

Přístup do systému CS OTE přes prohlížeče Firefox s certifikátem PostSignum a I.CA

Stáhněte si nejnovější verzi Firefox a nainstalujte <u>http://www.mozilla.org/cs/firefox/new/</u>

Stáhněte si podpisovou komponentu a nainstalujte ji <u>http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/files-konfigurace-pc/PKIComponent-OTE-setup.exe</u>

Instalace veřejných částí certifikačních autorit

Mám softwarový komerční certifikát od PostSignum

Do prohlížeče Firefox vložte adresu <u>www.postsignum.cz/certifikaty_autorit.html</u> (na odkaz stačí kliknout levým tlačítkem myši)

Na stránce najděte tabulku *Ruční instalace certifikátů certifikačních autorit*. Na plochu si uložte 3 veřejné části certifikační autority *PostSignum Root QCA 2* ve formátu DER.

Klikněte pravým tlačítkem myši na první certifikát DER a zvolte uložit odkaz jako... Ruční instalace certifikátů certifikačních autorit

Stáhněte si soubory s certifikáty autorit (pro OS Windows DER) a v instalaci postupujte dle návodu k příslušné aplikaci.

Otevřít odkaz v <u>n</u> ovém panelu	Soubory s certifikáty a	utorit PostSignum Root QCA 2:
Otevřít odkaz v novém okně	B DER B PEM	kořenová certifikační autorita PostSignum Root QCA 2
O <u>t</u> evřít odkaz v novém anonymním okně	B DER B PEM	kvalifikovaná certifikační autorita PostSignum Qualified CA 2
Při <u>d</u> at odkaz do záložek		kvalifikovaná certifikační autorita PostSignum Qualified CA 3
<u>U</u> ložit odkaz jako		kvalnikovana cerdikacih autorita Postolgiralih Qualnica erk o
Kopírovat adre <u>s</u> u odkazu	🖻 <u>DER</u> 🖻 <u>PEM</u>	komerční certifikační autorita PostSignum Public CA 2
Hedat "DER" na webu "Google"		
Prozkoumat prvek		

Vyberte místo uložení Plocha a dejte Uložit.



Stejným způsobem uložte zbylé tři certifikáty ve formátu DER.



Poté ve Firefoxu zvolte Nabídka – Možnosti.



Přepněte se do Rozšířené – Certifikáty – Certifikáty.

*	Možnosti	× (+	
(Firefox about:pref	ferences#advanced	
.0.	Obecné	Rozšířené	
۹	Vyhledávání	Obecné Možnosti blášení Síť Aktualizace Certifikáty	٦
Ê	Obsah		_
¢	Aplikace	Pokud server vyžaduje osobní certifikát:	
œ	Soukromí	Zvolit <u>a</u> utomaticky	
≙	Zabezpečení	Vždy se dotázat	
Q	Sync 1	Aktuální platnost certifikátů ověřovat na serverech OCSP	
٤	Rozšířené	3.	
		<u>C</u> ertifikáty <u>B</u> ezpečnostní zařízení	

V záložce Autority naimportujte všechny 3 veřejné části certifikační autority PostSignum, které máte uloženy na ploše. Při importu nastavte u každého certifikátu první dvě volby.

	1	Správce certifikátů	-		×
Osobní Lidé	Serven Autority Ostatní				
	Servery ristorily Ostatin				
Tyto certifik	áty jsou dostupné pro identifi	ikaci certifikačních autorit:			
Jméno cert	fikátu	Bezpečnostní zařízení	i i i i i i i i i i i i i i i i i i i	E.	
⊿(c) 2005 T	ÜRKTRUST Bilgi İletişim ve Bil	lişim G		^	
TÜRKT	UST Elektronik Sertifika Hizm	et Sağ Builtin Object Token			
▲A-Trust G	es. f. Sicherheitssysteme im el	lektr. D			
A-Trust	-nQual-03	Builtin Object Token			
▲AC Came	rfirma S.A.				
Chamb	ers of Commerce Root - 2008	Builtin Object Token			
Global	Chambersign Root - 2008	Builtin Object Token			
▲AC Came	firma SA CIF A82743287				
Chamb	ers of Commerce Root	Builtin Object Token			
Global	Chambersign Root	2 Builtin Object Token			
A A et alie S e	A /02250520067				1
Zo <u>b</u> razit	Upr <u>a</u> vit důvěru <u>I</u> m	portovat Exportovat	S <u>m</u> azat nebo nedůvěřovat.		
		Stažení certifikátu		×	h
	V V				۳.
Byli jst	e požádáni o uznání nové Cer	tifikační Autority (CA).			
Chcete	uznat "PostSignum Root QC	A 2" pro následující účely?			
🗸 Uz	nat tuto CA pro identifikaci se	erverů.			
V Uz	nat tuto CA pro identifikaci ui	živatelů poštv. 3			
	at the CA and identification	(all a loss)			ľ
	hat tuto CA pro identifikaci vy	robcu software.			
DY 1		P ZY LL A VP L			F
Pred u	znanim teto CA, a to pro jakył nky (nokud isou dostupné)	koliv učel, byste meli prozkoum	at jeji čertifikat, jeji pravidla	а	
pouni	ing (porad jsod dostapile).				
	Table 1 - COLOR	•			
Zob	razit Zobrazit certifikat C/	A			
		4	OK 7		E
		4	Zrusit	·	
				_	



