API Dokumentace

SAPI v2.1

05.12.2017

www.ssls.cz/api

**Novinky ve verzi 2.1:**

* Přidána metoda **quickReissue** pro přegenerování SSL certifikátů
* Přidána metoda **mustReissueSymantec**, která vrátí seznam SSL certifikátů, které je nutné přegenerovat v souvislosti s přechodem SSL certifikátů rodiny Symantec na PKI infrastrukturu certifikační autority DigiCert
* Zrušeno ověření domény metodou META u certifikátů Certum a SpaceSSL
* Drobné opravy v textu a upřesnění některých metod
* Úprava limitů v sekci *Omezení* – maximální počet dotazů za minutu/hodinu

# Základní informace o API

API bylo navrženo tak, aby bylo zcela nezávislé na platformě a programovacím jazyce. Pro vývojáře znamená komunikace s API **pouze několik řádků jednoduchého kódu**, viz. www.ssls.cz/api

## Účel API

* **automatizace procesů** s SSL certifikáty (objednávka, ověření, zjištění stavu, stažení atp.)
* přístup k zákaznickému účtu na www.ssls.cz

### API umožňuje mj.:

* zobrazit detailní seznam dostupných SSL certifikátů, včetně cen
* zobrazit stav kreditního účtu (pro objednávku SSL certifikátů je potřeba mít dostatečný kredit)
* vygenerovat privátní klíč a CSR žádost
* ověřit údaje v CSR žádosti a zjistit SHA1 a MD5 hash
* získat seznam autorizačních e-mailových adres pro ověření domény
* získat seznam serverů pro výběr platformy, pro niž je certifikát určen
* objednat nový SSL certifikát
* prodloužit (obnovit) SSL certifikát
* přegenerovat SSL certifikát
* zjistit stav objednávky/SSL certifikátu
* stáhnout vystavený SSL certifikát

## Aktivace API

API je nutné nejprve aktivovat – přihlaste se ke svému účtu na www.ssls.cz, aktivujte API přístup a vygenerujte token. Token je unikátní kód, kterým budete identifikovat všechny API dotazy.

Zároveň nastavte seznam IPv4 adres, ze kterých bude vaše aplikace přistupovat k API. Můžete zadat více IP adres oddělených mezerami. Z bezpečnostních důvodů doporučujeme nastavit pouze IP adresy, které nevyužívají třetí osoby (např. na sdílené webhostingové službě).

## Přístup k API

K API rozhraní SAPI v 2.0 přistupujete pomocí **cURL** na URL adrese:

**https://api.ssls.cz/v2/**{metoda}**/**

Komunikace s API musí probíhat na zabezpečeném protokolu HTTPS. V případě přístupu přes protokol HTTP bude spojení zamítnuto.

## Dotazy a odpovědi

Všechny dotazy musí být odesílány metodou **POST**.

Vzorový kód pro **PHP** najdete na https://www.ssls.cz/api-priklad-php.html a pro **Python** na https://www.ssls.cz/api-priklad-python.html

### Povinný parametr „token“

Každý dotaz musí obsahovat parametr „token“ – unikátní identifikátor, který získáte po přihlášení ke svému účtu na www.ssls.cz

### Volitelný parametr „private“

Potřebujete-li párovat dotazy a odpovědi ve frontě, můžete ke každému dotazu volitelně přidat „private“ s libovolnou hodnotou. Hodnota „private“ bude vrácena v odpovědi.

### Volitelný parametr „accountDetail“

V kterémkoliv dotazu také můžete přidat „accountDetail“ s hodnotou true. Odpověď bude doplněna o některé informace o stavu účtu, např. aktuální výši kreditu. Výchozí hodnota je false.

### Příklad odpovědi na dotaz „product“:

Odpověď je vždy ve formátu JSON. V tomto případě bude odpověď následující:

{

"auth": { "responseID":"1394562148KdD" },

"product": {

"productCode":"positive",

"productName":"PositiveSSL",

"CA":"COMODO",

"price":[259,229,189],

"currency":"czk" }

}

## Chybové odpovědi

Je-li v dotazu chyba, bude do odpovědi přidáno pole „errors“ a původní dotaz se **neprovede**:

{

"auth": { "responseID":"1394562148KdD" },

"errors": {

"isError":true,

"errorCode":1002,

"errorMessage":"Invalid token"}

}

Kompletní seznam všech chybových odpovědí byl z dokumentace vypuštěn a pro přehlednost nahrazen popisem konkrétní chyby v „errorMessage“.

## Omezení

Maximální počet dotazů na API z jednoho účtu je **60 / min** a **2000 / hod**. V případě překročení těchto limitů bude přístup k API dočasně zablokován – poprvé na 15 minut, podruhé na 60 minut a poté vždy na 24 hodin. O předčasné odblokování můžete požádat technickou podporu.

Pro **hromadné dotazy** doporučujeme **vytvořit frontu** požadavků s časovou prodlevou několika vteřin mezi jednotlivými dotazy.

### Poznámka:

Veškerý vstup i výstup API je tzv. case-sensitive, tzn. **rozlišuje** *VELKÉ* a *malé* znaky.

