

Certifikační autorita EET

Modelové postupy instalace certifikátu

Verze 1.0, 1.9.2016

OBSAH

1	Úvod	3
2	Instalace 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	Instalace 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	Instalace certifikátu v iOS.....	13
4.1	Instalace kořenového certifikátu CA	13
4.2	Instalace vlastního certifikátu	13
5	Instalace 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
2. **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:

1. Spusťte **Průvodce importem certifikátu** poklepnutím 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.
7. 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)

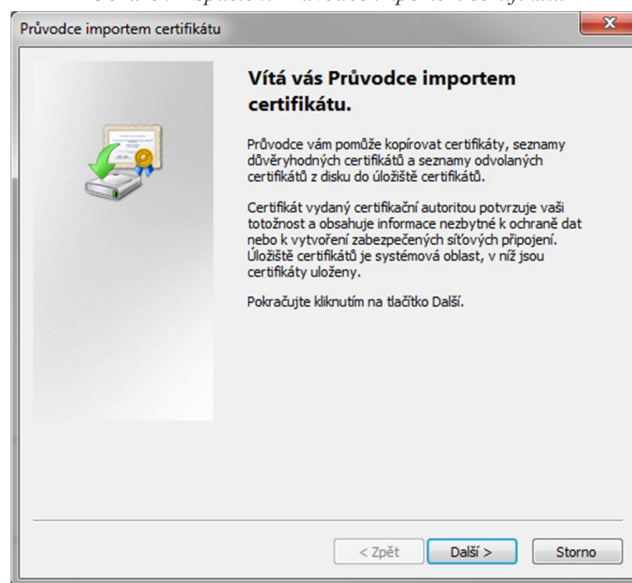
Pokud jste certifikát vytvořili pomocí souboru žádosti, nebo máte k dispozici soubor ve formátu PEM (*přípona .cer nebo .pem*), lze instalaci provést pouze v systému, ve kterém byla vytvořena žádost o certifikát (a je zde stále dostupný soukromý klíč). V takovém případě:

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

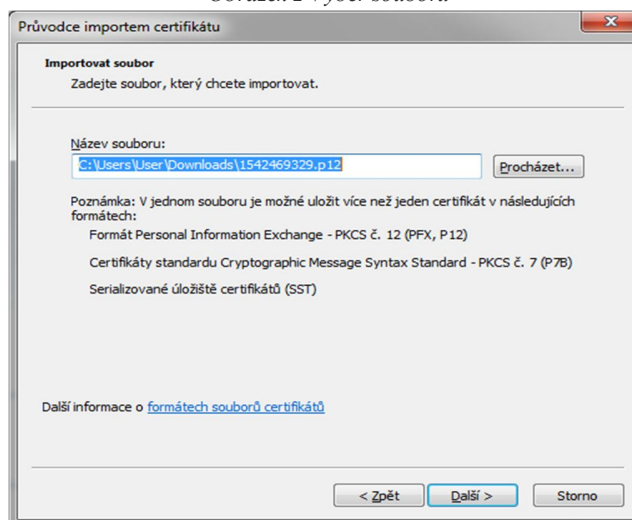
2. Poklepáním na stažený soubor certifikátu (*přípona .cer*) spusťte **Průvodce importem certifikátu** a postupujte obdobně jako při instalaci certifikátu ze souboru .p12 popsané výše.
3. Pro vydaný certifikát by měl systém automaticky najít odpovídající soukromý klíč a nainstalovat jej do úložiště osobních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

Obrazová příloha

Obrázek 1 Spuštění Průvodce importem certifikátu



Obrázek 2 Výběr souboru



Obrázek 3 Vložení hesla

Průvodce importem certifikátu

Heslo
Z důvodu zajištění zabezpečení byl privátní klíč chráněn heslem.

Zadejte heslo k privátnímu klíči.

