CS OTE

Dokumentace pro externí uživatele

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

Obsah

Použité zkratky 2
1 Úvod 3
2 Termíny 3
3 Podporované autority 3
4 Dopady 5
4.1 Registrace certifikátů v CS OTE 5
4.2 Ověření nutnosti nového certifikátu 5
4.2.1 Příklad 1 6
4.2.2 Příklad 2 6
4.3 Webový portál CS OTE 7
4.4 OTE-COM 7
4.5 Automatická komunikace CS OTE 7
4.5.1 Webové služby 8
4.5.2 AMQP 8
4.6 Zabezpečený email 8
4.6.1 Ověření nutnosti nového typu certifikátu 8
5 Příloha 1 10
5.1 Seznam důvěryhodných autorit vydávající kvalifikované certifikáty 10
6 Příloha 2 15
6.1 Seznam důvěryhodných autorit vydávající komerční certifikáty 15

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

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. Používání kvalifikovaných certifikátů v CS OTE respektuje stanovisko ministerstva vnitra, které je dostupné – zde.

2 Termíny

Nové úpravy budou implementovány do systému CS OTE s platností od 1.7.2017. Od tohoto data bude systém vyžadovat při registraci certifikátů striktnější pravidla popsaná níže. Stávající registrace budou fungovat beze změny a to až do konce přechodného období 30.9.2017. Po skončení této doby od 1.10.2017 bude striktně vyžadováno využití nově uváděných pravidel pro certifikáty. Více informací je uvedeno ve zprávě na webových stránkách OTE.

3 Podporované autority

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

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

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

Autorita	Země	Komerční CA (autentizace a šifrování)	Kvalifikovaná CA (pouze el. podpis/značka/pečeť)	Pozn.
První certifikační autorita, a.s.	CZ	Ano – všechny komerční certifikáty	Ano – viz Příloha 1 I.CA Qualified 2 CA/RSA 02/2016 I.CA - Qualified Certification Authority, 09/2009 I.CA - Qualified root certificate	
Česká pošta, s.p.	CZ	Ano – všechny komerční certifikáty	Ano – viz Příloha 1 *PostSignum Qualified CA* *PostSignum Qualified CA 2* *PostSignum Qualified CA 3*	
eIdentity a.s.	CZ	Ano – všechny komerční certifikáty	Ano – viz Příloha 1 *ACAeID2.1 - Qualified Issuing Certificate (kvalifikovaný systémový certifikát vydávající*	

			CA)	
NetLock Ltd	HU	Ano – viz Příloha 2 *NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó* *NETLOCK Trust Advanced CA*	Ano – viz Příloha 1 *NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado* *NetLock Minősített Eat. (Class Q Legal) Tanúsítványkiadó* *NetLock Minősített Közigazgatási (Class Q) Tanúsítványkiadó* *NetLock Minősített Eat. Spec. (Class Q Legal Spec.) Kiadó*	
GLOBALTRUST	AU	Ano – viz Příloha 2 *GLOBALTRUST ADVANCED 1* *GLOBALTRUST CLIENT 1* *A-CERT CLIENT (jen stávající)* *A-CERT ADVANCED (jen stávající)*	Ano – viz Příloha 1 *GLOBALTRUST QUALIFIED 1* *GLOBALTRUST 2015 QUALIFIED 1*	Dříve ARGE DATEN
QuoVadis	CH/BE	Ano – viz Příloha 2 *QuoVadis Swiss Advanced CA G2*	Ano – viz Příloha 1 *QuoVadis Belgium Issuing CA G1* *QuoVadis Belgium Issuing CA G2*	
GeoTrust	US	Ano – viz Příloha 2 *GeoTrust SSL CA - G3*	Ne	
GoDaddy.com	US	Ano – viz Příloha 2 *Go Daddy Root Certificate Authority - G2*	Ne	

Tabulka 1 – Seznam podporovaných důvěryhodných autorit pro CS OTE s rozdělením na komerční a kvalifikované autority

