Certum by asseco

# API User Guide

**Wersja 5.10**

# 1. Spis treści

# 2. Wstęp

Program Partnerski Certum oferuje elastyczne i wydajne rozwiązanie oparte o SOAP (Simple Object Access Protocol) pozwalające na składanie zamówień na certyfikaty, sprawdzanie stanu ich realizacji, a w dalszym etapie również zarządzanie certyfikatami bezpośrednio z systemu partnera.

Certum Partner API pozwala na złożenie zamówienia na certyfikat o dowolnym typie (zgodnie z podpisaną umową partnerską) oraz monitorowanie statusu zamówienia w miarę jego przetwarzania. Certum obsługuje proces weryfikacji domeny i adresu email oraz może kontaktować się z klientem partnera w przypadku, gdy niezbędne jest dostarczenie dokumentów.

W ramach umowy z partnerskiej ustalane są między innymi takie kwestie jak:

- produkty, które partner może zmawiać,
- w przypadku certyfikatów personalizowanych – dedykowane polityki dla partnera,
- treści maili wysyłanych automatycznie przez system w procesie wydawania certyfikatów,
- zasady kontaktu Certum z klientami partnera.

## 2.1. Repozytorium API

Niniejsza dokumentacja jest cały czas rozwijana i uzupełniana o nowe informacje oraz metody dodawane do API.

Najnowsza wersja dokumentacji oraz biblioteki dostępna jest zawsze pod adresem:

http://repository.certum.pl/API/

API WSDL:

https://gs.test.certum.pl/service/PartnerApi.wsdl dla środowiska testowego

https://gs.certum.pl/service/PartnerApi.wsdl dla środowiska produkcyjnego

Dodatkowo Certum udostępnia interfejs www dostępny pod adresami:

https://gs.test.certum.pl/muc-api-client/ dla środowiska testowego

https://gs.certum.pl/muc-api-client/ dla środowiska produkcyjnego

# 3. Produkty dostępne przez API

## 3.1. Certyfikaty SSL

### 3.1.1. Commercial SSL

Certyfikaty Commercial SSL to certyfikaty oferowane na 1 rok, w wariancie SSL, MultiDomain SSL oraz Wildcard SSL. Wydanie certyfikatu Commercial SSL wymaga weryfikacji dostępu do domeny. Wynikiem pozytywnej weryfikacji będzie automatyczne wydanie certyfikatu.

### 3.1.2. Trusted SSL

Certyfikaty Trusted SSL to certyfikaty oferowane na 1 rok, w wariancie SSL, MultiDomain SSL oraz Wildcard SSL. Wydanie certyfikatu Trusted SSL wymaga weryfikacji dostępu do domeny oraz dodatkowej weryfikacji Subskrybenta i organizacji.

### 3.1.3. Premium EV SSL

Certyfikaty Premium EV SSL to certyfikaty oferowane na 1 rok, w wariancie SSL i MultiDomain SSL, nie mają dostępnej opcji Wildcard. Wydanie certyfikatu Premium EV SSL wymaga weryfikacji dostępu do domeny oraz dodatkowej weryfikacji Subskrybenta i organizacji.

## 3.2. Certyfikaty Certum S/MIME

**Uwaga:** Od 2023-09-01 wszystkie certyfikaty S/MIME, wystawione po tej dacie, muszą być zgodne z S/MIME Baseline Requirements v1.0.0. Dotychczasowe produkty E-mail ID są wycofane z oferty i zastąpione nowymi produktami Certum S/MIME dostosowanymi do regulacji. Wszystkie zamówienia na dotychczasowe produkty E-mail ID niewystawione do 2023-08-28, zostaną odrzucone. Nie będzie możliwości wydawania, odnawiania i reissue istniejących certyfikatów E-mail ID.

### 3.2.1. Certum S/MIME Mailbox

Certyfikaty Certum S/MIME Mailbox to certyfikaty oferowane w wariancie na 1-2 lata i wystawiane są zawsze dla pojedynczego adresu email. Pozwalają na podpisywanie i szyfrowanie poczty. Wydanie certyfikatu Certum S/MIME Mailbox wymaga weryfikacji adresu email. Wynikiem pozytywnej weryfikacji będzie automatyczne wydanie certyfikatu.

### 3.2.2. Certum S/MIME Individual

Certyfikaty Certum S/MIME Individual to certyfikaty oferowane w wariancie na 1-2 lata i wystawiane są zawsze dla pojedynczego adresu email. Pozwalają na podpisywanie i szyfrowanie poczty. Wydanie certyfikatu Certum S/MIME Individual wymaga weryfikacji adresu email oraz dodatkowej weryfikacji Subskrybenta.

### 3.2.3. Certum S/MIME Sponsor

Certyfikaty Certum S/MIME Sponsor to certyfikaty oferowane w wariancie na 1-2 lata i wystawiane są zawsze dla pojedynczego adresu email. Pozwalają na podpisywanie i szyfrowanie poczty. Wydanie certyfikatu Certum S/MIME Sponsor wymaga weryfikacji adresu email oraz dodatkowej weryfikacji Subskrybenta i organizacji.

### 3.2.4. Certum S/MIME Organization

Certyfikaty Certum S/MIME Organization to certyfikaty oferowane w wariancie na 1-2 lata i wystawiane są zawsze dla pojedynczego adresu email. Pozwalają na podpisywanie i szyfrowanie poczty. Wydanie certyfikatu Certum S/MIME Organization wymaga weryfikacji adresu email oraz dodatkowej weryfikacji organizacji.

## 3.3. Certyfikaty Code Signing

### 3.3.1. Standard Code Signing w chmurze

Certyfikaty Standard Code Signing w chmurze to certyfikaty oferowane w wariancie 1-3 lata. Umożliwiają twórcom podpisanie oryginalnego oprogramowania, a odbiorcom zweryfikowanie integralności oprogramowania oraz tożsamości podpisującego. Wydanie certyfikatu Standard Code Signing w chmurze wymaga dodatkowej weryfikacji Subskrybenta i organizacji.

### 3.3.2. EV Code Signing w chmurze

EV Standard Code Signing w chmurze to certyfikaty oferowane w wariancie 1-3 lata. Umożliwiają twórcom podpisanie oryginalnego oprogramowania, a odbiorcom zweryfikowanie integralności oprogramowania oraz tożsamości podpisującego. Zapewniają eliminację filtra Microsoft SmartScreen. Wydanie certyfikatu EV Code Signing w chmurze wymaga dodatkowej weryfikacji Subskrybenta i organizacji.

## 3.4. Certyfikaty Document Signing w chmurze

Certyfikaty Document Signing w chmurze to certyfikaty oferowane w wariancie 1-3 lata. Umożliwiają podpisywanie dokumentów PDF. Wydanie certyfikatu Document Signing w chmurze wymaga weryfikacji adresu email oraz dodatkowej weryfikacji Subskrybenta i organizacji. Zgodnie z obowiązującymi regulacjami AATL, weryfikacja Subskrybenta musi być zrealizowana metodą F2F lub równoważną.

## 3.5. Lista kodów produktów

Lista kodów dostępnych dla danego partnera konfigurowana jest indywidualnie i zależy od zakresu umowy partnerskiej.

**Uwaga:** Nowe produkty S/MIME mają nowe kody. Kody na dotychczasowe produkty E-mail ID zostaną wyłączone 2023-08-28.

| Nazwa produktu | Ważność w dniach | Wydanie | Odnowienie |
|---|---|---|---|
| Commercial SSL | 365 | 601 | 606 |
| Commercial Wildcard SSL | 365 | 741 | 746 |
| Commercial MultiDomain SSL 300 Domen | 365 | 931 | 936 |
| Commercial MultiDomain Wildcard SSL 300 Domen | 365 | 961 | 966 |
| Trusted SSL | 365 | 631 | 636 |
| Trusted Wildcard SSL | 365 | 681 | 686 |
| Trusted MultiDomain SSL 300 Domen | 365 | 921 | 926 |
| Trusted MultiDomain Wildcard SSL 300 Domen | 365 | 971 | 976 |
| Premium EV SSL | 365 | 641 | 646 |
| Premium EV MultiDomain SSL 300 Domen | 365 | 981 | 986 |
| Certum S/MIME Mailbox | 365 | 501 | 506 |
| Certum S/MIME Mailbox | 730 | 502 | 507 |
| Certum S/MIME Individual | 365 | 511 | 516 |
| Certum S/MIME Individual | 730 | 512 | 517 |
| Certum S/MIME Sponsor | 365 | 521 | 526 |
| Certum S/MIME Sponsor | 730 | 522 | 527 |
| Certum S/MIME Organization | 365 | 531 | 536 |
| Certum S/MIME Organization | 730 | 532 | 537 |
| Standard Code Signing w chmurze | 365 | 831 | 836 |
| Standard Code Signing w chmurze | 730 | 832 | 837 |
| Standard Code Signing w chmurze | 1095 | 833 | 838 |
| EV Code Signing w chmurze | 365 | 316 | 321 |
| EV Code Signing w chmurze | 730 | 317 | 322 |
| EV Code Signing w chmurze | 1095 | 318 | 323 |
| Document Signing w chmurze | 365 | 281 | 286 |
| Document Signing w chmurze | 730 | 282 | 287 |
| Document Signing w chmurze | 1095 | 283 | 288 |

# 4. Proces zamawiania i wystawiania certyfikatów

## 4.1. Informacje dotyczące wydawania certyfikatów

Certyfikaty jakie można zamawiać przez API dzielą się na kilka typów: certyfikaty DV wystawiane automatycznie, certyfikaty IV, OV i EV. Typy produktów są rozróżniane ze względu na:

- limit gwarancji finansowych,
- dane zawarte w certyfikacie,
- proces wydania,
- obowiązek podania dodatkowych danych przez Web Service.

W niniejszym rozdziale zawarte są przykładowe realizacje procesu zamawiania i wystawiania certyfikatów, oraz innych informacji dotyczących składania zamówień z wykorzystaniem API.

## 4.2. Wymagalność pól w certyfikatach

W zależności od typu certyfikatu wymagane są inne dane, które trzeba podać w CSR lub sekcji danych do certyfikatu. Poniżej tabela zawierająca zestawienie pól wymaganych i opcjonalnych dla poszczególnych typów certyfikatów.

**Uwaga:** Nowe produkty S/MIME mają nowe pola imię i nazwisko oraz inną wymagalność pól w porównaniu z dotychczasowymi produktami E-mail ID.

**W –** wymagane
**W* –** wymagane jedno z dwóch
**O –** opcjonalne
**A –** wstawiane automatycznie

| Rodzaj certyfikatu | CN | GN | SN | O | L | SP | C | E | Org. identifier | SN | BC | ST | P | JoILN | JoISoPN | JoISoCN | SAN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Commercial SSL<br>Commercial Wildcard SSL<br>Commercial MultiDomain SSL<br>Commercial MultiDomain Wildcard SSL | W | | | | | | | | | | | | | | | | W |
| Trusted SSL<br>Trusted Wildcard SSL<br>Trusted MultiDomain SSL<br>Trusted MultiDomain Wildcard SSL | W | | | W | W* | W* | W | | | | | | | | | | W |
| Premium EV SSL<br>Premium EV MultiDomain SSL | W | | | W | W* | W* | W | | | W | W | O | O | W* | W* | W | W |
| Certum S/MIME Mailbox | A | | | | | | | W | | | | | | | | | A |
| Certum S/MIME Individual | W | W | W | | | | | W | | | | | | | | | A |
| Certum S/MIME Sponsor | W | W | W | W | W | O | W | W | A | | | | | | | | A |
| Certum S/MIME Organization | W | | | W | W | O | W | W | A | | | | | | | | A |
| Standard Code Signing w chmurze | W | | | W | W* | W* | W | | | | | | | | | | |
| EV Code Signing w chmurze | W | | | W | W* | W* | W | | | W | W | O | O | W* | W* | W | |
| Document Signing w chmurze | W | | | W | W* | W* | W | W | | | | | | | | | A |

Zawartość poszczególnych pól

| Pole | Nazwa | Opis pola |
|---|---|---|
| **CN** | commonName | Nazwa powszechna. Dla certyfikatów SSL jest to pierwsza z domen zawartych w certyfikacie. Dla pozostałych certyfikatów jest to najczęściej imię i nazwisko właściciela certyfikatu. |
| **GN** | givenName | Imię lub imiona Subskrybenta. |
| **SN** | surname | Nazwisko Subskrybenta. |
| **O** | organization | Nazwa organizacji. |
| **L** | locality | Miejscowość – siedziba podmiotu, dla którego wystawiany jest certyfikat. |
| **SP** | state | Województwo – siedziba podmiotu, dla którego wystawiany jest certyfikat. Pole jest dodatkowo walidowane gdy C posiada wartość PL. |
| **C** | country | Kraj – siedziba podmiotu, dla którego wystawiany jest certyfikat. Pole jest walidowane z listą dozwolonych wartości dwuliterowych kodów ISO. |
| **E** | email | Adres email |
| **Org. Id.** | organizationIdentifier | Numer rejestrowy podmiotu, zgodny z zapisem wymaganym przez Baseline, wykorzystywany wyłącznie w certyfikatach S/MIME. |
| **SN** | serialNumber | Numer rejestrowy podmiotu, wykorzystywany wyłącznie w certyfikatach EV |
| **BC** | businessCategory | Kategoria biznesowa – w zależności od działalności podmiotu, dla którego wystawiany jest certyfikat, wykorzystywane wyłącznie w certyfikatach EV. Pole jest walidowane z listą dozwolonych wartości. |
| **ST** | streetAddress | Adres – adres siedziby podmiotu, dla którego wystawiany jest certyfikat, wykorzystywany wyłącznie w certyfikatach EV. |
| **P** | postalCode | Kod pocztowy – kod pocztowy siedziby podmiotu, dla którego wystawiany jest certyfikat, wykorzystywany wyłącznie w certyfikatach EV. |
| **JoILN** | Jurisdiction of Incorporation Locality Name | Miejscowość – miejscowość rejestracji podmiotu, dla którego wystawiony jest certyfikat, wykorzystywana wyłącznie w certyfikatach EV. |
| **JoISoPN** | Jurisdiction of Incorporation State or Province Name | Województwo – województwo rejestracji podmiotu, dla którego wystawiany jest certyfikat. – wykorzystywane wyłącznie w certyfikatach EV. Pole jest dodatkowo walidowane gdy C posiada wartość PL. |
| **JoISoCN** | Jurisdiction of Incorporation Country Name | Kraj rejestracji podmiotu, dla którego wystawiony jest certyfikat, wykorzystywany wyłącznie w certyfikatach EV. Pole jest walidowane z listą dozwolonych wartości dwuliterowych kodów ISO. |
| **SAN** | Subject Alternative Name | W tym polu dodawane są wszystkie domeny zawarte w certyfikacie. |

Jeśli w polu C lub polu joISoCN podana jest wartość PL, odpowiednio pola SP oraz joISoPN są walidowane z następującym słownikiem:

- dolnośląskie
- kujawsko-pomorskie
- lubelskie
- lubuskie
- łódzkie
- małopolskie
- mazowieckie
- opolskie
- podkarpackie
- podlaskie
- pomorskie
- śląskie
- świętokrzyskie
- warmińsko-mazurskie
- wielkopolskie

- zachodniopomorskie

Dla pozostałych wartości pola C i joISoCN województwa nie są dodatkowo walidowane.

### 4.2.1. Unikalność pola customer w zamówieniu

Certum rozróżnia użytkowników końcowych po polu **`customer`**. Oznacza to, że każde zamówienie pochodzące od innego klienta powinno być identyfikowane różną wartością pola **`customer`**. Pole nie musi zawierać rzeczywistego loginu, może to być numer zamówienia z zewnętrznego systemu partnera, lub inny identyfikator, unikalny dla danego klienta.

W przypadku produktów w chmurze, pole **`customer`** musi zawierać adres e-mail będący loginem użytkownika do usługi SimplySign.

Identyfikator użytkownika końcowego w polu **`customer`** nie może być loginem partnera.

**Uwaga:** W przypadku zastosowania jednej wartości dla pola **`customer`** wszystkie zamówienia będą traktowane jak zamówienia składane przez tego samego użytkownika co może mieć wpływ na proces wydawania certyfikatów.

### 4.2.2. Metody weryfikacji domeny dla certyfikatów SSL

Certum udostępnia trzy metody automatycznej weryfikacji domeny z certyfikatu SSL:

1. Metoda weryfikacji domeny za pomocą adresu email administratora domeny
   - Nazwa metody w API: ADMIN
   - Dopuszczalne adresy email, na które może zostać wysłany link weryfikacyjny to: admin@*domena.com*, administrator@*domena.com*, hostmaster@*domena.com*, webmaster@*domena.com*, postmaster@*domena.com*. Należy się upewnić, że jeden z tych adresów email jest utworzony dla każdej weryfikowanej domeny.
   - Emaile wysyłane są na adresy utworzone na podstawie podanego w elemencie **`approverEmailPrefix`** prefixu oraz listy z domen z zamówienia.
   - Wysłanych będzie tyle maili weryfikacyjnych, ile domen podano w zamówieniu.
   - Nie można wyłączyć wysyłania maili weryfikacyjnych dla metody ADMIN.
   - Aby ukończyć weryfikację za pomocą adresu email administratora domeny, należy kliknąć w link zawarty w mailu.

