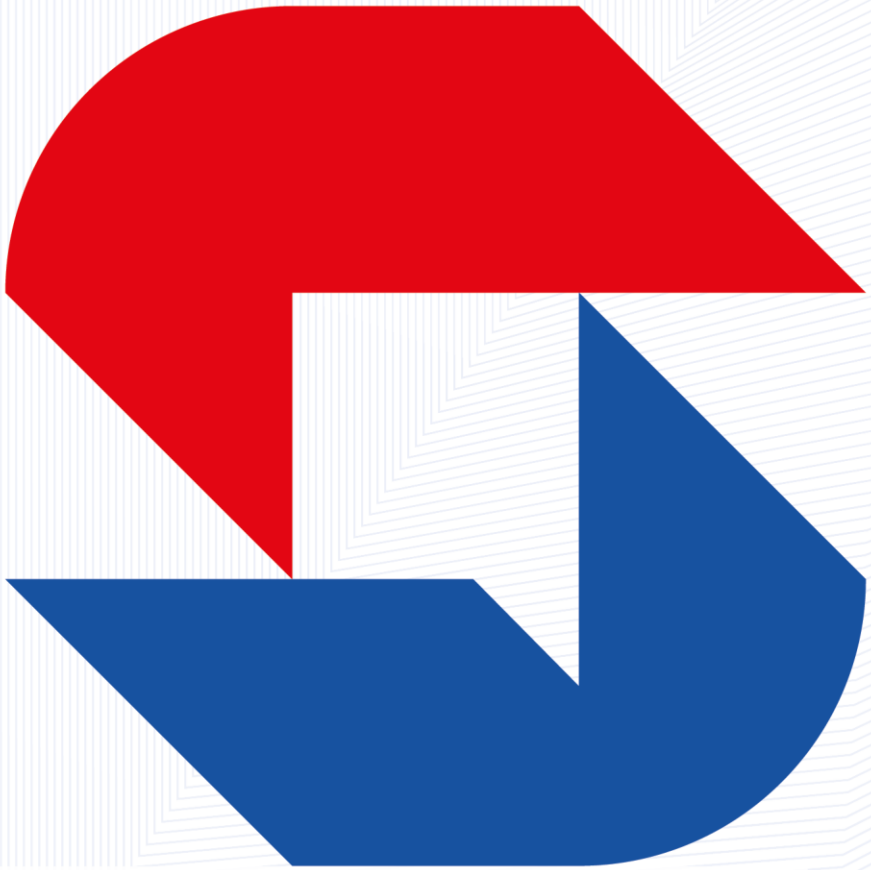
SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU



Certifikační autorita EET v 1.0

Veřejný souhrn certifikační politiky

Obsah

Úvod

Certifikační autorita EET v 2.0 (dále jen „*CA EET*“) vydává X.509 certifikáty (dále nazývané „pokladní certifikáty“) pro subjekty evidující tržby dle ZoET (dále jen "poplatníky") identifikované evidenčním identifikačním číslem EIČ (Evidenční identifikační číslo dle zákona ZoET). Vlastníkem a držitelem pokladního certifikátu a podepisující osobou (využívající odpovídající soukromý klíč) je vždy poplatník.

CA EET poskytuje následující externí certifikační služby:

- Vydání pokladního certifikátu.
- Automatizovanou obnovu pokladního certifikátu.
- Zneplatnění pokladního certifikátu.
- Vydávání seznamu zneplatněných pokladních certifikátů (dále jen „CRL“).

CA EET dále poskytuje webovou aplikaci pro správu pokladních certifikátů tzv. *Obslužný portál EET*. *Obslužný portál* je přístupný na portálu *MOJE daně*, který je dostupný na URL https://mojedane.gov.cz, z aplikace *Daňová informační schránka plus (DIS+).*

Autentizaci poplatníka pro služby poskytované *CA EET* a *Obslužného portálu* zajišťuje *portál MOJE daně (DIS+)*.

