



**Polityka świadczenia usługi weryfikacji  
podpisu elektronicznego i pieczęci  
elektronicznej w trybie online**

Wersja 6

Data wydania: 04.06.2024

MADKOM SA

Al. Zwycięstwa 96/98

81-451 Gdynia

Autorskie prawa majątkowe do tej dokumentacji oraz oprogramowania wykorzystywanego do świadczenia usług niekwalifikowanych przysługują MADKOM SA z siedzibą w Gdyni, Aleja Zwycięstwa 96/98.

Powyższe prawa są chronione ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r., poz. 2509).

Zabrania się kopiowania, drukowania i rozpowszechniania tejże dokumentacji bez zgody Madkom SA.

## Spis treści

1.	Wstęp .....	4
2.	Definicje i pojęcia .....	4
3.	Podstawy prawne świadczenia Usług .....	4
4.	Rodzaje i zakres świadczenia usług zaufania.....	5
a.	Weryfikacja podpisu elektronicznego.....	5
b.	Weryfikacja autentyczności Poświadczenia weryfikacji .....	6
5.	Wynik weryfikacji podpisu i pieczęci elektronicznej .....	6
6.	Przetwarzanie danych, w tym danych osobowych .....	8
7.	Rejestrowanie zdarzeń.....	9
8.	Zabezpieczenia komunikacji.....	9
9.	Administrowanie Polityką .....	9
10.	Historia dokumentu .....	10

## 1. Wstęp

Polityka świadczenia usługi weryfikacji podpisu elektronicznego i pieczęci elektronicznej w trybie online pozostając w zgodzie z wymaganiami Ustawy określa rodzaj, zakres, rozwiązania techniczne i organizacyjne świadczonych usług niekwalifikowanych w zakresie weryfikacji podpisu elektronicznego oraz pieczęci elektronicznej w trybie online przez MADKOM SA. Działalność MADKOM SA w zakresie świadczonych usług opiera się na obowiązujących aktualnie na terenie Rzeczypospolitej Polskiej przepisach prawnych.

## 2. Definicje i pojęcia

**Dostawca usług zaufania** – dostawca usług zaufania, o którym mowa w Artykule 3 pkt 19 EIDAS wpisany do jawnego Rejestru Dostawców usług zaufania prowadzonego przez Ministra właściwego do spraw informatyzacji,

**EIDAS** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE z późniejszymi zmianami.

**Polityka** – niniejszy dokument o nazwie „Polityka świadczenia usługi weryfikacji podpisu elektronicznego w trybie online”.

**Poświadczenie weryfikacji** – dokument zawierający kompletny wynik weryfikacji podpisu elektronicznego lub pieczęci elektronicznej zawierający datę i czas wygenerowania, oraz unikalny Identyfikator weryfikacji zapisany w pliku w formacie PDF, JSON lub HTML.

**Profil Zaufany** – środek identyfikacji elektronicznej o którym mowa w Art. 3 pkt 14 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

**Regulamin** – dokument Regulaminu świadczenia usług związanych z weryfikacją podpisów i pieczęci elektronicznych w Serwisie obowiązujący w Serwisie funkcjonującym na stronie internetowej pod adresem <https://weryfikacjapodpisu.pl>.

**Rejestr dostawców usług zaufania** – rejestr, o którym mowa w Art. 2 Ustawy.

**Identyfikator weryfikacji** – identyfikator weryfikacji, o którym mowa w Regulaminie.

**Umowa** – umowa będąca podstawą świadczenia usług związanych z weryfikacją podpisów i pieczęci zawarta z Usługodawcą,

**Usługi** – usługi, o których mowa w Regulaminie,

**Usługodawca** – firma MADKOM SA,

**Ustawa** – Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2024 r., poz. 422),

**Użytkownik** – użytkownik, o którym mowa w Regulaminie,

**Wynik weryfikacji** – wynik weryfikacji o którym mowa w Regulaminie.

## 3. Podstawy prawne świadczenia Usług

Świadczenie Usług odbywa się przy uwzględnieniu następujących regulacji wewnątrzspółnotowych i krajowych:

- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2020 r. poz. 344),
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO),
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (EIDAS) z późniejszymi zmianami,
- Ustawa z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej (t.j. Dz. U. z 2024 r., poz. 422),
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781),
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r., poz. 307),
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2024 r., poz. 34),
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r., poz. 902),

MADKOM SA jest Dostawcą usług zaufania i funkcjonuje zgodnie z obowiązującym na terenie Rzeczypospolitej Polskiej prawem na podstawie wpisu do Rejestru dostawców usług zaufania prowadzonego przez Narodowe Centrum Certyfikacji – usługi niekwalifikowane.

