

tekst ujednolicony według stanu prawnego na dzień 30 czerwca 2025 r.,
w brzmieniu przyjętym uchwałą Zarządu KDPW nr 166/16 z dnia 11.03.2016 r.
obowiązującą od 11.03.2016 r.,
uwzględniający zmiany dokonane uchwałą:
nr 699/16 z dnia 25.10.2016 r. obowiązującą od 14.11.2016 r.,
nr 861/17 z dnia 18.12.2017 r. obowiązującą od 3.01.2018 r.,
nr 316/2018 z dnia 23.05.2018 r. obowiązującą od 6.06.2018 r.,
nr 383/2018 z dnia 18.06.2018 r. obowiązującą od 2.07.2018 r.,
nr 321/2019 z dnia 18.06.2019 r. obowiązującą od 1.07.2019 r.,
nr 22/2020 z dnia 14.01.2020 r. obowiązującą od 3.02.2020 r.,
nr 750/2020 z dnia 14.08.2020 r. obowiązującą od 28.08.2020 r.
nr 512/2022 z dnia 8 czerwca 2022 r., obowiązującą od dnia 1.07.2022 r., z wyjątkiem w § 1 pkt 4, 5 i 7, które
obowiązują od dnia 1.11.2022 r.
nr 518/2025 z dnia 11.06.2025 r., obowiązującą od dnia 30.06.2025 r.

REGULAMIN SYSTEMU WYMIANY INFORMACJI

§ 1.

1. Regulamin Systemu Wymiany Informacji, zwany dalej „Regulaminem SWI”, stosuje się w stosunkach prawnych wynikających z Porozumień SWI zawieranych przez Krajowy Depozyt Papierów Wartościowych S.A. z uczestnikami SWI.
2. Regulamin SWI określa, w szczególności, system komunikacji elektronicznej dla potrzeb wymiany dokumentów w postaci elektronicznej pomiędzy Uczestnikiem SWI a Krajowym Depozytem Papierów Wartościowych S.A., zasady i warunki korzystania z tego systemu w ramach SWI, przyjęte w SWI zasady identyfikacji użytkowników oraz stosowane w SWI środki służące zapewnieniu bezpieczeństwa wymiany dokumentów za ich pośrednictwem, w tym także zasady składania oświadczeń i przesyłania dokumentów w postaci elektronicznej.

I. Definicje i skróty

§ 2.

Definicje i skróty użyte w treści Regulaminu SWI oznaczają:

- 1) **System Wymiany Informacji** lub **SWI** – zestaw środków technicznych oraz informatycznych, które umożliwiają składanie oświadczeń woli i przysyłanie innych informacji pomiędzy Krajowym Depozytem a Uczestnikami SWI, w drodze elektronicznej transmisji danych, przy wykorzystaniu systemu komunikacji elektronicznej, o którym mowa w pkt 3, oraz środków bezpieczeństwa generowanych i wydawanych zgodnie z postanowieniami Regulaminu SWI;
- 2) **Krajowy Depozyt** – spółkę Krajowy Depozyt Papierów Wartościowych S.A.;
- 3) **ESDI/WEB** – administrowany przez Krajowy Depozyt system komunikacji elektronicznej, o którym mowa w § 3;
- 4) **weryfikacja autentyczności wiadomości** - proces weryfikacji integralności dokumentu polegający na sprawdzeniu, czy wiadomość nie została w sposób nieuprawniony zmodyfikowana, tj. czy tekst wiadomości odebranej jest taki sam, jak tekst wiadomości nadanej, wykonywany poprzez porównanie wartości funkcji skrótu (hash) z dokumentu z wartością wyliczoną i wskazaną przez KDPW. W wyniku weryfikacji autentyczności wiadomości uzyskuje się również, na podstawie danych pochodzących z procesu uwierzytelnienia certyfikatem, informację, czy nadawca wiadomości jest tą osobą, za którą się podaje. Weryfikację autentyczności wiadomości uznaje się za negatywną, jeżeli treść wiadomości została zniekształcona (nastąpiło naruszenie integralności wiadomości), albo, jeśli nadawca wiadomości nie jest osobą, za którą się podaje;
- 5) **dokumenty** – dokumenty w rozumieniu Porozumienia SWI;
- 6) **dokumenty systemowe** – dokumenty, które są generowane bezpośrednio z systemu informatycznego Krajowego Depozytu, lub dokumenty, które są rejestrowane bezpośrednio w

systemie informatycznym Krajowego Depozytu w stosunkach pomiędzy Krajowym Depozytem oraz Uczestnikami SWI;

