



INSTRUKCJA DLA INTEGRATORA

Z SYSTEMEM WĘZEŁ PODPISU

Spis treści

1	Historia zmian	3
2	Cel i zakres dokumentu	4
2.1	Słownik pojęć i skrótów	4
3	Dostęp do usług sieciowych systemu Węzeł Podpisu	7
3.1	Bezpieczeństwo - REST Security.....	7
4	Definicja usługi sieciowej REST signing REST	8
4.1	Dokumentacja Swagger UI	9

1 Historia zmian

Wersja	Data	Opis
0.1	22.09.2023	Opracowanie i utworzenie szablonu dokumentu.
0.2	26.09.2023	Uzupełnienie dokumentu
0.3	05.10.2023	Utworzenie i dodanie do załączników przykładowych żądań, odpowiedzi serwera oraz podpisanego dokumentu.
0.4	04.12.2023	Dodanie plików XML dla certyfikatu kwalifikowanego oraz certyfikatu podpisu osobistego
0.5	21.02.2024	Uzupełnienie kodów błędów
0.6	04.06.2025	Aktualizacja dokumentu
1.0	22.08.2025	Aktualizacja dokumentu
1.1	28.11.2025	Uzupełnienie dokumentu o informacje związane z usługą signing REST.
1.2	23.02.2026	Uzupełnienie dokumentu w zakresie odwołania do aktualnej dokumentacji Swagger UI.
2.0	Maj 2026	Dostosowanie treści dokumentu do prezentowania zawartości tylko architekturze REST
2.1	Lipiec 2026	Aktualizacja w zakresie odwołania do nowej wersji instrukcji weryfikacji podpisanego dokumentu

2 Cel i zakres dokumentu

Niniejszy dokument opisuje usługi sieciowe systemu **Węzeł Podpisu** na poziomie technicznym. Dokument przeznaczony jest dla twórców systemów integrujących się z systemem **Węzeł Podpisu** w ramach stylu architektonicznego REST.

Informacje dotyczące REST znajdują się w rozdziale [Definicja usługi sieciowej REST signing REST](#).

Dostęp do usługi weryfikacji podpisanego dokumentu SignatureVerification (udostępnianej w ramach systemu Profil Zaufany) opisany został w dokumencie „Instrukcja dla Integratora - weryfikacja podpisanego dokumentu 1.3”.

2.1 Słownik pojęć i skrótów

Pojęcie/skrót	Znaczenie
System Węzeł Podpisu	System umożliwiający złożenie podpisu zaufanego, podpisu kwalifikowanego przy użyciu certyfikatu kwalifikowanego lub podpisu osobistego z wykorzystaniem certyfikatu z e-dowodu.
Profil Zaufany	Środek identyfikacji elektronicznej zawierający zestaw danych identyfikujących i opisujących osobę fizyczną, która posiada pełną albo ograniczoną zdolność do czynności prawnych, który został wydany w sposób, o którym mowa w art. 20c albo art. 20cb ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2005 nr 64, poz.565; t.j. Dz. U. 2021 poz. 670).
Podpis zaufany	Podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający: <ol style="list-style-type: none"> dane identyfikujące osobę, ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie, o którym mowa w art. 20aa pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, obejmujące: <ul style="list-style-type: none"> imię (imiona), nazwisko, numer PESEL, identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony, czas jego złożenia.
Podpis osobisty	Jest to zaawansowany podpis elektroniczny. Prawdziwość danych posiadacza podpisu potwierdza certyfikat podpisu osobistego, zawierający imię (imiona), nazwisko, obywatelstwo oraz numer PESEL. Podpis osobisty ma taki sam skutek prawny jak podpis własnoręczny. Podpis osobisty może być wykorzystywany również w kontaktach z podmiotami innymi niż publiczne, ale tylko, jeżeli obie strony wyrażą na to zgodę. Podpis osobisty może służyć m.in. do złożenia podpisu dokumentów elektronicznych wysyłanych do urzędu.