Heslo:
●●●●

Povolit silnou ochranu privátního klíče (pokud zvolíte tuto možnost, budete vždy při použití privátního klíče aplikací vyzváni k potvrzení akce)

Označit tento klíč jako exportovatelný; později bude možné klíč zálohovat či přenést

Zahrnout všechny rozšířené vlastnosti

Další informace o [ochraně privátních klíčů](#)

< Zpět Další > Storno

Obrázek 4 Výběr úložiště

Průvodce importem certifikátu

Úložiště 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

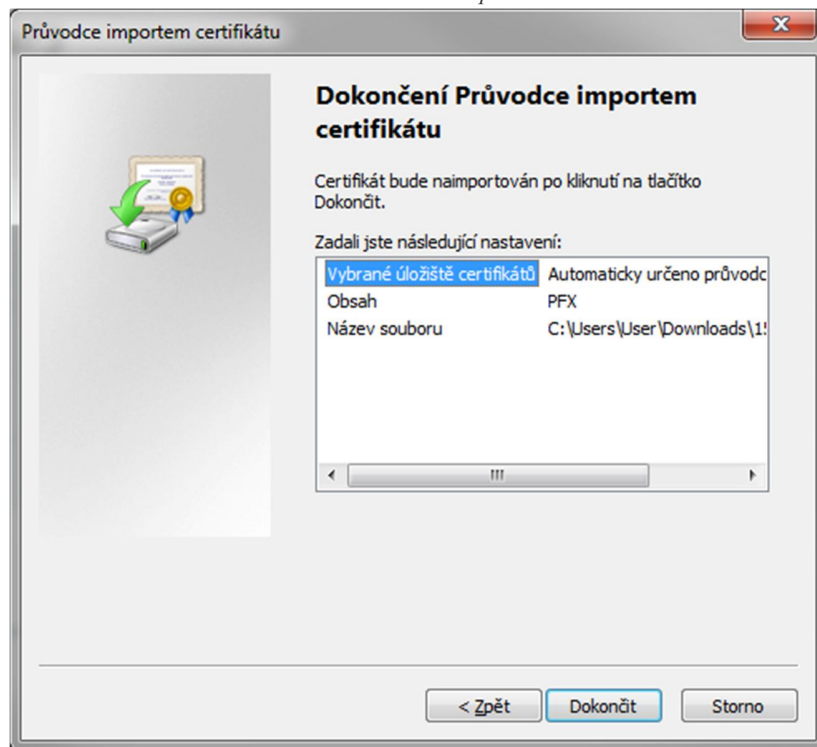
Všechny certifikáty umístit v následujícím úložišti

Úložiště certifikátů:
[] Procházet...

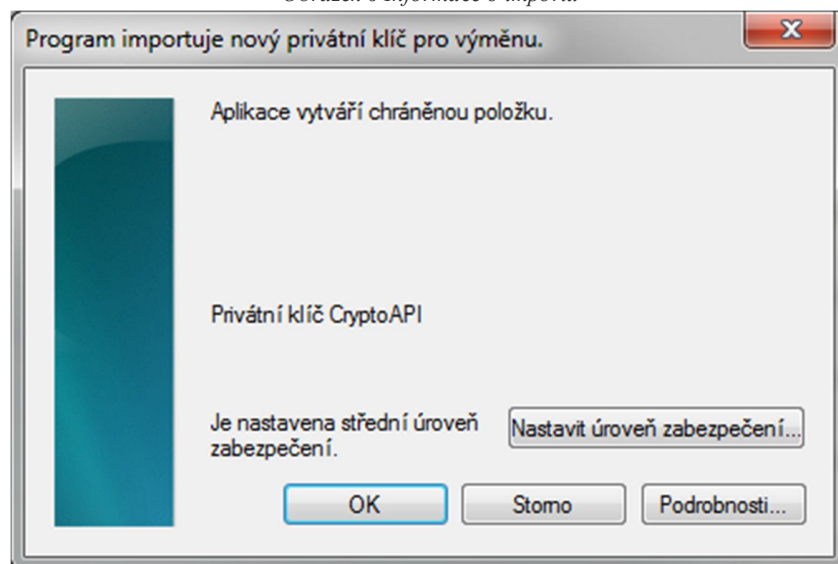
Další informace o [úložištích certifikátů](#)

