

## CS OTE

#### Dokumentace pro externí uživatele

# **OTE-**

## Nastavení lokálního úložiště certifikátů

Pro správnou funkčnost lokálního úložiště je nezbytné vytvořit zálohu privátní části elektronického podpisu, tj. soubor s koncovkou \*.**p12** nebo \*.**pfx**. Soubor je možné exportovat z počítače, ve kterém je certifikát již nainstalovaný. Pro vytvoření zálohy privátní části certifikátu Vám doporučujeme využít postup uvedený níže.

Upozorňujeme, že tento manuál je univerzální pro všechny podporované verze operačního systému Windows a je možné, že se bude v některých instruktážních snímcích lišit oproti vašemu zařízení. Manuál byl vytvořen na poslední verzi operačního systému Windows nicméně postup je obdobný jako u starších verzí.





#### Export privátní části certifikátu v systému Windows

Spusťte nabídku Start nebo stiskněte na klávesu a vyhledejte "certmgr.msc" nebo "Certifikát". (stačí otevřít nabídku a začít psát, nemusíte hledat žádné vyhledávací okno)

• V případě certmgr.msc zvolte tuto možnost:



>

• V případě certifikátu zvolte tuto možnost:





V obou dvou případech se dostanete na stejnou stránku, s kterou budeme následně pracovat.



• Rozklikněte záložku osobní → osobní

Soubor       Akce       Zobrazit       Nápověda         Image: Soubor       Image: Soubor       Image: Soubor         Image: Soubor       Image: Soubor       Image: Soubor <t< th=""><th>🚟 certmgr - [Certifikáty – aktuální v</th><th>ıživatel] — 🗆 🗙</th></t<>	🚟 certmgr - [Certifikáty – aktuální v	ıživatel] — 🗆 🗙
	<ul> <li>Certifikáty – aktuální u</li> <li>Soubor Akce Zobrazit Nápov</li> <li>Akce Zobrazit Nápov</li> <li>Soubor Akce Zobrazit Nápov</li> <li>Certifikáty – aktuální uživatel</li> <li>Osobní</li> <li>Důvěryhodné kořenové certifi</li> <li>Důvěryhodné kořenové certifikační au</li> <li>Uživatelský objekt služby Acti</li> <li>Důvěryhodní vydavatelé</li> <li>Nedůvěryhodné certifikáční autority</li> <li>Nedůvěryhodné cosby</li> <li>Vystavitelé ověření klienta</li> <li>Ostatní uživatelé</li> </ul>	vživatel] – C ×
Duveryhodne kořeny čipových karet	Coral NonRemovable Certific     MSIEHistoryJournal     Požadavek na zápis certifikátu     Důvěryhodné kořeny čipovýc	<ul> <li>Ostatní uživatelé</li> <li>Local NonRemovable Certificates</li> <li>MSIEHistoryJournal</li> <li>Požadavek na zápis certifikátu</li> <li>Důvěryhodné kořeny čipových karet</li> </ul>

Zvolte váš certifikát a klikněte na něj pravým tlačítkem → všechny úkoly → exportovat





Contractions	DoctSignum Quali Otevřít	fied CA 4 29 10
	Všechny úkoly >	Otevřít
	Vyjmout Kopírovat Odstranit Vlastnosti	Požádat o certifikát s novým klíčem Obnovit certifikát s novým klíčem Upřesnit operace >
	Nápověda	

# Průvodce exportem certifikátu

• V průvodci exportem certifikátu pokračujte tlačítkem Další (N ext).

	×
Průvodce exportem certifikátu	
Vítá vás Průvodce exportem certifikátu.	
Průvodce vám pomůže kopírovat certifikáty, seznamy důvěryhodných certifikátů a seznamy odvolaných certifikátů z úložiště certifikátů na disk.	
Certifikát vydaný certifikační autoritou potvrzuje vaši totožnost a obsahuje informace nezbytné k ochraně dat nebo k vytvoření zabezpečených síťových připojení. Úložiště certifikátů je systémová oblast, v níž jsou certifikáty uloženy.	
Pokračujte kliknutím na tlačítko Další.	
Další Zru	šit



• V druhém kroku zvolte možnost "Ano, exportovat privátní část" (Yes, export the private key) a klikněte na tlačítko Další (Next).