Po instalaci uvidíte 3 veřejné části certifikátu certifikační autority PostSignum v záložce Autority.

Ę
E‡
₽₽,
^
~
it
)K

Mám softwarový komerční certifikát od I.CA

Do prohlížeče Firefox vložte adresu <u>www.ica.cz/SHA2-Komercni</u> (na odkaz stačí kliknout levým tlačítkem myši)

Na plochu si uložte veřejné části certifikační autority I.CA ve formátu DER. Klikněte pravým tlačítkem myši na první certifikát DER a zvolte uložit odkaz jako...

Kořenový certifikát certifikační autority pro vydávané komerční certifikáty SHA2

Kryptografický algoritmus: SHA-256 Délka kryptografického klíče pro algoritmus RSA: 2048 bitů Doba platnosti: od 1.9.2009 do 1.9.2019



Vyberte místo uložení Plocha a dejte Uložit.

2	Zadejte název souboru pro uložení	×
🔄 🦻 🝷 ↑ 🔳 Plocha →	✓ C Prohledat: Plocha	Q
Uspořádat 🔻 Nová složka		0
 ▲ ★ Oblíbené položky ▲ ★ Oblíbené položky ▲ Naposledy navšti ■ Plocha 	Knihovny Systémová složka	^
ᠾ Stažené soubory	Uzivatel Systémová složka	
 ▲ □ Knihovny ▶ □ Dokumenty ▶ ↓ Hudba 	Počítač Systémová složka	
▷ 🔄 Obrázky ▷ 🛃 Videa	Síť Systémová složka	
🖌 📭 Počítač 🗸 🖌	sica_root_key_20090901	~
Název souboru: sica_root_	key_20090901	~
Uložit jako typ: der File		~
Skrýt složky	2. Uložit Storn	o:



Poté ve Firefoxu zvolte Nabídka – Možnosti.



Přepněte se do Rozšířené -Certifikáty - Certifikáty.



V záložce Autority naimportujte veřejnou část certifikační autority, kterou máte uloženou na ploše. Při importu nastavte u certifikátu první dvě volby.

Jineno certifikatu	Bezpečnostní zařízení	E
▲ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim TÜRKTRUST Elektronik Sertifika Hizmet Sa	ı G ağ Builtin Object Token	^
A-Trust Ges. f. Sicherheitssysteme im elektr. A-Trust-nQual-03	. D Builtin Object Token	
Chambers of Commerce Root - 2008 Global Chambersign Root - 2008	Builtin Object Token Builtin Object Token	
Chambers of Commerce Root Global Chambersign Root	Builtin Object Token Builtin Object Token	,
Zo <u>b</u> razit Upr <u>a</u> vit důvěru <mark>Import</mark>	tovat Exportovat S <u>m</u> azat nebo nedůvěřovat	
Staž	žení certifikátu	×
Byli jste požádáni o uznání nové Certifikačn	ní Autority (CA).	
Chcete uznat "I.CA - Standard Certification	Authority, 09/2009" pro následující účely?	
☑ Uznat tuto CA pro identifikaci serverů.	2	
 Uznat tuto CA pro identifikaci serverů. Uznat tuto CA pro identifikaci uživatelů 	pošty.	
 Uznat tuto CA pro identifikaci serverů. Uznat tuto CA pro identifikaci uživatelů Uznat tuto CA pro identifikaci výrobců s 	i pošty. software.	
 Uznat tuto CA pro identifikaci serverů. Uznat tuto CA pro identifikaci uživatelů Uznat tuto CA pro identifikaci výrobců s Před uznáním této CA, a to pro jakýkoliv úč podmínky (pokud jsou dostupné). 	i pošty. software. šel, byste měli prozkoumat její certifikát, její pravidla a	



V záložce Autority si zkontrolujte nainstalovanou veřejnou část certifikátu I.CA.

