CS OTE

Dokumentace pro externí uživatele



Zákon č. 297/2016 Sb. a změny v CS OTE

© 2026 CGI IT Czech Republic s.r.o.

Obsah

Použité zkratky ... 3
1 Úvod ... 4
2 Podporované autority ... 4
3 Požadavky na certifikáty a jejich použití ... 5
3.1 Registrace certifikátů v CS OTE ... 5
3.1.1 Příklady ... 5
3.2 Webový portál CS OTE ... 6
3.3 OTE-COM ... 7
3.4 Automatická komunikace CS OTE ... 7
3.4.1 Webové služby ... 7
3.4.2 AMQP ... 8

© 2026 CGI IT Czech Republic s.r.o.

Použité zkratky

Zkratka	Význam
OTE	Společnost OTE, a.s.
CS OTE	Informační systém OTE
OTECA	Certifikační autorita provozovaná pro CS OTE
TLS	Komunikační kanál transparentně využívající šifrování pro zabezpečení dat
AMQP	Protokol používaný pro rychlou výměnu zpráv

© 2026 CGI IT Czech Republic s.r.o.

1 Úvod

Nařízení Evropského parlamentu a Rady Evropské unie č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce a zákon č. 297/2016 Sb., o službách vytvářejících důvěru, v kontextu vyjádření Energetického regulačního úřadu, vyžadují změny v CS OTE. Zákon vyžaduje důvěryhodnější úroveň elektronické komunikace mezi subjekty a státem založenou právnickou osobou OTE, a.s. Primárně se jedná o typ používaných certifikátů a jejich důvěryhodnost.

2 Podporované autority

Podle účelu je možno využívat certifikáty podporovaných certifikačních autorit pro systém CS OTE a to následovně:

a. Pro přístup do aplikace OTECOM a šifrování e-mailových zpráv je možné využít pouze komerční certifikáty od komerčních autorit
b. Pro elektronický podpis/značku/pečeť je vyžadováno použití kvalifikovaných certifikátů od kvalifikovaných autorit.

Seznam důvěryhodných certifikačních autorit ke komunikaci s CS OTE je dostupný na Veřejném webu OTE nebo také k dispozici v Seznamu certifikačních autorit v sekci „Sestavy“ v portálu IS OTE.

Výše uvedený seznam je možné rozšířit na základě žádosti účastníka trhu o prověření dané autority operátorem trhu – kontaktujte prosím services@ote-cr.cz

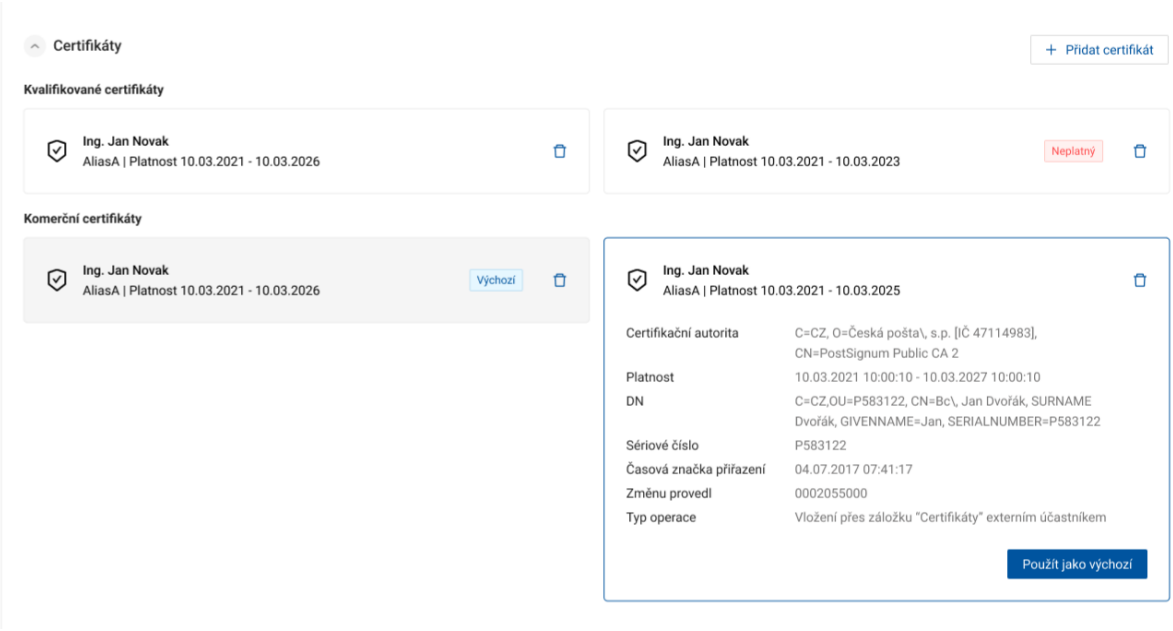
© 2026 CGI IT Czech Republic s.r.o.