Autorita	Země	Webový portál, OTE-COM, AMQP	Automatická komunikace pomocí webových služeb, zabezpečený e-mail	Pozn.
První certifikační autorita, a.s.	CZ	Ano	Ano	
Česká pošta, s.p.	CZ	Ano	Ano	
eIdentity a.s.	CZ	Ano	Ano	
NetLock Ltd	HU	Ano	Ano	
GLOBALTRUST	AU	Ano	Ano	Dříve ARGE DATEN
QuoVadis	CH/BE	Ne	Ano	
GeoTrust	US	Ne	Ano	
GoDaddy.com	US	Ne	Ano	

Tabulka 2 – Seznam důvěryhodných podporovaných autorit pro CS OTE s rozdělením dle oblasti CS OTE. Účel použití (autentizace, šifrování, el. podpis/značka/pečeť) závisí na typu autority viz Tabulka 1.

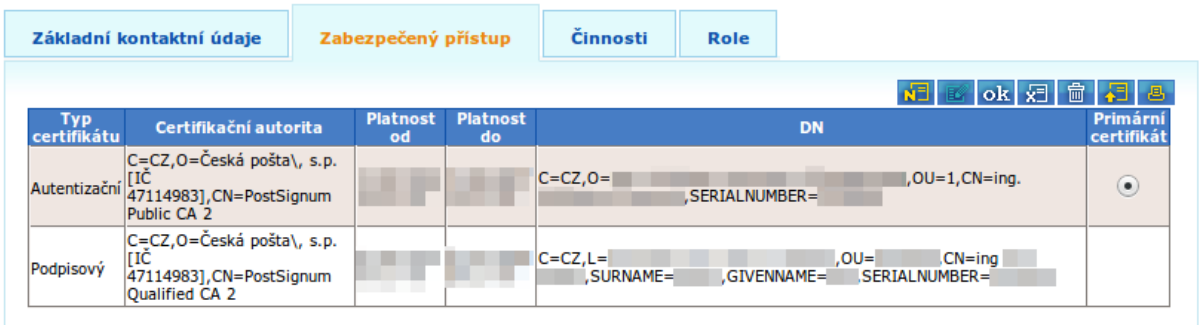
Vydávání certifikátů OTECA pro přístup do CS OTE včetně obnovy certifikátů bude ukončeno k 1.5.2017. Používání certifikátů OTECA bude umožněno ještě během přechodného období. Od 1.10.2017 nebude použití certifikátu OTECA v CS OTE umožněno.

4 Dopady

4.1 Registrace certifikátů v CS OTE

V CS OTE v části Kmenová data – zabezpečený přístup bude možné registrovat pouze odpovídající certifikáty:

- Typ „Komerční“ (do 1.7. 2017 Autentizační) – slouží pro účely přístupu OTE-COM, TLS autentizace a šifrování e-mailových zpráv. U tohoto certifikátu bude kontrolován vydavatel a typ certifikátu (komerční), který musí být ze seznamu podporovaných komerčních certifikačních autorit dle Tabulka **1.**
- Typ „Kvalifikovaný“ (do 1.7.2017 Podpisový) – slouží pro účely elektronického podpisu, značky nebo pečetě. U tohoto certifikátu bude kontrolován vydavatel a typ certifikátu (kvalifikovaný), který musí být ze seznamu podporovaných kvalifikovaných certifikačních autorit uvedených v části Příloha 1.



Obrázek 1 – Registrace certifikátů v CS OTE

Pokud bude uživatel (nebo externí systém) disponovat pouze kvalifikovaným certifikátem, nebude druhý typ certifikátu nutné do CS OTE registrovat (příslušné pole zůstane od 1.7.2017 prázdné).

Na konci přechodného období budou nerelevantní certifikáty automaticky odregistrovány, tedy z položky „Komerční“ (dříve Autentizační) budou odebrány všechny kvalifikované, z položky „Kvalifikovaný“ (dříve Podpisový) všechny komerční certifikáty.

4.2 Ověření nutnosti nového certifikátu

Pokud uživatel (nebo systém) nebude mít registrován certifikát od podporované autority pro příslušný typ certifikátu, bude nutné, aby si jej vyměnil, resp. pořídit si certifikát nový.