#### 4. Rodzaje i zakres świadczenia usług zaufania

Usługodawca świadczy usługi zaufania szczegółowo opisane w Regulaminie. Usługi są świadczone przy wykorzystaniu serwisu internetowego i usług sieciowych. System do weryfikacji podpisów i pieczęci wykorzystuje unijny system list zaufania (TSL).

##### a. Weryfikacja podpisu elektronicznego

Usługa weryfikacji podpisu elektronicznego i pieczęci elektronicznej cechuje się właściwościami szczegółowo określonymi w tabeli poniżej.

Dostęp do usługi:	<a href="https://weryfikacjapodpisu.pl">https://weryfikacjapodpisu.pl</a> <a href="https://weryfikacjapodpisu.pl/en">https://weryfikacjapodpisu.pl/en</a>
Obsługiwane formaty podpisów i pieczęci:	XAdES – ETSI EN 319 132 PAdES – ETSI EN 319 142 CAdES – ETSI EN 319 122 ASiC – ETSI EN 319 162
Profile podpisu:	XadES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA, C, X, XL, PadES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA, CadES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA ASiC: ASiCS-XAdES, ASiCE-XAdES
Zaufane listy	TSL zgodnie z ETSI TS 119 612
Status certyfikatu online	CRL OCSP
Rozszerzenia profili	XAdES: <ul style="list-style-type: none"> <li>• Otaczający (enveloping)</li> </ul>

	<ul style="list-style-type: none"> <li>• Otoczony (enveloped)</li> <li>• Dołączony (detached)</li> </ul> CAdES: <ul style="list-style-type: none"> <li>• Otaczający (enveloping)</li> <li>• Dołączony (detached)</li> </ul> PAdES: <ul style="list-style-type: none"> <li>• Otoczony (enveloped)</li> </ul> ASiC: <ul style="list-style-type: none"> <li>• ASiCS: XAdES</li> <li>• ASiCE: XAdES</li> </ul>
Weryfikacja znacznika czasu	Tak
Odtwarzanie ścieżki certyfikacji dla certyfikatów podpisujących	Tak
Odtwarzania ścieżki certyfikacji dla znaczników czasu	Tak
Formaty Poświadczeń weryfikacji	Plik w formacie JSON Plik w formacie PDF Plik w formacie HTML
Algorytmy funkcji skrótu	SHA-1, SHA-224, SHA-256, SHA-512
Algorytmy podpisu	RSA
Sprawdzenie integralności podpisanych danych	Tak
Wykrywanie ataku kolizyjnego SHA-1	Tak
Maksymalna liczba jednocześnie weryfikowanych plików	20 plików
Status weryfikacji certyfikatu podpisującego	Pozytywny Warunkowo pozytywny Negatywny

Wynik weryfikacji podpisu i pieczęci elektronicznej jest zmienny w czasie ze względu na upływ ważności danych służących składaniu podpisów, pieczęci i znaczników czasu. Stąd dla celów dowodowych system generuje Poświadczenie weryfikacji, które użytkownik może przechowywać. Poświadczenie weryfikacji zawiera unikalny Identyfikator weryfikacji pozwalający użytkownikom zweryfikować treści Wyniku weryfikacji z momentu weryfikacji.

*UWAGA: Jeśli podpis elektroniczny lub pieczęć elektroniczna zawiera znacznik czasu to weryfikacja dokonywana jest na moment czasu zawarty w znaczniku czasu, w przeciwnym wypadku – na bieżący moment.*

#### **b. Weryfikacja autentyczności Poświadczenia weryfikacji**

Usługa umożliwia uzyskanie potwierdzenia autentyczności Poświadczenia weryfikacji, poprzez uzyskanie dostępu do pełnego Wyniku weryfikacji dysponując wyłącznie unikalnym Identyfikatorem weryfikacji. Pozwala na odtworzenie Wyniku weryfikacji z momentu weryfikacji podpisu i pieczęci, dla którego Użytkownik dysponuje Identyfikatorem weryfikacji.

