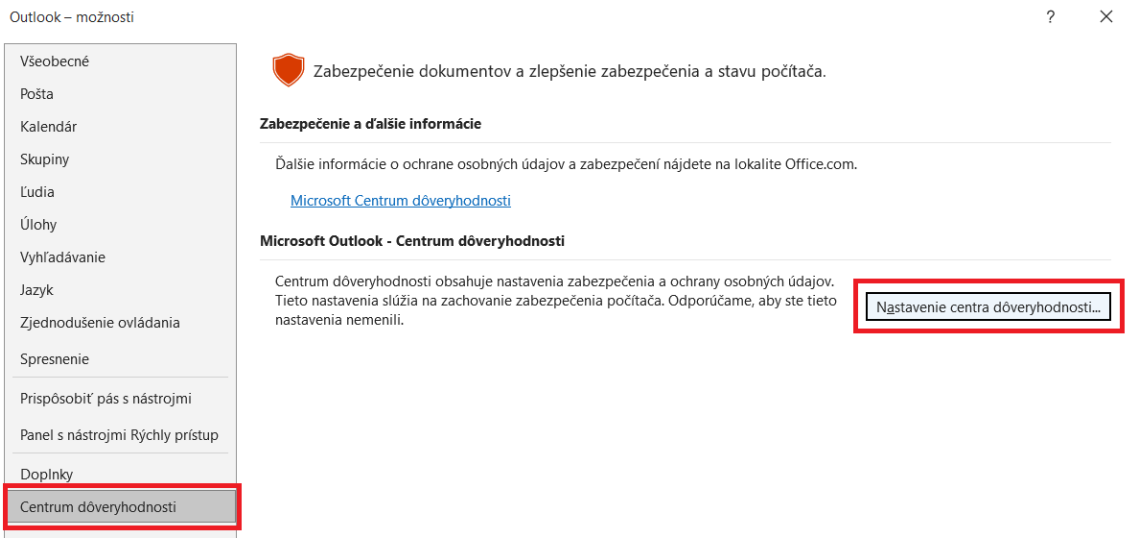
1. V aplikácii Outlook klikneme na možnosť ***Súbor*** v ľavom hornom rohu.



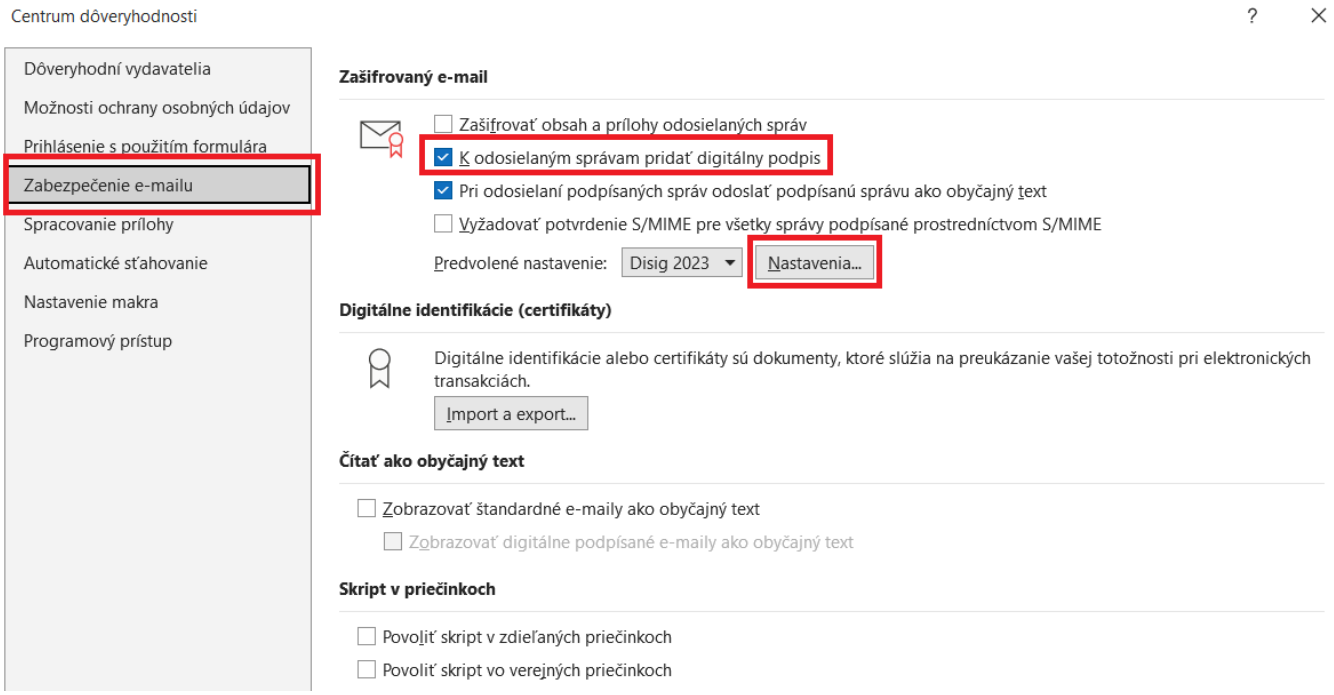
2. V ľavom dolnom rohu vyberieme ***Možnosti***.



3. Z bočného panela zvolíme ***Centrum dôveryhodnosti*** a následne ***Nastavenie centra dôveryhodnosti***.

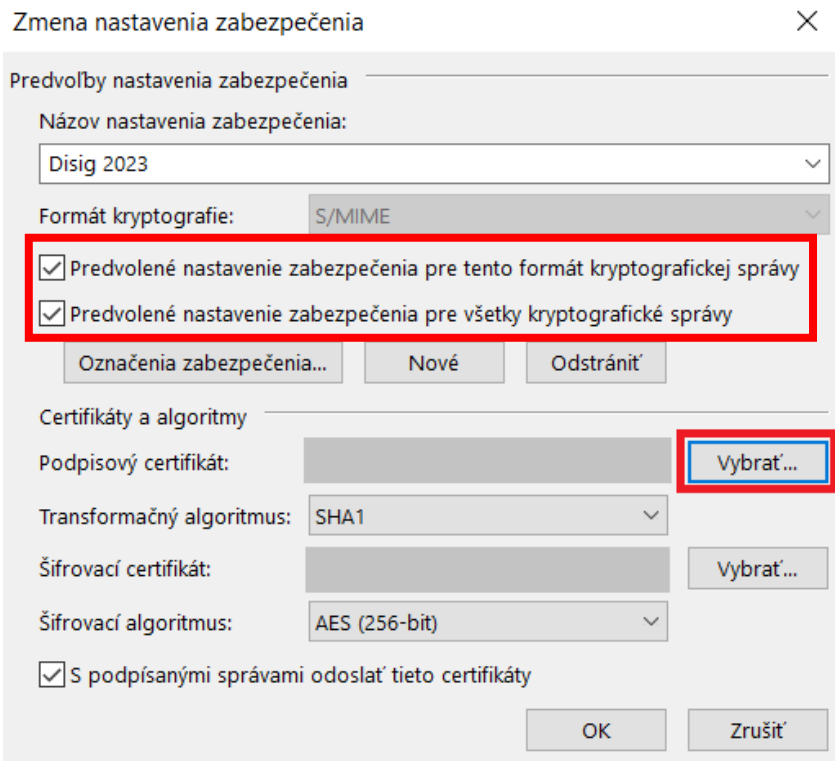


4. Zvolíme možnosť ***Zabezpečenie e-mailu***. Pre automatické pridanie digitálneho podpisu ku každej správe, môžeme označiť možnosť *K odosielaným správam pridať digitálny podpis*.