Postup pro ověření:

1. Přihlášení do CS OTE portálu
2. Zobrazení detailu registrace certifikátů pro osobu (systém) v části Registrace/Kmenová data, záložka „Zabezpečený přístup“

3. Pokud není registrován komerční certifikát viz Tabulka **1** je nutné, aby si uživatel zajistil takový certifikát v případě, že uživatel (systém) bude požadovat **příjem šifrovaných e-mailových zpráv nebo se přihlašovat do aplikace OTE-COM**.
4. Pokud není registrován kvalifikovaný certifikát od podporované autority viz Příloha 1 je nutné si zajistit kvalifikovaný certifikát, který bude nutné využít pro přihlášení do CS OTE portálu pomocí přihlašovacího formuláře pro kvalifikované certifikáty.

4.2.1 Příklad 1

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. V příkladu je v řádku Podpisový uvedena autorita s CN=PostSignum Public CA 2. Tato certifikační autorita není uvedena v Tabulce 1 jako kvalifikovaná CA, a certifikát nebude možné používat pro elektronický podpis. Bude z kategorie Podpisový automaticky odebrán na konci přechodného období. Je nutné si v předstihu zajistit certifikát kvalifikovaný.

4.2.2 Příklad 2

Uživatel má v CS OTE registrován pouze kvalifikovaný certifikát:

V řádku Autentizační je uvedena autorita s CN= PostSignum Qualified CA 2. Tato autorita je uvedena v Tabulce 1 jako kvalifikovaná, a certifikát nebude možné používat pro přístup do aplikace OTE-COM a k šifrování zpráv. Bude z kategorie Autentizační automaticky odebrán na konci přechodného období. Pokud bude uživatel chtít přijímat šifrované emaily z CS OTE anebo se přihlašovat do aplikace OTE-COM, tak si musí předtím zajistit jeden z komerčních certifikátů viz Tabulka **1**.

4.3 Webový portál CS OTE

Veškerá zadávaná data budou muset být po konci přechodného období 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 Příloha 1 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 Podpisový. Toto může provést uživatel pro svou registraci nebo administrátor společnosti s rolí „Správa vlastních údajů“ pro všechny uživatele v rámci společnosti. Od začátku přechodného období **bude možné certifikát využívat i pro autentizaci založenou na elektronickém podpisu** srozumitelného textu na novém přihlašovacím formuláři.

Tento požadavek platí pro všechny uživatele CS OTE portálu, tedy smluvní partnery, výrobce, povinně vykupující i pro uživatele evidence záruk původu.

4.4 OTE-COM

Pro **aplikaci OTECOM** bude muset účastník trhu pro přihlášení k aplikaci použít komerční certifikát od 1.10.2017, který uživatel používá jako za současného stavu. Pro elektronický podpis dat platí stejná pravidla jako v případě webového portálu, tzn. veškerá data musí být od 1. 10. 2017 podepsána pouze kvalifikovaným certifikátem, viz Tabulka 1 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 vlastních údajů“ pro všechny uživatele v rámci společnosti.

4.5 Automatická komunikace CS OTE

Pro elektronický podpis **v automatické komunikaci** (vytváření elektronické značky) bude možné od 1.7.2017 až do odvolání registrovat pouze kvalifikované systémové certifikáty a to až do doby, kdy budou dostupné kvalifikované certifikáty pro elektronické pečetě, které tyto systémové certifikáty nahradí. Od 1.10.2017 nebude možné použít komerční certifikáty k vytváření elektronické značky (automatizovanému podpisu).

Každý subjekt zasílající automatizovaně značená nebo pečetěná data do CS OTE bude muset mít nejpozději do 30.9.2017 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

Registraci těchto typů certifikátů je možné v systému CS OTE provádět již nyní.

Některé typy dat nebude možné vůbec elektronicky značit, resp. pečetit a tedy odesílat pomocí automatické komunikace. Od ukončení přechodného období bude možné je 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

4.5.1 Webové služby

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

Nebude možné navazovat TLS spojení kvalifikovaným certifikátem. Pokud bude systém disponovat pouze certifikátem pro kvalifikovanou elektronickou značku nebo pečeť bude možné navázat spojení bez klientské autentizace. Údaje pro ověření systému budou získávány z WS-Security hlavičky.

