# Certifikační autorita EET

# Modelové postupy instalace certifikátu

Verze 1.0, 1.9.2016

## OBSAH

1	Ú٧	vod	3
2	Ins	stalace certifikátu ve Windows 7	4
	2.1	Instalace ze souboru .p12 (formát PKCS#12)	4
	2.2	Instalace ze souboru .cer (formát PEM)	4
3	Ins	stalace certifikátu ve Windows 10	9
	3.1	Instalace ze souboru .p12 (formát PKCS#12)	9
	3.2	Instalace ze souboru .cer (formát PEM)	9
4	Ins	stalace certifikátu v iOS	13
	4.1	Instalace kořenového certifikátu CA	13
	4.2	Instalace vlastního certifikátu	13
5	Ins	stalace certifikátu pro Android	18
	5.1	Instalace ze souboru .p12 (formát PKCS#12)	18
	5.2	Instalace ze souboru .cer (formát PEM)	18

### 1 Úvod

Uvedené postupy jsou označovány jako modelové, neboť konkrétní postup závisí vždy na konkrétním typu pokladního zařízení. Při práci s certifikáty pro evidenci tržeb doporučujeme postupovat podle instrukcí dodavatele či výrobce vašeho pokladního zařízení.

Uvedené postupy zahrnují práci se soukromým klíčem. Soukromý klíč musí být chráněn proti zcizení a zneužití, neboť právě soukromý klíč slouží k vytváření elektronických podpisů. Ochrana soukromých klíčů proti zneužití je dle zákona povinností poplatníka.

K instalaci certifikátu budete potřebovat soubor s certifikátem v jednom ze dvou formátů:

- 1. **PKCS#12** s příponou *.p12*, který získáte exportem na základě podání žádosti v prohlížeči, nebo
- ve formátu PEM s příponou .*crt*, který získáte pomocí vložení souboru žádosti do webové aplikace CA EET, či při stažení souboru certifikátu ze seznamu vydaných certifikátů.

Soubor .p12 **obsahuje i soukromý klíč** a proto jej vždy ukládejte do umístění, ke kterému máte přístup pouze vy, popřípadě osoba oprávněná k manipulaci se soukromým klíčem.

Soubor .crt neobsahuje takto citlivé informace, k zajištění funkčnosti **potřebuje soukromý klíč**, který byl v takovém případě vytvořen jiným způsobem, typicky při vytváření žádosti o certifikát.

Tento návod ukazuje obecné postupy instalace certifikátu na obvyklých platformách.

## 2 INSTALACE CERTIFIKÁTU VE WINDOWS 7

Obecný postup instalace certifikátu ve Windows 7 a kompatibilních OS je závislý na typu souboru certifikátu:

## 2.1 INSTALACE ZE SOUBORU .P12 (FORMÁT PKCS#12)

Pokud jste vytvořili certifikát v prohlížeči a uložili jej do souboru .p12, nebo jste takový soubor získali exportem z úložiště certifikátů, pak:

- Spusťte Průvodce importem certifikátu poklepáním na stažený soubor certifikátu (*přípona .p12*). Po nastavení jednotlivých kroků importu vždy pokračujte stisknutím tlačítka Další.
- 2. Zkontrolujte a potvrďte název a umístění souboru certifikátu.
- 3. Vložte heslo pro soukromý klíč zadané při vytváření certifikátu.
- 4. Zvolte úložiště certifikátů, kam má být certifikát uložen. (*Pokud chcete certifikát používat pouze na tomto počítači, zvolte automatický výběr úložiště*).
- 5. **Dokončete** průvodce importem
- 6. V dalším kroku aplikace importuje soukromý klíč a vytvoří certifikát. Pokud není dosud instalován kořenový certifikát certifikační autority, zobrazí se upozornění, že bude nainstalován.
- Po stisknutí tlačítka OK je certifikát nainstalován a je možné jej zkontrolovat ve zvoleném úložišti pomocí modulu *snap-in*.

