

REGULAMIN DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH KRAJOWEGO DEPOZYTU PAPIERÓW WARTOŚCIOWYCH

Rozdział 1

Postanowienia ogólne

§ 1

1. Regulamin dostępu do systemów informatycznych Krajowego Depozytu Papierów Wartościowych, zwany dalej „regulaminem”, określa zasady otwierania konta dostępowego, uwierzytelniania do konta dostępowego, zasady uzyskiwania dostępu do aplikacji KDPW udostępnianych w ramach Portalu usług <https://online.kdpw.pl> oraz zasady wymagane do zestawiania połączenia systemowego z aplikacjami KDPW.
2. Regulamin stosuje się w stosunkach prawnych wynikających z umów zawieranych przez KDPW z uczestnikami lub innymi podmiotami będącymi odbiorcami świadczonych przez KDPW usług oraz funkcjonalności, które są udostępniane z wykorzystaniem systemów informatycznych - w zakresie, jaki został określony w regulacjach KDPW dotyczących tych usług lub funkcjonalności.

§ 2

Ilekcroć w przepisach regulaminu mowa jest o:

- 1) aplikacji KDPW – rozumie się przez to każdą aplikację, wykorzystywaną do komunikacji elektronicznej z KDPW w ramach danej usługi, umożliwiającą wymianę komunikatów pomiędzy uczestnikiem a KDPW, przy wykorzystaniu transmisji danych, udostępnianą z wykorzystaniem dedykowanego punktu dostępowego lub poprzez interfejs A2A;
- 2) Portalu usług – rozumie się przez to portal usług dostępny poprzez stronę <https://online.kdpw.pl>;
- 3) punkcie dostępowym – rozumie się przez to adres URL kierujący do aplikacji KDPW poprzez interfejs U2A;
- 4) usłudze – rozumie się przez to świadczoną przez KDPW usługę albo funkcjonalności, udostępniane uczestnikom z wykorzystaniem aplikacji KDPW;
- 5) uczestniku – rozumie się przez to podmiot, który jest stroną umowy o uczestnictwo zawartej na podstawie regulaminu usługi, albo stroną innej umowy zawartej zgodnie z regulaminem usługi, albo podmiot uzyskujący dostęp do innych funkcjonalności udostępnianych przez KDPW z wykorzystaniem aplikacji KDPW;
- 6) regulaminie usługi – rozumie się przez to wzorzec umowy kształtujący treść stosunku prawnego pomiędzy KDPW a uczestnikiem, obowiązujący w ramach danej usługi, albo inną umowę zawartą przez KDPW z uczestnikiem o świadczenie danej usługi;
- 7) komunikacie - rozumie się przez to informację lub oświadczenie, które zgodnie z postanowieniami regulaminu usługi, w relacji pomiędzy uczestnikiem a KDPW, mogą albo powinny być przekazane z wykorzystaniem środków komunikacji elektronicznej;

- 8) komunikacji elektronicznej – rozumie się przez to składanie i odbieranie oświadczeń woli i informacji, które zgodnie z regulaminem usługi, w stosunkach z KDPW mogą lub powinny być, przez uczestnika lub temu uczestnikowi, przekazywane z wykorzystaniem aplikacji KDPW;
- 9) KDPW – rozumie się przez to spółkę Krajowy Depozyt Papierów Wartościowych S.A.;
- 10) KDPW_CCP – rozumie się przez to spółkę zależną od KDPW, KDPW_CCP S.A.;
- 11) dniu roboczym – rozumie się przez to każdy dzień tygodnia, który nie jest dniem ustawowo wolnym od pracy oraz sobotą.