< Zpět Další > Storno

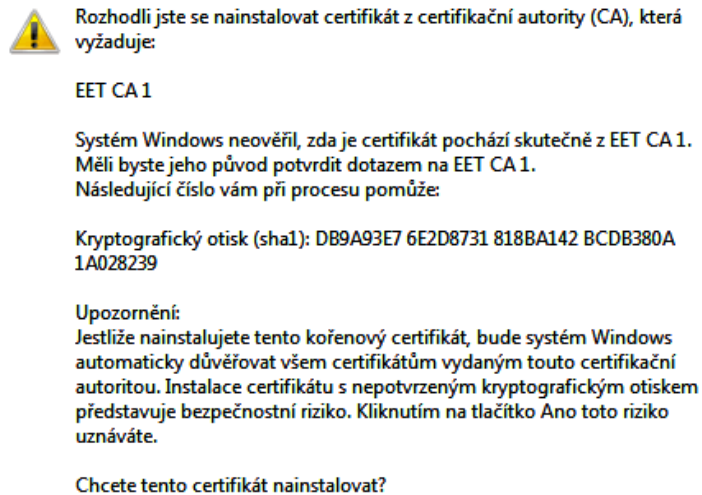
Obrázek 5 Dokončení průvodce



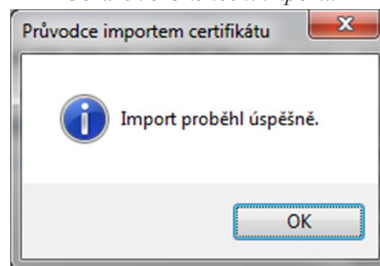
Obrázek 6 Informace o importu



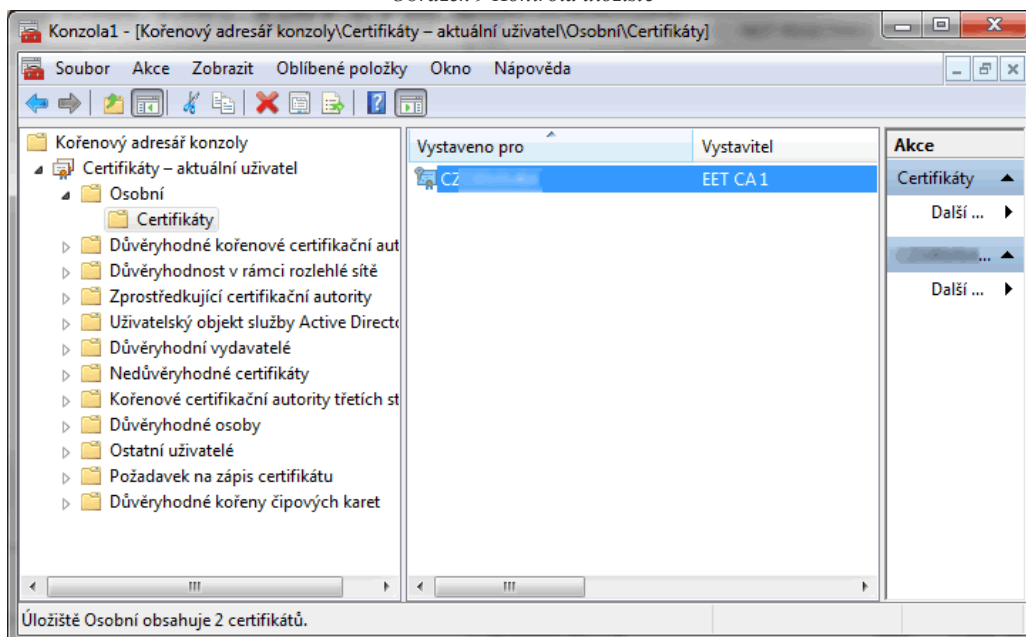
Obrázek 7 Instalace kořenového certifikátu CA



