Používání certifikátů v poštovní aplikaci Mozilla Thunderbird

První certifikační autorita, a.s.

Verze 8.15



Obsah

1.	Import certifikátu ve formátu PFX	3
2.	Zavedení podpory pro certifikáty uložené na čipové kartě Starcos 3.0 s aplikací I.CA SecureStore	5
3.	Nastavení důvěryhodnosti kořenovým certifikátům	9
4.	Přiřazení certifikátu k uživatelskému účtu	10

1. Import certifikátu ve formátu PFX

Otevřete aplikaci **Mozilla Thunderbird**. V pravém horním rohu klikněte na **ikonu menu** a **Možnosti**. V rozevírací nabídce vyberte znovu **Možnosti**.



Zde zvolte nabídku Rozšířené a tlačítko Certifikáty.

Možnosti								×		
	Aa		=	90		D	Ĩ			
Obecné	Zobrazení	Vytváření	Chat	Soukromí	Bezpečnost	Přílohy	Rozšířené	Kalendář		
Obecné Mož	nosti hlášení Sŕ	ť a místo na disk	u Aktualizace	Certifikáty						
Pokud serve	er vyžaduje osoł	oní certifikát:								
⊖ Zve	○ Zvolit <u>a</u> utomaticky Vž <u>d</u> y se dotázat									
🗹 Aktuálr	ní <u>p</u> latnost certif	ikátů ověřovat n	a serverech OC	SP						
<u>C</u> ertifikáty	<u>B</u> ezpečno	ostní zařízení								
						C	OK	Zrušit		



Jmeno certifikatu	Bezpečnostní zařízení	Sériové číslo	Platný do	E,

Klikněte na tlačítko Certifikáty a přejděte na kartu Osobní.

Zde stiskněte tlačítko Importovat.

Otevře se dialogové okno, kde vyberete soubor *.pfx s Vaším certifikátem a zvolte Otevřít.

Soubor s certifikaterri k	mportu						1
• 🔿 • 🛧 📙 > T	ento počítač 🔹 Dokur	menty > záloha			√ Ō	Prohledat: záloha	P
Jspořádat 🔻 Nová sl	ožka						1
🔜 Plocha 🛛 🖈 ^	Název	^	Datum změny	Тур	Velikost		
Dokumenty 🖈	🈼 certifikat		19. 8. 2015 11:08	Personal Informati	3	kB	
📰 Obrázky 🛛 🖈							
ConeDrive							
💻 Tento počítač							
Dokumenty							
👌 Hudba							
📰 Obrázky							
E Plocha							
🖶 Stažené soubory							
Videa							
🏪 Místní disk (C:)							
🛫 spolecne (\\phq							
🛫 spolecne (\\phq							
🛫 spolecne (\\phq 💣 Síť 🛛 🗸 Náze	v souboru: certifikat				~	PKCS12 Soubory	~



Nyní budete požádání o zadání hesla, které jste si zvolili při exportu certifikátu.

Požado	váno heslo	×
?	Zadejte heslo, kterým byla zašifrována tato zálo	ha <mark>certifikátů</mark> :
	1	

Pokud zadané heslo je správné, dojde k úspěšnému importu certifikátu do úložiště Mozilla Thunderbird.

Výstraha	×
<u> </u>	/áše bezpečnostní certifikáty a soukromý klíče byly úspěšně obnoveny.

2. Zavedení podpory pro certifikáty uložené na čipové kartě Starcos 3.0 s aplikací I.CA SecureStore

Otevřete aplikaci **Mozilla Thunderbird**. V pravém horním rohu klikněte na **ikonu menu** a **Možnosti**. V rozevírací nabídce vyberte znovu **Možnosti**.





Možnosti								×
			=	00	A	Ņ	Ĩ	
Obecné	Zobrazení	Vytváření	Chat	Soukromí	Bezpečnost	Přílohy	Rozšířené	Kalendář
Obecné Mož	ínosti hlášení S	íť a místo na disk	u Aktualizace	e Certifikáty				
Pokud serv	er vvžaduje oso	bní certifikát:						
⊖ Zv	olit <u>a</u> utomaticky	y ● Vž <u>d</u> y se d	otázat					
_								
Aktuál	ní <u>p</u> latnost certif	fikátů ověřovat n	a serverech O	CSP				
Certifikát	/ Bezpečn	ostní zařízení						
						_		
							ОК	Zrušit

Zde zvolte nabídku Rozšířené a tlačítko Bezpečnostní zařízení

V pravé části zvolte Načíst.

Správce bezpečnostních zařízení		-	- 🗆 X	
Bezpečnostní moduly a zařízení «NSS Internal PKCS #11 Module Obecné šifrovací služby Softw. bezp. zařízení «Zabudovaný kořenový modul Builtin Object Token	Detaily	Hodnota	<u>P</u> řihlásit <u>O</u> dhlásit Změnit <u>h</u> eslo <u>N</u> ačíst <u>U</u> volnit Povolit <u>F</u> IPS	
			ОК	

Otevře se okno pro přidání nového bezpečnostního modulu.