۷	Správ	ce certifikátů	-	
Osobní Lidé Servery Autority Os	statní			
Tyto certifikáty jsou dostupné pro	identifikaci cer	tifikačních autorit:		
Jméno certifikátu		Bezpečnostní zařízení		E\$
⊿PM/SGDN				^
IGC/A		Builtin Object Token		
První certifikační autorita, a.s.				
I.CA - Standard Certification	Authority, 09/	Softw. bezp. zařízení		
▲QuoVadis Limited				
QuoVadis Root CA 2		Builtin Object Token		
QuoVadis Root Certification	Authority	Builtin Object Token		
QuoVadis Root CA 3		Builtin Object Token		
▲RSA Security Inc				
RSA Security 2048 v3		Builtin Object Token		
ASECOM Trust Surfame COLLTD				*
Zo <u>b</u> razit Upr <u>a</u> vit důvěru.	. <u>I</u> mportova	t Exportovat	S <u>m</u> azat nebo nedůvěřovat	
				OK
RSA Security 2048 v3	. <u>I</u> mportova	Builtin Object Token it E <u>x</u> portovat	S <u>m</u> azat nebo nedůvěřovat	ск ОК

Nyní budete importovat Váš privátní certifikát od PostSignum případně I.CA do Firefoxu. Zvolte Nabídka – Možnosti.

		- 🗇 🗙
	☆ 🗎 🖡	↑ 9 ≡
🙏 Vyjmout	Kopírovat	🚊 Vložit <mark>1</mark> .
-	100%	+
	8	
Nové okno	Anonymní okno	Uložit stránku
	C	∢⊒►
Tisk	Historie	Celá obrazovka
Q	0	
Najít	Možnosti	Doplňky
J.	2.	
Vývojář		
🚺 Přihlášení k	Sync	
+ Přizpůsobit		0 U

Přepněte se do Rozšířené -Certifikáty - Certifikáty.

🏘 Možnosti	× +	
Firefox about:pre	ferences#advanced	
<u>0</u> Obecné	Rozšířené	
Q Vyhledávání	Obecné Možnosti blášení Síť Aktualizace	Certifikáty
📄 Obsah		Certificaty
🚖 Aplikace	Pokud server vyžaduje osobní certifikát:	Ζ.
🗢 Soukromí	Zvolit <u>a</u> utomaticky	
🖴 Zabezpečení	Vždy se dotázat	
🚯 Sync 🚹	Aktuální <u>p</u> latnost certifikátů ověřovat na serverech OCSP	
🔬 Rozšířené	5. <u>C</u> ertifikáty <u>B</u> ezpečnostní zařízení	

V záložce Osobní zvolte Importovat a vyberte místo, kde máte uložený privátní klíč. Privátní klíč poznáte podle koncovky ***.pfx** nebo ***.p12**

Certifikát s koncovkou *.pem, *.der, *.cer jsou veřejné části certifikátu, které se zde neimportují!

	Správce cer	rtifikátů	-	
Dsobní Lidé Servery Au	Itority Ostatní			
Tyto certifikáty jsou do	stupné pro vaši osobní identifikac	ii:		
Jméno certifikátu	Bezpečnostní zařízení	Sériové číslo	Platný do	₽₽,
Zo <u>b</u> razit Zá <u>l</u> oh	ovat Zál <u>o</u> hovat vše <u>I</u> n	nportovat <u>S</u> mazat		



Zadejte heslo k certifikátu. Potvrďte OK.

Dialog zadání hesla × Prosím zadejte heslo, které bylo použito pro zašifrování zálohy certifikátu. Heslo:	F	Bezpečnostní zařízení	Sériové číslo	Platný	ído E
Prosím zadejte heslo, které bylo použito pro zašifrování zálohy certifikátu. Heslo: ••••		Dialog zadá	ní hesla	×	
OK Zrušit	Heslo:	••••	1		

Hláška o úspěšném naimportování certifikátu

Výstraha	×
Váše bezpečnostní certifikáty a soukromý klíče byly úspěšně obnove	eny.
ОК	

Pohled na naimportované certifikáty s privátním klíčem od I.CA a PostSignum. Potvrďte OK.

