Centralny Punkt Rejestracji Cencert
tel. 22 720 79 55 | 666 028 044
ul. Jagiellońska 78 03-301 Warszawa, II piętro, pok. 345

Zawartość raportu kwalifikowanej usługi walidacji GetValid

Wersja z dnia 15.07.2024

Spis treści

1. WSTĘP

Niniejszy dokument zawiera opis zawartości raportu walidacji usługi GetValid prezentującego wyniki walidacji podpisów i pieczęci elektronicznych dokumentu elektronicznego.

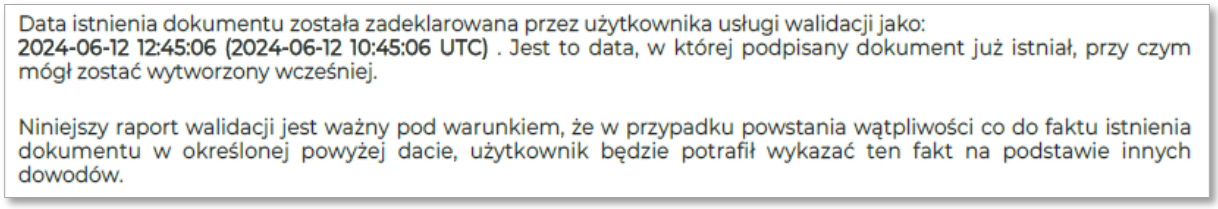
Opis został przedstawiony na przykładzie oryginalnego raportu, dla którego zaprezentowano i omówiono możliwą zawartość oraz znaczenie poszczególnych pól raportu.

Ponieważ z technicznego punktu widzenia pomiędzy podpisem elektronicznym, a pieczęcią elektroniczną nie ma różnic, to wszystkie informacje odnoszące się do podpisów odnoszą się również do pieczęci, chyba że w treści dokumentu dokonano wyraźnego rozróżnienia obu przypadków.

2. RAPORT WALIDACJI

2.1. Strona główna raportu

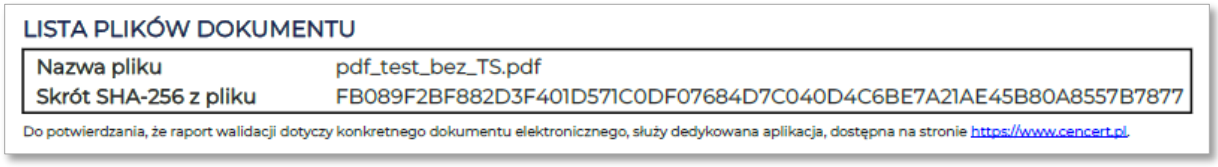
Nagłówek raportu



- **Numer raportu** – numer jednoznacznie identyfikujący raport.
- **Data przedłożenia dokumentu do walidacji** – data określająca moment, w którym serwer usługi GetValid otrzymał dokument do walidacji[1]. Data podana jest zarówno w czasie urzędowym RP jak i w czasie UTC.
- **Data wystawienia raportu** – data określająca moment wygenerowania raportu walidacji.
- **Data istnienia dokumentu zadeklarowana przez użytkownika** – informacja o dacie istnienia dokumentu pojawia się w raporcie tylko w przypadku, gdy użytkownik wprowadzając dokument do walidacji wskazał konkretną datę, w której podpisany dokument wg. użytkownika już istniał. Jakie znaczenie ma ta data i kiedy powinno się ją wprowadzać zostało opisane w **rozdziale 3**.

[1] W rzeczywistości do serwera GetValid nie są przesyłane dokumenty, a wyłącznie skróty z dokumentów oraz same podpisy.

Nazwa pliku i Skrót SHA-256 z pliku


LISTA PLIKÓW DOKUMENTU

Nazwa pliku	pdf_test_bez_TS.pdf
Skrót SHA-256 z pliku	FB089F2BF882D3F401D571C0DF07684D7C040D4C6BE7A21AE45B80A8557B7877

Do potwierdzania, że raport walidacji dotyczy konkretnego dokumentu elektronicznego, służy dedykowana aplikacja, dostępna na stronie https://www.cencert.pl.

Sekcja zawiera listę plików jakie składają się na podpisany dokument (podpis pod dokumentem może być w osobnym pliku lub dokument może mieć załączniki). Raport prezentuje nazwy plików oraz skróty SHA-256 z ich zawartości. Dane te pozwalają powiązać dokument z raportem walidacji, przy czym, aby uzyskać pewność, że dany raport dotyczy wskazanego dokumentu, należy użyć dedykowanej aplikacji dostępnej na stronach Cencert, która wykonuje takie sprawdzenie.