	×
🗧 🚑 Průvodce exportem certifikátu	
<b>Exportovat privátní klíč</b> Můžete se rozhodnout exportovat privátní klíč s certifikátem.	
Privátní klíče jsou chráněny heslem. Chcete-li exportovat privátní klíč s certifikátem, musíte v pozdějším dialogu zadat heslo.	
Chcete exportovat privátní klíč s certifikátem? Ano, exportovat privátní klíč Ne, neexportovat privátní klíč	
Další Zru	śit



• Ponechte předvolenou možnost "Personal Information Exchange - .pfx" a pokračujte tlačítkem Další (Next).

A Průvodce exportem certifikátu
Formát souboru pro export Certifikáty lze exportovat v různých formátech.
Vyberte formát, který chcete použít:
O Binární X. 509, kódování DER (CER)
🔿 X.509, kódování Base-64 (CER)
🔘 Certifikáty standardu Cryptographic Message Syntax Standard - PKCS č. 7 (P7B)
Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné
<ul> <li>Formát Personal Information Exchange - PKCS č. 12 (PFX)</li> <li>Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné</li> </ul>
Odstranit privátní klíč v případě úspěšného exportu
Exportovat všechny rozšířené vlastnosti
Zapnout ochranu osobních údajů u certifikátu
🔿 Serializované úložiště certifikátů (SST)
Dalčí 7ruč
Další Zruš



Dále zaheslujte soubor (zvolte heslo, kterým bude privátní klíč chráněn). Potvrďte heslo a klikněte na tlačítko **Další** (Next).

Zabez	pečení						
V za	zájmu zabez abezpečení.	pečení je nutné	e privátní klíč d	hránit pomoc	í hesla nebo (	objektů	
	] Názvy sku	oin a uživatelska	á jména (dopo	ručeno)			
					Přidat		
					Odebrat		
					Ouebrat		
	Z Heslor						
	•••••	•••••					
	Potvrzení l	nesla:					
	•••••	•••••					
Ši	frování:	TripleDES-SHA1	~		J		



Následně vyberte místo, kam privátní část certifikátu požadujete uložit – klikněte na tlačítko Procházet (Browse), soubor pojmenujte, klikněte na Uložit (Save) a poté pokračujte na **Další** (Next).

×	🦝 Uložit jako	×
🗲 🗧 Privodce exportem cettifikätu	← → ▼ ↑ 🗄 → Tento počítač → Dokumenty	✓ ひ Prohledat: Dokumenty
	Uspořádat 🔻 Nová složka	III 🕶 😲
Soubor pro export Zadejte název souboru, do nějž chcete data exportovat. Název souboru:	<ul> <li>Rychlý přístup</li> <li>Dokumenty</li> <li>Stažené soubory</li> <li>Obrázky</li> <li>Q00</li> <li>Plocha</li> <li>WEB</li> <li>OreDrive - OTE a.S</li> <li>Tento počítač</li> <li>3D objekty</li> <li>Disk H</li> <li>Dokumenty</li> <li>Hudba</li> <li>Ohrázky</li> <li>Plocha</li> <li>Wisev souboru: Záloha_centifikátů</li> <li>Uložit jako typ: Formát Personal Information Exchange (*.pfx)</li> <li>Skrýt složky</li> </ul>	Název MyJabberFiles Zdroje dat Kalis soubory Sound recordings Zzruky Původu Demo Builder Movies CP Poznámkové bloky aplikace OneNote SAP Lumira Documents Lexicon ABBY Downloads Demo Builder Animations Vlastní šablony Office SAP Uložit Zrušit
Další <b>Zrušit</b>		