(3) Načtení zařízení PKCS#11	_		\times
Zadejte informace o modulu, který chcete přidat.			
J <u>m</u> éno modulu: Nový modul PKCS#11			
<u>N</u> ázev souboru modulu:		<u>P</u> rocház	et
ОК		Zruši	t

Klikněte na Procházet a najděte ve svém počítači následující soubor:

C:\Windows\System32\SecureStorePkcs11.dll

Následně klikněte na **Otevřít** a nabídku potvrďte **OK**.

Ovyberte PKCS#11 zařízení							×
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow Ter	nto počítač > Místní disk (C:) > Window:	s > System32		√ Č	Prohledat: System32		Q
Uspořádat 👻 Nová slo	žka						?
📃 Plocha 🛛 🖈 ^	Název	Datum změny	Тур	Velikost			^
🚆 Dokumenty 🖈	🔁 SecEdit	10. 7. 2015 13:00	Aplikace	37 k	В		
S Obrázky	📧 secinit	10. 7. 2015 13:00	Aplikace	15 k	В		
	🚳 secproc.dll	10. 7. 2015 13:00	Rozšíření aplikace	343 k	В		
a OneDrive	🚳 secproc_isv.dll	10. 7. 2015 13:00	Rozšíření aplikace	342 k	В		
Tento nočítač	🚳 secproc_ssp.dll	10. 7. 2015 13:00	Rozšíření aplikace	89 k	В		
	🚳 secproc_ssp_isv.dll	10. 7. 2015 13:00	Rozšíření aplikace	89 k	В		
Dokumenty	🚳 secur32.dll	10. 7. 2015 13:00	Rozšíření aplikace	24 k	В		
Hudba	SecureStoreCore.dll	9. 12. 2013 10:41	Rozšíření aplikace	485 k	В		
📰 Obrázky	SecureStoreCsp.dll	6. 3. 2014 12:33	Rozšíření aplikace	172 k	В		
Plocha	SecureStoreCspRes.dll	9. 12. 2013 10:43	Rozšíření aplikace	446 k	В		
👆 Stažené soubory	SecureStoreKSign.dll	16. 3. 2015 13:05	Rozšíření aplikace	92 k	В		- 14
📕 Videa	📑 SecureStoreKSignReg	9. 12. 2013 10:43	Aplikace	60 k	В		
Mistní disk (Ci)	SecureStorePkcs11.dll	9. 12. 2013 10:42	Rozšíření aplikace	160 k	в		
initial disk (c.)	🚳 security.dll	10. 7. 2015 13:00	Rozšíření aplikace	5 k	В		
g spolecne (\\pnq	SecurityAndMaintenance	10. 7. 2015 13:01	Soubor PNG	6 k	В		
🚽 Síť 🗸 🗸	SecurityAndMaintenance_Alert	10. 7. 2015 13:01	Soubor PNG	3 k	В		\sim
Název	souboru: SecureStorePkcs11.dll			~	Všechny soubory		\sim
					Otevřít	Zrušit	



Dojde k přidání čtečky čipových karet do seznamu bezpečnostních zařízení. Okno zavřete stisknutím **OK**.



Nyní již je v aplikaci Mozilla Thunderbird nainstalována podpora pro používání karet Starcos 3.0. Práce s certifikáty na kartě probíhá stejně jako s certifikáty uloženými v počítači / v aplikaci Mozilla Thunderbird, přičemž je potřeba mít ve čtečce připojené k počítači kartu s daným certifikátem. Při práci s kartou můžete být dotázáni na PIN ke kartě, a to pravděpodobně následujícím dialogem, kde bude uvedeno označení vložené/používané karty.

Požadov	áno heslo	\times
?	Prosím zadejte hlavní heslo pro 9203030000031562.	
	1	
	OK Zrušit	



3. Nastavení důvěryhodnosti kořenovým certifikátům

Před použitím certifikátů k podpisu e-mailů bude pravděpodobně potřeba nastavit důvěryhodnost kořenovým certifikátům naší autority.

Postupujte jako v předchozím případě, kdy otevřete menu Možnosti a kartu Rozšířené.

Možnosti								×		
	Ra	_/	=	00		Q	Ĩ			
Obecné	Zobrazení	Vytváření	Chat	Soukromí	Bezpečnost	Přílohy	Rozšířené	Kalendář		
Obecné Mo	žnosti hlášení S	íť a místo na disl	ku Aktualizace	Certifikáty						
Pokud sen	Pokud server vyžaduje osobní certifikát:									
0 Z	olit <u>a</u> utomatick	y () Vž <u>d</u> y se d	lotázat							
🗹 Aktuál	ní <u>p</u> latnost certi	fikátů ověřovat n	a serverech OC	SP						
Castifikit	Perneža	ostol začízaní								
Certifikat	<u>B</u> ezpech	ostni zarizeni								
							ОК	Zrušit		

Nyní klikněte na tlačítko Certifikáty.