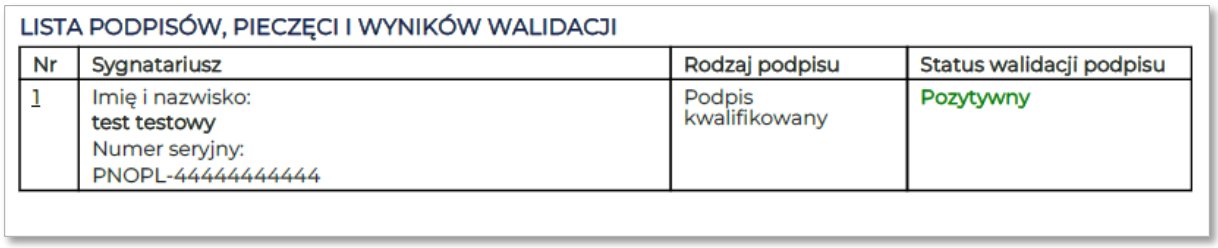
Ostrzeżenia związane z dokumentem


OSTRZEŻENIA ZWIĄZANE Z DOKUMENTEM

Brak

Usługa GetValid bada nie tylko ważność podpisów i pieczęci, ale stara się ostrzec użytkownika przed takimi manipulacjami, które nie naruszając ważności podpisu mogą wprowadzić użytkownika w błąd co do treści dokumentu. Na przykład, do podpisanej umowy w formacie PDF, bez naruszania podpisu można dodać dodatkowy paragraf i w ten sposób próbować zmanipulować jej treść. Szczegółowy opis możliwych ostrzeżeń znajduje się w **rozdziale 3.2.**

Lista podpisów, pieczęci i wyników walidacji


LISTA PODPISÓW, PIECZĘCI I WYNIKÓW WALIDACJI

Nr	Sygnatariusz	Rodzaj podpisu	Status walidacji podpisu
1	Imię i nazwisko: **test testowy** Numer seryjny: PNOPL-44444444444	Podpis kwalifikowany	Pozytywny

Sekcja zawiera podstawowe informacje dotyczące sygnatariuszy, podpisów oraz wyników ich walidacji.

Kolumna	Znaczenie
Sygnatariusz	Dla podpisów, kolumna zawiera: o Imię i nazwisko osoby, która złożyła podpis o Numer PESEL lub numer dokumentu jednoznacznie identyfikującego osobę, która złożyła podpis Dla pieczęci, kolumna zawiera wszystkie pola identyfikatora wyróżniającego właściciela certyfikatu użytego do złożenia podpisu.
Rodzaj podpisu	Określa rodzaj podpisu. Pełna lista znajduje się w **rozdziale 3.4.**

Status walidacji podpisu	Zawiera wynik walidacji danego podpisu: o Pozytywny – podpis jest ważny o Negatywny – podpis jest nieważny o Nieokreślony – zebrane przesłanki nie pozwalają na jednoznaczne określenie wyniku walidacji Wyniki „**pozytywny**" i „**negatywny**" są ostateczne i nie należy oczekiwać, że przy powtórzeniu walidacji możemy otrzymać inny rezultat, chyba że zmieni się informacja na temat daty podpisania dokumentu tj. użytkownik ponowi walidację samodzielnie wprowadzając inną datę istnienia podpisanego dokumentu. Wynik „**nieokreślony**" oznacza, że usługa nie jest w stanie zdecydować ani o ważności danego podpisu, ani o jego nieważności. Dalsze działania użytkownika powinny zależeć od informacji, opisanych w polu **Szczegóły statusu walidacji** w części raportu zawierającej szczegóły walidacji danego podpisu (**patrz rozdziały 2.2 i 3.5**.

2.2. Szczegóły walidacji podpisów

- **Sygnatariusz**

Sygnatariusz	Kraj: PL Nazwisko: **testowy** Imię: **test** Nazwa powszechna: test testowy Numer seryjny: PNOPL-44444444444

Pole zawiera pełną informację o identyfikatorze wyróżniającym właściciela certyfikatu użytego do złożenia podpisu.

- **Użyto pseudonimu**

Użyto pseudonimu	Nie

Pole wskazuje, czy identyfikator właściciela certyfikatu zawiera w miejsce imienia i nazwiska pseudonim. Możliwe wartości: Tak, Nie

- **Rodzaj podpisu**

Rodzaj podpisu	Podpis kwalifikowany

Pełna lista dostępnych rodzajów podpisów znajduje się w **rozdziale 3.4**.