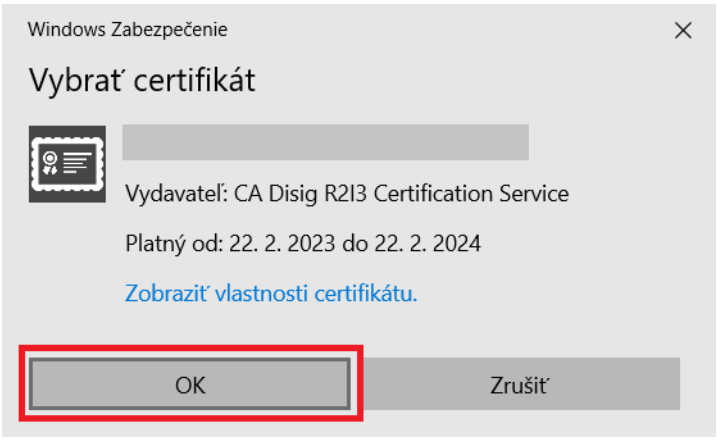


5. Otvorte *Nastavenia.*

6. Môžete si zvoliť vlastný názov nastavenia certifikátu. Skontrolujte, či sú zaškrtnuté políčka nastavenia zabezpečenia viď. obrázok. Pri možnosti ***Podpisový certifikát*** klikneme na *Vybrať.*

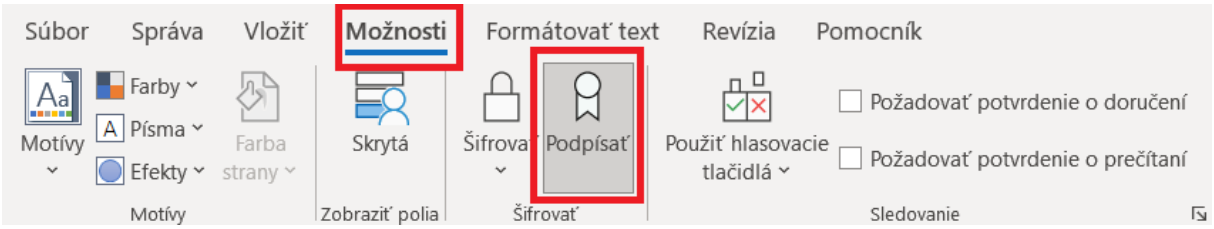


7. Vyberieme požadovaný certifikát a potvrdíme.



8. Všetky otvorené okná (Centrum dôveryhodnosti, Outlook - možnosti) zavrieme stlačením tlačidla OK, čím sa uložia nové nastavenia.

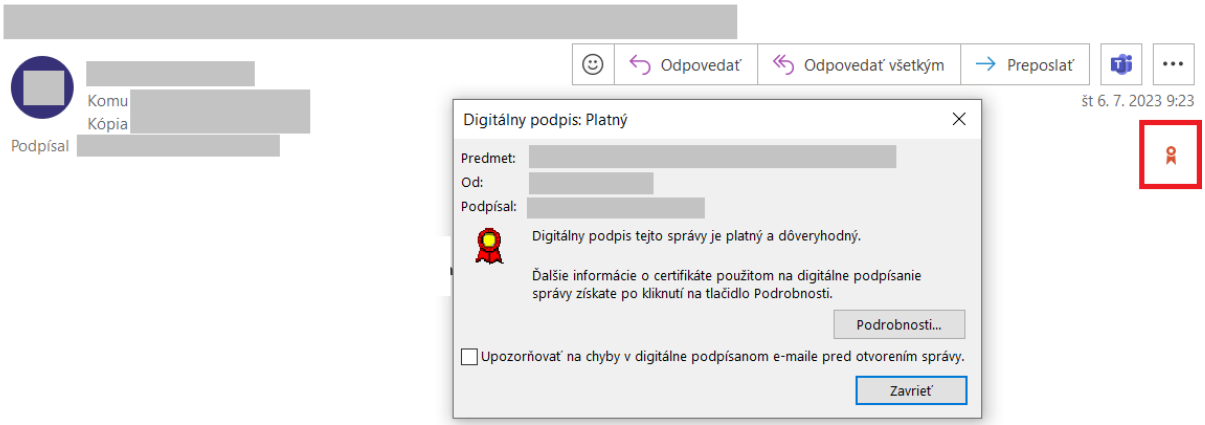
9. Správne nastavenie si môžete overiť pri písaní novej e-mailovej správy v časti *Možnosti*. Ak ste si nastavili automatické podpisovanie, ikonka *Podpísať* bude zvýraznená. Ak ste túto možnosť nezvolili, pre odoslanie podpísanej správy musíte najprv správu podpísať kliknutím na ikonku *Podpísať.*



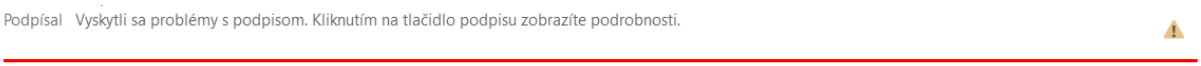
Overovanie dôveryhodnosti digitálneho podpisu v MS Outlook

1. Otvoríme správu, ktorá bola digitálne podpísaná, t.j. zobrazuje sa pri nej symbol pečate.

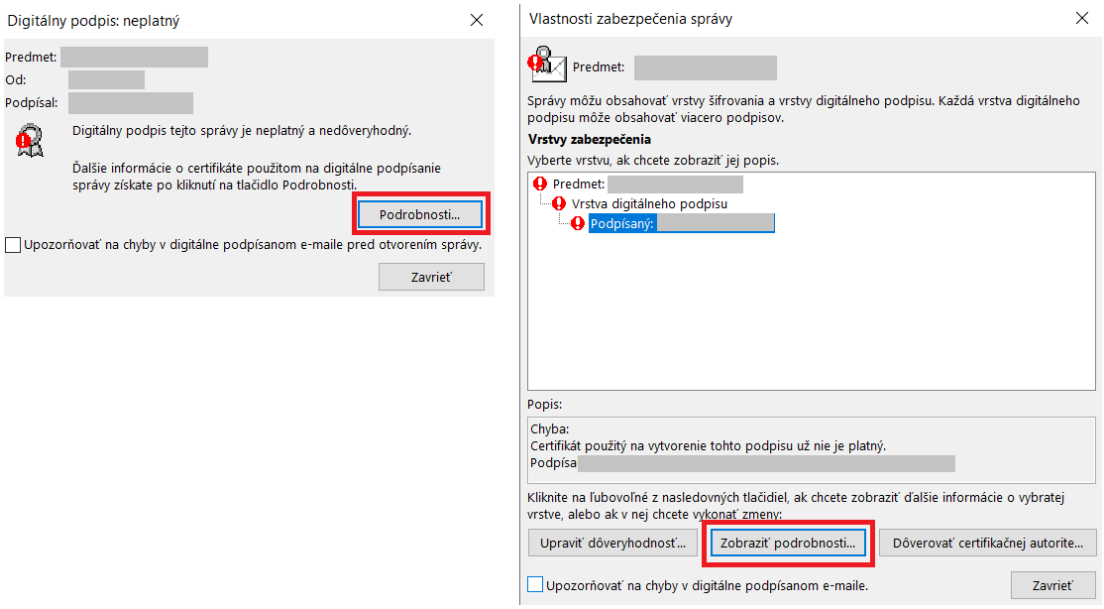
2. Na pravej strane klikneme na ikonu pečate, zobrazí sa nové okno s popisom digitálneho certifikátu.



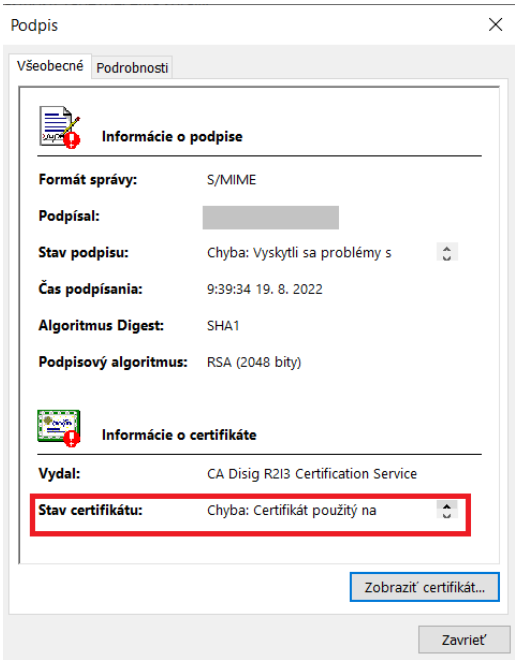
3. V prípade, že je podpis **neplatný**, na vrchu správy sa zobrazí upozornenie (viď. obrázok). Kliknutím na výstražný trojuholník (vpravo) sa zobrazia podrobnosti.