§ 3

1. Komunikacja elektroniczna z KDPW dostępna jest poprzez następujące interfejsy komunikacyjne:
 - 1) interfejs U2A, będący interfejsem graficznym, wspierającym manualną wymianę danych z aplikacją KDPW dostępny w postaci interfejsu wprowadzania danych albo przekazywania ustrukturyzowanych komunikatów do dedykowanych kolejek, lub
 - 2) interfejs A2A, będący interfejsem wspierającym automatyczną wymianę danych pomiędzy aplikacją KDPW a aplikacją uczestnika, przy wykorzystaniu dedykowanych kolejek.
2. Interfejsy komunikacyjne określone są dla każdej z usług odrębnie zgodnie z przyjętymi w danej usłudze zasadami dotyczącymi komunikacji.
3. Komunikaty przekazane przez uczestnika do KDPW z wykorzystaniem interfejsu U2A, poprzez interfejs wprowadzania danych, uznaje się za doręczone z chwilą przyjęcia komunikatu przez KDPW, przy czym za przyjęcie komunikatu uważa się jego zapisanie w odpowiedniej aplikacji KDPW. Komunikaty przekazane przez KDPW uczestnikowi z wykorzystaniem interfejsu U2A, poprzez interfejs wprowadzania danych, uznaje się za doręczone z chwilą zamieszczenia komunikatu w aplikacji albo, jeżeli tak postanowiono w danej usłudze, z chwilą wysłania uczestnikowi przez KDPW notyfikacji mailowej o umieszczeniu komunikatu w aplikacji. Adresem mailowym do doręczeń notyfikacji jest adres wskazany w formularzu, o którym mowa w § 7 ust. 3 pkt 1, jako adres do korespondencji. Adres ten potwierdza uczestnik składając oświadczenie w sprawie udzielenia osobie, o której mowa w § 7 ust. 7 pkt 1, upoważnienia do działania w jego imieniu, a w przypadku, gdy dostępu udziela osoba upoważniona przez uczestnika, o której mowa w § 7 ust. 7 pkt 2, potwierdza go ta osoba, poprzez udzielenie dostępu do aplikacji.
4. Komunikaty przekazane do KDPW z wykorzystaniem interfejsu A2A albo interfejsu U2A poprzez ustrukturyzowane komunikaty do dedykowanych kolejek uznaje się za doręczone z chwilą przyjęcia komunikatu przez KDPW, przy czym za przyjęcie komunikatu uznaje się rozpoczęcie kontroli tego komunikatu w aplikacji KDPW. Komunikaty przekazane przez KDPW uczestnikowi z wykorzystaniem interfejsu A2A uznaje się za doręczone z chwilą umieszczenia w kolejce wyjściowej uczestnika.
5. Przyjęte dla danej usługi zasady komunikacji mogą wprowadzać dodatkowe obowiązki uczestnika związane z przekazywaniem komunikatów, w szczególności mogą wymagać potwierdzenia w procesie uwierzytelniania lub opatrzenia komunikatu podpisem elektronicznym.
6. KDPW oraz uczestnicy uznają skuteczność doręczeń komunikatów, z zachowaniem warunków przewidzianych w niniejszym regulaminie, oraz wyrażają zgodę na przeprowadzenie wszelkich dowodów na fakt dokonania tych czynności.

§ 4

1. Z zastrzeżeniem ust. 2 - 4, komunikacja elektroniczna z KDPW dostępna jest dla uczestnika w trybie 24/7.

2. KDPW może wprowadzić przerwę techniczną w działaniu aplikacji KDPW, zgodnie z zasadami określonymi w regulaminach usług lub przyjętymi w danej usłudze zasadami komunikacji.
3. KDPW może również wprowadzić przerwę techniczną w działaniu interfejsów komunikacyjnych.
4. W komunikacji z wykorzystaniem interfejsu A2A może również wystąpić przerwa w dostępności kolejek komunikacyjnych spowodowana kilkuminutowymi przerwami technicznymi związanymi ze zmianą konfiguracji ustawień tych kolejek.
5. W przypadku wykorzystywania do komunikacji z aplikacjami KDPW interfejsu A2A, uczestnik zobowiązany jest do skonfigurowania w swoim systemie automatycznego wznowienia połączenia do kolejek komunikacyjnych.