3 Požadavky na certifikáty a jejich použití

3.1 Registrace certifikátů v CS OTE

V CS OTE v části Kmenová data – zabezpečený přístup je možné registrovat pouze certifikáty s minimální délkou RSA klíče 2048 b. Odpovídajícími typy certifikátu jsou:

- Typ „Komerční“ – slouží pro účely přístupu OTE-COM, TLS autentizace a šifrování e-mailových zpráv. U tohoto certifikátu je kontrolován vydavatel a typ certifikátu (komerční), který musí být ze seznamu podporovaných certifikačních autorit.
- Typ „Kvalifikovaný“ – slouží pro účely elektronického podpisu, značky nebo pečetě. U tohoto certifikátu je kontrolován vydavatel a typ certifikátu (kvalifikovaný), který musí být ze seznamu podporovaných certifikačních autorit.



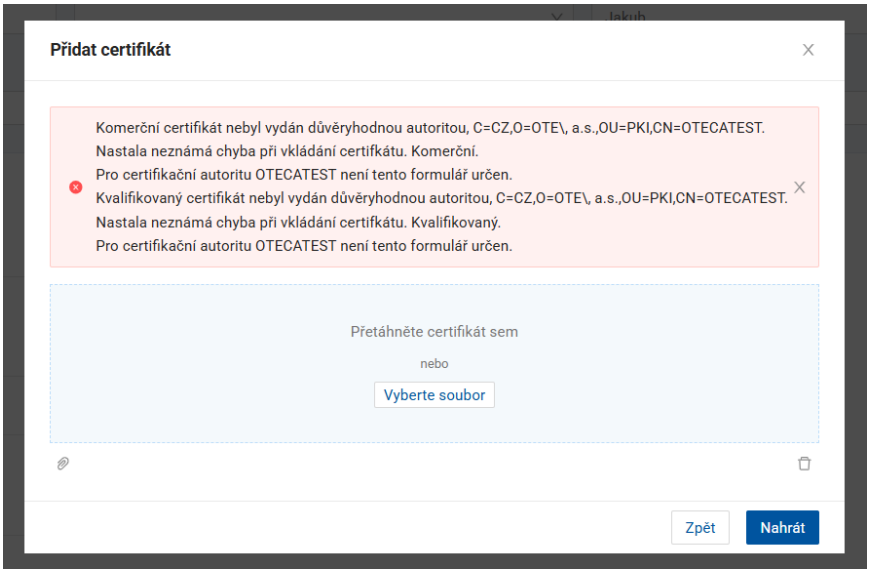
Obrázek 1 - Registrace certifikátů v CS OTE

Pokud uživatel (nebo externí systém) disponuje pouze kvalifikovaným certifikátem, nebude druhý typ certifikátu nutné do CS OTE registrovat (příslušné pole zůstane prázdné).

3.1.1 Příklady

V případě, že se uživatel pokusí zaregistrovat komerční/kvalifikovaný certifikát od nepodporované CA, je zobrazena následující chybová hláška na základě typu vloženého certifikátu.

© 2026 CGI IT Czech Republic s.r.o.



Obrázek 2 - Chybová hláška při pokusu o vložení nepodporovaného certifikátu

Uživatel má v CS OTE registrován pouze komerční certifikát:

- V tomto případě si musí uživatel zajistit kvalifikovaný certifikát pro přístup do webového portálu CS OTE a elektronické podepisování.

Uživatel má v CS OTE registrován pouze kvalifikovaný certifikát:

- certifikát není možné používat pro přístup do aplikace OTE-COM a k šifrování zpráv. Pokud bude uživatel chtít přijímat šifrované emaily z CS OTE anebo se přihlašovat do aplikace OTECOM, tak si musí předtím zajistit jeden z komerčních certifikátů viz kapitola 2 - Podporované autority.