- **Format podpisu** dla norm XAdES, PAdES, CAdES, ASiC.

Forma podpisu	XAdES T

- **Status walidacji podpisu**

Możliwe wartości zostały opisane w części "Lista podpisów, pieczęci i wyników walidacji" w **rozdziale 2.1**.

- **Szczegóły statusu walidacji**

Pole wypełniane jest dla przypadku statusu walidacji innego niż pozytywny i wskazuje przyczynę niepoprawnej walidacji np. unieważnienie certyfikatu, czy użycie skompromitowanego algorytmu SHA-1. Szczegółowa lista przyczyn wraz z omówieniem ich znaczenia znajduje się w **rozdziale 3.5**. Więcej informacji o akceptacji podpisów złożonych z użyciem algorytmu SHA-1 znajduje się w **rozdziale 3.8.**

- **Weryfikacja integralności**

Pole określa status weryfikacji integralności dokumentu. Możliwe wartości:

- Pozytywna – zawartość dokumentu nie została zmodyfikowana po złożeniu podpisu
- Negatywna – zawartość dokumentu lub podpisu została zmodyfikowana po złożeniu podpisu

- **Weryfikacja certyfikatu**

Pole określa status weryfikacji ważności certyfikatu użytego do weryfikacji podpisu. Możliwe wartości:

- Pozytywna – certyfikat jest ważny dla przyjętej daty dowodu istnienia podpisu
- Negatywna – certyfikat jest nieważny dla przyjętej daty dowodu istnienia podpisu
- Nieokreślona – ważności certyfikatu nie można określić dla przyjętej daty dowodu istnienia podpisu

Statusowi mogą towarzyszyć informacje dodatkowe:

- Źródło informacji o unieważnieniach:
  - OCSP + [data wystawienia odpowiedzi OCSP] – źródłem jest serwer OCSP
  - CRL + [data wystawienia listy CRL] – źródłem jest lista CRL
- Źródło + data dowodu istnienia podpisu. Możliwe wartości to:
  - Kwalifikowany znacznik czasu
  - Niekwalifikowany znacznik czasu
  - Data podana przez użytkownika
  - Data przedłożenia do walidacji

- **Znacznik czasu**

Pole "Znacznik czasu" określa, czy podpis został oznakowany czasem, przy czym wykazywane są wyłącznie znaczniki czasu, których weryfikacja się powiodła i które mają zastosowanie do danego typu podpisu[2]. Możliwe wartości:

- Nie – podpis nie został oznakowany znacznikiem czasu.
- Kwalifikowany + [data ze znacznika czasu] – podpis został oznakowany kwalifikowanym znacznikiem czasu.
- Niekwalifikowany + [data ze znacznika czasu] – podpis został oznakowany niekwalifikowanym znacznikiem czasu.

W przypadku, gdy podpis oznakowany jest wieloma znacznikami czasu, to prezentowana jest data ze znacznika najwcześniejszego, czyli złożonego w momencie najbliższym momentowi złożenia podpisu.

Więcej na temat kwalifikowanego znacznika czasu **w rozdziale 3.6**.

- **Deklarowany czas złożenia podpisu**

Pole zawiera informację o czasie złożenia podpisu umieszczaną w strukturach podpisu przez aplikację podpisującą, w oparciu o bieżący czas komputera, na którym składano podpis. Pole to ma jedynie wartość informacyjną i nie jest wykorzystywane podczas walidacji, gdyż bieżący czas komputera, na którym składano podpis mógł być błędny lub celowo zmanipulowany.

- **Zweryfikowany czas złożenia podpisu**

Obecnie technologia nie pozwala na określenie dokładnej daty złożenia podpisu. Kwalifikowany znacznik czasu, którym opatrzono dokument po złożeniu podpisu, pozwala jedynie ustalić, że podpis został złożony "nie później niż" data kwalifikowanego znacznika czasu. Możliwe jest jednak określenie przedziału czasu, w którym podpis został złożony, pod warunkiem, że również uprzednio (przed złożeniem danego podpisu) dokument został opatrzony kwalifikowanym znacznikiem czasu. Taki wcześniejszy znacznik czasu pozwala ustalić, że podpis został złożony "nie wcześniej niż" data tego znacznika.