4. Podrobnosti, prečo je certifikát neplatný, si môžete pozrieť v *Podrobnostiach.* Označte najnižšiu vrstvu zabezpečenia, pri ktorej sa zobrazuje červený výkričník a kliknite na *Zobraziť podrobnosti...*



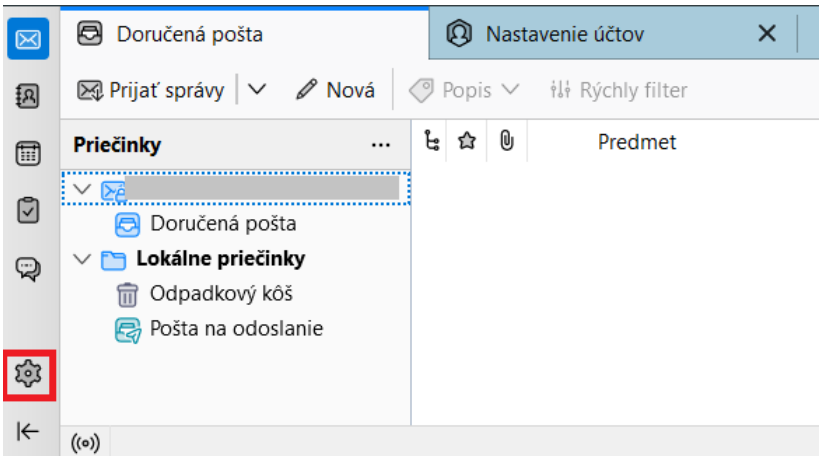
5. Tu si viete pozrieť napr. *Stav certifikátu* či *Zobraziť certifikát.* V tomto prípade sa jedná o certifikát, ktorému skončila (alebo ešte nezačala) platnosť, preto sa aj digitálny podpis zobrazil ako neplatný.



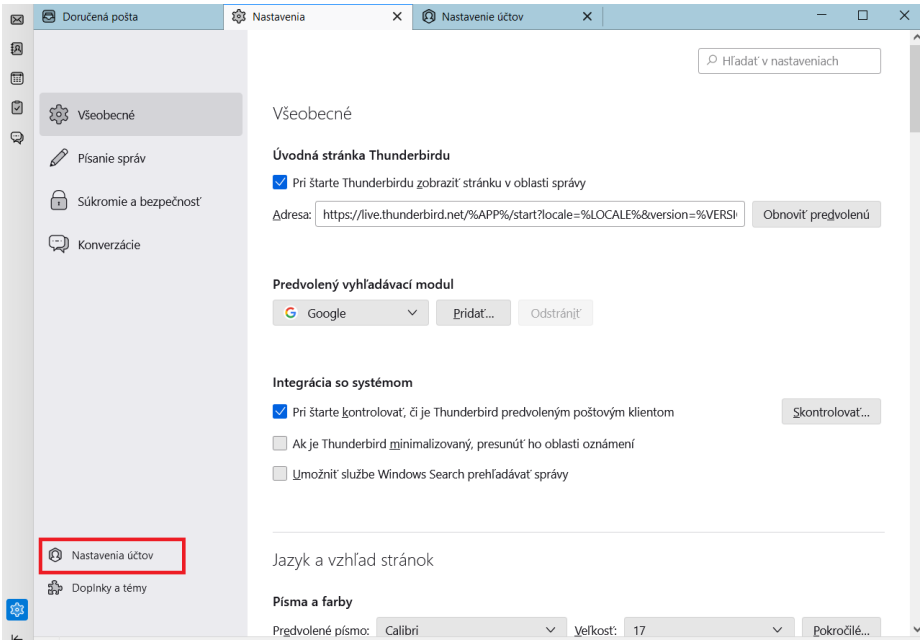
Využívanie certifikátu s poštovým klientom Thunderbird

Importovanie certifikátu

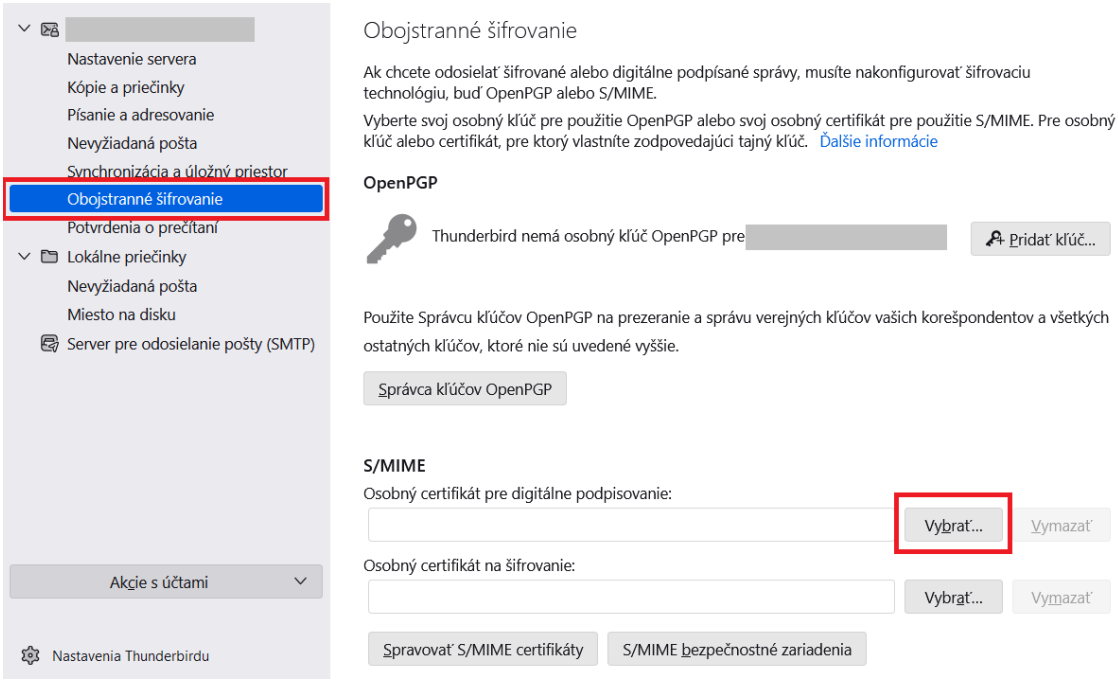
1. Prejdite do *Nastavení* kliknutím na ikonku v ľavom dolnom rohu.



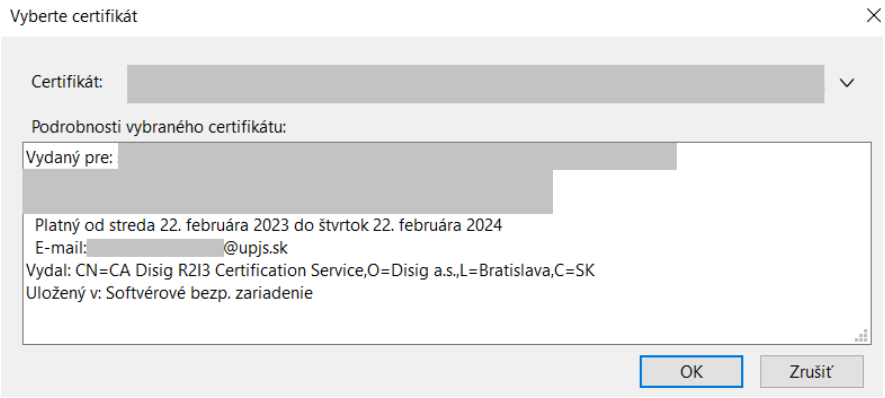
2. Kliknite na *Nastavenia účtov.*



3. Prejdite na *Obojstranné šifrovanie* a v sekcii *S/MIME* kliknite na *Vybrať* osobný certifikát pre digitálne podpisovanie.



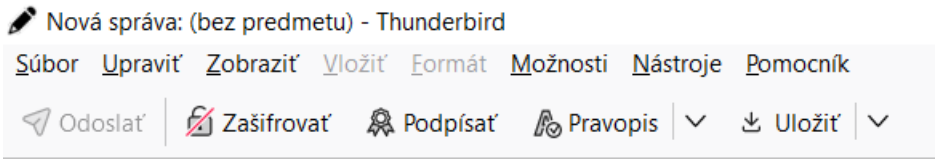
4. Vyberte svoj platný digitálny certifikát a potvrďte výber.