COI - Informacja publiczna

Pojęcie/skrót	Znaczenie
Podpis kwalifikowany	<p>Jest to zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego (Dz.U.U.E.910/2014).</p> <p>Podpis kwalifikowany to powszechnie używana nazwa bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu. Z uwagi na bezpieczeństwo obrotu prawnego dokumenty przedkładane usługodawcy przez usługobiorcę za pośrednictwem środków komunikacji elektronicznej muszą być zabezpieczone przed niekontrolowaną modyfikacją, a więc muszą być elektronicznie podpisane.</p> <p>Podpis kwalifikowany jest autoryzowanym sposobem potwierdzenia tożsamości. Centra Certyfikacji wydają certyfikaty kwalifikowane służące do złożenia podpisu kwalifikowanego. Dokument w ten sposób podpisany jest prawnie wiążącym.</p>
e-dowód	Dowód osobisty (dokument tożsamości) posiadający warstwę elektroniczną, umożliwiającą jego posiadaczowi uwierzytelnienie w usługach online za pomocą profilu osobistego oraz potwierdzenie obecności w określonym czasie i miejscu.
System zewnętrzny	System używający usług sieciowych systemu Węzeł Podpisu .
Administrator systemu PZ	Użytkownik systemu Profil Zaufany posiadający m.in. uprawnienie do zarządzania słownikiem systemów zewnętrznych.
REST	Representational State Transfer, to styl architektoniczny do tworzenia usług sieciowych, który umożliwia komunikację między różnymi systemami komputerowymi poprzez Internet. Jest to zestaw zasad i wytycznych dla tworzenia skalowalnych i wydajnych usług, które wykorzystują protokół HTTP i operacje na zasobach (np. pobieranie, dodawanie, aktualizacja, usuwanie danych).
JSON	JavaScript Object Notation, lekki format wymiany danych komputerowych. JSON jest formatem tekstowym, bazującym na podzbiorze języka JavaScript.
XAdES	<p>Format podpisu elektronicznego, który służy do podpisywania dokumentów w formacie XML.</p> <p>Specyfikacja techniczna wskazana w Decyzji wykonawczej Komisji (UE) 2015/1506 z dnia 8 września 2015 r. ustanawiającej specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego to ETSI TS 103171 v.2.1.1.</p> <p>W usłudze są dostępne dwa rodzaje podpisu XAdES: otoczony i otaczający. Różnią się one strukturą podpisanego pliku.</p>
XAdES otoczony (enveloped)	Podpis znajduje się w strukturze dokumentu – jest „otoczony” treścią dokumentu. Jeśli taki dokument podpisuje więcej osób, ich podpisy zostaną umieszczone w strukturze dokumentu obok siebie i mogą zostać odczytane jednocześnie.

COI - Informacja publiczna

Pojęcie/skrót	Znaczenie
XAdES otaczający (enveloping)	Treść dokumentu znajduje się w strukturze podpisu – jest „otoczona” podpisem. Jeśli taki dokument podpisuje więcej osób, struktura każdego kolejnego podpisu będzie „otaczała” treść dokumentu z wcześniejszym podpisem. Oznacza to, że podczas odczytywania pliku nie zostaną wyświetlone wszystkie podpisy jednocześnie.
PAdES	Format podpisu elektronicznego, który służy do podpisywania dokumentów w formacie PDF. Specyfikacja techniczna wskazana w Decyzji wykonawczej Komisji (UE) 2015/1506 z dnia 8 września 2015 r. ustanawiającej specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego to ETSI TS103172 v.2.2.2.

3 Dostęp do usług sieciowych systemu Węzeł Podpisu

Przed przystąpieniem do integracji z usługami sieciowymi systemu Węzeł Podpisu należy spełnić kryteria formalne określone w dokumencie „Procedura integracji systemów oraz wymiany certyfikatu do integracji systemów z podpisem zaufanym” umieszczonym na stronie BIP MC.

Wszystkie usługi sieciowe systemu **Węzeł Podpisu** zabezpieczone są za pomocą mechanizmu mTLS (*Mutual TLS authentication*), który stanowi rozszerzenie protokołu TLS. Uzyskanie dostępu do usługi przez system zewnętrzny związane jest ze spełnieniem wszystkich poniższych warunków:

- Nawiązując połączenie mTLS do systemu Węzeł Podpisu klient musi dołączyć certyfikat kliencki, który wymagany jest w procesie wzajemnego uwierzytelniania.
- System zewnętrzny musi być wpisany przez administratora systemu PZ na listę znanych systemów zewnętrznych w systemie Profil Zaufany.
- Certyfikat kliencki użyty przez system zewnętrzny do podpisania żądania musi być dodany przez administratora systemu PZ do listy certyfikatów systemu zewnętrznego w systemie Profil Zaufany.
- System zewnętrzny musi być oznaczony przez administratora systemu PZ, jako aktywny w systemie Profil Zaufany.
- System zewnętrzny musi mieć przyznane przez administratora systemu PZ uprawnienie do wywoływania operacji usługi sieciowej w systemie **Węzeł Podpisu**.

