

# SSL Reseller

Dokumentacja techniczna  
v.1.9  
z dnia 2021-07-22



# 1. Dostęp do API

Dostęp do API realizowany jest za pomocą żądań POST.

Adres API: <https://www.mserwis.pl/sslapi>

## 2. Katalog komend:

### a. CheckBalance

Komenda zwraca stan salda partnera

parametry:

Nazwa	Typ	Wymagany	opis
user	string	TAK	Login konta partnera
password	string	TAK	Hasło partnera
command	string	TAK	przyjmuje wartość "CheckBalance"

Odpowiedź:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>545.40</resultMessage>
</result>
</response>
```

Wartość salda zawarta jest w polu <resultMessage />

## b) ValidateOrder

Komenda sprawdza poprawność danych przesłanych do złożenia zamówienia na certyfikat SSL. Nie zamawia certyfikatu SSL i nie pobiera opłaty. Można ją używać do celów testowych.

parametry:

Nazwa	Typ	Wymagany	opis
user	string	TAK	Login konta partnera
password	string	TAK	Hasło partnera
command	string	TAK	przyjmuje wartość "ValidateOrder"
product	string	TAK	rodzaj certyfikatu zgodnie z załącznikiem A
period	int	TAK	okres rejestracji certyfikatu (sprawdź uwagi niżej)
csr	string	TAK	CSR
first_name	string	TAK	Imię usługobiorcy
last_name	string	TAK	Nazwisko usługobiorcy
phone	string	TAK	Numer telefonu usługobiorcy w formacie +48.501222333
email	string	TAK	Adres email usługobiorcy
admin_email	string	TAK	Adres email weryfikacyjny. Jeden z adresów: admin@, webmaster@, administrator@, hostmaster@ lub postmaster@ w domenie, dla której zakupiony jest certyfikat
company	string	NIE	Nazwa firmy usługobiorcy
address	string	TAK	Adres usługobiorcy
city	string	TAK	Miasto usługobiorcy

district	string	TAK	Województwo
zip	string	TAK	Kod pocztowy w formacie XX-XXX
country	string	TAK	Dwuliterowy kod kraju usługobiorcy
language	string	NIE	Kod języka emaili (domyślnie PL)
http_validation	string	NIE	Potwierdzenie własności domeny za pomocą umieszczenia pliku na stronie. Należy podać wartość 'true' małymi literami. Opcja dostępna tylko dla certyfikatów Symantec/Geotrust/RapidSSL.
dns_validation	string	NIE	Potwierdzenie własności domeny za pomocą rekordów DNS. Należy podać 'true' małymi literami. Opcja dostępna tylko dla certyfikatów Symantec/Geotrust/RapidSSL.

**UWAGA!** Nie można podać równocześnie parametru `http_validation` oraz `dns_validation`. W jednym zamówieniu może wystąpić, albo jeden z nich, albo - w przypadku standardowej walidacji za pomocą e-maila nie należy ich podawać wcale.

Uwaga odnośnie parametru `period`. Od sierpnia 2020 roku wystawiane certyfikaty SSL mogą być ważne maksymalnie 398 dni, a więc 1 rok + okres dodatkowy. Jeśli dany typ certyfikatu wspiera usługę subskrypcyjną, można go zamówić na okres nawet do 5 lat. Certyfikat zostanie jednak wydany na okres do 398 dni a pod koniec tego okresu należy wykonać darmowy reissue, aby uzyskać certyfikat ważny na kolejny okres.

Odpowiedź gdy wystąpił błąd:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>6009</resultCode>
<resultMessage>Nieprawidłowy adres</resultMessage>
</result>
```

```
</response>
```

**Odpowiedź gdy operacja zakończona sukcesem:**

```
<?xml version="1.0" encoding="UTF-8"?>  
<response>  
<result>  
<resultCode>1000</resultCode>  
<resultMessage>OK</resultMessage>  
</result>  
</response>
```

## c) PlaceOrder

Składa zamówienie na certyfikat SSL.

Zamówienie realizowane jest online, pobierana jest opłata zgodna z cennikiem partnera.

Parametry żądania są identyczne jak dla ValidateOrder, z tym że pole command przyjmuje wartość "PlaceOrder"

Odpowiedź gdy operacja zakończona sukcesem:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>OK</resultMessage>
<resultId>R12345</resultId>
</result>
</response>
```

W polu <resultId/> zawarty jest numer zamówienia.

Odpowiedź gdy operacja zakończona sukcesem i podano parametr http\_validation:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>OK</resultMessage>
<resultId>R12345</resultId>
<filename>
  <![CDATA[ q4lusav8.htm ]]>
</filename>
<content>
  <![CDATA[ 23M6m3P6O1ymJbQ9ZWzU ]]>
</content>
</result>
</response>
```

Na serwerze pod domeną, dla której ma być wydany certyfikat należy umieścić plik o nazwie zawartej w polu 'filename' o treści zawartej w polu 'content', czyli w powyższym przykładzie należy umieścić plik o nazwie q4lusav8.htm i treści 23M6m3P6O1ymJbQ9ZWzU.

**UWAGA!** Dla certyfikatów **Sectigo/Symantec/GeoTrust** plik należy umieszczać w folderze `/.well-known/pki-validation/`

Przykładowo - ścieżka do pliku walidującego domenę będzie wyglądać tak:

<http://example.com/.well-known/pki-validation/8D74EE158718C552568B8B7D79F6FD9E.txt>

zmieniło się także rozszerzenie pliku z `.htm` na `.txt`.