## **2.2** INSTALACE ZE SOUBORU.CER (FORMÁT PEM)

Pokud jste certifikát vytvořili pomocí souboru žádosti, nebo máte k dispozici soubor ve formátu PEM *(přípona .cer nebo .pem)*, lze instalaci provést pouze v systému, ve kterém byla vytvořena žádost o certifikát (a je zde stále dostupný soukromý klíč). V takovém případě:

 Nejprve nainstalujte certifikát certifikační autority (např. pomocí odkazu certifikát CA na úvodní straně webové aplikace CA EET) do úložiště "Důvěryhodné kořenové certifikační úřady".

- 2. Poklepáním na stažený soubor certifikátu *(přípona .cer)* spusťte **Průvodce importem certifikátu** a postupujte obdobně jako při instalaci certifikátu ze souboru .p12 popsané výše.
- Pro vydaný certifikát by měl systém automaticky najít odpovídající soukromý klíč a nainstalovat jej do úložiště osobních certifikátů. Kontrolu certifikátu lze provést opět pomocí modulu *snap-in*.

## Obrazová příloha



Obrázek 2 Výběr souboru

Průvodce importem certifikátu	3
Importovat soubor	
Zadejte soubor, který chcete importovat.	
Název souboru:	
C:\Users\User\Downloads\1542469329.p12 Procházet	
Poznámka: V jednom souboru je možné uložit více než jeden certifikát v následujících formátech:	
Formát Personal Information Exchange - PKCS č. 12 (PFX, P12)	
Certifikáty standardu Cryptographic Message Syntax Standard - PKCS č. 7 (P7B)	
Serializované úložiště certifikátů (SST)	
Další informace o formátech souborů certifikátů	
Zpět Další > Storno	

Průvodce importem certifikátu	×
Heslo Z důvodu zajištění zabezpečení byl privátní klíč chráněn heslem.	
Zadejte heslo k privátnímu klíči.	
Heslo:	
<ul> <li>Povolit silnou ochranu privátního klíče (pokud zvolite tuto možnost, budete vždy při použití privátního klíče aplikací vyzváni k potvrzení akce)</li> <li>Označit tento klíč jako exportovatelný; později bude možné klíč zálohovat či přenést</li> <li>Zahrnout všechny rozšířené vlastnosti</li> <li>Další informace o ochraně privátních klíčů</li> </ul>	
< Zpět Další > Storna	•

Obrázek 3 Vložení hesla

růvod	ce importem certifikátu
Úlo	žiště certifikátů Úložiště certifikátů jsou oblasti systému, kde jsou uloženy certifikáty.
	Systém Windows může automaticky vybrat úložiště certifikátů, nebo můžete zadat umístění certifikátu.
	Automaticky vybrat úložiště certifikátů na základě typu certifikátu
	Všechny certifikáty umístit v následujícím úložišti
	Úložiště certifikátů:
Dal	ší informace o <u>úložištích certifikátů</u>
	< Zpět Další > Storno

Obrázek 4 Výběr úložiště



Obrázek 5 Dokončení průvodce

Program importuje nový privátní klíč pro výměnu.				
	Aplikace vytváří chráněnou položku.			
	Privátní klíč CryptoAPI			
	Je nastavena střední úroveň Nastavit úroveň zabezpečení			
	OK Stomo Podrobnosti			

Obrázek 7 Instalace kořenového certifikátu CA



vyžaduje:

EET CA 1

Systém Windows neověřil, zda je certifikát pochází skutečně z EET CA 1. Měli byste jeho původ potvrdit dotazem na EET CA 1. Následující číslo vám při procesu pomůže:

Kryptografický otisk (sha1): DB9A93E7 6E2D8731 818BA142 BCDB380A 1A028239

#### Upozornění:

Jestliže nainstalujete tento kořenový certifikát, bude systém Windows automaticky důvěřovat všem certifikátům vydaným touto certifikační autoritou. Instalace certifikátu s nepotvrzeným kryptografickým otiskem představuje bezpečnostní riziko. Kliknutím na tlačítko Ano toto riziko uznáváte.