3.1 Bezpieczeństwo - REST Security

Aby mieć możliwość skorzystania z usługi należy w nagłówku przekazać:

- X-API-Version – wersja API do użycia
- X-Client-Cert - Base64 zakodowany certyfikat klienta w formacie DER.

Przykład:

```
"X-API-Version: 1"
```

```
-H "X-Client-Cert: 2JzNiTBKMbaJhRTPL5C..."
```

4 Definicja usługi sieciowej REST

signing REST

Usługa służy do złożenia podpisu pod dokumentem/ dokumentami w ramach utworzonego żądania podpisu, a podpisany dokument może posiadać załącznik/ załączniki. Po złożeniu podpisu istnieje możliwość pobrania podpisanego dokumentu/ dokumentów.

Usługa signing REST umożliwia złożenie podpisu w formacie:

- PAdES - służy do złożenia podpisu dla pliku w formacie *.pdf.; podpis można sprawdzić po otwarciu podpisanego pliku
- XAdES - służy do złożenia podpisu dla większości pozostałych formatów plików, np. *.doc, *.docx, *.odt, *.xls, *.jpg, *.png, *.xml ale i *.pdf; po złożeniu podpisu powstaje plik XML, w którym zawarte będą dane dokument i podpisu; do odczytania podpisu potrzebne jest odpowiednie oprogramowanie od dostawców usług kwalifikowanych.

W ramach formatu XAdES możliwe jest złożenie podpisu:

- XAdES otoczony (enveloped) - podpis znajduje się w strukturze dokumentu – jest „otoczony” treścią dokumentu. Jeśli taki dokument podpisuje więcej osób, ich podpisy zostaną umieszczone w strukturze dokumentu obok siebie i mogą zostać odczytane jednocześnie.
- XAdES otaczający (enveloping) - treść dokumentu znajduje się w strukturze podpisu – jest „otoczona” podpisem. Jeśli taki dokument podpisuje więcej osób, struktura każdego podpisu będzie „otaczała” treść dokumentu z wcześniejszym podpisem. Oznacza to, że podczas odczytywania pliku nie zostaną wyświetlone wszystkie podpisy jednocześnie.

Proces podpisu z wykorzystaniem usługi signing przebiega w następujących krokach:

1. Klient usługi signing przy pomocy endpointu `POST service/api/sgws/signings` tworzy żądanie podpisu. Utworzone żądanie może od razu zawierać dokument.
2. Za pomocą endpointu `POST service/api/sgws/signings/{signRequestId}/documents`, można rozszerzyć istniejące żądanie o kolejne dokumenty.
3. Po złożeniu podpisu/ podpisów pod dokumentem/ dokumentami, za pomocą endpointu `GET /service/api/sgws/signings/{signRequestId}/documents/signed/{documentId}` możliwe jest pobranie podpisanego dokumentu/ dokumentów.

Pozostałe endpointy:

- `GET /external-service/api/sgws/signings/{signRequestId}/documents/signed` – zwraca metadane podpisanych dokumentów danego żądania podpisu
- `GET /external-service/api/sgws/signings/{signRequestId}/documents/unsigned` – zwraca niepodpisane dokumenty danego żądania podpisu

COI - Informacja publiczna

- DELETE /external-service/api/sgws/signings/{signRequestId}/documents/remove - usuwa dokumenty z żądania podpisu

4.1 Dokumentacja Swagger UI

Aktualna dokumentacja dla signing REST znajduje się pod adresem <https://int.podpis.gov.pl/api-docs/sgws/swagger-ui/index.html>

Istotne pola w komunikacji REST:

Pole	Uwagi
attachments	Lista załączników dla dokumentu (pole attachment). Każde wystąpienie załącznika musi posiadać unikalną wartość pola uri. Element może występować wielokrotnie.
cancelUrl	URL na który zostanie przekierowany użytkownik w przypadku anulowania podpisu dokumentu, będący poprawnym adresem URL.
content	Dokument do podpisu wysyłany jest w [string(\$byte)].
documentId	Identyfikator dokumentu
documentIds	Lista identyfikatorów dokumentów do usunięcia z żądania podpisu. Należy podać min jeden identyfikator dokumentu.
documents	Lista dokumentów do podpisania. Zawiera informacje dotyczące podpisywanych dokumentów (pole document). Element może występować wielokrotnie.
externalRepositoryId	Dopuszczalne wartości identyfikatorów zewnętrznych repozytoriów. Enum EPUAP. Repozytorium ePUAP - elektroniczna Platforma Usług Administracji Publicznej.
failureUrl	URL na który zostanie przekierowany użytkownik w przypadku niepowodzenia podpisu dokumentu, będący poprawnym adresem URL.
fileHash	skrót zapisanego pliku.
fileId	Identyfikator pliku w repozytorium. <i>Jeśli występuje externalRepositoryId oraz fileId, to nie ma content.</i>
fileName	Pełna nazwa pliku (wraz z rozszerzeniem).
fileSize	Wielkość pliku podana w Bajt

COI - Informacja publiczna

information	Informacje dodatkowe o pliku.
contentType	Typ MIME załącznika. W przypadku braku pola w żądaniu zostanie przyjęta domyślna wartość „application/octet-stream”.
signatureFormat	Format podpisu; dozwolone wartości: <ul style="list-style-type: none"> • XAdES_ENVELOPED • XAdES_ENVELOPING • PAdES <p>XAdES enveloped – (otoczony) to typ podpisu elektronicznego XAdES, gdzie dane podpisu są umieszczane wewnątrz struktury podpisywanego dokumentu XML.</p> <p>XAdES enveloping – podpis typu otaczającego, w którym struktura podpisywanego dokumentu zawarta jest w kodzie podpisu, a efektem jest jeden podpisany plik z rozszerzeniem xades lub xml. Rozwiązanie to jest rzadziej stosowane, bo pozwala złożyć na dokumencie tylko jeden podpis.</p> <p>PAdES - wykorzystuje się tylko przy podpisywaniu pliku PDF. Użycie tego formatu pozwala na zawarcie wielu podpisów pod dokumentem PDF.</p>
signatureMethod	Dopuszczalne metody podpisu: <ul style="list-style-type: none"> • PZ_PZ – Podpis zaufany – autoryzacja za pomocą profilu zaufanego. • PZ_SIE – Podpis zaufany - autoryzacja za pomocą profilu osobistego (eDowód). • PS – podpis osobisty. • PQ – podpis kwalifikowany. • MO – podpis za pomocą aplikacji mObywatel. <p>Uwaga!</p> <p>Dla podpisu jednego dokumentu w formacie XAdES dostępne są wszystkie metody podpisu.</p> <p>Dla podpisu wielu dokumentów w formacie XAdES dostępne metody podpisu to: PZ_PZ, PZ_SIE, MO.</p> <p>Dla podpisu jednego lub wielu dokumentów w formacie PAdES dostępne metody podpisu to: PZ_PZ, PZ_SIE, MO.</p>
signatureMethods	Lista dopuszczalnych metod podpisu. Efektem jest wyświetlenie użytkownikowi, w ramach GUI, dostępnych metod podpisu (pole signatureMethod). Element może występować wielokrotnie.
signingRequestUrl	Url który przechodzi do WP.

COI - Informacja publiczna

signRequestId	Identyfikator żądania podpisu.
successUrl	URL na który zostanie przekierowany użytkownik w przypadku gdy dokument zostanie poprawnie podpisany, będący poprawnym adresem URL.
uri	Identyfikator URI; unikalny w ramach dokumentu, np. nazwa dokumentu.
xsltUrl	URL transformaty określającej wygląd dokumentu elektronicznego w formacie xml. Wspierane są wyłącznie następujące domeny: <ul style="list-style-type: none">• http://crd.gov.pl/• https://test.epuap.gov.pl/• https://test3.mobywatel.gov.pl/