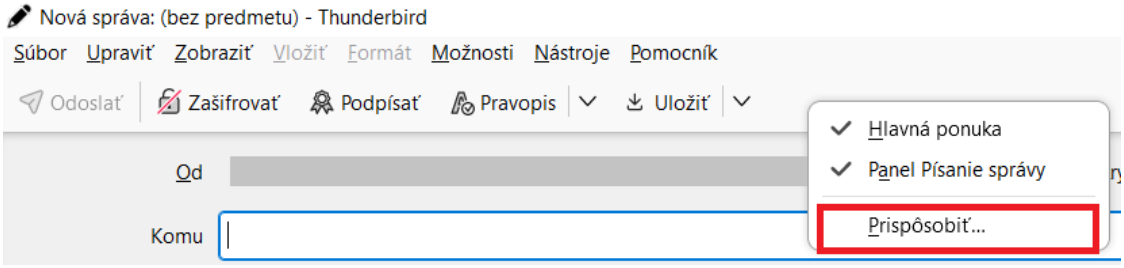
5. Zobrazí sa okno, či chcete nastaviť aj certifikát pre šifrovanie. Zvoľte nie.

Podpísanie správy

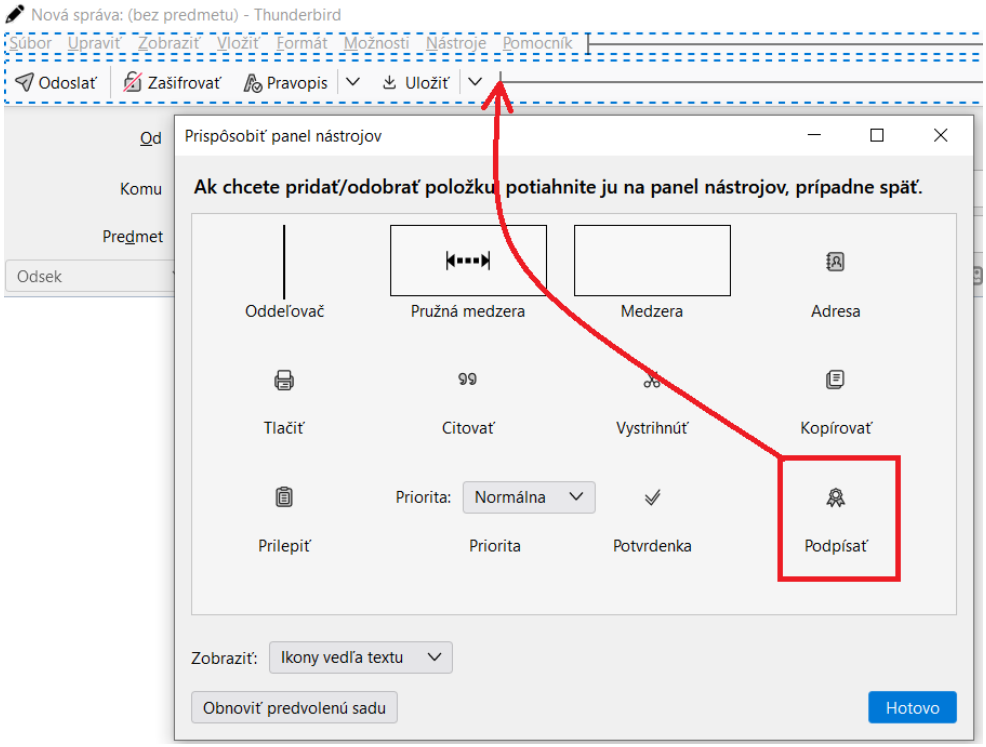
1. Ak sa vám pri písaní novej správy nezobrazuje v hornej lište možnosť *Podpísať* (viď. obrázok), je potrebné túto možnosť doplniť, preto pokračujete krokom 2 a 3. V opačnom prípade stačí správu podpísať podľa kroku 4.



2. Kliknite pravým tlačidlom myši na panel, kde sú možnosti ako Šifrovať, Pravopis, Uložiť... Zobrazí sa niekoľko možností, kliknite na *Prispôsobiť.*



3. Na novom okne nájdite možnosť *Podpísať* , kliknite na ňu a potiahnite ju na panel nástrojov, kde chcete, aby sa táto ikonka zobrazovala. Potom kliknite na *Hotovo.* Teraz by ste mali v paneli nástrojov vidieť aj možnosť *Podpísať*, podobne ako je to v kroku 1.



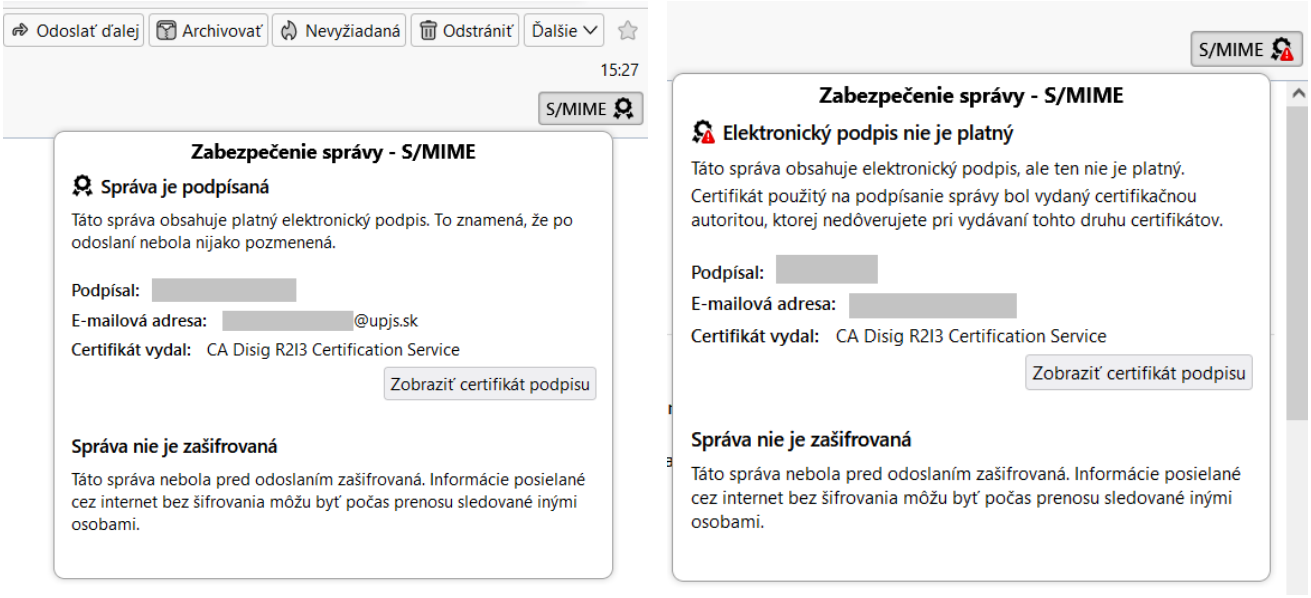
4. Pre podpísanie správy stačí kliknúť na *Podpísať.* Prvý krát môžete byť ešte požiadaní o výber certifikátu na podpis, kde si vyberiete Váš aktuálny certifikát.

Overenie dôveryhodnosti digitálneho podpisu v Thunderbird

Podpísané správy sa vyznačujú ikonou s popisom S/MIME v pravom hornom rohu. Kliknutím na ňu si môžeme pozrieť podrobnejšie informácie.

V prípade neplatného podpisu sa pri ikonke S/MIME zobrazí červená výstraha (pravý obrázok).

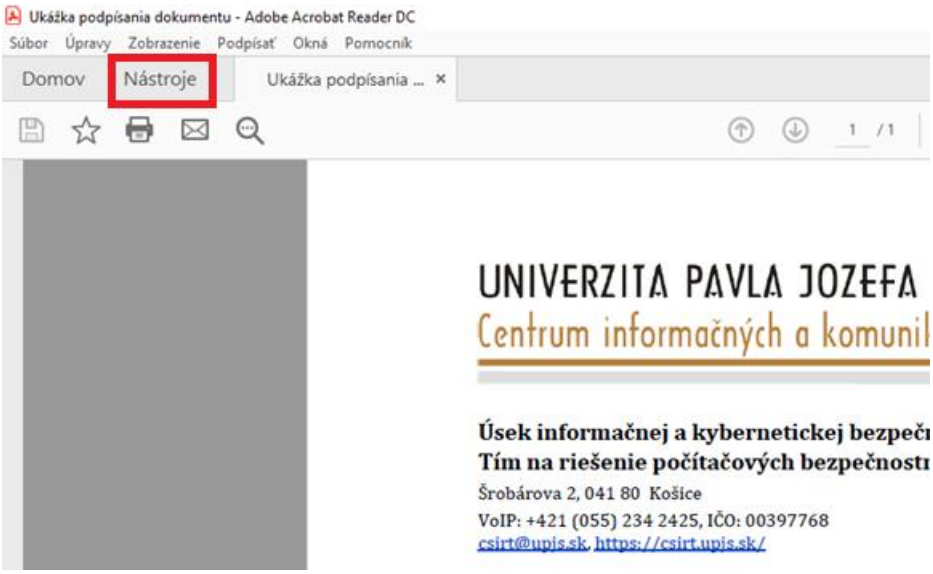
Kliknutím na *Zobraziť certifikát podpisu* si môžete pozrieť ďalšie detaily, napr. v akom období bol certifikát platný, kto tento certifikát vydal a pre koho.



