# Certifikační autorita EET

# Veřejný souhrn certifikační politiky

Verze 1.0, 1.9.2016

**Vymezení obsahu dokumentu**

*Tento dokument obsahuje informace o zásadách a postupech činnosti Certifikační autority EET, provozované Finanční správou jako součást společného technického zařízení správce daně pro účely zákona č. 112/2016, o evidenci tržeb (dále jen „ZoET“). Dokument je určen držitelům certifikátů pro evidenci tržeb, žadatelům o certifikáty pro evidenci tržeb i veřejnosti.*

# Obsah

# 1 ÚVOD

Certifikační autorita EET (dále jen „CA EET“) poskytuje následující certifikační služby:

- vydání certifikátu pro evidenci tržeb,
- zneplatnění certifikátu pro evidenci tržeb,

CA EET dále poskytuje webovou aplikaci pro správu certifikátů (dále jen „webová aplikace CA EET“), přístupnou na stránkách Daňového portálu, prostřednictvím webové aplikace Elektronická evidence tržeb (dále jen „webová aplikace EET“).

CA EET vydává X. 509 certifikáty pro povinné subjekty dle ZoET (dále jen „poplatníky“), identifikované daňovým identifikačním číslem (DIČ). Subjektem evidence tržeb je v souladu s ustanovením § 3 ZoET poplatník daně z příjmů fyzických osob a poplatník daně z příjmů právnických osob. Vlastníkem a držitelem certifikátu, žadatelem o certifikát a podepisující osobou (využívající odpovídající soukromý klíč k vytváření elektronických podpisů) je ve smyslu ZoET vždy poplatník. Při přístupu k webové aplikaci CA EET je poplatník reprezentován pojmenovaným uživatelem webové aplikace EET (jeden poplatník může být reprezentován více uživateli).

# 2 CERTIFIKÁTY A JEJICH POUŽITÍ

Certifikáty vydané podle této Certifikační politiky se mohou použít pouze pro účely evidence tržeb dle ZoET a to pouze pro podepisování datových zpráv o evidovaných tržbách.

Všechny platné certifikáty jednoho poplatníka jsou z hlediska evidence tržeb rovnocenné.

Certifikáty je možno použít pouze na produkčním prostředí rozhraní pro příjem datových zpráv evidovaných tržeb.

Soukromý klíč vlastníka certifikátu musí být chráněn proti zneužití. Ochrana soukromých klíčů proti zneužití je dle § 16 ZoET povinností poplatníka. Certifikační politika neurčuje další požadavky na zabezpečení soukromých klíčů.

## 2.1 SPECIFIKACE CERTIFIKÁTŮ PRO EVIDENCI TRŽEB

DIČ je jediným povinným identifikátorem vlastníka certifikátu. Pro každého poplatníka je možno vydat libovolný počet certifikátů. DIČ poplatníka je obsahem pole CN (Common name) a je obsaženo v poli Subject ve formě DN (Distinguished Name).

Certifikáty jednoho poplatníka se odlišují pouze svým sériovým číslem a nepovinnou poznámkou v poli Description. Poznámka nehraje žádnou roli při vlastní evidenci tržeb, slouží pouze poplatníkovi pro usnadnění správy certifikátů. V poznámce lze použít národní znakové sady v kódování UTF8.

Poplatník může mít více certifikátů se stejným či jiným DN v poli Subject.

| *Položka* | *Obsah* |
|---|---|
| *Version* | 3 |
| *Serial Number* | *Náhodně generované* |
| *Subject* | DESCRIPTION=*volitelný krátký popis*, CN=*DIČ*, DC=CZ |
| *Issuer* | CN=EET CA 1, O=Česká Republika – Generální Finanční Ředitelství, DC=CZ |
| *Certificate Policies* | OID 1.2.203.27112489.1.200.1.1.1 |
| *Basic Constraints* | Klientský certifikát |
| *Subject Key Identifier* | *Odpovídající klíči* |
| *Authority Key Identifier* | *Odpovídající klíči CA* |
| *CRL distribution points* | http://crl.ca1.eet.cz/eetca1/all.crl<br>http://crl2.ca1.eet.cz/eetca1/all.crl<br>http://crl3.ca1.eet.cz/eetca1/all.crl |
| *Key Usage* | digitalSignature<br>nonRepudiation |
| *Algoritmus podpisu* | SHA-256 s RSA |
| *Klíč* | RSA 2048 |