Obrázek 8 Ukončení importu



Obrázek 9 Kontrola úložiště



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:

1. Poklepáním na stažený soubor certifikátu (*přípona .p12*) zobrazte náhled certifikátu a pokud je certifikát v pořádku, zvolte **Nainstalovat certifikát**.
2. 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.
7. 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)

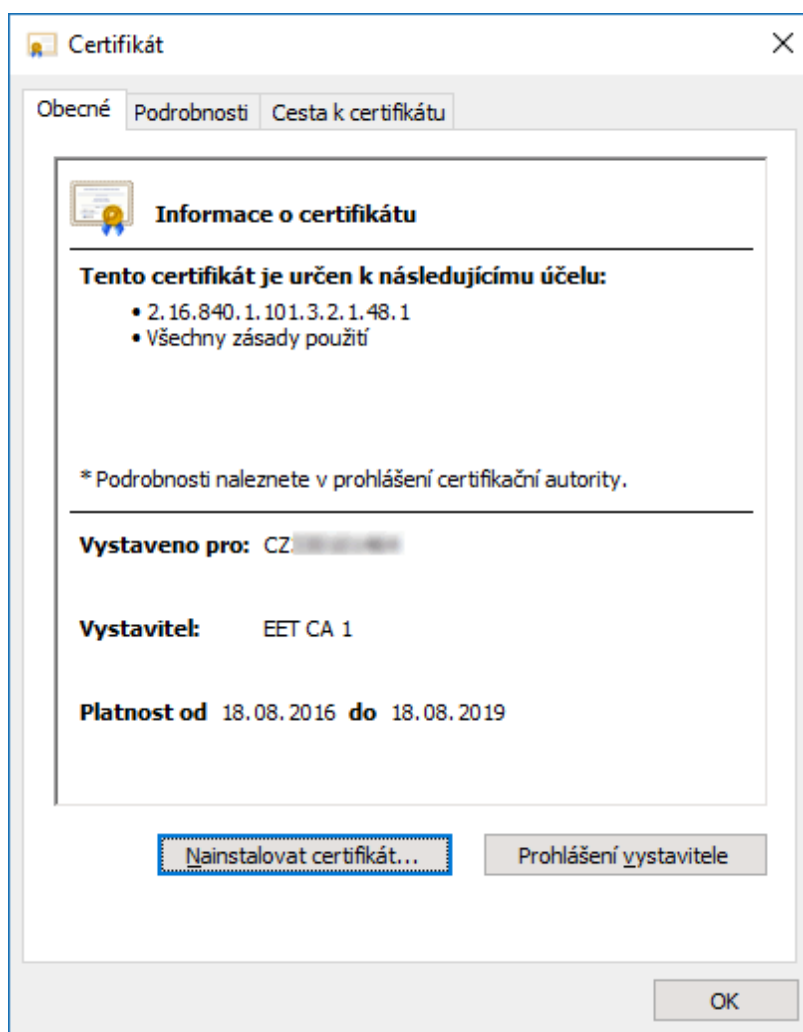
Pokud jste certifikát vytvořili pomocí souboru žádosti, nebo máte k dispozici soubor ve formátu PEM (*přípona .cer nebo .pem*), lze instalaci provést pouze v systému, ve kterém byla vytvořena žádost o certifikát (a je zde stále dostupný soukromý klíč). V takovém případě:

1. 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.
3. 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



Obrázek 11 Spuštění průvodce importem

Vítá vás Průvodce importem certifikátu.

Průvodce vám pomůže kopírovat certifikáty, seznamy důvěryhodných certifikátů a seznamy odvolaných certifikátů z disku do úložiště certifikátů.

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.

Umístění úložiště

Aktuální uživatel

Místní počítač

Pokračujte kliknutím na tlačítko Další.