2. Metoda weryfikacji domeny przez umieszczenie pliku na serwerze
   - Nazwa metody w API: FILE
   - Email wysyłany jest na adres podany w **`approverEmail`**.
   - Wysłany będzie jeden mail z jednym kodem weryfikacyjnym dla wszystkich domen z zamówienia.
   - Aby system nie wysyłał wiadomości weryfikacji FILE należy wyłączyć wysyłanie maili weryfikacyjnych na koncie partnera.
   - Gdy wysyłanie maili weryfikacyjnych jest wyłączone, **`quickOrder`** zwraca kod weryfikacyjny.
   - W otrzymanym mailu podana jest nazwa pliku, kod weryfikacyjny do umieszczenia w pliku, oraz link, w który należy kliknąć po wykonaniu opisanych czynności.
   - Aby ukończyć weryfikację należy umieścić w katalogu: **`/.well-known/pki-validation`** weryfikowanej domeny pliku o określonej nazwie, w którego treści musi być zawarty kod weryfikacyjny zakończony suffixem **`-certum.pl`** i kliknąć w link z maila lub wykonać **`perfomSanVerification`**.

**Uwaga:** Od 2021-12-01, w wyniku głosowania SC45, metoda FILE nie może być wykorzystywana do wydawania certyfikatów Wildcard SSL oraz nie może być wykorzystywana do weryfikacji domen podrzędnych na podstawie zweryfikowanej domeny głównej. W wyniku tej zmiany nie będzie można złożyć zamówienia na certyfikat Multidomenowy zawierający jednocześnie domenę Wildcard i adres IP.

3. Metoda weryfikacji domeny przez umieszczenie kodu w rekordzie DNS
    - Nazwa metod w API:
        - DNS_TXT – umieszczenie kodu w rekordzie TXT dla nazwy domeny
        - DNS_CNAME – umieszczenie kodu zakończonego suffixem **`.certum.pl`** w rekordzie CNAME dla nazwy domeny
        - DNS_TXT_PREFIX – umieszczenie kodu w rekordzie TXT dla nazwy domeny poprzedzonej prefiksem **`_certum`** (np. _certum.twojadomena.pl)
        - DNS_CNAME_PREFIX – umieszczenie kodu zakończonego suffixem **`.certum.pl`** w rekordzie CNAME dla nazwy domeny poprzedzonej prefiksem **`_certum`** (np. _certum.twojadomena.pl)

**Uwaga:** Wprowadzenie nowych metod weryfikacji opartych o rekordy DNS wymusiło dodanie nowych nazw metod: DNS_CNAME, DNS_TXT_PREFIX i DNS_CNAME_PREFIX. Dotychczasowa nazwa metody określanej jako DNS została dostosowana do przyjętej konwencji i zmieniona na DNS_TXT. Nazwa DNS jest wspierana w tej wersji API i działa identycznie jak DNS_TXT, można ją stosować, ale rekomendujemy jej zmianę na DNS_TXT. Wartość DNS docelowo zostanie usunięta z API.

- Email wysyłany jest na adres podany w **`approverEmail`**.
- Wysłany będzie jeden mail z jednym kodem weryfikacyjnym dla wszystkich domen z zamówienia.
- Aby system nie wysyłał wiadomości weryfikacji DNS należy wyłączyć wysyłanie maili weryfikacyjnych na koncie partnera.
- Gdy wysyłanie maili weryfikacyjnych jest wyłączone, **`quickOrder`** zwraca kod weryfikacyjny.
- W otrzymanym mailu podany jest kod weryfikacyjny oraz link, w który należy kliknąć po utworzeniu rekordu DNS.
- Aby ukończyć weryfikację należy umieścić kod w rekordzie DNS zgodnie z wybraną nazwą metody i kliknąć w link z maila lub wykonać **`perfomSanVerification`**.
- Należy pamiętać że aktualizacja wpisów w DNS może trwać do 24 godzin.

**Uwaga:** W niektórych przypadkach, np. w przypadku popularnych domen, lub domen dla instytucji takich jak bank, Certum może zażądać przesłania dodatkowych dokumentów w celu pełniejszej weryfikacji zamówienia.

### 4.2.3. Metody weryfikacji Subskrybenta i organizacji

Po złożeniu zamówienia na certyfikat, system wysyła wiadomość o przyjęciu zamówienia z informacjami o dalszych krokach zgodnie z produktem dla którego złożono zamówienie – wiadomość wysyłana jest na adres podany w elementach **`orderParameters/email`** lub **`requestorInfo/email`**. Aby system nie wysyłał wiadomości o przyjęciu zamówienia należy wyłączyć wysyłanie maili informacyjnych na koncie partnera.

Na podstawie danych w sekcji **`organizationInfo`** nastąpi weryfikacja danych organizacji zawartych w certyfikacie. Informacje o organizacji są weryfikowane w publicznie dostępnych rejestrach np. KRS, GUS, CEiDG, DUNS. Ten krok jest wykonywany przez Certum i nie wymaga zaangażowania Subskrybenta. Jeśli organizacja nie figuruje w rejestrze, należy dostarczyć ważny dokument rejestrowy firmy wykorzystując **`verifyOrder`**, podając jako typ dokumentu **`ORGANIZATION`**.

Na podstawie danych w sekcji **`requestorInfo`** nastąpi potwierdzenie tożsamości Subskrybenta. Potwierdzenie przeprowadzane jest z wykorzystaniem dokumentów tożsamości lub systemu ARIADNEXT. W przypadku ARIADNEXT na adres podany w **`requestorInfo`** zostanie wysłana wiadomość zawierająca link pozwalający rozpocząć automatyczne potwierdzenie tożsamości. Jeśli tożsamość ma być potwierdzona na podstawie dokumentów, należy dostarczyć ważny dokument potwierdzający tożsamość Subskrybenta wykorzystując **`verifyOrder`**, podając jako typ dokumentu **`APPLICANT`**.

Dodatkowo jeżeli osoba występująca o certyfikat nie jest upoważniona do samodzielnego reprezentowania danej instytucji, należy dostarczyć ważny dokument świadectwa pracy lub upoważnienia wykorzystując **`verifyOrder`**, podając jako typ dokumentu **`AUTHORIZATION`**.

W uzasadnionych przypadkach, zespół Certum może poprosić o dodatkowe dokumenty niezbędne do prawidłowej weryfikacji. Należy je dostarczyć wykorzystując **`verifyOrder`**, podając jako typ dokumentu **`ADDITIONAL`**.

Aby sprawdzić jaki jest status weryfikacji dokumentów, dostępna jest metoda **`getDocumentsList`**, która zwraca listę dokumentów wraz z ich statusami i datami wygaśnięcia takiej weryfikacji.

Aby sprawdzić jaki jest status weryfikacji Subskrybenta i organizacji, dostępna jest metoda **`getOrderState`**, która zwraca statusy powiązane z weryfikacją dokumentów, odpowiednio **`ORGANIZATION`**, **`APPLICANT`** i **`AUTHORIZATION`**. Jeśli na podstawie dostarczonych dokumentów dokonano weryfikacji, status zmieni się z **`REQUIRED`** na **`VERIFIED`**.

### 4.2.4. Dodatkowe opcje konfiguracyjne

Aby partner mógł korzystać z API, niezbędne jest skonfigurowanie następujących danych konta w systemie Certum:

- Adres IP, z którego łączy się partner.
- Kody produktów, które partner może zamawiać.
- Domyślny język do wysyłania powiadomień.
- Konfiguracja wysyłania maili weryfikacyjnych dla weryfikacji DNS i FILE – wszystkie wiadomości email są podpisane cyfrowo.
    - Istnieje możliwość wyłączenia wysyłki maila weryfikującego kontrolę Subskrybenta nad domeną metodami DNS i FILE dla pojedynczych zamówień, korzystając z parametru **`verificationNotificationEnabled`** w elemencie **`SanApprovers`**, jednak parametr ten mysi być ustawiany osobno dla każdego zamówienia.
- Konfiguracja wysyłania maili informacyjnych – wszystkie wiadomości email są podpisane cyfrowo.
    - Przyjęcie zamówienia – wysyłany po złożeniu zamówienia w systemie Certum.
    - Nieukończona weryfikacja zamówienia – email przypominający o weryfikacji zamówienia, wysyłany jednorazowo po 23 dniach od złożenia zamówienia. Kodeks Postępowania Certyfikacyjnego określa po jakim czasie zamówienie będzie odrzucone jeśli subskrybent nie

dopełnił formalności.

- Wydanie certyfikatu – wysyłany po wydaniu certyfikatu.
- Unieważnienie certyfikatu – wysyłany po unieważnieniu certyfikatu.
- Wygasanie certyfikatu – email przypominający o zbliżającym się terminie wygaśnięcia certyfikatu (wysyłany na 30, 14, 7 i 1 dzień przed upływem ważności certyfikatu). Odnowienie certyfikaty wyłącza wysyłkę maili przypominających o wygasaniu.
- Wygaśnięcie certyfikatu – email wysyłany po wygaśnięciu certyfikatu.

**Uwaga:** Jeśli wysyłka maili przez Certum jest wyłączona, partner jest zobowiązany do informowania Subskrybenta o powyższych czynnościach samodzielnie, przy czym należy pamiętać, że w przypadku wysyłania przez partnera wiadomości email do swoich Subskrybentów, wiadomości te, zgodnie z wymogami WebTrustSM/TM 2.0, **muszą być podpisane cyfrowo.**

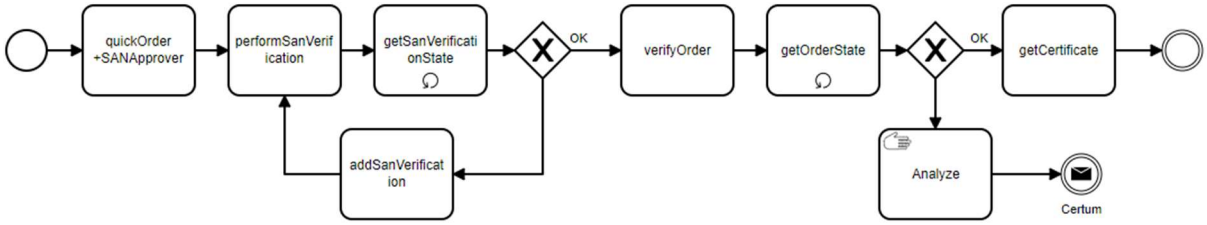
Elementy dodatkowe, których konfiguracja jest opcjonalna (w przypadku gdy nie zostaną skonfigurowane stosowane są standardowe szablony Certum)

- Dedykowany nagłówek i stopka wiadomości email wysyłanych przez system Certum.
- Dedykowane treści wiadomości email wysyłanych przez system Certum.

## 4.3. Proces zamawiania certyfikatów Trusted SSL i Premium EV SSL

### 4.3.1. Złożenie zamówienia

Dla certyfikatów Trusted SSL i Premium EV SSL w żądaniu **quickOrder** konieczna jest obecność sekcji **SanApprover** oraz **SANEntries** a także **requestorInfo** i **organizationInfo**.




### 4.3.2. Ukończenie weryfikacji

Po złożeniu zamówienia na certyfikat system wysyła dwa typy wiadomości email:

- wiadomość o przyjęciu zamówienia z informacjami o dalszych krokach dotyczących weryfikacji Subskrybenta i organizacji,
- wiadomość dla wybranej metody: ADMIN, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX lub FILE zgodnie opisem weryfikacji domeny dla certyfikatów SSL.

Dla metod DNS i FILE otrzymany kod należy umieścić odpowiednio w konfiguracji DNS lub w pliku na serwerze, a następnie należy zainicjować weryfikację wywołując **perfomSanVerification.** Dla metody ADMIN należy kliknąć w link zawarty w mailu.

Status weryfikacji domen dla zamówienia można sprawdzić wywołując **getSanVerificationState**. Metoda zwraca nie tylko status weryfikacji dla każdej domeny, ale również informacje o tym jakie problemy wystąpiły. Jeśli odpowiedź zawiera informację o błędach weryfikacji, należy usunąć ich przyczynę, a następnie ponownie wywołać metodę **perfomSanVerification**.

W przypadku problemów z weryfikacją, wygaśnięcia kodu lub zmiany metody weryfikacji można wygenerować nowy kod wywołując **addSanVerification**.

W przypadku wymaganych dokumentów, należy je dostarczyć wykorzystując **verifyOrder**.

### 4.3.3. Uzyskanie certyfikatu

Przy pomocy metody **getOrderState** można monitorować jakie weryfikacje są wymagane dla zamówienia oraz jaki jest ich status. Kiedy status zamówienia zmieni się na **ENROLLED**, można pobrać wystawiony certyfikat.

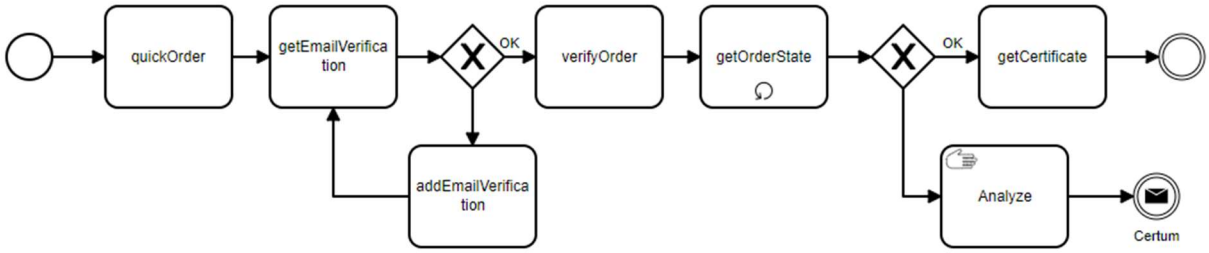
W przypadku certyfikatów SSL wymagane będzie zweryfikowanie domen, rozdzielone na dwie weryfikacje: **SYSTEM** i **DOMAIN**. Weryfikacja **SYSTEM** przeprowadzana jest automatycznie przez systemy Certum i nie trzeba jej wywoływać przez API. Weryfikacja **DOMAIN** to weryfikacja domen w certyfikacie omówiona w poprzednim punkcie. Dzięki metodzie **getSanVerificationState** można zdiagnozować problemy występujące podczas obu weryfikacji.

Poza certyfikatem wystawionym dla domeny należy pamiętać o zainstalowaniu na serwerze certyfikatu głównego CA (rootCA) i pośrednich (subCA) – za pomocą **getCertificate** możliwe jest pobranie tych wszystkich certyfikatów w formacie PEM.

## 4.4. Proces zamawiania certyfikatów Certum S/MIME Sponsor

### 4.4.1. Złożenie zamówienia

Dla certyfikatów Certum S/MIME Sponsor w żądaniu **`quickOrder`** konieczna jest obecność sekcji **`requestorInfo`** i **`organizationInfo`**. Obecność sekcji **`SanApprover`** oraz **`SANEntries`** będzie traktowana jako błąd.




### 4.4.2. Ukończenie weryfikacji

Po złożeniu zamówienia na certyfikat system wysyła dwa typy wiadomości email:

- wiadomość o przyjęciu zamówienia z informacjami o dalszych krokach dotyczących weryfikacji Subskrybenta i organizacji,
- wiadomość zawierająca link weryfikacyjny adres podany w polu **`orderParameters/email`**.

Aby ukończyć weryfikację adresu email, należy kliknąć w link zawarty w mailu. Nie można wyłączyć wysyłania maili weryfikacyjnych dla pola E (email).

Status weryfikacji maila dla zamówienia można sprawdzić wywołując **`getEmailVerification.`**

W przypadku problemów z weryfikacją można ponowić wysłanie maila wywołując **`addEmailVerification`**.

W przypadku wymaganych dokumentów, należy je dostarczyć wykorzystując **`verifyOrder`**.

### 4.4.3. Uzyskanie certyfikatu

Przy pomocy metody **`getOrderState`** można monitorować jakie weryfikacje są wymagane dla zamówienia oraz jaki jest ich status. Kiedy status zamówienia zmieni się na **`ENROLLED`**, można pobrać wystawiony certyfikat.

Wystawiony certyfikat można pobrać za pomocą **`getCertificate`**.

## 4.5. Proces zamawiania certyfikatów Standard Code Signing w chmurze

Proces wygląda analogicznie jak proces dla Certum S/MIME Sponsor, z tą różnicą, że w certyfikacie Standard Code Signing w chmurze nie ma pola email, czyli jego weryfikacja nie będzie potrzebna.

Ponieważ to jest produkt w chmurze, pole **`customer`** musi zawierać adres e-mail będący loginem użytkownika do usługi SimplySign.

Przy pomocy metody **`getOrderState`** można monitorować jakie weryfikacje są wymagane dla zamówienia oraz jaki jest ich status. Kiedy status zamówienia zmieni się na **`ENROLLED`**, można pobrać wystawiony certyfikat. W przypadku certyfikatów Standard Code Signing w chmurze, jeśli zweryfikowanie **`EMAIL`** nie będzie wymagane, dla tego pola zostanie zwrócony status **`NOT_REQUIRED`**.