Např. budete-li volat metodu „csrgen“ na URL adrese https://api.ssls.cz/v2/csrgen/, bude vrácena chyba – správně je „csrGen“ s velkým „G“ na adrese https://api.ssls.cz/v2/csrGen/

# Postupy

## Nový SSL certifikát

### Scénář pro objednávku uživatelem/zákazníkem:

Pro objednávku nového SSL certifikátu stačí dodržet jednoduchý postup ve třech krocích:

1. Metodou **csr** ověříte validitu zákazníkem poskytnuté CSR žádosti a získáte v ní uvedené informace
2. Zvolí-li uživatel ověření e-mailem (doporučeno), získáte seznam povolených adres metodou **emails**, ze kterých uživatel vybere jednu adresu, na kterou bude zaslán autorizační e-mail. Tento krok se týká pouze DV certifikátů, včech certifikátů GeoTrust, Comodo, Certum a SpaceSSL. V ostatních případech je možné tento krok ignorovat.
3. Volitelně metodou **servers** získáte seznam serverů, ze kterého uživatel vybere konkrétní typ serveru, na který bude SSL certifikát nainstalován. Tento krok není nezbytný; certifikát bude v každém případě vystaven ve formátu PEM.
4. Odešlete příkaz k objednávce nového SSL certifikátu metodou **newOrder**

### Scénář pro úplnou automatizaci procesu:

Pro objednávku nového SSL certifikátu stačí dodržet jednoduchý postup ve třech krocích:

1. Volitelně, chcete-li proces vystavení SSL certifikátu plně automatizovat, můžete CSR žádost i privátní klíč vygenerovat metodou **csrGen** - v odpovědi získáte jak CSR, tak privátní klíč. CSR a privátní klíč můžete vygenerovat na serveru (bezpečnější). Oba klíče nikam neukládáme, musíte je ihned uložit na serveru.
2. Metodou **csr** ověříte validitu poskytnuté CSR žádosti a získáte v ní uvedené informace. Pakliže již tyto informace máte (v případě generování CSR přímo na serveru), pak je možné tento krok vynechat.
3. Volitelně můžete metodou **servers** získat seznam serverů, z nichž můžete jedním specifikovat konkrétní typ serveru, na který bude SSL certifikát nainstalován. Výchozí je Apache s OpenSSL/ModSSL; certifikát bude v každém případě vystaven ve formátu PEM, a tudíž je možné tento krok vynechat.
4. Odešlete příkaz k objednávce nového SSL certifikátu metodou **newOrder**. Je-li ověření prováděno jinou metodou než e-mailem (FILE, DNS), získáte metodou **newOrder** validační kód (pro metodu DNS) nebo název a obsah souboru (pro metodu FILE).
5. Metodou **certStatus** můžete průběžně zjišťovat, zda byl SSL certifikát již vystaven (doporučeno u DV certifikátů jednou za 30 min, OV jednou za 3 hodiny a EV jednou za 8 hodin). Pakliže ano, můžete metodou **getCert** získat SSL certifikát i intermediate certifikáty a rovnou je automatizovaně nainstalovat na server.

Konkrétní příklad dotazu objednávky SSL certifikátu najdete v dokumentaci metody **newOrder**.

## Prodloužení SSL certifikátu

Postup je stejný jako u objednávky nového SSL certifikátu – jen s tím rozdílem, že k dotazu metodou **newOrder** přidáte parametr orderType = ’renew‘, viz. dokumentace metody **newOrder**.

Prodloužit lze i SSL certifikáty, které byly dříve objednány u jiného prodejce, kromě certifikátů Certum a SpaceSSL.

# Metody ověření

## EMAIL (výchozí metoda)

**Doporučená metoda** - nejrychlejší a nejspolehlivější.

Na e-mailovou adresu bude zaslán autorizační e-mail, ve kterém je nutné kliknout na odkaz, jímž žádost o vystavení SSL certifikátu potvrdíte sami nebo koncový zákazník. Lze použít pouze jednu e-mailovou adresu ze seznamu adres získaného metodou **emails**.

Ověření e-mailem se provádí u všech DV certifikátů a všech certifikátů GeoTrust, Certum a Comodo.

## FILE

Ověření souborem, který je umístěn na server. Autorizační soubor (zpravidla .txt nebo .html) musí mít specifický název a obsah. Tento soubor musí být přístupný na konkrétní doméně (u multidoménových certifikátů na každé uvedené) přes nezabezpečený protokol http://.

Ověření metodou FILE lze provést u všech certifikátů PositiveSSL (kromě wildcard multidomain), Comodo (kromě wildcard multidomain), Certum a SpaceSSL.

## DNS

Metoda ověření DNS spočívá ve vytvoření příslušného DNS záznamu pro doménu uvedenou v CSR a v případě multidoménových SSL certifikátů i pro každou doménu uvedenou v polích SAN.

Ověření touto metodou může trvat až 48 hodin, a proto ji doporučujeme použít pouze v případě, kdy z nějakého důvodu nelze použít žádnou jinou metodou ověření.

Ověření metodou DNS je možné pouze u SSL certifikátů Certum a SpaceSSL.

## META

~~Do HTML kódu výchozí (úvodní) stránky v sekci <head></head> umístíte <meta /> s autorizačním kódem.~~

~~Ověření metodou META je možné pouze u SSL certifikátů Certum a SpaceSSL.~~

**Tato metoda ověření byla 14.02.2017 zrušena.**

# Seznam API metod (dotazů)

#### allProducts všechny dostupné produkty

URL: https://api.ssls.cz/v2/**allProducts**/

Vrátí seznam všech SSL certifikátů dostupných přes API seřazených podle certifikační autority, včetně cen a dalších informací o každém certifikátu.

**Parametry dotazu:** *pouze „token“*

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
**$response** = SAPI('**allProducts**', $dotaz);

#### productDetail informace o produktu

URL: https://api.ssls.cz/v2/**productDetail**/

Vrátí informace o požadovaném certifikátu, např. ceny, podle „productCode“. Seznam všech dostupných kódů SSL certifikátů získáte metodou **allProducts**.

**Parametry dotazu:**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| productCode | **ano** | Kód produktu – unikátní identifikátor SSL certifikátu. productCode pro všechny certifikáty zjistíte metodou **allProducts** |

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘productCode‘] = ‘positive‘;

**$response** = SAPI('**productDetail**', $dotaz);

#### csrGen generování CSR

URL: https://api.ssls.cz/v2/**csrGen**/

Vygeneruje pár 2048-bit RSA privátního klíče a CSR žádosti. Také vrací SHA1 a MD5 hash vygenerované CSR žádosti. Údaje musí být bez české diakritiky a nesmí obsahovat znak "&" (ten zaměňte za "and").