Obrázek 12 Výběr úložiště

Úložiště 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:

Obrázek 13 Dokončení průvodce

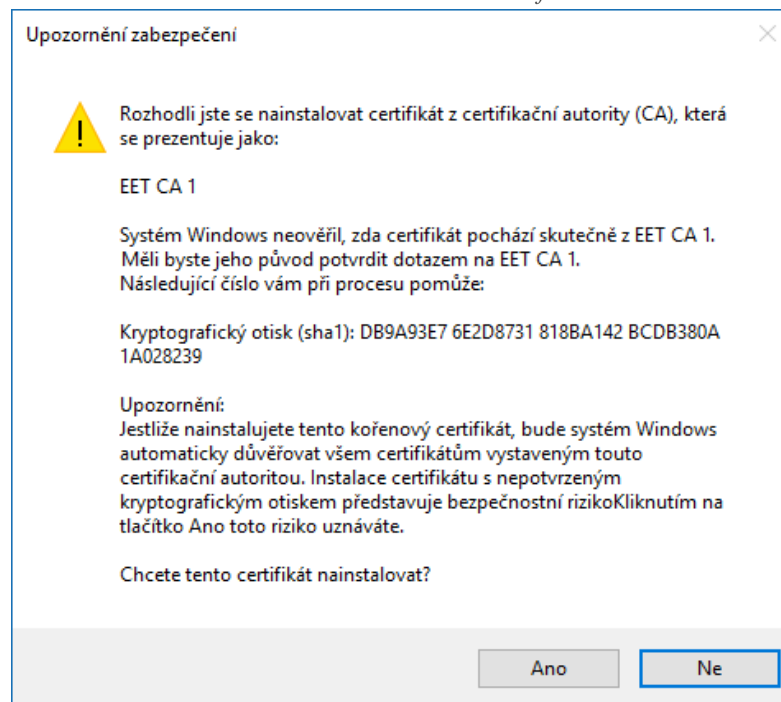
Dokončení Průvodce importem certifikátu

Certifikát bude nainportován po kliknutí na tlačítko Dokončit.

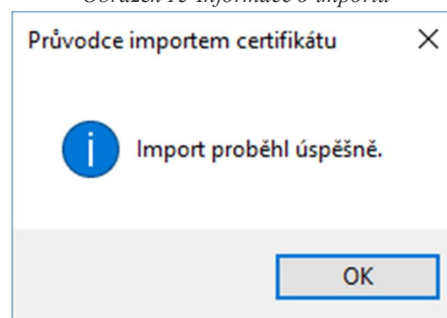
Zadali jste následující nastavení:

Vybrané úložiště certifikátů	Automaticky určeno průvodcem
Obsah	Certifikát

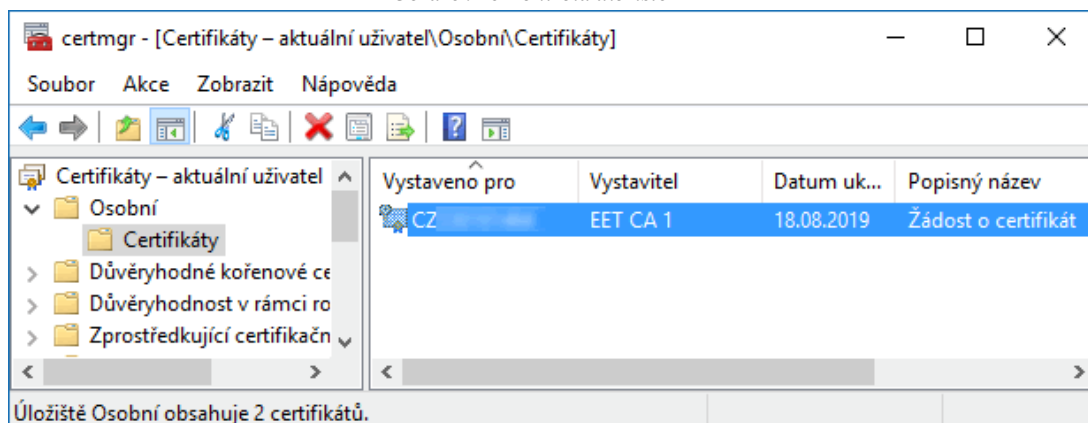
Obrázek 14 Instalace kořenového certifikátu CA



