

Přístup do Cloudu ESO9 z OS Windows – žádost o certifikát z certifikační authority



ESO9 international a.s.
U Mlýna 22
141 00, Praha

..... www.eso9.cz

Úvod.....	3
Nastavení před žádostí o certifikát.....	3
Nastavení Microsoft Edge.....	4
Žádost o certifikát a jeho instalace.....	5
Vystavení žádosti o vydání klientského certifikátu.....	5
Stažení a instalace certifikátu na PC klienta.....	6
Přístup do aplikace.....	7
Problémy při instalaci - kořenový certifikát.....	7
Export a import certifikátu.....	8
Export nainstalovaného certifikátu.....	8
Import certifikátu ve Windows.....	11

Úvod

Pro přístup do aplikace provozované na Cloudu ESO9 musí mít uživatel nainstalovaný klientský certifikát. Tento certifikát je pro každého uživatele jedinečný. Dokument popisuje postup žádosti a instalace z webového prostředí certifikační autority, pro nové žádosti (u nových uživatelů).

- O certifikáty (zejména v případě obnovy existujícího certifikátu) lze také žádat přímo ze zákaznické aplikace ESO9, viz samostatný dokument **Obnova certifikátu ze zákaznické aplikace ESO9**.

Z webového prostředí certifikační autority lze zažádat o certifikát pouze v prohlížečích Internet Explorer a Microsoft Edge!

- Ostatní prohlížeče v operačním systému Windows (např. Google Chrome) používají certifikáty nainstalované ve Windows.
- Postup zprovoznění certifikátu v mobilních zařízeních (Android, iOS) nebo Apple zařízeních je uveden v samostatném dokumentu **Přístup do Cloudu ESO9 ze zařízení s Androidem a z Apple (iOS, macOS) - import a nastavení certifikátu**.

POZOR, po žádosti nezavírejte prohlížeč. Při jeho ukončení (zavření) se ztratí vazba mezi žádostí a schváleným certifikátem. V takovém případě pak certifikát nebude možné nainstalovat.

Po schválení žádosti je třeba certifikát nainstalovat. Po instalaci se musí do aplikace zapsat číslo nového certifikátu. Zapsání nového čísla certifikátu do aplikace se neděje se automaticky, protože by poté nebyl funkční přístup původním certifikátem. Podrobnější popis celého postupu, od žádosti přes instalaci až po případný export a import certifikátu, je uveden níže.

Certifikáty si musí zákazník (uživatel) zálohovat sám, na straně poskytovatele (ESO9 international a.s.) nejsou certifikáty uživatelů zálohovány.

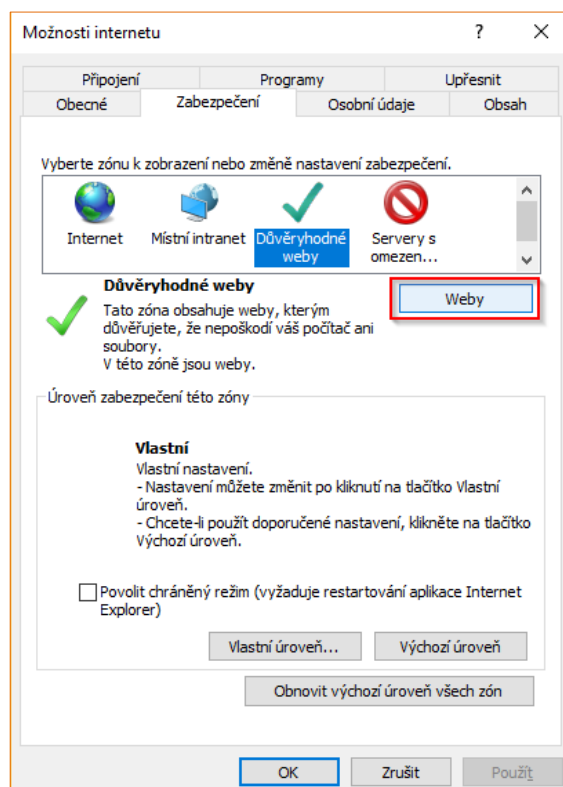
Při blížícím se konci platnosti certifikátu je na toto uživatel upozorněn při přístupu do aplikace. Vystavení nového certifikátu mimo aktuální platnost původního certifikátu je zpoplatněno dle platného Ceníku služeb.