Chcete tento certifikát nainstalovat?



#### Obrázek 9 Kontrola úložiště

Konzola1 - [Kořenový adresář konzoly\Certifiká	ty – aktuální uživateľ\Os	obní\Certifikáty]	
Soubor Akce Zobrazit Oblíbené položky	_ 8 ×		
🗢 🔿 🔁 🗊 🦨 💺 🖾 🚱			
Kořenový adresář konzoly	Vystaveno pro	Vystavitel	Akce
Certifikáty – aktuální uživatel	🛐 CZ	EET CA 1	Certifikáty 🔺
⊿ Osobní Certifikáty			Další 🕨
Důvěryhodné kořenové certifikační aut			
Důvěryhodnost v rámci rozlehlé sítě			D.I.Y.
Zprostředkující certifikační autority			Dalsi 🕨
Uživatelský objekt služby Active Directo			
Důvěryhodní vydavatelé			
Nedůvěryhodné certifikáty			
Kořenové certifikační autority třetích st			
Důvěryhodné osoby			
Ostatní uživatelé			
Požadavek na zápis certifikátu			
Důvěryhodné kořeny čipových karet			
Uloziste Usobni obsahuje 2 certifikátů.			

## **3** INSTALACE CERTIFIKÁTU VE WINDOWS **10**

Obecný postup instalace certifikátu ve Windows 10 a kompatibilních OS je závislý na typu souboru certifikátu.

## 3.1 INSTALACE ZE SOUBORU .P12 (FORMÁT PKCS#12)

Pokud jste vytvořili certifikát v prohlížeči uložili a jej do souboru .p12, nebo jste takový soubor získali exportem z úložiště certifikátů, pak:

- Poklepáním na stažený soubor certifikátu (*přípona .p12*) zobrazte náhled certifikátu a pokud je certifikát v pořádku, zvolte Nainstalovat certifikát.
- Spustí se Průvodce importem certifikátu, kde v prvním kroku vyberte umístění podle toho, zda bude certifikát využíván pouze aktuálně přihlášeným uživatelem, nebo všemi uživateli na tomto počítači. Pokračujte stisknutím tlačítka Další.
- 3. Vložte heslo pro soukromý klíč zadané při vytváření certifikátu.
- 4. Zvolte úložiště certifikátů, kam má být certifikát uložen. (*Pokud chcete certifikát používat pouze na tomto počítači, zvolte automatický výběr úložiště*).
- 5. **Dokončete** průvodce importem
- 6. V dalším kroku může aplikace vyžadovat instalaci kořenového certifikátu certifikační autority (pokud již není nainstalován). Zvolte **Ano** pro instalaci certifikátu CA.
- Po stisknutí tlačítka OK je certifikát nainstalován a je možné jej zkontrolovat ve zvoleném úložišti pomocí Správce Certifikátů.

## **3.2** INSTALACE ZE SOUBORU.CER (FORMÁT PEM)

Pokud jste certifikát vytvořili pomocí souboru žádosti, nebo máte k dispozici soubor ve formátu PEM *(přípona .cer nebo .pem)*, lze instalaci provést pouze v systému, ve kterém byla vytvořena žádost o certifikát (a je zde stále dostupný soukromý klíč). V takovém případě:

 Nejprve nainstalujte certifikát certifikační autority (např. pomocí odkazu certifikát CA na úvodní straně webové aplikace CA EET) do úložiště "Důvěryhodné kořenové certifikační úřady".

- 2. Poklepáním na stažený soubor certifikátu *(přípona .cer)* spusťte **Průvodce importem certifikátu** a postupujte obdobně jako při instalaci certifikátu ze souboru .p12 popsané výše.
- Pro vydaný certifikát by měl systém automaticky najít odpovídající soukromý klíč a nainstalovat jej do úložiště osobních certifikátů. Kontrolu certifikátu lze provést opět pomocí Správce Certifikátů.