Obrázek 15 Informace o importu



Obrázek 16 Kontrola úložiště



4 INSTALACE CERTIFIKÁTU V IOS

Obecný postup instalace certifikátu na zařízeních s operačním systémem iOS spočívá ve dvou krocích popsanych 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

1. 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

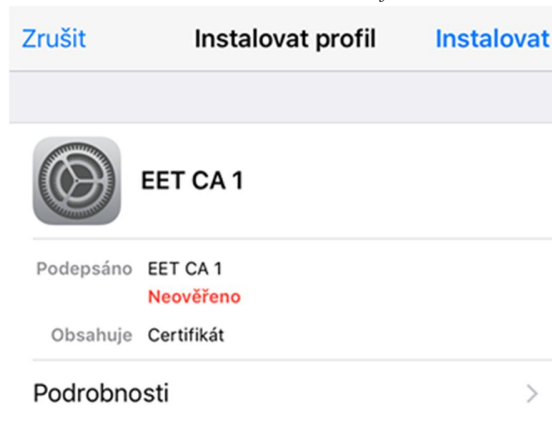
Obrázek 17 Stažení kořenového certifikátu CA

Informace o certifikační autoritě

Můžete si stáhnout [certifikát CA](#) nebo [aktuální CRL](#).

Generální finanční ředitelství
Lazarská 7, 117 22 Praha 1 | Technická podpora: [ePodpora](#)