- 7) **Główny Poręczyciel** – osoba, którą jest pracownik Krajowego Depozytu wyznaczony przez Zarząd Krajowego Depozytu, spełniająca w systemie ESDI/WEB rolę tzw. zaufanej trzeciej strony, generująca środki bezpieczeństwa oraz będąca podmiotem poświadczającym, że nadawca i odbiorca dokumentu w tych systemach są faktycznie podmiotami, za które się podają. Główny Poręczyciel, z wykorzystaniem sprzętowych modułów kryptograficznych służących do generowania prywatnych kluczy kryptograficznych i publicznych kluczy kryptograficznych spełnia w tych systemach rolę Urzędu Certyfikacji;
- 8) **Porozumienie SWI** – Porozumienie w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej, zawarte pomiędzy Uczestnikiem SWI a Krajowym Depozytem, którego integralną częścią jest Regulamin SWI;
- 9) **Uczestnik SWI** – Powszechne Towarzystwo Emerytalne, Otwarty Fundusz Emerytalny albo inny podmiot będący stroną Porozumienia SWI zawartego z Krajowym Depozytem.

II. System komunikacji elektronicznej ESDI/WEB

§ 3.

1. Zakres zastosowania systemu ESDI/WEB:
 - 1) system dedykowany do obsługi wymiany danych, wykorzystujący mechanizmy aplikacji internetowych w oparciu o internetowe kanały komunikacyjne. Wymiana danych odbywa się w trybie manualnym (user - system) poprzez przeglądarkę internetową lub w trybie automatycznym (system - system) poprzez system informatyczny Uczestnika SWI;
 - 2) system ESDI/WEB zapewnia możliwość przesłania przez Uczestnika SWI do Krajowego Depozytu:
 - a) dokumentów systemowych w formacie własnym XML i stałopolowym KDPW przekazywanych w trybie manualnym przez Uczestnika SWI za pośrednictwem przeglądarki internetowej do systemu informatycznego Krajowego Depozytu;
 - b) dokumentów systemowych w formacie własnym XML i stałopolowym KDPW przekazywanych w trybie automatycznym przez system informatyczny Uczestnika SWI do systemu informatycznego Krajowego Depozytu;
 - c) dokumentów korespondencyjnych (w formacie dowolnym) przekazywanych przez Uczestnika SWI do komórek organizacyjnych Krajowego Depozytu;
 - 3) system ESDI/WEB zapewnia możliwość przesłania przez Krajowy Depozyt do Uczestnika SWI:
 - a) dokumentów systemowych w formacie własnym XML i stałopolowym KDPW przekazywanych przez Krajowy Depozyt do Uczestników SWI. Dostęp do dokumentów będzie możliwy za pośrednictwem przeglądarki internetowej lub systemu informatycznego Uczestnika SWI;
 - b) dokumentów korespondencyjnych (w formacie dowolnym) przekazywanych przez komórki organizacyjne Krajowego Depozytu do Uczestników SWI. Dostęp do dokumentów będzie możliwy za pośrednictwem przeglądarki internetowej lub systemu informatycznego Uczestnika SWI;
 - 4) zakres oraz strukturę komunikatów własnych XML i stałopolowych KDPW, które mogą być przekazywane w ramach SWI przy wykorzystaniu systemu ESDI/WEB, Krajowy Depozyt określa na swojej witrynie internetowej.
2. System ESDI/WEB działa na zasadzie wymiany wiadomości w postaci elektronicznej za pośrednictwem dedykowanej witryny internetowej dostępnej na stronie www.kdpw.pl, z zastosowaniem środków technicznych umożliwiających zachowanie poufności i integralności przesyłanych informacji oraz zapewnienie niezaprzeczalności nadawcy. Mechanizmy bezpieczeństwa zastosowane w ESDI/WEB bazują na uznanych standardach kryptograficznego

zabezpieczenia transmisji danych oraz wykorzystaniu mechanizmów weryfikacji autentyczności wiadomości. W skład systemu ESDI/WEB wchodzi:

- 1) system centralny (serwer witryny internetowej) – którego zadaniem jest umożliwienie wysyłania i odbierania dokumentów elektronicznych pomiędzy Krajowym Depozytem a Uczestnikami SWI;
 - 2) stacje klienckie Uczestników SWI, wyposażone w przeglądarkę internetową lub inne oprogramowanie klienckie, umożliwiające komunikację użytkowników z systemem centralnym.
3. Zasady eksploatacji:
- 1) dokumenty przesyłane do Krajowego Depozytu za pośrednictwem systemu ESDI/WEB należy uważać za zarejestrowane w tym systemie z chwilą otrzymania przez nadawcę potwierdzenia dostarczenia dokumentu do odbiorcy. Potwierdzeniem dostarczenia dokumentu jest specjalny komunikat esdk.acc.001.01 wysyłany przez system ESDI/WEB do nadawcy;
 - 2) dokumenty przesyłane z Krajowego Depozytu za pośrednictwem ESDI/WEB należy uważać za zarejestrowane w tym systemie z chwilą umieszczenia ich na systemie centralnym.

III. Przesyłanie dokumentów w ramach SWI przy wykorzystaniu systemu ESDI/WEB

§ 4.