Nastavení před žádostí o certifikát

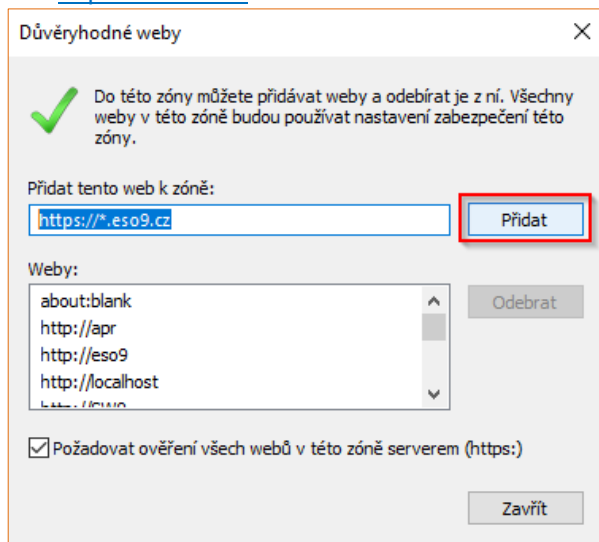
Před samotnou žádostí a instalací certifikátu je třeba přidat web certifikační autority **mezi důvěryhodné servery**.

V opačném případě nebude možné o certifikát zažádat.

Je třeba otevřít **Ovládací panely**, např. přes vyhledávání z hlavního panelu. Poté zvolit (vyhledat) **Možnosti internetu**. Zde na záložce Zabezpečení vybrat ikonu Důvěryhodné servery/weby a pak použít tlačítko **Weby** (případně Servery):



Zde tlačítkem **Přidat** adresu ve tvaru https://*.eso9.cz:

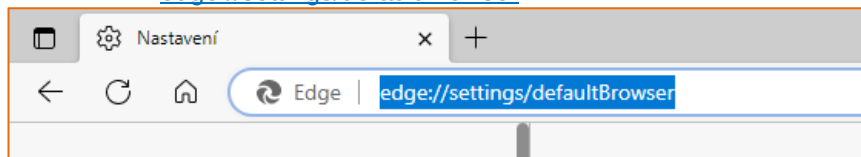


Následně lze v Internet Exploreru přejít k žádosti o certifikát.

V **Microsoft Edge** je navíc třeba nastavit kompatibilitu s Internet Explorerem.

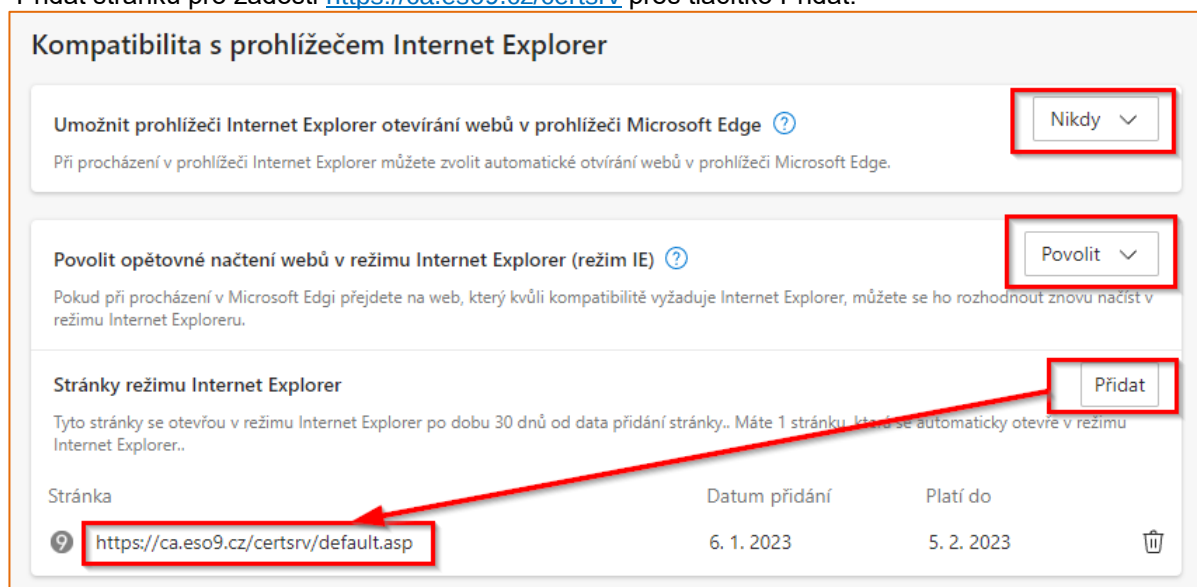
Nastavení Microsoft Edge

Do adresního řádku je třeba zadat <edge://settings/defaultBrowser>:



Dojde k otevření Nastavení, zde je nutné nastavit následující možnosti:

- Umožnit prohlížeči Internet Explorer otevírání webů v prohlížeči Microsoft Edge na Nikdy.
- Povolit opětovné načtení webů v režimu Internet Explorer (režim IE) na Povolit
- Přidat stránku pro žádosti <https://ca.eso9.cz/certsrv> přes tlačítko Přidat.

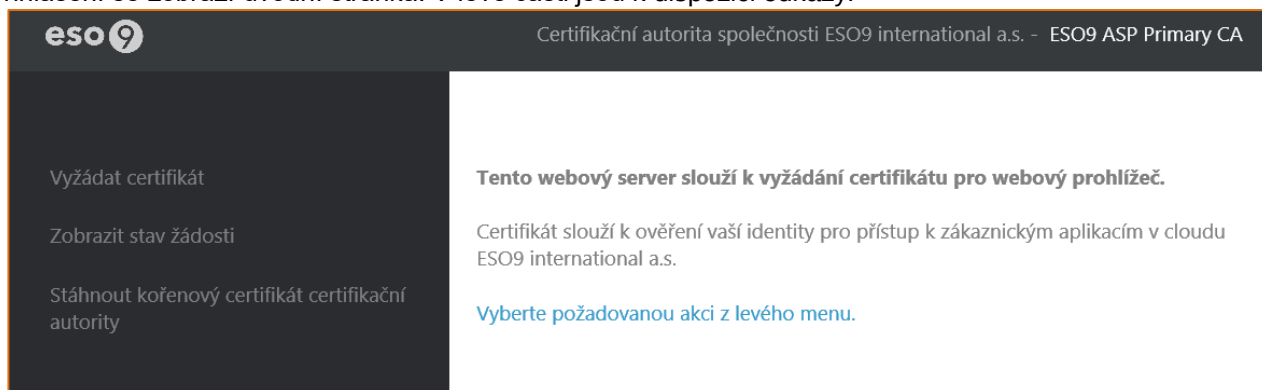


POZNÁMKA: Stránce pro žádosti nejde nastavit delší platnost, sama časem ze Stránky režimu Internet Explorer vypadne. Je třeba si ji tam pak znovu přidat.

Žádost o certifikát a jeho instalace

Žádost o vydání klientského certifikátu by měla být vystavena na stanici, na které bude následně certifikát používán. K žádosti a instalaci certifikátu slouží web certifikační autority <https://ca.eso9.cz>. Na web je třeba se nejprve přihlásit. Přihlašovací údaje získáte na vyžádání u pracovníků ESO9 international a.s.

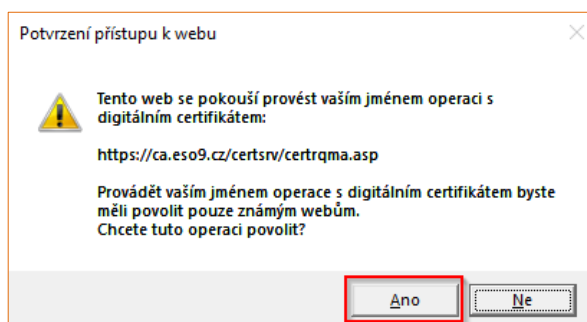
Po přihlášení se zobrazí úvodní stránka. V levé části jsou k dispozici odkazy.



Vystavení žádosti o vydání klientského certifikátu

Postup vystavení žádosti:

- a) Je třeba použít odkaz **Vyžádat certifikát**. Zobrazí se žádost o potvrzení přístupu k webu. Tu je třeba potvrdit tlačítkem **Ano**.



- b) Zobrazí se stránka pro zadání vašich osobních údajů. Formulář vyplňte pravdivými údaji, jinak nebude možné žádost schválit. Žádost potvrďte stiskem tlačítka **Odeslat** v dolní části formuláře.

Upřesnit žádost o certifikát
Vyplňte prosím všechny údaje. Neúplná žádost nebude schválena!