**Parametry dotazu:**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| CN | **ano** | Common Name, plně kvalifikované doménové jméno (FQDN, např. www.ssls.cz) nebo doména ve wildcard formátu s hvězdičkou (např. \*.ssls.cz). |
| C | **ano** | Stát – 2 znaky, dle ISO 3166-1 (např. CZ, SK, US, DE atd.) |
| ST | **ano** | Kraj, pro spolkové země stát nebo teritorium |
| L | **ano** | Město |
| O | **ano** | Organizace, název společnosti nebo celé jméno |
| OU | **ano** | Organizační složka, např. „IT“ |
| E | **ano** | E-mail |

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘CN‘] = ‘www.ssls.cz‘;

$dotaz[‘C ‘] = ‘CZ‘;

$dotaz[‘ST‘] = ‘Praha‘;

$dotaz[‘L‘] = ‘Praha 10‘;

$dotaz[‘O‘] = ‘Alpiro s.r.o.‘;

$dotaz[‘OU‘] = ‘IT Security‘;

$dotaz[‘E‘] = ‘info@ssls.cz‘;

**$response** = SAPI('**csrGen**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| rsaPair.key | vždy | *(string)* privátní klíč |
| rsaPair.csr | vždy | *(string)* CSR žádost |
| csrHash.sha1 | vždy | *(string)* SHA-1 otisk CSR žádosti. |
| csrHash.md5 | vždy | *(string)* MD5 otisk CSR žádosti. |

#### csr validace CSR

URL: https://api.ssls.cz/v2/**csr**/

Validuje CSR žádost ve formátu X.509 a vrátí její obsah. Obsahuje-li nepovolená rozšíření, vrátí chybu.

Pro wildcard certifikáty je nutné v CSR žádosti v poli commonName (CN) uvést doménu ve formátu s hvězdičkou, například \*.ssls.cz. Toto ověření je součástí odpovědi metody **csr** – hodnota isWildcard je true (pokud je CN s hvězdičkou) nebo false (je-li CN bez hvězdičky). Pro wildcard certifikáty nelze poskytnout CSR žádost s doménou uvedenou bez hvězdičky, a naopak pro standardní SSL certifikáty nelze poskytnout CSR s doménou ve wildcard formátu.

Také vrací SHA1 a MD5 hash poskytnuté CSR žádosti.

**Parametry dotazu:**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| csr | **ano** | CSR žádost ve formátu PEM (X.509). |

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘csr‘] = ‘-----BEGIN CERTIFICATE REQUEST-----

MIIC4zCCAcsCAQAwgZ0xCzAJBgNVBAYTAkNaMQ4wDAYDVQQIEwVQcmFoYTERMA8G

A1UEBxMIUHJhaGEgMTAxFjAUBgNVBAoTDUFscGlybyBzLnIuby4xHDAaBgNVBAsT

.................

E1NTTFMuQ1ogSVQgU2VjdXJpdHkxFjAUBgNVBAMTDXRlc3Q3LnNzbHMuY3oxHTAb

IR5rXLNxD92tJCqF7+fPqMqPuBsVb8c=

-----END CERTIFICATE REQUEST-----‘;

**$response** = SAPI('**csr**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| csr.CN | vždy | Doména |
| csr.O | vždy | Organizace |
| csr.OU | vždy | Organizační složka |
| csr.L | vždy | Město |
| csr.ST | vždy | Kraj |
| csr.C | vždy | Stát |
| csr.E | vždy | E-mail |
| csr.isWildcard | vždy | Je-li doména ve wildcard formátu (např. \*.ssls.cz, pouze pro wildcard certifikáty), pak vrátí true, jinak false. |
| csr.hash.sha1 | vždy | sha1 hash CSR žádosti |
| csr.hash.md5 | vždy | md5 hash CSR žádosti |

{

"auth":

{

"responseID":"1392261777CJo"

},

"csr":

{

"CN":"www.ssls.cz",

"O":"Alpiro s.r.o.",

"OU":"SSLS.CZ - IT Security",

"L":"Praha 10",

"ST":"Praha",

"C":"CZ",

"E":"info@ssls.cz",

"isWildcard":false,

"hash":

{

"sha1":"D2BB8DBCCCE35B7788A4A85F78953605870891BF",

"md5":"2BA63316A20F8BE82E7AD24343CF847A"

}

}

}

#### emails autorizační e-mailové adresy

URL: https://api.ssls.cz/v2/**emails**/

Vrátí seznam všech autorizačních e-mailových adres pro danou doménu a produkt. Tuto metodu je nutné zavolat před dotazem „**newOrder**“. Protože se seznam autorizačních e-mailových adres může lišit pro každý produkt. Je nutné uvést i kód produktu, který máte v úmyslu objednat.

Touto metodou je nutné získat seznam autorizačních e-mailových adres pro:

* všechny certifikáty s ověřením domény (DV), pokud nemíníte ověření provést alternativní metodou
* všechny SSL certifikáty Comodo, včetně OV a EV certifikátů
* všechny SSL certifikáty Certum a SpaceSSL, včetně OV a EV certifikátů
* všechny OV i EV certifikáty GeoTrust řady True BusinessID

Pro multidoménové (UC/SAN) certifikáty je nutné zavolat metodu **emails** pro **každou doménu**, která bude uvedena v SSL certifikátu – jednak pro doménu uvedenou v CSR žádosti v poli commonName (CN), tak i pro každou doplňkovou SAN doménu.