1. Uaktywnienie wymiany dokumentów za pośrednictwem ESDI/WEB wymaga złożenia przez Uczestnika SWI w Krajowym Depozycie:
 - 1) pisemnego pełnomocnictwa udzielonego zgodnie ze wzorem zawartym w Załączniku nr 1 do Regulaminu SWI, wskazującego osobę upoważnioną do składania w jego imieniu oświadczeń woli oraz do przysyłania dokumentów za pośrednictwem ESDI/WEB; Uczestnik SWI może zamiast pełnomocnictwa przekazać Krajowemu Depozytowi aktualny odpis z właściwego rejestru sądowego, jeżeli osobą, o której mowa w zdaniu poprzedzającym, będzie osoba upoważniona do jego samodzielnego reprezentowania i ujawniona w tym rejestrze,
 - 2) wypełnionego przez osobę, o której mowa w pkt 1, formularza certyfikacyjnego, którego wzór zawiera Załącznik nr 3 do Regulaminu SWI, a także złożenia przez tę osobę, pisemnego oświadczenia o autoryzacji wydanego jej prywatnego klucza kryptograficznego w brzmieniu określonym w Załączniku nr 4 do Regulaminu SWI, przy czym oświadczenie to powinno zostać podpisane w obecności Głównego Poręczyciela.
2. Uczestnik SWI zobowiązany jest do bieżącego kontrolowania aktualności danych zawartych w treści składanych w Krajowym Depozycie formularzy certyfikacyjnych dotyczących osób działających w jego imieniu na podstawie pełnomocnictw, o których mowa w ust. 1 pkt 1, jak również do niezwłocznego zapoznania tych osób z treścią Porozumienia SWI oraz Regulaminu SWI, a także ich późniejszych zmian.
3. Uczestnik SWI zobowiązuje się nie dokonywać zmiany zakresu umocowania wynikającego z udzielonych przez niego pełnomocnictw, o których mowa w ust.1 pkt 1.
4. Uczestnik SWI jest zobowiązany zawiadomić na piśmie Głównego Poręczyciela, najpóźniej z jednodniowym wyprzedzeniem, o terminie wygaśnięcia lub odwołania pełnomocnictwa, o którym mowa w ust. 1 pkt 1. Jeżeli zachowanie tego terminu okazałoby się niemożliwe, zawiadomienia należy dokonać niezwłocznie po wygaśnięciu lub odwołaniu pełnomocnictwa.
5. Uczestnik SWI ponosi wyłączną odpowiedzialność za skutki prawne niewykonania lub wadliwego wykonania zobowiązania, o którym mowa w ust. 4.

§ 5.

Za pośrednictwem ESDI/WEB mogą być przekazywane pomiędzy stronami Porozumienia SWI dokumenty sporządzone w postaci plików komputerowych, w tym także dokumenty systemowe sporządzone w formacie XML.

§ 6.

1. Dokumenty przekazywane za pośrednictwem ESDI/WEB powinny być przekazane przez osobę uwierzytelnioną z wykorzystaniem certyfikatu.
2. Niezachowanie warunku, o którym mowa w ust. 1, jest równoznaczne z niezachowaniem zastrzeżonej w Regulaminie SWI formy składania oświadczeń woli oraz przekazywania innych oświadczeń lub informacji za pośrednictwem ESDI/WEB, i powoduje niedokonanie skutecznego doręczenia drugiej stronie Porozumienia SWI oświadczenia lub informacji zawartych w dokumencie.
3. Weryfikacja autentyczności wiadomości przekazanej ESDI/WEB jest dokonywana z wykorzystaniem wyznaczonego w ESDI/WEB hashu i porównanie go z wartością wygenerowaną przez stronę-nadawcę, w oparciu o odpowiednie algorytmy oraz narzędzia własne bądź pochodzące od niezależnych dostawców. O każdym przypadku stwierdzonych niezgodności każda ze stron powinna powiadomić drugą stronę.

§ 7.

1. W wypadku wykrycia jakichkolwiek przekłamań, błędów lub innych nieprawidłowości w treści doręzonego dokumentu, które powstały w czasie jego transmisji, strona-odbiorca jest zobowiązana niezwłocznie zawiadomić o tym stronę-nadawcę.
2. Żadna ze stron Porozumienia SWI nie odpowiada za szkody poniesione przez drugą stronę Porozumienia SWI wskutek awarii ESDI/WEB albo w związku z działaniem tego systemu, jak również wskutek awarii środków łączności pomiędzy stronami, z tym, że odpowiedzialność za szkody nie jest wyłączona, jeżeli strona:
 - 1) nie zawiadomiła niezwłocznie drugiej strony o negatywnej weryfikacji autentyczności wiadomości albo o wykrytym błędzie, przekłamaniu lub innej nieprawidłowości w treści dokumentu, w wykonaniu obowiązków, o których mowa w ust. 1 oraz § 6 ust. 3 albo
 - 2) na skutek nie dołożenia należytej staranności nie wykryła w treści dokumentu elektronicznego błędu, przekłamania lub innej nieprawidłowości, o których mowa w ust. 1.