Certyfikaty Standard Code Signing w chmurze nie mogą być wydawane w sposób automatyczny.

## 4.6. Proces zamawiania certyfikatów Document Signing w chmurze

Proces wygląda analogicznie jak proces dla Certum S/MIME Sponsor.

Ponieważ to jest produkt w chmurze, pole **`customer`** musi zawierać adres e-mail będący loginem użytkownika do usługi SimplySign.

Przy pomocy metody **`getOrderState`** można monitorować jakie weryfikacje są wymagane dla zamówienia oraz jaki jest ich status. Kiedy status zamówienia zmieni się na **`ENROLLED`**, można pobrać wystawiony certyfikat. W przypadku certyfikatów Document Signing w chmurze wymagane będzie zweryfikowanie **`EMAIL`**.

Certyfikaty Document Signing w chmurze nie mogą być wydawane w sposób automatyczny.

W przypadku certyfikatów Document Signing w chmurze, tożsamość Subskrybenta musi być zweryfikowana metodą F2F lub równoważną, nie ma możliwości przeprowadzenia weryfikacji tożsamości Subskrybenta na podstawie dokumentów.

# 5. Przegląd metod WebService

## 5.1. Zamówienie certyfikatu

### 5.1.1. Pobranie listy dostępnych produktów

Za pomocą **`getProductList`** można pobrać listę dostępnych kodów produktów, wraz z szczegółowymi informacjami o produktach.

### 5.1.2. Zamówienie nowego certyfikatu

Za pomocą **`quickOrder`** przekazywane są wszystkie informacje niezbędne do złożenia zamówienia:

- identyfikator klienta,
- kod produktu,
- dane do certyfikatu czyli CSR
- dane pozwalające na weryfikację Subskrybenta i organizacji w przypadku certyfikatów IV, OV i EV.
- w rozszerzeniu SAN (ang. Subject Alternative Name), możliwe jest umieszczenie w certyfikacie wielu domen, które ma zabezpieczać (w przypadku certyfikatów wielodomenowych), oraz opcji z www dla certyfikatów zabezpieczających jedną domenę.
- wskazana jedna metoda weryfikacji dotyczy wszystkich domen zawartych w zamówieniu.

W przypadku wszystkich certyfikatów multidomenowych, należy podać jawnie wszystkie domeny jakie mają być umieszczone w rozszerzeniu SANEntry, system dla takich certyfikatów nie dodaje automatycznie żadnych dodatkowych wpisów.

### 5.1.3. Weryfikacja poprawności danych w zamówieniu

Za pomocą metody **`validateOrderParameters`** sprawdzane są wszystkie dane zawarte w zamówieniu. Sprawdzeniu podlegają zgodność danych zawartych w CSR z typem certyfikatu, oraz zakres dostarczonych danych. W szczególności sprawdzane są:

Login partnera:

- poprawność loginu i hasła,
- aktywność konta.

Zamówienie:

- czy identyfikator zamówienia jest unikalny w bazie i poprawnie skonstruowany,
- czy jest podany identyfikator klienta,
- czy produkt jest dostępnych dla partnera,
- czy data wygaśnięcia certyfikatu mieści się w liczbie dni, jakie są przypisane dla danego kodu produktu, jeśli nie ma podanego zakresu dat certyfikat będzie wystawiony z datą początkową równą momentowi wystawienia i datą końca maksymalną dla danego produktu.

CSR:

- czy klucz nie występuje ani na blackliście ani na liście wykorzystanych kluczy,
- czy wypełnione są wszystkie wymagane pola – wymagalność pól jest określana w ramach typu certyfikatu,
- czy pola mają dozwolony format,
- weryfikacja poprawności danych dotyczących rozszerzenia SAN,
- w odpowiedzi metoda zwraca dane jakie trafią do certyfikatu uwzględniając zarówno dane z CSR jak i dane z żądania nadpisujące dane z CSR.

### 5.1.4. Reissue – ponowne wydanie certyfikatu

Ponowne wydanie jest dostępne dla wszystkich certyfikatów w okresie ich ważności. Za pomocą **`reissueCertificate`** można ponowne wydać certyfikat na nowe klucze i te same dane z zachowaniem daty końca ważności bazowego certyfikatu.

**Uwaga:** W wyniku głosowania CSC13, związanego z zapewnieniem generowania klucza w sprzętowym module kryptograficznym, który jest zgodny co najmniej ze standardem FIPS 140-2 Level 2 lub Common Criteria EAL 4+, wyłączono możliwość wykonania reissue dla certyfikatów Code Signing wystawianych na karty fizyczne.

Wydanie nowego certyfikatu w wyniku reissue, spowoduje automatyczne unieważnienie poprzedniego certyfikatu po upływie 14 dni od wydania. W konsekwencji Subskrybent zawsze posiada jeden ważny certyfikat.

### 5.1.5. Odnowienie certyfikatu

Za pomocą **`renewCertificate`** można odnowić, czyli wydać nowy certyfikat na nowe klucze i te same dane z nowym okresem ważności. Dane w nowym certyfikacie zostaną przepisane z odnawianego certyfikatu, nie można ich zmienić składając zamówienie na odnowienie.Status złożonego zamówienia

### 5.1.6. Sprawdzenie statusu weryfikacji zamówienia

Za pomocą **`getOrderState`** możliwe jest pobranie szczegółowych informacji o weryfikacji dla danego identyfikatora zamówienia. Na podstawie dostarczonego identyfikatora zamówienia można ustalić:

- czy weryfikacja wszystkich domen została pomyślnie ukończona,
- czy jest potrzebna weryfikacja adresu email,
- czy w danym zamówieniu weryfikacji podlegają dane Subskrybenta i organizacji,
- czy certyfikat został wystawiony.

### 5.1.7. Pobranie danych zamówienia

Za pomocą **`getOrderByOrderID`** możliwe jest pobranie pojedynczego zamówienia dla danego identyfikatora zamówienia. Opcjonalnie można pobrać dodatkowe dane o zamówieniu i powiązanych z nim certyfikatach.

### 5.1.8. Anulowanie zamówienia

Za pomocą **`cancelOrder`** możliwe jest anulowanie zamówienia. Można anulować wyłącznie zamówienie złożone ze swojego konta. Zamówienie zostanie anulowane, jeżeli certyfikat nie został wydany. Jeśli certyfikat został wystawiony, nie można zmienić statusu zamówienia, należy unieważnić wystawiony certyfikat. Unieważnienie certyfikatu nie powoduje anulowania zamówienia.

## 5.2. Weryfikacja domeny – certyfikaty SSL

### 5.2.1. Pobranie szczegółowego statusu weryfikacji domen

Za pomocą **`getSanVerificationState`** możliwe jest pobranie statusów weryfikacji wszystkich domen dla danego zamówienia wraz z informacjami o problemach z weryfikacją po stronie klienta, oraz dodatkowych problemach dotyczących domeny, które mogą zablokować wydanie certyfikatu jak niepoprawny wpis CAA czy obecność domeny na listach Phishingowych. W przypadku pozytywnej weryfikacji dodatkowe informacje nie są zwracane.

### 5.2.2. Wygenerowanie nowych weryfikacji domen

Za pomocą metody **`addSanVerification`** możliwe jest utworzenie nowych kodów weryfikacyjnych. Metoda pozwala na utworzenie dowolnej liczby weryfikacji tego samego typu, jak również tworzenie weryfikacji nowego typu dla zamówienia. Tworzenie nowego kodu weryfikacyjnego nie dezaktywuje poprzednich kodów.

### 5.2.3. Uruchomienie weryfikacji domen w zamówieniu

Za pomocą **`performSanVerification`** możliwe jest uruchomienie procesu asynchronicznej weryfikacji wszystkich domen z zamówienia dla metod DNS i FILE. Aby uzyskać informację o wyniku weryfikacji należy skorzystać z metody **`getSanVerificationState`**.

## 5.3. Weryfikacja pola E (email) – certyfikaty S/MIME i Document Signing w chmurze

### 5.3.1. Wysłanie maila weryfikacyjnego dla pola E (email)

Za pomocą **`addEmailVerification`** możliwe jest wysłanie maila z linkiem weryfikacyjnym na adres z pola E (email) umieszczonego w certyfikacie. Metoda pozwala na wysłanie dowolnej ilości weryfikacji. Weryfikacja pola email dotyczy certyfikatów S/MIME i Document Signing w chmurze.

### 5.3.2. Pobranie statusu weryfikacji dla pola E (email)

Za pomocą **`getEmailVerification`** możliwe jest pobranie statusu weryfikacji adresu z pola E (email) umieszczonego w certyfikacie. Weryfikacja pola email dotyczy certyfikatów S/MIME i Document Signing w chmurze.

## 5.4. Weryfikacja Subskrybenta i organizacji – certyfikaty IV, OV i EV

### 5.4.1. Dodanie dokumentów

Za pomocą **`verifyOrder`** możliwe jest dodanie do zamówienia dokumentów, które umożliwią weryfikację zamówienia i wydanie certyfikatu. Dokumenty mogą być wymagane w przypadku składania zamówienia na certyfikat IV, OV lub EV.

Metoda dodawania dokumentów jest ograniczona kilkoma warunkami:

- Dokumenty można dodać tylko do złożonego zamówienia, nie można dodać dokumentu nie powiązanego z żadnym zamówieniem.
- Podczas jednego wywołania metody istnieje możliwość dodania dokumentu składającego się z kilku plików (np. każda strona dokumentu zeskanowana w osobnym pliku).
- Nie ma możliwości usuwania lub zmieniania dodanych wcześniej dokumentów i plików.
- Dla nowych zamówień oraz dla certyfikatów odnawianych dokumenty oraz informacje z rejestrów publicznych nie mogą być starsze niż 13 miesięcy.
- Dokumenty autoryzujące, niezależnie czy są terminowe czy nie – pozostają ważne przez 13 miesięcy od daty wydania.

## 5.5. Status wydanego certyfikatu

### 5.5.1. Pobranie certyfikatu

Za pomocą **`getCertificate`** możliwe jest pobranie certyfikatu w formacie PEM. Poza certyfikatem użytkownika zwracane są wszystkie certyfikaty pośrednie (subCA) oraz certyfikat nadrzędny (rootCA) również w formacie PEM. W przypadku istnienia certyfikatów reissue zwracany jest najnowszy aktywny certyfikat dla danego identyfikatora zamówienia.

### 5.5.2. Unieważnienie certyfikatu

Za pomocą **`revokeCertificate`** możliwe jest unieważnienie certyfikatu. Można unieważnić wyłącznie certyfikaty wygenerowane ze swojego konta. Certyfikat można unieważnić w okresie jego ważności.

## 5.6. Raporty

### 5.6.1. Raport zamówień złożonych w danym okresie czasu

Za pomocą **`getOrdersByDateRange`** możliwe jest pobranie informacji o zamówieniach i certyfikatach, (jeśli zostały wystawione) dla danego okresu czasu. Opcjonalnie można pobrać dodatkowe dane o zamówieniu i powiązanych z nim certyfikatach. Wyniki są stronicowane, na jednej stronie zwracana jest informacja o maksymalnie 100 zamówieniach.

### 5.6.2. Raport zamówień, których status uległ zmianie w danym okresie czasu

Za pomocą **`getModifiedOrders`** możliwe jest pobranie informacji o zamówieniach i certyfikatach, (jeśli zostały wystawione), których status uległ zmianie w zadanym okresie. Opcjonalnie można pobrać dodatkowe dane o zamówieniu i powiązanych z nim certyfikatach. Wyniki są stronicowane, na jednej stronie zwracana jest informacja o maksymalnie 100 zamówieniach.

### 5.6.3. Raport wygasających certyfikatów

Za pomocą **`getExpiringCertificates`** możliwe jest pobranie listy certyfikatów wygasających w najbliższym czasie – certyfikaty wygasające w zakresie od 1-30 dni.

# 6. Struktura WebService

W poniższej dokumentacji zastosowane jest następujące oznaczenie:

```
Pola wymagane - minimalny zestaw danych dla żądania i odpowiedzi
Pola opcjonalne
Pola dodane w bieżącej wersji
Pola które będą usuwane w kolejnych wersjach
Pola które zostały usunięte w bieżącej wersji
```

## 6.1. Nagłówki żądań

Każde żądanie wysyłane do API wymaga podania danych autoryzacyjnych jak login i hasło.

```
<requestHeader>
  <authToken>
    <userName>255 String
    <password>255 String
  </authToken>
</requestHeader>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **userName** | TAK | 255 String | Identyfikator partnera ustalony z Certum, konto w SSO. |
| **password** | TAK | 255 String | Hasło zgodne z hasłem w SSO. |

Każda odpowiedź zwraca nagłówek z kodem potwierdzającym wykonanie operacji, lub kodami błędów pozwalającymi zidentyfikować problem. Dane dotyczące stronicowania wyników dotyczą wyłącznie żądań zwracających raporty.

W przypadku wystąpienia błędów, dane opisane w poszczególnych Response dla metod API nie będą zwracane. Lista kodów błędów znajduje się w osobnym rozdziale.

```
<responseHeader>
  <successCode>3
  <errors>
    <error>
      <errorCode>
    </error>
  </errors>
  <currentPage>1..100
  <pagesCount>1..100
  <returnCount>5
  <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
</responseHeader>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **successCode** | TAK | 3 | Kod 0 oznacza prawidłowe przyjęcie zamówienia. Kod 1 i 3 oznaczają błąd. |
| **errorCode** | NIE | 5 String | Kody błędów jakie wystąpiły podczas wykonywania żądania. |
| **currentPage** | NIE | 1..100 | Informacja, która strona wyników jest zwracana. |
| **pagesCount** | NIE | 1..100 | Informacja o całkowitej liczbie stron. |
| **returnCount** | NIE | 5 | Informacja o całkowitej liczbie rekordów, jeśli w wyniku zwracany jest więcej niż jeden rekord. |
| **timestamp** | TAK | Timestamp | Data i czas odpowiedzi. |

## 6.2. getProductListRequest

Żądanie pozwala pobrać listę produktów skonfigurowanych dla danego konta.

```
<getProductList>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <hashAlgorithm>true, false
</getProductList>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **hashAlgorithm** | NIE | true, false | Brak wartości jest równoważny z ustawieniem false. Zwraca dodatkowe informacje o dostępnych funkcjach skrótu dla produktu. |

## 6.3. getProductListResponse

Odpowiedź zawiera informacje o dostępnych produktach i szczegółach ich konfiguracji.

```
<getProductListResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <products>
    <product>
      <code>3 String
      <type>ISSUE, RENEWAL
      <validityPeriod>4
      <certificateNotificationEnabled>true, false
      <verificationNotificationEnabled>true, false
      <supportedHashAlgorithms>
        <hashAlgorithm>RSA-SHA256, ECC-SHA256
      </supportedHashAlgorithms>
    </product>
  </products>
</getProductListResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **code** | TAK | 3 String | 3-cyfrowy kod produktu. |
| **type** | TAK | Lista | ISSUE – produkty na wydanie, wykorzystywane w quickOrder,<br>RENEWAL – produkty na odnowienie, wykorzystywane w renewCertificate. |
| **validityPeriod** | TAK | Liczba | okres ważności certyfikatu w dniach |
| **certificateNotificationEnabled** | TAK | true/false | Informacja czy maile informacyjne są wysyłane. |
| **verificationNotificationEnabled** | TAK | true/false | Informacja czy maile weryfikacyjne dla metod DNS i FILE są wysyłane. |
| **hashAlgorithm** | TAK | Timestamp | RSA-SHA256, ECC-SHA256 – funkcje skrótu dostępne dla produktu. |

## 6.4. quickOrderRequest

Żądanie powinno zawierać wszystkie dane potrzebne do złożenia zamówienia takie jak CSR w postaci PKCS#10, kod produktu, dane zamawiającego certyfikat oraz inne dane wymagane przez konkretny typ certyfikatu jak np. dane weryfikacji dla certyfikatów SSL.

```
<quickOrder>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderParameters>
    <customer>64 String
    <orderID>50 String
    <userAgent>255 String
    <language>2 String
    <revocationContactEmail>255 String
    <productCode>3 String
    <CSR>4000 String
    <hashAlgorithm> RSA-SHA256, ECC-SHA256
    <shortenedValidityPeriod>25 YYYY-MM-DD
    <email>64 String
    <commonName>64 String
    <givenName>16 String
    <surname>40 String
    <organization>64 String
    <organizationalUnit>64 String
    <locality>128 String
    <state>128 String
    <country>2 String
    <serialNumber>64 String
    <businessCategory>Private Organization, Business Entity, Non-Commercial Entity,
Government Entity
    <streetAddress>64 String
    <postalCode>40 String
    <joILN>128 String
    <joISoPN>128 String
    <joISoCN>2 String
  </orderParameters>
  <SANEntries>
    <SANEntry>
      <DNSName>230 String
    </SANEntry>
  </SANEntries>
  <SANApprover>
    <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <approverEmail>255 String
    <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
    <verificationNotificationEnabled>true, false
  </SANApprover>
  <requestorInfo>
    <email>255 String
    <firstName>16 String
    <lastName>40 String
    <phone>32 String
  </requestorInfo>
  <organizationInfo>
    <taxIdentificationNumber>32 String
  </organizationInfo>
</quickOrder>
```

Dane produktu i klienta – jest to identyfikator klienta i identyfikator kodu produktu, zawsze jeden produkt oraz dodatkowe dane.

```
  <orderParameters>
    <customer>64 String
    <orderID>50 String
    <userAgent>255 String
    <language>2 String
    <revocationContactEmail>255 String
    <productCode>3 String
  </orderParameters>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **customer** | TAK | 64 String | Identyfikator klienta lub login klienta do usługi SimplySign. |
| **orderID** | NIE | 50 String | Unikalny identyfikator zamówienia którym będzie posługiwał się partner. W przypadku, gdy nie zostanie podany, jest automatycznie nadawany przez API. |
| **userAgent** | NIE | 255 String | Przeglądarka i system operacyjny. |
| **language** | NIE | 2 String | Język dla mailingów, jeśli ma być inny niż domyślny język ustawiony dla partnera. |
| **revocationContactEmail** | NIE | 255 String | Adres email, który zostanie użyty do powiadomienia klienta wyłącznie w sytuacji unieważnienia certyfikatu w wyniku zgłoszenia niezgodności. Podany adres nie może być loginem partnera. |
| **productCode** | TAK | 3 String | 3-cyfrowy kod produktu. |

Dane do certyfikatu – dane które mają trafić do certyfikatu. Wymagalność pól wynika z wybranego produktu. Podając CSR, można uzupełnić brakujące pola lub nadpisać błędne podane dane przez dodatkowe pola zawarte w żądaniu.