Rozdział 2

Komunikacja elektroniczna z wykorzystaniem interfejsu U2A

Oddział 1

Otwarcie konta dostępowego

§ 5

1. Komunikacja elektroniczna z KDPW z wykorzystaniem interfejsu U2A wymaga otwarcia konta dostępowego poprzez stronę internetową KDPW.
2. Konto dostępowe otwiera osoba fizyczna działając we własnym imieniu, poprzez wypełnienie dedykowanego formularza, wymaganymi w tym formularzu danymi tej osoby. Przy wypełnianiu formularza osoba ta składa oświadczenie wyrażające zgodę na przetwarzanie przez KDPW jej danych osobowych zawartych w formularzu. Nieudzielenie takiej zgody uniemożliwia otwarcie konta dostępowego oraz złożenie wniosku o uzyskanie dostępu do aplikacji KDPW, a jej cofnięcie skutkuje zamknięciem konta dostępowego oraz utratą wszystkich uzyskanych dostępu do aplikacji KDPW. Otwarcie konta dostępowego możliwe jest po weryfikacji adresu poczty elektronicznej podanego w formularzu, która dokonywana jest poprzez wprowadzenie do formularza wygenerowanego przez aplikację i przekazanego na ten adres kodu weryfikacyjnego.
3. Adres poczty elektronicznej podany w formularzu jest identyfikatorem konta dostępowego (loginem). Login nie podlega zmianie. W przypadku zmiany adresu poczty elektronicznej, osoba fizyczna powinna otworzyć nowe konto oraz ponownie uzyskać dostęp do aplikacji KDPW.
4. Szczegółowe informacje dotyczące otwarcia konta dostępowego oraz sposobu korzystania z konta dostępowego przez jego posiadacza, znajdują się w instrukcji użytkownika konta, zamieszczonej na stronie internetowej KDPW.
5. Uczestnik zobowiązany jest niezwłocznie zgłosić KDPW każde podejrzenie możliwości wykorzystania konta dostępowego osoby, która uzyskała dostęp do aplikacji KDPW w jego imieniu, przez osobę nieuprawnioną.
6. KDPW dokonuje blokady konta dostępowego w przypadku, gdy utrzymywanie tego konta zagraża bezpieczeństwu systemów informatycznych KDPW.
7. KDPW może przeprowadzać weryfikację aktywności kont dostępowych, polegającą na zweryfikowaniu dostępu osób będących posiadaczami kont dostępowych do adresów poczty elektronicznej, będących identyfikatorami tych kont. W przypadku braku uzyskania przez KDPW potwierdzenia aktywności danego konta, KDPW może zarówno zablokować jak i usunąć konto,

odbierając jednocześnie osobie, która wskazała ten adres w formularzu, dostęp do aplikacji KDPW.