IV. Środki bezpieczeństwa stosowane w ESDI/WEB**§ 8.**

1. Krajowy Depozyt, ani też Główny Poręczyciel nie są kwalifikowanymi dostawcami usług zaufania w rozumieniu Rozporządzenia 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. W związku z powyższym certyfikaty wydawane przez Głównego Poręczyciela nie są kwalifikowanymi certyfikatami podpisu elektronicznego w rozumieniu tego rozporządzenia. Oznacza to w szczególności, że podpisowi elektronicznemu weryfikowanemu przy pomocy tych certyfikatów, w myśl przepisów w/w rozporządzenia oraz w myśl postanowień art. 78¹ ust. 2 Kodeksu cywilnego, nie można przypisać skutków prawnych równoważnych podpisowi własnoręcznemu.
2. Zarząd Krajowego Depozytu wyznacza spośród jego pracowników Zastępców Głównego Poręczyciela, którzy w czasie nieobecności Głównego Poręczyciela będą wykonywać jego czynności. Postanowienia Regulaminu SWI dotyczące Głównego Poręczyciela, stosuje się odpowiednio do Zastępców Głównego Poręczyciela.

§ 9.

1. Przeznaczone dla stron Porozumienia SWI środki bezpieczeństwa, to jest:
 - 1) certyfikaty zawierające prywatne klucze kryptograficzne wraz z publicznymi kluczami kryptograficznymi strony (certyfikaty do ESDI/WEB),
 - 2) certyfikaty Urzędu Certyfikacji zawierające klucze publiczne Urzędu,
 - 3) hasła zabezpieczające,- są generowane przez Głównego Poręczyciela.

2. Certyfikaty udostępniane stronom Porozumienia SWI przez Głównego Poręczyciela zawierają, poza odpowiednim kluczem publicznym, także dodatkowe informacje pozwalające na identyfikację właściciela certyfikatu, wskazanie wystawcy, wskazanie okresu ważności certyfikatu i jego identyfikator oraz informację o algorytmie, których autentyczność jest potwierdzona przez Urząd Certyfikacji, w formie podpisu elektronicznego, złożonego przy wykorzystaniu prywatnego klucza kryptograficznego Urzędu Certyfikacji.

§ 10.

1. Przeznaczone dla strony Porozumienia SWI środki bezpieczeństwa wygenerowane przez Głównego Poręczyciela i zarejestrowane na odpowiednich nośnikach Główny Poręczyciel wydaje w lokalu siedziby Krajowego Depozytu osobie pisemnie przez tę stronę upoważnionej do ich odbioru. Od chwili wydania niebezpieczeństwo ich przypadkowej utraty lub ujawnienia obciąża wyłącznie stronę Porozumienia SWI, która dokonała ich odbioru.
2. Prywatny klucz kryptograficzny może zostać wydany wyłącznie osobie, która poprzez ten klucz ma być identyfikowana w ramach Systemu Wymiany Informacji, i która została wskazana w treści pełnomocnictwa udzielonego przez tę stronę Porozumienia SWI zgodnie z § 6 ust. 1 pkt 1 albo – w przypadku pobierania przez Uczestnika SWI internetowych środków bezpieczeństwa - osobie imiennie upoważnionej przez Uczestnika SWI wskazanej w formularzu certyfikacyjnym.
3. Uczestnik SWI zobowiązany jest zachować w tajemnicy wydane mu prywatne klucze kryptograficzne, hasła zabezpieczające, a także zobowiązany jest stworzyć osobom, którym udzielił pełnomocnictw, o których mowa w § 6 ust. 1 pkt 1, warunki zapewniające bezpieczne ich przechowywanie, a w szczególności zabezpieczające je przed utratą, zniszczeniem i dostępem osób nieuprawnionych.

§ 11.

1. Krajowy Depozyt stworzy Głównemu Poręczycielowi warunki zapewniające zachowanie pełnej poufności generowanych przez niego prywatnych kluczy kryptograficznych oraz haseł zabezpieczających.
2. Główny Poręczyciel nie przechowuje kopii prywatnych kluczy kryptograficznych i haseł zabezpieczających wydanych Uczestnikowi SWI.

§ 12.