CA EET pro EET v 2.0 se od CA EET pro EET v 1.0 liší v těchto aspektech:

- *CA EET* pro EET v 2.0 má hierarchickou strukturu, tj. certifikační cesta je tvořena kořenovým certifikátem, mezilehlým certifikátem a koncovým (pokladním) certifikátem.
- Kořenový certifikát používá kryptografii RSA s délkou klíče 4096 b.
- Koncové certifikáty mají nový profil certifikátu, např. v certifikátu nejsou uváděny distribuční body CRL.
- Koncové certifikáty mají platnost 366 dní.
- Klíčový pár o délce 2048 b pro pokladní certifikát je generován bezpečným způsobem v systému *CA EET*.

Pokladní certifikáty a jejich použití

Pokladní certifikáty vydané *CA EET* se mohou použít pouze pro účely elektronické evidence tržeb, a to pouze pro autentizaci datových zpráv o evidovaných tržbách.

Poplatník může používat více pokladních certifikátů, všechny platné pokladní certifikáty jednoho poplatníka jsou z hlediska evidence tržeb rovnocenné.

Soukromý klíč (klíče) poplatníka tj. vlastníka pokladního certifikátu musí být chráněn(y) proti zneužití. Ochrana soukromých klíčů proti zneužití je povinností poplatníka.

Specifikace pokladních certifikátů

EIČ (resp.: DIČ/RČ/VČP) je jediným povinným identifikátorem vlastníka pokladního certifikátu. Pro každého poplatníka je možné vydat libovolný počet pokladních certifikátů. EIČ poplatníka je obsahem atributu *commonName* (zkráceně CN) v poli *subject*.

Pokladní certifikáty jednoho poplatníka se odlišují pouze sériovým číslem a nepovinnou poznámkou v atributu *description*. Poznámka nehraje žádnou roli při vlastní evidenci tržeb, slouží pouze poplatníkovi pro usnadnění správy pokladních certifikátů. V poznámce lze použít české znaky - text v kódování UTF8.

Poplatník může mít více certifikátů se stejným polem *subject*.

Pole	Obsah
version	v3 (0x2)
serialNumber	jedinečné sériové číslo pokladního certifikátu
signatureAlgorithm	sha256withRSAEncryption
issuer	stejné atributy a hodnoty jako v poli subject vydavatele pokladního certifikátu
validity	
notBefore	počátek platnosti pokladního certifikátu (UTC)
notAfter	notBefore + 366 dnů
subject	
commonName	EIČ (resp.: DIČ/RČ/VČP) poplatníka
description	poznámka zadaná poplatníkem, max 64 znaků
countryName	CZ
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	2048 bitů
extensions	rozšíření pokladního certifikátu
signature	digitální podpis vydavatele pokladního certifikátu (vydávající mezilehlé CA)

Rozšíření	
certificatePolicies	
policyInformation	
policyIdentifier	1.2.203.19122063.10.1.102.x.y Kde x.y je verze.subverze politiky
policyQualifiers	
userNotice	
keyUsage	digitalSignature, nonRepudiation
subjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) v tomto certifikátu
authorityKeyIdentifier	
keyIdentifier	hash veřejného klíče vydávající mezilehlé CA

Specifikace kořenového certifikátu CA EET (Root CA)

Pole	Obsah
version	v3 (0x2)
serialNumber	jedinečné sériové číslo vydávaného certifikátu
signatureAlgorithm	sha256WithRSAEncryption
issuer	
commonName	EETv2 NCA Root CA RSA *MM*/*RRRR*
organizationName	Správa státních služeb vytvářejících důvěru
organizationIdentifier	NTRCZ-19122063
countryName	CZ
validity	
notBefore	počátek platnosti certifikátu
notAfter	notBefore + 10let
subject	stejný obsah jako issuer výše
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	veřejný klíč 4096 bitů
extensions	rozšíření certifikátu
signature	digitální podpis vydavatele certifikátu (zde selfsign podpis kořenové CA)
Rozšíření	
certificatePolicies	
policyinformation	
policyIdentifier	anyPolicy (2.5.29.32.0)
basicConstraints	
cA	True
keyUsage	keyCertSign, cRLSign
subjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) v tomto certifikátu