Podpisovanie PDF dokumentu v Adobe Acrobat Reader DC

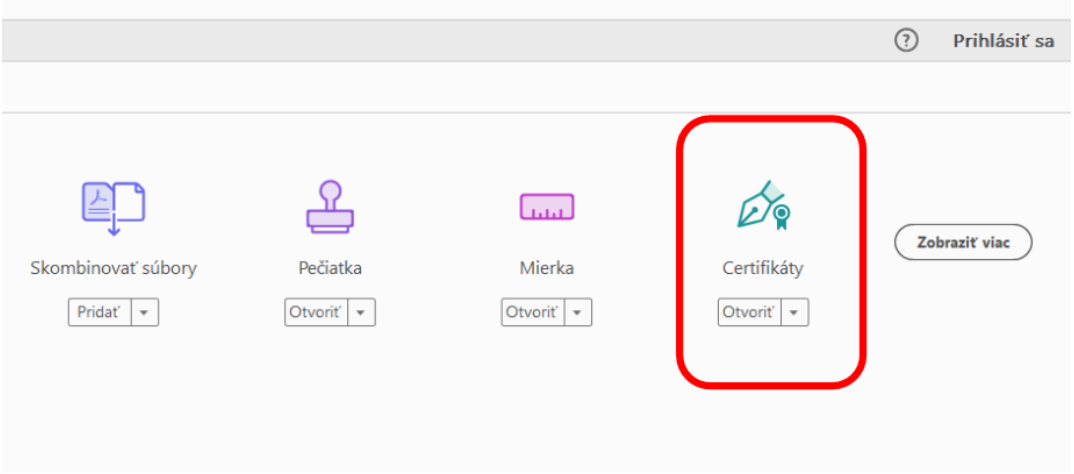
1. Otvoríme si dokument, ktorý chceme podpísať v Adobe Acrobat Reader DC.

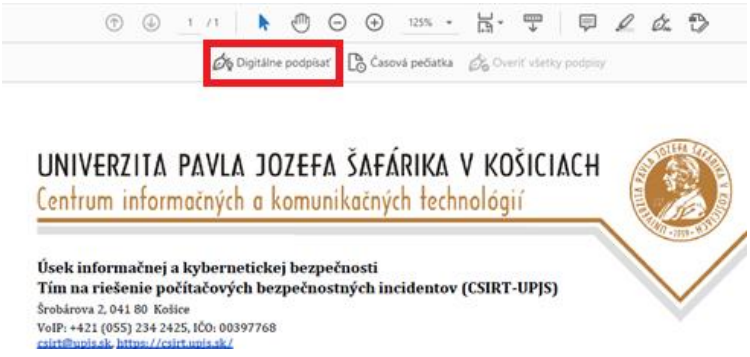
2. Zvolíme možnosť *Nástroje* v ľavom hornom rohu.



3. Vyberieme možnosť *Certifikáty*.

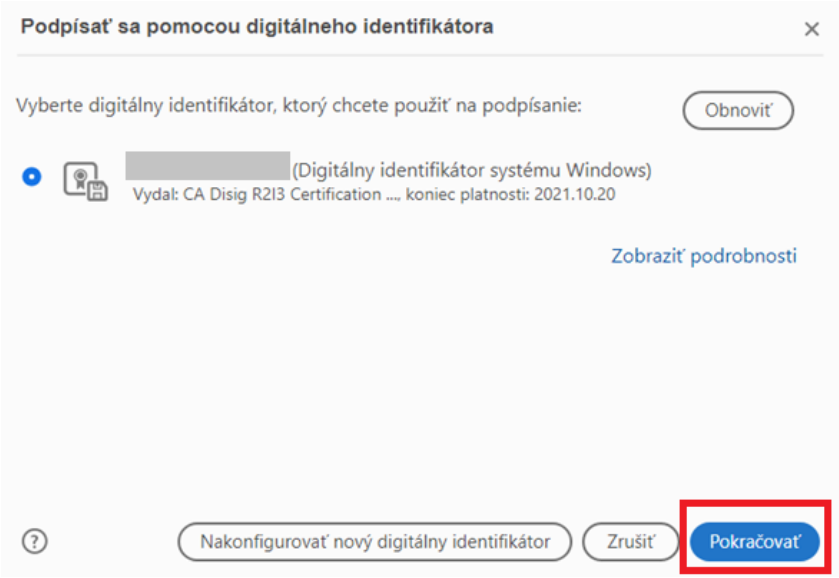
4. Na paneli nám pribudnú možnosti pre digitálny podpis. Vyberieme možnosť *Digitálne podpísať*.





5. Zobrazí sa okno s inštrukciami pre výber oblasti pre podpis. Stačí kliknúť myšou a potiahnuť, čím sa vyznačí oblasť pre digitálny podpis. Kliknite na *OK* a zobrazí sa okno na výber digitálneho certifikátu.

6. Vyberte podpis, ktorý chcete použiť a zvoľte *Pokračovať*.



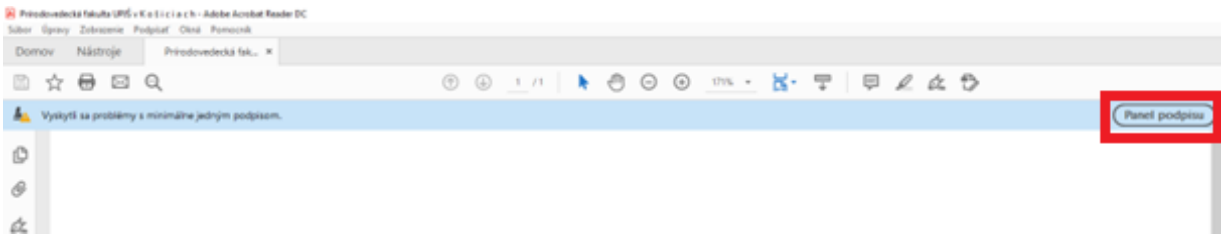
7. Zobrazí sa okno s náhľadom podpisu, zvoľte možnosť Podpísať.

8. Podpíšte dokument na požadovanom mieste potiahnutím myšou a uložte dokument.

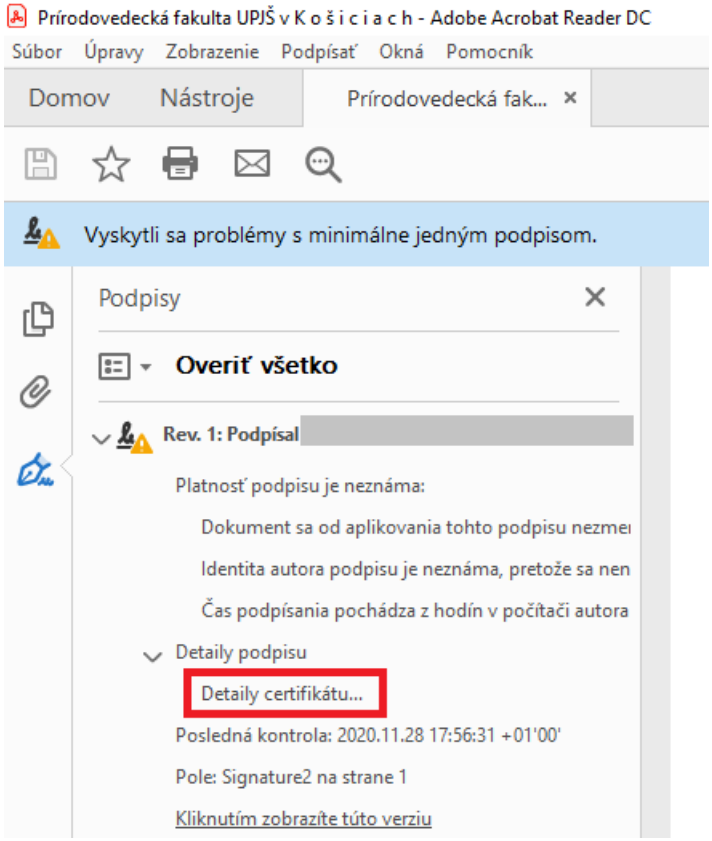
Pridanie certifikačnej autority Disig, a.s. na zoznam dôveryhodných certifikačných autorít

Pri prvej práci s elektronickými podpismi v Acrobat Reader je potrebné pridať certifikačnú autoritu Disig na zoznam dôveryhodných certifikačných autorít.