1. Z zastrzeżeniem § 13 ust. 2 zd. pierwsze, klucze kryptograficzne i certyfikaty tracą ważność wraz z upływem terminu ważności certyfikatu.
2. Przesłanie dokumentu po upływie terminu ważności prywatnego klucza kryptograficznego zawartego w certyfikacie, nie wywołuje żadnych skutków prawnych, a w szczególności nie prowadzi do skutecznego złożenia oświadczenia lub doręczenia informacji zawartej w takim dokumencie.
3. Główny Poręczyciel dokonuje wydania nowych kluczy kryptograficznych, certyfikatów oraz haseł zabezpieczających w lokalu siedziby Krajowego Depozytu do rąk osoby upoważnionej przez stronę Porozumienia SWI na podstawie pełnomocnictwa, o którym mowa w § 4 ust. 1 pkt 1, w terminie uzgodnionym przez tę osobę z Głównym Poręczycielem.
4. Wydanie nowych kluczy kryptograficznych oraz certyfikatu w miejsce dotychczas stosowanych przez Uczestnika SWI, może także nastąpić w drodze zarejestrowania wniosku wygenerowanego z wykorzystaniem ważnych dotychczasowych kluczy kryptograficznych oraz certyfikatu. W takim przypadku wydanie nowych kluczy kryptograficznych oraz certyfikatu następuje z chwilą ich pobrania ze strony internetowej <https://cert.kdpw.pl>. Złożenie wniosku oraz pobranie nowych kluczy kryptograficznych oraz certyfikatu następuje zgodnie z procedurą określoną na w/w stronie internetowej.
5. Postanowień ust. 4 nie stosuje się w przypadku, gdy złożony w Krajowym Depozycie formularz certyfikacyjny dotyczący danej osoby będącej pełnomocnikiem Uczestnika SWI zawiera nieaktualne dane dotyczące tej osoby. W takim przypadku Uczestnik SWI zobowiązany jest podjąć działania uniemożliwiające tej osobie zarejestrowanie wniosku, o którym mowa w ust. 4, oraz - jeżeli

zamierza utrzymać w mocy udzielone jej pełnomocnictwo - zapewniające, by wydanie tej osobie nowych kluczy kryptograficznych oraz certyfikatów nastąpiło w sposób określony w ust. 3.

6. Do wydawania nowych kluczy kryptograficznych i certyfikatów stosuje się odpowiednio postanowienia § 4 ust. 1 oraz § 9-11.
7. Do wydawania nowych internetowych środków bezpieczeństwa ust. 3 – 5 nie stosuje się. Wydanie nowych internetowych środków bezpieczeństwa wymaga złożenia przez Uczestnika SWI wniosku w postaci formularza certyfikacyjnego, wypełnionego i wysłanego za pośrednictwem witryny internetowej www.kdpw.pl oraz dostarczenia do Krajowego Depozytu pisemnego oświadczenia złożonego w imieniu Uczestnika SWI przez osoby uprawnione do jego reprezentowania, potwierdzającego prawidłowość danych zamieszczonych w tym formularzu.

§ 13.

1. W razie powstania uzasadnionego podejrzenia ujawnienia lub złamania prywatnego klucza kryptograficznego, strona Porozumienia SWI, dla której klucz ten został wygenerowany i której został on wydany, powinna złożyć Głównemu Poręczycielowi na piśmie wniosek o wymianę dotychczas przez nią stosowanych kluczy, certyfikatu i haseł zabezpieczających wraz z jego uzasadnieniem.
2. Niezwłocznie po otrzymaniu wniosku, o którym mowa w ust. 1, Główny Poręczyciel unieważnia dotychczas stosowany przez stronę zgłaszającą wniosek certyfikat oraz powiązane z nim klucze i hasła zabezpieczające. Postanowienie § 9 ust. 2 stosuje się odpowiednio.
3. Niezwłocznie po unieważnieniu certyfikatu, informacja o tym jest udostępniana przez Głównego Poręczyciela na witrynie internetowej www.kdpw.pl.
4. Do momentu wydania stronie zgłaszającej wniosek, o którym mowa w ust. 1, nowych kluczy, certyfikatu i haseł zabezpieczających, wszelkie dokumenty adresowane do tej Strony, jak i od niej pochodzące, będą doręczane wyłącznie z zastosowaniem środków bezpieczeństwa niepodlegających wymianie,.
5. Postanowienia ust. 1-4 stosuje się odpowiednio w przypadku zaistnienia okoliczności wywołujących konieczność dokonania zmiany danych zawartych w certyfikacie wydanym stronie Porozumienia SWI.

V. Przesyłanie i odbieranie dokumentów za pośrednictwem innej osoby prawnej

§ 14.