**Parametry dotazu:**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| productCode | **ano** | Kód produktu – unikátní identifikátor SSL certifikátu. productCode pro všechny certifikáty zjistíte metodou **allProducts**. |
| domain | **ano** | Doména (FQDN) uvedené v CSR žádosti v poli commonName (CN), zjistíte metodou **csr**. Pro žádné SSL certifikáty již není povolena intranetová doména, NetBIOS jméno ani interní IP adresa. |

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘domain‘] = ‘www.ssls.cz‘;

**$response** = SAPI('**emails**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| emails | vždy | Seznam e-mailových adres, které je možné použít pro autorizaci pro daný certifikát productCode |

{

"auth":

{

"responseID":"1392261777CJo"

},

"emails":

[

"admin@ssls.cz",

"administrator@ssls.cz",

"hostmaster@ssls.cz",

"postmaster@ssls.cz",

"webmaster@ssls.cz",

"admin@www.ssls.cz",

"administrator@www.ssls.cz",

"hostmaster@www.ssls.cz",

"postmaster@www.ssls.cz",

"webmaster@www.ssls.cz"

]

}

#### servers typy serverů

URL: https://api.ssls.cz/v2/**servers**/

Vrátí seznam všech typů serverů.

Pro každý SSL certifikát je vrácen seznam možných serverů s různými hodnotami, a tudíž je nutné uvést kód produktu, který máte v úmyslu objednat.

**Parametry dotazu:**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| productCode | **ano** | Kód produktu – unikátní identifikátor SSL certifikátu. productCode pro všechny certifikáty zjistíte metodou **allProducts**. |

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘productCode‘] = ‘positive‘;

**$response** = SAPI('**servers**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| servers | vždy | Seznam serverových platforem a jejich hodnot pro parametr server metody **newOrder**. |

{

"auth":

{

"responseID":"1392261777CJo"

},

"servers":

{

"Apache+OpenSSL":"2",

"Apache+ModSSL":"2",

"ApacheSSL":"3",

"AOL":"1",

"Citrix":"34"

*... atd. ...*

"WHM cPanel":"31",

"Zeus Web Server":"28",

"Jiný":"-1"

}

}

#### newOrder nový certifikát / prodloužení certifikátu

URL: https://api.ssls.cz/v2/**newOrder**/

Odešle objednávku certifikátu (nové certifikáty nebo prodloužení dle orderType).

Pro úspěšné provedení je nutné mít na svém účtu na www.ssls.cz dostatečný kredit. Kredit bude stržen pouze tehdy, bude-li dotaz úspěšný.

Povinné parametry pro úspěšné zpracování dotazu **newOrder** se liší v závislosti na certifikační autoritě, na úrovni ověření (DV, OV, EV) i na typu certifikátu (standardní, multidoménové atd.). Zatímco u DV certifikátů stačí poskytnout jen nejzákladnější údaje, u OV a EV certifikátů je nutné poskytnout velmi detailní informace.

**Parametry dotazu:**

**Poznámka:** Tečkou ’.’ v parametru je označováno multidimenzionální (víceúrovňové) pole. Např.: dcv.method je ekvivalentem pro request[‘dcv’][‘method’]

