CS OTE

User Manual for External Users



This document is made according to Law no. 297/2016 and according to changes in CS OTE

© 2026 CGI IT Czech Republic s.r.o.

Table of Contents

List of Abbreviations 3
1 Introduction 4
2 Supported authorities 4
3 Certificate requirements and usage 5
3.1 Certificate registration in CS OTE 5
3.1.1 Examples 5
3.2 CS OTE web portal 6
3.3 OTE-COM 7
3.4 CS OTE Automatic communication 7
3.4.1 Web services 7
3.4.2 AMQP 8

© 2026 CGI IT Czech Republic s.r.o.

List of Abbreviations

Abbreviation	Meaning
OTE	OTE, a.s. company
CS OTE	OTE information system
OTECA	CS OTE Certified authority
TLS	Communication channel that transparently uses encryption for data security
AMQP	Protocol that is used for fast message exchange

© 2026 CGI IT Czech Republic s.r.o.

1 Introduction

According to Regulation no. 910/2014 of the European parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and according to Law no. 297/2016 on trust services in context of Energy Regulation Office statement, changes in CS OTE are needed. According to above mentioned laws, more trustworthy level of electronic communication between subjects and OTE a.s. company is demanded

2 Supported authorities

According to usage, it is possible to use certificates of supported certificate authorities for CS OTE system as follows:

a. Access to OTE-COM application and e-mail message encryption – only so-called commerce certificates provided by commerce authorities are possible to use.
b. Digital signature/mark/seal – only so-called qualified certificates provided by qualified authorities are possible to use.

List of trusted certificate authorities used for communication with CS OTE is available at Public web OTE or also available in List of certification authorities in "Reports" sections in OTE WebPortal.

It is possible to extend trusted authorities list based on market participant request. In such case, please contact services@ote-cr.cz.

© 2026 CGI IT Czech Republic s.r.o.

3 Certificate requirements and usage

3.1 Certificate registration in CS OTE

IN CS OTE section My certificates it is possible to register certificates with minimal RSA key strength 2048b. Appropriate certificates are:

- "Commerce" type – used for access to OTE-COM application, TLS authentication and e-mail message encryption. At this certificate, provider and type (commerce type) attributes are checked to meet list of certification authorities.
- "Qualified" type – used for the purpose of digital signature, mark or seal. At this certificate, provider and type (qualified) are checked to meet list of certification authorities.

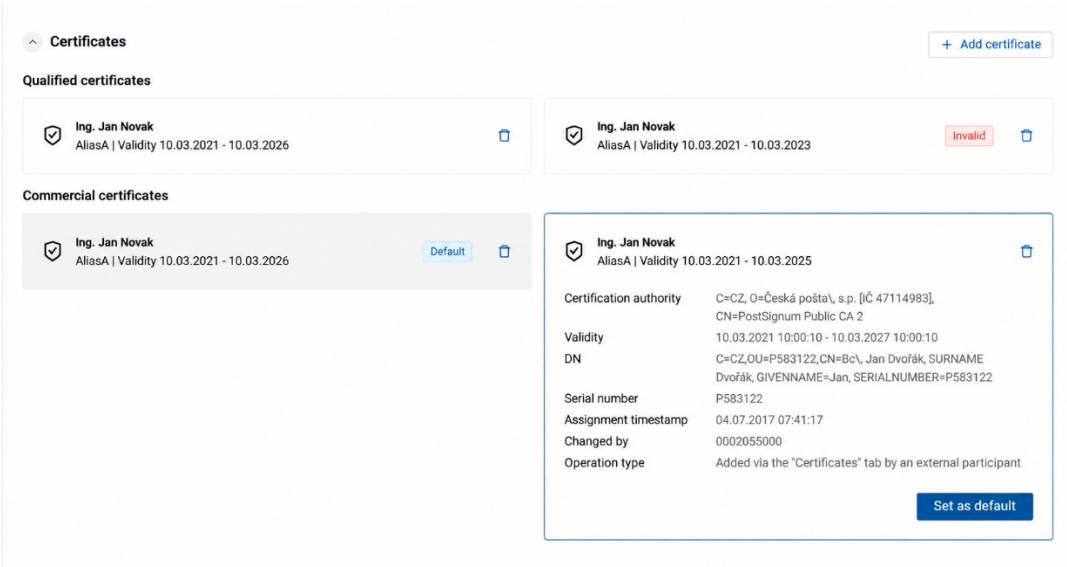


Figure 1 - Certificate registration in CS OTE

If user (or external system) holds only qualified type of certificate, he/she won't register the second one. The relevant field may stay empty.

3.1.1 Examples

If a user attempts to register a commercial or qualified certificate issued by an unsupported CA, the following error message is displayed based on the type of certificate submitted.

© 2026 CGI IT Czech Republic s.r.o.