4.5.2 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.

4.6 Zabezpečený email

Stejně jako v případě automatické komunikace budou muset být všechny e-mail zprávy odesílané do CS OTE opatřeny elektronickým podpisem, značkou nebo pečetí vytvořenou kvalifikovaným certifikátem jako v případě webového portálu nebo automatické komunikace.

Při požadavku na příjem e-mail zpráv od CS OTE vyžadující šifrování je nutné mít od konce přechodného období (od 1.10.2017) v CS OTE zaregistrován komerční certifikát pro typ „Autentizace“ – viz Registrace certifikátů.

4.6.1 Ověření nutnosti nového typu certifikátu

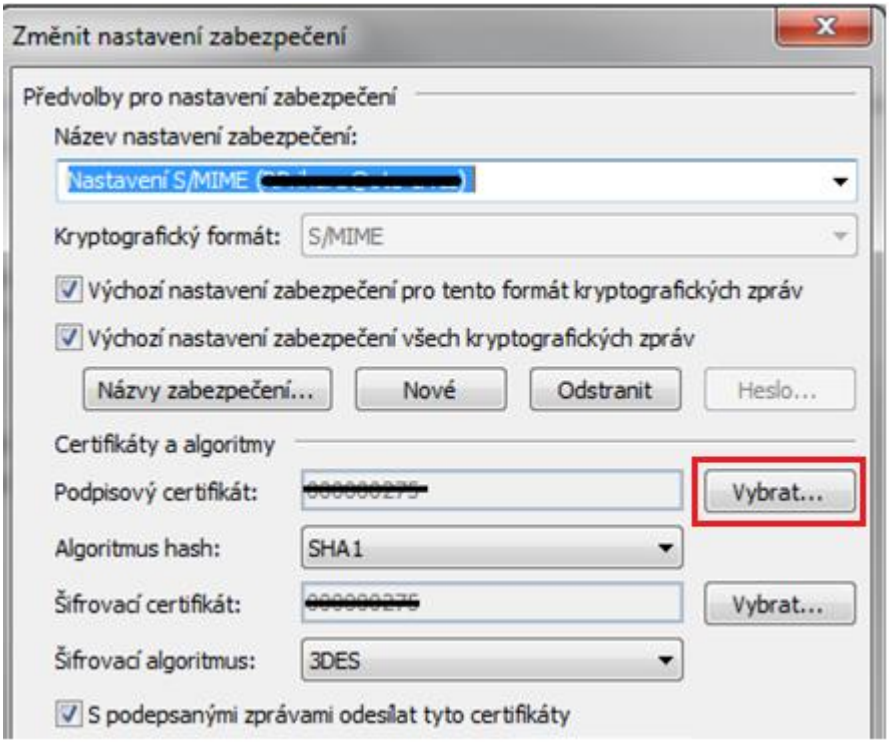
Primárně je třeba zkontrolovat stav registrace certifikátů u daného účtu v části „Zabezpečení přístup“ viz Ověření nutnosti nového certifikátu.

Pro použití v e-mail klientovi musí být pro odesílání nastaven kvalifikovaný certifikát pro elektronický podpis.

