

CS OTE
User Manual for External Users



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

Table of Contents

List of Abbreviations.....	2
1 Introduction	3
2 Terms.....	3
3 Supported authorities.....	3
4 Impacts	5
4.1 Certificate registration in CS OTE	5
4.2 Verification, if replacement of current certificate is necessary	5
4.2.1 Example 1.....	6
4.2.2 Example 2.....	6
4.3 CS OTE web portal	7
4.4 OTE-COM.....	7
4.5 CS OTE Automatic communication.....	7
4.5.1 Web services.....	8
4.5.2 AMQP	8
4.6 Secured email	8
4.6.1 Verification, if replacement of current certificate is necessary	8
5 Appendix 1	10
5.1 The list of trusted authorities that provide qualified certificates	10
6 Appendix 2	15
6.1 The list of trusted authorities that provide commerce certificates.....	15

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
eIDAS	EU regulation on electronic identification and trust services for electronic transactions in the internal market

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. Certificate types and its trustfulness are described in this documentation. The qualified certificates in CS OTE are used in compliance with the statement of the Ministry of Interior - available under the following [link](#).

2 Terms

New changes will be implemented into the CS OTE system effective from 1st July 2017. From this date, registration process will have more strict rules. Current registrations, that had been made before this date (1 July 2017) will stay without change until the end of so-called “transitional period” valid until 30 September 2017. After the transitional period end (from 1 October 2017), new rules for certificate usage will be strictly required. You can find more info at [this link](#).

3 Supported authorities

According to usage, it will be 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 will be possible to use.
- b. Digital signature/mark/seal - only so-called qualified certificates provided by qualified authorities will be possible to use.

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

Authority	Country	Commerce CA (authentication and encryption)	Qualified CA (Digital signature/mark/seal)	Note
První certifikační autorita, a.s.	CZ	Yes – all the commerce certificates	Yes – see Appendix 1 <i>I. CA Qualified 2 CA/RSA 02/2016</i> <i>I. CA - Qualified Certification Authority, 09/2009</i> <i>I. CA - Qualified root certificate</i>	
Česká pošta, s.p.	CZ	Yes – all the commerce certificates	Yes – see Appendix 1 <i>PostSignum Qualified CA</i> <i>PostSignum Qualified CA 2</i> <i>PostSignum Qualified CA 3</i>	
eIdentity a.s.	CZ	Yes – all the commerce certificates	Yes – see Appendix 1 <i>ACAeID2.1 - Qualified Issuing Certificate (kvalifikovaný systémový)</i>	

			<i>certifikát vydávající CA)</i>	
NetLock Ltd	HU	Yes – see Appendix 2 <i>NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó</i> <i>NETLOCK Trust Advanced CA</i>	Yes – see Appendix 1 <i>NetLock Minosített Kozjegyzoi (Class OA)</i> <i>Tanusitvanykiado</i> <i>NetLock Minositett Eat. (Class Q Legal) Tanúsítványkiadó</i> <i>NetLock Minősített Közigazgatási (Class Q) Tanúsítványkiadó</i> <i>NetLock Minősített Eat. Spec. (Class Q Legal Spec.) Kiadó</i>	
GLOBALTRUST	AU	Yes – see Appendix 2 <i>GLOBALTRUST ADVANCED 1</i> <i>GLOBALTRUST CLIENT 1 A-CERT CLIENT (only issued ones)</i> <i>A-CERT ADVANCED (only issued ones)</i>	Yes – see Appendix 1 <i>GLOBALTRUST QUALIFIED 1</i> <i>GLOBALTRUST 2015 QUALIFIED 1</i>	Formerly known as ARGE DATEN
QuoVadis	CH/BE	Yes – see Appendix 2 <i>QuoVadis Swiss Advanced CA G2</i>	Yes – see Appendix 1 <i>QuoVadis Belgium Issuing CA G1</i> <i>QuoVadis Belgium Issuing CA G2</i>	
GeoTrust	US	Yes – see Appendix 2 <i>GeoTrust SSL CA - G3</i>	No	
GoDaddy.com	US	Yes – see Appendix 2 <i>Go Daddy Root Certificate Authority - G2</i>	No	

Table 1: List of commerce and qualified authorities for CS OTE

Authority	Country	Web portal, OTE-COM, AMQP	Web services automatic communication, secure e-mail	Note
První certifikační autorita, a.s.	CZ	Yes	Yes	
Česká pošta, s.p.	CZ	Yes	Yes	
eIdentity a.s.	CZ	Yes	Yes	
NetLock Ltd	HU	Yes	Yes	
GLOBALTRUST	AU	Yes	Yes	Formerly known as ARGE DATEN
QuoVadis	CH/BE	No	Yes	
GeoTrust	US	No	Yes	
GoDaddy.com	US	No	Yes	

Table 2: The list of supported authorities for CS OTE. The usage (authentication, digital signature/mark/seal) is connected to authority type – see Table 1.