Ponieważ dokładność określenia daty złożenia podpisu może mieć dla użytkowników istotne znaczenie dowodowe lub prawne, usługa GetValid prezentuje w polu "Zweryfikowany czas złożenia podpisu" przedział czasu, w którym podpis został złożony,

[2] W przypadku, gdy weryfikowany podpis **kwalifikowany** jest opatrzony **niekwalifikowanym** znacznikiem czasu, to taki znacznik nie jest brany pod uwagę podczas walidacji i nie jest wykazywany na raporcie.

wyznaczony przez najbliższe podpisowi kwalifikowane znaczniki czasu, którymi opatrzono dokument przed i po złożeniu podpisu. Możliwe wartości:

- Nie – brak kwalifikowanych znaczników czasu w dokumencie
- Nie później niż + [data ze znacznika czasu] – jeżeli dokument został opatrzony kwalifikowanym znacznikiem czasu jedynie po złożeniu podpisu
- Nie wcześniej niż + [data ze znacznika czasu]; nie później niż + [data ze znacznika czasu] – jeżeli dokument został opatrzony kwalifikowanym przed i po złożeniu podpisu

Dla danego podpisu uwzględniane są kwalifikowane znaczniki czasu (uprzedni i następczy) najbliższe momentowi złożenia podpisu.

Dla uzyskania największej dokładności w określeniu czasu złożenia podpisu proponujemy postępować zgodnie ze wskazówkami zawartymi w **rozdziale 3.6**.

- **Informacja o unieważnieniu uzyskana na podstawie**

Informacja o unieważnieniu uzyskana na podstawie	OCSP 2024-06-12 10:53:38 UTC

Pole to informuje na podstawie jakiego źródła usługa GetValid badała, czy certyfikat jest ważny. Możliwe wartości:

- OCSP + [data wystawienia odpowiedzi OCSP] – źródłem jest serwer OCSP
- CRL + [data wystawienia listy CRL] – źródłem jest lista CRL

- **Data unieważnienia**

Data unieważnienia	Nie dotyczy

Jeśli certyfikat został unieważniony lub zawieszony, to w tym polu znajduje się informacja o dacie unieważnienia lub zawieszenia.

- **Przyczyna unieważnienia**

Przyczyna unieważnienia	Nie dotyczy

Jeśli certyfikat został unieważniony, to w tym polu znajduje się informacja o przyczynie unieważnienia certyfikatu. Informacja ta ma znikome znaczenie praktyczne, gdyż niezależnie od przyczyny unieważnienie certyfikatu skutkuje nieważnością podpisów złożonych po tym fakcie.

- **Numer certyfikatu sygnatariusza**

Numer certyfikatu sygnatariusza	018BFA3256E7BEDE
Wystawiony przez	Kraj: PL Organizacja: Enigma Systemy Ochrony Informacji Sp. z o.o. Nazwa powszechna: CenCert QTSP CA Identyfikator organizacji: VATPL-5261029614

Pola określają numer seryjny certyfikatu sygnatariusza oraz identyfikator podmiotu będącego wystawcą certyfikatu użytego do weryfikacji podpisu.

- **Daty ważności**

Daty ważności	Od: 2024-06-12 09:04:56 UTC Do: 2025-06-12 23:59:59 UTC

Pole zawiera przedział ważności certyfikatu sygnatariusza użytego do weryfikacji podpisu.

- **Skrót z podpisanych danych**

Skrót z podpisanych danych	SHA-256 47DC16890375DF1DD4D6DFE5D1D3684D4688A1B932E2FAF0E973A70C247E8B6F

Pole zawiera informacje o algorytmie i wartości skrótu podpisanych danych.

- **Ostrzeżenia**

Ostrzeżenia	Brak

Pole zawiera ostrzeżenia związane z danym podpisem, które nie wpływają na wynik walidacji podpisu, ale o których użytkownik powinien zostać poinformowany. Opis dostępnych ostrzeżeń znajduje się w **rozdziale 3.3.**

3. INFORMACJE SZCZEGÓŁOWE

3.1. Data istnienia dokumentu zadeklarowana przez użytkownika

Zgodnie z prawem podpis uznaje się za ważny, jeśli został złożony w momencie, gdy certyfikat użyty do tego celu był ważny. Gdyby certyfikat został unieważniony, usługa porównałaby datę złożenia podpisu z datą unieważnienia certyfikatu. Jeśli podpis został złożony przed momentem unieważnienia, to podpis jest ważny. Jeśli został złożony po momencie unieważnienia, to podpis jest nieważny.