Na kartě **Autority**, vyhledejte certifikáty od První certifikační autorita, a.s., poté označte jeden z certifikátů a klikněte na tlačítko **Upravit důvěru**.

🎯 Správce certifikátů	- 0	×					
Osobní Lidé Servery Autority Ostatní							
Tyto certifikáty jsou dostupné pro identifikaci certifikačních autorit:							
Jméno certifikátu	Bezpečnostní zařízení	₽₽					
NetLock Arany (Class Gold) Főtanúsítvány	Builtin Object Token	^					
ANetwork Solutions L.L.C.							
Network Solutions Certificate Authority	Builtin Object Token						
▲PM/SGDN							
IGC/A I	Builtin Object Token						
První certifikační autorita, a.s.							
I.CA - Standard Certification Authority, 0 9	9203030000031562						
I.CA - Qualified Certification Authority, 0	9203030000031562						
		~					
Zo <u>b</u> razit Upr <u>a</u> vit důvěru <u>I</u> mportova	at Exportovat S <u>m</u> azat nebo nedůvěřovat						
	O	<					

Zaškrtněte všechna nastavení důvěryhodnosti a stiskněte OK.

Upravit nastavení důvěryhodnosti CA	Х
Certifikát "I.CA - Standard Certification Authority, 09/2009" představuje Certifikační autorit	u.
Upravit nastavení důvěryhodnosti:	
Tento certifikát může identifikovat server.	
Tento certifikát může identifikovat uživatele e-mailu.	
Tento certifikát může identifikovat výrobce software.	
OK Zrušit	

Stejný postup opakujte pro zbylé certifikáty od I.CA.

4. Přiřazení certifikátu k uživatelskému účtu

V pravém horním rohu klikněte na **ikonu menu**. Dále v nabídce zvolte **Možnosti** a **Nastavení účtu**.





Přejděte do kategorie Zabezpečení.

astavení účtu	-				
A desiration @gmail.com	Zabezpečení				
Kopie a složky	Pro příjem a odesílání podepsaných nebo zašifrovaných zpráv musíte zadat jak certifikát pro elektronický podpis tak i certifikát pro šifrování.				
Vytváření zpráv a adresová	Elektronický podpis				
Nevyžádaná pošta	Používat tento certifikát pro elektronický podpis odesílaných zpráv:				
Synchronizace a úložiště	Vy <u>b</u> rat Vy <u>m</u> azat				
Potvrzení o přečtení	Elektronicky podepsat zprávy (výchozí)				
Zabezpečení	<u> </u>				
IVIISTNI SIOZKY	Sifrování Boužít tento certifikát pro začifrování a dečifrování obdržených zpráv				
Misto na disku	Vorbrat				
Server odchozí pošty (SMTP)	Výchozí nastavení šifrování při odesílání zpráv: <u>N</u> ikdy (nepoužívat šifrování) <u>V</u> yžadováno (nelze odeslat zprávy, pokud všichni příjemci nemají certifikáty)				
	Certifikáty				
	Zobrazit certifikáty Bez <u>p</u> ečnostní zařízení				
<u>A</u> kce účtu •					
	OK Zružit				

V sekci **Elektronický podpis** zvolte **Vybrat**. Zde vyberte požadovaný certifikát, kterým chcete e-maily podepisovat potvrďte tlačítkem **OK**.

Výběr certifi	cátu	×
Certifikát:	9203030000031562:Aleš Pospíchal (22a) [00:A8:7C:24] 🛛 🗸	
Podrobno	sti o vybraném certifikátu:	
Vydáno p Sériové č Platný o Použití k E-mail: p Vydal: OU a.s.",CN= Uskladněr	ro: serialNumber=ICA - 10347473,O="První certifikační autorita, a.s.",CN=Aleš Pospíchal,C=CZ ííslo: 00:A8:7C:24 d 8. 7. 2015 13:26:43 do 7. 7. 2016 13:26:43 líče certifikátu: Podpisování,Nepopiratelnost ospichal@ica.cz =I.CA - Accredited Provider of Certification Services,O="První certifikační autorita, "I.CA - Qualified Certification Authority, 09/2009",C=CZ no v: 9203030000031562	
	OK Zrušit	



Nyní je vše připraveno k odesílání podepsaných zpráv.

🚖 Psaní :	zprávy: (bez pi	éedmětu)		-		\times
Soubor Ú	Jpr <u>a</u> vy <u>Z</u> obra	zení V <u>l</u> ožit <u>F</u> ormát <u>N</u>	<u>Možnosti Nástroje Nápov</u> ěda			
IIII Odesla	it 🖋 Pravi	Alaž Dasníchol o kol ož	Zabezpeceni V Ulozit V			
•	<u>U</u> a: Komu:	Ales Pospichal 4	<u>E</u> lektronicky podepsat zprávu			
			Z <u>o</u> brazit informace o zabezpečení			
	Pře <u>d</u> mět:					
Tělo	\sim	Proporcionální	✓ ▲ A' A' A A A HE 担 程 程 目 = ■ · ◎ ·			
					•	く
						× .