## 2.2 SPECIFIKACE KOŘENOVÉHO CERTIFIKÁTU CA EET

| *Položka* | *Obsah* |
|---|---|
| *Version* | 3 |
| *Serial Number* | *Náhodně generované* |
| *Subject* | CN=EET CA 1, O= Česká Republika – Generální finanční ředitelství, DC=CZ |
| *Issuer* | CN=EET CA 1, O= Česká Republika – Generální finanční ředitelství, DC=CZ |
| *Certificate Policies* | OID 1.2.203.27112489.1.200.1.1.1 |
| *Basic Constraints* | CA, délka cesty 0 |
| *Subject Key Identifier* | *Odpovídající klíči* |
| *Authority Key Identifier* | *Odpovídající klíči* |
| *CRL distribution points* | http://crl.ca1.eet.cz/eetca1/all.crl<br>http://crl2.ca1.eet.cz/eetca1/all.crl<br>http://crl3.ca1.eet.cz/eetca1/all.crl |
| *Key Usage* | CRL Sign, Certificate Sign |
| *Algoritmus podpisu* | SHA-256 s RSA |
| *Klíč* | RSA 2048 |

## 2.3 DOBA PLATNOSTI CERTIFIKÁTŮ

| ***Typ certifikátu*** | ***Parametr*** | ***Hodnota*** |
|---|---|---|
| *Kořenový certifikát CA EET* | Doba platnosti | 6 let |
| *Kořenový certifikát CA EET* | Aktivní období používání certifikátu | 3 roky |
| *Certifikát pro evidenci tržeb* | Doba platnosti | 3 roky |

# 3 VYDÁVÁNÍ CERTIFIKÁTŮ

Roli registrační autority (ověření identity žadatelů o certifikát) plní webová aplikace EET. Autentizační údaje pro přístup do webové aplikace EET získává poplatník postupem dle § 13 a 14 ZoET.

Podmínkou vydání certifikátu pro evidenci tržeb je přihlášení uživatele do webové aplikace EET. Vydávání certifikátu probíhá ve webové aplikaci CA EET a to dvěma možnými způsoby:

1. vytvořením žádosti v prohlížeči. V tomto případě jsou soukromý klíč a žádost o certifikát vytvořeny webovou aplikací CA EET a na závěr je vytvořen exportní soubor ve formátu PKCS#12. Tyto kroky jsou řízené webovou aplikací, ale probíhají na zařízení uživatele.
2. načtením žádosti ze souboru. V tomto případě webová aplikace CA EET přijímá žádost ve formátu PKCS#10, obsahující RSA klíč o velikosti 2048 bitů.

Generování soukromých klíčů probíhá vždy na zařízení poplatníka. Poplatník je odpovědný za bezpečnost použitého zařízení.

DIČ poplatníka je při vydání certifikátu ověřováno proti přihlášení do webové aplikace EET. Jedinou neověřovanou informací v žádosti o certifikát je nepovinná poznámka. Přijaty budou pouze unikátní veřejné klíče.

V obvyklém případě je certifikát vydán a předán uživateli do 5 sekund. Pokud je překročen časový limit 5s, webová aplikace CA EET oznámí uživateli, že žádost probíhá a po vydání certifikátu jej na nový certifikát upozorní zprávou na přihlašovací stránce.

Vydávání certifikátů pro evidenci tržeb je pro poplatníky bezplatné.

# 4 ZNEPLATNĚNÍ CERTIFIKÁTŮ

Poplatník musí neprodleně požádat o zneplatnění certifikátu v případě, kdy hrozí nebezpečí zneužití soukromého klíče. Zneplatnit certifikát může i Finanční správa. Zneplatněný certifikát nemůže být znovu obnoven.

O zneplatnění certifikátu může požádat poplatník prostřednictvím webové aplikace CA EET po přihlášení do webové aplikace EET.

Certifikát je zneplatněn neprodleně a automaticky následuje vydání CRL v následujících časových intervalech:

- pravidelný interval vydávání CRL 15 minut
- vydání nového CRL do 1 minuty od zneplatnění certifikátu.

Možnost ověřování statutu certifikátu online (OCSP) není poskytována.

# 5 ZVEŘEJŇOVÁNÍ INFORMACÍ

CA EET zveřejňuje kořenový certifikát Certifikační autority EET.

CA EET zveřejňuje seznam zneplatněných certifikátů (Certificate revocation list – CRL). Aktuální seznam (poslední platný) bude dostupný vždy nejméně na jednom místě v elektronické formě ve formátu CRL na adresách:

- http://crl.ca1.eet.cz/eetca1/all.crl
- http://crl2.ca1.eet.cz/eetca1/all.crl
- http://crl3.ca1.eet.cz/eetca1/all.crl

Každý poplatník má prostřednictvím webové aplikace CA EET k dispozici seznam všech svých certifikátů včetně zneplatněných a s ukončenou platností.

CA EET zveřejňuje tento dokument a další dokumenty a informace související s technickou podporou služeb CA (nápověda k webové aplikaci CA EET, odpovědi na časté otázky apod).