Skąd usługa walidacji wie, kiedy został złożony podpis? Źródłem pozwalającym na określenie daty złożenia podpisu[3] może być:

- Kwalifikowany znacznik czasu.
- Moment przedłożenia dokumentu do walidacji.
- Data zadeklarowana przez użytkownika.

Najpewniejszym rozwiązaniem jest opatrzenie dokumentu kwalifikowanym znacznikiem czasu w momencie składania podpisu, względnie w możliwie najkrótszym czasie po nim. Wówczas usługa walidacji ma pewność, że podpis został złożony nie później niż data kwalifikowanego znacznika czasu i na ten moment będzie weryfikowała ważność certyfikatu podpisu (więcej na temat kwalifikowanego znacznika czasu w **rozdziale 3.6).**

W przypadku, gdy dokument nie został oznakowany czasem, wówczas usługa walidacji będzie weryfikować ważność certyfikatu podpisu na moment przedłożenia dokumentu do walidacji. Jeżeli pomiędzy momentem złożenia podpisu a momentem poddania dokumentu walidacji upłynęło dużo czasu, certyfikat podpisu mógł wygasnąć lub zostać unieważniony, a wówczas wynik walidacji nie będzie pozytywny.

W takiej sytuacji jedyną możliwością uzyskania pozytywnego wyniku walidacji będzie wprowadzenie (zadeklarowanie) daty istnienia podpisanego dokumentu przez użytkownika. Należy jednak pamiętać, że ciężar dowodu poprawności tej daty spoczywa na użytkowniku. Raport walidacji będzie ważny pod warunkiem, że w przypadku powstania wątpliwości co do faktu istnienia dokumentu w określonej dacie, użytkownik będzie potrafił wykazać ten fakt na podstawie innych dowodów.

[3] W rzeczywistości usługa określa datę złożenia podpisu z pewnym przybliżeniem (nie później niż). Z własności podpisu elektronicznego wynika, że jeśli certyfikat ważny był w pewnym momencie czasu, to ważny był również w dowolnym momencie wcześniejszym, a w szczególności w tym w którym faktycznie został użyty do złożenia podpisu. Dlatego dla walidacji podpisu wystarczy wykazać ważność certyfikatu w dowolnym momencie późniejszym niż złożenie podpisu.

3.2. Ostrzeżenia związane z dokumentem

Ostrzeżenie	Znaczenie
Brak	Nie wykryto żadnych problemów z dokumentem.
Dokument zawiera aktywną zawartość, która może wpływać na prezentowaną treść.	W dokumencie PDF znajduje się JavaScript, który może wpływać na prezentowaną użytkownikowi treść podczas wyświetlania dokumentu np. prezentując różną zawartość dokumentu w zależności od daty. JavaScript może jednak pełnić pożyteczne funkcje np. walidować poprawność pól formularza.
W dokumencie, na stronach <numery stron> znajduje się treść nieobjęta przez wszystkie podpisy. lub W dokumencie, na stronach <numery stron> (oraz dalszych, łączna liczba takich stron wynosi <liczba stron>) znajduje się treść nie objęta przez wszystkie podpisy.	Dokument PDF zawiera zawartość, która nie jest objęta przez wszystkie podpisy. Może to być celowa próba manipulacji, ale może być to również działanie całkowicie zamierzone i nieszkodliwe np.: • Do podpisanego dokumentu dodano komentarze czy adnotacje. W takim przypadku adnotacje nie są objęte podpisem, ale nie są również próbą manipulacji treścią dokumentu. • Autor formularza podpisał formularz po czym użytkownik wypełnił formularz i złożył własny podpis. W takim przypadku oba podpisy obejmują różną zawartość.

3.3. Ostrzeżenia związane z podpisem

Ostrzeżenie	Znaczenie
Brak podpisanego atrybutu: 'SigningCertificate'.	Ostrzeżenie to dotyczy konkretnego podpisu i oznacza, że w podpisanych danych nie zamieszczono wskazania na certyfikat do weryfikacji podpisu. Oznacza to, że gdyby istniało dwa lub więcej certyfikatów wystawionych na ten sam klucz, ale zawierających różniące się od siebie dane właściciela certyfikatu, to nie można by rozstrzygnąć którym certyfikatem wykonano faktyczny podpis. Byłaby więc możliwość wskazania jako autora innego subskrybenta posługującego się tym samym kluczem. Oprogramowanie Acrobat Reader, które często jest używane do podpisywania dokumentów PDF

	posiada opcję, która ustawia zastosowanie formatu podpisu (PKCS#7) niezgodnego z europejskim prawem i niezawierającego wymaganego atrybutu. Niestety opcja ta domyślnie jest włączona, co może oznaczać, że wiele dokumentów PDF jest podpisywanych bez zamieszczenia tego atrybutu. Ryzyko akceptacji dokumentu bez atrybutu 'SigningCertifiate' wydaje się małe, gdyż uzyskanie certyfikatów kwalifikowanych zawierających różne dane subskrybenta na ten sam klucz publiczny jest mało prawdopodobne, a potencjalne ataki są ograniczone.