Oddział 2

Uwierzytelnienie do konta dostępowego

§ 6

1. Logowanie do aplikacji KDPW wymaga przeprowadzenia procesu uwierzytelnienia do konta dostępowego. Przez uwierzytelnienie rozumie się proces polegający na potwierdzeniu przez posiadacza konta dostępowego zadeklarowanej przez niego, przy otwieraniu tego konta, tożsamości.
2. Podstawowym mechanizmem uwierzytelnienia do konta dostępowego wymaganym przy logowaniu do wszystkich aplikacji KDPW jest podanie loginu i ustanowionego przez posiadacza konta, hasła do konta dostępowego.
3. Logowanie do aplikacji KDPW udostępnianych w ramach Portalu usług, wymaga użycia dodatkowego mechanizmu uwierzytelnienia, jakim jest potwierdzenie deklarowanej tożsamości z wykorzystaniem dedykowanej aplikacji mobilnej KDPW Group Authenticator.
4. Potwierdzenie z wykorzystaniem aplikacji mobilnej KDPW Group Authenticator jest wymagane przy każdym kolejnym logowaniu do Portalu usług.
5. Potwierdzenie, o którym mowa w ust. 4, nie jest wymagane, w przypadku, gdy logowanie następuje na komputerze lub urządzeniu mobilnym z wykorzystaniem przeglądarki, która przez posiadacza konta została zarejestrowana jako zaufana. Posiadacz konta ma możliwość zarządzania przeglądarkami oznaczonymi jako zaufane za pomocą aplikacji dostępnej pod adresem <https://identity.kdpw.pl>.
6. Uwierzytelnienie do konta dostępowego, z użyciem dodatkowego mechanizmu uwierzytelnienia, o którym mowa w ust. 3, pozwala posiadaczowi konta na dostęp do wszystkich aplikacji KDPW, do których uzyskał wcześniej dostęp, a także do aplikacji KDPW_CCP udostępnianych przez Portal usług, zgodnie z odrębnymi regulacjami przyjętymi przez tę spółkę. W przypadku gdy posiadacz konta dokona logowania do aplikacji KDPW poprzez punkt dostępowy, do którego wymagane jest wyłącznie potwierdzenie podstawowym mechanizmem uwierzytelnienia, logowanie do Portalu usług będzie wymagać ponownego uwierzytelnienia do konta dostępowego.
7. KDPW określa wymagania techniczne dla urządzeń mobilnych, na których aplikacja KDPW Group Authenticator może zostać uruchomiona. Uczestnik jest zobowiązany zapewnić osobie, o której mowa w § 7 ust.7, dostęp do urządzenia spełniającego te wymagania.
8. Za pobranie oraz korzystanie z aplikacji KDPW Group Authenticator KDPW nie pobiera opłat.
9. Szczegółowe informacje dotyczące pobrania oraz korzystania z aplikacji mobilnej KDPW Group Authenticator, w tym wymagań technicznych dla urządzeń mobilnych, na jakich aplikacja może zostać uruchomiona, oraz zasady zarządzania przeglądarkami oznaczonymi jako zaufane znajdują się w instrukcji użytkownika konta, zamieszczonej na stronie internetowej KDPW.

Oddział 3

Uzyskanie dostępu do aplikacji KDPW udostępnianych w ramach Portalu usług

§ 7

1. Uzyskanie dostępu do aplikacji KDPW przez osobę będącą posiadaczem konta dostępowego następuje na podstawie wniosku.
2. Uzyskanie dostępu do aplikacji KDPW może wymagać podania dodatkowych danych identyfikujących osobę upoważnioną przez uczestnika, którymi są: numer PESEL – w przypadku osób z polskim obywatelstwem, albo data urodzenia – w przypadku osób z obywatelstwem innym niż polskie.
3. Złożenie wniosku polega na:
 - 1) wypełnieniu przez osobę upoważnioną przez uczestnika dedykowanego formularza internetowego udostępnionego w ramach Portalu usług oraz
 - 2) dostarczeniu do KDPW oświadczenia złożonego przez uczestnika w sprawie udzielenia tej osobie upoważnienia do działania w jego imieniu w zakresie wskazanym w tym oświadczeniu oraz potwierdzającego dane osobowe tej osoby wskazane przez nią w formularzu, o którym mowa w pkt 1. Dostarczenie oświadczenia do KDPW nie jest wymagane w przypadku, gdy dostępu udziela osoba upoważniona przez uczestnika, o której mowa w ust. 7 pkt 2; poprzez udzielenie dostępu do aplikacji, osoba ta potwierdza jednocześnie dane osobowe ustanowionego przez nią pełnomocnika.
4. Oświadczenie, o którym mowa w ust. 3 pkt 2, uczestnik dostarcza do KDPW w formie pisemnej albo elektronicznej (w postaci dokumentu opatrzonego kwalifikowanym podpisem elektronicznym). Oświadczenie może zostać dostarczone w postaci skanu nieopatrzonego kwalifikowanym podpisem elektronicznym, w przypadku usługi, dla której taka forma oświadczenia została wskazana jako dopuszczalna osobie upoważnionej przez uczestnika w wiadomości mailowej wygenerowanej automatycznie po wypełnieniu przez tą osobę formularza, o którym mowa w ust. 3 pkt 1.
5. Uzyskanie dostępu do danej aplikacji KDPW, może również nastąpić, o ile przewidują to postanowienia właściwego regulaminu usługi, na podstawie uprzednio uzyskanych przez daną osobę uprawnień dostępowych, w szczególności poprzez przyznanie dostępu do aplikacji KDPW w sposób automatyczny osobie, która posiada już uprawnienia do działania w innej aplikacji.
6. Wniosek, o którym mowa w ust. 3, powinien zostać złożony nie później niż na 5 dni roboczych przed dniem, w którym osoba upoważniona przez uczestnika, zamierza po raz pierwszy przekazać albo otrzymać komunikat za pośrednictwem aplikacji KDPW.
7. O ile regulamin usługi nie stanowi inaczej, wniosek może dotyczyć uzyskania przez osobę upoważnioną przez uczestnika uprawnienia do:
 - 1) komunikacji elektronicznej z KDPW w imieniu uczestnika, a w przypadku, gdy uczestnik działa w ramach danej usługi w imieniu innego lub innych podmiotów, również do komunikacji elektronicznej z KDPW w imieniu tych innych podmiotów (rola użytkownika), albo
 - 2) udzielania innym osobom, które poprzez wypełnienie formularza, o którym mowa w ust.3 pkt 1, wystąpią o uzyskanie dostępu do aplikacji KDPW w zakresie określonym w pkt 1, upoważnień do komunikacji elektronicznej z KDPW w imieniu uczestnika, a także odwoływania takich upoważnień, poprzez, odpowiednio, udzielanie albo odbieranie im dostępu do aplikacji KDPW, a w przypadku, gdy uczestnik działa w ramach danej usługi w imieniu innego lub innych podmiotów - również do działania w powyższym zakresie w imieniu tych innych podmiotów (rola administratora).