1. Otvoríme podpísaný PDF dokument. Zvolíme možnosť *Panel podpisu*.

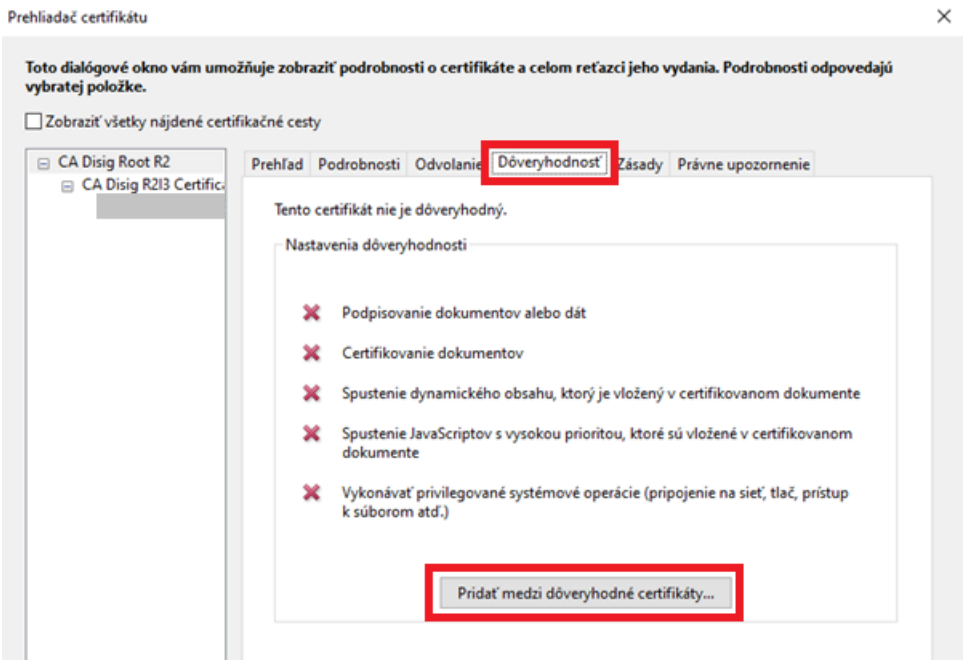


2. Zvolíme možnosť *Detaily certifikátu*.



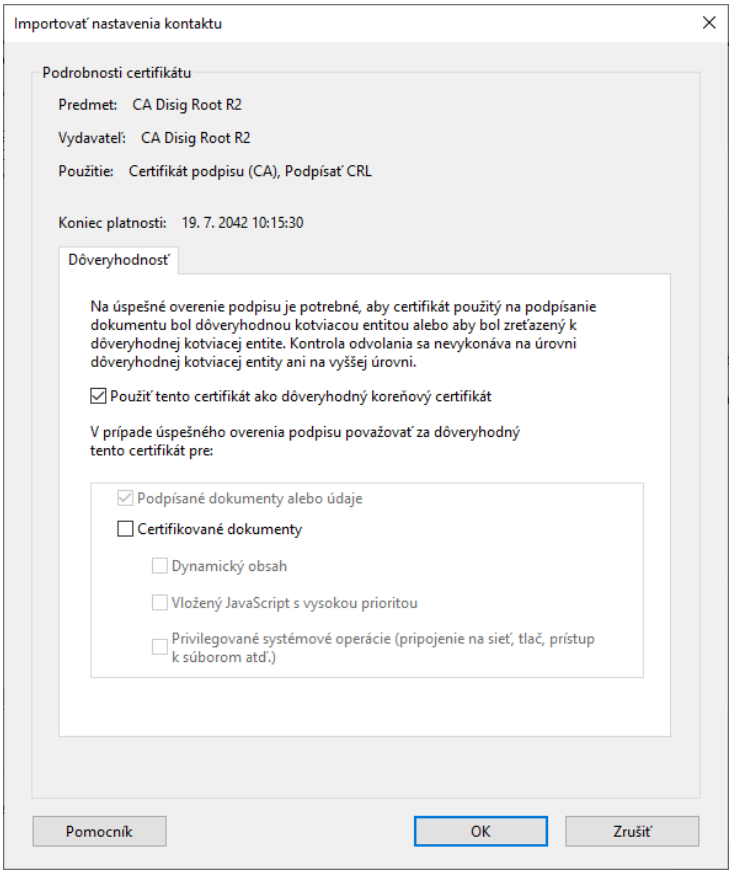
3. Otvorí sa okno *Prehliadač certifikátu*, kde v ľavom paneli vyberieme možnosť CA Disig Root R2.

4. Vyberieme kartu *Dôveryhodnosť* a zvolíme možnosť *Pridať medzi dôveryhodné certifikáty*.

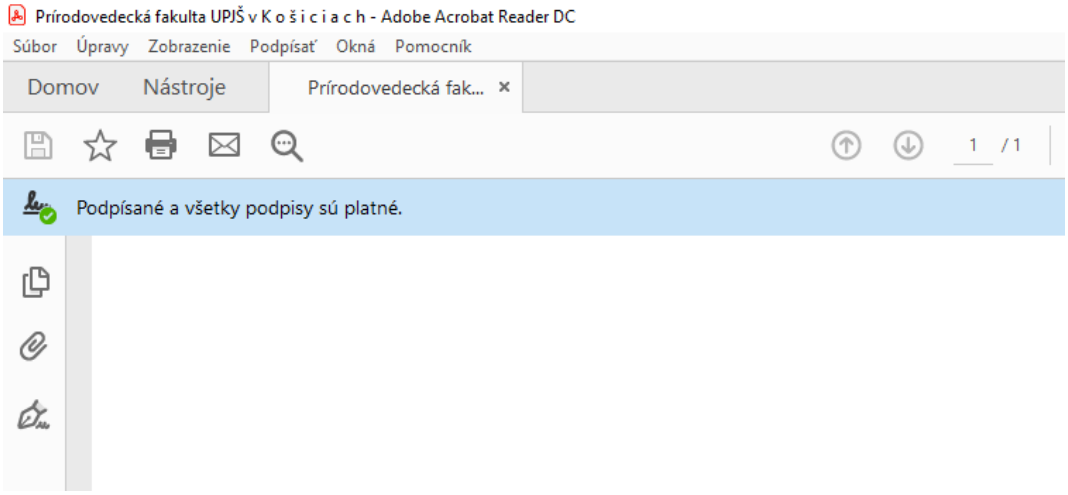


5. Zobrazí sa potvrdzujúce okno, kde kliknite OK.

6. Zobrazí sa okno *Importovať nastavenia kontaktu.* Opäť len klikáme *OK*.



Po úspešnom overení podpisu sa bude na vrchu dokumentu zobrazovať, že sú všetky podpisy platné.



