



Zakład Ubezpieczeń Społecznych

00-701 Warszawa, ul. Czerniakowska 16

Zasady
elektronicznego
przekazywania
dokumentów
ubezpieczeniowych
do ZUS

wersja 2.7

Poradnik

Zasady elektronicznego przekazywania dokumentów do ZUS.
Poradnik dla płatników składek
wersja 2.7

Poradnik
data aktualizacji: 5-04-2005 r.
Poradnik dostępny bezpłatnie w serwisie www.zus.pl

Spis treści

WSTĘP	4
CELE ZASTOSOWANIA ELEKTRONICZNEJ WYMIANY DOKUMENTÓW	6
BEZPIECZEŃSTWO DANYCH W ELEKTRONICZNEJ WYMIANIE DOKUMENTÓW	8
2.1 PODPIS CYFROWY.....	9
2.2 SZYFROWANIE DOKUMENTÓW ELEKTRONICZNYCH	9
2.3 OBOWIĄZKI UCZESTNIKÓW ELEKTRONICZNEJ WYMIANY DOKUMENTÓW	9
2.3.1 <i>Ochrona klucza prywatnego</i>	10
2.3.2 <i>Autentyczność klucza publicznego</i>	10
2.4 KOMUNIKAT ELEKTRONICZNY	10
STRONY BIORĄCE UDZIAŁ W ELEKTRONICZNEJ WYMIANIE DOKUMENTÓW	11
3.1 PŁATNIK	11
3.2 ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH	11
3.3 CENTRUM CERTYFIKACJI UNIZETO CERTUM	12
SYSTEM DWUSTRONNEJ WYMIANY INFORMACJI	14
PRZEKAZYWANIE DOKUMENTÓW W IMIENIU PŁATNIKA	16
5.1. SZCZEGÓŁOWE PROCEDURY OBSŁUGI UPOWAŻNIEŃ	17
BIEŻĄCA ELEKTRONICZNA WYMIANA DOKUMENTÓW POMIĘDZY PŁATNIKIEM A ZUS	20
6.1. AUTOMATYCZNE WYSYŁANIE DOKUMENTÓW BEZPOŚREDNIO Z PROGRAMU PŁATNIK	21
6.2. PRZYGOTOWANIE NOŚNIKA CD ZAWIERAJĄCEGO DOKUMENTY UBEZPIECZENIOWE	22
6.3. PRZESYŁANIE DOKUMENTÓW UBEZPIECZENIOWYCH DROGĄ TELETRANSMISJI	23
ZAŁĄCZNIK - SŁOWNIK PODSTAWOWYCH TERMINÓW I SKRÓTÓW	25

WSTĘP

Idea wykorzystania sieci **Internet** do **sprawnego, szybkiego i bezpiecznego** przesyłania danych w formie **dokumentów elektronicznych** wkracza coraz powszechniej do różnorodnych form życia gospodarczego i społecznego. Niniejsze opracowanie przeznaczone jest dla **płatnika składek ZUS**, zwanego w skrócie **płatnikiem**, który został zobowiązany na mocy ustawy z dnia 18 grudnia 2002 roku o zmianie ustawy o systemie ubezpieczeń społecznych oraz niektórych innych ustaw (Dz. U. Nr 8 poz. 64) lub zechce skorzystać z tej wygodnej i nowoczesnej formy komunikacji do przekazywania dokumentów ubezpieczeniowych w postaci elektronicznej do **Zakładu Ubezpieczeń Społecznych**.

Warunki jakie muszą spełnić płatnicy przystępujący do elektronicznego przekazywania dokumentów ubezpieczeniowych do ZUS określa Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 3 lipca 2001 roku w sprawie warunków, jakie muszą spełnić płatnicy składek przekazujący dokumenty ubezpieczeniowe w formie dokumentu elektronicznego poprzez teletransmisję danych (Dz. U. Nr 73 poz. 774).

W opracowaniu przedstawiono procedury postępowania przy przystąpieniu płatnika do elektronicznej wymiany dokumentów oraz przy przekazywaniu dokumentów ubezpieczeniowych w formie elektronicznej do ZUS przy wykorzystaniu sieci internet i nośników CD.

Opisano również w sposób ogólny metody ochrony przesyłanych elektronicznie danych, zakładając że czytelnik nie jest specjalistą z zakresu kryptologii.

Szczegółowy opis wszystkich procedur związanych z obsługą certyfikatu klucza publicznego zostały opisane w dokumencie „Zasady komunikacji pomiędzy płatnikiem, Centrum Certyfikacji i Punktem Rejestracji” dostępnym na stronach internetowych ZUS <http://e-inspektorat.zus.pl> i na płycie CD z programem Płatnik.

Na końcu opracowania zamieszczono załącznik – słownik podstawowych terminów i skrótów.

Stosowane symbole

W dokumencie stosowane są też następujące symbole graficzne:

Symbol	Znaczenie
	Uwaga bardzo ważna dla realizacji zadania lub opisująca istotne aspekty merytoryczne.
	Informacja pomocnicza.



1

Rozdział

CELE ZASTOSOWANIA ELEKTRONICZNEJ WYMIANY DOKUMENTÓW

Elektroniczna wymiana dokumentów posiada dwie istotne cechy świadczące o celowości tej formy korespondencji: **wygoda i bezpieczeństwo**.



WYGODA

Po wykonaniu czynności wstępnych, związanych z instalacją na swoim komputerze programu Płatnik i potwierdzeniem swego uczestnictwa w systemie elektronicznej wymiany dokumentów, korespondencja Płatnika z terenowymi jednostkami organizacyjnymi ZUS staje się w dużym stopniu zautomatyzowana. Większość rutynowych operacji, związanych z wypełnianiem formularzy zawierających dane Płatnika oraz redagowaniem wiadomości przeznaczonych dla odbiorcy, którym jest ZUS, wykonywana jest automatycznie przez program służący do tego celu.

Wysyłając dokument elektroniczny do ZUS poprzez sieć internetową i pobierając tą samą drogą potwierdzenie użytkownik oszczędza czas, który dotychczas był przeznaczony na przygotowywanie dokumentów papierowych, jak również przeznaczony na osobiste wizyty w ZUS lub czynności związane z nadawaniem i odbiorem klasycznych przesyłek pocztowych.

Dodatkowym atutem jest możliwość **archiwizowania i przechowywania** w formie elektronicznej dokumentów wysyłanych i potwierdzeń ich odbioru. Dzięki temu istnieje możliwość łatwego i szybkiego odtworzenia dotychczasowej korespondencji, np. w przypadku sporów dotyczących jej przebiegu.