Jméno a příjmení:	Karel Nový
E-mailová adresa:	karel.novy@eso9.cz
Společnost:	ESO9 international a.s.
Oddělení:	obchod
Město:	Praha
Telefon:	+420 123456789
Země/oblast:	CZ

Odeslat

- c) Pokud se Vám zobrazí informační hlášení o porušení scriptů, zvolte možnost *Ano*.
- d) Zobrazí se informace potvrzující přijetí žádosti. Vaší žádosti je přiděleno identifikační číslo (ID požadavku), které si poznamenejte. Kliknutím na odkaz „**Odešlete prosím upozornění správci**“ zašlete informační e-mail do společnosti ESO9 international a.s.

Čekající žádost

Žádost o certifikát byla přijata, ale musíte počkat, než správce ověří správnost zadaných údajů a žádaný certifikát vystaví.

[Odešlete prosím upozornění správci \(ID požadavku 8090\)](#)

[Vraťte se na tuto webovou stránku za jeden nebo dva dny a vyzvedněte si certifikát.](#)

Certifikát musíte vyzvednout pomocí **tohoto** webového prohlížeče **během 10 dní**.

Stažení a instalace certifikátu na PC klienta

Vaše žádost bude po kontrole zadaných údajů schválena. Po schválení Vás informujeme e-mailem, poté budete moci certifikát nainstalovat.

Po obdržení informace o schválení proveďte instalaci certifikátu na vaší stanici. Postup je následující:

- a) Na úvodní stránce zvolte vlevo odkaz **Zobrazit stav žádosti**. Zobrazí se stránka s informacemi o vašich žádostech o certifikát. Klikněte na odkaz s žádostí (v závorce je uveden datum a čas podání žádosti).

Zobrazit stav žádosti o certifikát čekající na vyřízení

Vyberte žádost o certifikát, kterou chcete zobrazit:

ID: 8090 - (7. ledna 2020 15:49:34)

- b) Pokud certifikát dosud není schválen, objeví se následující upozornění:

Čekající žádost

Žádost o certifikát stále čeká na vyřízení. Musíte počkat, než vám správce žádaný certifikát vystaví.

[Vraťte se na tuto webovou stránku za jeden nebo dva dny a vyzvedněte si certifikát.](#)

Certifikát musíte vyzvednout pomocí **tohoto** webového prohlížeče **během 10 dní**.

Odebrat tuto žádost ze seznamu čekajících žádostí

Odebrat

POZOR, u čekající žádosti je tlačítko *Odebrat*. Pokud byste na něj klikli, nebude možné žádost schválit! Bude pak nutné zažádat o další certifikát. Taková žádost je již dle platného Ceníku služeb zpoplatněna.

- c) Pokud je žádost schválena, zobrazí se dotaz k potvrzení přístupu. Tu je třeba potvrdit tlačítkem **Ano**.

Potvrzení přístupu k webu

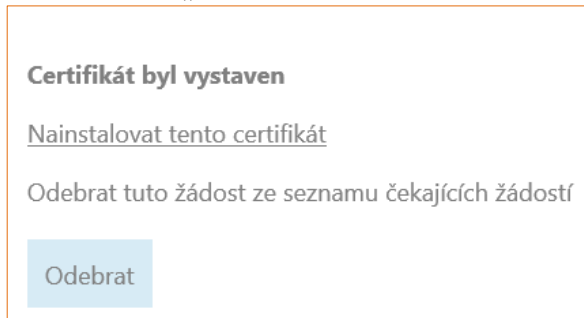
 Tento web se pokouší provést vaším jménem operaci s digitálním certifikátem:

<https://ca.eso9.cz/certsrv/certfnsh.asp>

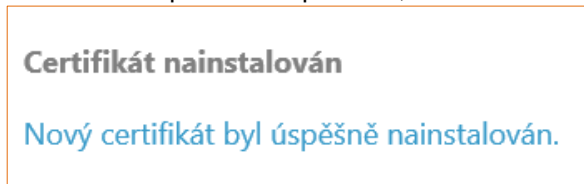
Provádět vaším jménem operace s digitálním certifikátem byste měli povolit pouze známým webům. Chcete tuto operaci povolit?

Ano Ne

d) Poté lze nainstalovat certifikát odkazem „**Nainstalovat tento certifikát**“



e) Pokud instalace certifikátu na vaše PC proběhla v pořádku, zobrazí se následující informace:



Přístup do aplikace

Po nainstalování certifikátu je nutné certifikát zapsat k uživateli do aplikace. Pokud u uživatele nebude certifikát zapsaný, nebude přístup tímto certifikátem funkční!