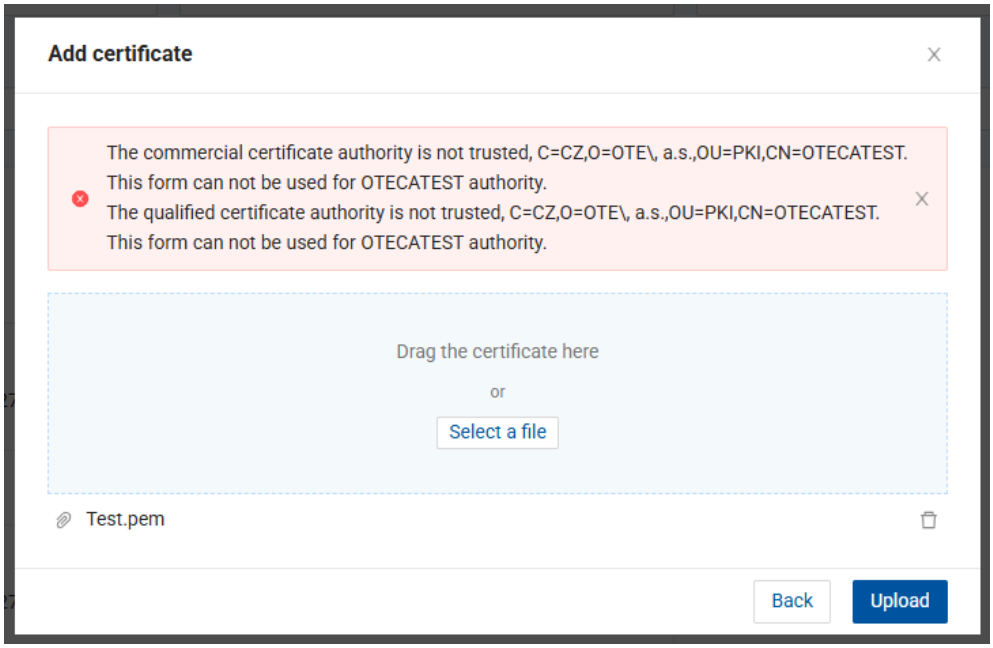


Figure 2 - Error message displayed when attempting to upload an unsupported certificate

User has registered only commerce certificate in CS OTE:

- In such case, user must obtain qualified certificate for his/her access to CS OTE web portal and for digital signature.

User has registered only qualified certificate in CS OTE:

- It won't be possible to use it for access to OTE-COM application and for message encryption. If the user would like to receive encrypted e-mails from CS OTE or sign into OTE-COM application, he/she must obtain commerce certificate

3.2 CS OTE web portal

All the provided data must contain following:

1. Certified digital signature - based on qualified certificate
2. Qualified digital signature - based on qualified certificate meet eIDAS rules

Users must have certificates only issued by the qualified authority (see chapter 2 - Supported authorities). These certificates should be stored on so-called software storage or on qualified equipment, i.e. certificated hardware equipment (USB token or chip card). Support of such HW equipment is fully managed by supplier (e.g. authority).

It is possible to register above mentioned certificates immediately (as Signing type). Certificate registration process can be made by user himself or by company administrator. Authorized person can manage other user accounts and certificates and may do the registration process for all the company users.

© 2026 CGI IT Czech Republic s.r.o.

3.3 OTE-COM

All market users must use commerce certificate for their login into OTE-COM application. There are the same rules for data digital signature as for web portal; it means that all the data must be signed only by qualified certificate (see chapter 2 - Supported authorities), stored on so-called **software storage** or **hardware equipment**.

It is possible to register relevant certificates with the relevant validity in CS OTE portal. Registration process can be made by user himself or by company administrator. The company administrator person can manage other users accounts and certificates and may do the registration process for all the company users.

3.4 CS OTE Automatic communication

Only qualified system certificates are possible for registration in CS OTE, for digital signature in **automatic communication** (electronic mark creation). This state will last until the time when qualified certificates are available for electronic seals from supported certificate authorities. These seals will replace system certificates. It is not possible to use the commerce certificates for electronic mark creation (automated signature).
All provided data to CSOTE from market participants, automatically marked or sealed must use one of below mentioned certificates:

a. Qualified system certificate, stored in software storage – user can use this kind of certificate until further notice; i.e. until qualified certificates for electronic seals will be available from supported certificate authorities.
b. Qualified certificate for electronic seal, stored on certified hardware equipment
    1. It can be more complicated due new hardware equipment. This will probably require changes on external market participant systems.
    2. Qualified certificates for electronic seal aren't offered by some certificate authorities now

Some data types cannot electronically mark (or to seal) and neither sends them via this automatic communication channel. It is possible to provide digital signed data only with user interaction in CS OTE portal. It means, using of digital signature by qualified certificate by user himself (legislation doesn't allow other uses). This limitation is connected to below mentioned message types:

- Renewal resources data or production data provided by producers or intermediaries
- All the messages in " Guarantees of Origin" module

3.4.1 Web services

WS-Security header and data entity itself must be signed (marked or sealed) by the qualified certificate.

© 2026 CGI IT Czech Republic s.r.o.

It is not possible to use qualified certificate for TLS authentication. If system contains only certificate for qualified electronic mark or digital signature, it is possible to establish connect without the client authentication. Data for authentication process are extracted from the WS-Security header.

3.4.2 AMQP

For the trading purpose on IM and BaIM markets, via AMQP server, it is necessary to have both kinds of certificates, it means for qualified digital signature (seal/mark), and commerce (server) certificate for the purpose of TLS authentication.

© 2026 CGI IT Czech Republic s.r.o.