Nyní stiskněte tlačítko **Dokončit** (Finish). Po úspěšném exportu již máte k dispozici na Vámi zvoleném místě privátní část certifikátu.

	vodce exportem (	certifikátu	
Zadali jeto pádodující pa	ntruonú		
Název souboru	staveni.	C-Marriel Terror	
Exportovat klíče		Ano	
Zahrnout všechny cert	tifikáty v cestě k certifikátu	Ano	
Formát souboru		Formát Personal Info	ormation Excha
<			>

## Nastavení lokálního úložiště certifikátu

- Lokální úložiště umožňuje uchovávat certifikáty pro podepisování dat.
- Lokální úložiště se vždy chrání heslem, pokud dojde k resetu stávajícího hesla, smaže otese z lokálního úložiště i aktuálně dohraný elektronický podpis.
- Do lokálního úložiště je třeba naimportovat privátní část certifikátu (soubor ve formátu \*.p12 nebo \*.pfx), kterou jste si vytvořili v předchozím kroku.
- Privátní klíč je importován pouze do webového úložiště prohlížeče, nikdo jiný než Vy k němu nemá přístup.
- Import certifikátu do lokálního úložiště je nutno provést po každé obnově certifikátu.

Při pokusu o elektronický podpis v prohlížečích **Google Chrome**, **Microsoft Edge**, **Mozilla Firefox** se Vám zobrazí upozornění, že je nutno napřed vložit certifikát do lokálního úložiště certifikátů. Po kliknutí na tlačítko **OK** budete přesměrovaní do lokálního úložiště s certifikáty.

OTE-Wr	
	Žádost o podepsání
» Přihlášení	Pro pokračování nastavte certifikát do lokálního uložiště, nebo nainstalujte podpisový balíček OTE PKI Client. Pro prád s certifikáty v lokálním úložišti potřeba nastavit heslo. Toto heslo bude vyžadováno při podepisování dat. Lokální uložiště není nutné nastavovat, pokud máte nanistalovaný podpisový bužický, vtr <u>a statavní certifikau</u> .
Elektronickým podpisem tohoto textu se přihlašuji k zabezpečenému portál	OK ) Zavřit )
Podepsat o	
Kontakt   Zásady používání	

V případě, že nemáte nastavené **heslo** v lokálním úložišti, tak je potřeba ho zde nastavit (min. 4 znaky). Toto heslo bude vyžadováno při novém přihlášení do aplikace. Po zadání hesla a jeho potvrzení klikněte na tlačítko **Uložit**.



Komponenta OTE PKI	
Nativní podpisová komponenta	Kliknutím na tlačítko "Instalovat" spusťte stažení podpisové komponenty. Instalovat OTE PKI komponenta nedetekována Detekovat V případě nefunkčního tlačítka "Instalovat" vyberte dle verze operačního systému správnou verzi komponenty. Podpisová komponenta pro 32 bit ke stažení ZDE. Podpisová komponenta pro 64 bit ke stažení ZDE.
Informace	
	Manuál pro přístup k systému OTE, a.s. naleznete <u>zde</u> .
Nastavení hesla do lokálního úložiště s cer	tifikáty 🔼
mentálně nemáte nastaveno žádné he slo bude vyžadováno při podepisování	slo. Pro práci s certifikáty v lokálním úložišti musíte mít nastavené heslo. Prosím nastavte si jej v následujícím formuláři. Toto dat.

Nyní je třeba naimportovat privátní část certifikátu, soubor ve formátu \*.**p12** nebo \*.**pfx**. Klikněte na tlačítko **Procházet** (Choose File) a vyhledejte zálohu Vašeho certifikátu. Po výběru certifikátu ve formátu \*.**p12** nebo \*.**pfx**, zadejte heslo k privátnímu klíči osobního certifikátu (jedná se o heslo, které jste si nastavili při zálohování **privátní části certifikátu**). Nakonec klikněte na tlačítko **Přidat**.