#### Obrazová příloha

Obrázek 10 Informace o certifikátu

📃 Certifikát	×
Obecné Podrobnosti Cesta k certifikátu	
Informace o certifikátu	
Tento certifikát je určen k následujícímu účelu: • 2.16.840.1.101.3.2.1.48.1 • Všechny zásady použití	
* Podrobnosti naleznete v prohlášení certifikační autority. <b>Vystaveno pro:</b> CZ	
Vystavitel: EET CA 1	
Platnost od 18.08.2016 do 18.08.2019	
Nainstalovat certifikát Prohlášení vystavitele	
OK	

Obrázek 11 Spuštěr	ní průvodce importem
Vítá vás Průvodce importe	m certifikátu.
Průvodce vám pomůže kopírovat certifikát seznamy odvolaných certifikátů z disku do	y, seznamy důvěryhodných certifikátů a úložiště certifikátů.
Certifikát vydaný certifikační autoritou po nezbytné k ochraně dat nebo k vytvoření certifikátů je systémová oblast, v níž jsou	tvrzuje vaši totožnost a obsahuje informace zabezpečených síťových připojení. Úložiště certifikáty uloženy.
Umístění úložiště	1
Aktuální uživatel	
🔿 Místní počítač	
Pokračujte kliknutím na tlačítko Další.	
Obrázek 12	Výběr úložiště
Úložiště certifikátů	

ičujte kliknutím na tlačítko Další.
Obrázek 12 Výběr úložiště
tě certifikátů
ožiště certifikátů jsou oblasti systému, kde jsou uloženy certifikáty.
ystém Windows může automaticky vybrat úložiště certifikátů, nebo můžete zadat nístění certifikátu.
Automaticky vybrat úložiště certifikátů na základě typu certifikátu
🔿 Všechny certifikáty umístit v následujícím úložišti

Obrázek 13 Dokončení průvodce



	Obrazek 14 Insulace korenoveno cerujikala CA	
Upozorně	iní zabezpečení	×
	Rozhodli jste se nainstalovat certifikát z certifikační autority (CA), která se prezentuje jako:	
	EET CA 1	
	Systém Windows neověřil, zda certifikát pochází skutečně z EET CA 1. Měli byste jeho původ potvrdit dotazem na EET CA 1. Následující číslo vám při procesu pomůže:	
	Kryptografický otisk (sha1): DB9A93E7 6E2D8731 818BA142 BCDB380A 1A028239	
Upozornění: Jestliže nainstalujete tento kořenový certifikát, bude systém Windows automaticky důvěřovat všem certifikátům vystaveným touto certifikační autoritou. Instalace certifikátu s nepotvrzeným kryptografickým otiskem představuje bezpečnostní rizikoKliknutím na tlačítko Ano toto riziko uznáváte. Chcete tento certifikát nainstalovat?		
	Ano Ne	

Obrázek 14 Instalace kořenového certifikátu CA

Obrázek 15 Informace o importu	
Průvodce importem certifikátu	×
import proběhl úspěšně.	
OK	

Obrázek 16 Kontrola úložiště

🚡 certmgr - [Certifikáty – aktuální uživatel\Osobní\Certifikáty] – 🛛 🗙			×		
Soubor Akce Zobrazit Nápov	/ěda				
🗢 🔿 🙋 📅 🖌 🖬 🗙 🛙	1 🔒 🛛 🖬				
🖓 Certifikáty – aktuální uživatel 🔺	Vystaveno pro	Vystavitel	Datum uk	Popisný náz	zev
V Osobní	🛱 CZ	EET CA 1	18.08.2019	Žádost o ce	rtifikát
> Důvěryhodné kořenové ce					
> Důvěryhodnost v rámci ro					
> 🚞 Zprostředkující certifikačn 🗸					
< >	<				>
Úložiště Osobní obsahuje 2 certifikátů	i.				