3.4. Rodzaje podpisów i pieczęci

- Podpis kwalifikowany
- Pieczęć kwalifikowana
- Podpis Osobisty – zaawansowany podpis elektroniczny składany za pomocą kluczy znajdujących się na dowodzie osobistym
- Podpis EPUAP – zaawansowany podpis elektroniczny składany przy pomocy platformy EPUAP
- Podpis zaawansowany weryfikowany kwalifikowanym certyfikatem
- Pieczęć zaawansowana weryfikowana kwalifikowanym certyfikatem
- Podpis zaawansowany
- Pieczęć zaawansowana
- Pieczęć kwalifikowanej usługi Walidacji Podpisów i Pieczęci
- Pieczęć kwalifikowanej usługi Rejestrowanej Poczty Elektronicznej
- Pieczęć kwalifikowanej usługi Elektronicznego Doręczenia
- Pieczęć kwalifikowanej usługi Konserwacji Podpisów i Pieczęci

3.5. Szczegóły statusu walidacji

3.5.1. Informacje szczegółowe dla przypadku statusu walidacji „**nieważny**"

Wartość	Opis
Skrót z dokumentu nie zgadza się z podpisanym skrótem	Dokument lub podpis został zmodyfikowany po wykonaniu podpisu lub podpis nie jest do tego dokumentu.
Podpis złożony certyfikatem po okresie ważności	Podpis został złożony po okresie ważności certyfikatu. **Możliwe działanie**: Rozważyć, czy istnieje dowód na istnienie podpisanego dokumentu

	wcześniej, w okresie ważności certyfikatu; jeśli tak – wprowadzić datę z tego dowodu przy powtórnym wywołaniu usługi walidacji
Podpis złożony unieważnionym certfikatem	Podpis został złożony po unieważnieniu certyfikatu. **Możliwe działanie**: Rozważyć, czy istnieje dowód na istnienie podpisanego dokumentu wcześniej, przed datą unieważnienia certyfikatu; jeśli tak – wprowadzić datę z tego dowodu przy powtórnym wywołaniu.
Błędny format podpisu	Przekazany do walidacji dokument posiada podpis, którego format jest niepoprawny co uniemożliwia jego walidację.
Podpis nie może być zweryfikowany kluczem publicznym z certyfikatu podpisu	Dokument lub podpis został zmodyfikowany po wykonaniu podpisu lub podpis nie jest do tego dokumentu.

3.5.2. Informacje szczegółowe dla przypadku statusu walidacji „**nieokreślony**”

Wartość	Opis
Atrybut wskazujący certyfikat do weryfikacji podpisu wskazuje na inny certyfikat niż użyty do złożenia podpisu	Błąd struktury podpisu (fałszerstwo lub błąd oprogramowania podpisującego)
Błąd weryfikacji ścieżki certyfikatów	Usługa nie jest w stanie zweryfikować ścieżki zaufania dla certyfikatu użytego do weryfikacji podpisu. Pojawienie się tego błędu jest skrajnie mało prawdopodobne, gdyż oznaczałoby błąd leżący po stronie wystawcy certyfikatu.
Nie można zbudować ścieżki certyfikacji dla certyfikatu podpisu	Nie da się zbudować ścieżki zaufania do certyfikatu użytego do złożenia podpisu, na podstawie posiadanych list TSL. Przyczyną jest to, że wystawca certyfikatu nie znajduje się na liście zaufanych wystawców certyfikatów kwalifikowanych i niekwalifikowanych uznanych przez EU.
Algorytm kryptograficzny nie spełnia warunków walidacji	Do złożenia podpisu lub do wystawienia jednego z analizowanych certyfikatów i list CRL został użyty algorytm kryptograficzny, co do