Doba platnosti certifikátů

Typ certifikátu	Doba platnosti
Kořenový certifikát CA EET	10 let
Mezilehlý certifikát CA EET	4 roky
Pokladní certifikát	366 dní

Vydávání pokladních certifikátů na Obslužném portálu EET

Podmínkou vydání pokladního certifikátu je přihlášení poplatníka do aplikace *Daňová informační schránka plus*, na stránkách portálu *MOJE daně* (https://mojedane.gov.cz).

Vydání pokladního certifikátu proběhne na základě žádosti zaslané poplatníkem z *Obslužného portálu EET*, na který je směrován po vstupu do *DIS+,* části *EVIDENCE TRŽEB*

Ověření identity žadatelů o pokladní certifikát probíhá přes *portál MOJE daně (aplikaci DIS+). CA EET* identitu žadatele zabezpečeně získává ze systému *DIS+.*

V pokladním certifikátu je použito EIČ poplatníka, získané v rámci autentizace do DIS+. Jedinou neověřovanou informací v pokladním certifikátu je nepovinná poznámka.

Generování páru klíčů probíhá zabezpečeně v prostředí CA EET. Pro vydání pokladního certifikátu jsou použity pouze unikátní veřejné klíče. Žadatel obdrží pár klíčů spolu s pokladním certifikátem ve formátu PKCS#12 jako zabezpečený soubor s příponou *.p12*.

Vydávání pokladních certifikátů pro evidenci tržeb je pro poplatníky bezplatné.

Obnova pokladních certifikátů

Obnovu pokladního certifikátu provede CA EET na základě žádosti o obnovu podepsané soukromým klíčem příslušným k platnému obnovovanému pokladnímu certifikátu.

Žádosti o obnovu pokladního certifikátu zasílá pokladní systém na API CA EET. Proces obnovy pokladního certifikátu je automatizovaný.

Obnovený pokladní certifikát je vydán k novému veřejnému klíči, naplnění položek pokladního certifikátu je přebíráno z obnovovaného pokladního certifikátu.

Certifikát, kterému skončila platnost nebo byl zneplatněn, není možné obnovit.

Zneplatnění pokladních certifikátů

Poplatník může požádat o zneplatnění pokladního certifikátu zasláním žádosti o zneplatnění pokladního certifikátu z *Obslužného portálu EET*.

Na základě žádosti o zneplatnění je pokladní certifikát v *CA EET* neprodleně zneplatněn.

O zneplatnění pokladního certifikátu žádá poplatník například v případě, kdy hrozí nebezpečí zneužití soukromého klíče.

CA EET vydává CRL v následujícím režimu:

- v pravidelných intervalech po 8 hodinách,
- bezprostředně po zneplatnění pokladního certifikátu (do 1 minuty).

Platnost CRL bude 24 hodin.

Na CRL budou uvedeny všechny pokladní certifikáty, které byly zneplatněny a jejich platnost skončila později než 3 dny před vydáním CRL.

Možnost ověřování statusu pokladního certifikátu on-line (OCSP) *CA EET* neposkytuje.

Zveřejňování informací

CA EET zveřejňuje kořenový certifikát *CA EET* a mezilehlý certifikát *CA EET*. Oba certifikáty jsou dostupné na úvodní stránce *Obslužného portálu EET*.

CA EET poskytuje CRL ke stažení.

Každý poplatník má prostřednictvím *Obslužného portálu EET* k dispozici seznam všech svých pokladních certifikátů včetně zneplatněných a s ukončenou platností.

CA EET zveřejňuje certifikační politiku. Pro poplatníka je k dispozici na *Obslužném portálu EET*.