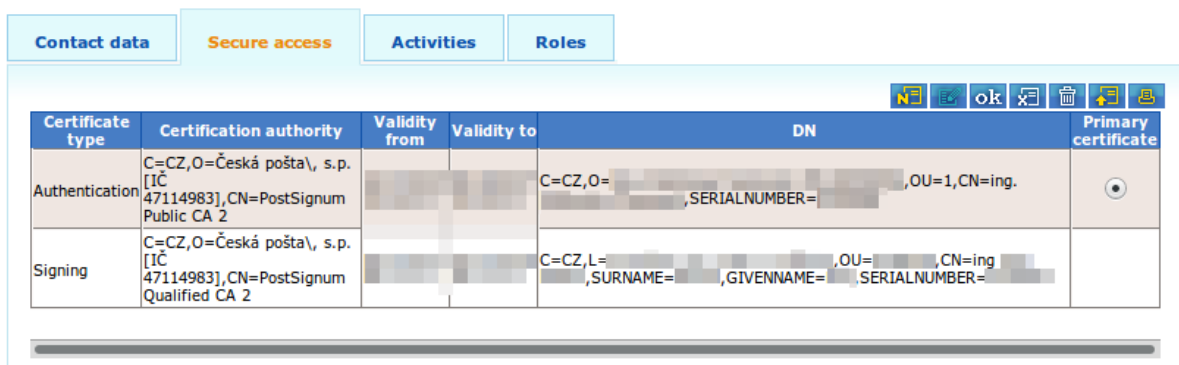
Generation of OTECA certificates for CS OTE system as well as their renewal process will be terminated until 1 May 2017. The usage of OTECA certificate will be allowed during the transitional period only. OTECA certificate won't be possible to use in CS OTE from 1 October 2017.

4 Impacts

4.1 Certificate registration in CS OTE

In CS OTE section “Mater data – Secure access” only appropriate certificates would be able to register:

- „Commerce“ type (Authentication until 1 July 2017) – used for access to OTE-COM application, TLS authentication and e-mail message encryption. At this certificate, provider and type (commerce type) attributes of the certificate will be checked to meet list of supported commerce certificate authority requirements, see *Table 1*.
- „Qualified“ type (Signing until 1 July 2017) – used for the purpose of digital signature, mark or seal. At this certificate, provider and type attributes of the certificate (qualified type) will be checked to meet list of supported qualified certificate authority requirements, see *Appendix 1*.



Certificate type	Certification authority	Validity from	Validity to	DN	Primary certificate
Authentication	C=CZ,O=Česká pošta\, s.p. [IC 47114983],CN=PostSignum Public CA 2			C=CZ,O= ,SERIALNUMBER= ,OU=1,CN=ing.	<input checked="" type="radio"/>
Signing	C=CZ,O=Česká pošta\, s.p. [IC 47114983],CN=PostSignum Qualified CA 2			C=CZ,L= ,SURNAME= ,GIVENNAME= ,SERIALNUMBER=	<input type="radio"/>

Figure 1: Process of certificate registration

If user (or external system) holds only qualified type of certificate, he/she won't register the second one. The relevant field will stay empty in that case from 1 July 2017.

Irrelevant certificates will be automatically removed from CS OTE system in the end of the transitional period. It means that qualified certificates will be deleted from “Commerce” type (originally used as Authentication), and commerce certificates will be deleted from “Qualified” type (originally used as Signing).

4.2 Verification, if replacement of current certificate is necessary

If user's (or external system's) registered certificate in CS OTE system doesn't meet the list of supported certificate authority for appropriate type of certificate, he/she will have to replace this certificate.