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| orderType | ne | Typ objednávky (***nový*** nebo ***prodloužení***) certifikátu. Pro prodloužení uveďte hodnotu „renew“. Výchozí hodnota je „new“ (nový certifikát, není nutné uvádět). |
| productCode | **ano** | Kód produktu – unikátní identifikátor SSL certifikátu. productCode pro všechny certifikáty zjistíte metodou **allProducts**. |
| csr | **ano** | CSR žádost ve formátu PEM (X.509). |
| san.***n*** | Pouze multi-doménové (UC/SAN) certifikáty | Doplňkové SAN domény.  Hlavní doménu uvedenou v CSR žádosti (CN) do pole „san“ **neuvádějte**.  Každou SAN uveďte ve vlastním číselném poli, které je podmnožinou pole „san“ a kde „***n***“ začíná nulou, např. 0, 1, 2, 3 atd.  Například 2 doplňkové SAN domény www.ssls.cz a www.alpiro.cz uveďte jako:  dotaz[‘san‘][0] = ‘www.ssls.cz’  dotaz[‘san‘][1] = ‘www.alpiro.cz’ |
| server | ne | Typ serveru, na který bude SSL certifikát nainstalován. Seznam kódů všech typů serverů získáte metodou „**servers**“. Pokud není uveden, bude certifikát vystaven pro Apache+OpenSSL. |
| period | ne | Délka platnosti SSL certifikátu v rocích. Výchozí hodnota je 1 (jeden rok). |
| dcv.method | ne | Metoda ověření domény. Pouze pro všechny DV certifikáty a dále všechny certifikáty Comodo, PositiveSSL, Certum, SpaceSSL a GeoTrust řady True BusinessID (OV). Možné hodnoty:  * email = výchozí hodnota * file – ověření souborem přes http, pouze Comodo a PositiveSSL (kromě SAN Wildcard certifikátů), Certum a SpaceSSL * dns – pouze certifikáty Certum a SpaceSSL   Musí být uvedeno malými znaky, tj. FILE (velkými písmeny) vrátí chybu. |
| dcv.method2 | ne | Metoda ověření domény. Pouze pro certifikát Certum Premium EV SSL, který je nutné ověřit jak metodou „email“ (dcv.method), tak navíc ještě jednou metodou: Možné hodnoty:  * „file“ = výchozí hodnota * „dns“   Musí být uvedeno malými znaky, tj. FILE (velkými písmeny) vrátí chybu. |
| dcv.email | Pouze pokud dcv.method = “email“ | E-mailová adresa, na kterou bude zaslán autorizační e-mail pro ověření domény. Seznam povolených e-mailových adres se liší v závislosti na konkrétním produktu (SSL certifikátu) a doméně – seznam získáte metodou „**emails**“.  **Povinné** pro všechny DV certifikáty a dále všechny certifikáty Comodo, PositiveSSL, Certum a GeoTrust řady True BusinessID. |
| dcv.emails | Povinné pro UC/SAN SSL a pokud dcv.method = “email“ | E-mailová adresa, na kterou bude zaslán autorizační e-mail pro ověření domény. Seznam povolených e-mailových adres se liší v závislosti na konkrétním produktu (SSL certifikátu) a doméně – seznam získáte metodou „**emails**“.  **Povinné** pro všechny DV certifikáty a dále všechny certifikáty Comodo, PositiveSSL, Certum a GeoTrust řady True BusinessID.  Uveďte autorizační e-mailové adresy **pro každou** SAN doménu uvedenou v certifikátu. Jednotlivé adresy oddělte čárkou **bez mezer**. E-mailové adresy musí být ve stejném pořadí jako domény v san.***n***.  **Například:** U objednávky certifikátu pro 4 domény www.ssls.cz (CN), www.alpiro.cz (SAN0), ssls.cz (SAN1) a alpiro.cz (SAN2) poskytněte následující textový řetězec:  “admin@alpiro.cz,admin@ssls.cz,admin@alpiro .cz” |
| admin.title | ne | Oslovení osoby vyřizující žádost o certifikát (Mr, Mrs, Board Member atd.) |
| admin.firstname | **ano** | Křestní jméno osoby vyřizující žádost o certifikát |
| admin.lastname | **ano** | Příjmení osoby vyřizující žádost o certifikát |
| admin.phone | **ano** | Telefon osoby vyřizující žádost o certifikát v mezinárodním formátu 00420123456789 (pouze číslice bez mezer, namísto znaku „+“ uveďte dvě nuly) |
| admin.email | **ano** | E-mail osoby vyřizující žádost o certifikát |
| admin.organization | Pouze OV a EV certifikáty + všechny certifikáty Certum | Organizace (název společnosti) osoby vyřizující žádost o certifikát |
| admin.city | Pouze OV a EV certifikáty + všechny certifikáty Certum | Město sídla organizace nebo pobytu osoby vyřizující žádost o certifikát |
| admin.country | **ano** | Stát sídla organizace nebo pobytu osoby vyřizující žádost o certifikát – 2 znaky, dle ISO 3166-1 (např. CZ, SK, US, DE atd.) |
| admin.fax | ne | Fax číslo osoby vyřizující žádost o certifikát. Pouze OV a EV certifikáty + všechny certifikáty Certum.  Výchozí hodnota je hodnota „admin.phone“ |
| tech.title | ne | Oslovení osoby technického kontaktu (Mr, Mrs, Board Member atd.).  Výchozí hodnota je hodnota admin.title |
| tech.firstname | ne | Křestní jméno osoby technického kontaktu  Výchozí hodnota je hodnota admin.firstname |
| tech.lastname | ne | Příjmení osoby technického kontaktu  Výchozí hodnota je hodnota admin.lastname |
| tech.phone | ne | Telefon osoby technického kontaktu v mezinárodním formátu 00420123456789 (pouze číslice bez mezer, namísto znaku „+“ uveďte dvě nuly)  Výchozí hodnota je hodnota admin.phone |
| tech.email | ne | E-mail osoby technického kontaktu.  **Pozor:** Na tuto e-mailovou adresu bude zaslán vystavený SSL certifikát.  Výchozí hodnota je hodnota admin.email |
| tech.organization | ne | Organizace (název společnosti) osoby technického kontaktu. Pouze OV a EV certifikáty + všechny certifikáty Certum.  Výchozí hodnota je hodnota admin.organization |
| tech.city | ne | Město sídla organizace nebo pobytu osoby technického kontaktu – 2 znaky, dle ISO 3166-1 (např. CZ, SK, US, DE atd.). Pouze OV a EV certifikáty + všechny certifikáty Certum.  Výchozí hodnota je hodnota admin.city |
| tech.country | ne | Stát sídla organizace nebo pobytu osoby technického kontaktu. Pouze OV a EV certifikáty + všechny certifikáty Certum.  Výchozí hodnota je hodnota admin.country |
| tech.fax | ne | Fax číslo osoby technického kontaktu. Pouze OV a EV certifikáty + všechny certifikáty Certum.  Výchozí hodnota je hodnota „tech.phone“. Není-li uveden „tech.phone“, je výchozí hodnotou hodnota „admin.fax“. Není-li uveden „admin.fax“, je výchozí hodnotou hodnota „admin.phone“. |
| org.street | Pouze OV a EV certifikáty + všechny certifikáty Certum a SpaceSSL | Ulice sídla organizace nebo jiného subjektu, pro který je certifikát objednáván. Jedná se o doplňující informaci k CSR, která tento údaj nemůže obsahovat. |
| org.postalcode | Pouze OV a EV certifikáty + všechny certifikáty Certum a SpaceSSL | PSČ organizace nebo jiného subjektu, pro který je certifikát objednáván. Jedná se o doplňující informaci k CSR, která tento údaj nemůže obsahovat. |
| org.email | Pouze certifikáty Certum a SpaceSSL a pouze pokud v CSR není uveden e-mail | E-mailová adresa organizace nebo jiného subjektu, pro který je certifikát objednáván.  **Povinné** pouze pro certifikáty Certum a pouze tehdy, pokud CSR žádost neobsahuje e-mailovou adresu (E) |
| org.businessId | Pouze OV a EV certifikáty Certum | IČ nebo DIČ organizace nebo jiného subjektu, pro který je certifikát objednáván. |
| org.duns | ne | D-U-N-S číslo (Dun & Bradstreet číslo) organizace nebo jiného subjektu, pro který je certifikát objednáván. Přestože není povinné, důrazně doporučujeme ho uvést u OV a EV certifikátů (výrazně zrychlí proces ověření). |
| org.phone | ne | Telefon organizace nebo jiného subjektu, pro který je certifikát objednáván.  Výchozí hodnota je hodnota admin.phone |
| org.fax | ne | Fax číslo organizace nebo jiného subjektu, pro který je certifikát objednáván.  Výchozí hodnota je hodnota admin.fax. Není-li uveden „admin.fax“, je výchozí hodnotou hodnota „admin.phone“. |