Obrázek 18 Instalace certifikátu



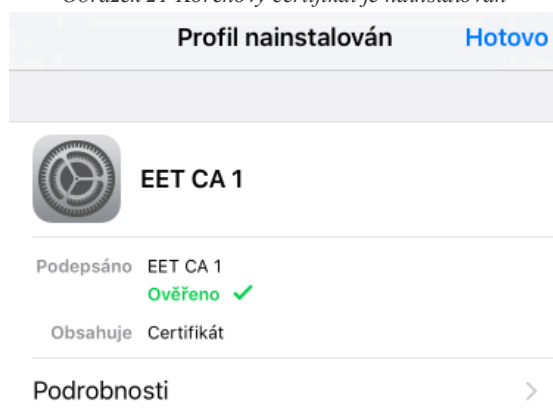
Obrázek 19 Zadání kódu (PIN) zařízení



Obrázek 20 Upozornění a instalace

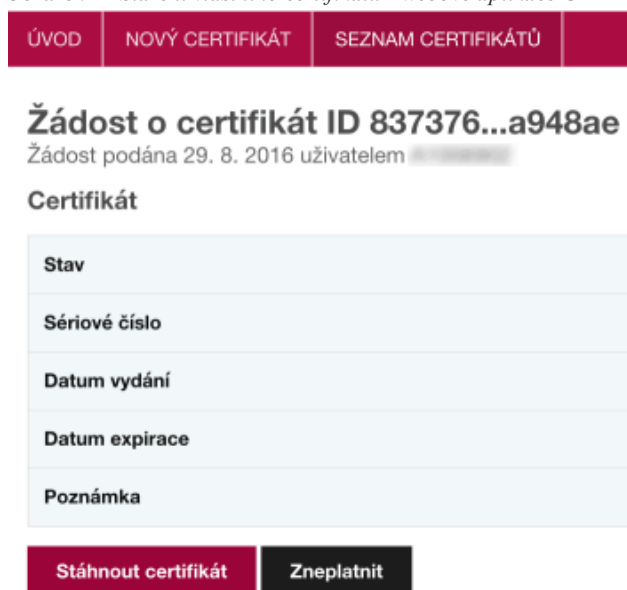


Obrázek 21 Kořenový certifikát je nainstalován

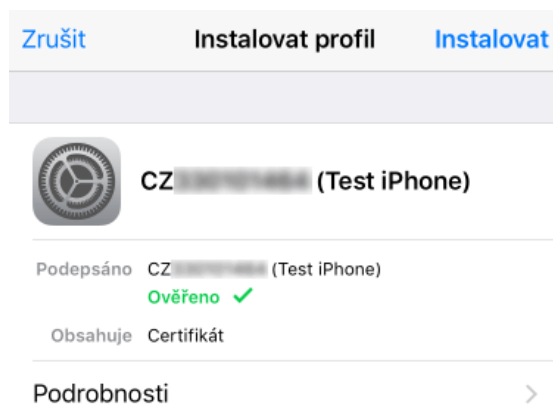


Instalace vlastního certifikátu

Obrázek 22 Stažení vlastního certifikátu z webové aplikace CA EET



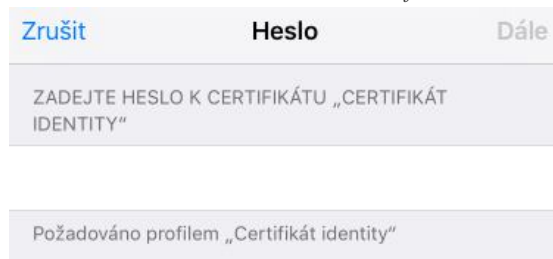
Obrázek 23 Instalace certifikátu



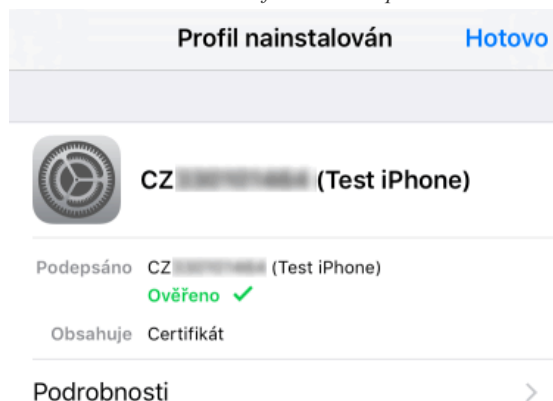
Obrázek 24 Zadání kódu (PIN) zařízení



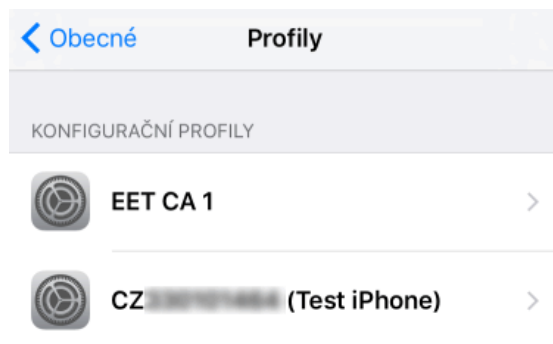
Obrázek 25 Zadání hesla k certifikátu



Obrázek 26 Informace o importu



Obrázek 27 Kontrola úložiště



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**.
3. Po stisknutí je nutné vybrat soubor certifikátu k instalaci. Soubor najdete 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**.
6. Uložení certifikátu v zařízení Android vyžaduje **zapnutý zámek obrazovky**. Není-li zámek zapnutý, budete vyzváni 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)