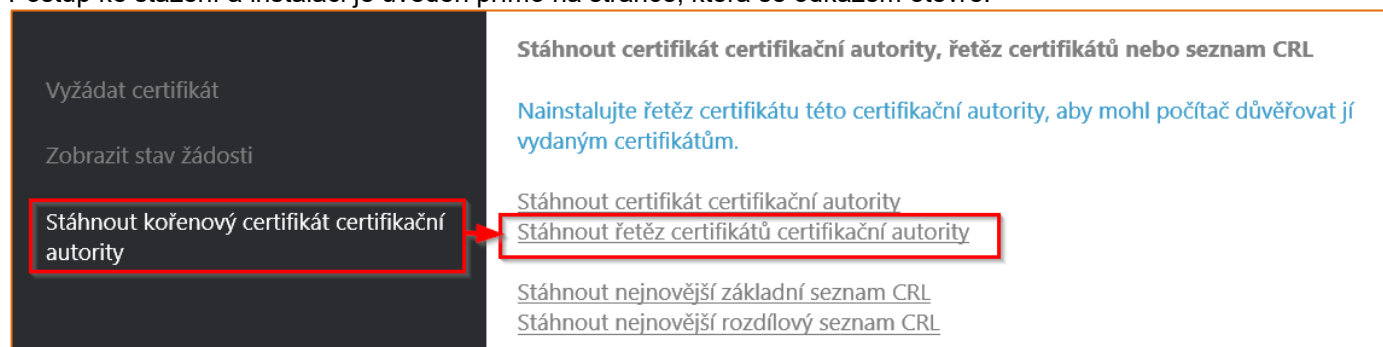
Zapsat certifikát (jeho sériové číslo) může buď správce aplikace, případně pracovníci ESO9 international a.s. O zapsání certifikátu požádejte e-mailem nebo telefonicky, uveďte při tom ID požadavku žádosti o certifikát, jméno uživatele a název společnosti (aplikace).

Pokud jste úspěšně splnili všechny výše popsané body, je vaše stanice připravena k přístupu do aplikace v Cloudu (na ASP serverech). K přístupu do aplikace slouží adresa ve tvaru **https://cloud.eso.cz/APLIKACE**, kde místo **APLIKACE** doplňte název Vaší aplikace.

Problémy při instalaci - kořenový certifikát

Kořenový certifikát se automaticky stáhne (a nainstaluje) spolu s klientským certifikátem. Pokud nelze certifikát nainstalovat a zobrazí se chyba, že není nainstalovaný kořenový certifikát, lze jej stáhnout a nainstalovat ručně. K tomu slouží odkaz ***Stáhnout kořenový certifikát certifikační autority***. Po instalaci kořenového certifikátu bude nutné znovu zažádat o klientský certifikát a nainstalovat jej.

Postup ke stažení a instalaci je uveden přímo na stránce, která se odkazem otevře.