### **5. Wynik weryfikacji podpisu i pieczęci elektronicznej**

W wyniku przeprowadzonej weryfikacji podpisu i pieczęci elektronicznej system prezentuje następujące dane dla każdego podpisu i każdej pieczęci odrębnie:

#### **Dane podstawowe**

Nazwa pliku	Nazwa pliku, w którym w procesie weryfikacji został odnaleziony co najmniej 1 podpis elektroniczny (lub pieczęć)
Integralność	Wynik weryfikacji integralności podpisanych danych
Podpisujący	Dane zawarte w nazwie powszechnej certyfikatu podmiotu podpisującego lub dane podmiotu posługującego się Profilem Zaufanym dla podpisów zaufanych (tylko PL) oraz nazwa podpisującego w przypadku podpisów osobistych (tylko PL).
Rodzaj uwierzytelnienia	Informacja o rodzaju podpisu elektronicznego, w przypadku podpisów zaufanych dodatkowo nazwa powszechna pieczęci elektronicznej wykorzystywanej przez system Profilu Zaufanego
Deklarowany czas złożenia podpisu	Deklarowany czas podpisania/złożenia pieczęci, z urządzenia podpisującego, zawarty w treści podpisu elektronicznego lub pieczęci elektronicznej wraz z informacją o czasie we właściwej strefie czasowej użytkownika weryfikującego
<b>Dane szczegółowe</b>	
Funkcja skrótu	Zastosowana w podpisie/pieczęci funkcja skrótu np. SHA-256
Profil podpisu/pieczęci	Profil podpisu/pieczęci, patrz tabela w punkcie 4.a
Podpisujący	Dane zawarte w nazwie powszechnej certyfikatu podmiotu podpisującego lub dane podmiotu posługującego się Profilem Zaufanym dla podpisów zaufanych (tylko PL) oraz nazwa podpisującego w przypadku podpisów osobistych (tylko PL).
Deklarowany czas złożenia podpisu	Deklarowany czas podpisania/złożenia pieczęci, z urządzenia podpisującego, zawarty w treści podpisu elektronicznego wraz z informacją o czasie we właściwej strefie czasowej użytkownika weryfikującego
Rodzaj uwierzytelnienia	Informacja o rodzaju podpisu elektronicznego, w przypadku podpisów zaufanych dodatkowo nazwa powszechna pieczęci elektronicznej
Podpisano dokument/plik	Informacja o podpisanym dokumencie, w tym nazwa pliku, nazwa pliku zewnętrznego (o ile został podpisany) oraz informacja o numerze podpisanej rewizji dla podpisu formacie PAdES
Powód	Szczegółowa informacja o powodach braku poprawnej weryfikacji
Podpis zaufany	O ile dotyczy to prezentowane są dane: Id konta Profilu Zaufanego, Imię, Nazwisko, PESEL (tylko PL).

Znacznik czasu	Czas wskazany w znaczniku czasu wraz z informacją o czasie we właściwej strefie czasowej użytkownika weryfikującego, rodzaj znacznika czasu, wystawca znacznika czasu oraz wynik weryfikacji znacznika
Certyfikat podpisującego	Dane zawarte w certyfikacie klucza publicznego, w tym: Nazwę powszechną, Organizację, Kraj, Serialnumber, Numer seryjny, Nazwa podmiotu wystawiającego, Informacja o zaufanych lub niezaufanych wystawcy (TSL), Status certyfikatu, Okres ważności certyfikatu, Informacja o wyniku weryfikacji statusu certyfikatu CRL i OCSP
Elementy podpisu	Lista referencji elementów objętych podpisem/piecczęcią, w tym identyfikatory i nazwy plików, wynik i weryfikacji skrótu/sygnatury oraz wartości certyfikatu
Pełna ścieżka certyfikacji	Jak w wierszu „Certyfikat podpisującego” dla wszystkich certyfikatów nadrzędnych w PKI
Pełna ścieżka certyfikacji dla znacznika czasu	Jw. w stosunku do znacznika czasu.

*Uwaga: Interpretacja i określenie skutków prawnych określonego Wyniku weryfikacji elektronicznych podpisów, pieczęci i znaczników czasu należy wyłącznie do Użytkownika. Usługodawca świadczy odpłatne usługi konsultacji związane z interpretacją Wyniku weryfikacji.*

## 6. Przetwarzanie danych, w tym danych osobowych

Przetwarzanie danych osobowych Użytkowników Serwisu odbywa się w zgodzie z Rozporządzeniem, Ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r. poz. 1000 z późn. zm. dalej „RODO”), Ustawą o świadczeniu usług drogą elektroniczną oraz Prawem telekomunikacyjnym (t.j. Dz.U. z 2019 r. poz. 2460 z późn. zm.), a Usługodawca stosuje odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych, w szczególności uniemożliwiające dostęp do nich osób trzecich lub ich przetwarzanie z naruszeniem przepisów prawa, zapobiegające utracie danych, ich uszkodzeniu lub zniszczeniu.

Usługi świadczone przez Usługodawcę zgodnie z niniejszą Polityką świadczone są na rzecz Użytkowników w oparciu o pozyskane od nich dane, które są przetwarzane w zasobach Usługodawcy.