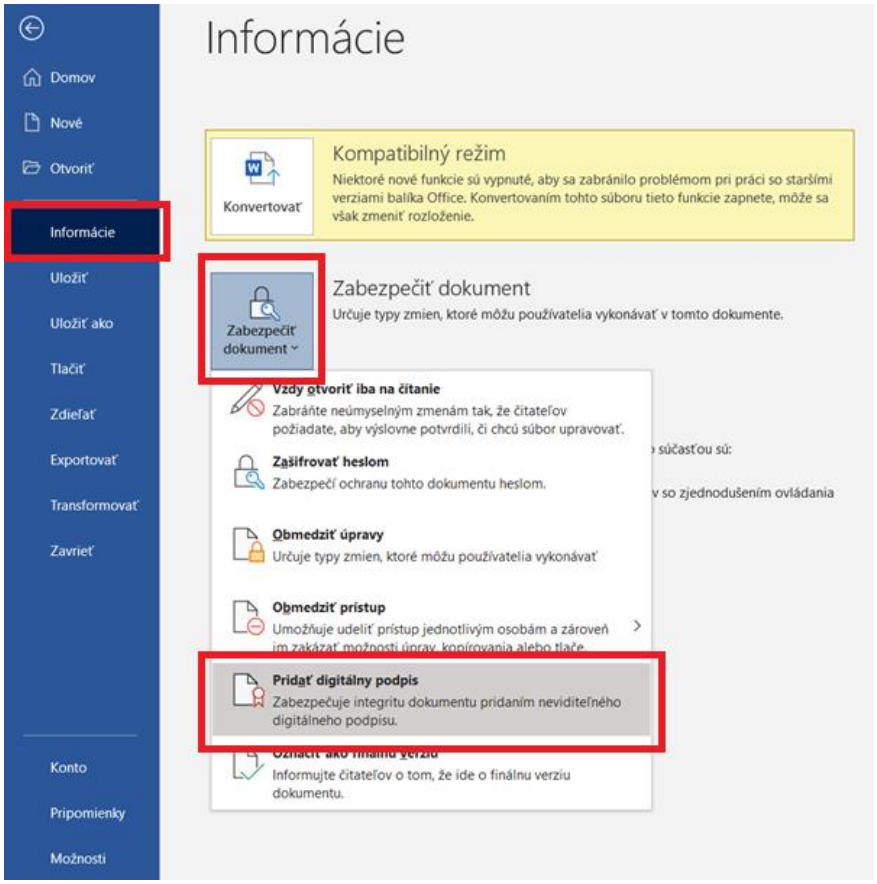
Podpisovanie Microsoft Word dokumentu

Textový dokument musí byť vo svojej finálnej podobe a musí byť uložený. Elektronické podpisovanie vykonávame ako posledný krok.

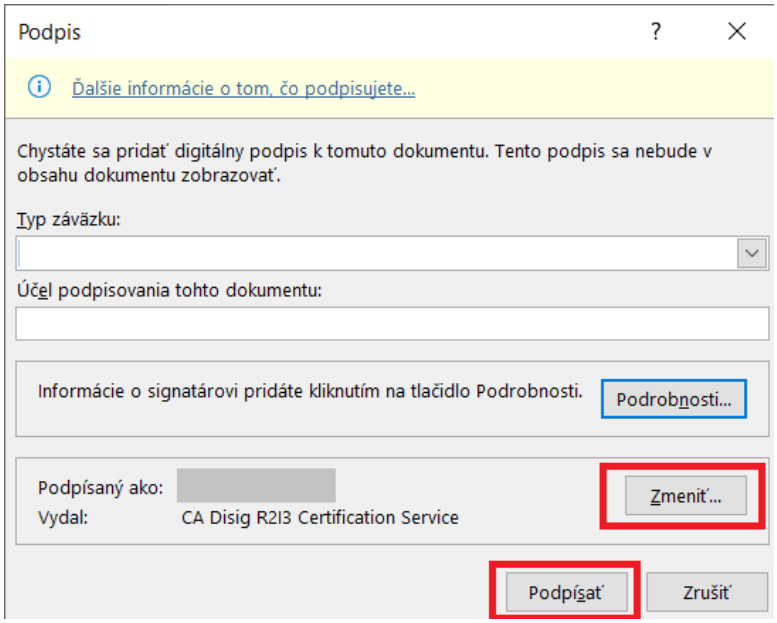
Podpis môžeme realizovať vložením viditeľného podpisu, ktorý sa zobrazí priamo v dokumente alebo podpisom bez vloženia riadku na podpis do dokumentu.

Pridanie neviditeľného podpisu

1. V časti *Súbor* prejdeme na sekciu *Informácie.* Klikneme na možnosť *Zabezpečiť dokument* a zvolíme možnosť ***Pridať digitálny podpis.***

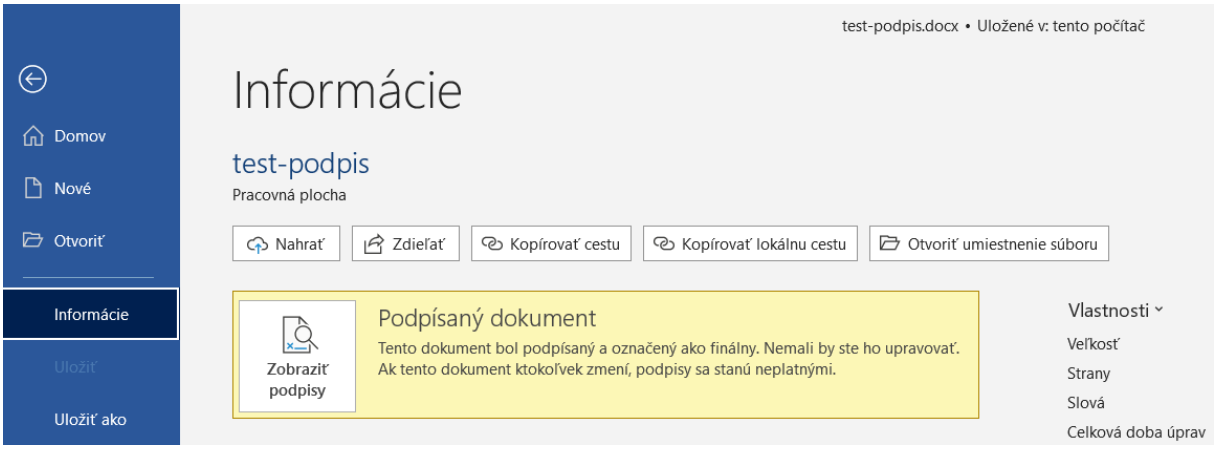


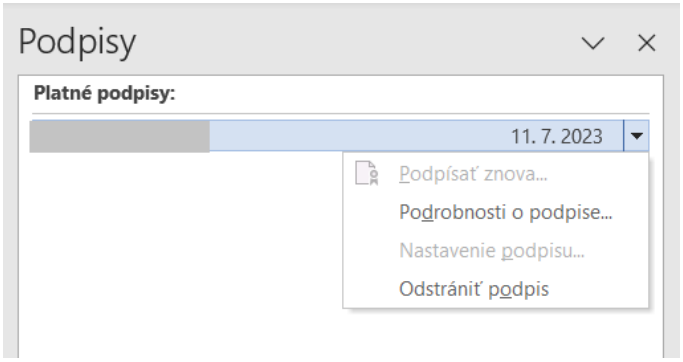
2. Zobrazí sa okno podpisu, kde môžete vyplniť viaceré nepovinné polia, ktoré popisujú účely podpisovania dokumentu ako aj podrobností o osobe, ktorá dokument podpisuje.



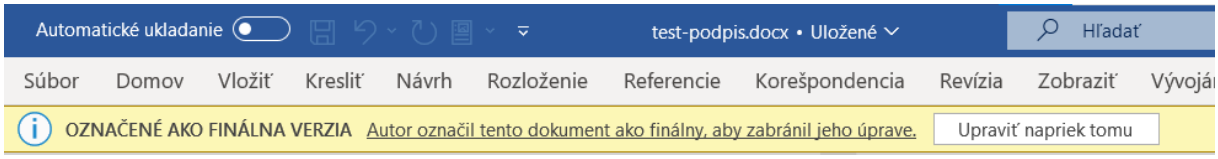
Na pridanie alebo zmenu digitálneho podpisu kliknite na tlačidlo *Zmeniť* a zvoľte Váš platný Disig certifikát.

3. Podpíšte dokument kliknutím na *Podpísať.* Zobrazí sa hlásenie o podpísaní dokumentu. V časti *Súbor, Informácie* sa zobrazí informácia o tom, že je dokument podpísaný. Kliknutím na túto informáciu sa otvorí tabla s podpismi, kde si viete pozrieť podrobnosti alebo podpis odstrániť.



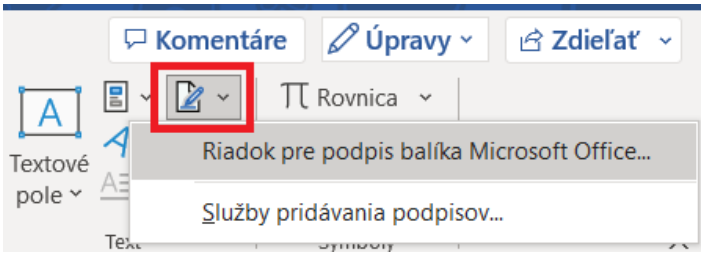


Dokument sa zároveň automaticky označí ako finálna verzia, čo sa zobrazuje aj v hornej časti po otvorení dokumentu (viď. obrázok).