8. Z zastrzeżeniem § 8, KDPW akceptuje albo odrzuca wniosek po przeprowadzeniu jego weryfikacji formalnej i merytorycznej.
9. KDPW posiada uprawnienie do automatycznego usunięcia z Portalu usług formularza, o którym mowa w ust. 3 pkt 1, po upływie terminu nie krótszego niż 90 dni kalendarzowych od dnia wypełnienia tego formularza, w przypadku, gdy w tym terminie wniosek o uzyskanie dostępu do aplikacji KDPW przez osobę, która wypełniła ten formularz, nie uzyska akceptacji KDPW.
10. W przypadku odrzucenia wniosku lub usunięcia formularza, uzyskanie dostępu do aplikacji KDPW wymaga ponownego złożenia wniosku.

§ 8

Określone dla danej usługi zasady dotyczące komunikacji, mogą przewidywać, że KDPW akceptuje albo odrzuca wyłącznie wnioski dotyczące uzyskania uprawnień, o których mowa w § 7 ust. 7 pkt 2 (rola administratora). W takim przypadku, uczestnik zobowiązany jest upoważnić przynajmniej jedną osobę do działania w jego imieniu w roli administratora. Uzyskanie dostępu do aplikacji KDPW przez osobę działającą w imieniu uczestnika w roli użytkownika, albo odebranie dostępu do aplikacji KDPW takiej osobie, może nastąpić wyłącznie przez osobę działającą w imieniu tego uczestnika, która uzyskała dostęp do tej aplikacji w roli administratora.

§ 9

1. Lista aplikacji KDPW dostępnych dla poszczególnych posiadaczy kont dostępowych w ramach Portalu usług jest uaktualniania w momencie każdego logowania.
2. W przypadku, gdy uprawnienia dostępu do aplikacji KDPW zostały nadane w trakcie aktywnej sesji posiadacza konta, uprawnienia te mogą być realizowane po wylogowaniu się z tej sesji i powtórnym zalogowaniu się.
3. Weryfikacja posiadanych przez posiadacza konta uprawnień dostępu do aplikacji KDPW przeprowadzana jest w czasie trwania sesji dostępowej. Brak możliwości potwierdzenia uprawnień skutkuje utratą dostępu.