### Příklad objednávky nového SSL certifikátu PositiveSSL (ověření domény, DV) na 2 roky:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘productCode‘] = ‘positive‘;

$dotaz[‘period‘] = ‘2‘;

$dotaz[‘csr’] = ‘*… CSR žádost pro www.ssls.cz …*’;

$dotaz[‘dcv’][‘email’] = ‘admin@ssls.cz’;

$dotaz[‘admin’][‘firstname’] = ‘Josef’;

$dotaz[‘admin’][‘lastname’] = ‘Novak’;

$dotaz[‘admin’][‘phone’] = ‘00420123456789’;

$dotaz[‘admin’][‘email’] = ‘info@ssls.cz’;

$dotaz[‘admin’][‘country’] = ‘CZ’;

**$response** = SAPI('**newOrder**', $dotaz);

### Příklad objednávky nového SSL certifikátu InstantSSL (ověření společnosti, OV) na 1 rok:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘productCode‘] = ‘instant‘;

$dotaz[‘csr’] = ‘*… CSR žádost pro www.ssls.cz …*’;

$dotaz[‘dcv’][‘email’] = ‘admin@ssls.cz’;

$dotaz[‘admin’][‘firstname’] = ‘Josef’;

$dotaz[‘admin’][‘lastname’] = ‘Novak’;

$dotaz[‘admin’][‘phone’] = ‘00420123456789’;

$dotaz[‘admin’][‘email’] = ‘info@ssls.cz’;

$dotaz[‘admin’][‘country’] = ‘CZ’;

$dotaz['admin']['organization'] = 'Alpiro s.r.o.';

$dotaz['admin']['city'] = 'Praha 10';

$dotaz['org']['street'] = 'Ulice cp. 123/45';

$dotaz['org']['phone'] = '00420739652775';

$dotaz['org']['postalcode'] = '10200';

$dotaz['org']['duns'] = '366901555';

**$response** = SAPI('**newOrder**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| orderID | vždy | Číslo objednávky |
| certID | vždy | ID certifikátu |
| fileAuth.fileName | Pouze při ověření metodou file. | Název autorizačního souboru. Např. 123456789.html nebo 1213456789.txt  Při přístupu k tomuto souboru musí server vrátit v HTTP hlavičce odpověď "200 OK" a nesmí dojít k žádnému přesměrování - ani na stejnou URL s protokolem https, musí být na http. |
| fileAuth.fileContent | Pouze při ověření metodou file. | Obsah autorizačního souboru. Pouze u certifikátů Comodo, PositiveSSL, Certum a SpaceSSL. |
| dnsAuth.code | Pouze při ověření metodou dns. | Autorizační kód. |
| dnsAuth.type | Pouze při ověření metodou dns. | Typ DNS záznamu (TXT, CNAME) |

{

"auth":

{

"responseID":"1392261777CJo"

},

"orderID":"123456",

"certID":"1234567890"

}

#### certStatus stav certifikátu

URL: https://api.ssls.cz/v2/**certStatus**/

Zjistí stav certifikátu/objednávky.

Mj. vrátí ID objednávky certifikační autority, které je nutné v případě potřeby kontaktovat přímo certifikační autoritu.

**Parametry dotazu:**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| certID | **ano** | ID certifikátu – vráceno metodou **newOrder**, popř. najdete na www.ssls.cz v sekci Můj účet > Moje certifikáty > Detail certifikátu na řádku „SSLS ID“ |

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘certID‘] = ‘123456789‘;

**$response** = SAPI('**certStatus**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| status.certID | vždy | ID certifikátu |
| status.vendorID | pokud již bylo přiděleno | ID objednávky v systému certifikační autority. Toto ID je nutné uvádět při řešení situací přímo s certifikační autoritou. |
| status.status | vždy | Stav certifikátu. Seznam možných hodnot najdete níže pod tabulkou. |
| status.message | vždy | Textová informace o stavu certifikátu |
| status.CN | vždy | Doména, která byla uvedena v CSR žádosti. |
| status.SAN | vždy | Seznam doplňkových SAN domén |
| status.NVB | pouze pokud status=A | *(UNIX TimeStamp)* Datum (popř. přesný čas), **od** kterého je certifikát platný |
| status.NVA | pouze pokud status=A | *(UNIX TimeStamp)* Datum (popř. přesný čas), **do** kterého je certifikát platný |
| status.dcv.method | vždy | Metoda ověření (email, file, dns) |
| status.dcv.method2 | pouze pro Certum EV | Druhá metoda ověření (file, dns) |
| status.dcv.email | pouze pokud method=email | Autorizační e-mailová adres. Jedná-li se o UC/SAN certifikát, je vrácen řetězec se seznamem všech autorizačních adres včetně hlavní domény CN (vždy na prvním místě), oddělené čárkami. |

{

"auth":

{

"responseID":"1392261777CJo"

},

"status":

{

"certID":"1504033",

"vendorID":"16011593",

"status":"A",

"message":"Vystaven a aktivní”,

"CN":"www.ssls.cz”,

"SAN":

[

“ssls.cz”,

“www.alpiro.cz”,

“alpiro.cz”

],

"NVB":1426287600,

"NVA":1518476400,

"dcv":

{

"method":"email",

"method2":"",

"email”:”admin@ssls.cz,admin@ssls.cz,admin@alpiro.cz,admin@alpiro.cz”

}

}

}

### Možné hodnoty stavu certifikátu:

* P – probíhá ověření, čeká na ověření, vystavení či přegenerování, anebo probíhá změna
* A – certifikát je aktivní (byl vystaven a je platný)
* R – certifikát byl přegenerován, je aktivní (byl vystaven a je platný), prakticky ekvivalent k „A“
* C – certifikát byl revokován (zneplatněn), objednávka byla zrušena nebo byl certifikát zamítnut
* U – nezjištěno; voláte-li **certStatus** ihned po **newOrder**, může být objednávka stále ve frontě – zkuste zavolat **certStatus** později (někdy může trvat i několik minut)
* N – certifikát dosud nebyl aktivován nebo příslušná objednávka nebyla uhrazena
* E – certifikát expiroval, je po splatnosti

#### getCert stažení certifikátu

URL: https://api.ssls.cz/v2/**getCert**/

Vrátí vystavený (aktivní) certifikát, včetně příslušných intermediate CA certifikátů. Pokud certifikát dosud nebyl vystaven nebo přegenerován, vrátí chybu.