BEZPIECZEŃSTWO

Wykorzystywane w systemie mechanizmy zapewniania bezpieczeństwa przesyłanej korespondencji oparte są na powszechnie akceptowanych i stosowanych rozwiązaniach, opartych na standardach ogólnosiwiatowych. Właściwie zorganizowana infrastruktura (uwzględniająca istnienie darzonego zaufaniem neutralnego arbitra, potwierdzającego wiarygodność uczestników elektronicznej wymiany dokumentów) sprawia, że:

- dokumenty wysyłane są w sposób poufny; odczytać je może jedynie uprawniony odbiorca, wskazany przez nadawcę dokumentu;
- nie istnieje możliwość sfałszowania przesyłanego dokumentu, ani wystania dokumentu w imieniu nadawcy bez jego zgody;
- każdy dokument jest „podpisany”; odbiorca może zatem jednoznacznie określić nadawcę dokumentu; z drugiej strony – nadawca (w tym przypadku inicjujący kolejną wymianę dokumentów elektronicznych) po odebraniu potwierdzenia odbioru wysłanej korespondencji jest w stanie stwierdzić, czy dokument dotarł do właściwego adresata.

2

Rozdział

BEZPIECZEŃSTWO DANYCH W ELEKTRONICZNEJ WYMIANIE DOKUMENTÓW

W proponowanej formie korespondencji duży nacisk położono na bezpieczeństwo przesyłanych i przechowywanych danych. Nieuniknione zatem było zastosowanie najsilniejszych znanych obecnie programowych oraz sprzętowych środków i metod zabezpieczania informacji, dzięki którym uzyskano **niezaprzeczalność**, **integralność** oraz **poufność** danych.



NIEZAPRZECZALNOŚĆ

Ta cecha wymiany danych oznacza brak możliwości wyparcia się swego uczestnictwa w całości lub części elektronicznej wymiany danych przez jednego z uczestników wymiany dokumentów. Dzięki temu uczestnik, który wysłał np. dokument z zachowaniem jego cech niezaprzeczalności nie będzie mógł się wyprzec tego działania. Podobnie, jeśli otrzyma np. poświadczenie o złożeniu dokumentu w ZUS, to może być pewien, iż nikt inny nie mógł tego poświadczenia wystawić i że będzie mógł zawsze tego dowieść.



INTEGRALNOŚĆ DANYCH

Właściwość przypisana danym polegająca na tym, że nie zostały one zmodyfikowane lub zniszczone w nieuprawniony sposób (ani przypadkowo, ani w sposób zamierzony). Inaczej mówiąc uczestnik elektronicznej wymiany dokumentów wysyłając dane lub je odbierając, co do których jest przekonany, że zachowują integralność; jest także całkowicie pewien, iż nikt tych danych w międzyczasie nie zmodyfikował, ani też nie uzupełnił o nowe informacje.



POUFNOŚĆ

Właściwość przypisana danym przesyłanym, odbieranym lub przechowywanym polegająca na tym, że informacja nie jest osiągalna lub nie jest dostępna stronom do tego nieuprawnionym; cecha ta więc zapobiega ujawnianiu informacji, która uważana jest za istotną z punktu widzenia interesów uczestników elektronicznej

Dwie pierwsze cechy (**niezaprzeczalność** i **integralność**) osiąga się poprzez stosowanie **podpisu cyfrowego**, trzecią cechę (**poufność**) - poprzez odpowiednie szyfrowanie przesyłanych danych.

2.1 Podpis cyfrowy

Podpis cyfrowy „składany” na dokumencie przez nadawcę służy odbiorcy do jednoznacznego zidentyfikowania nadawcy (**niezaprzeczalność**) oraz do zweryfikowania treści otrzymanej wiadomości w celu stwierdzenia, że dotarła ona w postaci nie zmienionej (**integralność**).

W praktyce podpisywanie polega na tym, że nadawca (po zaakceptowaniu treści przesyłanej wiadomości) uruchamia funkcję programu, która tworzy automatycznie **podpis cyfrowy** dla tej wiadomości. **Podpis cyfrowy** tworzony jest zgodnie z przyjętymi regułami kryptograficznymi przy wykorzystaniu tajnego, unikatowego kodu zwanego **kluczem prywatnym** nadawcy. Odbiorca tej wiadomości może zweryfikować autentyczność podpisu nadawcy dzięki znajomości jego (nadawcy) jawnego, unikatowego kodu zwanego **kluczem publicznym**.

Swój klucz publiczny każdy uczestnik elektronicznej wymiany dokumentów udostępnia wszystkim pozostałym uczestnikom, z którymi prowadzi elektroniczną korespondencję. Natomiast klucz prywatny pozostaje zawsze tajny i dostępny tylko danemu użytkownikowi.

2.2 Szyfrowanie dokumentów elektronicznych

Poufność przesyłanych wiadomości drogą elektroniczną jest zapewniona przez **szyfrowanie wiadomości** przez nadawcę w taki sposób, że tylko wskazany (przez nadawcę) odbiorca może ją zdeszyfrować. Dlatego do szyfrowania nadawca wykorzystuje klucz publiczny adresata, co daje pewność, że tylko adresat posługujący się swoim kluczem prywatnym będzie w stanie zdeszyfrować wiadomość.

2.3 Obowiązki uczestników elektronicznej wymiany dokumentów

Należy podkreślić, że zastosowane metody kryptograficzne będą skuteczne tylko wtedy, gdy spełnione zostaną poniższe dwa warunki:



1. Każdy uczestnik elektronicznej wymiany dokumentów chroni swój klucz prywatny w taki sposób, że nikt poza nim nie może go w jakikolwiek sposób wykorzystać.

W przeciwnym przypadku może dojść do powstawania dokumentów fałszywych, opatrzonych podpisem uczestnika elektronicznej wymiany dokumentów.



2. Każdy uczestnik elektronicznej wymiany dokumentów musi upewnić się, że używany przez niego klucz publiczny drugiego uczestnika jest autentyczny.

W przeciwnym razie mogą zaistnieć dwa przypadki:

- ❑ posłużenie się błędnym kluczem publicznym, co uniemożliwia elektroniczną wymianę dokumentów,
- ❑ posłużenie się fałszywym kluczem publicznym, co w konsekwencji może doprowadzić do niepożądanego ujawnienia treści wysyłanego dokumentu lub przyjęcia dokumentu fałszywego jako autentycznego.

2.3.1 Ochrona klucza prywatnego

Klucz prywatny jest generowany i chroniony przez program. Dlatego uczestnik elektronicznej wymiany dokumentów musi być pewny prawidłowego działania oprogramowania, którego używa. Należy zatem instalować program licencjonowany, pochodzący z pewnego źródła.

Następnie użytkownik musi sam zadbać o to, aby z programu nie korzystały osoby nieupoważnione. W szczególności dotyczy to użycia funkcji tworzącej podpis cyfrowy. Funkcja ta może być uruchamiana tylko przez osobę upoważnioną, która jest przez program identyfikowana przede wszystkim poprzez podanie właściwego **hasła**.

Istnieją również możliwości zastosowania bardziej wyrafinowanych metod identyfikacji, które użytkownik może zastosować, jeżeli uważa to za stosowne.



Za utrzymanie w sekrecie swojego klucza prywatnego odpowiedzialny jest tylko i wyłącznie dany uczestnik elektronicznej wymiany dokumentów..