§ 10

1. Osobę, która uzyskała dostęp do aplikacji KDPW w roli użytkownika, w związku z dostarczeniem przez uczestnika oświadczenia, o którym mowa w § 7 ust.3 pkt 2, albo na podstawie upoważnienia udzielonego jej zgodnie z § 7 ust.7 pkt 2, uważa się za osobę upoważnioną przez uczestnika do komunikacji elektronicznej z KDPW realizowanej za pośrednictwem tej aplikacji, a czynności dokonane przez taką osobę uznaje się za czynności dokonane przez tego uczestnika w imieniu własnym lub w imieniu reprezentowanego przez niego w ramach tej aplikacji podmiotu. Postanowienie zdania poprzedzającego stosuje się także w przypadku, gdy formularz lub oświadczenie, o których mowa w § 7 ust.3, zawiera nieprawidłowe dane osobowe osoby, której dotyczą.
2. Osobę, która uzyskała dostęp do aplikacji KDPW w roli administratora, w związku z dostarczeniem przez uczestnika oświadczenia, o którym mowa w § 7 ust.3 pkt 2, uważa się za osobę upoważnioną do udzielania innym osobom upoważnień uprawniających je do komunikacji elektronicznej z KDPW realizowanej za pośrednictwem tej aplikacji przez uczestnika działającego w imieniu własnym lub w imieniu reprezentowanego przez niego w ramach tej aplikacji podmiotu. Postanowienie ust.1 zd. drugie stosuje się odpowiednio.

3. Uczestnik zobowiązany jest, odpowiednio:
 - 1) zapewnić należytą ochronę danych wykorzystywanych do logowania się przez osobę upoważnioną do aplikacji KDPW a także zapewnić tej osobie warunki do właściwego zabezpieczenia urządzeń, z wykorzystaniem których osoba ta loguje się do tej aplikacji, oraz ochrony tych urządzeń przed złośliwym oprogramowaniem lub dostępem osób nieuprawnionych, albo
 - 2) na bieżąco weryfikować, czy stosowane przez osobę upoważnioną, metody i środki mające zapewnić ochronę danych wykorzystywanych przez nią do logowania się do aplikacji KDPW oraz mające chronić urządzenia, z wykorzystaniem których osoba ta loguje się do tej aplikacji, przed złośliwym oprogramowaniem lub dostępem osób nieuprawnionych, są adekwatne i zapewniają należyty poziom tej ochrony.
4. Ryzyko związane z doбором stosowanych środków ochrony lub metod zabezpieczenia danych lub urządzeń, o których mowa w ust.3 pkt 1 lub 2, obciąża wyłącznie uczestnika. Jeżeli środki ochrony lub metody zabezpieczenia danych lub urządzeń, o których mowa w ust.3 pkt 1 lub 2, okażą się z jakichkolwiek powodów niewystarczające lub zawodne, wyłączną odpowiedzialność za skutki takiego stanu ponosi uczestnik. Odpowiedzialność ta jest niezależna od winy uczestnika.
5. KDPW nie ponosi odpowiedzialności za działania i zaniechania osób upoważnionych przez uczestnika, w szczególności za utratę lub udostępnianie przez te osoby danych do logowania osobom trzecim.

§ 11

1. Odebranie dostępu do aplikacji KDPW może zostać dokonane:
 - 1) przez KDPW – w wyniku odwołania przez uczestnika upoważnienia udzielonego osobie, o której mowa w § 7 ust. 7 pkt 1 lub 2;
 - 2) przez KDPW – w przypadku zgłoszenia przez uczestnika:
 - a) podejrzenia uzyskania dostępu do aplikacji KDPW, przy użyciu danego konta dostępowego, przez osobę nieuprawnioną,
 - b) naruszenia ochrony danych wykorzystywanych do logowania do aplikacji KDPW;
 - 3) przez osobę upoważnioną przez uczestnika, występującą w roli administratora - poprzez odebranie dostępu do aplikacji KDPW osobie, o której mowa w § 7 ust.7 pkt 1.
2. Odwołanie upoważnienia, o którym mowa w ust. 1 pkt 1, staje się skuteczne względem KDPW z upływem drugiego dnia roboczego po dniu dostarczenia do KDPW oświadczenia uczestnika w tej sprawie, złożonego w formie pisemnej albo elektronicznej (w postaci dokumentu opatrzonego kwalifikowanym podpisem elektronicznym).