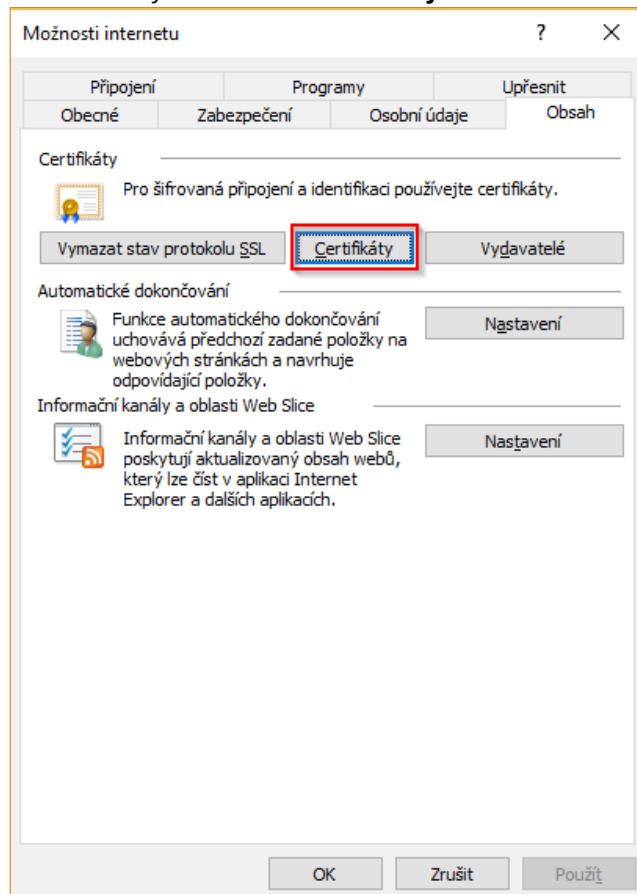
Export a import certifikátu

Jestliže je např. třeba přistupovat do aplikace z různých zařízení (počítač, notebook), je možné si certifikát po instalaci vyexportovat a poté na dalším zařízení nainstalovat.

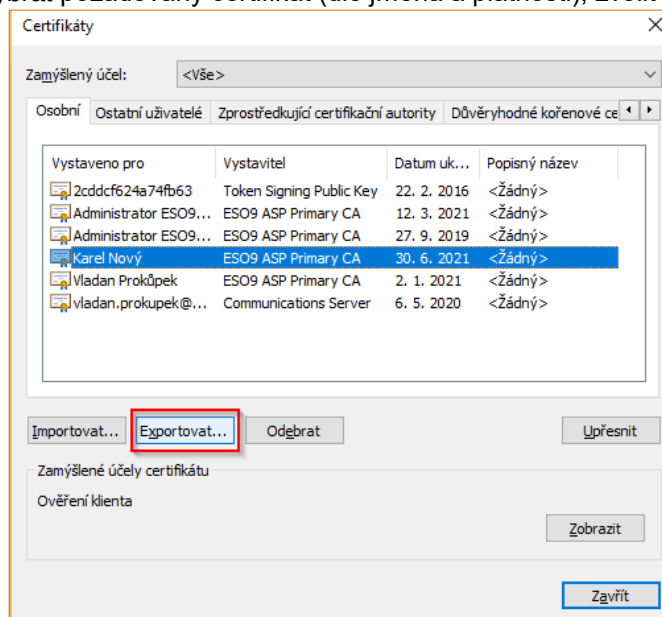
POZOR, nelze se přihlásit jedním certifikátem současně z více stanic.

Export nainstalovaného certifikátu

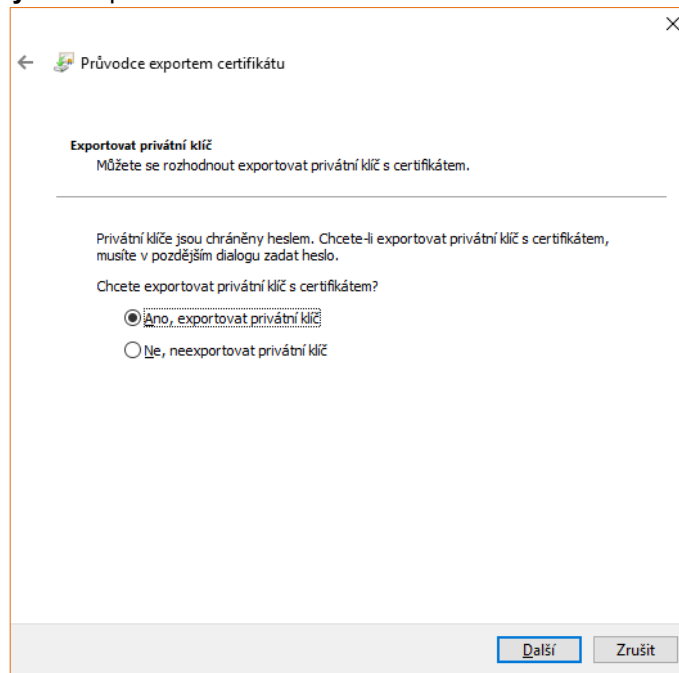
- a) Je třeba otevřít **Ovládací panely**, např. přes vyhledávání z hlavního panelu. Poté zvolit (vyhledat) **Možnosti internetu**. Zde na záložce Obsah vybrat tlačítko **Certifikáty**:



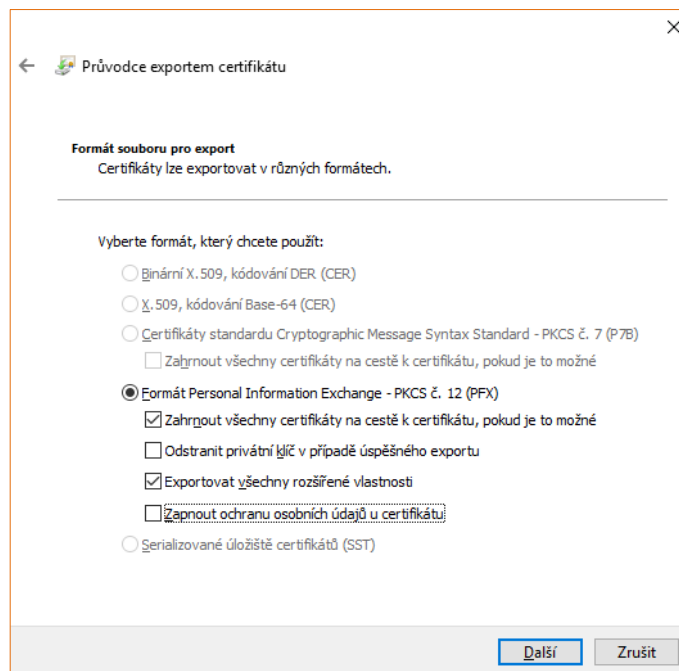
- b) Na záložce **Osobní** vybrat požadovaný certifikát (dle jména a platnosti), zvolit tlačítko **Exportovat**:



- c) Otevře se Průvodce exportem certifikátu, je třeba pokračovat tlačítkem *Další*. Na dalším dialogu zvolit **Ano**, **exportovat soukromý klíč** a pokračovat tlačítkem *Další*:



- d) Je třeba vybrat formát PKCS č.12 (PFX) a u něj zaškrtnout možnosti **Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné** a **Exportovat všechny rozšířené vlastnosti**. Poté pokračovat opět tlačítkem *Další*:



Volitelně lze zaškrtnout možnost **Odstranit privátní klíč v případě úspěšného exportu**. V tom případě bude po exportu klientský certifikát odstraněn. Má význam v případě, že o certifikát bylo zažádáno na jiné stanici, než z které se bude uživatel do aplikace přihlašovat. Je tedy nežádoucí, aby na této stanici certifikát zůstal nainstalovaný.

- e) Je třeba zaškrtnout **Heslo** a zadat jej. Toto heslo si musí uživatel sám vymyslet, bude vyžadováno při následném importu certifikátu. Poté pokračovat opět tlačítkem *Další*:

The screenshot shows the 'Průvodce exportem certifikátu' window at the 'Zabezpečení' (Security) step. The title bar includes a back arrow, a certificate icon, and the text 'Průvodce exportem certifikátu'. Below the title bar, the section 'Zabezpečení' is followed by the instruction: 'V zájmu zabezpečení je nutné privátní klíč chránit pomocí hesla nebo objektů zabezpečení.' There are two options: 'Názvy skupin a uživatelská jména (doporučeno)' (unchecked) and 'Heslo:' (checked). The 'Heslo:' option has a text field with five dots. Below it is a 'Potvrzení hesla:' (Confirm password) field, also with five dots. A 'Šifrování:' (Encryption) dropdown menu is set to 'TripleDES-SHA1'. To the right of the password fields are 'Přidat' (Add) and 'Odebrat' (Remove) buttons. At the bottom right are 'Další' (Next) and 'Zrušit' (Cancel) buttons.

- a) Přes tlačítko **Procházet** si vybrat, kam se certifikát uloží (a zadat jeho název). Poté pokračovat opět tlačítkem *Další*:

The screenshot shows the 'Průvodce exportem certifikátu' window at the 'Soubor pro export' (Export File) step. The title bar is the same as the previous screenshot. The section 'Soubor pro export' is followed by the instruction: 'Zadejte název souboru, do nějž chcete data exportovat.' Below this is a text field labeled 'Název souboru:' containing the path 'C:\TEMP\KNovy.pfx'. To the right of the text field is a button labeled 'Procházet...' (Browse...). At the bottom right are 'Další' (Next) and 'Zrušit' (Cancel) buttons.