2.3.2 Autentyczność klucza publicznego

Aby być wiarygodnym uczestnikiem elektronicznej wymiany dokumentów, każdy uczestnik tej wymiany musi posiadać **certyfikat** swojego klucza publicznego, wydany i podpisany przez organ certyfikujący, pełniący rolę „zaufanej trzeciej strony” dla wszystkich uczestników.



Autentyczność klucza publicznego uczestnika elektronicznej wymiany dokumentów poświadcza „zaufana trzecia strona” poprzez wydanie odpowiedniego certyfikatu klucza publicznego.

Autentyczność organu certyfikującego można jednoznacznie zweryfikować dzięki znajomości jego klucza publicznego, który jest ogólnie dostępny (np. Internet czy biuletyn urzędowy).

2.4 Komunikat elektroniczny

W dalszej części niniejszego poradnika będzie używana nazwa „komunikat” na określenie kompletnej informacji przesyłanej między uczestnikami elektronicznej wymiany dokumentów.

Standardowy komunikat jest zawsze w postaci zaszyfrowanej i zawiera zestaw dokumentów ubezpieczeniowych, podpis cyfrowy oraz certyfikat klucza publicznego nadawcy.

3

Rozdział

STRONY BIORĄCE UDZIAŁ W ELEKTRONICZNEJ WYMIANIE DOKUMENTÓW

W elektronicznej wymianie dokumentów uczestniczą następujące strony (rys. 1):

- Płatnik składek ZUS, posługujący się aplikacją Płatnik,
- ZUS poprzez swoje terenowe jednostki organizacyjne;
- Centrum Certyfikacji Unizeto Certum czyli organ zarządzający certyfikatami kluczy publicznych uczestników elektronicznej wymiany dokumentów.

3.1 Płatnik

W dalszej części niniejszego poradnika dla określenia płatnika składek ZUS lub innego podmiotu zewnętrznego będzie używana nazwa **Płatnik składek**.

3.2 Zakład Ubezpieczeń Społecznych

ZUS uczestniczy w elektronicznej wymianie dokumentów poprzez swoje terenowe jednostki organizacyjne, w których zlokalizowane są Punkty Rejestracji (PR). Aktualny wykaz punktów rejestracji w terenowych jednostkach organizacyjnych ZUS znajduje się na stronach internetowych Zakładu pod adresem:

<http://www.zus.pl/instyt/Oddzialy/default.asp>

Płatnicy składek kontaktują się z Punktem Rejestracji tylko w wyjątkowych sytuacjach, ale wymaga to **zawsze osobistej** obecności upoważnionego przedstawiciela płatnika.

Do zadań **Punktu Rejestracji** należy:

- stwierdzenie tożsamości reprezentanta Płatnika (osoby, która w jego imieniu zgłosiła się do Punktu Rejestracji) i poprawności danych zawartych w przyjmowanych wnioskach o:

- rejestrację nowego Płatnika, który zgłasza chęć przekazywania dokumentów ubezpieczeniowych w formie elektronicznej;
 - odnowienie certyfikatu z przyczyny: modyfikacji danych identyfikacyjnych płatnika lub końca terminu ważności dotychczas posiadanego przez płatnika certyfikatu;
 - unieważnianie certyfikatu klucza publicznego Płatnika w przypadku, gdy Płatnik „zgubił” swój klucz prywatny, lub podejrzewa jego „kradzież” (skompromitowanie klucza);
- wystawianie potwierdzeń powyższych operacji.
 - rejestracja upoważnieni do występowania innych podmiotów w imieniu Płatnika podczas elektronicznej komunikacji z ZUS.

3.3 Centrum Certyfikacji Unizeto Certum

Centrum Certyfikacji Unizeto Certum związane jest z zaufanym organem zarządzającym certyfikatami klucza publicznego stron – uczestników elektronicznej wymiany danych, tzn. **Płatników** i **terenowych jednostek ZUS**. Wymiana informacji między Płatnikiem (lub jednostką organizacyjną ZUS) a Centrum Certyfikacji Unizeto Certum odbywa się tylko na drodze elektronicznej.

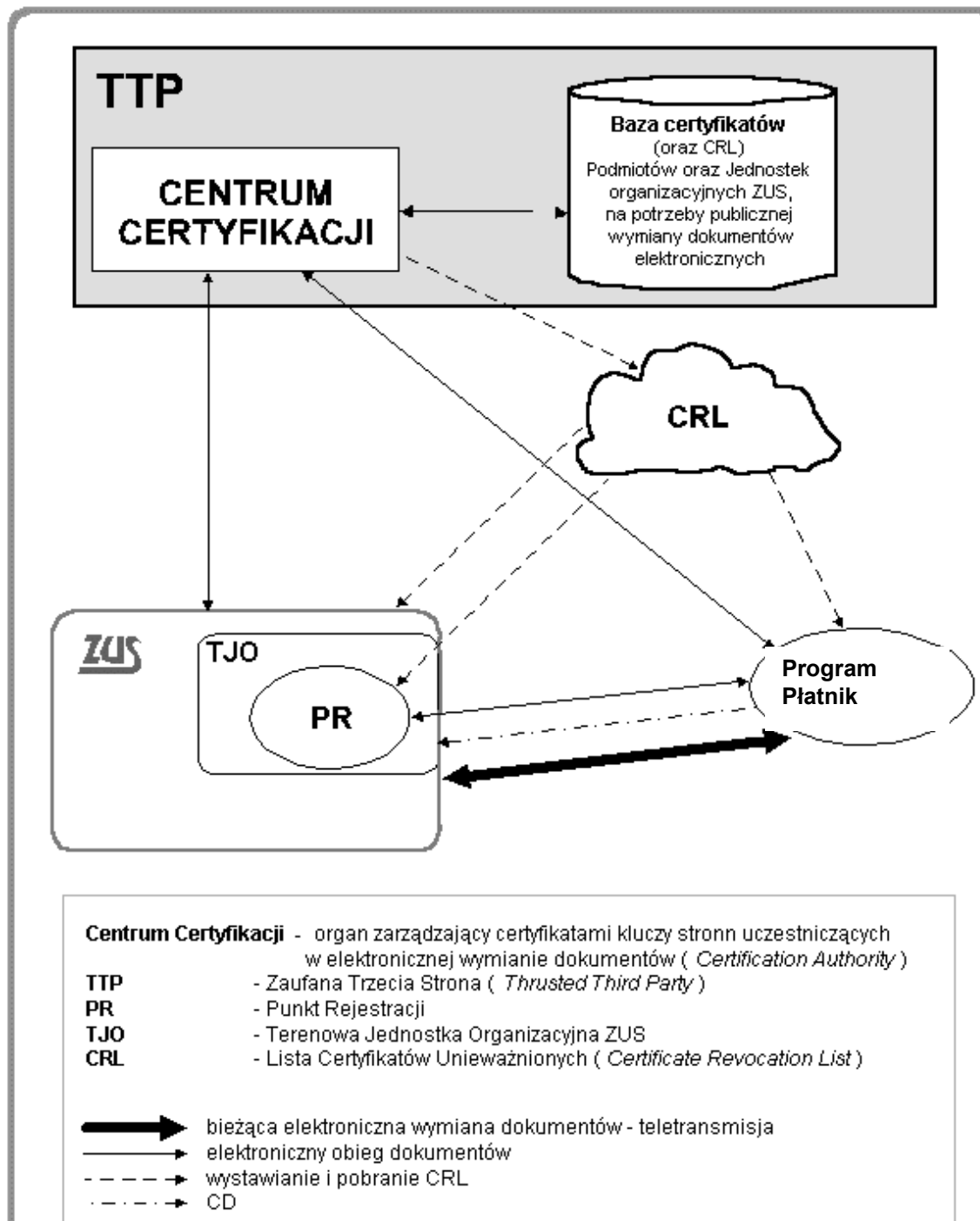
Do głównych zadań **Centrum Certyfikacji Unizeto Certum** należą:

- wydawanie certyfikatów klucza publicznego;
- unieważnianie certyfikatów klucza publicznego;
- odnawianie certyfikatów klucza publicznego (wydawanie Płatnikom nowych certyfikatów klucza publicznego w związku ze zgłoszeniem przez Płatnika nowej pary kluczy do certyfikacji, zmiany danych Płatnika mających wpływ na zawartość certyfikatu klucza publicznego);
- udostępnianie swego własnego certyfikatu klucza publicznego;
- ogłaszanie i udostępnianie listy certyfikatów unieważnionych (CRL);
- weryfikowanie wiarygodności certyfikatów klucza publicznego;
- wystawianie potwierdzenia powyższych operacji.

Funkcję Centrum Certyfikacji Unizeto Certum pełni UNIZETO Sp. z o.o.

70-486 Szczecin, ul. Królowej Korony Polskiej 21-23

tel. (091) 48 01 340 <http://www.cc.unet.pl>, e-mail: info@cc.unet.pl



4

Rozdział

SYSTEM DWUSTRONNEJ WYMIANY INFORMACJI

Zakład Ubezpieczeń Społecznych realizując kolejny etap usprawniania wymiany informacji pomiędzy płatnikiem składek i Zakładem rozszerzył dotychczasową funkcjonalność elektronicznego kanału informacyjnego.

Nowy elektroniczny kanał informacyjny - System Dwustronnej Wymiany Informacji (SDWI) pomiędzy płatnikiem składek i Zakładem zapewnia możliwość wysłania dokumentów i odbioru potwierdzeń odbioru.

Nowy elektroniczny kanał informacyjny ma za zadanie usprawnienie i stopniowe rozszerzanie wymiany informacji między płatnikami składek a ZUS. Pozwala on na stosowanie upoważnień dla osób fizycznych i prawnych do przekazywania dokumentów w imieniu firmy, ponadto podnosi wydajność i zwiększa bezpieczeństwo przesyłania dokumentów ubezpieczeniowych oraz odbioru potwierdzeń i komunikatów.

Odbierania informacji zwrotnej w SDWI odbywa się z dowolnego węzła internetowego.

SDWI działa równolegle z dotychczasowym systemem przekazu elektronicznego, a sposób wysyłania dokumentów ubezpieczeniowych w formie elektronicznej bezpośrednio z programu lub za pośrednictwem serwerów WWW nie uległ zmianie.



SDWI ze względów bezpieczeństwa systemu informatycznego nie będzie obsługiwał wysyłania dokumentów poprzez pocztę elektroniczną.

Każdy płatnik, który już przekazuje do ZUS dokumenty drogą elektroniczną może uruchomić SDWI na swoim komputerze. Aby korzystanie z nowej usługi było możliwe niezbędne jest:

- zainstalowanie na komputerze programu Płatnik w wersji 6.03.001,
- zainstalowanie pakietu aktywującego kanał SDWI, który znajduje się na płycie CD wraz z programem Płatnik,
- aktywowanie SDWI poprzez wybranie z menu programu Płatnik funkcji "Przekaz" / "Ustawienia przekazu elektronicznego" / "Metoda przekazu" i zaznaczenie opcji "System Dwustronnej Wymiany Informacji",
- skonfigurowanie programu Płatnik tak, aby wysyłał dokumenty na serwer obsługujący SDWI (informacja, które serwery ZUS obsługują SDWI jest publikowana w serwisie <http://e-inspektorat.zus.pl> .

PRZEKAZYWANIE DOKUMENTÓW W IMIENIU PŁATNIKA

Zgodnie z obowiązującymi przepisami każdy płatnik zobowiązany do przekazywania dokumentów ubezpieczeniowych do ZUS w formie elektronicznej może upoważnić do tych czynności inną osobę fizyczną lub prawną (Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 3 lipca 2001 roku w sprawie warunków, jakie muszą spełnić płatnicy składek przekazujący dokumenty ubezpieczeniowe w formie dokumentu elektronicznego poprzez teletransmisję danych (Dz. U. Nr 73 poz. 774).

Od momentu wdrożenia SDWI wszystkie podmioty przekazujące dokumenty elektroniczne do ZUS w imieniu innych płatników, będą zobowiązane do rejestracji upoważnień w terenowej jednostce organizacyjnej ZUS (na zasadach podobnych, jak dotychczas przebiega proces uzyskiwania przez płatnika składek certyfikatu klucza publicznego). Przedstawiciel płatnika składek lub podmiotu upoważnionego (np. biura rachunkowego) zgłasza się w jednostce terenowej ZUS wraz z dokumentami potwierdzającymi tożsamość firm i osoby zgłaszającej wnioski oraz pisemnym pełnomocnictwem upoważniającym do działania w imieniu płatnika. Pracownik ZUS zarejestruje w bazie danych Zakładu dane upoważniającego płatnika i upoważnionego podmiotu.

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych przekazywanych w formie elektronicznej między płatnikiem a ZUS wprowadzono system rejestracji upoważnień. Płatnik składek, który chce upoważnić inny podmiot do przekazywania w jego imieniu danych do ZUS musi ten fakt zgłosić do Zakładu. Informacje o upoważnieniach są rejestrowane przez ZUS w bazie danych i służą do weryfikacji, czy dany podmiot jest upoważniony przez płatnika do przekazywania w jego imieniu dokumentów ubezpieczeniowych i otrzymywania danych z ZUS. Dzięki informacjom zawartym w bazie upoważnień zmniejszone zostanie prawdopodobieństwo wystąpienia sytuacji, w której osoba nieuprawniona będzie mogła występować w imieniu płatnika w procesie elektronicznej komunikacji z ZUS.

Rozdział ten zawiera opis wszystkich procedur, które zostały opracowane i zaimplementowane w systemie w celu uregulowania zasady obsługi upoważnień w systemie SDWI.