3.2 Webový portál CS OTE

Veškerá zadávaná data musí být opatřena:

1. uznávaným elektronickým podpisem, který je založený na kvalifikovaném certifikátu
2. kvalifikovaným elektronickým podpisem založený na kvalifikovaném certifikátu dle eIDAS.

Je tedy nutné mít certifikát od kvalifikované autority viz kapitola 2 - Podporované autority a to uložený buď na tzv. softwarovém úložišti anebo na kvalifikovaném prostředku, tedy certifikovaném hardwarovém zařízení jako je USB token nebo čipová karta. Uživatelská podpora pro tato zařízení je plně v kompetenci dodavatele zařízení (např. autority).

Tento certifikát je možné registrovat s okamžitou platností jako typ Kvalifikovaný. Toto může provést uživatel pro svou registraci nebo administrátor společnosti s rolí „Správa údajů RÚT“ pro všechny uživatele v rámci společnosti.

© 2026 CGI IT Czech Republic s.r.o.

3.3 OTE-COM

Pro **aplikaci OTECOM** musí účastník trhu pro přihlášení k aplikaci použít komerční certifikát. Pro elektronický podpis dat platí stejná pravidla jako v případě webového portálu, tzn. veškerá data musí být podepsána pouze kvalifikovaným certifikátem, viz kapitola 2 - Podporované autority opět buď na tzv. **softwarovém úložišti** nebo **hardwarovém zařízení**.

Příslušné certifikáty je možné s odpovídající platností registrovat v CS OTE portálu. Toto může provést přímo uživatel pro svou registraci nebo administrátor společnosti s rolí „Správa údajů RÚT“ pro všechny uživatele v rámci společnosti.

3.4 Automatická komunikace CS OTE

Pro elektronický podpis **v automatické komunikaci** (vytváření elektronické značky) je možné registrovat pouze kvalifikované systémové certifikáty, a to až do doby, kdy budou dostupné kvalifikované certifikáty pro elektronické pečetě, které tyto systémové certifikáty nahradí. Není tedy možné použít komerční certifikáty k vytváření elektronické značky (automatizovanému podpisu).

Každý subjekt zasílající automatizovaně značená nebo pečetěná data do CS OTE musí mít pro systém jeden ze dvou možných kvalifikovaných certifikátů:

a. kvalifikovaný systémový certifikát, který může být uložen na softwarovém úložišti – tento typ je možný mít do odvolání, tj. do doby, kdy budou dostupné kvalifikované certifikáty pro elektronické pečetě
b. kvalifikovaný certifikát pro elektronickou pečeť na certifikovaném hardwarovém zařízení
    1. Vzhledem k implementaci hardwarového zařízení do informačního systému uživatele vyžaduje nutné zásahy na straně účastníků
    2. Kvalifikované certifikáty pro elektronickou pečeť nejsou prozatím u některých autorit nabízeny

Některé typy dat není možné vůbec elektronicky značit, resp. pečetit, a tedy odesílat pomocí automatické komunikace. Tato data lze zadávat pouze za vědomé interakce uživatele na CS OTE portálu za použití elektronického podpisu kvalifikovaným certifikátem, protože to legislativa nepovoluje. Toto omezení se vztahuje na následující typy zpráv:

- Informace o podporované výrobě zprostředkovatelem nebo vlastním výrobcem.
- Veškeré zprávy v modulu Evidence záruk původu

3.4.1 Webové služby

WS-Security hlavička i vlastní datová entita musí být podepsány (resp. opatřeny elektronickou značkou nebo pečetí) kvalifikovaným certifikátem.

© 2026 CGI IT Czech Republic s.r.o.

Není možné navazovat TLS spojení kvalifikovaným certifikátem. Pokud systém disponuje pouze certifikátem pro kvalifikovanou elektronickou značku nebo pečeť, je možné navázat spojení bez klientské autentizace. Údaje pro ověření systému jsou získávány z WS-Security hlavičky.

3.4.2 AMQP

Pro účely obchodování na VDT a VT prostřednictvím AMQP serveru je nutné nejen disponovat stejnými prostředky pro kvalifikovaný elektronický podpis (pečeť/značka) - viz výše, ale rovněž používat komerční (serverový) certifikát pro účely TLS autentizace.

© 2026 CGI IT Czech Republic s.r.o.