User manual
Of information System

User manual

for external users - Certification authority verification

This document and its content are confidential. It is forbidden to reproduce the document or its parts, to show it to third parties or to use it for any other purposes than it was provided for without prior written agreement by OTE, a.s.

Revize dne:
27.10.2023

Document name:
User manual - Certification authority verification
OTE

Date	Description of changes
27.10.2023	Description of categories for certificate application

1 Specification for a qualified certificate for access to CS-OTE 3

1.1 eIDAS 3

1.2 Verification of eIDAS approval status 3

1.3 Evaluation of conditions 5

2 Access to CS-OTE portal and OTE-COM 6

2.1 Certificate for access to the CS-OTE portal 6

2.2 Certificate for access to the OTE-COM application... 6

2.3 Detailed description.. 6

1 Specification for a qualified certificate for access to CS-OTE

When requesting the inclusion of an authority in the list of trusted qualified authorities of CS OTE, it is necessary that the certificate of the authority has the required identification of the service for issuing certificates enabling qualified electronic signature or seal according to eIDAS Regulation EU No 910/2014.

The URI identifying this service is http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures. Alternatively, http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals for creating electronic seals.

1.1 eIDAS

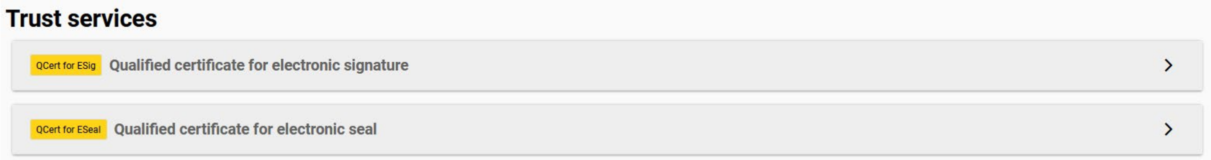
The following link shows a list of approved eIDAS certification authorities for each country: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

When you click on the details of a specific CA, you can see the individual categories.

The authority for a qualified user certificate must be in the following categories:

Qualified certificate for electronic signature

Qualified certificate for electronic seal



Trust services

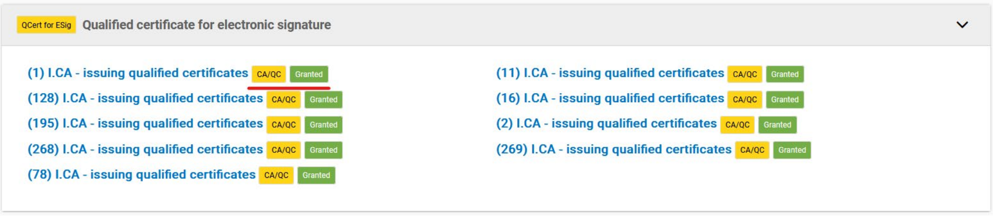
QCert for ESig Qualified certificate for electronic signature

QCert for ESeal Qualified certificate for electronic seal

Pic. 1 – Certificate Categories

1.2 Verification of eIDAS approval status

1. After expanding the category Qualified certificate for electronic signature or Qualified certificate for electronic seal, we see a list of certificate types, where we look for the yellow label "CA/QC" and the green label "Granted".



QCert for ESig Qualified certificate for electronic signature

(1) I.CA - issuing qualified certificates CA/QC Granted
(128) I.CA - issuing qualified certificates CA/QC Granted
(195) I.CA - issuing qualified certificates CA/QC Granted
(268) I.CA - issuing qualified certificates CA/QC Granted
(78) I.CA - issuing qualified certificates CA/QC Granted
(11) I.CA - issuing qualified certificates CA/QC Granted
(16) I.CA - issuing qualified certificates CA/QC Granted
(2) I.CA - issuing qualified certificates CA/QC Granted
(269) I.CA - issuing qualified certificates CA/QC Granted