Odpowiedź gdy operacja zakończona sukcesem i podano parametr `dns_validation`:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>OK</resultMessage>
<resultId>R12345</resultId>
<RecordAuthName>
  DNS TXT Record
</RecordAuthName>
<RecordAuthValue>
  2017082600000137r13zfcevcgj7x3x9d8056v0kpgqwgk7jcjxlvolc4f58kjja
</RecordAuthValue>
</result>
</response>
```

Na serwerze DNS należy do strefy obsługującej domenę, dla której wydawany jest certyfikat dodać rekord TXT z wartością przekazaną w polu `RecordAuthValue`



## d) CheckOrder

Funkcja służy do sprawdzenia statusu zamówienia.

parametry:

Nazwa	Typ	Wymagany	opis
user	string	TAK	Login konta partnera
password	string	TAK	Hasło partnera
command	string	TAK	przyjmuje wartość "CheckOrder"
order_id	string	TAK	numer zamówienia

Odpowiedź gdy operacja zakończona sukcesem:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>COMPLETE - COMPLETED</resultMessage>
<certificate>...<certificate>
</result>
</response>
```

Zamówienie może być w stanie:

"PENDING - WF\_DOMAIN\_APPROVAL" - oczekuje na weryfikację

"CANCELLED" - zamówienie anulowane

"COMPLETE - COMPLETED" - zamówienie zakończone

## d) GetApprovalEmails

Funkcja służy do pobrania listy emaili, które mogą być użyte jako email autoryzacyjny do weryfikacji własności domeny dla certyfikatu SSL.

parametry:

Nazwa	Typ	Wymagany	opis
user	string	TAK	Login konta partnera
password	string	TAK	Hasło partnera
command	string	TAK	przyjmuje wartość "GetApprovalEmails"
domain	string	TAK	nazwa domeny
product	string	TAK	rodzaj certyfikatu zgodnie z załącznikiem A

Odpowiedź gdy operacja zakończona sukcesem:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>
<emails>
<email>admin@domena.pl</email>
<email>postmaster@domena.pl</email>
</emails>
</resultMessage>
</result>
</response>
```

## e) ReissueCertificate

Funkcja służy do ponownego wydania certyfikatu SSL.

parametry:

Nazwa	Typ	Wymagany	opis
user	string	TAK	Login konta partnera
password	string	TAK	Hasło partnera
command	string	TAK	przyjmuje wartość "ReissueCertificate"
order_id	string	TAK	numer pierwotnego zamówienia
csr	string	TAK	nowy CSR

Odpowiedź gdy operacja zakończona sukcesem:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>OK</resultMessage>
</result>
</response>
```

## f) ResendVerificationEmail

Funkcja służy do ponownego wysłania wiadomości weryfikacyjnej.

parametry:

Nazwa	Typ	Wymagany	opis
user	string	TAK	Login konta partnera
password	string	TAK	Hasło partnera
command	string	TAK	przyjmuje wartość "ResendVerification Email"
order_id	string	TAK	numer pierwotnego zamówienia

Odpowiedź gdy operacja zakończona sukcesem:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>1000</resultCode>
<resultMessage>OK</resultMessage>
</result>
</response>
```

Odpowiedź gdy operacja zakończona błędem:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>
<resultCode>999</resultCode>
<resultMessage>Błąd połączenia z rejestrem</resultMessage>
</result>
</response>
```

# 3. Przykładowe wywołanie komendy z PHP

```
function sendCommand($command){
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, "https://www.mserwis.pl/sslapi");
    curl_setopt($ch, CURLOPT_PORT, 443);
    curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 5);
    curl_setopt($ch, CURLOPT_TIMEOUT, 15);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER,1);
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $command);
    $result=curl_exec($ch);
    curl_close($ch);
    return $result;
}

$command = array('user' => 'test@mserwis.pl',
    'password' => 'haslo',
    'command' => 'CheckOrder',
    'order_id' => 'R12345'
);

$resp = sendCommand($command);

$xml = new SimpleXMLElement($resp, LIBXML_NOCDATA);

if ($xml->response->result->resultCode == 1000)
{
    echo "Zamówienie w statusie: ".$xml->response->result->resultMessage;
}
else
{
    echo "Wystąpił błąd: ".$xml->response->resultMessage;
}
```

# ZAŁĄCZNIK A - Dozwolone typy certyfikatów

parametr type	Nazwa certyfikatu
rapidssl	RapidSSL
rapidssl_wildcard	RapidSSL Wildcard
geotrust_quicksslpremium	GeoTrust QuickSSL Premium
geotrust_trueid	GeoTrust True BusinessID
geotrust_ev	GeoTrust True BusinessID EV
geotrust_wildcard	GeoTrust True BusinessID Wildcard
geotrust_quicksslmultidomain	GeoTrust QuickSSL Premium Multidomain
geotrust_truemultidomain	GeoTrust True BusinessID Multidomain
geotrust_truemultidomain_ev	GeoTrust True BusinessID EV Multidomain
symantec_secure	Symantec Secure Site
symantec_securepro	Symantec Secure Site Pro
symantec_ev	Symantec Secure Site EV
symantec_evpro	Symantec Secure Site Pro EV
comodo_positive	Sectigo (Comodo) Positive SSL
comodo_instant	Sectigo (Comodo) Instant OV
comodo_ev	Sectigo (Comodo) EV
comodo_ev_multidomain	Sectigo (Comodo) EV Multidomain
comodo_wildcard	Sectigo (Comodo) Essential Wildcard
comodo_wildcard_premium	Sectigo (Comodo) Premium Wildcard
comodo_multidomain	Sectigo (Comodo) Multidomain
comodo_multidomain_wildcard	Sectigo (Comodo) Multidomain Wildcard