Rozdział 3

Komunikacja elektroniczna z wykorzystaniem interfejsu A2A

§ 12

1. Komunikacja z wykorzystaniem interfejsu A2A działa w oparciu o kolejki służące przekazywaniu komunikatów, utworzone w ramach poszczególnych kanałów komunikacyjnych.
2. Kanały komunikacyjne mogą być powoływane niezależnie dla każdej aplikacji KDPW. Dopuszcza się również wykorzystanie kanału komunikacyjnego do dostępu do więcej niż jednej aplikacji KDPW, poprzez tworzenie dedykowanych im kolejek.
3. Wszystkie kolejki udostępniane w ramach interfejsu A2A tworzone są na zasadach zgodnych z regulaminami usług oraz przyjętymi w danej usłudze zasadami komunikacji. W ramach

ustanawianej komunikacji, przewiduje się tworzenie par kolejek, odrębnie dla każdego kierunku komunikacji.

4. Dostęp do kolejek komunikacyjnych realizowany jest po uwierzytelnieniu dostępu do kanału komunikacyjnego, w ramach którego są one utworzone, z wykorzystaniem pobranego przez uczestnika certyfikatu elektronicznego. Komunikacja wewnątrz kanałów komunikacyjnych zabezpieczona jest protokołem szyfrowania TLS.
5. Połączenie do infrastruktury KDPW może być realizowane zarówno w modelu klient-serwer jak również serwer-serwer. Wymagane jest wykorzystanie połączenia opartego o VPN z uwierzytelnianiem opartym o mechanizm współdzielonego klucza (pre-shared key).

§ 13

KDPW zastrzega sobie prawo do usuwania z kolejek komunikacyjnych komunikatów, które nie zostały odebrane przez adresata, po upływie 30 dni od dnia przekazania komunikatu, albo w terminie krótszym, jeżeli został uzgodniony z uczestnikiem.

§ 14

1. Ustanowienie komunikacji elektronicznej z wykorzystaniem interfejsu A2A, wymaga pobrania przez uczestnika certyfikatu elektronicznego.
2. Pobranie certyfikatu elektronicznego wymaga wypełnienia przez osobę upoważnioną przez uczestnika, dedykowanego formularza zamieszczonego na stronie internetowej KDPW, wymaganymi w tym formularzu danymi, oraz dostarczenia do KDPW złożonego w formie pisemnej albo elektronicznej (w postaci dokumentu opatrzonego kwalifikowanym podpisem elektronicznym), oświadczenia uczestnika w sprawie uznania skuteczności doręczeń komunikatów dokonywanych z wykorzystaniem tego certyfikatu. KDPW doręcza certyfikat uczestnikowi na adres poczty elektronicznej wskazany przez osobę upoważnioną przez uczestnika w formularzu oraz potwierdzony przez uczestnika w dostarczonym oświadczeniu.
3. Certyfikat elektroniczny służy do uwierzytelnienia uczestnika składającego komunikat z wykorzystaniem tego certyfikatu do dedykowanego kanału komunikacyjnego.
4. Uczestnik zobowiązany jest przechowywać pobrany certyfikat elektroniczny w sposób zapewniający dostęp do certyfikatu wyłącznie osobom upoważnionym. Od chwili pobrania certyfikatu do chwili unieważnienia tego certyfikatu ryzyko jego utraty lub ujawnienia obciąża wyłącznie uczestnika.