	Správce cer	tifikátů	-	
sobní Lidé Servery Auto	ority Ostatní			
Tyto certifikáty jsou dost	upné pro vaši osobní identifikac	i:		
Jméno certifikátu	Bezpečnostní zařízení	Sériové číslo	Platný do	Ę
 První certifikační autori Michal Raška DiS. Česká pošta, s.p. [IČ 47 Michal Pačka, DiS 	t Softw. bezp. zařízení 1 Softw. bezp. zažízení		18. 1. 2014	
Zo <u>b</u> razit Zá <u>l</u> ohov	/at Zál <u>o</u> hovat vše <u>I</u> n	nportovat Smaza	ət	
				ОК

Přihlaste se na adresu obchodního systému CS OTE



Při prvním přihlašováním Vám vyskočí hláška o přidání stránek obchodního portálu OTE do důvěryhodných. Klikněte na řádek "Vím, o co se jedná" a potom na "Přidat výjimku".

Ž	Požádali jste Firefox o zabezpečené připojení k serveru portal.ote-cr.cz , ale nelze ověřit, že tomu tak			
	skutečně je.			
	Pokud je požadováno zabezpečené připojení, měl by server předložit důvěryhodnou identifikaci a tím prokázat, že se připojujete na správné místo. Nicméně, identita tohoto serveru nemohla být ověřena.			
	Co mám teď dělat?			
	Pokud se k tomuto serveru obvykle připojujete bez problému, může tato chyba znamenat, že se za tento server někdo snaží vydávat, a neměli byste pokračovat.			
	Rychle odsud pryč!			
	Technické detaily			
	Vím, o co se jedná			
	Pokud chápete rizika, můžete Firefox požádat o výjimku a začít identifikaci tohoto serveru důvěřovat. když tomuto serveru důvěřujete, může tato chyba znamenat, že vám někdo odposlouchává připojení.			
	Nepřidávejte výjimku, pokud si nejste jisti, že tento server má dobrý důvod nepoužívat důvěryhodnou identifikaci.			
	Pridet výjimku			

V dalším okně klikněte na "Získat certifikát" a potom na "Schválit bezpečnostní výjimku"

Přidání bezpečnostní výjimky					
Chystáte se změnit způsob, jakým aplikace Firefox identifikuje tento server. Legitimní banky, obchody a ostatní veřejné servery vás o toto žádat nebudou.					
Server					
Adresa:	https://portal.ote-cr.cz/				
Stav certifikátu					
Tento se	rver se prokazuje neplatnými informacemi. <u>Z</u> obrazit				
Neznám	Neznámá identita				
Certifikát je nedůvěryhodný, protože nebyl ověřen důvěryhodnou autoritou pomocí bezpečného podpisu.					
 <u>U</u> loži	it tuto výjimku trvale				
	Schválit bezpečnostní výjimku Zrušit				

MTF-W PLYN 1 přihlášený uživatel Přihlášený: ELEKTŘINA Registrace POZE » Úvod Novinky vývěska DENNÍ TRH EVIDENCE REALIZAČNÍCH DIAGRAMŮ -Opravná seance DD Otevřený obchodní den: 16.02.2013 Otevřený obchodní den: 16.02.2013 14:00:00 CET Zavřeno 14:15:00 CET Výsledky VNITRODENNÍ TRH - Hodina17 BLOKOVÝ TRH - DB130218 20:00:00 CET Otevřeno 15:00:00 CET Otevřeno • 20:00:00 CET Otevřeno BLOKOVÝ TRH - DB130219 20:00:00 CET Otevřeno

Nyní jste se přihlásili do obchodního systému CS OTE prostřednictvím prohlížeče Firefox

Důležité upozornění chování prohlížeče Firefox při odesílání a podepisování dat!

Při odesílání dat Vám vyskočí okno, kde si zkontrolujete, jakým certifikátem data podepisujete. Ve spodní části okna je pole pro zadání hesla. Jde o dodatečné/extra heslo, které je možné ve Firefoxu zadat navíc k Vašemu certifikátu. Nejde o heslo, jaké máte nastavené u certifikátu, které jste použili při importu certifikátu. Pokud jste si sami toto dodatečné heslo nenastavili (v tomto manuálu to není popsáno), tak toto pole nevyplňujte!!!