## 4 INSTALACE CERTIFIKÁTU V IOS

Obecný postup instalace certifikátu na zařízeních s operačním systémem iOS spočívá ve dvou krocích popsaných v části 4.1 a 4.2:

## 4.1 INSTALACE KOŘENOVÉHO CERTIFIKÁTU CA

- 1. Stáhněte kořenový certifikát CA z úvodní strany webové aplikace CA EET
- 2. Spustí se průvodce instalací profilu, klepněte na Instalovat.
- 3. Zadejte kód zařízení (PIN).
- 4. Zobrazí se informace, že bude instalován *kořenový certifikát*, klepněte na volbu a poté na tlačítko **Instalovat**.
- 5. Kořenový certifikát CA je nainstalován a systém bude nyní důvěřovat jí vydaným certifikátům.

## 4.2 INSTALACE VLASTNÍHO CERTIFIKÁTU

- Získejte certifikát ve webové aplikaci CA EET na základě žádosti v prohlížeči nebo ze souboru žádosti a vyexportujte soubor, nebo jděte do SEZNAMU CERTIFIKÁTŮ, klikněte na příslušný certifikát a zvolte Stáhnout certifikát.
- 2. Spustí se průvodce instalací profilu, zde klepněte na Instalovat.
- 3. Zadejte kód zařízení (PIN).
- 4. Pokud instalujete kompletní certifikát (z exportovaného souboru) zadejte heslo k exportnímu souboru. Po jeho zadání klepněte na **Dále**.
- 5. Kořenový certifikát CA je nainstalován a ověřen.
- 6. Instalované certifikáty lze zkontrolovat v profilech zařízení Nastavení > Obecné > Profily

## Obrazová příloha

### Instalace kořenového certifikátu CA

Obrázek 17 Stažení kořenového certifikátu CA

## Informace o certifikační autoritě

Můžete si stáhnout certifikát CA nebo aktuální CRL.

Generální finanční ředitelství Lazarská 7, 117 22 Praha 1 | Technická podpora: ePodpora

Zrušit	Instalovat profil	Instalovat
	EET CA 1	
Podepsáno	EET CA 1	
	Neovereno	
Obsahuje	Certifikát	
Podrobno	eti	

Za	dejte kóc	ł	Zrušit
Za	adejte kód		
		-	

Obrázek 19 Zadání kódu (PIN) zařízení

	1	
Zrušit	Varování	Instalovat
KOŘENOVÝ CE	RTIFIKÁT	
Instalací bud přidán do se v iPhonu.	le certifikát "EET CA 1 <sup>:</sup> znamu důvěryhodnýcl	" n certifikátů
Obrázek 21	l Kořenový certifikát je na	instalován
	Profil nainstalován	Hotovo
EE	ET CA 1	
Podepsáno EE	eT CA 1 věřeno 🗸	
Obsahuje Ce	ertifikát	
Dedrehment		

#### Obrázek 20 Upozornění a instalace

## Instalace vlastního certifikátu

Obrázek 2	2 Stažení vlastního cei	rtifikátu z webové aplikace CA EET
ÚVOD	NOVÝ CERTIFIKÁT	SEZNAM CERTIFIKÁTŮ
Žádo Žádost Certifil	podána 29. 8. 2016 u kát	<b>t ID 837376a948ae</b> živatelem
Stav		
Sériov	é číslo	
Datum	vydání	
Datum	expirace	
Pozná	mka	
Stáhr	nout certifikát Zr	neplatnit



ovat	Instal	ovat profil	Instal	Zrušit
	hone)	(Test iP	CZ	
		(Test iPhone)	CZ Ověřeno 🗸	Podepsáno
			Certifikát	Obsahuje
			Certifikát	Obsahuje

Obrázek 24 Zadání kódu (PIN) zařízení

Zadejte kód	Zrušit
Zadejte kód	



Zrušit	Heslo	Dále
ZADEJTE HESL IDENTITY"	O K CERTIFIKÁTU "CERTIFII	KÁT

Požadováno profilem "Certifikát identity"