```
  <orderParameters>
    <CSR>4000 String
    <hashAlgorithm> RSA-SHA256, ECC-SHA256
    <shortenedValidityPeriod>25 YYYY-MM-DD
    <email>255 String
    <commonName>64 String
    <givenName>16 String
    <surname>40 String
    <organization>64 String
    <organizationalUnit>64 String
    <locality>128 String
    <state>128 String
    <country>2 String
    <serialNumber>64 String
    <businessCategory>Private Organization, Business Entity, Non-Commercial Entity,
Government Entity
    <streetAddress>64 String
    <postalCode>40 String
    <joILN>128 String
    <joISoPN>128 String
    <joISoCN>2 String
  </orderParameters>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **CSR** | TAK | 4000 String | Żądanie wydania certyfikatu w formacie PKCS#10. |
| **hashAlgorithm** | NIE | Lista | RSA-SHA256, ECC-SHA256 – jeśli nie zostanie podana, przyjęta zostanie domyślna wartość skonfigurowana dla danego produktu partnera. Dostępne funkcje |

| | | | |
|---|---|---|---|
| | | | skrótu można uzyskać przez wywołanie metody getProductList |
| **shortenedValidityPeriod** | NIE | YYYY-MM-DD | Data końca ważności certyfikatu, musi być mniejsza niż bieżąca data + liczba dni wynikająca z produktu (np.: bieżąca data + 364 dni dla certyfikatu na 365). Można ustawiać tą wartość, jeśli potrzebne jest aby certyfikat stracił ważność konkretnego dnia. |
| **email** | NIE | 64 String | Nadpisanie lub uzupełnienie pola E z CSR. |
| **commonName** | NIE | 64 String | Nadpisanie lub uzupełnienie pola CN z CSR. |
| **givenName** | NIE | 16 String | Nadpisanie lub uzupełnienie pola GN z CSR. |
| **surname** | NIE | 40 String | Nadpisanie lub uzupełnienie pola SN z CSR. |
| **organization** | NIE | 64 String | Nadpisanie lub uzupełnienie pola O z CSR. |
| **locality** | NIE | 128 String | Nadpisanie lub uzupełnienie pola L z CSR. |
| **state** | NIE | 128 String | Nadpisanie lub uzupełnienie pola SP z CSR. |
| **country** | NIE | 2 String | Nadpisanie lub uzupełnienie pola C z CSR. |
| **serialNumber** | NIE | 64 String | Nadpisanie lub uzupełnienie pola SN z CSR. |
| **businessCategory** | NIE | Lista | Private Organization, Business Entity, Non-Commercial Entity, Government Entity – nadpisanie lub uzupełnienie pola BC z CSR. |
| **streetAddress** | NIE | 64 String | Nadpisanie lub uzupełnienie pola ST z CSR. |
| **postalCode** | NIE | 40 String | Nadpisanie lub uzupełnienie pola P z CSR. |
| **joILN** | NIE | 128 String | Nadpisanie lub uzupełnienie pola JoILN z CSR. |
| **joISoPN** | NIE | 128 String | Nadpisanie lub uzupełnienie pola JoISoPN z CSR. |
| **joISoCN** | NIE | 2 String | Nadpisanie lub uzupełnienie pola JoISoCN z CSR. |

**Uwaga:** Produkty S/MIME w polu CommonName muszą mieć wartości zgodne z pozostałymi polami w `quickOrder`. To oznacza, że dla Individual i Sponsor `CN = GN+" "+SN`, dla Organization `CN = O`, opcjonalnie dla wszystkich produktów `CN = E`. Jeśli dane nie będą się zgadzać, API zwróci błąd.

Dane do certyfikatu SSL – lista domen wraz z wybraną metodą weryfikacji. Domeny nie są wczytywane z CSR, należy je podać osobno w żądaniu. Dane te są wymagane w przypadku składania zamówienia na certyfikat SSL.

```
<SANEntries>
  <SANEntry>
    <DNSName>230 String
  </SANEntry>
</SANEntries>
<SANApprover>
  <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
  <approverEmail>255 String
  <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
  <verificationNotificationEnabled>true, false
</SANApprover>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **DNSName** | TAK | 230 String | Dowolna domena, która ma trafić do certyfikatu. |
| **approverMethod** | TAK | Lista | ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – jedna z dopuszczalnych metod weryfikacji. |
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **approverEmailPrefix** | NIE | Lista | ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER – jeśli wybrano metodę ADMIN, należy podać prefix na jaki zostaną wysłane maile weryfikacyjne. |

| | | | |
|---|---|---|---|
| **verificationNotificationEnabled** | NIE | true/false | FALSE – Parametr wyłączający wysyłkę maili weryfikacyjnych, jeśli wybrano metodę DNS lub FILE. Dla metody ADMIN maile weryfikacyjne zawsze są wysyłane. Brak wartości oznacza przyjęcie wartości domyślnej skonfigurowanej dla partnera. Aktualną konfigurację można uzyskać przez wywołanie metody getProductList |

Dane Subskrybenta – wymagane do weryfikacji osoby składającej zamówienie. Dane te są wymagane w przypadku składania zamówienia na certyfikat OV lub EV.

```
  <requestorInfo>
    <email>230 String
    <firstName>16 String
    <lastName>40 String
    <phone>32 String
  </requestorInfo>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **email** | TAK | 230 String | Adres email Subskrybenta. |
| **firstName** | TAK | 16 String | Imię Subskrybenta. |
| **lastName** | TAK | 40 String | Nazwisko Subskrybenta. |
| **phone** | NIE | 32 String | Numer telefonu Subskrybenta. |

Dane organizacji – wymagane do weryfikacji organizacji, której dane są w certyfikacie. Dane te są wymagane w przypadku składania zamówienia na certyfikat OV lub EV.

```
  <organizationInfo>
    <taxIdentificationNumber>32 String
  </organizationInfo>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **taxIdentificationNumber** | TAK | 32 String | NIP, KRS albo inny numer identyfikacji podatkowej. |

## 6.5. quickOrderResponse

Odpowiedź zwraca potwierdzenie przyjęcia zamówienia wraz z jego numerem. Jeśli wymagana jest weryfikacja domeny, zwraca dodatkowe informacje dotyczące tej weryfikacji.

```
<quickOrderResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <orderID>50 String
  <SANVerification>
    <approverMethod>FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <code>50 String
    <approverEmail>255 String
    <FQDNs>
      <FQDN>230 String
    </FQDNs>
  </SanVerification>
</quickOrderResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia którym będzie posługiwał się partner. W przypadku, gdy nie zostanie podany, jest automatycznie nadawany przez API. |
| **approverMethod** | NIE | Lista | FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – wybrana metoda weryfikacji. Dane weryfikacji nie są zwracane, jeśli wybrano metodę ADMIN. |
| **code** | NIE | 50 String | Kod weryfikacyjny. |
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **FQDN** | NIE | 230 String | Domena dla której wymagana jest weryfikacja. |

## 6.6. validateOrderParametersRequest

Żądanie pozwala na przekazanie danych do walidacji. Struktura całego żądania jest taka sama jak w przypadku **`quickOrder`**. Sprawdzeniu podlegają zgodność danych zawartych w CSR z typem certyfikatu, oraz zakres dostarczonych danych. Te same walidatory są wykorzystywane w momencie składania zamówienia metodą **`quickOrder`**.

```
<validateOrderParameters>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderParameters>
    <customer>64 String
    <orderID>50 String
    <userAgent>255 String
    <language>2 String
    <revocationContactEmail>255 String
    <productCode>3 String
    <CSR>4000 String
    <hashAlgorithm>RSA-SHA256, ECC-SHA256
    <shortenedValidityPeriod>25 YYYY-MM-DD
    <email>64 String
    <commonName>64 String
    <givenName>16 String
    <surname>40 String
    <organization>64 String
    <organizationalUnit>64 String
    <locality>128 String
    <state>128 String
    <country>2 String
    <serialNumber>64 String
    <businessCategory>Private Organization, Business Entity, Non-Commercial Entity,
Government Entity
    <streetAddress>64 String
    <postalCode>40 String
    <joILN>128 String
    <joISoPN>128 String
    <joISoCN>2 String
  </orderParameters>
  <SANEntries>
    <SANEntry>
      <DNSName>230 String
    </SANEntry>
  </SANEntries>
  <SANApprover>
    <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
```

```
    <approverEmail>255 String
    <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
    <verificationNotificationEnabled>true, false
  </SANApprover>
  <requestorInfo>
    <email>255 String
    <firstName>16 String
    <lastName>40 String
    <phone>32 String
  </requestorInfo>
  <organizationInfo>
    <taxIdentificationNumber>32 String
  </organizationInfo>
</validateOrderParameters>
```

## 6.7. validateOrderParametersResponse

Odpowiedź zwraca wyniki walidacji żądania certyfikacyjnego. Poprawna odpowiedź zwraca dane pobrane z CSR i pól w żądaniu w zakresie pól, które zostaną dodane do certyfikatu, pozostałe pola są pomijane.

```
<validateOrderParametersResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <parsedCSR>
    <email>64 String
    <commonName>64 String
    <givenName>16 String
    <surname>40 String
    <organization>64 String
    <organizationalUnit>64 String
    <locality>128 String
    <state>128 String
    <country>2 String
    <serialNumber>64 String
    <businessCategory>Private Organization, Business Entity, Non-Commercial Entity,
Government Entity
    <streetAddress>64 String
    <postalCode>40 String
    <joILN>128 String
    <joISoPN>128 String
    <joISoCN>2 String
  </parsedCSR>
</validateOrderParametersResponse>
```

## 6.8. reissueCertificateRequest

Żądanie powinno zawierać wszystkie dane potrzebne do reissue certyfikatu takie jak CSR z nowymi kluczami w postaci PKCS#10 i opcjonalne nowe domeny. Aby dokonać reissue trzeba wskazać najnowszy, ważny certyfikat albo załączając jego plik w formacie PEM albo podając jego numer seryjny. Dane w nowym certyfikacie zostaną przepisane z odnawianego certyfikatu, nie będą wczytane z CSR.

```
<reissueCertificate>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
```

```
    </authToken>
  </requestHeader>
  <userAgent>255 String
  <CSR>4000 String
  <X509Cert>4000 String
  <serialNumber>32 String
  <hashAlgorithm>RSA-SHA256, ECC-SHA256
  <SANEntries>
    <SANEntry>
      <DNSName>230 String
    </SANEntry>
  </SANEntries>
  <SANApprover>
    <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <approverEmail>255 String
    <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
    <verificationNotificationEnabled>true, false
  </SANApprover>
</reissueCertificate>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **userAgent** | NIE | 255 String | Przeglądarka i system operacyjny. |
| **CSR** | TAK | 4000 String | Żądanie wydania certyfikatu w formacie PKCS#10. |
| **X509Cert** | TAK | 4000 String | Ponownie wydawany certyfikat w formacie PEM (Base64). |
| **serialNumber** | TAK | 32 String | Numer seryjny ponownie wydawanego certyfikatu w formacie HEX. |
| **hashAlgorithm** | NIE | Lista | RSA-SHA256, ECC-SHA256 – jeśli nie zostanie podana, przyjęta zostanie domyślna wartość skonfigurowana dla danego produktu partnera. Dostępne funkcje skrótu można uzyskać przez wywołanie metody getProductList |

Dane do certyfikatu SSL – lista domen jest pobierana z poprzedniego certyfikatu. W ramach reissue można dodać nową domenę, przy czym wszystkie nowe domeny wymagają weryfikacji. Dane te są wymagane w przypadku składania reissue na certyfikaty SSL z nowymi domenami.

```
  <SANEntries>
    <SANEntry>
      <DNSName>230 String
    </SANEntry>
  </SANEntries>
  <SANApprover>
    <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <approverEmail>255 String
    <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
    <verificationNotificationEnabled>true, false
  </SANApprover>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **DNSName** | TAK | 230 String | Nowa domena, która ma trafić do certyfikatu. |
| **approverMethod** | TAK | Lista | ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – jedna z dopuszczalnych metod weryfikacji. |
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **approverEmailPrefix** | NIE | Lista | ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER – jeśli wybrano metodę ADMIN, należy podać prefix na jaki zostaną wysłane maile weryfikacyjne. |

| | | | |
|---|---|---|---|
| **verificationNotificationEnabled** | NIE | true/false | FALSE – Parametr wyłączający wysyłkę maili weryfikacyjnych, jeśli wybrano metodę DNS lub FILE. Dla metody ADMIN maile weryfikacyjne zawsze są wysyłane. Brak wartości oznacza przyjęcie wartości domyślnej skonfigurowanej dla partnera. Aktualną konfigurację można uzyskać przez wywołanie metody getProductList |

## 6.9. reissueCertificateResponse

Odpowiedź zwraca potwierdzenie przyjęcia zamówienia wraz z jego numerem. Jeśli wymagana jest weryfikacja domeny, zwraca dodatkowe informacje dotyczące tej weryfikacji. Struktura całego żądania jest taka sama jak w przypadku **`quickOrder`**.

```
<reissueCertificateResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <orderID>50 String
  <SANVerification>
    <approverMethod>FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <code>50 String
    <approverEmail>255 String
    <FQDNs>
      <FQDN>230 String
    </FQDNs>
  </SanVerification>
</reissueCertificateResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia którym będzie posługiwał się partner. W przypadku, gdy nie zostanie podany, jest automatycznie nadawany przez API. |
| **approverMethod** | NIE | Lista | FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – wybrana metoda weryfikacji. Dane weryfikacji nie są zwracane, jeśli wybrano metodę ADMIN. |
| **code** | NIE | 50 String | Kod weryfikacyjny. |
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **FQDN** | NIE | 230 String | Domena dla której wymagana jest weryfikacja. |

## 6.10. renewCertificateRequest

Żądanie powinno zawierać wszystkie dane potrzebne do odnowienia certyfikatu takie jak CSR z nowymi kluczami w postaci PKCS#10 i kod produktu. Aby dokonać odnowienia trzeba wskazać przedni certyfikat albo załączając jego plik w formacie PEM albo podając jego numer seryjny. Dane w nowym certyfikacie zostaną przepisane z odnawianego certyfikatu, nie będą wczytane z CSR.