Procedury te wykonywane są przez płatników składek (lub osoby przez nich upoważnione), którzy chcą upoważnić inny podmiot do przekazywania w swoim imieniu dokumentów ubezpieczeniowych w ramach Systemu Dwustronnej Wymiany

Informacji. Płatnik lub podmiot przez niego upoważniony zgłasza się w jednostce terenowej ZUS w następujących sytuacjach:

- rejestracji upoważnienia,
- modyfikacji upoważnienia,
- unieważnienia upoważnienia.

Każde zarejestrowane upoważnienie zawiera:

- datę rejestracji,
- dane identyfikacyjne płatnika składek, który występuje w roli upoważniającego,
- dane identyfikacyjne podmiotu upoważnianego (te same, które zostały wpisane do wydanego dla tego podmiotu certyfikatu klucza publicznego) - w tej roli może wystąpić inny płatnik składek lub osoba nie będąca płatnikiem,
- zakres wydanego upoważnienia - obecnie upoważnienie może obejmować: wysyłanie dokumentów i odbieranie potwierdzeń,
- okres wydanego upoważnienia - obecnie upoważnienie można wydać na czas określony (określając datę początku i końca jego obowiązywania) lub bezterminowo (określając jedynie datę początku jego obowiązywania).

Ponadto płatnik lub podmiot upoważniony zawsze ma możliwość zgłoszenia się w celu ustalenia, czy w ZUS zarejestrowane są jakieś upoważnienia, których jest on stroną upoważniającą lub upoważnioną.

Do dokumentów umożliwiających zarejestrowanie/modyfikację/unieważnienia upoważnienia należą:

- kopia umowy zawarta z biurem rachunkowym lub kopia pełnomocnictwa wystawionego przez płatnika dla biura rachunkowego względnie upoważnienia wystawionego przez płatnika dla biura rachunkowego do prowadzenia rozliczeń z Zakładem Ubezpieczeń Społecznych
- decyzja w sprawie nadania numeru identyfikacji podatkowej, zawierającej numer NIP (lub jej kopii),
- zaświadczenie z Urzędu Statystycznego o otrzymaniu w systemie identyfikacji podmiotów gospodarki narodowej REGON statystycznego numeru identyfikacyjnego REGON oraz nazwie pełnej i skróconej płatnika (lub kopia),
- dowód tożsamości osoby zgłaszającej upoważnienie
- pisemne pełnomocnictwo dla przedstawiciela biura rachunkowego do działania w jego imieniu,



5.1. Szczegółowe procedury obsługi upoważnień

Rejestracja upoważnienia:

Płatnik składek musi przejść procedurę rejestracji upoważnienia jeżeli chce, aby w jego imieniu wskazany przez niego podmiot przekazywał do ZUS dokumenty ubezpieczeniowe w formie elektronicznej.

Rejestracja upoważnienia ma na celu jednoznaczne potwierdzenie tożsamości płatnika upoważniającego i podmiotu upoważnianego – wymaga to osobistej obecności płatnika lub upoważnionego przez niego przedstawiciela w jednostce terenowej ZUS.

1. Z dokumentami potwierdzającymi tożsamość upoważniającego oraz upoważnianego, płatnik składek lub osoba przez niego upoważniona udaje się

do jednostki terenowej ZUS i przedstawia je do wglądu pracownikowi Zakładu.

Do upoważnienia należy podać te same dane identyfikacyjne podmiotu upoważnionego jakie są wykorzystywane w jego certyfikacie klucza publicznego którym podpisuje przesyłki przekazywane w imieniu płatnika do ZUS.

2. Pracownik ZUS na podstawie przedstawionych dokumentów wprowadza do bazy danych odpowiednie upoważnienie.
3. Płatnik składek lub podmiot składający wniosek otrzymuje (w formie papierowej) potwierdzenie rejestracji upoważnienia.
4. Zarejestrowane upoważnienie jest aktywne w systemie od następnego dnia po rejestracji.

Modyfikacja upoważnienia:

Dane zawarte we wcześniej zarejestrowanym upoważnieniu można zmodyfikować ze względu na:

- zmianę danych płatnika upoważniającego lub podmiotu upoważnionego,
- zmianę zakresu upoważnienia.

Płatnik upoważniający powinien w upoważnieniu dokonać zmian w przypadku, kiedy uległy zmianie jego dane identyfikacyjne, a płatnik złożył odpowiedni dokument zmiany danych ZUS ZIPA.

Zmiany danych podmiotu upoważnionego należy dokonać w przypadku, kiedy zmieniły się jego dane w certyfikacie klucza publicznego, którym podpisuje przesyłki przekazywane w imieniu płatnika do ZUS. Dane identyfikacyjne podmiotu upoważnionego zapisane w upoważnieniu i w certyfikacie powinny być takie same.

Zmiany zakresu upoważnienia należy dokonać w przypadku, kiedy zachodzi konieczność zmiany okresu, na jaki zostało ono wydane lub zmiany jego zakresu np. gdy trzeba zmienić upoważnienie wydane na czas określony na bezterminowe.

Jednocześnie można dokonać zmian w całym zakresie upoważnienia; oznacza to że realizując tę procedurę można zmodyfikować upoważnienie we wszystkich zakresach jednocześnie.

Rejestracja modyfikacji upoważnienia wymaga osobistej obecności płatnika lub upoważnionego przez niego przedstawiciela w jednostce terenowej ZUS wraz z dokumentami potwierdzającymi jego tożsamość.

1. W przypadku modyfikacji danych płatnika w upoważnieniu, płatnik składek lub osoba przez niego upoważniona udaje się do jednostki terenowej ZUS wraz z dokumentami potwierdzającymi jego tożsamość.

W przypadku modyfikacji danych podmiotu upoważnionego płatnik składek (lub osoba przez niego upoważniona) lub przedstawiciel podmiotu upoważnionego udaje się do jednostki terenowej ZUS wraz z dokumentami potwierdzającymi jego tożsamość.

W przypadku modyfikacji upoważnienia w zakresie okresu na jaki zostało wydane i/lub jego zakresu, płatnik składek (lub osoba przez niego upoważniona) lub

przedstawiciel podmiotu upoważnionego udaje się do jednostki terenowej w ZUS wraz z dokumentami potwierdzającymi jego tożsamość.

2. Pracownik ZUS na podstawie przedstawionych dokumentów wprowadza do bazy danych odpowiednie zmiany w upoważnieniu.
3. Płatnik składek lub podmiot składający wniosek otrzymuje (w formie papierowej) potwierdzenie modyfikacji upoważnienia.
4. Zarejestrowane zmiany w upoważnieniu są aktywne w systemie od następnego dnia po rejestracji.

Unieważnienie upoważnienia:

Płatnik w każdej chwili może wycofać (unieważnić) upoważnienie wydane dla danego podmiotu. Również podmiot upoważniony może wycofać (unieważnić) upoważnienie. Od momentu unieważnienia upoważnienia dany podmiot nie będzie mógł w imieniu płatnika przekazywać do ZUS dokumentów ubezpieczeniowych w formie elektronicznej.