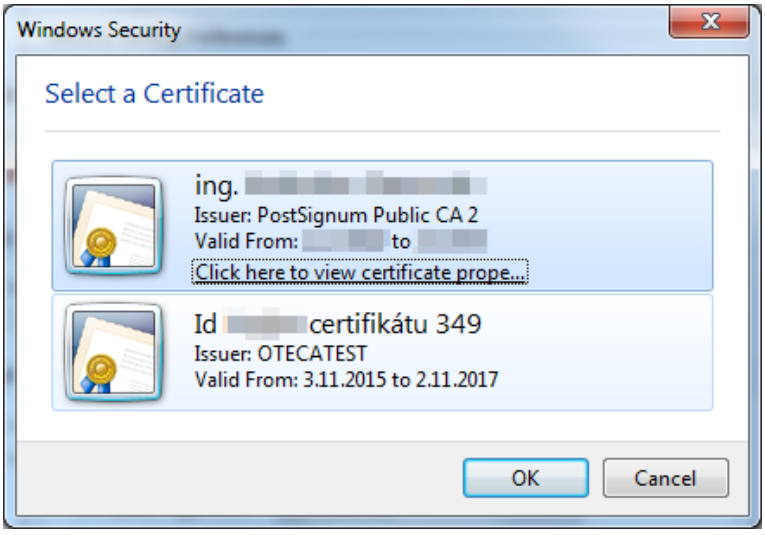
4.6.1.1 Příklad pro MS Outlook 2010

- Spuštění poštovního klienta a vyhledání si nastavení šifrování a podepisování, jak je uvedeno např. v dokumentu http://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/files-konfigurace-pc/d4-instalace-ms-outlook-2010-settings-cz.pdf

- Přejít na nastavení zabezpečení



- Stisknutí tlačítka Vybrat u položky „Podpisový certifikát“ je nutné vybrat certifikát, který je vydán jednou za autorit uvedených v části Příloha 1.



- Pokud uživatel takovým certifikátem nedisponuje, je nutné si zajistit jeho vydání u některé z podporovaných kvalifikovaných certifikačních autorit viz Příloha 1.

5 Příloha 1

5.1 Seznam důvěryhodných autorit vydávající kvalifikované certifikáty

Východiskem je seznam poskytovatelů důvěryhodných služeb EU:
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

Česká republika

https://tsl.gov.cz/publ/TSL_CZ.pdf - níže uvedený seznam vychází z dokumentu platného minimálně do 3.5.2017 14:00:00.

První certifikační autorita, a.s.

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání certifikátů určených pro kvalifikovaný podpis, značku nebo pečeť.

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.

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání certifikátů určených pro kvalifikovaný podpis, značku nebo pečeť.

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.

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání certifikátů určených pro kvalifikovaný podpis, značku nebo pečeť.

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

Maďarsko

http://www.nmhh.hu/tl/pub/HU_TL.pdf - níže uvedený seznam vychází z dokumentu vydaného dne 20.12.2016 16:00:00 CET. Je vybrána pouze autorita, která byla ověřena v CS OTE.

NetLock Ltd.

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání certifikátů určených pro kvalifikovaný podpis, značku nebo pečeť.

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 Minősített Eat. (Class Q Legal) Tanúsítványkiadó

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 Minősített Közigazgatási (Class Q) Tanúsítványkiadó

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

Rakousko

https://www.signatur.rtr.at/currenttl.xml - níže uvedený seznam vychází z dokumentu vydaného dne 19.1.2017 02:00:00 CET, platného do 19.7.2017 02:00:00 CEST. Je vybrána pouze autorita, která byla ověřena v CS OTE.

GLOBALTRUST

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání certifikátů určených pro kvalifikovaný podpis, značku nebo pečeť.

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

Belgie

https://tsl.belgium.be/tsl-be.xml - níže uvedený seznam vychází z dokumentu vydaného dne 16.2.2017 02:00:00 CET, platného do 13.8.2017 02:00:00 CEST. Je vybrána pouze autorita, která byla již používána v CS OTE pro automatickou komunikaci.

QuoVadis

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání certifikátů určených pro kvalifikovaný podpis, značku nebo pečeť.

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 Příloha 2

6.1 Seznam důvěryhodných autorit vydávající komerční certifikáty

První certifikační autorita, a.s.

Všechny komerční certifikáty.

Česká pošta, s.p.

Všechny komerční certifikáty.

eIdentity a.s.

Všechny komerční certifikáty.

NetLock Ltd.

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání komerčních certifikátů vhodných pro autentizaci a šifrování dat.

NetLock Üzleti 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

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání komerčních certifikátů vhodných pro autentizaci a šifrování dat.

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

Dočasně pouze do vypršení aktuálně platných certifikátů (březen 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

Dočasně pouze do vypršení aktuálně platných certifikátů (září 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

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání komerčních certifikátů vhodných pro autentizaci a šifrování dat.

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

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání komerčních certifikátů vhodných pro autentizaci a šifrování dat.

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

Níže jsou uvedeny identifikace platných certifikátů autorit pro vydávání komerčních certifikátů vhodných pro autentizaci a šifrování dat.

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
```