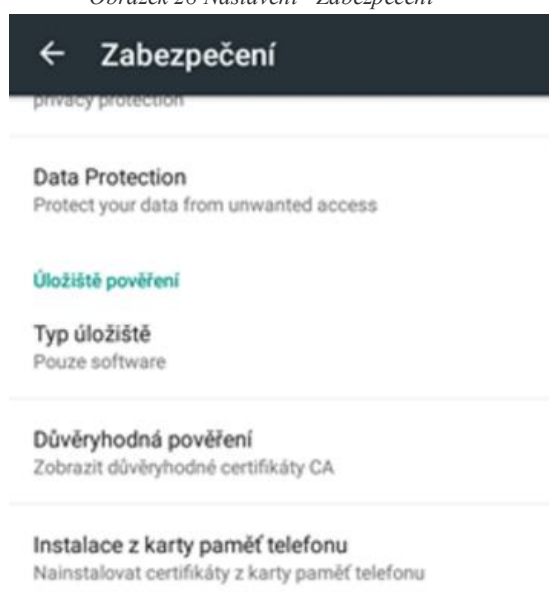
Pokud jste certifikát vytvořili pomocí souboru žádosti, nebo máte k dispozici soubor ve formátu PEM (*přípona .cer nebo .pem*), lze instalaci provést pouze v systému, ve kterém byla vytvořena žádost o certifikát (a je zde stále dostupný soukromý klíč). V takovém případě:

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

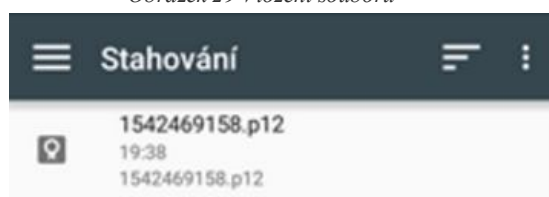
2. Nainstalujte certifikát ze staženého souboru obdobně jako při instalaci certifikátu ze souboru .p12 popsané výše.
3. Pro vydaný certifikát by měl systém automaticky najít odpovídající soukromý klíč a nainstalovat jej do úložiště osobních certifikátů.

Obrazová příloha

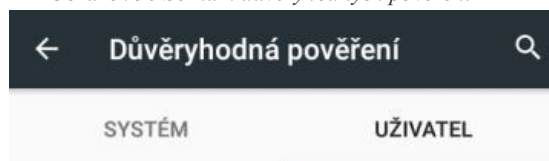
Obrázek 28 Nastavení - Zabezpečení



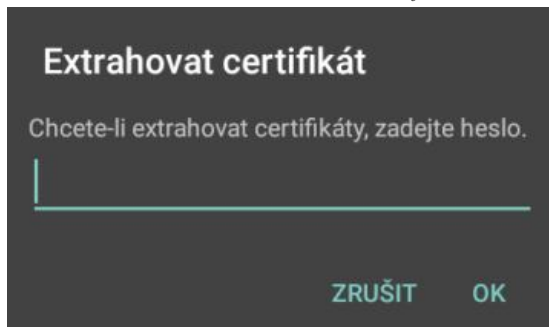
Obrázek 29 Vložení souboru



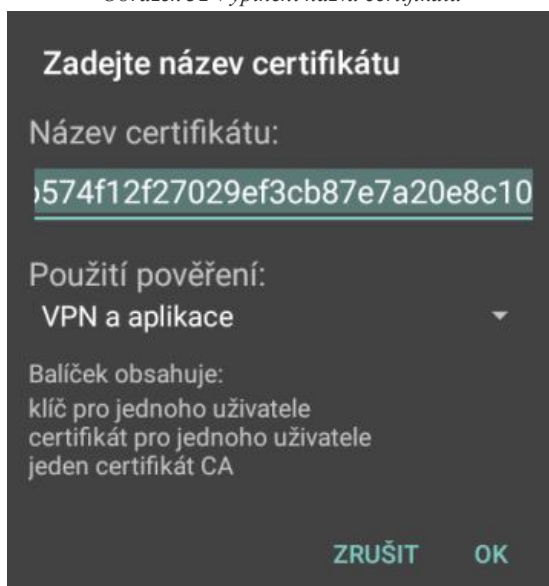
Obrázek 30 Seznam důvěryhodných pověření



Obrázek 31 Rozbalení balíku certifikátů



Obrázek 32 Vyplnění názvu certifikátu



Obrázek 33 Upozornění na zabezpečení