**Parametry dotazu:**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| certID | **ano** | ID certifikátu – vráceno metodou **newOrder**, popř. najdete na www.ssls.cz v sekci Můj účet > Moje certifikáty > Detail certifikátu na řádku „SSLS ID“ |

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
$dotaz[‘certID‘] = ‘123456789‘;

**$response** = SAPI('**getCert**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| certificates.***n***.FileName | vždy | Název souboru certifikátu. Z hlediska instalace certifikátu nemá FileName význam, můžete pojmenovat dle vlastního uvážení.  ***n*** je číselné pole seznamu certifikátů. |
| certificates.***n***.Contents | vždy | Certifikát ve formátu PEM.  Nové řádky jsou odděleny znaky \n  Dopředná lomítka / jsou "escapována" zpětným lomítkem, např. \/ |

{

"auth":

{

"responseID":"1392261777CJo"

},

"certificates":

[

{

"FileName":"www.ssls.cz.cer",

"Contents":"-----BEGIN CERTIFICATE-----

MIIGBzCCBO+gAwIBAgIRAKIKREfgOHrewIYnk+jTdFQwDQYJKoZIhvcNAQELBQAw

…

4dKj3bsibgvB5s1SELVDuHtn/foXTIecI66iCjXQmCijGlah7hzYfhx/DdC3qH4f

bu78EtTUnsVzgoE=

-----END CERTIFICATE-----"

},

{

"FileName":"Intermediate\_CA\_chain.cer",

"Contents":"-----BEGIN CERTIFICATE-----

MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU

…

c4g/VhsxOBi0cQ+azcgOno4uG+GMmIPLHzHxREzGBHNJdmAPx/i9F4BrLunMTA5a

mnkPIAou1Z5jJh5VkpTYghdae9C8x49OhgQ=

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

eHRlcm5hbCBDQSBSb290MB4XDTAwMDUzMDEwNDgzOFoXDTIwMDUzMDEwNDgzOFow

…

BmeBDAECATBMBgNVHR8ERTBDMEGgP6A9hjtodHRwOi8vY3JsLmNvbW9kb2NhLmNv

bS9DT01PRE9SU0FDZXJ0aWZpY2F0aW9uQXV0aG9yaXR5LmNybDBxBggrBgEFBQcB

-----END CERTIFICATE-----"

}

]

}

#### myCerts moje certifikáty

URL: https://api.ssls.cz/v2/**myCerts**/

Vrátí seznam všech certifikátů k účtu Partnera (objednané přes API i přes webové rozhraní na www.ssls.cz).

**Parametry dotazu:** *pouze „token“*

### Dotaz:

$dotaz[‘token‘] = ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ‘;  
**$response** = SAPI('**myCerts**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| myCerts.***n***.certID | vždy | ID certifikátu  ***n*** je číselné pole seznamu certifikátů. |
| myCerts.***n***.orderType | vždy | Nový certifikát (new) nebo prodloužení (renew) |
| myCerts.***n***.orderDate | vždy | *(UNIX TimeStamp)* Datum objednávky |
| myCerts.***n***.paidDate | vždy | *(UNIX TimeStamp)* Datum úhrady objednávky  Je-li datum 0, pak objednávka dosud nebyla uhrazena. |
| myCerts.***n***.paymentMethod | vždy | Platební metoda (Credit) |
| myCerts.***n***.invoiceNumber | vždy | Číslo faktury. Pokud dosud nebyla vystavena, je hodnota 0. |
| myCerts.***n***.productName | vždy | Název certifikátu |
| myCerts.***n***.period | vždy | Délka platnosti certifikátu v rocích. |
| myCerts.***n***.status | vždy | Stav certifikátu. Seznam možných hodnot najdete v dokumentaci metody **certStatus**. |
| myCerts.***n***.NVB | vždy | *(UNIX TimeStamp)* Datum (popř. přesný čas), **od** kterého je certifikát platný |
| myCerts.***n***.NVA | vždy | *(UNIX TimeStamp)* Datum (popř. přesný čas), **do** kterého je certifikát platný |
| myCerts.***n***.CN | vždy | Doména, která byla uvedena v CSR žádosti. |
| myCerts.***n***.SAN | vždy | Seznam doplňkových SAN domén oddělené čárkami |

{

"auth":

{

"responseID":"1392261777CJo"

},

"myCerts":

[

{

"certID”:”1000001”,

"orderType":"new",

"orderDate":1392261777,

"paidDate":1392261778,

"paymentMethod":"Credit",

"invoiceNumber":12345678,

"productName":"PositiveSSL Multidomain",

"period":3,

"status”:”A”,

"NVB":1504033,

"NVA":16011593,

"CN":"www.alpiro.cz",

"SAN":"alpiro.cz,www.ssls.cz,ssls.cz"

}

]

}

#### quickReissue přegenerování certifikátu

URL: https://api.ssls.cz/v2/**quickReissue**/

Odešle žádost o přegenerování certifikátu.