	którego są wątpliwości, czy jest wystarczająco bezpieczny. Więcej informacji o akceptacji podpisów złożonych z użyciem algorytmu SHA-1 znajduje się w **rozdziale** Błąd! Nie można odnaleźć źródła odwołania.
Niepoprawna kolejność znaczników czasu	Co najmniej jeden ze znaczników czasu dołączonych do dokumentu wskazuje niepoprawną datę (został dodany później, a mimo to wskazuje na wcześniejszą datę). Pojawienie się tego błędu jest skrajnie mało prawdopodobne, gdyż oznaczałoby błąd leżący po stronie dostawcy usługi znakowania czasem.
Niedostępny certyfikat podpisu	Certyfikat użyty do złożenia podpisu nie został załączony do dokumentu i nie jest dostępny dla usługi walidacji.
Certyfikat podpisu został unieważniony natomiast nie określono daty dowodu istnienia podpisu lub Certyfikat wystawcy certyfikatów został unieważniony natomiast nie określono daty dowodu istnienia podpisu lub Certyfikat podpisu jest poza okresem ważności natomiast nie określono daty dowodu istnienia podpisu	Dokument przekazany do walidacji nie został oznakowany czasem ani użytkownik nie wskazał manualnie daty istnienia dokumentu w związku tym usługa przyjęła jako datę istnienia podpisu czas bieżący. Dla tak przyjętej daty występuje wskazany problem z ważnością certyfikatu, który być może nie występował w momencie składania podpisu. **Możliwe działanie**: Rozważyć, czy istnieje dowód na istnienie podpisanego dokumentu wcześniej, przed datą unieważnienia lub przeterminowania certyfikatu; jeśli tak – wprowadzić datę z tego dowodu przy powtórnym wywołaniu walidacji.
Algorytm kryptograficzny nie spełnia obecnych warunków walidacji natomiast nie określono daty dowodu istnienia podpisu	Dokument przekazany do walidacji nie został oznakowany czasem ani użytkownik nie wskazał manualnie daty istnienia dokumentu w związku tym usługa przyjęła jako datę istnienia podpisu czas bieżący. Dla tak przyjętej daty występuje problem z bezpieczeństwem wskazanego algorytmu, który być może nie występował w momencie składania podpisu. **Możliwe działanie**:

	Rozważyć, czy istnieje dowód na istnienie podpisanego dokumentu wcześniej, przed datą uznania algorytmu za niebezpieczny; jeśli tak – wprowadzić datę z tego dowodu przy powtórnym wywołaniu walidacji. Więcej informacji o akceptacji podpisów złożonych z użyciem algorytmu SHA-1 znajduje się w **rozdziale 3.8.**
Certyfikat podpisu zawieszony lub Certyfikat wystawcy certyfikatów zawieszony	Certyfikat został zawieszony przez wystawcę więc ważność podpisu nie może zostać określona do czasu uchylenia zawieszenia lub unieważnienia certyfikatu. **Możliwe działania:** Powtórzyć usługę walidacji po pewnym czasie (czas zawieszenia certyfikatu na ogół nie przekracza kilku dni). Ewentualnie rozważyć, czy istnieje dowód na istnienie podpisanego dokumentu wcześniej, przed zawieszeniem certyfikatu; jeśli tak – wprowadzić datę z tego dowodu przy powtórnym wywołaniu usługi walidacji.
CRL/OCSP niedostępny lub ARL/OCSP niedostępny	Usługa walidacji nie ma dostępu do informacji o unieważnieniach, którą powinien publikować wystawca certyfikatu, w związku tym nie można zweryfikować ważności certyfikatu użytego do weryfikacji podpisu. Brak dostępu może być spowodowany awarią po stronie wystawcy certyfikatu podpisu. **Możliwe działania:** Powtórzyć usługę walidacji po pewnym czasie.
CRL/OCSP przeterminowany oraz brak daty dowodu istnienia podpisu. lub ARL/OCSP przeterminowany oraz brak daty dowodu istnienia podpisu	Dokument przekazany do walidacji nie został oznakowany czasem ani użytkownik nie wskazał manualnie daty istnienia dokumentu w związku tym usługa przyjęła jako datę istnienia podpisu czas bieżący. Dla tak przyjętej daty występuje problem ze świeżością posiadanej przez usługę informacji o unieważnieniach, który być może nie występował w momencie składania podpisu. Brak odpowiednio świeżej

	informacji o unieważnieniach może być spowodowany awarią po stronie wystawcy certyfikatu podpisu. **Możliwe działania:** Powtórzyć usługę walidacji po pewnym czasie. Rozważyć, czy istnieje dowód na istnienie podpisanego dokumentu wcześniej, przed datą bieżącą; jeśli tak – wprowadzić datę z tego dowodu przy powtórnym wywołaniu usługi walidacji.
CRL/OCSP wystawiony przed datą złożenia podpisu lub ARL/OCSP wystawiony przed datą złożenia podpisu	Usługa walidacji nie ma dostępu do wystarczająco świeżej informacji o unieważnieniach, którą powinien publikować wystawca certyfikatu, w związku tym nie można zweryfikować ważności certyfikatu użytego do weryfikacji podpisu. Brak dostępu może być spowodowany awarią po stronie wystawcy certyfikatu podpisu. **Możliwe działania:** Powtórzyć usługę walidacji po pewnym czasie.