1. Uczestnik SWI może dokonywać wszelkich czynności związanych z przesyłaniem oraz odbieraniem dokumentów przy użyciu ESDI/WEB za pośrednictwem innej osoby prawnej. W takim przypadku Uczestnik SWI powinien udzielić tej osobie prawnej pełnomocnictwa zgodnego ze wzorem zawartym w Załączniku nr 2 do Regulaminu SWI.
2. W przypadku, o którym mowa w ust. 1, dokonywanie wymiany dokumentów za pośrednictwem ESDI/WEB wymaga dokonania czynności, o których mowa w § 4 ust. 1, odpowiednio, przez osobę prawną, której Uczestnik SWI udzielił pełnomocnictwa, o którym mowa w ust. 1, oraz przez osobę fizyczną będącą dalszym pełnomocnikiem Uczestnika SWI. Wzór pełnomocnictwa dla dalszego pełnomocnika Uczestnika SWI zawarty został w Załączniku nr 2a do Regulaminu SWI.
3. W przypadku, o którym mowa w ust. 1, Główny Poręczyciel wygeneruje środki bezpieczeństwa, o których mowa w § 9 ust. 1, dla osoby prawnej będącej pełnomocnikiem Uczestnika SWI. Środki te będą wydawane do rąk osób będących dalszymi pełnomocnikami Uczestnika SWI, przy odpowiednim stosowaniu § 10 ust. 1 i 2 oraz zmieniane na zasadach ogólnych, przy czym w przypadku, o którym mowa w § 13 ust. 1, wniosek o zmianę środków bezpieczeństwa może zgłosić Uczestnik SWI zarówno bezpośrednio, jak i poprzez pełnomocnika. Zawiadomienie Krajowego Depozytu, o którym mowa w § 6 ust. 3, dokonywane będzie wyłącznie względem pełnomocnika Uczestnika SWI.

4. W przypadku, o którym mowa w ust. 1, dokumenty przesyłane przez Uczestnika SWI przy użyciu ESDI/WEB będą uwierzytelnione na podstawie certyfikatu identyfikującego Uczestnika SWI poprzez jego dalszego pełnomocnika.

IX. Postanowienia końcowe

§ 15.

1. Wszystkie załączniki do Regulaminu SWI stanowią jego integralną część.
2. Krajowy Depozyt jest uprawniony do dokonywania zmian Regulaminu SWI.
3. Dokonanie zmiany Regulaminu SWI wymaga powiadomienia Uczestnika SWI o treści zmian oraz dacie ich wejścia w życie. Powiadomienie następuje w drodze przesłania w/w zmian Uczestnikowi SWI, w formie pisemnej, na ostatni wskazany przez Uczestnika SWI adres, albo w postaci elektronicznej, z wykorzystaniem systemu ESDI/WEB.
4. W przypadku, gdy Uczestnik SWI nie wyraża zgody na dokonanie zmiany Regulaminu SWI, o których został powiadomiony zgodnie z postanowieniami ust. 3, przysługuje mu prawo wypowiedzenia Porozumienia SWI z zachowaniem jednomiesięcznego terminu wypowiedzenia. Wypowiedzenie powinno zostać doręczone do Krajowego Depozytu w formie pisemnej, w terminie dwóch tygodni, od dnia otrzymania przez Uczestnika SWI powiadomienia, o którym mowa w ust. 3.
5. Jeżeli Uczestnik SWI nie doręczył Krajowemu Depozytowi wypowiedzenia Porozumienia SWI zgodnie z ust. 4, w terminie tam określonym, oznacza to, że Uczestnik SWI wyraził zgodę na zmiany Regulaminu SWI, o których został powiadomiony zgodnie z postanowieniami ust. 3.

**Pełnomocnictwo
do składania oświadczeń woli przy użyciu Systemu Wymiany Informacji**

.....
miejsowość, data.....
kod instytucji

W związku z treścią § 4 ust. 1 pkt 1 Regulaminu SWI oraz łączącym Krajowy Depozyt Papierów Wartościowych S.A. i (nazwa (firma) mocodawcy) („**Uczestnik SWI**”) Porozumieniem w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej („**Porozumienie SWI**”), niżej podpisany/i działając w imieniu Uczestnika SWI udziela/ją niniejszym pełnomocnictwa Panu/Pani (imię i nazwisko pełnomocnika), posiadającemu/posiadającej numer identyfikacyjny PESEL/numer paszportu*, urodzonemu/urodzonej dnia* (DD-MM-RRRR) do składania i odbierania w imieniu i ze skutkiem dla Uczestnika SWI, przy użyciu systemu ESDI/WEB, oświadczeń i informacji, o których mowa w § 1 pkt 3 Porozumienia SWI, do występowania o wygenerowanie przeznaczonych dla Uczestnika SWI nowych środków bezpieczeństwa zgodnie z § 12 ust. 3 i 4 Regulaminu SWI, a także do odbioru z Krajowego Depozytu środków bezpieczeństwa ESDI/WEB oraz środków bezpieczeństwa dla wersji testowych ESDI/WEB.