Po kliknutí na tlačítko se certifikát zobrazí v sekci *Stávající certifikáty v lokálním úložišti*. Následně můžete přejít na případnou registraci certifikátu nebo přihlášení

» Nastavení certifikátů				🚬 💥 🛛 🔰 Zpět na přihlašovací obrazovku
⊌ Komponenta OTE PKI				<b>•</b>
⊌ Informace				<b>A</b>
Manuál pro přístup k syst	ému OTE, a	a.s. nalezne	ete <u>zde</u> .	
⊌ Přidání nového certifikátu				
PRIVÁTNÍ ČÁST osobního certifikátu - formát p12/pfx Zvolit soubor zaloha_certifika	tu.pfx			
Heslo k privátnímu klíči osobního certifikátu *				
Pozn.: Privátní část není odesílána na server. Je uložena lokálně v adresáři prohlížeče. Zabezpečena v podo	bě PKCS#12 sou	boru.		
Pridat >				
⊌ Stávající certifikáty v lokálním úložišti				
			Coriová	
DN	Platnost od	Platnost do	čislo	Certifikační autorita
DN C=CZ, organizationIdentifier=NTRCZ-26463318, O=OTE, a.s., OU=103, CN=Tomáš Tůma, SN=Tůma, G=Tomáš, serialName=P618989	Platnost od 09.06.2020 10:27:20	Platnost do 29.06.2023 10:27:20	číslo 0151f23b	Certifikační autorita C=CZ, organizationIdentifier=NTRCZ-47114983, O=Česká pošta, s.p., CN=PostSignum Qualified CA 4
DN C=CZ, organizationIdentifier=NTRCZ-26463318, O=OTE, a.s., OU=103, CN=Tomáš Tůma, SN=Tůma, G=Tomáš, serialName=P618989 Tměna hesla do lokálního úložište s certifikáty	Platnost od 09.06.2020 10:27:20	Platnost do 29.06.2023 10:27:20	číslo 0151f23b	Certifikační autorita C=CZ, organizationIdentifier=NTRCZ-47114983, O=Česká pošta, s.p., CN=PostSignum Qualified CA 4
DN           Smazat         C=CZ, organizationIdentifier=NTRCZ-26463318, 0=OTE, a.s., 0U=103, CN=Tomáš Tůma, SN=Tůma, G=Tomáš, serialName=P618989           Změna hesla do lokálního úložište s certifikáty	Platnost od 09.06.2020 10:27:20	Platnost do 29.06.2023 10:27:20	číslo 0151f23b	Certifikační autorita C=CZ, organization1dentifier=NTRC2-47114983, O=Česká pošta, s.p., CN=PostSignum Qualified CA 4
DN       Smazat     C=CZ, organizationIdentifier=NTRCZ:26463318, 0=0TE, a.s., 0U=103, CN=Tomáš Tůma, SN=Tůma, G=Tomáš, serialName=P618989       Změna hesla do lokálního úložište s certifikáty       Kontakt     Zásady používání	Platnost od 09.06.2020 10:27:20	Platnost do 29.06.2023 10:27:20	číslo 0151f23b	Certifikační autorita C=CZ, organizationLdentifier=NTRCZ-47114983, O=Česká pošta, s.p., CN=PostSignum Qualified CA 4
DN       Smazat     C=CZ, organization1dentifier=NTRCZ-26463318, 0=OTE, a.s., 0U=103, CN=Tomáš Tůma, SN=Tůma, G=Tomáš, serialName=P618989       Změna hesla do lokálního úložište s certifikáty       Kontakt     Zásady používání       ©2020 OTE, a.s., all rights reserved	Platnost od 09.06.2020 10:27:20	Platnost do 29.06.2023 10:27:20	číslo 0151f23b	Certifikační autorita C=C2, organizationIdentifier=NTRCZ-47114983, O=Česká pošta, s.p., CN=PostSignum Qualified CA 4

Nyní se můžete úspěšně přihlásit - Portál OTE (ote-cr.cz)