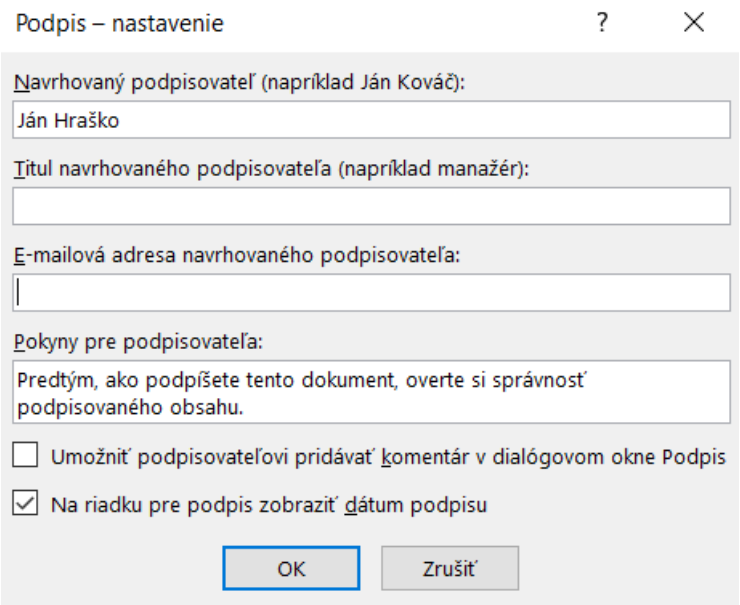


Pridanie viditeľného podpisu

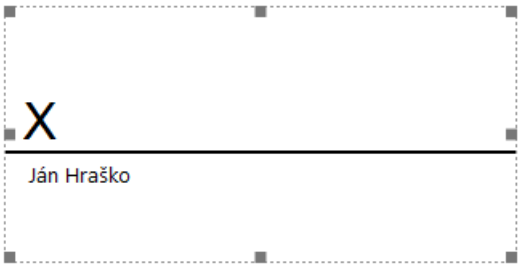
1. V časti *Vložiť*, na pravej strane kliknite na vyznačenú ikonku a zvoľte možnosť *Riadok pre podpis balíka Microsoft Office.*



2. Zobrazí sa okno, kde si môžete nastaviť text, ktorý sa má zobraziť pri riadku na podpis. Vyplňte podľa potreby a potvrďte to.

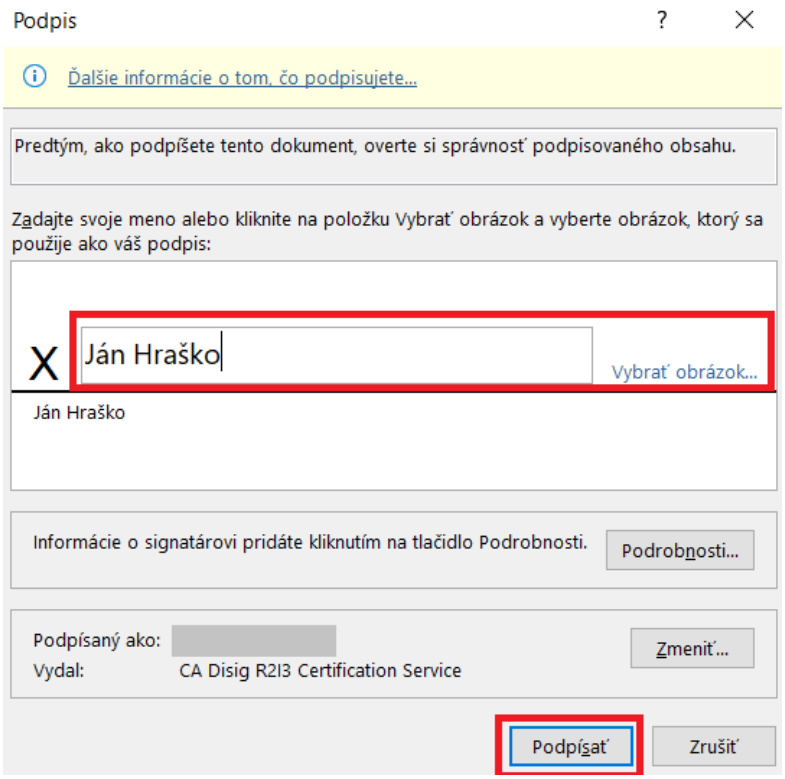


3. Do dokumentu sa vloží riadok pre podpis.



4. Dvakrát rýchlo kliknite na pole s riadkom pre podpis. Zobrazí sa okno na podpísanie dokumentu. Zadajte meno alebo obrázok, ktorý sa použije ako Váš podpis. V dolnej časti skontrolujte, či je zvolený správny certifikát na podpis a kliknite na *Podpísať.*

UPOZORNENIE: pri prvom podpisovaní môže podpisovanie prebiehať aj niekoľko minút.



5. Dokument sa automaticky označí ako finálna verzia. Dvojitým kliknutím na riadok podpisu alebo v informáciách o dokumente je možné skontrolovať vytvorený podpis.

Obnovenie platnosti certifikátu

Mesiac pred ukončením platnosti Vášho digitálneho certifikátu Vám príde od Disig-u notifikácia o ukončení platnosti. Ak aj naďalej potrebujete využívať digitálny certifikát, je potrebné vygenerovať si novú žiadosť o vydanie certifikátu a zaslať ju na správu AIO – postup je úplne rovnaký ako pri prvom generovaní žiadosti.

Po obdržaní certifikátu je potrebné si nový certifikát opäť nainštalovať a importovať do zariadenia. Odporúčané je certifikát si opäť zálohovať.

Ďalej je potrebné vykonať zmenu vo všetkých službách, kde tento certifikát používate. Všetky postupy ostávajú rovnaké, je však potrebné dbať na výber správneho certifikátu, teda pozerajte na dátum platnosti (starý certifikát si zachovajte, môže sa zísť pri dešifrovaní).

Slovník pojmov

Certifikát

Certifikát (inak aj certifikát verejného kľúča) je elektronický dokument, ktorým vydavateľ certifikátu (certifikačná autorita) potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný. Certifikát je určený na overovanie správnosti elektronického podpisu, a to na základe overenia pomocou prislúchajúceho verejného kľúča a overenia platnosti identifikačných údajov o osobe, ktorej bol certifikát vydaný.

Certifikát má obmedzenú dobu platnosti. Po uplynutí doby platnosti alebo po zrušení certifikátu sa certifikát nesmie používať, a to ani na účel, na ktorý je určený

Certifikačná autorita alebo
Poskytovateľ dôveryhodných služieb

Poskytovateľ dôveryhodných služieb je entita, ktorá vydáva, overuje, validuje a uchováva digitálne certifikáty, elektronické podpisy, pečate a pod.

Elektronický podpis

Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať požiadavky zákona č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

Elektronický podpis predstavuje elektronickú obdobu klasického podpisu. Obidva typy podpisov (klasický aj elektronický) slúžia na potvrdenie autenticity podpisovaného dokumentu a na identifikáciu autora podpisu. Na jeho vytvorenie je potrebné, aby autor vlastnil súkromný kľúč a k nemu prislúchajúci certifikát, pričom identitu autora podpisu potvrdzuje dôveryhodná tretia strana - certifikačná autorita. Pomocou kryptografických algoritmov a súkromného kľúča je vytvorená štruktúra, ktorá je následne spolu s certifikátom prislúchajúcim k použitému súkromnému kľúču pripojená k elektronickému dokumentu. Prostredníctvom tejto štruktúry s použitím pripojeného certifikátu je možné kedykoľvek neskôr zistiť, či elektronický dokument je autentický alebo v ňom boli vykonané zmeny.

S/MIME

S/MIME poskytuje šifrovanie, ktoré chráni obsah e-mailových správ, a digitálne podpisy, ktoré overujú totožnosť odosielateľa.

Súkromný kľúč

Súkromným kľúčom je tajná informácia, ktorá slúži na vyhotovenie elektronického podpisu elektronického dokumentu.

Verejný kľúč

Verejným kľúčom je informácia dostupná adresátovi (overovateľovi) podpísaného elektronického dokumentu, ktorá slúži na overenie pravosti elektronického podpisu vyhotoveného pomocou odpovedajúceho súkromného kľúča.