```
<renewCertificate>
  <requestHeader>
    <authToken>
      <userName>255 String
```

```
      <password>255 String
    </authToken>
  </requestHeader>
  <customer>64 String
  <userAgent>255 String
  <revocationContactEmail>255 String
  <productCode>3 String
  <CSR>4000 String
  <X509Cert>4000 String
  <serialNumber>32 String
  <hashAlgorithm> RSA-SHA256, ECC-SHA256
  <shortenedValidityPeriod>25 YYYY-MM-DD
  <SANApprover>
    <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <approverEmail>255 String
    <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
    <verificationNotificationEnabled>true, false
  </SANApprover>
</renewCertificate>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **customer** | TAK | 64 String | Identyfikator klienta lub login klienta do usługi SimplySign. |
| **userAgent** | NIE | 255 String | Przeglądarka i system operacyjny. |
| **revocationContactEmail** | NIE | 255 String | Adres email, który zostanie użyty do powiadomienia klienta wyłącznie w sytuacji unieważnienia certyfikatu w wyniku zgłoszenia niezgodności. Podany adres nie może być loginem partnera. |
| **productCode** | TAK | 3 String | 3-cyfrowy kod produktu. |
| **CSR** | TAK | 4000 String | Żądanie wydania certyfikatu w formacie PKCS#10. |
| **X509Cert** | TAK | 4000 String | Odnawiany certyfikat w formacie PEM (Base64). |
| **serialNumber** | TAK | 32 String | Numer seryjny odnawianego certyfikatu w formacie HEX. |
| **hashAlgorithm** | NIE | Lista | RSA-SHA256, ECC-SHA256 – jeśli nie zostanie podana, przyjęta zostanie domyślna wartość skonfigurowana dla danego produktu partnera. Dostępne funkcje skrótu można uzyskać przez wywołanie metody getProductList |
| **shortenedValidityPeriod** | NIE | YYYY-MM-DD | Data końca ważności certyfikatu, musi być mniejsza niż bieżąca data + liczba dni wynikająca z produktu (np.: bieżąca data + 364 dni dla certyfikatu na 365). Można ustawiać tą wartość, jeśli potrzebne jest aby certyfikat stracił ważność konkretnego dnia. |

Dane do certyfikatu SSL – lista domen jest pobierana z odnawianego certyfikatu, ale wszystkie domeny wymagają ponownej weryfikacji. Dane te są wymagane w przypadku składania zamówienia na certyfikat SSL.

```
  <SANApprover>
    <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <approverEmail>255 String
    <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
    <verificationNotificationEnabled>true, false
  </SANApprover>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **approverMethod** | TAK | Lista | ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – jedna z dopuszczalnych metod weryfikacji. |

| | | | |
|---|---|---|---|
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **approverEmailPrefix** | NIE | Lista | ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER – jeśli wybrano metodę ADMIN, należy podać prefix na jaki zostaną wysłane maile weryfikacyjne. |
| **verificationNotificationEnabled** | NIE | true/false | FALSE – Parametr wyłączający wysyłkę maili weryfikacyjnych, jeśli wybrano metodę DNS lub FILE. Dla metody ADMIN maile weryfikacyjne zawsze są wysyłane. Brak wartości oznacza przyjęcie wartości domyślnej skonfigurowanej dla partnera. Aktualną konfigurację można uzyskać przez wywołanie metody getProductList |

## 6.11. renewCertificateResponse

Odpowiedź zwraca potwierdzenie przyjęcia zamówienia wraz z jego numerem. Jeśli wymagana jest weryfikacja domeny, zwraca dodatkowe informacje dotyczące tej weryfikacji. Struktura całego żądania jest taka sama jak w przypadku **`quickOrder`**.

```
<renewCertificateResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <orderID>50 String
  <SANVerification>
    <approverMethod>FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <code>50 String
    <approverEmail>255 String
    <FQDNs>
      <FQDN>230 String
    </FQDNs>
  </SanVerification>
</renewCertificateResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia którym będzie posługiwał się partner. W przypadku, gdy nie zostanie podany, jest automatycznie nadawany przez API. |
| **approverMethod** | NIE | Lista | FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – wybrana metoda weryfikacji. Dane weryfikacji nie są zwracane, jeśli wybrano metodę ADMIN. |
| **code** | NIE | 50 String | Kod weryfikacyjny. |
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **FQDN** | NIE | 230 String | Domena dla której wymagana jest weryfikacja. |

## 6.12. getOrderStateRequest

Żądanie pozwala pobrać status i szczegóły weryfikacji dla podanego identyfikatora zamówienia.

```
<getOrderState>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID>50 String
</getOrderState>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia |

## 6.13. getOrderStateResponse

Odpowiedź zawiera informację o statusie zamówienia oraz każdej z weryfikacji jaka realizowana jest dla zamówienia.

```
<getOrderStateResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <orderStatus>AWAITING, VERIFICATION, ACCEPTED, ENROLLED, REJECTED
  <lastUpdateDate>YYYY-MM-DDTHH:MM:SS.000Z
  <verifications>
    <verification>
      <type>PRODUCT, APPLICANT, ORGANIZATION, AUTHORIZATION, SYSTEM, DOMAIN, EMAIL,
EXTENDED_VALIDATION
      <state>NOT_REQUIRED, REQUIRED, FAILED, VERIFIED
      <expireDate>YYYY-MM-DDTHH:MM:SS.000Z
    </verification>
  </verifications>
</getOrderStateResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderStatus** | TAK | Lista | AWAITING – nowe zamówienie oczekujące na weryfikację,<br>VERIFICATION – zamówienie w trakcie weryfikacji,<br>ACCEPTED – zamówienie zweryfikowane,<br>ENROLLED – certyfikat wystawiony,<br>REJECTED – zamówienie anulowane przez cancelOrder lub odrzucone przez Certum |
| **lastUpdateDate** | TAK | Timestamp | Data ostatniej aktualizacji zamówienia. |
| **type** | TAK | Lista | PRODUCT – weryfikacja czy produkt nie jest wycofany<br>APPLICANT – weryfikacja Subskrybenta z requestorInfo<br>ORGANIZATION – weryfikacja danych organizacji zawartych w certyfikacie<br>AUTHORIZATION – weryfikacja upoważnienia Subskrybenta do reprezentowania organizacji<br>SYSTEM – weryfikacja CAA i blacklist dla domen z zamówienia |

| | | | |
|---|---|---|---|
| | | | DOMAIN – weryfikacja kontroli Subskrybenta nad domenami z zamówienia<br>EMAIL – weryfikacja adresu email dla certyfikatów innych niż SSL<br>EXTENDED_VALIDATION – dodatkowa weryfikacja dla EV |
| **state** | TAK | Lista | NOT_REQUIRED – weryfikacja tego typu nie jest wymagana,<br>REQUIRED – weryfikacja tego typu jest wymagana,<br>VERIFIED – weryfikacja jest ukończona,<br>FAILED – weryfikacja nie powiodła się. |
| **expireDate** | NIE | Timestamp | Data do kiedy dana weryfikacja, jeśli jest ukończona, pozostanie ważna. |

## 6.14. getOrderByOrderIDRequest

Żądanie pozwala pobrać zamówienie dla podanego identyfikatora zamówienia. Wszystkie pozostałe parametry ustawione są domyślnie na false.

```
<getOrderByOrderID>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID> 50 String
  <orderOption>
    <orderStatus>true, false
    <orderDetails>true, false
    <certificateDetails>true, false
  </orderOption>
</getOrderByOrderID>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia |
| **orderStatus** | NIE | true/false | TRUE – zwraca podstawowe informacje o zamówieniu w tym status przetwarzania. |
| **orderDetails** | NIE | true/false | TRUE – zwraca szczegóły zamówienia. |
| **certificateDetails** | NIE | true/false | TRUE – zwraca szczegóły certyfikatu jeśli został wydany |

## 6.15. getOrderByOrderIDResponse

Odpowiedź zawiera informacje określone w żądaniu.

```
<getOrderByOrderIDResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <returnCount>5
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <orders>
    <Order reissue="true">
      <orderStatus>
        <orderID>50 String
        <orderStatus>AWAITING, VERIFICATION, ACCEPTED, ENROLLED, REJECTED
```

```
        <orderDate>YYYY-MM-DDTHH:MM:SS.000Z
        <productCode>3 String
        <customer>64 String
        <serialNumber>32 String
      </orderStatus>
      <orderDetails>
        <requestorInfo>
          <email>255 String
          <firstName>16 String
          <lastName>40 String
          <phone>32 String
        </requestorInfo>
        <organizationInfo>
          <taxIdentificationNumber>32 String
        </organizationInfo>
      </orderDetails>
      <certificateDetails>
        <certificateStatus>VALID, REVOKING, REVOKED
        <startDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <endDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <commonName>64 String
        <serialNumber>32 String
        <subjectName>3000 String
        <DNSNames>300 String
        <revokedDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <X509Cert>4000 String
      </certificateDetails>
    </Order>
  <orders>
</getOrderByOrderIDResponse>
```

Podstawowe informacje o zamówieniu, jeśli są zwracane w odpowiedzi.

```
    <Order reissue="true">
      <orderStatus>
        <orderID>50 String
        <orderStatus>AWAITING, VERIFICATION, ACCEPTED, ENROLLED, REJECTED
        <orderDate>YYYY-MM-DDTHH:MM:SS.000Z
        <productCode>3 String
        <customer>64 String
        <serialNumber>32 String
      </orderStatus>
    </Order>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **reissue="true"** | NIE | true | Oznacza certyfikat powstały w wyniku reissue. |
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia. |
| **orderStatus** | TAK | Lista | AWAITING – nowe zamówienie oczekujące na weryfikację,<br>VERIFICATION – zamówienie w trakcie weryfikacji,<br>ACCEPTED – zamówienie zweryfikowane,<br>ENROLLED – certyfikat wystawiony,<br>REJECTED – zamówienie anulowane przez cancelOrder lub odrzucone przez Certum |
| **orderDate** | TAK | Timestamp | Data złożenia zamówienia. |
| **productCode** | TAK | 3 String | 3-cyfrowy kod produktu. |
| **customer** | TAK | 64 String | Identyfikator klienta. |
| **serialNumber** | NIE | 32 String | Numer seryjny certyfikatu, zwracany wyłącznie gdy certyfikat istnieje, numer certyfikatu w formacie HEX. |

Rozszerzone informacje o zamówieniu, jeśli są zwracane w odpowiedzi.

```
<orderDetails>
  <requestorInfo>
    <email>255 String
    <firstName>16 String
    <lastName>40 String
    <phone>32 String
  </requestorInfo>
  <organizationInfo>
    <taxIdentificationNumber>32 String
  </organizationInfo>
</orderDetails>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **email** | TAK | 3 String | Adres email Subskrybenta. |
| **firstName** | TAK | 16 String | Imię Subskrybenta. |
| **lastName** | TAK | 40 String | Nazwisko Subskrybenta. |
| **phone** | TAK | 32 String | Numer telefonu Subskrybenta. |
| **taxIdentificationNumber** | TAK | 64 String | NIP, KRS albo inny numer identyfikacji podatkowej. |

Rozszerzone informacje o certyfikacie, jeśli są zwracane w odpowiedzi.

```
<certificateDetails>
  <certificateStatus>VALID, REVOKING, REVOKED
  <startDate>25 YYYY-MM-DDTHH:MM:SS.000Z
  <endDate>25 YYYY-MM-DDTHH:MM:SS.000Z
  <commonName>64 String
  <serialNumber>32 String
  <subjectName>3000 String
  <DNSNames>300 String
  <revokedDate>25 YYYY-MM-DDTHH:MM:SS.000Z
  <X509Cert>4000 String
</certificateDetails>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **certificateStatus** | TAK | List | VALID – Certyfikat ważny, aktualny,<br>REVOKING – Certyfikat w trakcie unieważnienia, taki status mogą mieć certyfikaty oczekujące na unieważnienie po dokonaniu reissue,<br>REVOKED – Certyfikat unieważniony. |
| **startDate** | TAK | Timestamp | Data początku ważności certyfikatu. |
| **endDate** | TAK | Timestamp | Data końca ważności certyfikatu. |
| **commonName** | TAK | 64 String | Nazwa powszechna może zawierać imię i nazwisko Subskrybenta dla certyfikatu ID, lub nazwę domeny dla certyfikatu SSL. |
| **serialNumber** | TAK | 32 String | Numer seryjny certyfikatu w formacie HEX. |
| **subjectName** | TAK | 3000 String | Zawartość pola Podmiot. |
| **DNSNames** | NIE | 300 String | Zawartość pola SAN, zwracana tylko dla certyfikatów SSL. |
| **revokedDate** | NIE | Timestamp | Data unieważnienia, zwracana tylko jeśli status certyfikatu to REVOKED. |
| **X509Cert** | TAK | 4000 String | Certyfikat w formacie PEM (Base64) |

## 6.16. cancelOrderRequest

Żądanie pozwala na anulowanie zamówienia, jeśli certyfikat nie został wydany.

```
<cancelOrder>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <cancelParameters>
    <orderID>50 String
    <note>255 String
  </cancelParameters>
</cancelOrder>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia. |
| **note** | NIE | 255 String | Informacja o przyczynie anulowania zamówienia. |

## 6.17. cancelOrderResponse

Odpowiedź nie zwraca danych. Jeśli do danego żądania został wydany certyfikat, zostanie zwrócony błąd oraz numer seryjny certyfikatu.

```
<cancelOrderResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
        <value>32 String
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
</cancelOrderResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **value** | NIE | 32 String | Numer seryjny certyfikatu w postaci HEX. |

## 6.18. getSanVerificationStateRequest

Żądanie pozwala pobrać informacje o weryfikacjach domen dla zamówienia. Weryfikacja domen dotyczy wyłącznie certyfikatów SSL.

```
<getSanVerificationState>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID>50 String
</getSanVerificationState>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | NIE | 50 String | Unikalny identyfikator zamówienia. |

## 6.19. getSanVerificationStateResponse

Odpowiedź zawiera informacje o statusie weryfikacji wszystkich domen dla danego zamówienia wraz z informacjami o problemach z weryfikacją.

```
<getSanVerificationStateResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <sanVerifications>
    <sanVerification>
      <FQDN> 255 String
      <manualVerification>
        <state>REQUIRED, VERIFIED, FAILED
        <expireDate>YYYY-MM-DDTHH:MM:SS.000Z
        <info>ALREADY_VERIFIED,  LINK_EXPIRED,  OTHER_ERROR,  FILE_INVALID_CONTENT,
FILE_CONNECTION_ERROR, FILE_HTTP_ERROR, DNS_NO_RECORDS, DNS_NO_PROPER_RECORDS
      </manualVerification>
      <systemVerification>
        <method> CAA, PHISHTANK, GOOGLE_SAFE_BROWSING, TOP_SITES, REVOKED_CERTIFICATE
      </systemVerification>
    </sanVerification>
  </sanVerifications>
</getSanVerificationStateResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **FQDN** | TAK | 255 String | Domena dla której sprawdzana jest weryfikacja. |
| **state** | TAK | Lista | REQUIRED – weryfikacja jest wymagana,<br>VERIFIED – weryfikacja jest ukończona,<br>FAILED – weryfikacja nie powiodła się. |
| **expireDate** | NIE | Timestamp | Data wygaśnięcia weryfikacji. |
| **info** | NIE | Lista | ALREADY_VERIFIED – weryfikacja została już pozytywnie wykonana,<br>LINK_EXPIRED – link weryfikacyjny wygasł,<br>OTHER_ERROR – nieznana przyczyna błędu,<br>FILE_INVALID_CONTENT – niepoprawna treść pliku weryfikacyjnego,<br>FILE_CONNECTION_ERROR – nie udało się znaleźć pliku weryfikacyjnego lub strona nie istnieje,<br>FILE_HTTP_ERROR – nie udało połączyć się ze wskazanym adresem,<br>DNS_NO_RECORDS – brak rekordów TXT na serwerze DNS,<br>DNS_NO_PROPER_RECORDS – brak odpowiednich rekordów TXT na serwerze DNS |
| **method** | NIE | Lista | CAA – błędny rekord CAA, należy poprawić rekord,<br>PHISHTANK – domena na liście phishingowej Phishtank,<br>GOOGLE_SAFE_BROWSING – domena na liście phishingowej Google,<br>TOP_SITES – popularna domena, skontaktuj się z Certum,<br>REVOKED_CERTIFICATE – domena na liście certyfikatów unieważnionych, skontaktuj się z Certum |

## 6.20. addSanVerificationRequest

Żądanie pozwala wygenerować nowe kody weryfikacyjne dla domen z zamówienia. Weryfikacja domen dotyczy wyłącznie certyfikatów SSL.

```
<addSanVerification>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID>50 String
  <SANApprover>
    <approverMethod>ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <approverEmail>255 String
    <approverEmailPrefix>ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER
    <verificationNotificationEnabled>true, false
  </SANApprover>
</addSanVerification>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia. |
| **approverMethod** | TAK | Lista | ADMIN, FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – jedna z dopuszczalnych metod weryfikacji. |
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **approverEmailPrefix** | NIE | Lista | ADMIN, ADMINISTRATOR, POSTMASTER, HOSTMASTER, WEBMASTER – jeśli wybrano metodę ADMIN, należy podać prefix na jaki zostaną wysłane maile weryfikacyjne. |
| **verificationNotificationEnabled** | NIE | true/false | FALSE – Parametr wyłączający wysyłkę maili weryfikacyjnych, jeśli wybrano metodę DNS lub FILE. Dla metody ADMIN maile weryfikacyjne zawsze są wysyłane. Brak wartości oznacza przyjęcie wartości domyślnej skonfigurowanej dla partnera. Aktualną konfigurację można uzyskać przez wywołanie metody getProductList |

## 6.21. addSanVerificationResponse

Odpowiedź, jeśli wybrano wysyłkę maili, nie zwraca dodatkowych informacji, ale maile dla brakujących weryfikacji są wysyłane. Jeśli wybrano opcję wyłączenia maili, zwracany jest kod weryfikacyjny.