.....
.....
*imiona i nazwiska osób uprawnionych
do reprezentowania mocodawcy*

* - niepotrzebne skreślić. W przypadku obywatela polskiego wpisać numer PESEL, w przypadku cudzoziemca wpisać numer paszportu oraz datę urodzenia

Pełnomocnictwo
do składania oświadczeń woli przy użyciu Systemu Wymiany Informacji
(wzór stosowany w przypadku udzielenia pełnomocnictwa innemu podmiotowi)

.....
miejsowość, data.....
kod instytucji

W związku z treścią postanowienia § 4 ust. 1 pkt 1 oraz § 17 ust. 1 Regulaminu SWI oraz łączącym Krajowy Depozyt Papierów Wartościowych S.A. i *(nazwa (firma) mocodawcy)* („**Uczestnik SWI**”) Porozumieniem w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej („**Porozumienie SWI**”), niżej podpisany/i działając w imieniu Uczestnika SWI udziela/ją niniejszym pełnomocnictwa *(nazwa pełnomocnika)* z siedzibą w pod adresem, numer właściwego rejestru sądowego:, do składania i odbierania w imieniu i ze skutkiem dla Uczestnika SWI, przy użyciu systemu ESDI/WEB, oświadczeń i informacji, o których mowa w § 1 pkt 3 Porozumienia SWI, do występowania o wygenerowanie przeznaczonych dla Uczestnika SWI nowych środków bezpieczeństwa zgodnie z § 12 ust. 3 i 4 Regulaminu SWI, a także do odbioru z Krajowego Depozytu środków bezpieczeństwa ESDI/WEB oraz środków bezpieczeństwa dla wersji testowych ESDI/WEB.

Pełnomocnik uprawniony jest do ustanawiania dalszych pełnomocników na rzecz Uczestnika SWI.

.....
.....
*imiona i nazwiska osób uprawnionych
do reprezentowania mocodawcy*

Pełnomocnictwo
do składania oświadczeń woli przy użyciu Systemu Wymiany Informacji
(wzór stosowany w przypadku ustanowienia dalszego pełnomocnika)

.....
miejscowość, data.....
kod instytucji

W związku z treścią postanowienia § 4 ust. 1 pkt 1 oraz § 17 ust. 1 i 2 Regulaminu SWI oraz łączącym Krajowy Depozyt Papierów Wartościowych S.A. i *(nazwa (firma) mocodawcy)* („**Uczestnik SWI**”) Porozumieniem w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej („**Porozumienie SWI**”), niżej podpisany/i działając na podstawie pełnomocnictwa udzielonego przez Uczestnika SWI w dniu, z prawem do ustanawiania dalszych pełnomocników na rzecz Uczestnika SWI, udzielam/y niniejszym dalszego pełnomocnictwa Panu/Pani, *(imię i nazwisko pełnomocnika)* posiadającemu/posiadającej numer identyfikacyjny PESEL/numer paszportu*, *(PESEL/ numer paszportu)* urodzonemu/urodzonej dnia* *(DD-MM-RRRR)* do składania i odbierania w imieniu i ze skutkiem dla Uczestnika SWI, przy użyciu systemu ESDI/WEB, oświadczeń i informacji, o których mowa w § 1 pkt 3 Porozumienia SWI, do występowania o wygenerowanie przeznaczonych dla Uczestnika SWI nowych środków bezpieczeństwa zgodnie z § 12 ust. 3 i 4 Regulaminu SWI, a także do odbioru z Krajowego Depozytu środków bezpieczeństwa ESDI/WEB oraz środków bezpieczeństwa dla wersji testowych ESDI/WEB.

.....
*imiona i nazwiska osób uprawnionych
do reprezentowania mocodawcy*

* - *niepotrzebne skreślić. W przypadku obywatela polskiego wpisać numer PESEL, w przypadku cudzoziemca wpisać numer paszportu oraz datę urodzenia*

FORMULARZ CERTYFIKACYJNY

SUBSKRYBENT		
A	DANE OSOBOWE	
	A1. Imię	
	A2. Nazwisko	
	A3. Kod kraju	A4. Obywatelstwo
	A5. PESEL ¹ / Data urodzenia ²	
	A6. Dokument tożsamości ☐ dowód osobisty ¹ ☐ paszport ²	
A	A7. Seria i numer	
	DANE KONTAKTOWE	
A8. e-mail		A9. Nr telefonu

DANE CERTYFIKACYJNE			
B	B1. Środowisko pracy: ☐ produkcyjne ☐ testowe	B2. Zastosowanie certyfikatu ☐ - certyfikat do systemu ESDI/WEB	B3. Kod instytucji
	B4. Nazwa Uczestnika SWI		

PODPIS SUBSKRYBENTA	
C	

INFORMACJA DLA SUBSKRYBENTA

Administratorem Pani/Pana danych osobowych jest Krajowy Depozyt Papierów Wartościowych S.A. z siedzibą w Warszawie (00-498) przy ul. Książęcej 4. Z KDPW S.A. można skontaktować się poprzez adres e-mail: kdpw@kdpw.pl lub pisemnie, pod adresem wskazanym powyżej.