Użytkowanie systemu wiąże się z akceptacją Regulaminu obowiązującego w Serwisie, który w §6 odnosi się do obszaru przetwarzania danych osobowych.

Kwestia przetwarzania danych, w tym danych osobowych, na urządzeniach końcowych została przedstawiona w postaci opisu stosowania plików cookies wykorzystywanych w serwisie weryfikacjapodpisu.pl pod adresem <https://weryfikacjapodpisu.pl/cookies.html>.

Procesy przetwarzania danych odbywają się bez ingerencji ludzkiej, czyli na żadnym etapie realizacji usługi dane Usługobiorcy nie są przetwarzane przez człowieka. Dane wykorzystywane w procesach świadczenia usług (pliki przesyłane do serwisu) są usuwane z zasobów Usługodawcy niezwłocznie po zrealizowaniu usługi. W zasobach Usługodawcy pozostają jednak wyniki uzyskane w ramach realizacji usługi weryfikacji podpisu elektronicznego, umożliwiające w późniejszym czasie zweryfikowanie autentyczności wystawionego przez system Poświadczenia weryfikacji, wśród których znajdują się publiczne dane z certyfikatu mogące zawierać dane osobowe (w tym także np. PESEL).



Pełny Wynik weryfikacji zawierający wszystkie dane z certyfikatów podpisujących, poddawany weryfikacji plik w ramach usługi weryfikacji autentyczności Poświadczenia weryfikacji, przechowywany jest przez okres wynikający z Umowy. Poświadczenie weryfikacji może być wykorzystywane w procesach dochodzenia roszczeń, w których pełny Wynik weryfikacji może być niezbędny.

## **7. Rejestrowanie zdarzeń**

W celu nadzoru nad sprawnym działaniem Usług oraz w celu rozliczania Użytkowników oraz pracowników usługodawcy z ich działań, w systemie rejestrowane są wszystkie te zdarzenia i działania, które mogą mieć istotny wpływ na bezpieczeństwo funkcjonowania systemu i świadczonych w nim Usług. Rejestr zdarzeń może być przeglądany wyłącznie przez upoważnionych pracowników Usługodawcy, a zapisy rejestru zdarzeń nie mogą być modyfikowane.

Wszelkie przesłane dokumenty do weryfikacji przez Użytkowników są usuwane natychmiast po przeprowadzeniu weryfikacji.

## **8. Zabezpieczenia komunikacji**

Komunikacja pomiędzy komputerem użytkownika a serwerem usług, jest zaszyfrowana z użyciem protokołu SSL (Secure Socket Layer). Protokół SSL to rodzaj zabezpieczenia, polegający na kodowaniu danych przed ich wysłaniem z przeglądarki użytkownika i dekodowaniu po bezpiecznym dotarciu na serwer. Informacja wysyłana z serwera do klienta jest również kodowana, a po dotarciu do celu dekodowana. Protokół SSL szyfruje, uwierzytelnia i zapewnia integralność wiadomości.

## **9. Administrowanie Polityką**

Dokument Polityki jest wersjonowany i każda kolejna wersja Polityki zaczyna obowiązywać z chwilą jej zatwierdzenia i opublikowania. Powodami wydania kolejnej wersji dokumentu mogą być uaktualnienia czy też błędy występujące w aktualnej wersji. Nowa wersja w trakcie opracowywania posiada status dokumentu roboczego i jest przygotowywana tylko i wyłącznie przez uprawnionych pracowników Usługodawcy. Dokument jest zatwierdzany przez Prezesa Zarządu spółki Usługodawcy.

**10. Historia dokumentu**

Data / wydanie	Opis zmiany
05.2017 / wyd.1	Nowe wydanie dokumentu
10.2017 / wyd.2	Aktualizacja – zmiana nazwy serwisu
01.2018 / wyd.3	Aktualizacja – zmiana nazwy serwisu
06.2019/ wyd. 3.2	Aktualizacja – korekta
19.09.2019/ wyd. 4.0	Aktualizacja polityki w zakresie świadczonych usług niekwalifikowanych
15.11.2019/ wyd.5.0	Aktualizacja polityki związana z aktualizacją serwisu
13.05.2020 / wyd. 5.1	Aktualizacja w zakresie doprecyzowania okresu przetwarzania danych osobowych
08.04.2024 / wyd. 5.2	Aktualizacja w zakresie zakresu świadczenia usługi zaufania weryfikacji podpisu elektronicznego oraz korekta błędów pisarskich tekstu Polityki.
04.06.2024 / wyd. 6	Aktualizacja dokumentu związana ze zmianami w świadczeniu usług i nowym Regulaminem.

© MADKOM SA 2024