```
<getSanVerificationStateResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <SANVerification>
    <approverMethod>FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX
    <code>50 String
    <approverEmail>255 String
    <FQDNs>
      <FQDN>230 String
    </FQDNs>
  </SanVerification>
</getSanVerificationStateResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **approverMethod** | NIE | Lista | FILE, DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX – wybrana metoda weryfikacji. Dane weryfikacji nie są zwracane, jeśli wybrano metodę ADMIN. |
| **code** | NIE | 50 String | Kod weryfikacyjny. |
| **approverEmail** | NIE | 255 String | Email na który zostanie wysłany kod weryfikacyjny – jeśli wybrano metodę DNS lub FILE. |
| **FQDN** | NIE | 230 String | Domena dla której wymagana jest weryfikacja. |

## 6.22. performSanVerificationRequest

Żądanie pozwala zainicjować weryfikację domen z zamówienia. Weryfikacja domen dotyczy wyłącznie certyfikatów SSL.

```
<performSansVerification>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <code>50 String
</ performSansVerification>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **code** | NIE | 50 String | Kod weryfikacyjny. |

## 6.23. performSanVerificationResponse

Odpowiedź nie zwraca danych. Aby sprawdzić status weryfikacji należy skorzystać z metody **`getSanVerificationState`**.

```
<performSanVerificationResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
</performSanVerificationResponse>
```

## 6.24. addEmailVerificationRequest

Żądanie pozwala stworzyć nową weryfikację pola E (email) umieszczonego w certyfikacie dla danego zamówienia. Weryfikacja pola email dotyczy certyfikatów S/MIME i Document Signing w chmurze.

```
<addEmailVerification>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
```

```
  </requestHeader>
  <orderID>50 String
</addEmailVerification>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia |

## 6.25. addEmailVerificationResponse

Odpowiedź nie zwraca danych, ale maile dla stworzonych weryfikacji są wysyłane.

```
<adddEmailVerificationResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
</adddEmailVerificationResponse>
```

## 6.26. getEmailVerificationRequest

Żądanie pozwala pobrać informację o weryfikacji pola E (email) umieszczonego w certyfikacie dla danego zamówienia. Weryfikacja pola email dotyczy certyfikatów S/MIME i Document Signing w chmurze.

```
<getEmailVerification>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID>50 String
</getEmailVerification>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia |

## 6.27. getEmailVerificationResponse

Odpowiedź zawiera informacje o statusie weryfikacji pola email umieszczonego w certyfikacie.

```
<getEmailVerificationResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <emailVerification>
    <email>64 String
    <verified>true, false
    <sendDate>YYYY-MM-DDTHH:MM:SS.000Z
```

```
    <verificationLinkValidityDate>YYYY-MM-DDTHH:MM:SS.000Z
    <verificationDate>YYYY-MM-DDTHH:MM:SS.000Z
    <verificationValidity>YYYY-MM-DDTHH:MM:SS.000Z
  </emailVerification>
</getEmailVerificationResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **email** | TAK | 64 String | Email z pola E (email), który podlega weryfikacji. |
| **verified** | TAK | true/false | Status weryfikacji. |
| **sendDate** | TAK | Timestamp | Data wysłania maila z linkiem do weryfikacji. |
| **verificationLinkValidityDate** | TAK | Timestamp | Data wygaśnięcia linka do weryfikacji. |
| **verificationDate** | NIE | Timestamp | Data przeprowadzenia weryfikacji. |
| **verificationValidity** | NIE | Timestamp | Data wygaśnięcia weryfikacji. |

## 6.28. verifyOrderRequest

Żądanie pozwala dodać dokumenty. W jednym wywołaniu metody można dodać wiele dokumentów zawierających wiele plików (np. Umowa zeskanowana w kilku oddzielnych plikach). Dokumenty mogą być wymagane w przypadku składania zamówienia na certyfikat IV, OV lub EV.

```
<verifyOrder>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID>50 String
  <note>200 String
  <documents>
    <document>
      <type>APPLICANT, ORGANIZATION, AUTHORIZATION, ADDITIONAL, VERIFICATION_REPORT
      <description>255 String
      <files>
        <file>
          <fileName>255 String
          <content>Base64
        </file>
      </files>
    </document>
  </documents>
</verifyOrder>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia. |
| **note** | TAK | 200 String | Notatka, która zostanie dodana do zamówienia. |
| **type** | TAK | Lista | APPLICANT – potwierdzenie tożsamości Subskrybenta, może to być dowód osobisty, paszport, karta stałego pobytu, prawo jazdy.<br>ORGANIZATION – potwierdzenie istnienia firmy, adres, oficjalni przedstawiciele, jeśli taka informacja jest dostępna. Może to być dokument założycielski firmy, wydruk lub wyciąg z oficjalnej agencji rejestracyjnej online lub rejestru rządowego.<br>AUTHORIZATION – potwierdzenie prawa Subskrybenta do ubiegania się o certyfikat w imieniu organizacji. Może to być świadectwo pracy lub upoważnienie (pełnomocnictwo).<br>ADDITIONAL – dokument potrzebny do weryfikacji, może to być faktura lub inny dokument potwierdzający posiadanie domeny, |

| | | | |
|---|---|---|---|
| | | | faktura potwierdzająca aktualny adres firmy, oświadczenie, umowa, informacje o zamówieniu itp.<br>VERIFICATION_REPORT – raport z weryfikacji, jeśli umowa z Certum obejmuje taki raport. |
| **description** | TAK | 255 String | Opis dodawanego dokumentu. W opisie należy podać numer dokumentu oraz imię i nazwisko osoby której dotyczy dokument lub nazwę organizacji. |
| **fileName** | TAK | 255 String | Nazwa dodawanego pliku. |
| **content** | TAK | Base64 | Zawartość pliku w postaci Base64 |

## 6.29. verifyOrderResponse

Odpowiedź nie zwraca danych.

```
<verifyOrderResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
</verifyOrderResponse>
```

## 6.30. getDocumentsListRequest

Żądanie pozwala pobranć listę dokumentów dla podanego identyfikatora zamówienia. Dokumenty mogą być dodawane przez verifyOrder lub przez Certum, na podstawie wcześniejszych weryfikacji.

```
<getDocumentsList>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID>50 String
</getDocumentsList>
```

| Field name | Req. | Type | Description |
|---|---|---|---|
| **orderID** | YES | 50 String | Unikalny identyfikator zamówienia. |

## 6.31. getDocumentsListResponse

Odpowiedź zwraca szczegóły statusu dokumentu w systemie, ale nie zwraca pliku dokumentu.

```
<getDocumentsListResponse >
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <documentsInfo>
```

```
    <documentInfo>
      <state> NEW, ACCEPTED, REJECTED
      <type> APPLICANT, ORGANIZATION, AUTHORIZATION, ADDITIONAL, VERIFICATION_REPORT,
VERIFICATION_REPORT_OTF
      <createDate> YYYY-MM-DDTHH:MM:SS.000Z
      <expireDate> YYYY-MM-DDTHH:MM:SS.000Z
    </documentInfo>
  </documentsInfo>
</getDocumentsListResponse>
```

| Field name | Req. | Type | Description |
|---|---|---|---|
| **state** | YES | List | NEW - nowy dokument oczekujący na weryfikację,<br>ACCEPTED - dokument zweryfikowany,<br>REJECTED - dokument odrzucony |
| **type** | YES | List | APPLICANT – potwierdzenie tożsamości Subskrybenta, może to być dowód osobisty, paszport, karta stałego pobytu, prawo jazdy.<br>ORGANIZATION – potwierdzenie istnienia firmy, adres, oficjalni przedstawiciele, jeśli taka informacja jest dostępna. Może to być dokument założycielski firmy, wydruk lub wyciąg z oficjalnej agencji rejestracyjnej online lub rejestru rządowego.<br>AUTHORIZATION – potwierdzenie prawa Subskrybenta do ubiegania się o certyfikat w imieniu organizacji. Może to być świadectwo pracy lub upoważnienie (pełnomocnictwo).<br>ADDITIONAL – dokument potrzebny do weryfikacji, może to być faktura lub inny dokument potwierdzający posiadanie domeny, faktura potwierdzająca aktualny adres firmy, oświadczenie, umowa, informacje o zamówieniu itp.<br>VERIFICATION_REPORT – raport z weryfikacji, jeśli umowa z Certum obejmuje taki raport. |
| **createDate** | YES | Timestamp | Data, kiedyj dany dokument został dodany do systemu. |
| **expireDate** | NES | Timestamp | Termin, do którego dany dokument, jeśli ACCEPTED, zachowuje ważność. |

## 6.32. getCertificateRequest

Żądanie pozwala pobrać certyfikat na podstawie numeru zamówienia lub numeru seryjnego certyfikatu.

```
<getCertificate>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <orderID>50 String
  <serialNumber>32 String
</getCertificate>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | NIE | 50 String | Unikalny identyfikator zamówienia. |
| **serialNumber** | NIE | 32 String | Numer seryjny certyfikatu w formacie HEX. |

## 6.33. getCertificateResponse

Odpowiedź zwraca plik certyfikatu oraz caBundle, czyli wszystkie certyfikaty pośrednie (subCA) oraz certyfikat główny (rootCA).

```
<getCertificateResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <certificateDetails>
    <startDate>25 YYYY-MM-DDTHH:MM:SS.000Z
    <endDate>25 YYYY-MM-DDTHH:MM:SS.000Z
    <revokedDate>25 YYYY-MM-DDTHH:MM:SS.000Z
    <X509Cert>4000 String
  </certificateDetails>
  <caBundle>
    <X509Cert>4000 String
  </caBundle>
</getCertificateResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **startDate** | TAK | Timestamp | Data początku ważności certyfikatu. |
| **endDate** | TAK | Timestamp | Data końca ważności certyfikatu. |
| **X509Cert** | TAK | 4000 String | Certyfikat w formacie PEM (Base64) |

## 6.34. revokeCertificateRequest

Żądanie pozwala unieważnić certyfikat.

```
<revokeCertificate>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <revokeCertificateParameters>
    <serialNumber>32 String
    <revocationReason>KEYCOMPROMISE,    AFFILIATIONCHANGED,    CESSATIONOFOPERATION,
UNSPECIFIED, SUPERSEDED
    <keyCompromitationDate>YYYY-MM-DD
    <note>200 String
  </revokeCertificateParameters>
</revokeCertificate>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **serialNumber** | TAK | 32 String | Numer seryjny certyfikatu w formacie HEX. |
| **revocationReason** | NIE | Lista | KEYCOMPROMISE - klucz prywatny został skompromitowany albo zgubiono kartę kryptograficzną z certyfikatem,<br>AFFILIATIONCHANGED - informacje o podmiocie takie jak nazwisko, nazwa organizacji lub adres zawarte w certyfikacie uległy zmianie,<br>SUPERSEDED - certyfikat został zastąpiony nowym certyfikatem, |

| | | | |
|---|---|---|---|
| | | | CESSATIONOFOPERATION - Subskrybent już nie kontroluje lub nie jest uprawniony do używania wszystkich domen wymienionych w certyfikacie,<br>UNSPECIFIED - jeśli inny powód nie ma zastosowania. |
| **keyCompromitationDate** | NIE | YYYY-MM-DD | Data kompromitacji klucza w przypadku podania przyczyny unieważnienia KEYCOMPROMISE |
| **note** | NIE | 255 String | Notatka dla CA dodawana do unieważnienia. |

## 6.35. revokeCertificateResponse

Odpowiedź nie zwraca danych.

```
<revokeCertificateResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
</revokeCertificateResponse>
```

## 6.36. getOrdersByDateRangeRequest

Żądanie pozwala pobrać wszystkie zamówienia złożone w podanym zakresie dat. Wszystkie pozostałe parametry ustawione są domyślnie na false.

```
<getOrderByDateRange>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <fromDate>YYYY-MM-DD
  <toDate>YYYY-MM-DD
  <orderOption>
    <orderStatus>true, false
    <orderDetails>true, false
    <certificateDetails>true, false
  </orderOption>
  <pageNumber>1..100
</getOrderByDateRange>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **fromDate** | TAK | YYYY-MM-DD | Zakres dat dla złożonych zamówień, parametr wyszukiwania. |
| **toDate** | TAK | YYYY-MM-DD | Zakres dat dla złożonych zamówień, parametr wyszukiwania. |
| **orderStatus** | NIE | true/false | TRUE – zwraca podstawowe informacje o zamówieniu w tym status przetwarzania. |
| **orderDetails** | NIE | true/false | TRUE – zwraca szczegóły zamówienia. |
| **certificateDetails** | NIE | true/false | TRUE – zwraca szczegóły certyfikatu, jeśli został wydany |
| **pageNumber** | NIE | 1…100 | Numer strony z wynikami. Przyjmuje wartości od 1 do 100. W jednym żądaniu zwracane jest maksymalnie 100 wyników. Jeśli liczba zwróconych rekordów jest większa niż 100 są one stronicowane. Brak wartości powoduje zwracanie pierwszej strony wyników. |

## 6.37. getOrdersByDateRangeResponse

Odpowiedź zwraca informacje określone w żądaniu. Jeśli wszystkie parametry były ustawione na false, zwraca jedynie sumę rekordów spełniających kryteria wyszukiwania.

```
<getOrderByDateRangeResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <currentPage>1..100
    <pagesCount>1..100
    <returnCount>5
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <orders>
    <Order reissue="true">
      <orderStatus>
        <orderID>50 String
        <orderStatus>AWAITING, VERIFICATION, ACCEPTED, ENROLLED, REJECTED
        <orderDate>YYYY-MM-DDTHH:MM:SS.000Z
        <productCode>3 String
        <customer>64 String
        <serialNumber>32 String
      </orderStatus>
      <orderDetails>
        <requestorInfo>
          <email>255 String
          <firstName>16 String
          <lastName>40 String
          <phone>32 String
        </requestorInfo>
        <organizationInfo>
          <taxIdentificationNumber>32 String
        </organizationInfo>
      </orderDetails>
      <certificateDetails>
        <certificateStatus>VALID, REVOKING, REVOKED
        <startDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <endDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <commonName>64 String
        <serialNumber>32 String
        <subjectName>3000 String
        <DNSNames>300 String
        <revokedDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <X509Cert>4000 String
      </certificateDetails>
    </Order>
  <orders>
</getOrderByDateRangeResponse>
```

Podstawowe informacje o zamówieniu, jeśli są zwracane w odpowiedzi.

```
      <orderStatus>
        <orderID>50 String
        <orderStatus>AWAITING, VERIFICATION, ACCEPTED, ENROLLED, REJECTED
        <orderDate>YYYY-MM-DDTHH:MM:SS.000Z
        <productCode>3 String
        <customer>64 String
        <serialNumber>32 String
      </orderStatus>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **reissue="true"** | NIE | true | Oznacza certyfikat powstały w wyniku reissue. |
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia. |
| **orderStatus** | TAK | Lista | AWAITING – nowe zamówienie oczekujące na weryfikację,<br>VERIFICATION – zamówienie w trakcie weryfikacji,<br>ACCEPTED – zamówienie zweryfikowane,<br>ENROLLED – certyfikat wystawiony,<br>REJECTED – zamówienie anulowane przez cancelOrder lub odrzucone przez Certum. |
| **orderDate** | TAK | Timestamp | Data złożenia zamówienia. |
| **productCode** | TAK | 3 String | 3-cyfrowy kod produktu. |
| **customer** | TAK | 64 String | Identyfikator klienta. |
| **serialNumber** | NIE | 32 String | Numer seryjny certyfikatu, zwracany wyłącznie gdy certyfikat istnieje, numer certyfikatu w formacie HEX. |

Rozszerzone informacje o zamówieniu, jeśli są zwracane w odpowiedzi.

```
<orderDetails>
  <requestorInfo>
    <email>255 String
    <firstName>16 String
    <lastName>40 String
    <phone>32 String
  </requestorInfo>
  <organizationInfo>
    <taxIdentificationNumber>32 String
  </organizationInfo>
</orderDetails>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **email** | TAK | 3 String | Adres email Subskrybenta. |
| **firstName** | TAK | 16 String | Imię Subskrybenta. |
| **lastName** | TAK | 40 String | Nazwisko Subskrybenta. |
| **phone** | NIE | 32 String | Numer telefonu Subskrybenta. |
| **taxIdentificationNumber** | TAK | 64 String | NIP, KRS albo inny numer identyfikacji podatkowej. |

Rozszerzone informacje o certyfikacie, jeśli są zwracane w odpowiedzi.