Po unieważnieniu upoważnienia nie ma możliwości ponownego uaktywnienia tego upoważnienia. Jeżeli płatnik chce ponownie upoważnić ten sam podmiot musi ponownie wykonać procedurę rejestracji upoważnienia.

Rejestracja unieważnienia upoważnienia wymaga osobistej obecności płatnika lub upoważnionego przez niego przedstawiciela w jednostce terenowej ZUS wraz z dokumentami potwierdzającymi jego tożsamość.

1. W przypadku unieważnienia upoważnienia przez płatnika, płatnik składek lub osoba przez niego upoważniona udaje się do wybranej jednostki terenowej ZUS wraz z dokumentami potwierdzającymi jego tożsamość.

W przypadku unieważnienia upoważnienia przez podmiot upoważniony, przedstawiciel podmiotu upoważnionego udaje się do jednostki terenowej ZUS wraz z dokumentami potwierdzającymi jego tożsamość.

2. Pracownik ZUS na podstawie przedstawionych dokumentów unieważnia upoważnienie. Jeśli wniosek składany jest przez płatnika, sprawdzana jest również zgodność danych płatnika z danymi w Centralnym Rejestrze Płatników. W przypadku niezgodności danych płatnika zawartych w danych do upoważnienia z danymi w Centralnym Rejestrze Płatników, płatnik otrzymuje informację o konieczności aktualizacji danych w Punkcie Informacyjnym.
3. Płatnik składek lub podmiot składający wniosek otrzymuje (w formie papierowej) potwierdzenie unieważnienia upoważnienia.
4. Unieważnienie upoważnienia jest aktywne w systemie od następnego dnia po rejestracji.

6

Rozdział

BIEŻĄCA ELEKTRONICZNA WYMIANA DOKUMENTÓW POMIĘDZY PŁATNIKIEM A ZUS

Bieżącą wymianę dokumentów elektronicznych z ZUS płatnik może prowadzić:

- Bezpośrednio z programu Płatnik z wykorzystaniem wcześniej zdefiniowanego w systemie połączenia do sieci Internet.
- drogą teletransmisji do ZUS, z wykorzystaniem sieci Internet. Przekazywanie dokumentów może być zrealizowane poprzez łącze stałe, jak również poprzez modem telefoniczny, ale dopiero po odpowiednim skonfigurowaniu połączenia do sieci Internet. Obecnie dokumenty ubezpieczeniowe można przekazywać do ZUS z wykorzystaniem następujących adresów stron internetowych:

Dla dotychczasowego sposobu przekazywania dokumentów:

- www.dokumenty.wroclaw.zus.pl

Dla Systemu Dwustronnej Wymiany Informacji:

- <https://www.sdwi.gdansk.zus.pl>
- <https://www.sdwi.warszawa.zus.pl>
- <https://www.sdwi.wroclaw.zus.pl>
- poprzez nośniki – płyta CD-ROM przekazywana do najbliższej jednostki ZUS. Przekazywanie dokumentów na CD-ROM możliwe jest tylko dla płatników składek po wcześniejszym uzyskaniu zgody ZUS.



Niezależnie od sposobu przekazywania dokumentów elektronicznych do ZUS, do ich sporządzenia Płatnik musi posiadać certyfikat swojego klucza publicznego oraz certyfikat klucza publicznego ZUS.



Certyfikat klucza publicznego ZUS Płatnik otrzymuje w Punkcie Rejestracji razem z potwierdzeniem wniosku o rejestrację. Certyfikat jest automatycznie rejestrowany w programie Płatnik przy rejestracji potwierdzenia.

Program Płatnik umożliwia przygotowanie dokumentów ubezpieczeniowych i ich wysyłkę. Dokumenty te uzyskują postać komunikatu, gotowego do przesłania do ZUS.

Komunikat zawiera w postaci zaszyfrowanej dokument, podpis cyfrowy i certyfikat płatnika. ZUS deszyfruje otrzymany komunikat, weryfikuje podpis cyfrowy płatnika oraz autentyczność dokumentu.

Następnie ZUS dla komunikatów przesłanych drogą teletransmisji tworzy potwierdzenia otrzymania dokumentów oraz poprawności ich struktury. Potwierdzenie takie w postaci komunikatu, czyli podpisanej i zaszyfrowanej wiadomości, może być przez Płatnika pobrane przy pomocy programu Płatnik lub przeglądarki, z odpowiedniej strony internetowej ZUS.

Program obsługujący elektroniczną wymianę dokumentów weryfikuje wiarygodność certyfikatu poprzez sprawdzenie: terminu ważności certyfikatu, autentyczności i integralności podpisu złożonego w certyfikacie przez Centrum Certyfikacji Unizeto Certum oraz upewnia się, że dany certyfikat nie został umieszczony na liście certyfikatów unieważnionych (CRL).

6.1. Automatyczne wysyłanie dokumentów bezpośrednio z programu Płatnik

Program PŁATNIK umożliwia automatyczne przekazywanie do ZUS przygotowanych zestawów dokumentów oraz pobieranie dla nich potwierdzeń odbioru. Przesyłanie dokumentów do ZUS drogą elektroniczną przy wykorzystaniu programu PŁATNIK wymaga zainstalowanego i właściwie skonfigurowanego modemu lub dostępu do Internetu przez sieć korporacyjną.

Aby wysłać zestaw dokumentów bezpośrednio z programu należy:

1. Ustawić w programie w parametrach przekazu elektronicznego opcję automatycznego wysyłania oraz wybrać serwer, do którego mają być przekazane dokumenty,
2. Uruchomić funkcję wysyłania dla wybranego zestawu dokumentów, program automatycznie uruchomi połączenie z wybraną stroną internetową ZUS na podstawie domyślnie zdefiniowanego w systemie połączenia,
3. Po przekazaniu dokumentów do ZUS identyfikator potwierdzenia zostanie automatycznie pobrany i zapisany w programie,

Aby pobrać bezpośrednio z programu Płatnik potwierdzenie odbioru dla wysłanych zestawów należy:

1. Otworzyć zestaw dokumentów, do którego będzie pobierane potwierdzenie odbioru (wybrany zestaw musi mieć status Wysłany i mieć zarejestrowany identyfikator potwierdzenia),
2. W oknie „Zestaw dokumentów” z menu „Narzędzie” wybrać polecenie „Pobierz i rejestruj potwierdzenie”, program automatycznie uruchomi połączenie z wybraną stroną internetową ZUS na podstawie domyślnie zdefiniowanego w systemie połączenia,
3. Potwierdzenie odpowiadające danej przesyłce zostanie pobrane i zarejestrowane w programie, treść potwierdzenia oraz lokalizacja pliku z potwierdzeniem jest widoczna w oknie „Zestaw dokumentów” w zakładce „Wysyłka”,

6.2. Przygotowanie nośnika CD zawierającego dokumenty ubezpieczeniowe

Jednym ze sposobów przekazywania dokumentów ubezpieczeniowych do ZUS jest dostarczenie ich na nośniku CD. Korzystanie z tego sposobu przekazywania dokumentów możliwe jest po wcześniejszym uzyskaniu zgody z ZUS. Utworzenie nośnika zawierającego dokumenty ubezpieczeniowe polega na wcześniejszym przygotowaniu zestawu dokumentów w programie Płatnik, a następnie zapisaniu go na nośniku CD.