Podstawa prawna oraz cel przetwarzania:

- wykonywania prawnie uzasadnionych interesów realizowanych przez KDPW S.A. polegających na potrzebie identyfikacji Pani/Pana jako osoby przesyłającej wiadomość do KDPW S.A. w imieniu podmiotu, który ustanowił Panią/Pana pełnomocnikiem/dalszym pełnomocnikiem do składania w jego imieniu oświadczeń za pośrednictwem ESDI/WEB zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przysyłania dokumentów w postaci elektronicznej oraz w celu zapewnienia bezpieczeństwa transakcji i innych czynności wykonywanych przez KDPW S.A., dochodzenia lub obrony ewentualnych roszczeń lub praw KDPW S.A. lub podmiotu, z którym KDPW S.A. łączy umowa, bądź inny stosunek prawny;
- wykonywania obowiązku prawnego – obowiązki takie wynikają z przepisów o przeciwdziałaniu praniu pieniędzy lub ustawy o obrocie instrumentami finansowymi.

¹ PESEL - dotyczy obywateli polskich.

² Data urodzenia – dotyczy obcokrajowców.

Dotyczące Pani/Pana dane osobowe możemy przekazywać do podmiotów lub organów, które są upoważnione do ich otrzymania na podstawie przepisów prawa.

Dotyczące Pani/Pana dane osobowe będą przechowywane przez okres nie dłuższy niż 10 lat od zakończenia uczestnictwa w systemie SWI podmiotu, który ustanowił Panią/Pana pełnomocnikiem/dalszym pełnomocnikiem do składania w jego imieniu oświadczeń za pośrednictwem ESDI/WEB zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej. Jeżeli toczy się spór, proces sądowy lub trwa inne postępowanie, okres przechowywania danych osobowych będzie liczony od dnia prawomocnego zakończenia sporu, a w przypadku wielu postępowań – prawomocnego zakończenia ostatniego z nich, bez względu na sposób jego zakończenia, chyba że przepisy prawa przewidują dłuższy okres przechowywania danych lub dłuższy okres przedawnienia dla roszczeń lub prawa, których/ego dotyczy postępowanie.

Przysługuje Pani/Panu prawo do żądania od KDPW S.A. dostępu do dotyczących Pani/Pana danych osobowych, prawo do ich sprostowania, gdy są niezgodne ze stanem rzeczywistym, a nadto, w przypadkach przewidzianych prawem, prawo do żądania ich usunięcia lub ograniczenia ich przetwarzania. Przysługuje Pani/Panu prawo do wniesienia sprzeciwu do przetwarzania danych osobowych. Przysługuje Pani/Panu prawo do przenoszenia danych.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego w zakresie przetwarzania Pani/Pana danych osobowych.

Podanie przez Panią/Pana danych osobowych jest dobrowolne i wynika ze stosunku prawnego pomiędzy KDPW S.A. a podmiotem, który ustanowił Panią/Pana pełnomocnikiem/dalszym pełnomocnikiem do składania w jego imieniu oświadczeń za pośrednictwem ESDI/WEB zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej. Niepodanie danych osobowych uniemożliwi wydanie Pani/Panu certyfikatu umożliwiającego przesyłanie wiadomości z wykorzystaniem systemu ESDI/WEB.

Pani/Pana dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji, w tym do profilowania, za wyjątkiem sytuacji, w których profilowanie może być związane z realizacją wymogów wynikających z przepisów prawa, np.: z koniecznością dokonania oceny ryzyka prania pieniędzy oraz finansowania terroryzmu.

	Potwierdzam zapoznanie się z powyższą informacją.
D	D1. Data i podpis subskrybenta.

Oświadczenie o autoryzacji prywatnego klucza kryptograficznego.....
miejsowość, data.....
kod instytucji

Ja, niżej podpisany/a zamieszkały/a
w przy ul., legitymujący/a
się dowodem osobistym/paszportem* serii nr wydanym przez
....., ważnym do dnia, oświadczam niniejszym, że:

1. uznaję wydany mi na podstawie Regulaminu SWI oraz Porozumienia w sprawie składania oświadczeń i przysyłania dokumentów w postaci elektronicznej zawartego pomiędzy Krajowym Depozytem Papierów Wartościowych S.A. a (nazwa (firma) mocodawcy) („**Uczestnik SWI**”) prywatny klucz kryptograficzny, odpowiadający certyfikatowi o nazwie (Common Name): za znak identyfikujący moją osobę w stopniu takim, jak mój własnoręczny podpis;
2. uznaję wszelkie dokumenty przesłane do Krajowego Depozytu Papierów Wartościowych S.A. przy użyciu systemu ESDI/WEB, za dokumenty przesłane przeze mnie, a wszelkie oświadczenia w nich zawarte za złożone przeze mnie w imieniu Uczestnika SWI, pod warunkiem, że przejdą one pozytywnie weryfikację autentyczności wiadomości;
3. zobowiązuję się używać wydanego mi prywatnego klucza kryptograficznego, o którym mowa powyżej, wyłącznie do składania oświadczeń w imieniu Uczestnika SWI przysyłanych przy użyciu systemu ESDI/WEB

.....
podpis osoby składającej oświadczenie

* - niepotrzebne skreślić