```
<certificateDetails>
  <certificateStatus>VALID, REVOKING, REVOKED
  <startDate>25 YYYY-MM-DDTHH:MM:SS.000Z
  <endDate>25 YYYY-MM-DDTHH:MM:SS.000Z
  <commonName>64 String
  <serialNumber>32 String
  <subjectName>3000 String
  <DNSNames>300 String
  <revokedDate>25 YYYY-MM-DDTHH:MM:SS.000Z
  <X509Cert>4000 String
</certificateDetails>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **certificateStatus** | TAK | List | VALID – certyfikat ważny, aktualny,<br>REVOKING – certyfikat w trakcie unieważnienia, taki status mogą mieć certyfikaty oczekujące na unieważnienie po dokonaniu reissue, |

| | | | |
|---|---|---|---|
| | | | REVOKED – certyfikat unieważniony. |
| **startDate** | TAK | Timestamp | Data początku ważności certyfikatu. |
| **endDate** | TAK | Timestamp | Data końca ważności certyfikatu. |
| **commonName** | TAK | 64 String | Nazwa powszechna – imię i nazwisko klienta dla certyfikatu ID, lub nazwę domeny dla certyfikatu SSL. |
| **serialNumber** | TAK | 32 String | Numer seryjny certyfikatu w formacie HEX. |
| **subjectName** | TAK | 3000 String | Zawartość pola Podmiot. |
| **DNSNames** | NIE | 300 String | Zawartość pola SAN, zwracana tylko dla certyfikatów SSL. |
| **revokedDate** | NIE | Timestamp | Data unieważnienia, zwracana tylko jeśli status certyfikatu to REVOKED. |
| **X509Cert** | TAK | 4000 String | Certyfikat w formacie PEM (Base64) |

## 6.38. getModifiedOrdersRequest

Żądanie pozwala pobrać wszystkie zamówienia dla których nastąpiła zmiana statusu w podanym zakresie dat. Wszystkie pozostałe parametry ustawione są domyślnie na false. Struktura całego żądania jest taka sama jak w przypadku **`getOrderByDateRange`**.

```
<getModifiedOrders>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <fromDate>YYYY-MM-DD
  <toDate>YYYY-MM-DD
  <orderOption>
    <orderStatus>true, false
    <orderDetails>true, false
    <certificateDetails>true, false
  </orderOption>
  <pageNumber>1..100
</getModifiedOrders>
```

## 6.39. getModifiedOrdersResponse

Odpowiedź zwraca informacje określone w żądaniu. Jeśli wszystkie parametry były ustawione na false, zwraca jedynie sumę rekordów spełniających kryteria wyszukiwania. Struktura odpowiedzi jest taka sama jak w przypadku **`getOrderByDateRange`**.

```
<getModifiedOrdersResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <currentPage>1..100
    <pagesCount>1..100
    <returnCount>5
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <orders>
    <Order reissue="true">
      <orderStatus>
        <orderID>50 String
        <orderStatus>AWAITING, VERIFICATION, ACCEPTED, ENROLLED, REJECTED
```

```
        <orderDate>YYYY-MM-DDTHH:MM:SS.000Z
        <productCode>3 String
        <customer>64 String
        <serialNumber>32 String
      </orderStatus>
      <orderDetails>
        <requestorInfo>
          <email>255 String
          <firstName>16 String
          <lastName>40 String
          <phone>32 String
        </requestorInfo>
        <organizationInfo>
          <taxIdentificationNumber>32 String
        </organizationInfo>
      </orderDetails>
      <certificateDetails>
        <certificateStatus>VALID, REVOKING, REVOKED
        <startDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <endDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <commonName>64 String
        <serialNumber>32 String
        <subjectName>3000 String
        <DNSNames>300 String
        <revokedDate>25 YYYY-MM-DDTHH:MM:SS.000Z
        <X509Cert>4000 String
      </certificateDetails>
    </Order>
  <orders>
</getModifiedOrdersResponse>
```

## 6.40. getExpiringCertificatesRequest

Żądanie pozwala pobrać raport z wygasających certyfikatów.

```
<getExpiringCertificates>
  <requestHeader>
    <authToken>
      <userName>255 String
      <password>255 String
    </authToken>
  </requestHeader>
  <validityDaysLeft>2
  <pageNumber>1..100
</getExpiringCertificates>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **validityDaysLeft** | TAK | 2 | Liczba dni określająca okres z jakiego mają zostać wyszukane wygasające certyfikaty – limit do 30 dni. |
| **pageNumber** | NIE | 1…100 | Numer strony z wynikami. Przyjmuje wartości od 1 do 100. W jednym żądaniu zwracane jest maksymalnie 100 wyników. Jeśli liczba zwróconych rekordów jest większa niż 100 są one stronicowane. Brak wartości powoduje zwracanie pierwszej strony wyników. |

## 6.41. getExpiringCertificatesResponse

Odpowiedź zwraca informacje określone w żądaniu.