§ 15

1. Z zastrzeżeniem ust. 3, certyfikaty elektroniczne zachowują ważność przez okres wskazany w treści certyfikatu, z uwzględnieniem okresu ważności certyfikatów urzędów certyfikacji, które wydają ten certyfikat.
2. Uczestnicy zobowiązani są do stałego monitorowania okresu ważności pobranych certyfikatów elektronicznych. Uczestnik powinien wystąpić do KDPW o wydanie nowego certyfikatu elektronicznego nie później niż na 10 dni roboczych przed dniem, utraty ważności tego certyfikatu.
3. KDPW może przed upływem terminu, o którym mowa w ust. 1, unieważnić certyfikat elektroniczny, z własnej inicjatywy z przyczyn technicznych, na wniosek uczestnika albo w związku z podejrzeniem, że certyfikatem elektronicznym posługuje się osoba nieupoważniona przez

uczestnika.

4. KDPW udostępnia uczestnikom, na swojej stronie internetowej, listy certyfikatów unieważnionych (CRL) niezbędne do weryfikacji ważności certyfikatów. Udostępnienie informacji o unieważnieniu certyfikatu na liście, następuje niezwłocznie po unieważnieniu tego certyfikatu elektronicznego.
5. W przypadku unieważnienia certyfikatu elektronicznego, KDPW niezwłocznie informuje o tym fakcie uczestnika, na adres poczty elektronicznej wskazany w formularzu, o którym mowa w § 14 ust. 2.

§ 16

1. W razie utraty certyfikatu elektronicznego albo powstania uzasadnionego podejrzenia udostępnienia certyfikatu elektronicznego osobie nieupoważnionej, uczestnik, który pobrał certyfikat elektroniczny, niezwłocznie zwraca się do KDPW o unieważnienie certyfikatu elektronicznego, wskazując przyczyny uzasadniające jego unieważnienie.
2. Unieważnienie certyfikatu elektronicznego z przyczyn, o których mowa w ust. 1, następuje niezwłocznie po otrzymaniu żądania unieważnienia tego certyfikatu. Żądanie uczestnik dostarcza do KDPW w formie pisemnej albo elektronicznej (w postaci dokumentu opatrzonego kwalifikowanym podpisem elektronicznym).
3. KDPW nie ponosi odpowiedzialności za szkody wyrządzone uczestnikowi w związku z utratą certyfikatu elektronicznego, w okresie jego ważności.

§ 17

KDPW nie jest kwalifikowanym dostawcą 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 uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L Nr 257, str. 73). W związku z powyższym, certyfikat, o którym mowa w § 14, nie jest kwalifikowanym certyfikatem podpisu elektronicznego w rozumieniu tego rozporządzenia. Oznacza to w szczególności, że uwierzytelnieniu komunikatów z wykorzystaniem 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.

Rozdział 4

Przepisy końcowe

§ 18

1. KDPW jest uprawniony do dokonywania zmian niniejszego regulaminu.
2. Treść zmian regulaminu, KDPW udostępnia uczestnikom na swojej stronie internetowej. Zmiany wchodzi w życie w terminie dwóch tygodni od dnia ich udostępnienia, chyba że uchwała Zarządu KDPW wprowadzająca zamiany będzie wskazywać dłuższy termin ich wejścia w życie.
3. Dokonanie zmiany regulaminu wymaga powiadomienia uczestnika o treści zmian oraz dacie ich wejścia w życie z zachowaniem terminu, o którym mowa w ust.2.
4. Przekazanie informacji o dokonanej zmianie regulaminu, przy wykorzystaniu poczty elektronicznej, na adres poczty elektronicznej osoby upoważnionej przez uczestnika do uzyskania dostępu do

aplikacji KDPW lub do pobrania certyfikatu, o którym mowa w § 14 ust. 2, uznaje się za skuteczne powiadomienie uczestnika o tej zmianie, o ile regulamin usługi nie stanowi inaczej.

5. W przypadku, gdy uczestnik nie wyraża zgody na dokonanie zmiany regulaminu, przysługuje mu prawo wypowiedzenia umowy z KDPW o świadczenie usługi, z zachowaniem warunków wypowiedzenia przewidzianych w regulaminie usługi.
6. Jeżeli uczestnik nie wypowiedział umowy o uczestnictwo zgodnie z ust. 5, oznacza to, że uczestnik wyraził zgodę na zmiany regulaminu, o których został powiadomiony zgodnie z postanowieniami ust. 3 - 4.