Verification process:

1. Login to CS OTE

2. Go to Registration – Master data – Secure Access

Certificate type	Certification authority	Validity from	Validity to	DN	Primary certificate
Authentication	C=CZ,O=Česká pošta, s.p. [IČ 47114983],CN=PostSignum Public CA 2				<input checked="" type="radio"/>
Signing	C=CZ,O=Česká pošta, s.p. [IČ 47114983],CN=PostSignum Qualified CA 2				<input type="radio"/>

- When commerce certificate is not registered for authentication by supported commerce authority (see *Table 1*), it is necessary for user to obtain such a certificate in case of receiving encrypted email messages or using OTE-COM application.
- When qualified certificate is not registered for signing by supported authority (see *Appendix I*), it is necessary for user to obtain such a certificate. It would be necessary to use such a qualified certificate for logging to CS OTE and sign entry logging web form.

4.2.1 Example 1

User has registered only commerce certificate in CS OTE:

Certificate type	Certification authority	Validity from	Validity to	DN	Primary certificate
Authentication	C=CZ,O=Česká pošta, s.p. [IČ 47114983],CN=PostSignum Public CA 2				<input checked="" type="radio"/>
Signing	C=CZ,O=Česká pošta, s.p. [IČ 47114983],CN=PostSignum Public CA 2				<input type="radio"/>

In such a case, user has to obtain qualified certificate for his/her access to CS OTE web portal and for digital signature. You can see Signing type “CN=PostSignum Public CA 2” on the print screen above. This authority is not mentioned in the *Table 1* as supported qualified certification authority and therefore it won’t be possible to use it for digital signature purpose. Certificate will be removed from signing category automatically in the end of transitional period. User will need to obtain new qualified certificate in advance for access and digital signature purpose.

4.2.2 Example 2

User has registered only qualified certificate in CS OTE:

Certificate type	Certification authority	Validity from	Validity to	DN	Primary certificate
Authentication	C=CZ,O=Česká pošta, s.p. [IČ 47114983],CN=PostSignum Qualified CA 2				<input checked="" type="radio"/>
Signing	C=CZ,O=Česká pošta, s.p. [IČ 47114983],CN=PostSignum Qualified CA 2				<input type="radio"/>

You can see Authentication type “CN= PostSignum Qualified CA 2” on the print screen above. This authority is mentioned in the *Table 1* as supported qualified certification authority. Therefore it won’t be possible to use it for access to OTE-COM application and for messages encryption. This certificate will be removed from Authentication category automatically in the end of transitional period. In case

of receiving encrypted e-mails from CS OTE, user will have to obtain the commerce certificate in advance (see *Table 1*).

4.3 CS OTE web portal

After the end of transitional period, all the provided data will have to contain following:

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

Users have to have certificates only issued by the qualified authority (see *Appendix 1*). These certificates should be stored on so-called **software storage** or on qualified equipment, i.e. certified **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. From the beginning of transitional period, **it will be possible to use the certificate also for authentication process, based on digital signature** of entry logging web form.

This rules applies to all CS OTE web portal users; i.e. all contractors, producers, Electricity retailers well as for Guarantees of Origin users.

4.4 OTE-COM

Effective from 1 October 2017, all market users will have to use commerce certificate for their login into OTE-COM application. In this particular case, there will be no change in certificate usage. There are the same rules for data digital signature as for web portal; it means that, effective from 1 October 2017, all the data must be signed only by qualified certificate (see *Table 1*), 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.

4.5 CS OTE Automatic communication

Effective from 1 July 2017, until further notice, only qualified system certificates would be 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 will be available for electronic seals from supported certificate authorities. These seals will replace system certificates. Effective from 1 October 2017, it won't be possible to use the commerce certificates for electronic mark creation (automated signature).

Effective from 30 September 2017, all provided data to CSOTE from market participants, automatically marked or sealed will have to 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

Registration of such certificate types is allowed already now in CS OTE system.

Some data types won't be able to electronically mark (or to seal) and neither sends them via this automatic communication channel. After the transitional period end, it will be 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

4.5.1 Web services

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

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

4.5.2 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.

4.6 Secured email

All the e-mail messages sent to CS OTE will have to contain digital signature, mark or seal generated by qualified certificate (the same as for web portal or automatic communication).