3.6. Kwalifikowany znacznik czasu

Zgodnie z rozporządzeniem UE 910/2014 (eIDAS) kwalifikowany elektroniczny znacznik czasu:

a) oparty jest na precyzyjnym źródle czasu powiązanym z uniwersalnym czasem koordynowanym,
b) wiąże datę i czas z danymi tak, aby w wystarczający sposób wykluczyć możliwość niewykrywalnej zmiany danych, oraz
c) jest podpisany przy użyciu zaawansowanego podpisu elektronicznego lub opatrzony zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania lub w inny równoważny sposób.

Dzięki temu korzysta, zgodnie z eIDAS, z domniemania dokładności daty i czasu, jakie wskazuje, oraz integralności danych, z którymi wskazywane data i czas są połączone.

Ponadto, zgodnie z polskim prawem, opatrzenie dokumentu elektronicznego kwalifikowanym znacznikiem czasu jest równoznaczne z nadaniem temu dokumentowi waloru daty pewnej na w rozumieniu art. 81 §2 pkt 3 kodeksu cywilnego.

3.7. Dokładna data złożenia podpisu

Aby usługa GetValid mogła wykazać dokładną datę złożenia podpisu wymagane jest świadome działanie osoby podpisującej dokument. Osoba podpisująca musi postąpić w następujący sposób (metoda działa wyłącznie dla dokumentów w formacie PDF):

1. Oznakować czasem przygotowany dokument PDF.
2. Podpisać dokument.
3. Oznakować czasem podpisany dokument.

W takim przypadku usługa GetValid wykaże, że podpis został złożony w przedziale dat pomiędzy pierwszym, a drugim znacznikiem czasu. Ponieważ wykonanie sekwencji: znakowanie czasem – podpis – znakowanie czasem, można wykonać w czasie pojedynczych sekund, to uzyskana w ten sposób data złożenia podpisu będzie znana z taką dokładnością.

3.8. Akceptacja podpisów z algorytmem SHA-1

Algorytm SHA-1 był powszechnie używany do składania podpisów elektronicznych, ale z czasem zostały odkryte skuteczne ataki, w tym umożliwiające demonstrację możliwości sfałszowania podpisu elektronicznego złożonego z użyciem SHA-1. Praktyczne wykonanie tego fałszerstwa wciąż jest dość trudne, ponieważ atakujący musi specjalnie wytworzyć dwie specjalnie spreparowane wersje dokumentu PDF, z których jedną daje do podpisania osobie upoważnionej, a potem może podmienić podpisany dokument na drugą wersję, bez naruszenia podpisu. Atak wymaga więc wcześniejszego przygotowania oraz wymaga, aby fałszerz był osoba zaufaną dla podpisującego i mógł podłożyć spreparowany dokument do podpisu. Wciąż nie jest możliwe sfałszowanie dowolnego podpisanego dokumentu, jednak odkryte ataki są na tyle poważne, że obecnie wykluczają zastosowanie SHA-1 do podpisów.

W związku z tymi słabościami, w normach dotyczących podpisów elektronicznych i wsystemach prawnych różnych krajów, algorytm SHA-1 przestał być uznawany za bezpieczny i obecnie do podpisów używane są algorytmy z rodziny SHA-2 (SHA-256, SHA-512 itd.). Trudno wskazać jednoznacznie dokładną datę końca użyteczności algorytmu SHA-1, ponieważ jest to kwestia prawna i może zależeć od kontekstu i konkretnego zastosowania podpisu. W usłudze GetValid przyjęto datę określoną w art. 137 ust. 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, to jest 1 lipca 2018 r. - podpisy walidowane na datę przypadającą przed 1 lipca 2018 r. (czyli podpisy złożone przed tą datą), są walidowane pozytywnie (w tamtym czasie atak na SHA-1 nie był znany, nie było więc praktycznej możliwości jego wykonania), a podpisy złożone później, są walidowane ze statusem „Nieokreślony”.