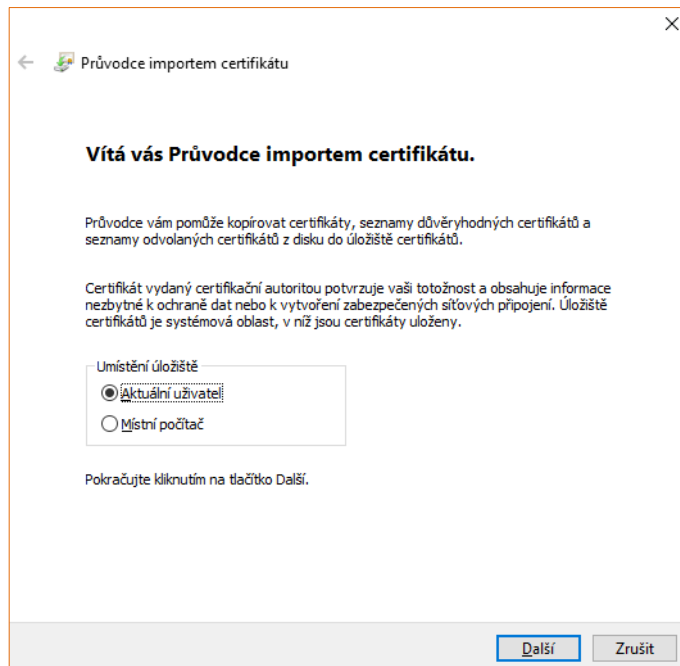
- b) Nakonec zvolit tlačítko **Dokončit**. Uložený (vyexportovaný) certifikát je třeba si přenést na vybranou stanici a zde nainportovat.

Import certifikátu ve Windows

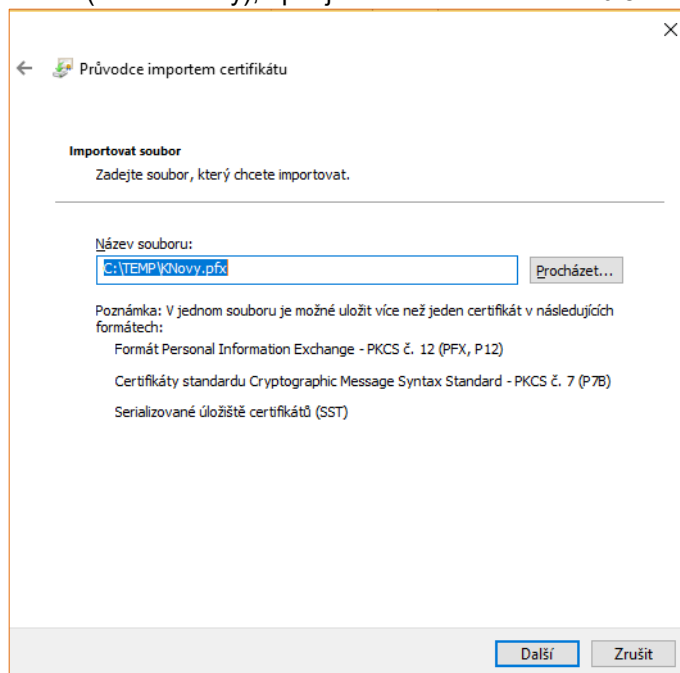
Certifikát lze nainportovat např. jeho spuštěním (po uložení), např. poklepnutím myši.

Po spuštění certifikátu (např. myší):

- a) Otevře se Průvodce importem certifikátu. Je nutné ponechat nastaveno umístění úložiště **Aktuální uživatel** a pokračovat tlačítkem *Další*:



- b) Zobrazí se samotný soubor (včetně cesty), opět je třeba zvolit tlačítko *Další*:



- c) Je nutné zadat **Heslo** (které si uživatel zvolil při exportu) a ponechat zaškrtnutou možnost **Zahrnout všechny rozšířené vlastnosti**. Poté pokračovat opět tlačítkem *Další*:

Dále lze zaškrtnout:

- Povolit silnou ochranu privátního klíče** – tím lze zabezpečit použití certifikátu. Na konci importu (po dokončení) pak bude možné zvolit úroveň zabezpečení (tlačítko „Nastavit úroveň zabezpečení“). Při volbě „Vysoká“ bude třeba si zvolit heslo a toto se pak bude zadávat pokaždé při použití certifikátu (při přihlašování). Heslo nelze zpětně z certifikátu odebrat.
- Označit tento klíč jako exportovatelný** – mý význam v případě, že i z této stanice by se měl certifikát dále exportovat.

- d) V dalším kroku ponechat automatický výběr úložiště a pokračovat tlačítkem *Další*:

- e) Nakonec zvolit tlačítko **Dokončit**. Poté bude přístup do aplikace funkční i z této stanice.