

**Uživatelská příručka
informačního systému**



**Uživatelský manuál
pro externí uživatele – Ověření certifikační autority**

Tento dokument a jeho obsah je důvěrný. Dokument nesmí být reprodukován celý ani částečně, ani ukazován třetím stranám nebo používán k jiným účelům, než pro jaké byl poskytnut, bez předchozího písemného schválení společností OTE, a.s.

2023 OTE, a.s.

Revize dne:
27.10.2023

Název dokumentu:
Uživatelský manuál Ověření
certifikační autority
OTE

Datum	Popis změny
27.10.2023	Popis kategorií pro žádost o certifikát

Obsah

1	Specifikace pro kvalifikovaný certifikát pro přístup do CS-OTE.....	3
1.1	<i>eIDAS.....</i>	3
1.2	<i>Ověření statusu schválení eIDAS.....</i>	3
1.3	<i>Vyhodnocení podmínek.....</i>	5
2	Přístup do CS-OTE portálu a OTE-COM	6
2.1	<i>Certifikát pro přístup do CS-OTE portálu.....</i>	6
2.2	<i>Certifikát pro přístup do aplikace OTE-COM.....</i>	6
2.3	<i>Detailní popis</i>	6

1 Specifikace pro kvalifikovaný certifikát pro přístup do CS-OTE

Při žádosti o zařazení autority do seznamu důvěryhodných kvalifikovaných autorit CS OTE je nutné, aby certifikát autority měl dle eIDAS nařízení EU č. 910/2014 požadovanou identifikaci služby pro vydávání certifikátů umožňujících kvalifikovaný elektronický podpis anebo pečeť.

URI identifikace této služby je <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>. Případně <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals> pro vytváření elektronických pečeti.

1.1 eIDAS

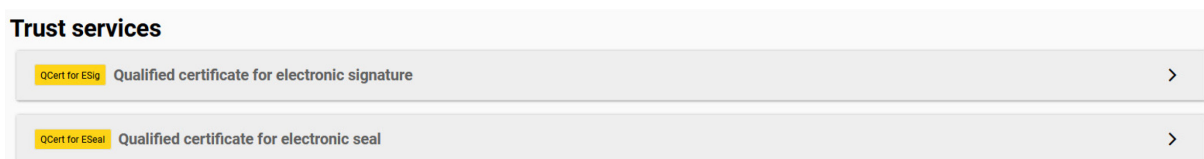
Na následujícím odkazu je možno zobrazit seznam schválených certifikačních autorit dle eIDAS pro jednotlivé země: <https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home>

Po rozkliknutí detailu konkrétní certifikační autority lze vidět jednotlivé kategorie.

Autorita pro kvalifikovaný uživatelský certifikát musí být v následujících kategoriích:

Qualified certificate for electronic signature

Qualified certificate for electronic seal



Obr. 1 – Kategorie certifikátů

1.2 Ověření statusu schválení eIDAS

1. Po rozbalení kategorie **Qualified certificate for electronic signature** nebo **Qualified certificate for electronic seal** vidíme seznam typů certifikátů, kde hledáme žluté označení “CA/QC” a zároveň zelené označení “Granted”.



Obr. 2 – Označení validního certifikátu

2023 OTE, a.s.

Revize dne:
27.10.2023

Název dokumentu:
Uživatelský manuál Ověření
certifikační autority
OTE

2. Při rozkliknutí daného certifikátu lze ověřit dle následujícího:

Type identifier:

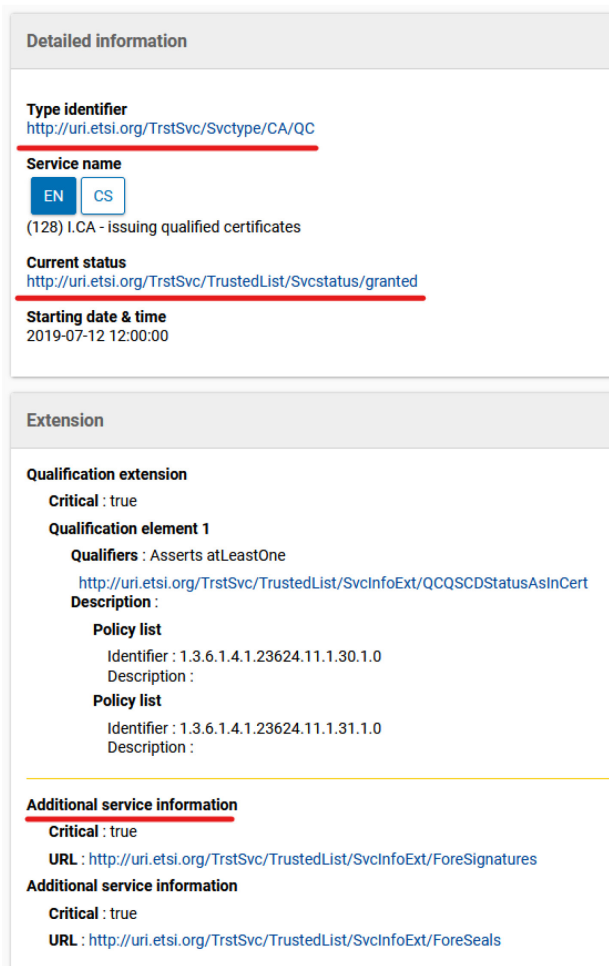
<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Current status:

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

Extension:

- Pro podpisový certifikát – elektronický podpis
<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>
- Pro vytváření elektronických pečeti – elektronická pečeť
<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>



The screenshot displays the details of a certificate. It is divided into two main sections: 'Detailed information' and 'Extension'.

Detailed information:

- Type identifier:** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>
- Service name:** EN CS (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
 - Description:** <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQCSDStatusAsInCert>
 - 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>

Obr 3. – Detail certifikátu

2023 OTE, a.s.

Revize dne:
27.10.2023

Název dokumentu:
Uživatelský manuál Ověření
certifikační autority
OTE

1.3 Vyhodnocení podmínek

Je nutné, aby certifikační autorita splňovala tyto podmínky, pouhá přítomnost na seznamu autorit bez označení konkrétního typu certifikátu “CA/QC” a “Granted” není dostačující.

V případě, že daný certifikát splňuje všechny dané podmínky dle EIDAS je možno si o daný typ certifikátu zažádat u certifikační autority pro potřeby přístupu do CS-OTE.

2 Přístup do CS-OTE portálu a OTE-COM

2.1 Certifikát pro přístup do CS-OTE portálu

Pro přístup do CS OTE portálu je nutné mít kvalifikovaný certifikát pro elektronický podpis vydaný certifikační autoritou, která splňuje příslušné podmínky dle nařízení eIDAS. Certifikát je pak v systému používán výhradně pro elektronický podpis.

Způsob ověření naleznete v kapitole 1.

2.2 Certifikát pro přístup do aplikace OTE-COM

Pro přístup do aplikace OTE-COM se využívá komerční certifikát, a to pouze pro ověření identity uživatele.

Již není nutné, aby příslušná autorita splňovala podmínky eIDAS, ale musí být uveden na seznamu důvěryhodných autorit informačního systému OTE.

2.3 Detailní popis

Zde lze nalézt detaily k určení jednotlivých certifikátů

[OTE - Smluvní partneři - Změna v certifikátech přechod na kvalifikované certifikáty v CS OTE](#)