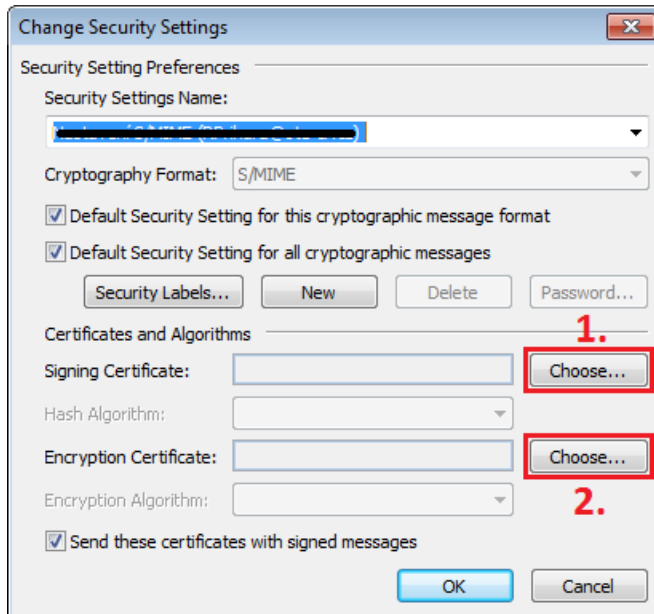
In case of receiving secure emails from CS OTE, it's necessary to have registered commerce certificate registered in CS OTE (“Authentication” type – see Certificate registration).

4.6.1 Verification, if replacement of current certificate is necessary

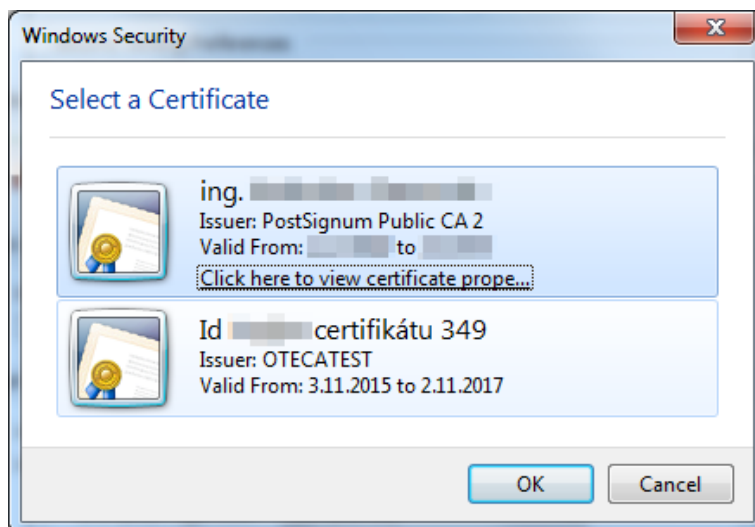
It is necessary to check certificate registration status at “Secured access” section, see *Verification, if replacement of current certificate is necessary*.

4.6.1.1 MS Outlook 2010 example

- In e-mail client, search for setting of encrypting and signing as described here <http://www.ote-cr.cz/registration-and-agreements/access-to-cs-ote/files-pc-configuration/d4-instalace-ms-outlook-2010-settings-en.pdf>



- Press button Choose at “Signing Certificate” section. It is necessary to choose certificate that is provided by one of certificate authorities, see *Chyba! Nenalezen zdroj odkazů.*



- If user doesn't have such a certificate, he/she has to obtain one from one of supported qualified certificate authorities – see *Chyba! Nenalezen zdroj odkazů.*

5 Appendix 1

5.1 The list of trusted authorities that provide qualified certificates

Below, find the list of EU trustworthy services providers:

https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

Czech Republic

https://tsl.gov.cz/publ/TSL_CZ.pdf - below mentioned list is based on the document that is valid until 3 May 2017, 14:00:00.

První certifikační autorita, a.s.

Below, find identification of valid certificate authorities that are able to provide certificates for qualified signature, mark and seal.

I.CA Qualified 2 CA/RSA 02/2016

Subject Key Identifier

74:82:08:91:E3:D9:64:68:71:85:D6:EB:31:E4:72:DF:8B:26:B1:6D

Thumbprint algorithm: SHA-256

Thumbprint:

07:6A:BC:22:69:32:7E:EF:50:0A:0C:57:52:72:62:BA:C8:31:F9:D2:DF:4E:F2
:D4:39:E7:4C:E1:70:36:AA:3A

I.CA - Qualified Certification Authority, 09/2009

Subject Key Identifier

79:CB:D0:23:E9:3A:67:70:91:74:4F:D3:51:E2:E0:20:FD:E1:28:FB

Thumbprint algorithm: SHA-256

Thumbprint:

C0:C0:5A:8D:8D:A5:5E:AF:27:AA:9B:91:0B:0A:6E:F0:D8:BB:DE:D3:46:92:8D
:B8:72:E1:82:C2:07:3E:98:02

I.CA - Qualified root certificate

Subject Key Identifier

68:9D:7E:D6:C4:25:39:FB:3B:A0:37:D6:4F:DC:8C:D1:7A:F0:56:59

Thumbprint algorithm: SHA-256

Thumbprint:

1A:A9:80:C8:C0:D3:16:F2:50:29:97:89:82:F0:33:CB:B3:A3:F4:18:8D:66:9F
:2D:E6:A8:D8:4E:E0:0A:15:75

Česká pošta, s.p.

Below, find identification of valid certificate authorities that are able to provide certificates for qualified signature, mark and seal.

PostSignum Qualified CA

Subject Key Identifier

A7:9F:B6:8E:89:93:9A:65:76:09:9A:95:F8:44:7E:69:82:6A:DE:0B

Thumbprint algorithm: SHA-256

Thumbprint:

6E:79:23:E2:86:CF:C4:A7:90:37:CF:C9:12:5E:1C:66:71:88:7B:1A:A5:E3:67
:3A:F9:8F:38:A4:67:DF:96:C3

PostSignum Qualified CA 2

Subject Key Identifier

89:E8:4C:DF:8B:26:39:3E:D7:24:2E:12:0E:7A:E7:E6:27:E5:D6:97

Thumbprint algorithm: SHA-256

Thumbprint:

3A:E4:F4:DE:5F:3E:20:70:A1:18:45:BD:FE:6D:CA:6E:41:2B:B7:E4:ED:84:FD
:4F:1B:7B:49:6C:AD:FF:2C:AC

PostSignum Qualified CA 3

Subject Key Identifier

F2:F8:CC:2A:57:61:DA:2B:17:33:59:E5:82:2D:EC:06:1C:8A:4F:4A

Thumbprint algorithm: SHA-256

Thumbprint:

D3:5E:25:0C:B0:2E:27:BB:3F:C5:2D:1F:1A:0D:FD:88:FA:98:13:BE:1B:77:73
:20:AA:E9:12:B5:4E:3B:1F:02

eIdentity a.s.

Below, find identification of valid certificate authorities that are able to provide certificates for qualified signature, mark and seal.

ACAeID2.1 - Qualified Issuing Certificate (kvalifikovaný systémový certifikát vydávající CA)

Subject Key Identifier

6C:54:CE:76:96:5E:D3:B0:29:EB:47:75:B6:EF:BE:BD:8F:22:2F:38

Thumbprint algorithm: SHA-256

Thumbprint:

CA:A0:25:8C:B1:98:42:17:CF:52:D6:64:DA:A7:C9:F6:87:92:F1:96:37:E6:3C
:59:F5:32:45:D2:1B:6D:6A:2E

Hungary

http://www.nmhh.hu/tl/pub/HU_TL.pdf - below mentioned list is based on the document that released on 3 May 2017, 14:00:00. Only authority that was verified in CS OTE was chosen.

NetLock Ltd.

Below, find identification of valid certificate authorities that are able to provide certificates for qualified signature, mark and seal.

NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado

Subject key identifier:

09:6A:62:16:92:B0:5A:BB:55:0E:CB:75:32:3A:32:E5:B2:21:C9:28

Thumbprint algorithm: SHA-256

Thumbprint:

E6:06:DD:EE:E2:EE:7F:5C:DE:F5:D9:05:8F:F8:B7:D0:A9:F0:42:87:7F:6A:17
:1E:D8:FF:69:60:E4:CC:5E:A5

NetLock Minositett Eat. (Class Q Legal) Tanusitvanykiado

Subject key identifier:

64:AF:81:8A:5C:30:B8:57:65:DA:5D:A5:3D:58:6E:47:62:42:34:AB

Thumbprint algorithm: SHA-256

Thumbprint:

62:84:A0:3B:AF:AE:86:1A:30:E3:A2:5A:03:04:28:30:6F:7E:B5:2B:D0:BA:57
:7A:1D:96:2A:80:9A:83:0C:9E

NetLock Minositett Kozigazgatasi (Class Q) Tanusitvanykiado

Subject key identifier:

D4:92:31:4D:32:8B:A9:51:09:12:89:53:6B:72:EA:AF:19:B4:AC:6D

Thumbprint algorithm: SHA-256

Thumbprint:

EB:A2:27:84:D2:09:02:A9:F9:AF:3F:64:0D:14:88:9A:53:D7:F3:C4:B5:B0:69
:70:16:B8:D7:49:AD:E9:7F:3E

NetLock Minősített Eat. Spec. (Class Q Legal Spec.) Kiadó

Subject key identifier:

25:6A:74:5B:55:2B:BA:7F:6F:AB:1E:8B:28:D8:E8:E8:5B:BE:AD:C2

Thumbprint algorithm: SHA-256

Thumbprint:

A5:F2:FD:0D:66:DB:4D:D7:7A:29:14:ED:3C:74:7C:BD:97:E7:34:CF:4E:2B:6F
:21:7F:B4:1A:A4:EA:FD:EA:D2

Austria

<https://www.signatur.rtr.at/currenttl.xml> - below mentioned list is based on the document that released on 19 January 2017 02:00:00 CET and is valid until 3 May 2017, 14:00:00. Only authority that was verified in CS OTE was chosen.

GLOBALTRUST

Below, find identification of valid certificate authorities that are able to provide certificates for qualified signature, mark and seal.

GLOBALTRUST QUALIFIED 1

Subject key identifier:

23:BD:9C:59:A4:B9:33:BF:75:44:DD:D0:14:43:84:D6:2C:10:78:A0

Thumbprint algorithm: SHA-256

Thumbprint:

AF:9F:3B:CE:85:77:9A:95:C5:6B:4E:4D:90:CD:BB:F8:D4:21:5B:9D:D5:B3:6C
:79:EA:80:B0:5D:A9:22:B1:B3

GLOBALTRUST 2015 QUALIFIED 1

Subject key identifier:

D6:57:61:0B:76:2E:66:75:3C:91:F6:B3:56:A0:45:65:6F:08:DC:A7

Thumbprint algorithm: SHA-256

Thumbprint:

01:2E:7F:A6:27:D3:AB:6E:D0:04:96:A8:BD:3C:7A:35:B7:A1:95:AB:E1:3E:45
:D9:53:63:FA:85:AC:F2:45:C4

Belgium

<https://tsl.belgium.be/tsl-be.xml> - below mentioned list is based on the document that released on 16 February 2017 02:00:00 CET and is valid until 13 August 2017 02:00:00 CEST. Only authority that was used for automatic communication in CS OTE was chosen.

QuoVadis

Below, find identification of valid certificate authorities that are able to provide certificates for qualified signature, mark and seal.

QuoVadis Belgium Issuing CA G1

Subject key identifier:

F8:0F:65:1C:7A:63:19:AA:BF:44:6F:A6:49:12:21:F3:7A:5D:E3:0D

Thumbprint algorithm: SHA-256

Thumbprint:

27:EB:AC:D8:6D:D3:BF:86:14:3D:A4:34:28:61:03:1A:57:CF:3F:A4:14:D4:0A
:86:E6:69:C3:F4:F1:D8:CF:24

QuoVadis Belgium Issuing CA G2

Subject key identifier:

87:C9:BC:31:97:12:7A:73:BB:7E:C0:3D:45:51:B4:01:25:95:51:AB

Thumbprint algorithm: SHA-256

Thumbprint:

D9:0B:40:13:23:06:D1:09:46:08:B1:B9:A2:F6:A9:E2:3B:45:FE:12:1F:EF:51
:4A:1C:9D:F7:0A:81:5A:D9:5C

6 Appendix 2

6.1 The list of trusted authorities that provide commerce certificates

První certifikační autorita, a.s.

All commerce certificates.

Česká pošta, s.p.

All commerce certificates.

eIdentity a.s.

All commerce certificates.

NetLock Ltd.

Below, find identification of valid certificate authorities that are able to provide commerce certificates for data authentication and encryption.