Pro ověření domény (či více domén u multidoménových UC/SAN certifikátů) bude použita autorizační metoda, která byla zvolena u původní objednávky certifikátu. Pokud tyto informace neuchováváte, pak autorizační metodu a e-mailovou adresu (v případě ověření metodou email) můžete zjistit ještě před odesláním žádosti o přegenerování pomocí metody **certStatus**.

U DV certifikátů stačí provést ověření domény. U OV a EV certifikátů certifikační autorita provede ručně některé další kroky spojené s procesem ověřením organizace, popř. si vyžádá další doklady.

**Pozn.:** Přegenerovat lze všechny SSL certifikáty kromě Certum a SpaceSSL. Tato metoda neumožňuje změnit SAN domény v certifikátu.

**UPOZORNĚNÍ:** Při hromadném přegenerování certifikátů, například v souvislosti s přechodem certifikátů rodiny Symantec na PKI infrastrukturu DigiCert (viz https://ssls.cz/l/symr), mějte na paměti **limity** – maximální počet API požadavků za minutu/hodinu, viz informace v sekci „Omezení“.

**UPOZORNĚNÍ:** **Vzhledem k enormnímu možství požadavků na přegenerování certifikátů rodiny Symantec doporučujeme odložit přegenerování nejdříve na leden/únor 2018.**

### Parametry dotazu:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Povinný** | **Poznámky** |
| certID | **ano** | ID certifikátu (SSLS ID) |
| csr | **ano** | **Nová** CSR žádost ve formátu PEM (X.509).  Common Name (CN) musí být totožná s doménou uvedenou v certifikátu. **Pozor:** www.ssls.cz ≠ ssls.cz  **Nelze použít dříve použitou CSR žádost!** |

### Příklad přegenerování SSL certifikátu:

$dotaz['token'] = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ';  
$dotaz['certID'] = '1234567890';

$dotaz['csr'] = '*… CSR žádost pro www.ssls.cz …*';

**$response** = SAPI('**quickReissue**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| certID | vždy | ID certifikátu (SSLS ID) |
| method | vždy | Metoda ověření (email, file, dns) |
| emailAuth | Při ověření metodou email. | E-mailová adresa, na kterou bude zaslán autorizační e-mail pro ověření domény.  U multidoménových (UC/SAN) certifikátů seznam e-mailových adres oddělených čárkou, například:  admin@ssls.cz,admin@ssls.cz,administrator@alpiro.cz |
| fileAuth.fileName | Při ověření metodou file. | Název autorizačního souboru. Např. 123456789.html nebo 1213456789.txt  Při přístupu k tomuto souboru musí server vrátit v HTTP hlavičce odpověď "200 OK" a nesmí dojít k žádnému přesměrování - ani na stejnou URL s protokolem https, musí být na http. |
| fileAuth.fileContent | Při ověření metodou file. | Obsah autorizačního souboru. Pouze u certifikátů Comodo, PositiveSSL, Certum a SpaceSSL. |
| dnsAuth.code | Při ověření metodou dns. | Autorizační kód. |
| dnsAuth.type | Při ověření metodou dns. | Typ DNS záznamu (TXT, CNAME) |

{

"auth":

{

"responseID":"1392261777CJo"

},

"certID":"1234567890",

"method":"email",

"emailAuth":"admin@ssls.cz"

}

#### mustReissueSymantec certifikáty Symantec k přegenerování

URL: https://api.ssls.cz/v2/**mustReissueSymantec**/

Vrátí seznam SSL certifikátů rodiny Symantec (AlpiroSSL, Symantec, GeoTrust, Thawte a RapidSSL), které je nutné přegenerovat v souvislosti s přechodem těchto certifikačních autorit na novou PKI infrastrukturu certifikační autority DigiCert. Čtěte více na https://ssls.cz/l/symr. Seznam certifikátů je totožný se seznamem na adrese https://ssls.cz/l/srm.

**Parametry dotazu:** *pouze „token“*

### Dotaz:

$dotaz['token'] = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ';  
**$response** = SAPI('**mustReissueSymantec**', $dotaz);

### Odpověď:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Odpověď** | **Poznámky** |
| mustReissueSymantec.***n***.certID | vždy | ID certifikátu (SSLS ID) |
| mustReissueSymantec.***n***.productName | vždy | Název certifikátu |
| mustReissueSymantec.***n***.NVB | vždy | Datum posledního vystavení/přegenerování SSL certifikátu v UNIX formátu |
| mustReissueSymantec.***n***.NVA | vždy | Datum expirace certifikátu v UNIX formátu |
| mustReissueSymantec.***n***.reissueBefore | vždy | Datum v UNIX formátu, do kterého musí být certifikát úspěšně přegenerován.  **Upozornění:** Důrazně doporučujeme přegenerování provést s dostatečným předstihem, protože systémy CA i technická podpora mohou být vzhledem k enormnímu množství žádostí přetížené. |
| mustReissueSymantec.***n***.CN | vždy | Doména certifikátu v poli Common Name |
| mustReissueSymantec.***n***.SAN | vždy | Seznam doplňkových SAN domén, oddělené čárkou. Může být prázdné. |
| totalToReissue | vždy | Celkový počet certifikátů, které je nutné přegenerovat |

{

"auth":

{

"responseID":"1392261777CJo"

},

"mustReissueSymantec":

[

{

"certID”:”1000001”,

"productName":"True BusinessID",

"NVB":1504033,

"NVA":16011593,

"reissueBefore":1522368001,

"CN":"www.alpiro.cz",

"SAN":"alpiro.cz,www.ssls.cz,ssls.cz"

},

{

"certID”:”1000002”,

"productName":"AlpiroSSL Wildcard",

"NVB":1504033,

"NVA":16011593,

"reissueBefore":1522368001,

"CN":"\*.alpiro.cz",

"SAN":""

}

],

"totalToReissue":2

}