Pic. 2 – Valid certificate marking

2. When you click on a certificate, you can verify it as follows:

   Type identifier:

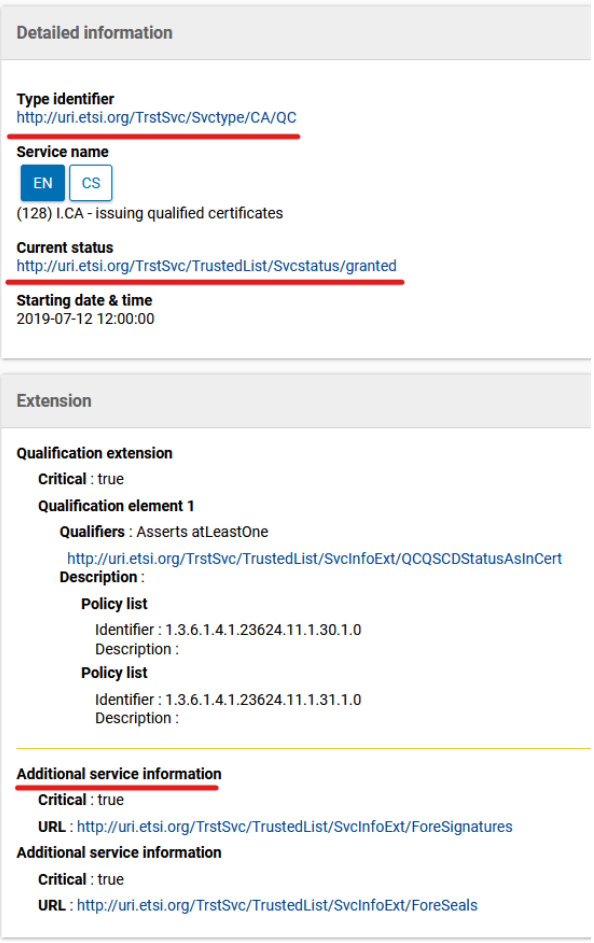
   http://uri.etsi.org/TrstSvc/Svctype/CA/QC

   Current status:

   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

   Extension:

   - For signature certificate - electronic signature http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
   - For creating electronic seals - electronic seal http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals



Detailed information

Type identifier
http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service name

(128) I.CA - issuing qualified certificates

Current status
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Starting date & time
2019-07-12 12:00:00

Extension

Qualification extension
Critical : true
Qualification element 1
Qualifiers : Asserts atLeastOne
http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert
Description :
Policy list
Identifier : 1.3.6.1.4.1.23624.11.1.30.1.0
Description :
Policy list
Identifier : 1.3.6.1.4.1.23624.11.1.31.1.0
Description :

Additional service information
Critical : true
URL : http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
Additional service information
Critical : true
URL : http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

Pic 3. – Detail of the certificate

1.3 Evaluation of conditions

It is necessary that the certification authority meet these conditions; the mere presence on the list of CAs without a specific certificate type designation of "CA/QC" and "Granted" is not sufficient.

If the given certificate meets all the conditions according to EIDAS, it is possible to apply for the given type of certificate at the certification authority for the purpose of access to CS-OTE.

2 Access to CS-OTE portal and OTE-COM

2.1 Certificate for access to the CS-OTE portal

To access the CS OTE portal, it is necessary to have a qualified certificate for electronic signature issued by a certification authority that meets the relevant conditions under the eIDAS Regulation. The certificate is then used in the system exclusively for electronic signature.

The verification method can be found in chapter 1.

2.2 Certificate for access to the OTE-COM application

For access to the OTE-COM application, a commercial certificate is used only to verify the user's identity.

It is no longer necessary for the authority in question to meet the eIDAS conditions, but it must be listed on the list of trusted authorities of the OTE information system.

2.3 Detailed description

Here you can find details on how to identify each certificate:

OTE - Business Partners - Change in certificates switching to qualified certificates in CS OTE