NetLock Ůzleti Eat. (Class B Legal) Tanúsítványkiadó

Subject key identifier:

34:1B:2C:C7:B2:3E:4A:72:53:3D:12:7F:40:66:BA:AE:B6:A4:E4:47

Thumbprint algorithm: SHA-256

Thumbprint:

1D:93:68:6C:A4:2C:70:39:4F:BD:C2:BC:1F:98:46:1D:19:87:1C:2A:00:07:8B
:81:54:99:31:2E:D9:F6:FE:0C

NETLOCK Trust Advanced CA

Subject key identifier:

6A:9D:0B:F8:8A:64:C8:7A:0E:25:64:BF:B0:3E:61:B8:1B:FF:BC:80

Thumbprint algorithm: SHA-256

Thumbprint:

D8:2F:87:F9:3D:31:D5:FC:81:8D:D6:6B:D5:0E:7F:31:9A:E1:79:FC:1C:5D:00
:54:7B:65:8E:8E:B3:F4:CE:56

GLOBALTRUST

Below, find identification of valid certificate authorities that are able to provide commerce certificates for data authentication and encryption.

GLOBALTRUST ADVANCED 1

Subject key identifier:

0C:02:A1:34:DD:A4:EF:EB:58:91:A6:AE:12:B7:99:69:11:AF:52:44

Thumbprint algorithm: SHA-256

Thumbprint:

D6:D2:44:74:2E:8F:C5:64:5B:15:01:0F:1C:D5:92:08:F7:A6:3E:3B:F1:00:08
:3E:14:6F:18:29:41:A6:1D:98

GLOBALTRUST CLIENT 1

Subject key identifier:

D3:E9:EA:AA:F8:CB:AD:3B:74:CB:E6:82:DC:B9:E4:F2:09:77:35:E9

Thumbprint algorithm: SHA-256

Thumbprint:

08:A0:FD:0A:B6:36:9E:E9:61:91:C1:C2:46:B7:99:71:A3:DB:5C:5F:2C:FC:6C
:4C:5C:D6:8C:DF:EB:BE:0E:73

A-CERT CLIENT

Temporary – until valid certificates expiration only (September 2019).

Subject key identifier:

52:33:10:F8:80:A8:98:5F:EE:4E:9C:81:0D:5B:F3:0F:D1:DC:33:97

Thumbprint algorithm: SHA-256

Thumbprint:

A7:B0:32:0F:B5:BE:AC:FD:A3:09:D8:7F:93:09:6C:27:F7:21:4F:1E:FE:0A:8D
:AF:5C:DD:65:86:7E:2E:AB:74

A-CERT ADVANCED

Temporary – until valid certificates expiration only (September 2019).

Subject key identifier:

3B:38:E2:2B:0F:E9:69:91:54:89:6F:68:2F:BE:66:5C:5D:E7:8E:82

Thumbprint algorithm: SHA-256

Thumbprint:

98:3C:25:2C:6F:75:90:CD:37:B9:10:C7:DF:34:F3:8D:38:75:49:4C:B8:F0:88
:54:09:44:B3:C5:52:BC:07:93

QuoVadis

Below, find identification of valid certificate authorities that are able to provide commerce certificates for data authentication and encryption.

QuoVadis Swiss Advanced CA G2

Subject key identifier:

A0:20:6D:6D:49:5D:BA:4A:85:D3:77:20:B2:7A:B8:8B:0E:ED:D5:9D

Thumbprint algorithm: SHA-256

Thumbprint:

50:44:F6:5E:10:42:CD:38:0B:0B:99:97:E4:28:33:58:F0:DE:EF:78:73:DA:72
:EF:DB:6F:02:47:4A:E3:7E:BE

GeoTrust

Below, find identification of valid certificate authorities that are able to provide commerce certificates for data authentication and encryption.

GeoTrust SSL CA - G3

Subject key identifier:

D2:6F:F7:96:F4:85:3F:72:3C:30:7D:23:DA:85:78:9B:A3:7C:5A:7C

Thumbprint algorithm: SHA-256

Thumbprint:

07:45:41:EC:DF:88:ED:99:2E:D5:AD:E3:EC:DD:EF:27:A2:6B:A1:B4:44:80:A1
:95:C0:A8:DA:DA:E2:52:1D:8E

GoDaddy.com

Below, find identification of valid certificate authorities that are able to provide commerce certificates for data authentication and encryption.

Go Daddy Root Certificate Authority - G2

Subject key identifier:

3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE

Thumbprint algorithm: SHA-256

Thumbprint:

3A:2F:BE:92:89:1E:57:FE:05:D5:70:87:F4:8E:73:0F:17:E5:A5:F5:3E:F4:03
:D6:18:E5:B7:4D:7A:7E:6E:CB