Obrázek 26 Informace o importu

	Profil nainsta	lován	Hotovo
	CZ (	Test iPho	ne)
Podepsáno	CZ (Test ił Ověřeno ✓	hone)	
Obsahuje	Certifikát		
Podrobno	sti		>

Obrázek 27 Kontrola úložiště

Cobecné Profily	
KONFIGURAČNÍ PROFILY	
EET CA 1	>
CZ (Test iPhone)	>

## 5 INSTALACE CERTIFIKÁTU PRO ANDROID

Obecný postup instalace certifikátu na zařízeních s operačním systémem Android se může lišit v závislosti na typu souboru certifikátu:

## 5.1 INSTALACE ZE SOUBORU .P12 (FORMÁT PKCS#12)

Pokud jste vytvořili certifikát v prohlížeči a uložili jej do souboru .p12, nebo jste takový soubor získali exportem z úložiště certifikátů, pak:

- 1. Přejděte do Nastavení Zabezpečení
- 2. Ve spodní části nabídky naleznete volbu Instalace z karty paměť telefonu.
- Po stisknutí je nutné vybrat soubor certifikátu k instalaci. Soubor najděte a klepněte na něj. Ve vyšších verzích systému Android (6+) postačí ke spuštění importu poklepat na stažený soubor v prohlížeči nebo souborovém manažeru
- 4. Budete vyzváni k zadání hesla, použitého při generování soukromého klíče. **Heslo vyplňte** a pokračujte tlačítkem **OK**.
- 5. Nyní si můžete zvolit a **vyplnit název certifikátu** a jeho použití. Název můžete nechat předdefinovaný a pokračujte tlačítkem **OK**.
- Uložení certifikátu v zařízení Android vyžaduje zapnutý zámek obrazovky. Není-li zámek zapnutý, budete vyzvání k Výběru odemknutí. Vyberte Vámi preferovaný zámek obrazovky a pokračujte podle instrukcí systému.
- 7. Dokončením procesu zámku obrazovky dojde k instalaci certifikátu do zařízení.

## 5.2 INSTALACE ZE SOUBORU .CER (FORMÁT PEM)

Pokud jste certifikát vytvořili pomocí souboru žádosti, nebo máte k dispozici soubor ve formátu PEM *(přípona .cer nebo .pem)*, lze instalaci provést pouze v systému, ve kterém byla vytvořena žádost o certifikát (a je zde stále dostupný soukromý klíč). V takovém případě:

 Nejprve nainstalujte certifikát certifikační autority (např. pomocí odkazu *certifikát CA* na úvodní straně webové aplikace CA EET)

- Nainstalujte certifikát ze staženého souboru obdobně jako při instalaci certifikátu ze souboru .p12 popsané výše.
- 3. Pro vydaný certifikát by měl systém automaticky najít odpovídající soukromý klíč a nainstalovat jej do úložiště osobních certifikátů.

Obrazová příloha
Obrázek 28 Nastavení - Zabezpečení
← Zabezpečení
privacy protection
Data Protection
Protect your data from unwanted access
Úložiště pověření
Typ úložiště Pouze software
Dûvêryhodná pověření Zobrazit důvěryhodné certifikáty CA
Instalace z karty paměť telefonu Nainstalovat certifikáty z karty paměť telefonu
Obrázek 29 Vložení souboru
≡ Stahování 🛛 🖛 i
1542469158.p12
1542469158.p12
Obrázek 30 Seznam důvěryhodných pověření
← Důvěryhodná pověření Q
SYSTÉM UŽIVATEL



Obrázek 32 Vyplnění názvu certifikátu

Zadejte název certifikátu Název certifikátu: 574f12f27029ef3cb87e7a20e8c10 Použití pověření: VPN a aplikace Balíček obsahuje: klíč pro jednoho uživatele certifikát pro jednoho uživatele jeden certifikát CA ZRUŠIT OK

Obrázek 33 Upozornění na zabezpečení