Aby przygotować nośnik CD z dokumentami ubezpieczeniowymi, które mogą być przekazane do ZUS należy:

1. Ustawić w programie w parametrach przekazu elektronicznego opcję przekazu dokumentów na płytach CD,
2. Uruchomić funkcję wysyłania dla wybranego zestawu dokumentów, program automatycznie przygotowuje odpowiednio zaszyfrowany plik (plik o rozszerzeniu *.szyfr) i zapisze go we wskazanej przez użytkownika lokalizacji na dysku komputera,
3. Nagrać przygotowany plik z dokumentami na nośnik CD,
4. Dostarczyć płytę CD na stanowisko przyjmowania dokumentów na nośnikach w jednostce ZUS,
5. Pracownik ZUS wysyła zapisany na płycie CD zestaw dokumentów na serwer przyjmowania dokumentów elektronicznych a następnie przekazuje płatnikowi wydruk zawierający informację potwierdzającą przesłanie dokumentów oraz identyfikator potwierdzenia danej wysyłki.



Nagrywanie na nośnik CD odbywa się przy wykorzystaniu oprogramowania dostarczanego wraz z nagrywarką. Oprogramowanie takie nie jest elementem aplikacji Płatnik.



Nagrywanie dokumentu elektronicznego na nośnik CD powinno odbywać się w sposób pozwalający na późniejsze dopisanie kolejnych dokumentów elektronicznych.

6.3. Przesyłanie dokumentów ubezpieczeniowych drogą teletransmisji

Przesyłanie dokumentów do ZUS drogą elektroniczną wymaga zainstalowania przeglądarki internetowej. Przesłanie danych tą drogą polega na wcześniejszym przygotowaniu zestawu dokumentów ubezpieczeniowych i przetworzeniu go do postaci zaszyfrowanego oraz podpisanego dokumentu elektronicznego przy pomocy programu Płatnik, a następnie przesłaniu go do ZUS za pośrednictwem odpowiedniej strony internetowej.



Strony internetowe udostępnione Płatnikom do przekazywania plików z dokumentami:

- <http://www.dokumenty.wroclaw.zus.pl>
- <https://www.sdwi.gdansk.zus.pl>
- <https://www.sdwi.warszawa.zus.pl>
- <https://www.sdwi.wroclaw.zus.pl>

Poniżej przedstawione zostały kolejno czynności, których prawidłowe wykonanie gwarantuje przesłanie dokumentów ubezpieczeniowych do ZUS:



Przesłanie dokumentu elektronicznego do ZUS wymaga posiadania zainstalowanego i skonfigurowanego modemu lub stałego łącza internetowego.

1. Ustawić w programie w parametrach przekazu elektronicznego opcję samodzielnego przekazywania dokumentów za pośrednictwem stron WWW,
2. Uruchomić funkcję wysyłania dla wybranego zestawu dokumentów, program automatycznie przygotuje odpowiednio zaszyfrowany plik (plik o rozszerzeniu *.szyfr) i zapisze go we wskazanej przez użytkownika lokalizacji na dysku komputera,



Aby móc nawiązać połączenie ze swoją skrytką SDWI należy:

zainstalować przeglądarkę internetową o sile szyfrowania 128 bitów (siłę szyfrowania można sprawdzić w oknie przeglądarki *Informacje o programie*), zarejestrować w przeglądarce certyfikat (wraz z kluczem prywatnym) wskazany w programie PŁATNIK jako certyfikat do komunikacji z ZUS.

Szczegółowy opis przygotowania przeglądarki www do połączenia z SDWI jest zamieszczony w dokumencie „Program Płatnika Podręcznik administratora” rozdział „Połączenie ze skrytką SDWI”.

3. Połączyć się z wybraną stroną internetową ZUS i przejść do części „Strona wysyłania elektronicznych dokumentów do ZUS”,

4. Korzystając z polecenia „Przełączaj” wskazać na dysku komputera wcześniej utworzony i zaszyfrowany plik z dokumentami (plik o rozszerzeniu *.szyfr) i wybrać polecenie „Wyślij”,
5. Po zakończeniu transmisji pliku identyfikator potwierdzenia zostanie wyświetlony na ekranie. Należy go skopiować i zapisać w programie korzystając z polecenia „Wprowadź identyfikator potwierdzenia” dostępnego z menu „Narzędzia” w otwartym oknie zestawu dokumentów,

Po wysłaniu dokumentów należy pobrać potwierdzenie ich odbioru. Potwierdzenie odbioru zawsze jest dostępne tylko na tej samej stronie internetowej, na którą wysłany został dany zestaw.

Potwierdzenie można pobrać automatycznie, bezpośrednio z programu Płatnik (sposób ten jest opisany w rozdziale 5.1) lub manualnie, pobierając plik potwierdzenia bezpośrednio ze strony internetowej.

Manualne pobieranie potwierdzenia odbioru dla wysłanego zestawu:

1. Połączyć się z wybraną stroną internetową ZUS, na którą wcześniej został wysłany zestaw dokumentów i przejść do części „Strona pobierania potwierdzenia wysłania dokumentów elektronicznych do ZUS”,
2. W polu „Identyfikator przesyłki” wprowadzić numer identyfikatora przesyłki i wybrać polecenie „Pobierz”,
3. Na ekranie zostanie wyświetlone okno, w którym należy wskazać gdzie na dysku komputera ma zostać zapisany plik z potwierdzeniem i wybrać polecenie „Zapisz”,
4. Jeżeli przesłany zestaw dokumentów zawierał błędy na stronie internetowej, do pobrania będzie dodatkowy plik zawierający ich opis. W celu pobrania tego pliku należy wybrać polecenie „Pobierz plik informacyjny” i wskazać miejsce na dysku gdzie ma on być zapisany na dysku komputera,
5. Otworzyć zestaw dokumentów, do którego będzie pobierane potwierdzenie odbioru (wybrany zestaw musi mieć status Wysłany i mieć zarejestrowany identyfikator przesyłki),
6. W oknie Zestaw dokumentów z menu „Narzędzia” wybrać polecenie „Rejestruj potwierdzenie z pliku”,
7. Na ekranie zostanie wyświetlone okno w którym należy wskazać, gdzie na dysku komputera znajduje się plik z potwierdzeniem i wybrać polecenie „Otwórz”,
8. Potwierdzenie odpowiadające danej przesyłce zostanie zarejestrowane w programie, treść potwierdzenia oraz lokalizacja pliku z potwierdzeniem jest widoczna w oknie „Zestaw dokumentów” w zakładce „Wysyłka”.