```
<getExpiringCertificatesResponse>
  <responseHeader>
    <successCode>3
    <errors>
      <error>
        <errorCode>5
      </error>
    </errors>
    <currentPage>1..100
    <pagesCount>1..100
    <returnCount>5
    <timestamp>YYYY-MM-DDTHH:MM:SS.000Z
  </responseHeader>
  <expiringCertificates>
    <orderID>50 String
    <serialNumber>32 String
    <expiringDate> YYYY-MM-DDTHH:MM:SS.000Z
    <validityDaysLeft>4
  <expiringCertificates>
</getExpiringCertificatesResponse>
```

| Nazwa pola | Wym. | Typ | Opis |
|---|---|---|---|
| **orderID** | TAK | 50 String | Unikalny identyfikator zamówienia. |
| **serialNumber** | NIE | 32 String | Numer seryjny certyfikatu, zwracany wyłącznie gdy certyfikat istnieje, numer certyfikatu w formacie HEX. |
| **expiringDate** | TAK | Timestamp | Data wygaśnięcia certyfikatu. |
| **validityDaysLeft** | TAK | 4 | Liczba dni do wygaśnięcia certyfikatu. |

# 7. Kody błędów

| Kod błędu | Opis |
|---|---|
| **0** | Zamówienie zostało poprawnie przetworzone. |
| **1** | Wystąpił ogólny błąd podczas przetwarzania zamówienia. Należy skontaktować się z Certum w celu zdiagnozowania problemu. |
| **3** | Dane autoryzacyjne w elemencie requestHeader/authToken nie są poprawne. |
| **1001** | Algorytm klucza publicznego z CSR-a nie jest obsługiwany. |
| **1002** | Element orderParameters/CSR nie został odnaleziony lub jest pusty. |
| **1006** | Element productCode zawiera kod produktu wycofanego z oferty. |
| **1007** | Element SANEntries nie został odnaleziony. |
| **1008** | Element SANEntries/SANEntry/DNSName zawiera błędną nazwę domeny. |
| **1009** | Element requestorInfo nie został odnaleziony. |
| **1010** | Element orderParameters nie został odnaleziony. |
| **1012** | Identyfikator zamówienia jest już zajęty. |
| **1013** | Niepoprawny numer produktu. |
| **1014** | Element orderParameters/productCode nie został odnaleziony. |
| **1015** | Atrybut CommonName nie został znaleziony. |
| **1016** | Atrybut Organization nie został znaleziony. |
| **1017** | Atrybut OrganizationUnit z CSR nie został znaleziony. |
| **1018** | Atrybut Locality z CSR nie został znaleziony. |
| **1019** | Atrybut State z CSR nie został znaleziony. |
| **1020** | Atrybut Country nie został znaleziony. |
| **1021** | Atrybut EmailAddress nie został znaleziony. |
| **1022** | Atrybut EmailAddress zawiera błędy. |
| **1023** | Wartość elementu orderParameters/customer nie może być taka sama jak wartość z elementu requestHeader/authToken/userName. |
| **1024** | Atrybut Common name musi być zakodowany jako UTF8String. |
| **1025** | Atrybut EmailAddress musi być zakodowany jako IA5String. |
| **1026** | Atrybut Country musi być zakodowany jako PrintableString. |
| **1027** | Atrybut State musi być zakodowany jako UTF8String. |
| **1028** | Atrybut Locality musi być zakodowany jako UTF8String. |
| **1029** | Atrybut OrganizationUnit musi być zakodowany jako UTF8String. |
| **1030** | Atrybut Organization musi być zakodowany jako UTF8String. |
| **1031** | Atrybut Common name musi być zakodowany jako PrintableString. |
| **1032** | Klucz publiczny z CSR-a został już wykorzystany. |
| **1033** | Zamówienie o podanym numerze nie istnieje. |
| **1037** | Adres email w elemencie approverEmail zawiera błędy. |
| **1042** | Metoda weryfikacji domeny nie jest obsługiwana. |
| **1043** | Identyfikator zamówienia zawiera niedozwolone znaki "&'<>. |
| **1045** | Domena podana w CommonName, nie występuje na liście domen w elemencie SANEntries. |
| **1046** | Tylko jedna domena w elemencie SANEntries może zawierać gwiazdkę w nazwie domeny. |
| **1048** | Brakuje elementu taxIdentificationNumber lub element ma niepoprawną wartość. |
| **1049** | Nie można odczytać klucza publicznego z CSR. |
| **1053** | Element requestorInfo/email nie został odnaleziony. |
| **1054** | Element requestorInfo/firstName nie został odnaleziony. |
| **1055** | Element requestorInfo/lastName nie został odnaleziony. |
| **1059** | Atrybut Country zawiera nieobsługiwany kod kraju. |
| **1060** | Adres email z elementu requestorInfo/email nie jest poprawny. |
| **1063** | Klucz publiczny z CSR-a znajduje się na czarnej liście. |
| **1065** | Wartość z elementu requestorInfo/lastName przekroczyła dopuszczalny rozmiar 40 znaków. |
| **1066** | Wartość z elementu requestorInfo/phone przekroczyła dopuszczalny rozmiar 32 znaków. |
| **1072** | Wartość z elementu requestorInfo/firstName przekroczyła dopuszczalny rozmiar 16 znaków. |
| **1075** | Partner nie ma uprawnień, aby złożyć zamówienia na dany produkt. |

| | |
|---|---|
| **1076** | Brakuje elementu customer lub jest on pusty. |
| **1077** | Wartość z elementu z customer przekroczyła dopuszczalny rozmiar 64 znaki. |
| **1079** | Wartość elementu orderId przekroczyła dopuszczalny rozmiar 50 znaków. |
| **1080** | Wartość z elementu productCode przekroczyła dopuszczalny rozmiar 3 znaków. |
| **1081** | Wartość z elementu requestorInfo/email przekroczyła dopuszczalny rozmiar 255 znaków. |
| **1083** | Wartość z elementu taxIdentificationNumber przekroczyła dopuszczalny rozmiar 32 znaków. |
| **1085** | Wartość z elementu SANEntries/SANEntry/DNSName przekroczyła dopuszczalny rozmiar znaków. |
| **1087** | Adres email w elemencie approverEmail przekroczył dopuszczalny rozmiar 255 znaków. |
| **1088** | Wartość z elementu orderParameters/language przekroczyła dopuszczalny rozmiar 2 znaków. |
| **1092** | Atrybut JoISoPN nie został znaleziony. |
| **1093** | Atrybut JoISoCN nie został znaleziony. |
| **1094** | Atrybut JoILN nie został znaleziony. |
| **1095** | Atrybut SerialNumber nie został znaleziony. |
| **1096** | Wartość atrybutu JoISoCN przekroczyła dopuszczalny rozmiar 2 znaków. |
| **1097** | Wartość atrybutu JoISoPN przekroczyła dopuszczalny rozmiar 128 znaków. |
| **1098** | Wartość atrybutu JoILN przekroczyła dopuszczalny rozmiar 128 znaków. |
| **1099** | Wartość atrybutu JoISoCN zawiera nieobsługiwany kod kraju. |
| **1100** | Wartość atrybutu SerialNumber przekroczyła dopuszczalny rozmiar 64 znaków. |
| **1101** | Wartość atrybutu CommonName przekroczyła dopuszczalny rozmiar 64 znaków. |
| **1102** | Wartość atrybutu Organization przekroczyła dopuszczalny rozmiar 64 znaków. |
| **1103** | Wartość atrybutu OrganizationalUnit przekroczyła dopuszczalny rozmiar 64 znaków. |
| **1104** | Wartość atrybutu Locality przekroczyła dopuszczalny rozmiar 128 znaków. |
| **1105** | Wartość atrybutu State przekroczyła dopuszczalny rozmiar 128 znaków. |
| **1106** | Wartość atrybutu EmailAddress przekroczyła dopuszczalny rozmiar 64 znaków. |
| **1107** | Ilość domen podanych w elemencie SANEntries przekroczyła dopuszczalną ilość domen dla produktu. |
| **1108** | Wartość z elementu approverEmailPrefix nie pasuje do listy prefixów. |
| **1110** | Data podana w elemencie fromDate jest błędna. |
| **1111** | Data podana w elemencie toDate jest błędna. |
| **1113** | Status zamówienia uniemożliwia wysłanie weryfikacji email. Zamówienie jest w trakcie realizacji lub zostało anulowane. |
| **1114** | Dla podanego zamówienia wszystkie weryfikacje są jeszcze aktualne. Maile weryfikacyjne nie zostały wysłane. |
| **1115** | Element SANEntries/SANEntry/DNSName zawiera domenę typu Wildcard, która nie jest dozwolona dla wybranego produktu. |
| **1116** | CommonName zawiera domenę typu Wildcard, która nie jest dozwolona dla wybranego produktu. |
| **1117** | CommonName nie zawiera domeny typu Wildcard, która jest wymagana dla tego produktu. |
| **1118** | Element SANEntries/SANEntry/DNSName nie zawiera domeny typu Wildcard, która jest wymagana dla tego produktu. |
| **1126** | Atrybut SerialNumber musi być zakodowany jako UTF8String. |
| **1127** | Atrybut JoILN musi być zakodowany jako UTF8String. |
| **1128** | Atrybut JoISoCN musi być zakodowany jako PrintableString. |
| **1129** | Atrybut JoISoPN musi być zakodowany jako UTF8String. |
| **1131** | Element revokeCertificate/RevokeCertificateParameters nie został odnaleziony. |
| **1133** | Brak certyfikatu o podanym numerze seryjnym. |
| **1135** | Nieprawidłowa wartość elementu revokeCertificate/RevokeCertificateParameters/revocationReason. |
| **1138** | Operacja nie może być wykonana. Skontaktuj się z Certum. |
| **1139** | Status zamówienia nie pozwala na jego odrzucenie. Jeśli błąd będzie się powtarzał skontaktuj się z Certum. |
| **1140** | Data podana w elemencie keyCompromitationDate musi być w formacie YYYY-MM-DD. |

| | |
|---|---|
| **1141** | Data podana w elemencie keyCompromitationDate musi zawierać się w przedziale pomiędzy datą początku ważności certyfikatu, a bieżącą datą. |
| **1142** | Wartość elementu revokeCertificate/RevokeCertificateParameters/note przekroczyła dopuszczalny rozmiar 250 znaków. |
| **1143** | Nie można unieważnić certyfikatu, ponieważ certyfikat jest w trakcie unieważniania. |
| **1144** | Nie można unieważnić certyfikatu, ponieważ certyfikat wygasł. |
| **1145** | Nie można unieważnić certyfikatu, ponieważ certyfikat został już unieważniony. |
| **1148** | Nie można złożyć zamówienia na lokalny adres IP. |
| **1151** | Zamówienie zostało już anulowane. |
| **1153** | Numer strony musi być z zakresu [1 - 100]. |
| **1154** | Zapytanie zwróciło zbyt dużą liczbę rekordów. |
| **1155** | Strona z wynikami o podanym numerze nie istnieje. |
| **1156** | Pole customer w orderParameters posiada niedozwolone znaki "&'<>. |
| **1157** | Element SANEntries/SANEntry/DNSName zawiera publiczną domenę najwyższego poziomu. |
| **1159** | Certyfikat nie został odnaleziony. |
| **1160** | Nie podano numeru seryjnego certyfikatu. |
| **1161** | Numer seryjny certyfikatu jest za długi (przekroczono dopuszczalny rozmiar 64 znaków). |
| **1162** | Wymagane parametry nie zostały podane w żądaniu (numer seryjny certyfikatu lub identyfikator zamówienia). |
| **1163** | W żądaniu podano parametry które nie mogą występować jednocześnie (numer seryjny certyfikatu i identyfikator zamówienia). |
| **1164** | Niepoprawna liczba parametrów identyfikujących certyfikat. Podany powinien być numer seryjny certyfikatu lub certyfikat w postaci PEM. |
| **1165** | Niepoprawny format PEM. |
| **1166** | Podany kod produktu nie jest kodem na odnowienie. |
| **1167** | Profil certyfikatu do odnowienia różni się od profilu certyfikatu odnawianego. |
| **1168** | CN certyfikatu różni się od CN certyfikatu odnawianego. |
| **1169** | Nazwa użytkownika w odnawianym certyfikacie jest inna niż podana. |
| **1170** | Odnawiany certyfikat został wystawiony przez innego partnera. |
| **1172** | Żądanie zawiera nadmiarowe elementy. Należy zweryfikować poprawność żądania z dokumentacją. |
| **1176** | Zamówienie jest w statusie, który uniemożliwia dołączanie nowych dokumentów oraz weryfikacji domeny. |
| **1181** | Podany kod produktu, nie jest kodem na wydanie certyfikatu. |
| **1182** | Element code nie został znaleziony. |
| **1183** | Wartość z elementu code przekroczyła dopuszczalny rozmiar 255 znaków. |
| **1184** | Kod weryfikacji domeny już wygasł. |
| **1186** | Kod weryfikacyjny jest niepoprawny. |
| **2005** | Żaden z podanych certyfikatów nie zawiera domen. |
| **2049** | Element verifyOrder/verifyOrderParameters/note nie został znaleziony lub jest pusty. |
| **2050** | Wartość elementu verifyOrderParameters/note przekroczyła dopuszczalny rozmiar 227 znaków. |
| **2051** | Niepoprawna wartość w polu CommonName. |
| **2052** | Element getExpiringCertificates/validityDaysLeft nie został znaleziony lub ma niepoprawną wartość. |
| **2053** | Element cancelParameters nie został odnaleziony. |
| **2055** | Element orderID nie został odnaleziony. |
| **2056** | Status zamówienia nie pozwala na wykonanie akcji. |
| **2057** | Wartość elementu toDate nie może być wcześniejsza od wartości elementu fromDate. |
| **2058** | Atrybut Locality lub StateOfProvince nie został znaleziony. |
| **2059** | Niepoprawna wartość w elemencie verificationNotificationEnabled. |
| **2063** | Element verifyOrder/verifyOrderParameters/documents/document nie został odnaleziony. |
| **2064** | Element verifyOrder/verifyOrderParameters/documents/document/type nie został odnaleziony. |

| | |
|---|---|
| **2065** | Element verifyOrder/verifyOrderParameters/documents/document/description nie został odnaleziony. |
| **2066** | Element verifyOrder/verifyOrderParameters/documents/document/files nie został odnaleziony. |
| **2067** | Element verifyOrder/verifyOrderParameters/documents/document/files/file nie został odnaleziony. |
| **2068** | Element verifyOrder/verifyOrderParameters/documents/document/files/file/filename nie został odnaleziony. |
| **2069** | Element verifyOrder/verifyOrderParameters/documents/document/files/file/content nie został odnaleziony. |
| **2070** | Element verifyOrder/verifyOrderParameters/documents/document/files/file/content powinien być w base64. |
| **2080** | Przekroczono dopuszczalny rozmiar dla żądania. |
| **2081** | Element fileName nie może zawierać znaków: \ / : * ? " < > \| |
| **2082** | Wartość elementu fileName ma nieprawidłową długość. Dopuszczalna długość: od 3 do 255 znaków. |
| **2083** | Typ dokumentu nie jest obsługiwany. |
| **2088** | Długość części domeny z elementu SANEntries/SANEntry/DNSName przekroczyła dopuszczalny rozmiar znaków. |
| **2089** | Algorytm nie jest skonfigurowany. |
| **2090** | W elemencie hashAlgorithm znajduje się niepoprawna wartość. |
| **2091** | Niepoprawna wartość w elemencie getProductList/HashAlgorithm. |
| **2092** | Nie można ponownie wydać certyfikatu, który jest certyfikatem typu reissue. |
| **2093** | Data ważności certyfikatu jest z przeszłości. |
| **2094** | Certyfikat nie spełnia warunków ponownego wydania. |
| **2095** | Element SANEntries/SANEntry/DNSName nie może być pusty. |
| **2096** | Element serialNumber musi być w postaci szesnastkowej. |
| **2097** | Element CSR nie jest poprawnym żądaniem CSR. |
| **2104** | Data kompromitacji klucza może być podana jedynie dla przyczyny unieważnienia Kompromitacja klucza. Data kompromitacji klucza jest niedostępna dla certyfikatów CodeSigning. |
| **2109** | Niedozwolona długość klucza publicznego. |
| **2111** | Element productCode jest pusty lub nie został odnaleziony. |
| **2122** | Reissue produktów w ramach usługi SimplySign jest niedostępne. |
| **2124** | Nieobsługiwana funkcja skrótu. |
| **2125** | CSR zawiera niepoprawny podpis. |
| **2126** | Nie można wydać ponownie certyfikatu reissue dla tego samego certyfikatu. |
| **2127** | Niepoprawna wartość w elemencie certificateDetails. |
| **2128** | Niepoprawna wartość w elemencie orderDetails. |
| **2129** | Niepoprawna wartość w elemencie order Status. |
| **2130** | Element SANEntries/SANEntry/DNSName zawiera domenę istniejącą w wydanym certyfikacie. |
| **2131** | Nie znaleziono zamówienia w bazie. |
| **2137** | Niepoprawna wartość atrybutu businessCategory (BC). |
| **2138** | Nie znaleziono atrybutu businessCategory (BC). |
| **2139** | Atrybut streetAddress (ST) nie został znaleziony. |
| **2140** | Wartość atrybutu streetAddress (ST) przekroczyła 64 znaki. |
| **2141** | Atrybut streetAddress (ST) musi być zakodowany jako UTF8String. |
| **2142** | Kod pocztowy nie został znaleziony. |
| **2143** | Wartość atrybutu postalCode (P) przekroczyła 40 znaków. |
| **2144** | Wartość atrybutu postalCode (P) musi być typu PrintableString. |
| **2153** | Zamówienie o podanym numerze nie zostało złożone przez API. |
| **2154** | Niepoprawna wartość atrybutu postalCode (P). |
| **2155** | Niepoprawna wartość atrybutu Jurisdiction of Incorporation State or Province Name (JoISoPN). |
| **2156** | Niepoprawna wartość atrybutu stateOrProvinceName (SP). |
| **2157** | Brakuje elementu approverMethod. |

| | |
|---|---|
| **2158** | Zbyt wiele elementów. Można podać tylko jeden approverEmail lub approverEmailPrefix. |
| **2159** | Wymagany element approverEmailPrefix nie został podany. |
| **2160** | Wymagany element approverEmail nie został podany. |
| **2162** | Element SANApprover nie został odnaleziony. |
| **2163** | Metoda nie obsługuje podanego typu produktu. |
| **2164** | Atrybut SerialNumber poiada niepoprawną wartość. |
| **2165** | Atrybut Joiln posiada nieproprawną wratość. |
| **2166** | Atrybut Locality posiada niepoprawną wartość. |
| **2167** | Atrybut OrganizationUnit posiada niepoprawną wartość. |
| **2168** | Atrybut Organization posiada niepoprawną wartość |
| **2169** | Atrybut streetAddress posiada niepoprawną wartość. |
| **2170** | Atrybut Description ma nieprawidłową długość. Maksymalna długość to 1000 znaków. |
| **2171** | Metoda weryfikacji nie jest wspierana dla adresu IP |
| **2172** | Wartość revocationContactEmail nie może być taka sama jak wartość z elementu requestHeader/authToken/userName. |
| **2173** | Adres e-mail w revocationContactEmail jest nieprawidłowy. |
| **2185** | Data podana w shortenedValidityPeriod lub ValidityPeriod/NotAfter jest z przeszłości. |
| **2186** | Metoda weryfikacji nie jest obsługiwana dla zamówień zawierających domenę Wildcard. |
| **2188** | Wniosek reissue wymaga ponownej weryfikacji domen. W związku ze zmianami w regulacjach dotyczących metod weryfikacji, istniejące weryfikacje nie mogą być ponownie wykorzystane. Reissue nie może zostać wykonane, złóż nowe zamówienie. |
| **2189** | Limit dokumentów dla zamówienia został przekroczony. |
| **2190** | Powód unieważnienia Zmiana danych nie jest dostępny dla certyfikatów DV. |
| **2191** | Zawartość przynajmniej dwóch załączników jest jednakowa. Nie można dodać dwóch takich samych załączników do jednego zamówienia. |
| **2192** | Certyfikat dla którego próbujesz wykonać operację zawiera niepoprawne domeny. Operacja nie może zostać wykonana, złóż nowe zamówienie. |
| **2193** | Adres IP nie jest dozwolony w certyfikatach EV SSL. |
| **2194** | Atrybut givenName nie został znaleziony. |
| **2195** | Atrybut givenName musi być zakodowany jako UTF8String. |
| **2196** | Wartość giveName Locality przekroczyła dopuszczalny rozmiar 16 znaków. |
| **2197** | Atrybut givenName ma nie poprawną wartość |
| **2198** | Atrybut surname nie został znaleziony. |
| **2199** | Atrybut surname musi być zakodowany jako UTF8String. |
| **2200** | Wartość atrybutu surname przekroczyła dopuszczalny rozmiar 40 znaków. |
| **2201** | Atrybut surname ma nie poprawną wartość |

# 8. Historia zmian

| Data | Wersja | Opis zmian |
|---|---|---|
| **2021-08-01** | 5.0 | Nowa wersja dokumentu. Reorganizacja rozdziałów. Usunięcie literówek. Poprawki w opisach metod API. Nowe diagramy i opisy procesów składania wniosków. |
| **2021-08-06** | 5.1 | Wprowadzenie oznaczenia zmian w metodach API:<br>• na zielono pola dodane do API<br>• na czerwono pola, które są deprecated i w kolejnej wersji będą usunięte<br>Dodanie pola:<br>• userAgent do metod renewCertificate, renewCertificate<br>• shortenedValidityPeriod do metod quickOrder, validateOrderParameters, renewCertificate<br>Opisanie zmiany dla pól z sekcji validityPeriod – pola będą usunięte w kolejnych wersjach, teraz jego działanie jest dostosowanie do shortenedValidityPeriod.<br>Usunięcie niewpieranej wartości RSA-SHA1 z listy hashAlgorithm.<br>Usunięcie kodów błędów 1044, 1070, 1071, 1109.<br>Dodanie kodu błędu 2185. |
| **2021-09-10** | 5.2 | Usunięto pola z żądań oznaczone jako wycofane:<br>• sekcję validityPeriod z quickOrder, validateOrderParameters<br>• pole verificationPhoneNumber z quickOrder getOrderByOrderID<br>• pole id z verifyOrder<br>• wartości słownikowe z pola businessCategory: PRIVATE_ORGANIZATION, BUSINESS_ENTITY, NON_COMMERCIAL_ENTITY, GOVERNMENT_ENTITY<br>Usunięto metody oznaczone jako wycofane:<br>• getDomainVerification<br>• changeApprovers<br>• verifyDomain<br>• sendNotifications<br>• getApproverList<br>• updateDocuments<br>Usunięto kody błędów powiązane z usuniętymi metodami.<br><br>Dodano nowy typ dla słownika approverMethod, wartość ADMIN zastąpi dotychczasową EMAIL.<br>Dodano nowy typ weryfikacji do getOrderState: AUTHORIZATION.<br>Dodano nowe typy dokumentów do verifyOrder: APPLICANT, ORGANIZATION, AUTHORIZATION, ADDITIONAL, VERIFICATION_REPORT, zamiast dotychczasowej listy.<br>Dodano dodatkowe uwagi dotyczące zmian w weryfikacji FILE i ADMIN w rozdziale 3.2.2.<br>Poprawiono interpunkcję i literówki. |
| **2021-10-31** | 5.3 | Dodano nowy tym maila informacyjnego Nieukończona weryfikacja zamówienia.<br>Zaktualizowano opisy kodów błędów: 1108, 1113, 1176, 1191<br>Dodano kody błędów: 2186, 2187, 2188<br>Usunięto kody błędów: 1034, 1035, 1036, 1039, 1041, 1073, 1074, 1086, 1112, 1130, 1158, 1171, 1173, 1174, 1175, 1177, 1178, 1179, 1180, 1188, 1189, 1190, 1192, 1193, 1202, 2060, 2062, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2084, 2086, 2087, 2099, 2116, 2117, 2118, 2119, 2121, 2135, 2145, 2161 |
| **2022-02-01** | 5.4 | Usunięto typ EMAIL ze słownika approverMethod, należy używać wartości ADMIN.<br>Usunięto typy dokumentów KRS, NIP, CEIDG, DUNS, OTHERREG, EMPLOY, CONTRACT, ORDER, NAMELIST, INVOICE, OTHER.<br>W rozdziale 3.2.3. dodano dodatkowe informacje dotyczące weryfikacji Subskrybenta i organizacji za pomocą dedykowanych typów dokumentów.<br>Zaktualizowano opisy kodów błędów: 1037, 1045, 1048, 1076, 1083, 1140, 1141, 1154, 2144, 2186<br>Usunięto kody błędów: 1149, 1185, 1187 |

| | | |
|---|---|---|
| **2022-03-17** | 5.5 | Zaktualizowano dokumentację getCertificateResponse usuwając pola których nie ma w odpowiedzi na API.<br>Dodano metodę getDocumentsListRequest |
| **2022-07-15** | 5.6 | W rozdziale 3.2. usunięto pole OU ze specyfikacji Trusted SSL i Premium EV SSL.<br>W rozdziale 3.2.2. Zmieniono nazwę metody weryfiacji DNS na DNS_TXT i dodano nowe metody: DNS_CNAME, DNS_TXT_PREFIX oraz DNS_CNAME_PREFIX.<br>W rozdziałach 4.1.4. i 4.1.5. dodano uwagę o zmianie dotyczącej pola OU w procesie reissue i odnowienia.<br>Nowe wartości DNS_TXT, DNS_CNAME, DNS_TXT_PREFIX, DNS_CNAME_PREFIX zostały dodane. Wartość DNS została oznaczona jako przestarzała.<br>Zmieniono opis w metodzie revokeCertificate i kodzie błędu 2104: dla certyfikatów CodeSigning nie można podać daty kompromitacji klucza.<br>Usunięto wartości oznaczone jako wycofane:<br>• typy dokumentów: KRS, NIP, CEIDG, DUNS, OTHERREG, EMPLOY, CONTRACT, ORDER, NAMELIST, INVOICE, OTHER<br>• metoda weryfikacji EMAIL |
| **2022-11-04** | 5.7 | W rozdziale 2.9 dodano listę nazw produktów• z kodami.<br>Zaktualizowano opis dla powodów unieważnienia, usunięto PRIVILEGEWITHDRAWN, dodano SUPERSEDED.<br>Dodano treść kodu błędy 2173, 2189, 2190, 2191, 2192. |
| **2023-05-25** | 5.8 | W rozdziale 2.4 i 2.5 dodano informajcę o terminie wycofania produktów E-mail ID.<br>Usunięto informacje o produktach Standard CodeSigning na kartę, dodano do nazw produktów Standard Codesigning, EV Code Signing i Document Signing brakujące dopiski "w chmurze".<br>W rozdziale 3.2.1 poprawiono opis zawartości pola customer dla produktów w chmurze i dodano informację o tym wymaganiu do rozdziałów 3.5 i 3.6.<br>W rozdziale 3.2.2 poprawiono opis metody weryfikacji ADMIN.<br>W rozdziale 4.1.4 dodano informację o zablokowaniu reissue dla produktów Code Signing wystawianych na kartę.<br>Poprawiono opis pola shortedValidityPeriod w metodach quickOrder i renewCertificate.<br>Zaktualizowano opisy kodów błędów: 1176, 2122<br>Dodano kody błędów: 1017, 1018, 1019, 1024, 1031, 2139, 2142, 2153, 2170, 2172, 2193<br>Usunięto kody błędów: 1089, 1090, 1147, 1191, 2043, 2044, 2048, 2061, 2085, 2098, 2187. |
| **2023-07-13** | 5.9 | W rozdziale 2 i 3 dodano nowe produkty S/MIME, usunięto E-mail ID:<br>• 2.1 zaktualizowano listę produktów, poprawiono podział i nazwy<br>• 2.2 dodano opisy nowych produktów S/MIME, usunięto E-mail ID<br>• 2.5 dodano nowe kody na produkty S/MIME, usunięto E-mail ID<br>• 3.2 uzupełniono tabele opisujące wymagane pola dla produktów S/MIME, usunięto z nich E-mail ID<br>• 3.4, 3.5 i 3.5 zaktualizowano nazwę produktu z E-mail ID na Certum S/MIME Sponsor<br>W całej dokumentacji zamieniono „E-mail ID (S/MIME)" na „S/MIME".<br>Dodano pola givenName i surname do metod: quickOrder i validateOrderParameters.<br>Usunięto wycofaną wartość DNS z listy approverMethod.<br>W rozdziale 5.34 usunięto wycofaną wartość PRIVILEGEWITHDRAWN.<br>W rozdziale 4.1.4 i 4.1.5 usunięto uwagę dotyczącą głosowania SC47.<br>Zaktualizowano opisy kodów błędów: 1059, 1099, 2056<br>Dodano kody błędów: 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201 |
| **2023-12-15** | 5.10 | W rozdziale 3.3, 4.2, 4.5, 5.3, 6.23 i 6.24 usunięto informację o obecności pola Email w certyfikatach Standard Code Signing w chmurze. Pole nie wystepuje już w certyfikatach Standard Code Signing w chmurze. |

| | |
|---|---|
| | W rozdziale 4.2 usunięto opcjonalne pole OU ze Standard CodeSigning w chmurze, EV Code Signing w chmurze, Document Signing w chmurze. Pole nie występuje już w żadnym z certyfikatów Certum.<br>W metodach QuickOrder i validateOrderParameters usunięto pole organizationalUnit z żądań API.<br>W sekcji requestorInfo, długość pól firstName i lastName została dostosowana, aby pasowała do występujących w certyfikacie givenName i surname.<br>W sekcji orderParameters, długość pola email została zmieniona na 64 String.<br>Zaktualizowano opisy kodów błędów: 1065, 1072, 1106 |