ZAŁĄCZNIK - SŁOWNIK PODSTAWOWYCH TERMINÓW I SKRÓTÓW

Centrum Certyfikacji Unizeto Certum – (*Certification Authority*) organ zarządzający certyfikatami kluczy publicznych uczestników elektronicznej wymiany dokumentów, wymiana informacji następuje wyłącznie na drodze elektronicznej. <http://www.cc.unet.pl>, e-mail: info@cc.unet.pl

Prowadzone przez: UNIZETO Sp. z o.o., ul. Królowej Korony Polskiej 21-23, 70-486 Szczecin, tel. (091) 423 30 41, e-mail: info@unizeto.com.pl

Certyfikat klucza publicznego – dokument elektroniczny wydany przez Centrum Certyfikacji Unizeto Certum zawierający dane identyfikacyjne Płatnika, jego klucza publiczny oraz początek i koniec okresu ważności certyfikatu klucza publicznego.

CRL – (*Certificate Revocation List*) Lista certyfikatów unieważnionych.

Elektroniczna wymiana dokumentów – korespondencja dokumentów elektronicznych za pomocą sieci Internet.

Klucz - Ciąg symboli, od którego w sposób istotny zależy wynik przekształcenia kryptograficznego (np. szyfrowania, deszyfrowania, podpisywania lub weryfikacji podpisu).

Klucz prywatny – tajny, unikatowy kod wykorzystywany przy tworzeniu podpisu cyfrowego nadawcy, dostępny tylko danemu użytkownikowi.

W **systemie podpisu asymetrycznego** klucz prywatny wykorzystywany jest do **podpisywania** wiadomości przez nadawcę. W **systemie szyfrowania asymetrycznego** klucz prywatny używany jest do **deszyfrowania** wiadomości przez odbiorcę wiadomości.

Klucz publiczny – jawny, unikatowy kod służący odbiorcy do zweryfikowania autentyczności podpisu nadawcy wiadomości, udostępniony przez nadawcę wszystkim uczestnikom, z którymi prowadzi elektroniczną wymianę dokumentów.

W **systemie podpisu asymetrycznego** klucz publiczny wykorzystywany jest do **weryfikowania** elektronicznego podpisu wiadomości przez odbiorcę wiadomości. W **systemie szyfrowania asymetrycznego** klucz publiczny używany jest do **szyfrowania** wiadomości przez nadawcę wiadomości.

Komunikat elektroniczny – kompletna informacja przesyłana między uczestnikami elektronicznej wymiany dokumentów, zawsze w postaci zaszyfrowanej, najczęściej zawiera dokument, podpis cyfrowy i certyfikat klucza publicznego nadawcy.

Kryptologia – dziedzina wiedzy obejmująca zagadnienia związane z ukrywaniem wiadomości (danych) przed osobami nieupoważnionymi poprzez szyfrowanie i odtwarzanie (deszyfrowanie) przez osoby upoważnione (kryptografia) lub nieupoważnione (kryptoanaliza).

NIP - Numer Identyfikacyjny Podatnika.

PESEL - Powszechny Elektroniczny System Ewidencji Ludności.

Płatnik – Płatnik składek ZUS.

podmiot (podmiot certyfikatu) - Właściciel **klucza prywatnego**, stanowiącego parę z **kluczem publicznym**. Określenie podmiot może odnosić się zarówno do wyposażenia lub urządzenia, przechowującego klucz prywatny, jak też do osoby fizycznej bądź prawnej (jeśli taka istnieje), która ma pod kontrolą to wyposażenie lub urządzenie. Podmiotowi przydzielana jest jednoznaczna nazwa, która wiąże go z kluczem publicznym zawartym w **certyfikacie**.

Podpis cyfrowy – Przekształcenie kryptograficzne danych, umożliwiające odbiorcy danych sprawdzenie autentyczności i integralności danych oraz zapewniające nadawcy i odbiorcy ochronę przed sfałszowaniem danych. Składany na dokumencie przez nadawcę, służy odbiorcy do jednoznacznego zidentyfikowania nadawcy oraz do stwierdzenia, że otrzymana wiadomość dotarła w postaci nie zmienionej.

Podpisywanie - Proces, który na wejściu pobiera wiadomość do podpisania i **klucz prywatny**, a na wyjściu zwraca wiadomość podpisaną. Podpisy cyfrowe tworzone są przy zastosowaniu algorytmów asymetrycznych.

Polityka certyfikacji - Dokument w postaci zestawu reguł, które są ściśle przestrzegane przez organ wydający certyfikaty w trakcie świadczenia przez niego usług certyfikacyjnych.

Punkt Rejestracji – Zaufana osoba prawna, działająca na podstawie upoważnienia **organu certyfikacji**, rejestrująca inne osoby prawne i fizyczne oraz przydzielająca im unikalne wartości (nazwa, identyfikator). Punkt Rejestracji, zlokalizowany w ZUS, z którym Płatnik kontaktuje się tylko w wyjątkowych sytuacjach i zawsze osobiście.

Program Płatnik – program komputerowy stosowany w systemie elektronicznej wymiany dokumentów, korespondencji Płatnika z jednostkami organizacyjnymi ZUS.

REGON - Państwowy Rejestr Podmiotów Gospodarczych.

Rejestracja Płatnika – ma na celu jednoznaczne potwierdzenie tożsamości Płatnika przystępującego do elektronicznej wymiany dokumentów.

SDWI - System Dwustronnej Wymiany Informacji

System kryptograficzny – system, w którym dokonuje się szyfrowania i deszyfrowania wiadomości

System podpisywania asymetrycznego - System uwierzytelniania oparty na algorytmach asymetrycznych, którego przekształcenie z udziałem klucza publicznego jest wykorzystywane do weryfikacji, a przekształcenie z udziałem klucza prywatnego jest wykorzystywane do podpisywania (patrz też podpis cyfrowy).

System szyfrowania asymetrycznego - Zestaw przekształceń tekstu jawnego w tekst zaszyfrowany i odwrotnie, w którym przekształcenia są definiowane przez algorytmy (funkcje matematyczne) i stosowane po wyborze kluczy. Przekształcenie z udziałem klucza publicznego jest wykorzystywane do szyfrowania, a przekształcenie z udziałem klucza prywatnego do deszyfrowania.

Szyfrowanie - Kryptograficzne przekształcenie danych, którego wynikiem jest tekst zaszyfrowany.

TJO – Terenowa Jednostka Organizacyjna ZUS.

TTP – (*Trusted Third Party*) Zaufana Trzecia Strona, niezależna instytucja darzona zaufaniem przez wszystkich uczestników systemu, świadcząca wiarygodne usługi związane z bezpieczeństwem danych, zarządzająca m.in. certyfikatami kluczy publicznych.

Użytkownik (certyfikatu) - Uprawniony podmiot, posługujący się certyfikatem jako właściciel, odbiorca lub strona ufająca, z wyłączeniem organu certyfikacji.

Weryfikacja podpisu - Proces, który na wejściu pobiera wiadomość podpisaną i klucz publiczny, a na wyjściu zwraca ważny lub nieważny wynik weryfikacji podpisu.

ZUS - Zakład Ubezpieczeń Społecznych.